Los servicios de seguridad

Diego Torrente

PID_00208849

UOC
Universitat Oberta de Catalunya

Índice

Introducción

El presente módulo se dedica a explicar cómo se planifican y gestionan los servicios de seguridad. Se comienza por aclarar que la seguridad y el riesgo se pueden analizar desde diferentes perspectivas académicas. Según la perspectiva que se adopte, las categorías de análisis son también distintas. Tanto la seguridad privada como la pública pueden analizar los riesgos desde cualquiera de ellas. También pueden seleccionar cualquier tipo de estrategia de seguridad a la hora de planificar, gestionar, o evaluar su actividad. De todas formas, la perspectiva racionalista es la más empleada por el sector privado de la seguridad. También las estrategias preventivas son las más utilizadas. Por todo ello, buena parte del módulo se dedica a explicar cómo se evalúan riesgos, o se realiza un plan de seguridad desde estas ópticas.

Objetivos

Los objetivos del módulo son:

1. Conocer las diferentes perspectivas en el análisis de riesgos.
2. Dominar el proceso utilizado en el análisis racional de riesgos.
3. Conocer el proceso de planificación, gestión, y evaluación de la seguridad.
4. Comprender las diferentes estrategias utilizadas en seguridad.
5. Entender cómo influyen las demandas de los clientes en los servicios.
6. Entender qué rol juega la tecnología en los servicios de seguridad.
7. Comprender la importancia del riesgo como factor en los servicios.

1. Análisis y gestión de la seguridad

La presente unidad tiene el objetivo de mostrar los fundamentos analíticos en los que se apoyan los servicios de seguridad, tanto públicos como privados. El apartado plantea tanto cuestiones teóricas como aplicadas. En primer lugar, se analiza el modelo de análisis racional de riesgos. Este es el marco más usado por el sector privado y, por ello, se le dedica más atención.

En el punto segundo se presentan otros modelos de análisis, como el psicológico, el sociológico, y otros. El siguiente apartado presenta la cuestión de la planificación y gestión de la seguridad. Estas se analizan también desde una perspectiva principalmente racionalista. Se discute qué es un plan de seguridad, y qué elementos lo forman. Se explica en qué consiste la gestión de riesgos y se comentan brevemente casos específicos como la gestión de emergencias. Finalmente, se explica qué es la evaluación, para qué sirve, qué modalidades existen, y qué criterios se pueden utilizar.

1.1. Análisis racional de riesgos

Se puede definir el "riesgo" como la posibilidad/probabilidad de que ocurra una situación adversa. Esa situación no deseada puede desencadenarse por una decisión propia, una situación del entorno, o la acción de una tercera persona. La idea de riesgo tiene dos componentes principales:

- un juicio de valor sobre unos resultados que no se desean, o que se ven como negativos, y cuyo impacto o daño se calcula;
- la estimación de una probabilidad/posibilidad de que ocurran esos resultados.

Expresado como fórmula sería:

R = D × P (Riesgo = Magnitud del daño × Probabilidad de que ocurra).

El concepto se suele utilizar en contextos donde hay una acción o decisión humana por medio. Se suele reservar el término *peligro* para designar un suceso desfavorable en el que no media una decisión humana (un azar de la naturaleza, un suceso no imputable al factor humano).

Se habla de *incertidumbre* cuando se desconocen tanto los posibles resultados (no se sabe si serán positivos o negativos), como la probabilidad de su ocurrencia. La diferencia fundamental entre riesgo e incertidumbre es que, en la

primera, asumimos que es calculable y gestionable; en el segundo caso, los cálculos no son posibles y la gestión resulta mucho más difícil. En el mejor de los supuestos, solo podemos dibujar posibles escenarios inciertos.

Por ejemplo, es lo que hacen los militares cuando tienen que ocupar un país y no saben exactamente qué va a pasar porque hay cientos de variables en juego. Algo similar ocurre en la vida política. En estos casos, se desconocen los *outputs* de la acción (los resultados posibles, ya sean buenos o malos). Ello hace muy difícil anticipar los acontecimientos, sus implicaciones y consecuencias. También se desconocen qué variables relevantes influyen en la acción y podrían ayudar a tomar una buena decisión. Como no es posible establecer relaciones causa/efecto, es casi imposible marcar objetivos o priorizarlos. Por otra parte, se desconocen las probabilidades de que ocurra nada. Con esas condiciones, generar conocimiento es prácticamente imposible.

La noción de riesgo forma parte de nuestra cultura colectiva y de la sociedad moderna. Pensamos y gestionamos el mundo en términos de riesgos y oportunidades. La economía, la ingeniería, la arquitectura y otros campos científicos utilizan constantemente la noción de riesgo. La idea de riesgo forma parte del paradigma de racionalidad que, según Max Weber (1964), es el gran motor de esa sociedad. Sin embargo, los sociólogos explican que hemos pasado de una sociedad moderna a una sociedad postmoderna en la que el paradigma racional se desvanece. La ciencia pierde capacidad de dar respuesta a los problemas que se presentan. En la sociedad postmoderna, la incertidumbre es cada vez mayor y se ha de aprender a convivir con ella. Muchos aspectos de la vida son cada vez más inciertos: los mercados laborales, los financieros, el calentamiento global, las pandemias de la gripe, el trabajo, la familia, etc. La sociedad global se convierte así en la sociedad del riesgo y, sobre todo, de la incertidumbre (Beck, 1992).

El riesgo se puede analizar desde diferentes disciplinas y, por tanto, desde diferentes perspectivas. La perspectiva dominante en el análisis de riesgos es el paradigma racional. Es la visión que se desarrolla desde las ingenierías, desde el cálculo actuarial, y otras muchas disciplinas técnicas. También es la perspectiva más extendida en el mundo de la seguridad privada, aunque no la única. Es muy frecuente que los análisis de riesgos de las consultoras de seguridad o de las propias empresas del sector se realicen desde esta visión. Sin embargo, no existe un determinismo y el sector privado puede trabajar eventualmente desde cualquiera de los modelos que se comentan en el capítulo. El paradigma o modelo racional parte de algunas premisas. La principal es que es posible analizar/evaluar objetiva y científicamente los riesgos. Por lo tanto, es posible planificar racionalmente la seguridad y prevenir riesgos. También se acepta, de forma más o menos general, que el punto de vista externo del experto es más racional que el de los actores implicados.

El concepto de **análisis de riesgos**, desde este punto de vista, es el proceso por el que se identifican y evalúan posibles amenazas, los puntos vulnerables del sistema a proteger, y se estiman las posibles consecuencias. Esa información se recoge en un **informe de riesgos**. Una vez realizado el también llamado *risk assessment,* se evalúan distintas alternativas o estrategias de actuación, se elige la mejor, y se proponen medidas (a veces llamadas también contramedidas)

para reducir los riesgos a un nivel aceptable. Toda esa información se refleja en un **plan de seguridad** en el que, además, se especifica cómo se va a implementar, quiénes son los responsables (*risk management*), qué va a costar, cómo y cuándo se va a evaluar y, si es el caso, otras cuestiones como la comunicación de riesgos a gestores o población (*risk communication*).

Existen algunos conceptos básicos en el **análisis racional de riesgos**. La amenaza se refiere a la posibilidad o probabilidad de que una eventualidad concreta (un rayo, una extorsión, un robo, etc.) se manifieste con una intensidad, tiempo y localización dada. La noción de vulnerabilidad es, dado su nivel de protección actual, la susceptibilidad de un bien o persona a sufrir un determinado nivel de daños o pérdidas de todo tipo debido a la realización de una amenaza particular. A veces se habla de impacto (estimado o real) para referirse a la pérdida o repercusión negativa causadas por la materialización de una amenaza. El concepto de medida (o contramedida) de seguridad designa a los instrumentos y mecanismos que tratan de reducir riesgos bien actuando sobre los daños potenciales o bien en la probabilidad de ocurrencia. Existen varios criterios para clasificarla. Suele distinguirse entre medidas preventivas que disuaden o reducen el impacto (vallas, cámaras); detectoras que avisan de que algo va mal (alarmas, detectores); correctoras que neutralizan los problemas identificados (un antivirus); o represoras que castigan a los infractores (detención, multas).

El análisis racional de riesgos utiliza un protocolo bastante establecido en el que hay varios pasos a seguir (ver cuadro 1) (Fisher y Green, 1998).

Cuadro 1. Protocolo del análisis racional de riesgos

1. Identificar los bienes, sistemas o personas a proteger. Estimar su valor.
2. Identificar y describir las amenazas y probabilidad de ocurrencia.
3. Identificar y evaluar los controles o contramedidas existentes.
4. Estimar la vulnerabilidad de bienes y sistemas (riesgo residual).
5. Calcular el impacto potencial (económico u otro) para cada zona y tipo de riesgo.
6. Proponer controles adecuados y justificarlos (recomendaciones).
7. Recoger toda esta información en un informe de riesgos.

Fuente: Elaboración propia

El primer paso es fijar un objetivo de seguridad. Se trata de establecer qué estándares de seguridad se consideran aceptables. El segundo es analizar o evaluar los riesgos (amenazas y vulnerabilidades) del sistema a proteger. Para ello, se realiza un inventario de todos los activos y objetos a proteger, analizando qué importancia económica y estratégica tiene cada uno en el funcionamiento global de la entidad. Esa importancia se estima normalmente en términos monetarios. Así se calcula en términos de dinero las jornadas perdidas, retroceso de posición en el mercado, las lesiones causadas, y cualquier otra situación. De esa forma, se puede hacer una valoración comparable de los distintos costes que tendría un eventual incidente. El objeto a proteger pueden ser personas (su integridad, salud, bienestar), recursos naturales (aire, agua, na-

turaleza), infraestructuras, edificios, mercancías, instalaciones, equipos, información (financiera, comercial, de productos, clientes, procedimientos, etc.) y otros intangibles.

El análisis racional de riesgos se basa en una metodología que se explica en el informe de auditoría de riesgos. En ella se explica el criterio que se sigue a la hora de atribuir un valor económico a un determinado objeto. Tiene que quedar claro cómo se calcula el valor de los objetos a proteger.

Por ejemplo, si se calcula el valor económico de una máquina saboteada, este puede calcularse respecto a su valor de compra, o de amortización, tener o no en cuenta los costes de reemplazarlo, o el valor de lo que se ha dejado de producir como consecuencia de la paralización.

La estimación de las distintas amenazas también tiene que tener una base objetiva. Además tiene que explicitarse un sistema para trasladar las distintas medidas de probabilidad a una que resulte comparable.

Por ejemplo, se puede apreciar el riesgo de inundación con datos de lluvia en la zona del Instituto Nacional de Meteorología expresados en litros por metro cuadrado. La probabilidad de un robo puede estimarse, usando las estadísticas policiales del distrito, en número de sucesos en un año.

Ambas unidades de medida no son comparables y hay que reconvertirlas en una misma escala que sí lo sea. Ello permite saber cuál de las dos eventualidades representa una amenaza mayor. Cuando daño y amenaza son comparables, es posible tomar decisiones informadas sobre qué merece la pena proteger más, o qué proporción del presupuesto sería aconsejable invertir. Las metodologías y fuentes de datos son diversas. Pueden ser series estadísticas. Caben diseños experimentales naturales o de laboratorio donde se compara una población sometida a ciertas eventualidades con otra de control. Se pueden montar paneles Delphi de expertos. Pueden tenerse en cuenta datos cualitativos sobre experiencias pasadas de riesgo. También caben técnicas como la del *tree analysis* que estudia fallos en sistemas complejos, entre otras muchas.

Para cada objeto a proteger, hay que pensar en las repercusiones que podrían tener todo tipo de **amenazas** (inundaciones, fuego, robos, sabotajes, etc.). Para ello, se parte del axioma que las amenazas son constantes e infinitas, aunque la probabilidad y formas de manifestarse varían. Se piensa en todas las posibles y a cada una se le atribuye una probabilidad en función de la información disponible (estadísticas, ocurrencias previas, estudios). La estimación del nivel de amenaza que se atribuye debe estar justificada por una metodología que permita asignarle un valor objetivo, así como hacer comparables amenazas muy distintas. Visto el valor de los espacios a proteger, y las amenazas probables, se analizan los medios de protección actualmente existentes y se identifican **vulnerabilidades**. Se trata de evaluar en cuánto podrían reducir el riesgo las medidas instaladas. Por ejemplo, un detector de humos no evita el incendio, pero acorta el tiempo de reacción y, por lo tanto, los destrozos causados.

Por ello, a la fórmula del riesgo se le añade el factor protección (p):

$$\mathbf{R = (D \times P)/p.}$$

El tipo de daños que puede causar la materialización de un tipo de amenaza es muy variable. Cada uno de esos daños puede ser de mayor o menor alcance.

Por ejemplo, un suceso de robo puede provocar la desaparición de un ordenador concreto, pero pueden existir también daños materiales (en su cubierta), una alteración del estado original (aparece manchado) una restricción temporal de la capacidad o calidad del servicio (se ha de reparar), una pérdida de confidencialidad (han accedidos a los datos), y otros.

Todo este proceso de evaluación de riesgos permite, al final, que el cliente tenga una visión global de todos los riesgos de su actividad. Esa información está ordenada de mayor a menor riesgo. Es decir, se conocen desde los elementos de más valor y más amenazados, hasta los de menos valor y menos amenazados (R = D × P)/p. Ello le va a permitir tomar decisiones racionales, como el invertir más dinero de su presupuesto en proteger los riesgos mayores. Una vez que se conoce la distribución de riesgos, el tercer y último paso del evaluador es decidir con el cliente si el riesgo es asumible o no. Si se decide que no, se concibe un plan de seguridad. Este parte de unos objetivos a conseguir y de considerar todas las alternativas posibles de actuación para lograrlos. De cada una de ellas se evalúan las ventajas e inconvenientes que puede tener. Lógicamente, pueden ser de diverso tipo. Finalmente, se trata de proponer al cliente la que se considere la mejor o mejores opciones. La opción desarrolla de forma detallada en el plan de seguridad.

Como puede apreciarse, en general, los análisis de riesgos son de una gran complejidad si se hacen bien. También resulta caro realizarlos, en particular si el sistema a proteger es grande y rico en procesos. En la práctica, las empresas de seguridad lo simplifican utilizando un **cuestionario de vulnerabilidad** (*security survey),* o bien **matrices de vulnerabilidad** donde se recoge, de forma esquemática y pautada, una serie de información clave sobre los objetos (espacios, bienes) a proteger, las rutinas de funcionamiento, las amenazas (tipo y probabilidad), y los controles y recursos existentes. Suele haber modelos prediseñados para cada tipo de actividad de los clientes. Esos instrumentos acostumbran a estar centrados en los riesgos objetivos y no tanto en los subjetivos. La información se recoge habitualmente por observación y se complementa, a menudo, con alguna entrevista.

El **cuadro 2** muestra el tipo de información que suele recogerse en los modelos protocolizados de evaluación de riesgos en el caso de almacenes de mercancías. Aunque no hay dos almacenes iguales, ese tipo de documentos sirve de guía de referencia a la que, después, se le puede añadir algún elemento específico.

Cuadro 2. Informaciones frecuentes en los formularios estandarizados utilizados en la evaluación de riesgos en almacenes

- Perímetro (vallas, accesos, iluminación, vías subterráneas)
- Parking (identificación, vehículos, horarios, vigilancia)
- Entradas (identificación, control de visitas y empleados, camiones, horarios)
- Control de llaves (número de copias, custodia)
- Ventanas (altura, rejas, conductos de ventilación, claraboyas)
- Mercancías (peligrosidad, manipulación, almacenaje, inventario)
- Valores (cajas fuertes, quién accede, cantidad de dinero)
- Ordenadores (tipo de información, nivel crítico, acceso, protección)
- Alarmas (tipo, localización de detectores, CCTV, mantenimiento)
- Fuego (salidas, extintores, *sprinklers*, inflamables, evacuación)
- Guardas (cuántos, horarios, rutas y patrullas, misión)

Fuente: Elaboración propia

El modelo racional se utiliza de forma generalizada. Sin embargo tiene límites. Con relación al análisis de riesgos, su racionalidad es limitada.

Por ejemplo, no siempre se consideran todas las amenazas existentes, otras veces no es posible cuantificarlas, u otras la calidad de los datos disponibles es mala. En otras ocasiones falta tiempo para hacer un análisis concienzudo, o este resulta demasiado caro, con lo que se reduce todo a un mero sistema estándar de indicadores.

Otro problema habitual es la propensión a considerar solo los riesgos objetivos, y a descuidar los subjetivos, o bien la tolerancia a los mismos. Por otra parte, el modelo racionalista funciona mejor en sistemas con riesgos simples, o donde la intervención humana en el sistema es poca. Además, desde esta perspectiva, se tiende a obviar a los actores (las preferencias de riesgo, motivaciones, confianza, etc. de las personas afectadas), y no se les suele permitir participar en la toma de decisiones. Con relación a la planificación de la seguridad, el paradigma también presenta problemas. Planificar es condición necesaria, pero no suficiente, para el éxito. El ideal es prevenir, pero la prevención tiene también costes de todo tipo que varían según el método elegido.

La segunda perspectiva de análisis es la económica. Se puede decir que, en realidad, es una extensión de la perspectiva racionalista. La economía estudia las formas en que se asignan recursos escasos. Aquí, el análisis parte de la premisa de que el hombre es un ser racional que busca maximizar los beneficios (u oportunidades) y minimizar los riesgos. Oportunidad y riesgo son los dos extremos de un mismo eje. Cualquier decisión conlleva costes y beneficios que pueden ser calculados. Extendiendo ese argumento, es posible calcular los costes que implica que se materialice un riesgo y también los costes que tiene crear una estructura de seguridad que trate de minimizar o impedir que llegue a ocurrir. La seguridad y el riesgo deben administrarse con criterios de eficacia y eficiencia.

Un objetivo del análisis económico de riesgos es conocer y comparar los costes de una eventualidad (un accidente, un incidente) y los beneficios derivados de su prevención. Es lo que se llama análisis de coste/beneficio. Ambos parámetros se expresan en términos monetarios. Se puede estudiar, por ejemplo, los costes que tienen los accidentes de tráfico y el ahorro que representa tener un programa de vigilancia policial en las carreteras que evite algunos (una vez

deducidos los costes de este). De esa forma, se pueden comparar costes de varios programas de prevención e identificar el más eficiente. Otro tipo de objetivo es comparar la eficacia de dos programas con relación a su coste. El análisis coste-efectividad expresa los costes en términos monetarios y los logros en unidades diversas p. ej., detenidos, accidentes, años de vida…).

Las metodologías son algo complejas. Al contabilizar costes se tiene que distinguir ente los que soporta la víctima directamente, terceras personas (su familia, por ejemplo), o la sociedad (a través del Estado). Son los llamados costes personales, externos y sociales. Los primeros se centran en las víctimas (o transgresores, si es el caso). El externo se llama así porque afecta a terceras personas que pagan sin haberlo decidido voluntariamente. Los sociales suponen gastos que pagan todos los contribuyentes, y que reducen la calidad de vida agregada de la sociedad. Por otra parte, existen diversos tipos de costes/beneficios: fijos o marginales, de oportunidad, tangibles o intangibles, a corto o largo plazo, etc. El método de cálculo puede ser directo, si se estima a través de fuentes primarias, o indirecto, mediante fuentes secundarias. En ocasiones, hay que determinar el valor de intangibles como la salud, la seguridad, la tranquilidad, o la vida humana, por ejemplo. En este caso, se puede estimar a través de lo que se suele pagar en indemnizaciones, o bien a través del método llamado de la disposición al pago. Otras veces hay que calcular el beneficio que reporta un programa o acción determinado. La dificultad está en cuánta de la variación en la realidad es atribuible al programa, y cuánta a otras circunstancias.

El análisis económico no está exento de dificultades. Existen, por ejemplo, controversias al decidir qué partidas se deben contabilizar en las estimaciones de costes o de beneficios y cómo. Por otra parte, existen determinados riesgos de los que se desconoce bastante su extensión y alcance. Un ejemplo sería la delincuencia organizada transnacional, o los llamados delitos de cuello blanco. Además, los valores realmente importantes para las personas son difíciles de medir, aunque se les trate como intangible y se les atribuya un valor arbitrario. El análisis económico también se centra mucho en el riesgo objetivo y olvida las cuestiones del riego percibido y tolerable. Pero, quizás, la crítica más de fondo es que la eficiencia, sobre la que gira en gran medida esta perspectiva no es el único objetivo de las políticas públicas, ni tampoco las de seguridad.

1.2. Otros modelos de análisis

Un tercer paradigma de análisis es el **psicológico**. Este modelo parte de la idea de que las percepciones, actitudes y conocimientos que las personas tienen son clave en la definición, evaluación y toma de decisiones de riesgo. Por lo tanto, bajo esta forma de análisis, lo que importa es cómo se perciben los riesgos (conocimiento, percepción), las predisposiciones o preferencias ante el riesgo (actitudes), y los factores que influyen esas percepciones y preferencias. Esas cuestiones tienen una aplicación práctica en la gestión de la inseguridad, comunicación de riesgos, el diseño ambiental y otros campos. Existe una amplia producción científica que analiza los factores que explican la percepción de

riesgo, la sensación de inseguridad, o el miedo. Se sabe que las personas toman decisiones de asumir (o no) riesgos y modelan su conductas, opiniones o, incluso, su voto, llevados, en buena medida, en base a esas percepciones. Por ello esta perspectiva tiene un eco en muchos planteamientos de las políticas públicas de seguridad. Sin embargo, su uso por parte de la seguridad privada es limitado. Quizás la razón más importante que lo explica es la gran influencia que tiene la perspectiva racionalista en un sector muy basado en la tecnología y en la vigilancia disuasiva (Gabrosky, 1998).

La percepción de inseguridad ciudadana o el miedo al delito es de los temas más estudiados. Existen principalmente **tres grandes grupos de factores** que explican ese miedo.

1) Un primer grupo es el grado de vulnerabilidad o protección. Ciertos colectivos (personas pobres, marginadas, mujeres, ancianos, inmigrantes, turistas) pueden vivir situaciones de mayor desprotección por diversas razones. Las consecuencias de una victimización pueden ser más impactantes o dolorosas porque tienen menos instrumentos para responder o reponerse a ella. La sensación de miedo aumenta si falta confianza en la Policía o en el sistema penal. Es frecuente, aunque no siempre, que se vean a sí mismos como colectivos de riesgo, como víctimas tipo.

2) Un segundo grupo son factores que actúan como protectores frente a la sensación de inseguridad. Las personas que cuentan con un mayor capital social, con una red de apoyo sólida, suelen sentirse más seguras y protegidas.

3) El tercer grupo de variables tienen que ver con las condiciones del entorno. La suciedad de las calles, las pintadas, el abandono de los espacios, las roturas de mobiliario público se interpretan por la población como signos de descontrol. Esos espacios se viven como "amenazantes". Lo mismo puede ocurrir si el desorden es social. Por ejemplo, la presencia de pandillas juveniles, personas sin hogar, alborotos, peleas se asocian con degradación, desorden, e imprevisibilidad (Wilson y Kelling, 1982).

En la medida en que se sabe que existen factores que influyen, una idea que se deriva es que el miedo se puede gestionar (Moore y Trojanowicz, 1988). Existen varias estrategias. Una consiste en cuidar la información a una comunidad. Es aconsejable dar información objetiva, realista y útil sobre la inseguridad.

> Por ejemplo, dar datos sobre el perfil de los delincuentes, sobre el nivel de riesgo real de la zona, sobre el tipo de víctimas más frecuentes, sobre cómo mejorar la propia seguridad, etc.

El riesgo real y el percibido tienden a coincidir cuanto más experiencia o información existe. Los riesgos se han de comunicar con coherencia, transparencia, puntualidad y sinceridad. Una información de calidad y útil conlleva una labor policial previa de investigación e inteligencia basada en el análisis de riesgos, en entender la lógica de los incidentes, o en diseñar actuaciones

transversales. También se puede incidir en el miedo a través de la educación y la formación. Es útil y efectivo enseñar hábitos seguros. Se trata de que el ciudadano también asuma algún protagonismo o responsabilidad en la propia seguridad. Eso le da más confianza.

Tanto para conocer el alcance de la sensación de inseguridad como para gestionarla, es necesario poder medirla. Una vía muy utilizada son las **encuestas de victimización** (Sabaté, Aragay y Torrelles, 1999; Thome y Torrente, 2003). Una dificultad que tiene el análisis de la percepción de inseguridad es un mismo riesgo puede desencadenar muchos estados emocionales de desigual intensidad, pero cuyas fronteras son difíciles de precisar. Algunas son la precaución, inseguridad, miedo, ansiedad, o pánico. Puede entenderse el miedo como una reacción emocional defensiva, y no siempre proporcional, ante una amenaza reconocida. Es un mecanismo natural de protección. Lo contrario es la rabia. Pero la persona que responde a una encuesta puede confundir miedo con precaución. Esta es una respuesta racional ante una amenaza (real o percibida). Tampoco está clara la frontera con la idea de inseguridad, entendida esta como un sentimiento de incertidumbre frente a situaciones futuras. La noción de ansiedad es el sentimiento vago de angustia ante amenazas que no pueden ser definidas claramente. Puede conllevar cuadros neuróticos. En el extremo final de la escala estaría la sensación de pánico. Es decir, una reacción emocional muy intensa que, además, conlleva pensamientos y actos irracionales y disfuncionales. Se manifiesta al lado de síntomas físicos.

El **miedo** no es un problema menor, o una mera cuestión subjetiva. Está claro que el miedo tiene **consecuencias** serias que no son deseables ni desde un punto de vista personal ni colectivo. Se sabe, por ejemplo, que las personas que tienen miedo al delito tienden hacia un mayor aislamiento. Reducen sus encuentros, evitan lugares y situaciones que perciben como de riesgo. Al hacerlo aumentan su neurosis. Ello también les lleva al cambio de sus hábitos cotidianos de consumo, ocio, transporte y otros. Todo ello acompañado, a veces, de un aumento en las medidas de protección. En el plano colectivo, las personas que viven en vecindarios donde se vive con miedo tienden a reducir sus salidas y con ellas se reduce el contacto entre las personas del barrio, y las actividades comunitarias. El barrio empieza a perder cohesión social y aumentan entonces las actitudes intolerantes. Desde un punto de vista del espacio, como las personas se desvinculan afectivamente de su barrio y de su cuidado, este se deteriora físicamente y a nivel de limpieza. Entonces, como esas áreas no invitan a permanecer en ellas, se reduce la presencia de peatones, e incluso se evita pasar por ellas. Quedan vacías y anónimas con lo que atraen conductas desordenadas e incluso delictivas. La falta de compromiso e identificación con el espacio, entonces, entra en una espiral ascendente.

Llegados a cierto punto, se produce una devaluación social y económica de ciertos lugares. Los vecinos ya no quieren vivir en el barrio y aumentan las migraciones. La economía se desacelera, algunos comercios cierran, y el precio de las viviendas cae. Desde el punto de vista político, el miedo lleva a la desle-

gitimación de la política y a la desconfianza en las instituciones. En las zonas con problemas de inseguridad, aumenta el descontento y el desinterés por la política. Ello favorece a los partidos y opciones políticas más demagógicas y reaccionarias. Por otra parte, aumenta la presión hacia el aumento del gasto público en seguridad y a la adopción de políticas más duras.

Otro ejemplo de las contribuciones de la perspectiva psicológica son los estudios sobre las **actitudes frente al riesgo**. Con una relativa independencia del tipo de riesgos de que se trate, las personas tienen una inclinación a asumirlos o a evitarlos. A veces se les denomina preferencias o gustos frente al riesgo. La idea es que dos personas, con igual información, toman decisiones distintas. Existen personas que tienen aversión al riesgo y ponen el énfasis en la posibilidad de que ocurra una adversidad, mientras que otras lo buscan y piensan más en la posibilidad de éxito. También existen actitudes pasivas de forma que la persona ni busca, ni evita el riesgo. Las motivaciones para asumirlos son diversas. Pueden responder a una decisión razonada o deliberada (cálculo, astucia), a una predisposición (personalidad, actitudes, creencias, valores), o a presiones sociales (influencia del grupo, valores sociales, compromisos). La motivación es mayor si esos tres factores van en la misma dirección. La actitud o predisposición es más decisiva en la medida en que la información sobre un riesgo es ambigua o incierta. Por regla general, las personas reaccionan más ante las amenazas que ante las oportunidades. Por ejemplo, a la mayoría de personas les preocupa más el evitar pérdidas que el tener beneficios económicos.

Como puede comprobarse, el modelo psicológico de análisis de riesgos es fructífero en ideas y tiene una larga trayectoria empírica. Sin embargo, también tiene también sus límites. Uno de ellos es que conocimientos, percepciones, o actitudes no son rasgos únicamente individuales. Están afectados por factores de grupo, sociales, culturales, o políticos. La persona y sus atributos psicológicos no se pueden aislar fácilmente de su contexto vital. Es más fácil que las políticas puedan incidir en los contextos que directamente en las personas tomadas de forma individual.

El cuarto gran paradigma en el análisis de riesgos es el **organizativo**. La premisa de partida es que la seguridad son productos y servicios que se venden y compran. Esos productos y servicios se idean y se llevan a cabo por empresas o instituciones. Esas empresas trabajan en entornos que les condicionan. El entorno de una organización está formado por sus clientes, proveedores, el marco legal, los accionistas, el mercado laboral, de materias primas, la tecnología, y otras fuerzas externas. El entorno presiona e influye en la toma de decisiones, en las estrategias de empresa, en sus actividades, y también en sus productos y servicios. El entorno afecta a la capacidad de una empresa de definir, organizar, gestionar y evaluar sus productos y servicios de seguridad.

Por ejemplo, una empresa de vigilancia que, en un contexto de alta competencia y escasez de vigilantes, quiere reducir sus costes de personal puede ofrecer servicios de acuda y custodia de llaves que requieren menos plantilla.

Esta perspectiva de análisis plantea que es posible explicar los objetivos, estrategias o los productos y servicios de una empresa (variable dependiente) en función de su entorno (variable independiente). Cuanto más poder relativo tienen alguno de esos elementos del entorno, más capacidad tienen de influir en las decisiones, estrategias, políticas o productos de una firma dada. La unidad 2 de este módulo, por ejemplo, intenta explicar los servicios de seguridad en función de la demanda de los clientes, y la tecnología.

Una de las grandes ventajas y aportaciones de esta perspectiva es que muestra cómo los productos y servicios de seguridad, incluso el concepto mismo, son el resultado de múltiples factores; no son algo estático o invariable. El diseño de un producto o la organización de un servicio tienen que ver con las necesidades de los clientes, el estado actual de la tecnología, el grado de competencia en la oferta, el nivel de riesgo del servicio, y otras variables, todas ellas del entorno de las organizaciones. Los factores son muchos. Aún cabrían otras razones. Cada una le lleva a formular un tipo de demanda distinto y a valorar el servicio recibido con diferentes criterios.

Por ejemplo, un cliente puede tener visiones distintas de lo que supone para él la seguridad. Sus motivaciones para contratar un servicio pueden ser también muy diversas. Puede querer contratar seguridad únicamente para cumplir la normativa (ya sea por obligación, o convencimiento), para prevenir daños materiales o pérdidas económicas, para prevenir responsabilidades civiles o penales, o para evitar daños o agresiones personales. También lo puede hacer por rebajar la prima de un seguro o contratarlo, abaratar los costes de producción, aumentar la calidad o valor añadido de productos o servicios, conseguir una información o conocimientos valiosos, transmitir o fomentar una imagen pública determinada, atender expectativas o demandas de clientes o empleados (o ciudadanos), contribuir a controlar o disminuir la delincuencia, u obtener un servicio auxiliar a su actividad a bajo coste.

La quinta perspectiva es la **sociológica**. La sociología estudia la lógica de las regularidades que se observan en la vida social. Las premisas del análisis parten de la idea de que los riesgos tienen causas y/o consecuencias sociales (Beck, 1995). Además, estos están distribuidos socialmente de forma desigual. Por otra parte, los riesgos no son una cuestión del todo objetiva sino que están también construidos social, política, y culturalmente (Foucault, 1992; Douglas, 1996). Existen numerosas razones para pensar que esa perspectiva sociológica resulta razonable. Por ejemplo, incluso los riesgos meteorológicos o los geológicos no son completamente "naturales". Las consecuencias dañinas de una inundación se producen fundamentalmente porque hubo la decisión humana de construir a las orillas del río. Un terremoto de la misma escala puede no destruir casi nada en Japón y resultar devastador en Haití. Lo definido como seguro o arriesgado varía en el espacio y tiempo. La seguridad y el riesgo no son cuestiones neutras y están siempre rodeados de conflictos. La seguridad de unos puede ser la inseguridad de otros.

Los planteamientos sociológicos ligan la noción de riesgo con procesos sociales y políticos. Sostienen, por ejemplo, que las culturas definen como riesgo lo que amenaza al orden social (Douglas, 1996); o que el poder define riesgos con objeto de disciplinar, gobernar y perpetuarse (Foucault, 1990). De la misma manera los ligan con procesos de desigualdad y consideran que la posición frente a los riesgos es un indicador importante de estratificación social. Los factores importantes de vulnerabilidad tienen que ver con la desigualdad socioeconómica, la discriminación y la exclusión social. Por ello, es importante analizar qué grupos están sujetos a una mayor exposición a ciertos riesgos, son más vulnerables a ellos, o carecen del poder y la capacidad para decidir sobre ellos. Recientemente, la visión sociológica del tema está dominada por la teoría de la sociedad del riesgo (Beck, 1992; Luckman, 1991). Según ella, en un mundo global y altamente interconectado las situaciones de riesgo se propagan rápidamente, por lo que estos tienden a ser cada vez más serios en sus consecuencias, universales en su extensión, e indiscriminados en la escala social.

Muy vinculado al paradigma sociológico está el **análisis político** de riesgos. Bajo esta perspectiva, el riesgo y la seguridad son cuestiones estrechamente vinculadas al ejercicio del poder. Se entiende por poder la capacidad de influir sobre otras personas o grupos, así como la de asegurarse para uno recursos valiosos que también desean otros. La idea de política hay que verla como el juego dirigido a ganar cuotas de poder, y así estar en mejores condiciones de influenciar en las prioridades, objetivos o decisiones públicas. Políticas son el conjunto de decisiones y actuaciones impulsadas desde el gobierno con el fin de responder a un problema público. La premisa de partida es que los problemas de seguridad son, antes que nada, construcciones sociales y políticas. Diferentes actores políticos (gobierno, partidos, sindicatos, grupos de intereses, medios, población…) influyen, según su grado de poder, en la percepción social, definición y gestión de los riesgos. Los gobiernos plantean políticas y planes de seguridad en función de los intereses propios y de otros actores con capacidad de influencia. Pero las políticas son solo el reflejo directo de los deseos de los poderosos. Influyen también las ideologías políticas, el conocimiento científico, la situación económica, los modelos de otros países que se imitan, el marco legal, o las estructuras burocráticas, ente otros factores.

El modelo se aplica perfectamente a la seguridad. La seguridad se convierte en un campo de confrontación política cada vez más central. Proteger al ciudadano es una misión central del Estado y una fuente de su legitimidad, pero este está cada día en peores condiciones de garantizarla (Mir, 1999). Las políticas de seguridad pública se ven en la necesidad de contar con nuevos aliados o encontrar nuevas estrategias. La seguridad privada es uno de esos posibles aliados. Una política de seguridad es el conjunto de principios, objetivos y medidas orientados a proteger a la población frente a un riesgo o conjunto de riesgos. La calidad de una política de seguridad depende de que persiga el interés general, sea efectiva y eficiente, así como lo más universal, equitativa, y socialmente justa posible. Además debería ser democrática, participativa, y

sus responsables deberían rendir cuentas (*accountability*) a los organismos representativos. Nadie pide a un plan de seguridad privado que cumpla unos requisitos parecidos. Únicamente se pide que defienda bien los intereses de su cliente y que, al hacerlo, no contravenga las leyes vigentes.

Desde un punto de vista del análisis político, es importante comprender los mecanismos que tiene el Estado para incidir en la realidad. Los gobiernos hacen políticas de seguridad a través de una serie de instrumentos. El primero son las sanciones o multas. Su objetivo es tratar de evitar o corregir conductas bajo la amenaza de una sanción. La regulación puede definir conductas deseables o indeseables, estándares a cumplir y un sistema de sanciones. La propia Ley de Seguridad Privada es un ejemplo. Las multas tienen la ventaja de que tienen el respaldo de una ley y existen instituciones que las aplican. Sin embargo, los inconvenientes son varios. El primero es que, a menudo, la vigilancia de ciertos ámbitos y la obtención de cierta información son laboriosas, y el mantener los controles resulta caro. Las reglas suelen ser complejas. Se critica también la rigidez de los estándares y el alto nivel de intervencionismo.

Otro instrumento de las políticas son los incentivos económicos. El objetivo es estimular conductas de prevención de riesgos a través de premiarlas económicamente. Eso se puede hacer bajando impuestos (por ejemplo, pagar menos impuestos por la gasolina sin plomo), o subvencionado (subvencionando la producción de bio-diesel). La ventaja de estas prácticas es que interfieren poco en el mercado, y que los costes de gestión son bajos. El inconveniente es que alguien puede preferir pagar y continuar con una mala práctica. Es lo del "yo contamino, y yo pago". La autorregulación es un instrumento cuyo objetivo es incentivar que los que producen riesgos se autocontrolen. La ventaja es que no es una medida impuesta. Son los propios implicados quienes, desde su conocimiento y experiencia del sector, deciden hasta dónde quieren llegar. Para la Administración el coste de información y seguimiento es bajo. El inconveniente es que las decisiones no se toman desde un órgano independiente, sino desde organizaciones que tienen unos intereses creados. Al ser entidades privadas, la rendición de cuentas se hace más limitada.

Otra alternativa política es conceder franquicias, otorgar contratos, o dar licencias. En este caso, se pretende que los creadores de riesgos puedan operar bajo ciertas condiciones y por un período de tiempo. La ventaja es que ese mecanismo permite tener un control sobre el desempeño y, eventualmente, se puede decidir no renovarlas si existen incumplimientos. El inconveniente, una vez más, es que el control de las condiciones de concesión puede resultar dificultoso y caro. Además, las condiciones impuestas pueden restar flexibilidad al mercado. Otro problema es que las empresas pueden acabar repercutiendo el aumento de sus costes en el consumidor. Otra estrategia distinta es publicitar los riesgos. El objetivo, en este caso, es obligar a los proveedores de productos o servicios de riesgo a dar información al consumidor sobre ellos (en el etiquetado, prospectos, catálogos). La ventaja es que el consumidor decide si asume el riesgo o no, y a qué precio. Todo ello conlleva poco interven-

cionismo de la Administración. Pero la información dada puede tener errores o ser ininteligible, manipuladora, o incompleta. Además el consumidor puede asumir riesgos excesivos porque el precio es barato. Finalmente se puede recurrir a los seguros. En este caso, las aseguradoras (públicas o privadas) imponen condiciones variables en las pólizas según el tipo de medidas de control y prevención que adopta el asegurado. A través del incentivo de la rebaja en las primas se pretende que mejoren las condiciones de seguridad. Esta medida comporta poco o ningún intervencionismo de la Administración ya que se trata de un pacto libre entre las partes. El problema es que la misma existencia de un seguro puede hacer bajar la vigilancia preventiva al asegurado.

Cada modelo de análisis de riesgos se enmarca en el contexto de una disciplina y una tradición académica. Cada disciplina científica se define porque tiene unas categorías y perspectivas de análisis más o menos propias con la que mira a la realidad. Pero los problemas y la realidad no pertenecen a ninguna disciplina, ni se reparten entre ellas. En la práctica, cualquier fenómeno puede explicarse desde varias perspectivas. Un ejemplo gráfico es la gran variedad de factores que inciden en cada una de las tres dimensiones del riesgo (riesgo real, percibido y tolerable). Los párrafos siguientes hacen un repaso de esa cuestión. El **riesgo real** deriva de una situación o decisión. Es inevitable por completo (siempre hay algún riesgo), y se conoce *a posteriori*. Los factores que causan situaciones de riesgo son incontables y varían según el área (riesgos infecciosos, financieros, laborales...). En el caso de la delincuencia, la criminología aporta una gran variedad de teorías y variables explicativas que incluyen factores sociológicos (privación relativa, anomia, tensión de valores, etiquetado, subcultura), políticos (criminología crítica), demográficos (estructura de edades de la población), psicológicos (trastornos de personalidad, impulsividad) o genéticos (Downes y Rock, 1995).

El **riesgo percibido** es el atribuido subjetivamente a una situación o conducta. Generalmente, no coincide con el real por una serie de razones (se habla entonces de infrarrepresentación o sobrerepresentación). Entre ellas está la falta de información o su distorsión. Factores psicológicos como el carácter (introversión), la personalidad, y otros condicionan su percepción. El miedo también parece responder a imágenes primarias de las cosas (Sjöberg, 2000). Es mayor frente a lo desconocido (Fischoff y otros, 1978). Pero el condicionamiento no solo es psicológico, también es social. Variables como el género, la edad, el sistema de valores, la ideología política, el nivel de salud, la existencia de grupos de apoyo, el aislamiento social y la soledad, la situación socio-económica, la incertidumbre económica, el nivel educativo, o las pautas de socialización, ente otras, influyen en los niveles de miedo.

El **riesgo aceptable o tolerable** es el nivel que una persona, o un grupo, consideran aceptable o asumible. De hecho, definimos la seguridad como el nivel de riesgo que una persona (o comunidad) considera aceptable. Esta dimensión es distinta del riesgo real, o del percibido. La tolerancia está directamente conectada a la toma de decisiones. Si se considera que un riesgo es aceptable

o tolerable, habrá una conducta. Si no, habrá otra. Aquí intervienen diversas cuestiones. La primera es que la decisión de aceptarlo o no es fruto de un balance de costes y beneficios esperados.

Conducir un automóvil, por ejemplo, puede ser valorado como peligroso, pero la percepción de riesgo se contrasta con los beneficios que reporta hacerlo. Según cómo se plantee ese balance, se tomará una decisión u otra.

Por supuesto, cada persona realiza su propio balance. Hay una gran cantidad de variables que se toman en cuenta. Por ejemplo, los riesgos parecen más asumibles si se presentan como justos, o sintonizan con ciertos valores (justicia, equidad, ética, consenso). Podemos estar dispuestos a asumir los riesgos que asumimos voluntariamente, pero, en general, cuesta más asumir riesgos por coacción. Los peligros naturales (inundaciones, terremotos, rayos) parecen justificarse mejor que los construidos por el hombre. Las situaciones de riesgo más familiares (por ejemplo, los accidentes domésticos) parecen más asumibles que las extrañas. Una persona puede aceptar más riegos si mantiene un nivel de adhesión o compromiso con ciertos grupos o instituciones. El balance de costes y beneficios puede resultar en una decisión distinta en función de si la información disponible es completa, está sesgada, o es comprensible. En la práctica, las informaciones rigurosas y objetivas que tienen las personas son limitadas y estas toman decisiones en función de sus percepciones. Pero, finalmente, el contenido de esas informaciones y las percepciones que tiene un sujeto están influidos por variables sociales y políticas.

Con relación a la forma en que las personas evalúan los riesgos y toman decisiones, se sabe que influyen factores contextuales. Por ejemplo, cuanto más grande es la "visibilidad" del riesgo y más cierto, inmediato o irreversible se ve el daño, o más incierto el resultado final, más grande se ve este. Se sabe también que los factores culturales (valores, expectativas y preferencias) modelan la percepción, definición y aceptabilidad de los riesgos. Se conoce que los factores de tipo psicológico (cognitivos, afectivo-motivacionales, o de personalidad) juegan un rol más importante en la evaluación de riesgos en la medida en que existe más incertidumbre. Son más importantes cuanta más incertidumbre existe. Funcionan también ciertos sesgos heurísticos (principios para reducir la complejidad real) en la valoración de riesgos. Así, se destacan ciertas propiedades de la realidad y se ignoran otras. Se sabe también que el efecto de las dinámicas de los grupos y organizaciones afectan de forma importante a las percepciones y decisiones de riesgo. Un grupo puede extremar tanto la aceptación, como la evitación individual de riegos.

La **confianza** es un factor fundamental tanto para evaluar, como para aceptar riesgos. Esta tiene una importancia creciente en una sociedad post-moderna y global donde la incertidumbre es grande, y los análisis racionales de riesgos son frágiles (Sjöberg, 1987). La confianza es, además, una condición clave para las relaciones económicas y para las humanas en general. Crear confianza es clave en seguridad. Pero esta es frágil, por lo que es más fácil de destruir que de construir. Las personas que se sienten manipuladas en su confianza tardan

en recuperarla. Una de las razones es porque la desconfianza se refuerza a sí misma una vez desencadenada. Además se producen asimetría en su percepción. Eso quiere decir que, por ejemplo, los sucesos negativos (errores, mentiras, accidentes) impactan más en ella que los positivos. De la misma forma, las noticias negativas tienden a tener más efecto en ella que las positivas.

1.3. Planificación y gestión

El presente apartado explica cómo se planifica y gestiona la seguridad siguiendo un esquema racionalista. Desde esa perspectiva, la **gestión de la seguridad** cabe entenderla como un proceso continuo y proactivo para establecer y mantener unos niveles de riesgo aceptables, o dentro de lo convenido con el cliente. El proceso es retroalimentado e incluye todo el ciclo que comienza con el análisis (o auditoría) de riesgos y elaboración del plan de seguridad; sigue con la implementación de ese plan y el control de su funcionamiento; incluye la evaluación de la consecución de los objetivos del mismo y la toma de medidas correctivas, y finaliza con el reanálisis de riesgos y reelaboración del plan de seguridad.

Un gestor de riesgos debe ser capaz de tomar decisiones en cualquiera de esas fases. Es necesario hacerlo ya que las condiciones del entorno cambian constantemente y eso acaba afectando a la seguridad.

Por ejemplo, una empresa puede iniciar una nueva línea de productos que implica almacenar materias primas inflamables que no se tenían cuando se diseñó el plan original de seguridad.

Delante de un riesgo cualquiera, existen varias posibilidades básicas de actuación. La consideración de esas alternativas es una cuestión previa al proceso mismo de planificación. La primera opción es asumirlo y aceptar sus consecuencias potenciales. Otra posibilidad es evitarlo; es decir, sabiendo que existe, apartarse de él, o no tomar decisiones arriesgadas. Se puede también intentar controlarlo, lo que implica identificarlo y vigilar los elementos vulnerables. Reducirlo sería una alternativa que lleva a poner contramedidas que reduzcan el daño potencial o la probabilidad de ocurrencia. Se puede tomar la opción de dispersarlo repartiendo los puntos vulnerables. También se pueden transferir los riesgos de forma que se pasan a otros, o bien se comparten. Finalmente, se pueden compensar contratando un seguro o con otras fórmulas. Una vez que se ha decidido dar una respuesta proactiva al riesgo es cuando comienza realmente el proceso de planificación o gestión.

Para planificar, se parte del análisis de riesgos, o bien de investigaciones que aportan información sobre las características de los factores que indicen en el problema a tratar. Los estudios que incluyen factores explicativos son los idóneos porque facilitan la toma de decisiones posterior. No siempre es posible partir de un buen estudio previo. Pero sin los datos adecuados no se pueden tomar decisiones informadas. En el peor de los casos, se puede recurrir a estudios sobre problemas similares o en contextos parecidos. Además, se hace,

realizando también una labor de documentación para obtener la máxima información posible sobre el fenómeno local (fuentes secundarias, estadísticas, entrevistas, etc.). Se trata de obtener el máximo conocimiento posible sobre él.

El siguiente paso es plantearse varias **estrategias de seguridad** y elegir una. Existen varias. Una posible estrategia es prevenir evitando o paliando daños o pérdidas. Eso se puede hacer de varias maneras, como se ve en el párrafo que sigue. Para prevenir es necesario entender esa lógica de los fenómenos. Se puede también reparar o compensar a través de seguros, u otros mecanismos. Una estrategia diferente es actuar sobre posibles transgresores a partir de conocer los perfiles de riesgo habituales. Otra opción es castigar a los delincuentes utilizando una vía penal (Foucault, 1990). Se puede también intentar reintegrar a estos a la sociedad mediante programas de reinserción. En lugar de actuar sobre los transgresores, es posible actuar sobre las víctimas. Por ejemplo, a través de educarlas en una cultura de la autoprotección. Se puede estudiar su perfil con la idea de identificarlas y actuar con ellas. Es posible mejorar la seguridad colectiva con programas de prevención comunitaria, o con políticas sociales. Otra posibilidad es actuar solo a nivel de la seguridad percibida gestionando la mejora de la sensación de seguridad. También mejorar la seguridad mejorando la tolerancia frente a los riesgos. Todas son estrategias de acción. El sector privado tiende a utilizar más las preventivas, y el público las reactivas.

Quizás las estrategias que más atención despiertan son la de **prevención** (Hughes, 1998). La gestión de la seguridad implica, con frecuencia, realizar prevención. Se entiende por ella cualquier acción proactiva (no reactiva) dirigida a evitar que se produzcan cualquier tipo de daño o pérdida, o bien a paliar su gravedad. Prevenir es fundamental ya que, en seguridad, prevención es, casi siempre, sinónimo de eficacia y eficiencia. La prevención implica planificación. Varias de las estrategias mencionadas en el párrafo anterior se consideran de prevención. Los manuales suelen clasificarlas según diferentes criterios. Uno de ellos es según el mecanismo que actúa. De esa forma, existe una prevención de base social (políticas educativas, de igualdad de oportunidades, subsidios de desempleo, etc.). El presupuesto es que a más igualdad social, menos delito. Otra estrategia es la comunitaria. Aquí el mecanismo que actúa es fortalecer los lazos de cohesión social y solidaridad a nivel local y de barrio. Existe una prevención basada en incidir en los transgresores que ya lo son. En algunos casos pretende evitar la reincidencia, reinsertar a la persona a la sociedad, o bien mantener cierta vigilancia disuasoria. La prevención centrada en transgresores potenciales se basa en identificar poblaciones de riesgo e incidir sobre ellas por la vía educativa, de ayudas específicas, u otras. También puede basarse en las víctimas potenciales y actuar sobre ellas, por ejemplo, mediante la educación para la prevención de riesgos. La prevención situacional se basa en incidir sobre la vigilancia y los objetivos de la transgresión o el delito.

La prevención es una estrategia para combatir la inseguridad objetiva, pero también se puede prevenir la inseguridad percibida. De hecho, algunas actuaciones en el primer terreno tienen también su efecto en el segundo. Así, la pre-

vención de base social mejora la vida del barrio, aumentando la confianza y cohesión vecinal. Esa cohesión refuerza tanto la seguridad real como la percibida. La situacional (basada en el urbanismo, diseño de objetos, o tecnologías de seguridad) suele salir más barata que la social y la relación coste/eficacia es buena. Si esas acciones mejoran la sensación de orden, el miedo desciende algo. Otra estrategia para combatir la inseguridad es la mera vigilancia. La visibilidad de la Policía, o incluso de la seguridad privada, es un factor tranquilizador. Un factor que recibe una atención creciente son las condiciones del entorno tanto sociales como físicas. La sensación de seguridad mejora cuando lo hace el civismo, la convivencia, y el orden social. El desorden llama a más desorden, y este al pequeño delito (Wilson y Kelling, 1982). No permitir conductas desordenadas por parte de ciertos colectivos mejora la seguridad real y percibida. El orden físico y la limpieza tienen una importancia grande para crear entornos seguros que se perciben además como tales. A través de la arquitectura y el urbanismo se pueden crear espacios más seguros.

Por ejemplo, aumentando los espacios urbanos de encuentro entre personas, favoreciendo la vigilancia mutua eliminando barreras, o reduciendo el tamaño de los bloques de pisos.

El miedo mejora sustancialmente si en la comunidad hay solidaridad y lazos comunitarios. Pueden ser redes de mutua vigilancia, apoyo o ayuda. También son efectivos los programas de reparación, mediación, arbitraje. Finalmente, la justicia social tiene un papel en la seguridad haciendo más equitativos el reparto de beneficios y riesgos de todo tipo.

La planificación y gestión de la seguridad implica contar con información sobre los riesgos. En el caso concreto de los datos sobre delincuencia, existen tres **proveedores básicos de información**: controladores (policía, juzgados, prisión, inspecciones, técnicos), víctimas, y transgresores. Las **estadísticas policiales** son el instrumento más común en el primer caso. El problema es que solo recogen los delitos que se denuncian, y que la probabilidad de que lo sean varía según su tipo. Las **encuestas de victimización** son la técnica de recolección de datos más utilizada en el segundo caso. Consisten en preguntar a una muestra representativa de la población por los delitos sufridos durante un período de referencia, así como por otras cuestiones relacionadas. Tienen la ventaja de que los resultados se pueden extrapolar a la población. Además permiten conocer una gran cantidad de información de la víctima y de sus actitudes y opiniones. Sin embargo, solo permiten conocer los datos del delincuente o determinados detalles del delito si esta los conoce. Las encuestas no son capaces de recoger todos los delitos ya que dependen de que estos tengan una víctima individual, que pueda responder, que sea consciente de serlo, y conozca los detalles del delito. Eso no ocurre con los delitos de víctima colectiva, o la mayoría de los de cuello blanco, o delincuencia organizada.

Los llamados **autoinformes** o **encuestas de autoinculpación** siguen el mismo método que las de victimización, pero en este caso preguntan por las conductas delictivas cometidas por el encuestado durante un período de referen-

cia, así como otras cuestiones relacionadas. Esta técnica permite recoger potencialmente más cantidad y variedad de datos que ninguna otra. Permite estudiar la prevalencia e incidencia. Además se reducen sesgos de género, edad, o clase presentes en otras fuentes, como las estadísticas policiales. Es capaz de proporcionar una gran cantidad de datos sobre el perfil del delincuente, sus valores, actitudes, entorno vital, técnicas, toma de decisiones, neutralización de la reacción social, hábitos, redes sociales, contactos con agencias de control, u otras conductas de riesgo (consumo de drogas, etc.). El problema es que suelen tener cuotas altas de no-respuesta. La tasa de respuesta varía según la muestra (adultos, delincuentes, minorías). A pesar de ello, funcionan aceptablemente bien con poblaciones jóvenes. Por eso se utilizan fundamentalmente en estudios de delincuencia juvenil.

La **planificación de la seguridad** es un proceso por el que, tras analizar los riesgos, se fijan unos objetivos de seguridad, se elige una estrategia que se despliega a través de toda una serie de actuaciones. Además, se prevén los recursos necesarios, se establece una organización de las tareas con sus procedimientos y controles, y se fijan las responsabilidades correspondientes. Suele incluirse, además, un protocolo de seguridad que define las reglas y procedimientos que sirven para coordinar las respuestas para diversos tipos de eventualidades, o aspectos concretos como las comunicaciones, por ejemplo. Se planifican todas las necesidades de formación o reciclaje del personal. Se prevén futuras evaluaciones y criterios para modificar o corregir el propio plan. En definitiva, se trata de crear un sistema ordenado que garantice que se alcanzan los objetivos propuestos. En el sector de la seguridad privada, las evaluaciones de riesgos y los planes de seguridad los pueden hacer las empresas consultoras, o bien las proveedoras de servicios.

El **plan de seguridad** es el documento donde se recogen de forma ordenada todas esas informaciones (ver cuadro 3). El plan sirve a un doble propósito de ayudar a vender el servicio y, una vez ha sido comprado, es una guía del trabajo a desarrollar. En ese sentido, equivale al plano y memoria de un arquitecto, o al proyecto de investigación de un científico, por poner dos ejemplos.

Cuadro 3. Estructura y contenido de un plan de seguridad tipo

Portada (Nombre del plan, autores, cliente y fecha)
Índice
Resumen (o resumen ejecutivo)
Presentación (Propósito del informe, alcance, relevancia, antecedentes)
Análisis o auditoría de riesgos (Suele incluirse. Se saca del informe de riesgo)
- Metodología (tipo de datos empleados, recolección y análisis)
- Objetos a proteger (coste, sensibilidad, y posición crítica)
- Amenazas (tipo y probabilidad de ocurrencia)
- Vulnerabilidad (medidas existentes, áreas vulnerables)
- Impacto (valorado en términos económicos u otos)

Objetivos y prioridades (priorizados y justificados)
Estrategia de seguridad
- Justificación de la estrategia (por ejemplo: análisis de coste-beneficio)
- Líneas estratégicas y actuaciones vinculadas

Actuaciones
- Acciones, procedimientos, protocolos (rutinarios y en emergencia)
- Contramedidas (necesarias y opcionales)
- Controles (equipo, personal, procedimientos)

Organización y gestión
- Recursos propios y ajenos (humanos, y materiales)
- Organización y atribución de cometidos
- Responsabilidad y jerarquías
- Selección y formación de personal
- Comunicación de riesgos (población, otras agencias)

Evaluación
- Criterios de evaluación
- Plan de auditorías de seguridad (periodicidad, responsabilidad)

Presupuesto
Bibliografía
Apéndices (su contenido varía)
- Legislación aplicable
- Protocolos o procedimientos de actuación (activación, aviso, evacuación, etc.)
- Convenios y contratos
- Documentos de soporte (teléfonos del personal, de instituciones, mapas, recursos)

Fuente: Elaboración propia

Con relación a lo primero, el plan, que incluye el análisis de riesgos, sirve para que el cliente tenga presente sus vulnerabilidades, y el impacto económico que puede tener para él las posibles incidencias. Con ello se hacen visibles sus necesidades de seguridad. A través del plan, el cliente también puede estudiar la propuesta de seguridad que se le hace y su coste. Es decir, va a poder apreciar la calidad de la propuesta y lo que esta incluye. En su toma de decisiones, inevitablemente, va a comparar los costes que pueden tener los potenciales incidentes con los costes del servicio de seguridad. Por eso es importante que toda la información que aparece sea clara y cuantificable para que le ayude a decidir. El plan también ayuda a que en el proceso de negociación entre proveedor y cliente sea más ordenado y concreto. Durante la ejecución, también sirve para proteger al proveedor de seguridad de posibles exigencias del cliente que no se habían incluido ni presupuestado en el plan. En la práctica, los

planes que se cobran al cliente suelen ser más detallados, mientras que los planes que no se cobran y sirven sobre todo de argumento de venta, suelen serlo menos.

El proceso de redacción de un plan de seguridad parte del análisis de riesgos. El siguiente paso es identificar objetivos, decidir las estrategias, actividades, organización y demás elementos mencionados. Todos aparecen en el plan. Si este implica la colaboración de otras organizaciones externas (ya sean públicas o privadas), es necesario entablar negociaciones con ellas y firmar convenios de colaboración o contratos que detallan el contenido de la asistencia, sus condiciones y costes. Las negociaciones se desarrollan antes de dar por definitivo el plan. Finalmente, viene la aprobación formal del plan, y su distribución a los responsables y actores implicados. En ocasiones, el personal encargado de llevarlo a cabo no está preparado y es necesario establecer un programa de formación y *training* antes de ponerlo en marcha.

Existen unas preguntas fundamentales que la persona que diseña un plan de seguridad debe hacerse. La primera es para qué controlar; es decir, cuáles son los objetivos de seguridad que se pretenden. Eso implica plantear qué estándares son los deseables o los aceptables. La segunda cuestión es qué, o a quién proteger. Es lo que se ha denominado el objeto a proteger. Después están las cuestiones de cómo (la estrategia), con qué (medios), cuándo controlar (secuenciación).

La planificación se realiza con arreglo a unos **principios** que se consideran más o menos universales y que, de alguna manera, muestran su bondad. Uno de ellos es el principio de eficacia; es decir, máxima consecución de los objetivos de seguridad. Eficiencia, o máxima protección al menor coste posible. Respeto por los derechos y libertades de las personas. Participación de todas las personas concernidas. Igualdad o equidad en la protección. En el caso de las empresas, se añaden otras cuestiones como mínima interferencia en los procesos o en la vida cotidiana de la organización. Integración o coordinación entre los objetivos, estrategias y controles de diferentes áreas de seguridad (por ejemplo, laboral, medioambiental, etc.). Finalmente, está la simplificación en los controles y contramedidas que se instalen. Hay más principios, pero estos son los más comunes.

Aparte de esos principios generales orientadores, existen **axiomas prácticos** que se aceptan de forma general. El primero es que, en el proceso de planificación, hay que prever todas las amenazas, aunque luego su probabilidad sea baja. Los sistemas más críticos se han de proteger primero, más y mejor. Cada contramedida concreta que se instala tiene niveles de eficacia y costes distintos.

El planificador debe conocer qué posibilidades y límites tiene cada tecnología con relación a un problema concreto. Algunos controles (o contramedidas) no alteran la probabilidad de que ocurra un incidente, solo reducen la vulnerabi-

lidad y el impacto potencial. Por ejemplo, un sistema de extinción automática de fuego no evitará el incendio pero, si funciona bien, reducirá los daños causados porque lo extinguirá en poco tiempo.

Otras medidas pueden alterar la probabilidad al tener un efecto disuasorio. Por ejemplo: una cámara de seguridad. En cualquier caso, el axioma es que no existe la invulnerabilidad absoluta. Los controles tienen niveles de vulnerabilidad en sí mismos. Siempre existe un riesgo residual, que ha de ser aceptable.

En función del área, existen varias modalidades de planes de seguridad especializados. Existen planes de emergencias, seguridad local, protección civil, seguridad laboral, entre otros muchos. También existen subplanes dentro de un plan general complejo. Por ejemplo, puede haber un plan de comunicación de riesgos, o de evacuación en el marco de otro mayor. La estructura básica de cualquier plan es la misma, aunque puede haber algunos matices.

Por ejemplo, los contenidos de los planes de protección civil suelen incluir un inventario de riesgos, un catálogo de recursos movilizables, una estructura operativa y de mando, los criterios de movilización y coordinación de recursos, y directrices de funcionamiento.

Existen dos tipos de planes de protección civil: los territoriales (por zonas geográficas), y los especiales (por sectores de actividad o riesgos específicos).

Normalmente, todo el proceso de planificación de la seguridad suele estar a cargo de un especialista. Si el sistema a proteger es complejo, puede participar un grupo pequeño de ellos junto con algunos responsables de diferentes departamentos de una empresa, por ejemplo. Sin embargo, realizar un plan de protección civil, o un plan de seguridad local o autonómico son tareas complejas que abarcan multitud de objetos a proteger y multitud de riesgos a considerar.

En estos casos, el proceso comienza con la organización de un equipo encargado de la planificación. Es mejor formar un equipo transversal, ya que se gana en corresponsabilidad, amplitud de miras, e implicación política. El tamaño va a depender, en parte, de los recursos disponibles y de la complejidad del trabajo a realizar.

Por ejemplo, para un plan de protección civil, el equipo puede proceder de áreas tan diversas como son la respuesta a la emergencia (operativa, sanidad, medio ambiente), comunicaciones (relaciones públicas, prensa), comunidad (relaciones con otras agencias), recursos humanos (funcionarios y voluntarios, sindicatos), o servicios de soporte (jurídicos, compras, mantenimiento, informática).

En el equipo de planificación es necesario establecer unas líneas de autoridad. Se ha de encontrar un equilibrio entre jerarquía (emergencias) y participación (*planning*). Una vez establecido, se han de fijar las misiones, establecer objetivos, y repartir responsabilidades. Establecer un calendario de trabajo donde se fijen fechas límites. Para poder realizar las tareas, es necesario contar previamente con un presupuesto detallado por partidas. Realizar un análisis de riesgos a gran escala (a nivel local o regional) es muy complejo. Es necesario

considerar factores históricos, geográficos, tecnológicos, y asentamientos y actividades humanas. Por ejemplo, para diseñar un plan de protección civil se comienza por el estudio de las vulnerabilidades. El esquema general es el mismo. Se realiza un inventario exhaustivo de puntos especialmente sensibles a proteger y de las actividades de riesgo en el área. Se estima la probabilidad de ocurrencia de las distintas eventualidades meteorológicas, riesgos industriales, accidentes en transporte de mercancías peligrosas, etc. Esas apreciaciones se basan en estadísticas, estudios, encuestas, y otras fuentes. Se evalúan posibles impactos humanos, materiales o económicos. Se hace un inventario de todos los medios públicos y privados disponibles. Se calcula el factor protección asignando un valor a la disponibilidad y adecuación de los recursos a cada riesgo particular. Una vez identificados los puntos vulnerables, se redacta el plan.

Los planes de protección civil (y todos) pueden diseñarse *ex novo* o ser revisiones de los existentes. De hecho, casi siempre suelen existir mínimas estructuras de protección, aunque no estén coordinadas en un plan. Por ello es necesario analizar la situación actual. Ello implica realizar una evaluación que incluye revisar los planes y políticas de protección ya existentes, e identificar la legislación que les afecta. Identificar los recursos internos y externos (personal, equipo, servicios, organizaciones, transportes y comunicaciones) que están comprometidos en el actual plan. También es necesario identificar las actividades, servicios, u operaciones críticas que realizan (comunicaciones, suministros, empresas vitales...) y revisar la cobertura de los seguros. Todo ello conlleva recabar una gran cantidad de información y reuniones múltiples con los responsables de bomberos, seguridad pública y privada, Cruz Roja, meteorología, sanidad, suministros, etc.

Un aspecto especial de la gestión del riesgo es la gestión de situaciones de **emergencia o crisis**. Este concepto designa el proceso para prevenir, responder y recuperarse de ella. Técnicamente hablando, se realizan las mismas tareas que en cualquier tipo de gestión (planificación, formación, dirección, comunicación, coordinación, o evaluación). Sin embargo, el contexto de emergencia o crisis requiere que la gestión de los recursos humanos y materiales, el análisis de información y la toma de decisiones sea más rápida y crítica. Determinadas áreas de la gestión, como la dirección y control, la logística, las comunicaciones, el salvamento, las relaciones con la comunidad, la protección de propiedades, la gestión política y mediática de la crisis, o la recuperación de la crisis y la restauración de la normalidad cobran una importancia clave.

La organización de respuesta a situaciones de emergencia o crisis está dirigida por la Autoridad de Protección Civil (más a nivel institucional y político), y cuenta, además, con un jefe operativo y un equipo de gestión de la emergencia. En contextos de emergencia o crisis, es importante contar con un mando único y ejecutivo que tome decisiones rápidas. Sin embargo, la envergadura de alguna de ellas y la diversidad de temas afectados (sanitarios, arquitectónicos, medioambientales...) demanda también cierta multidisciplinariedad, participación y coordinación. De ahí la importancia que cobra el equipo de gestión

de emergencias. Ese equipo da soporte a la dirección operativa ocupándose de los múltiples aspectos colaterales al incidente, como puede ser la comunicación con la prensa, asegurar los recursos materiales necesarios, la relación con colaboradores, hospitales, etc., asegurar que las comunicaciones funcionan y otros.

La dirección operativa se ocupa del mando de las personas y medios empleados en el incidente. Da órdenes, evalúa la situación, fija estrategias, implementa el plan, activa recursos, requiere la colaboración externa, ordena evacuaciones, supervisa la respuesta, y da por finalizada la emergencia. Depende directamente de la Autoridad de Protección Civil. Entre las funciones críticas que realizan, está el movilizar y coordinar al personal de emergencias, informar y aconsejar a la población afectada sobre el riesgo, y dar cuentas a la opinión pública (medios de comunicación). Con relación al primer aspecto, en situaciones de crisis las comunicaciones son vitales, ya que hay que coordinar a un gran número de personas. El plan de emergencias debe prever alternativas en el caso de un fallo, debe prever todas las líneas posibles de comunicación, y separar los canales de comunicación operativa y los de soporte. Con relación al último aspecto, es muy importante la claridad, coherencia y consistencia de los mensajes. Por ello se aconseja designar un único portavoz y canal oficial. La información debe ser completa, exacta y aprobada. Se debe dar igual acceso a todos los medios de comunicación, y se deben evitar las especulaciones y los portavoces no autorizados.

1.4. Evaluación de la seguridad

> Evaluar es emitir un juicio de valor sobre la necesidad, diseño, implementación, eficacia, impacto, o eficiencia de un programa o actuación basándose en el análisis de información empírica recogida de forma sistemática.

La evaluación debe entenderse como un proceso continuo que facilita la mejora constante. Sus resultados sirven para, eventualmente, modificar y enriquecer el plan que se evalúa. Existen varios tipos de evaluación. La más conocida es la que se centra en medir hasta qué punto los objetivos de un plan o programa se han cumplido. Sin embargo, la mera respuesta a esa cuestión no proporciona información útil sobre si el programa estaba bien diseñado, sobre qué fases o actividades del mismo no salieron bien y, sobre todo, por qué han fallado.

Por todo ello las preguntas de evaluación se han ido ampliando. Se pueden plantear cuestiones como:

- ¿Es necesaria una actuación?
- ¿Está bien definido el programa?

- ¿Es evaluable?
- ¿Se ha implementado adecuadamente?
- ¿Qué efectos ha tenido?
- ¿Ha sido eficiente?

Normalmente se distingue entre lo que son evaluaciones previas al programa, evaluaciones que se hacen durante su implementación, y evaluaciones sobre sus resultados. Por otra parte, está la cuestión de quién participa en la evaluación. Tradicionalmente, tanto la elaboración de programas y su evaluación se plantean desde el poder y se conciben como un proceso vertical. Sin embargo, en la ejecución de los programas participan muchos actores y sus consecuencias afectan a otros muchos. El éxito de un programa depende de que todas las personas se sientan implicadas en él. Eso es más fácil si esas personas han sido participes en su definición y desarrollo.

Existen, por lo tanto, varios tipos de evaluaciones y todos son aplicables a la seguridad.

La **evaluación de necesidades** es previa al programa. Consiste en conocer las características del problema que se quiere solucionar y su alcance. Se trata de evaluar las necesidades que existen y viendo la distancia que existe entre lo que hay y lo que debería ser con arreglo a lo que ocurre en otros lugares, lo que dice la ley, aconsejan los expertos, o sencillamente, demandan las personas/clientes. Una modalidad es la evaluación de riesgos.

La **evaluación del diseño de programa** se realiza sobre el papel y consiste en ver su consistencia lógica con relación al problema que se quiere solucionar. Se analiza si los objetivos y las acciones previstas son coherentes y siguen una secuencia lógica, si el modelo de intervención está contrastado, o si el presupuesto es suficiente, entre otras muchas cuestiones.

La **evaluación de la evaluabilidad** consiste en ver si el programa, tal y como está diseñado, podrá evaluarse. La evaluación de la implementación se realiza cuando el programa ya está en marcha. Consiste en detectar discrepancias o desviaciones entre lo previsto y la realidad. Por ejemplo, actuaciones que no se llevan a cabo, o resistencias de los profesionales o de los destinatarios.

La **evaluación de la cobertura** consiste en ver si el programa llega a toda la población objeto y si existen barreras de acceso al programa. La monitorización o seguimiento de programas suponen una evaluación continuada de los programas cuyo desarrollo se prolonga en el tiempo. Se basa en diseñar unos indicadores de funcionamiento y recoger periódicamente información en base a ellos.

La **evaluación de resultados** consiste en medir hasta qué punto se han cumplido los objetivos en la población diana. Se analiza también si existen efectos no queridos.

La **evaluación del impacto** es lo mismo, pero sobre el resto de la población no objeto del programa.

Existe una evaluación económica que analiza el coste/beneficio del programa, o su coste/eficacia, entre otros parámetros.

Si evaluar consiste en juzgar el valor de algo, ese juicio se realizará sobre la base de unos criterios. Esos criterios, o preguntas de evaluación, tienen que ser justificables y deben concretarse en una serie de indicadores con los que medirlos. Así, los criterios para evaluar la eficacia se deben justificar en base a los objetivos concretos de seguridad que se pretenden. Si se quiere ver, por ejemplo, hasta qué punto la seguridad en una tienda de ropa de marca ha mejorado después de instalar un sistema de seguridad para prevenir robos, hay que explicitar qué indicadores se utilizan. El lugar para hacerlo es el plan de seguridad. Estos pueden ser varios: el número robos de género, la cuantía de lo robado, los robos que se evitaron porque sonó el detector de pinzas de alarma, el volumen de ventas, la sensación de seguridad de los clientes, de los empleados, u otros. Además, siendo rigurosos, es necesario poder atribuir una eventual mejora al efecto del sistema y no a otros factores.

A veces se habla de **evaluación de la calidad**. Sin embargo, el concepto de calidad puede significar muchas cosas y tener múltiples indicadores. El sector privado suele utilizar una variedad de **criterios** para aproximarse al concepto de calidad de la seguridad. Un primer criterio son los **daños o pérdidas humanas o materiales evitados**. Sería un criterio adecuado para medir la eficacia, pero la medida es compleja, ya que implica medir lo prevenido. El ideal es hacerlo a través de un método experimental con un grupo de control (sin seguridad) y otro experimental (con seguridad). Sin embargo, eso no siempre es posible. Como alternativa se puede comparar con años anteriores, u otros lugares controlando el efecto de terceras variables.

Otro criterio frecuente es la **ausencia de errores e incidencias en los servicios/equipos**. Aquí se cambian los indicadores de resultados por los de funcionamiento. El presupuesto es que los sistemas van a cumplir su función si funcionan bien. Como medida de eficacia es inadecuada. Otro criterio que se utiliza es la **capacidad de respuesta técnica a las demandas** o necesidades. Aquí se introduce un criterio de capacidad de servicio. Otra aproximación es la satisfacción subjetiva del cliente (o del ciudadano, en el caso de la seguridad pública). Se pretende que sea un indicador de calidad del servicio, pero es indirecto. También se ha utilizado como criterio el **cambio de actitudes** y conductas del cliente hacia la seguridad. Este deja de verla como un gasto y la ve como una inversión. Sin embargo, se mide más la persuasión que otra

cosa. Finalmente, hay empresas que utilizan la motivación de su personal de seguridad como un criterio. Pero ese criterio mide la calidad del servicio que prestan demasiado indirecta e inciertamente.

La seguridad es un bien intangible. Un estudio utiliza los criterios mencionados para estudiar cómo entienden la calidad un grupo de directivos de empresas españolas (Torrente, 2006). El más referido es la capacidad de la empresa de responder a las necesidades y demandas del cliente. En segundo lugar figura el grado de ausencia de errores o incidencias en los servicios. En el tercer puesto se menciona la satisfacción del cliente. En cuarto lugar, la importancia de los daños o pérdidas evitados con el servicio. En quinto lugar, la capacidad de influir o educar al cliente. Finalmente, está el grado en que la empresa es capaz de motivar a su personal. Como la seguridad es una actividad de servicios, la capacidad de atender cualquier eventualidad del cliente se ve como muy importante, sobre todo por el subsector de base tecnológica (seguridad contra incendios, sistemas electrónicos). Este subsector coincide con el de la vigilancia en destacar la importancia de la ausencia de incidencias en los servicios y, algo menos, la satisfacción del cliente. Llama la atención que un criterio más centrado en los resultados como es la cuantía de daños o pérdidas evitadas se nombra poco. Una posible explicación es la dificultad en su medición. En general, existe un desacuerdo notorio en los criterios de calidad. En cualquier caso, los más citados son la capacidad de respuesta, la ausencia de incidencias y la satisfacción del cliente. El acento en ese tipo de criterios revela que el sector español da más importancia al servicio mismo que a la eficacia. Si un indicador del grado de desarrollo de un sector es el consenso a la hora de definir la calidad y la excelencia en sus servicios, según el estudio mencionado, en España queda terreno por recorrer.

Resumiendo las ideas del capítulo, un riesgo es básicamente un suceso no deseado al que se le asocia una probabilidad. Existe, por lo tanto, una gran diversidad de ellos (medioambientales, delictivos, laborales, médicos, etc.). Los riesgos se pueden analizar desde diferentes perspectivas. La más utilizada y simple es la racionalista. El sector de la seguridad privada la utiliza extensamente. La razón es que tiende a definir la seguridad como la evitación de daños y pérdidas, y a plantearse estrategias de vigilancia y prevención situacional. Por tanto, el objetivo y el camino están claros y, normalmente, existe poca complejidad en el entorno. El modelo racional encaja perfectamente con esas condiciones. Otros modelos de análisis de riesgos son más complejos porque involucran procesos psicológicos, sociales o políticos.

2. Diseño de los servicios

La presente unidad trata de explicar la lógica que existe detrás de los servicios de seguridad privada. El análisis parte de la idea, vista en la unidad anterior, de que existen múltiples estrategias para responder a los problemas de seguridad. Estas se concretan en determinados productos y servicios que comercializa el sector. La forma en que estos son diseñados, vendidos, llevados a cabo y evaluados depende de determinados factores que se discuten en este capítulo. El primer factor que se estudia son las necesidades y prioridades del cliente. En segundo lugar, se analiza el papel que tiene la tecnología en desarrollo de productos y servicios. En tercer lugar, se discute la forma como influye el nivel de riesgo de determinados servicios o clientes. Existen, además, otros factores del entorno de las empresas que afectan a sus servicios, como el marco legal, el mercado laboral, el accionariado o las presiones de la competencia, entre otros. Todos juntos acaban por configurar la oferta de servicios de seguridad privada.

2.1. Estrategias y servicios de seguridad

La seguridad consiste básicamente en situar las situaciones de riesgo en límites aceptables. Esas situaciones pueden ser diversas, pero también existen múltiples posibilidades para darles respuesta; es decir, diversas formas de gestionarlas.

> Las estrategias de seguridad se pueden entender como un conjunto coherente y anticipado de acciones orientadas hacia un objetivo. Una estrategia es, por tanto, una combinación más o menos ordenada de respuestas y objetivos.

Existen diversas estrategias para crear o potenciar la seguridad. Esas estrategias se pueden clasificar de diferente forma. Allan Horwitz (1990) distingue cuatro **estilos de control social**:

- El penal implica el castigo a las personas que se desvían. Existen varios criterios y consideraciones a la hora de escoger y escalar un castigo.
- El compensatorio consiste en que los transgresores recompensan económicamente a sus víctimas.
- El conciliatorio consiste en la negociación conjunta de las partes, ya sea con mediador o sin él, para buscar una solución conjunta al agravio.
- El terapéutico conlleva el tratamiento experto de las personas que se desvían con el ánimo de reintegrarlos a la normalidad.

Todas las estrategias mencionadas son reactivas. Es decir, se ponen en marcha como respuesta a un hecho ya producido. Sin embargo, también existen estrategias preventivas que intentan evitar que se produzca un hecho no deseado o, en todo caso, minimizar sus consecuencias negativas.

La seguridad tiene tres dimensiones: la objetiva, la subjetiva y la tolerable. Por lo tanto, una forma de producirla es gestionar la percepción de inseguridad (o miedo). Se sabe que existen diferentes factores que afectan a esa percepción (informaciones distorsionadas, entornos sucios y desordenados, poca confianza en las instituciones de seguridad, etc.). Se trata, entonces, de actuar sobre ellos. Otra estrategia de seguridad consiste en lograr una mayor tolerancia de la población a ciertos actos desviados, o a determinados colectivos.

La naturaleza misma de los riesgos no determina completamente las estrategias para darles respuesta. Estas son más el fruto de una decisión política y social. Las instituciones pueden utilizar diferentes estrategias en función del momento histórico o de las circunstancias. También pueden combinar varias distintas. Las estrategias institucionales no son inamovibles. La Policía, por ejemplo, está condicionada por el marco del estado de derecho y del sistema penal donde está inmersa. Ello le lleva a desarrollar una estrategia penal predominante en sus respuestas. Sin embargo, la Policía ha ido incorporando estrategias de mediación, de prevención situacional o comunitaria, educativas, etc. en función de los condicionantes que encuentra. Tampoco cabe pensar que la seguridad privada está abocada a utilizar siempre las mismas estrategias. De hecho, la seguridad privada se caracteriza por su flexibilidad para adaptarse a las necesidades de sus clientes.

Así, por ejemplo, una empresa que colabora estrechamente con la Policía tiende a mimetizar sus respuestas penales. Sin embargo, esa misma empresa puede emplear estrategias de prevención situacional con otro cliente.

Por lo tanto, las empresas de seguridad utilizan en la protección de sus clientes diversas estrategias. En algunos casos la seguridad se basa en la obtención de información relevante (detectives privados). En otros el acento recae en la prevención de daños, ya sean personales o económicos (vigilancia, videovigilancia, sensores, disuasión mediante uso de perros). La reparación de daños y pérdidas es otra opción (seguros). También lo es trasladar un caso al sistema penal (denuncia). La recopilación y análisis de información se da en el sector de los servicios (aseguradoras sobre todo) y entre los particulares que recurren a detectives privados. Puede optarse por crear sensación de seguridad a través de mejorar la iluminación o borrar grafitis. En general, **la seguridad privada sigue una estrategia preventiva** y no tanto reactiva. Dicho de otra forma: la seguridad privada vende prevención de daños y pérdidas materiales y personales. Es una prevención vinculada más a la vigilancia y la disuasión que no a atacar las causas de los problemas. En buena medida juega también con la creación de sensación de seguridad. Las respuestas reactivas, como denunciar delitos, se dan, pero son menos frecuentes que en la seguridad pública. La idea

importante en todo esto es que **las estrategias de seguridad son contingentes**; no son intrínsecamente privadas o públicas. La cuestión relevante es qué factores explican la elección de una u otra.

Un servicio de seguridad tiene básicamente tres componentes:

- un objeto a proteger,
- un riesgo o amenaza del que protegerlo, y
- una estrategia para hacerlo.

El objetivo final suele ser evitar o minimizar el daño o la pérdida. De las estrategias de seguridad ya se ha hablado.

Con relación al primer aspecto, el **objeto a proteger**, los clientes de la seguridad privada pueden querer proteger a personas, instalaciones, o bienes materiales. Todos ellos son elementos tangibles. Pero también podrían desear evitar otras consecuencias negativas, como incurrir en responsabilidades por incumplimiento de normas, accidentes o incidentes, perder reputación, encarecer los seguros etc. Incluso, pueden también querer proteger aspectos internos, como sus procesos de producción, o externos, como su posición en el mercado.

Las posibles **amenazas** son incontables. Estas pueden provenir de fenómenos naturales, inundaciones, rayos, terremotos y demás meteoros. Pueden tener origen en accidentes o incidentes que se producen en el transcurso normal de su actividad, como incendios, cortocircuitos, caídas de mercancía, resbalones de trabajadores, atropellos, y otras muchas. Pueden ser el resultado de conductas deliberadas y malintencionadas, como sabotajes, intrusiones, robos, secuestros, extorsiones y un largo etcétera. No todos los riesgos son iguales. Si se analiza la historia de una compañía o se realizan estudios, se ve que cada riesgo va asociado a una probabilidad o posibilidad de que ocurra. Tampoco las consecuencias son las mismas. El daño potencial que produce una inundación en la sala donde están los servidores informáticos de la empresa será mucho mayor que su efecto en los vestuarios. A su vez, el tipo de consecuencias negativas es muy diverso: pérdidas de jornadas laborales, de producto terminado, de información, de imagen corporativa, de posiciones en el mercado, etc. En última instancia, todos estos daños y pérdidas pueden ser estimados en términos monetarios. Como se aprecia, tanto los objetos a proteger, como los riesgos de protegerlos, son muchos y diversos. Todo ello ofrece a la industria de la seguridad un enorme campo de actividad y de especialización (De Waard, 1999).

Cada cliente centra su demanda (y su gasto) en proteger los elementos que tienen una importancia estratégica en su actividad. De la misma forma, también intenta protegerse de aquellas eventualidades más probables. De hecho, el análisis de riesgos consiste precisamente en identificar esos elementos, valorar el grado de exposición que tienen, y calcular las consecuencias que tendría para el cliente que se materializara una eventualidad. Diferentes activida-

des pueden ser sensibles a amenazas de procedencia muy distinta: pérdidas de inventario, absentismo de empleados, accidentes, inundaciones, interrupciones en el suministro eléctrico, plagios, responsabilidades civiles o penales, agresiones contra sus directivos, filtración de información a la competencia, entre otros.

Para una multinacional farmacéutica, impedir un acceso a sus ordenadores de investigación es crucial. Una filtración sobre el último modelo de coche puede resultar catastrófica para una marca. Para el Estado es vital proteger instalaciones críticas, o a sus líderes políticos, entre otros elementos. Para una cadena de supermercados es importante mantener la actividad de la línea de cajas. Si el cliente es un particular, posiblemente protegerá sus propiedades o patrimonio.

Visto desde una perspectiva empresarial, la seguridad es un activo económico: ayuda a mantener o mejorar la calidad, cantidad, o el valor añadido de la producción.

Por lo tanto, cada tipo de cliente tiene un perfil distinto de objetos a proteger. La protección de bienes e instalaciones afecta a todo tipo de clientes, aunque algo más al sector industrial, construcción, y Administración pública. Las empresas que provienen de sectores sujetos a una regulación intensa y a un sistema de responsabilidad como el sector industrial, la banca, la Administración pública, o algunos servicios que contratan seguridad privada, además de otros motivos, para evitar sanciones o no incurrir en responsabilidades. El sector de la seguridad español gira mucho en torno a la protección de instalaciones y bienes. Sin embargo, la protección de otros elementos que implican mayor especialización no se asume tanto, o se acaban derivando a empresas fuera del sector. Uno de ellos es la protección de la posición en el mercado. Esta puede verse amenazada por diversas causas (por ejemplo, filtración de patentes, problemas en la producción, desfase tecnológico, uso de información inadecuada o falseada). La seguridad toma aquí aspectos de inteligencia organizacional, de espionaje industrial, o de protección de la propiedad intelectual, entre otros.

La demanda de servicios de seguridad corporativa adquiere cada vez mayor complejidad y entronca con otras actividades especializadas de consultoría de negocios o ingeniería industrial. Lo mismo ocurre con la seguridad de los procesos de producción. Esta se conecta con aspectos de organización del trabajo, seguridad laboral o control de la calidad. La información es un bien estratégico en la sociedad del conocimiento. De manera creciente, así lo entienden muchas empresas y despachos que ofrecen servicios de seguridad informática, protección de bases de datos, contraespionaje, investigación comercial o investigación privada. El cliente es muy transversal y proviene de cualquier actividad, aunque quizás algo más los servicios públicos y privados. Estos ejemplos hacen pensar que ciertas actividades de seguridad muy cualificadas todavía no han alcanzado todo su desarrollo potencial en España, aunque se echan en falta estudios comparativos.

2.2. Demandas de clientes

La oferta de productos y servicios de seguridad está condicionada en buena medida por la demanda del cliente; y esta, por la forma en que este identifica, conceptualiza y prioriza sus necesidades de seguridad (Torrente, 2006). Las empresas, como las personas, realizan sus propios análisis de riesgos. En ocasiones se basan en las percepciones subjetivas de sus responsables, en otras son estudios que realizan los directores de seguridad, gabinetes especializados, o los proveedores de servicios. De forma más o menos informada, las empresas mantienen concepciones sobre qué objetos habría que proteger, de qué riesgos, de qué manera, y cuánto dinero se está dispuesto a invertir en ello. La demanda que finalmente realiza el cliente depende de cómo evalúa esos elementos, pero también de si concibe la seguridad como un gasto o una inversión.

La seguridad tiene una dificultad intrínseca que superar para poder venderse. Esta consiste en que, lo normal, es que no pase nada. Para las personas o empresas que mantienen esta creencia, pagar un servicio de seguridad puede no tener sentido, o no ser una prioridad. En esos casos, la percepción del **valor añadido** de la seguridad es poca. Entonces, probablemente, no habrá demanda a no ser que se esté obligado por la legislación o las condiciones de su seguro a adoptar ciertas medidas de seguridad. Por el contrario, otras empresas perciben la seguridad como una inversión. Su objetivo al contratar un servicio de seguridad es prevenir los costes económicos importantes que supondría la materialización de ciertos riesgos a los que está expuesto. Por otra parte, también puede valorar otros beneficios, como ofrecer una imagen de seguridad o de prestigio social a sus clientes, transmitir mensajes disuasorios a potenciales transgresores, apoyar a sus directivos preocupándose de su integridad física, abaratar la prima del seguro, o protegerse de eventuales sanciones y reclamaciones.

Según los directivos de las empresas de seguridad españolas (Torrente, 2006), la motivación principal de sus clientes para demandar seguridad es prevenir daños y pérdidas directas, o evitar sanciones por no cumplir con la normativa. La demanda de seguridad va poco asociada a cuestiones de imagen (salvo quizás en algunos servicios de cara al público), protección personal, apoyo a los procesos productivos, o como forma de abaratar las primas de los seguros. Quizás por ello las empresas de seguridad se ven a sí mismas más como proveedoras de servicios de prevención de daños y costes, que como colaboradores en el funcionamiento de la actividad de sus clientes. Tienden a pensar que buena parte de las demandas que reciben, incluyendo las del sector público, conciben la seguridad más como un gasto que como una inversión. Hasta cierto punto, tampoco se contemplan a sí mismas como reforzadoras de la seguridad pública.

El tipo de demanda varía según el **tipo de clientes**. Por ejemplo, entre los clientes del sector industrial los riesgos suelen ser explícitos y vinculados al tipo de materias primas con las que trabajan, o sus procesos de producción. En

las grandes firmas industriales, los responsables de riesgos laborales, industriales, de mantenimiento, o los directores de seguridad tienen un protagonismo en el hecho de definir necesidades de seguridad. Por ello, las exigencias a los proveedores de este nicho del mercado suelen ser mayores que en el sector de los servicios privados o públicos, y las discusiones se tornan más técnicas. En las grandes compañías suele existir un responsable o director de seguridad, en las más pequeñas esas funciones, a veces, las realizan los encargados del mantenimiento. Como consecuencia de todo ello, el sector industrial valora la capacidad de servicio y técnica de los proveedores de seguridad.

El **tamaño de la empresa** de seguridad se relaciona, en parte, con el tipo y carácter de los servicios que ofrece (Torrente, 2006). Pero lo hace, en buena medida, porque tienen clientes distintos. Las empresas de seguridad muy grandes ofrecen unos servicios más diversificados y generalistas (aunque con un peso importante de la vigilancia), mientras que las empresas medianas y pequeñas ofrecen servicios más especializados. Los clientes importantes del sector suelen consumir muchos servicios de vigilancia, mientras que el montaje y mantenimiento de equipos tiene una mayor importancia relativa entre los clientes medianos y pequeños. Por otra parte, a medida que aumenta el tamaño de la empresa de seguridad, los servicios que se venden ponen más el acento en la planificación. En la práctica, eso significa que van más acompañados de estudios previos de riesgos. Eso sucede sobre todo en las empresas de cierto tamaño, que son las que suelen tener clientes importantes y con necesidades complejas que hay que analizar y planificar bien. Ese análisis se hace en colaboración con los directores de seguridad, que son una figura presente, sobre todo, en las grandes firmas. En ese sentido, se puede afirmar que la capacidad del proveedor de definir el servicio de seguridad es menor cuando el cliente es una empresa grande o multinacional. Las negociaciones con ese tipo de clientes suelen ser duras. Por el contrario, las empresas de seguridad más pequeñas suelen tener también clientes menores con los que se da una mayor confianza y cercanía. A pesar de ello, los clientes multinacionales ofrecen al sector un gran volumen de facturación. Además permiten a los proveedores de seguridad expandirse a través de ellas en otros países, o beneficiarse de su gran red social.

2.3. Rol de la tecnología

La innovación y el desarrollo tecnológico tienen una incidencia no solo en la oferta de productos y servicios, sino también en la dinamización de la demanda. La innovación comprende nuevos conceptos de seguridad, formas de organizarla y aplicaciones técnicas. Más que tecnologías de la seguridad, existen tecnologías aplicadas a la seguridad (Gabrosky, 1998). La evolución de estas es muy rápida. Sin embargo, el rol que juega en el sector es más complejo de lo que se piensa habitualmente. Un primer debate es si las tecnologías de la seguridad, cada vez más fiables y baratas, suplen al factor humano, cada vez más escaso y caro. Posiblemente ciertas tareas claves en seguridad que realiza un vigilante (mediar, tranquilizar, incluso disuadir) no pueden mecanizarse. Pero quizás otras sí. En el fondo, la cuestión central es qué ventajas y límites

tiene la tecnología respecto a los servicios de base humana. Por otra parte, no todas las tecnologías son iguales ni en su eficacia, ni en su capacidad de generar ventas (Gabrosky, 1998).

Los directivos de las empresas de seguridad españolas valoran más la inversión para desarrollar productos o procesos nuevos, incluso para mejorar la organización (Torrente, 2006). Sin embargo, la inversión para el desarrollo de conocimiento básico, compra de patentes, se valora como menos importante. Por otra parte, las razones declaradas por las que merece la pena invertir en I+D son mantener o aumentar la cuota de mercado y formar o capacitar al personal. Curiosamente no se vincula la investigación básica o la compra de patentes a esos fines. Los directivos mantienen diferencias de percepción sobre la importancia de la tecnología en los servicios según el tamaño de la empresa o su actividad. Los de empresas pequeñas subrayan la importancia que tiene conocer de cerca las necesidades del cliente y el trato personal, las medianas ponen énfasis en la capacidad de darle un buen servicio, y las grandes prefieren un equilibrio entre profesionalización y tecnología.

Existen ciertos segmentos, como la prevención de incendios, donde dominan los sistemas basados en la tecnología. Pero en este caso, se trata solo de activar automáticamente la extinción ante el indicio de fuego. Pero en el sector del *security* siempre hace falta, ante un aviso de emergencia, que alguien tome decisión sobre cómo actuar. La duda es si el decisor debe realizar también las labores de vigilancia. En cualquier caso, los directivos del sector coinciden en que la tendencia es tener menos vigilantes, pero más especializados y preparados. Pero, para ello, es necesario que el cliente también conciba la seguridad como un servicio especializado y de alto valor añadido.

Una de las tendencias en el desarrollo tecnológico es hacia la confluencia e **integración de diferentes tecnologías** (Gabrosky, 1998). Ello está llevando una mayor convergencia entre ramas diferentes de la seguridad (incendios, intrusión, vigilancia, etc.). Existen numerosos ejemplos en que la domótica, las tecnologías informáticas, o las de comunicaciones se han integrado. Al hacerlo, las organizaciones deben entrar en áreas de negocio nuevas. Normalmente la innovación es más fácil en empresas pequeñas y flexibles. Otra posibilidad es la colaboración estratégica entre compañías cuya tecnología tiende a converger. Otra tendencia es ir hacia sistemas más **inteligentes e interactivos**. Los sistemas no solo detectan con sus sensores, sino que estos están conectados a sistemas informáticos. El resultado es que son capaces de buscar, analizar y comunicar información en tiempo real. Esa integración ente las tecnologías sensoriales (detectores, escáneres, cámaras), de la información (bases de datos, computadores) y de las comunicaciones (telefonía digital, satélites) ofrece unas posibilidades enormes en el campo.

Las nuevas tecnologías producen ciertos cambios en las formas de trabajar (Gabrosky, 1998). Un ejemplo es el efecto de internet en la investigación privada. El trabajo del detective privado consiste en proporcionar información a

su cliente. Esa información tiene que ser relevante y presentarse en la forma adecuada según el fin. Pueden ser pruebas para un juicio, informes comerciales técnicos, evidencias de conductas, datos personales reservados, o datos financieros sobre empresas. Es decir, se pide información que ayude a la toma de decisiones. Normalmente, se trata de informaciones que este no puede conseguir fácilmente, ni son públicas o accesibles. Ciertas informaciones las obtienen a través de seguimientos, pesquisas, simulaciones, o a través de contactos en ciertas instituciones. En algunos casos existen acuerdos informales de reciprocidad entre despachos o detectives. Los despachos más grandes mantienen relaciones con otros gabinetes extranjeros que les ponen en contacto con bufetes de abogados o instituciones de otros países. Internet cambia el trabajo del detective al permitir obtener una cantidad de información de las redes sociales o de otros muchos sitios virtuales. También porque facilita y agiliza el intercambio de información entre colegas o entre despachos. Sin embargo, las nuevas tecnologías no desplazan totalmente a los métodos tradicionales. La profesión de detective sigue utilizando las redes de contactos que facilitan el acceso a determinadas informaciones.

La innovación y la tecnología también introducen cambios en la organización de los servicios (Fisher y Green, 1998; Gabrosky, 1998). Un ejemplo son los servicios de vigilancia, que cada vez son más tecnificados y con menos personal. La mecanización completa de la vigilancia es difícil porque, como se ha comentado, en los momentos críticos es necesario tener a alguien en el lugar y momento justo para que evalúe la situación y tome decisiones. La existencia de alarmas conectadas a centrales receptoras y a los móviles de los propietarios permite innovar en los servicios.

Un ejemplo son los llamados servicios de "acuda" que buscan racionalizar el uso del vigilante. Este solo acude al espacio protegido cuando se produce una alarma y entra en él con la llave cedida previamente por el propietario. Otro cambio que permite la tecnología es hacer copartícipe al cliente en la toma de decisiones cuando se produce una situación de alarma. La señal de alarma en una vivienda se envía, junto con imágenes y sonidos en tiempo real, al teléfono móvil del propietario y a la central de la compañía de seguridad. La central de alarmas entra en contacto con el propietario y valoran juntos si se trata de una verdadera situación de alarma o no.

Los cambios tecnológicos producen, a menudo, desajustes entre la realidad del mercado y su regulación (Rubise, 1994). La innovación en el sector va muy rápida y la innovación legislativa es más lenta. Un ejemplo gráfico es la tendencia hacia la integración de sistemas. Así, los nuevos sistemas demóticos integran y gestionan sistemas diferentes de un hogar, desde la temperatura, iluminación, videosupervisión de niños, monitorización de ancianos o enfermos, o la alarma antirrobo. La información que procesan puede tener múltiples aplicaciones en seguridad, ocio, en medicina, o en asistencia social. Esos sistemas son capaces de comunicarse con centrales de alarma que, a su vez, pueden recibir y gestionar información procedente de diversas fuentes (por ejemplo, señales telefónicas e imágenes digitales, señales de GPS, o información de Internet). El problema se plantea cuando, en contra de la tendencia

a la integración de sistemas y funciones, la legislación de seguridad privada insiste en separar las funciones de seguridad de otras funciones. Ello dificulta la realización de servicios integrales al hogar.

2.4. Control del riesgo

El sector de la seguridad trabaja con el riesgo. Sin embargo, dado que están sobreexpuestos a los mismos, tienen la necesidad de valorarlos bien y saber evitar los más serios o, al menos, mantenerlos bajo control. De hecho, la clave de su negocio está en asumir los menores riesgos posibles como empresa. Eso mismo ocurre con otras actividades relacionadas con la seguridad (y con todas en general). Así, lo primero que aprende un policía es a gestionar las situaciones conflictivas y no exponerse personalmente. Las compañías de seguros realizan constantemente cálculos actuariales con el objeto de no asumir riesgos financieros excesivos.

Los expertos en riesgo lo son porque saben controlarlo. Protegiendo la seguridad de sus clientes, el sector de la seguridad puede verse expuesto también a riesgos para sus empleados, sus equipos, o a la propia empresa (riesgos financieros, responsabilidades penales y civiles, entre otras). Las fuentes son muy diversas: riesgos tecnológicos (informáticos, de las comunicaciones), industriales (accidentes nucleares o químicos), naturales (inundaciones, terremotos, tormentas), financieros, de mercado (espionaje industrial, fuga de cerebros) pequeña delincuencia (robos, hurtos, violencia), delincuencia organizada (terrorismo, tráfico ilegítimo de mercancías), delincuencia de las organizaciones (fraudes en productos, publicidad falsa, contaminación), etc.

Por lo tanto, no hay nadie que valore tanto la seguridad como una empresa de seguridad (o de seguros). Su continuidad depende de controlar el riesgo. Los riesgos que asume el sector varían, en parte, según la actividad del cliente. Por ello, el cliente ideal sería el que valora la seguridad como un valor añadido, se deja asesorar, tiene una capacidad de compra alta, un potencial de expansión en sus compras, y no presenta riesgos o problemas extraordinarios; y si tiene alguno, no de forma continuada. La preferencia entonces es asumir servicios de riesgo moderado y derivar hacia otros actores o hacia el Estado los servicios de mayor riesgo. La empresa de seguridad necesita también de un entorno relativamente seguro donde realizar su actividad económica. El garante último de ese entorno es el Estado. Ello plantea el debate teórico de si se está produciendo una división de funciones en la que el sector privado está asumiendo los casos de bajo riesgo y el Estado los de alto riesgo (Becker, 1974).

Delante de un riesgo destacado, la empresa puede decidir asumirlo pactando toda una serie de salvaguardas con el cliente, subiendo el precio, contratando seguros adicionales, subcontratando otras compañías para determinadas

tareas, o modificando el formato u organización de los servicios de seguridad. El riesgo se convierte así en un elemento más que influye en el diseño de los productos y la organización de los servicios de seguridad.

Por ejemplo, el uso de cristales blindados en bancos, gasolineras, administraciones de loterías, etc. surge en una época de gran auge de la heroína y donde se producen muchos asaltos ligados a su consumo.

También puede decidir no asumir el riesgo y no trabajar con él. Siempre es interesante analizar qué tipo de riesgos no son asumidos por la industria de la seguridad, y las razones que existen para ello. La decisión de rechazar un servicio se suele producir cuando los posibles riesgos no compensan la rentabilidad del mismo.

En España no existen apenas estudios sobre el tipo de **situaciones o problemas** que se detectan en los servicios de las empresas de seguridad. Un estudio afirma que se dan tres grupos de situaciones (Torrente y otros, 2005).

- En un primer grupo están las más numerosas, que tienen que ver con la propiedad y, dentro de ellas, los pequeños robos y, algo menos, el vandalismo. Llama la atención que, desde el mundo privado, se observan también situaciones que se pueden relacionar con la delincuencia organizada, o al menos con delitos de grupo (robos en polígonos industriales o chalets a cargo de bandas, sabotajes sofisticados, tráfico de drogas, amenazas terroristas…).

- En un segundo grupo estarían las situaciones más relacionadas con los conflictos de convivencia, violencia cotidiana, y medio ambiente (conflictos, peleas…).

- En tercer lugar está una diversidad de situaciones contra la empresa (como ataques a la seguridad informática), u otras que tienen que ver con determinadas malas prácticas de la propia organización a la que sirven.

La seguridad privada puede ser un observador privilegiado sobre ellas. Sin embargo, los delitos contra el medio ambiente, el blanqueo de dinero, o el mal uso de fondos públicos no se detectan según ese estudio. El autor concluye que, en general, la seguridad privada española está asumiendo riesgos moderados, y que los campos de mayor riesgo o conflictividad quedan relativamente fuera de sus servicios.

El sector de la seguridad privada detecta de forma creciente riesgos derivados de una nueva delincuencia global, o al menos transnacional. Son incidentes que implican a redes o bandas internacionales de delincuentes, ataques informáticos, terrorismo internacional, o accidentes a gran escala. La extensión de la amenaza, las graves consecuencias que puede tener, el poder de los grupos, su sofisticación, o los limitados instrumentos para afrontarla hace que algu-

nas firmas se replanteen algunos servicios. Un ejemplo es el impacto que tuvo entre las compañías aseguradoras y de seguridad los atentados del 11 S en Estados Unidos y 11 M en España.

Responsabilizarse de la seguridad de un gran aeropuerto o asegurarlo dejó de ser un negocio muy atractivo. El problema no se resuelve mediante la adopción de nuevas medidas de seguridad, o que estas sean más sofisticarlas. No se trata de buscar nuevas vías para sacar ventaja en la tradicional carrera entre el mundo de la seguridad y el del delito. El problema es responder ante las enormes consecuencias y responsabilidades por la quiebra de la seguridad.

Ante estos nuevos riesgos globales existe la necesidad de contar con información adecuada sobre las redes de delincuencia, sus estrategias o sus actividades. A pesar de que las grandes compañías pueden obtener y analizar informaciones procedentes de sus sedes centrales, la mejor información está en manos de la Policía y de las redes de colaboración policial internacional. La inteligencia policial es clave para combatirlas. Ese hecho es un aliciente para que el sector privado busque la colaboración y ayuda del sector público. Pero, por otra parte, las grandes multinacionales de la seguridad podrían ayudar mucho dado que tienen presencia en muchos países y recogen gran cantidad de información en su tarea diaria de proteger a sus clientes. Todo ello plantea el debate sobre las posibilidades de una cooperación frente a ese tipo de amenazas.

Una de las incertidumbres más importantes para el sector son las consecuencias financieras que se derivan de las grandes catástrofes naturales, la delincuencia global, o los actos del terrorismo internacional. Ello está alterando las reglas de juego en el sector. Las compañías de seguros y de seguridad cada vez son más reticentes a aceptar los riesgos de proteger determinadas instalaciones. Incluso algunos Estados están fijando techos en su responsabilidad. Pero, por otro lado, en algunos sectores concretos, concretamente en los de transportes y comunicaciones, los atentados terroristas de Nueva York y Washington provocan un aumento de la demanda en seguridad. En general, y salvo en esos sectores económicos concretos, el impacto de los atentados no ha sido palpable, sin embargo, se aprecia un cambio de sensibilidad general hacia los temas de seguridad. En países como Francia, las compañías de seguros y las de seguridad se coordinan tanto en el mercado como en sus acciones de lobby para reformas legislativas. Es lógico si se piensa que el riesgo depende de la probabilidad de que ocurra un incidente multiplicado por la gravedad potencial de sus consecuencias. Las empresas de seguridad inciden en la probabilidad y las de seguros en compensar los costes de esas consecuencias. En España no hay tanta tradición, pero teniendo en cuenta las dinámicas señaladas, la tendencia es ir hacia una mayor coordinación.

En teoría, el sector privado puede asumir cualquier tipo de servicios de seguridad. Sin embargo, determinados tipos de delitos cruciales para la seguridad de los países, como el terrorismo internacional, el tráfico de drogas a gran escala, o el tráfico de inmigrantes ilegales, no generan una demanda desde el merca-

do. Únicamente el Estado es capaz de generar esta demanda. Si existe esa demanda pública, el sector privado puede colaborar. Sin embargo, hay otro tipo de límites. Un principio básico de las empresas de seguridad (y de todas) es no entrar en colisión con las actividades ni los intereses de sus clientes. Por ello se dice que una limitación del sector privado a la hora de asumir cualquier tipo de servicios es que, en función de la composición de sus clientes principales, pueden entrar en contradicciones.

Por ejemplo, difícilmente una empresa que presta sus servicios a un banco estará interesada en investigar el blanqueo de capitales, en especial si es un buen cliente.

Una empresa de seguridad puede servir al mismo tiempo, y sin conflictos, a dos clientes que compiten en el mercado. Sin embargo, potenciales demandas del Estado en su lucha contra la delincuencia de las organizaciones resulta difícil trasladarlas al sector privado (Mir, 1999). Existe todo un debate sobre la relación Estado y mercado de la seguridad que se analiza en la primera unidad del módulo “La seguridad privada en España”.

Actividades

1. Localizad un informe de seguridad en Internet y mirad primero su estructura (su índice) y su contenido. Comparad la estructura con el modelo que aparece en el cuadro 3.

2. Localizad un cuestionario de seguridad o una matriz de riesgos en Internet. Estudiadla y explicadle a un compañero/a cómo funciona.

3. Elegid un almacén de un familiar, una tienda que conozcáis, vuestra empresa (si es pequeña), o cualquier otro espacio al que tengáis un acceso fácil. Realizad la evaluación de riesgos y escribid los resultados en un documento con la estructura adecuada.

4. Elegid 5 artículos de revistas que traten sobre una realidad delictiva. Decid cuáles de esos artículos tienen un enfoque descriptivo o explicativo.

Ejercicios de autoevaluación

Unidad 1

1. ¿Qué es el análisis de riesgos?

2. ¿Podríais dar una definición de "vulnerabilidad"?

3. Explicad en qué consiste la planificación de la seguridad.

4. ¿Qué utilidad práctica tiene un plan de seguridad?

5. ¿Qué ventajas tienen las encuestas de victimización sobre las estadísticas policiales como fotos de la realidad delictiva?

Unidad 2

6. ¿Cuáles son los tres componentes básicos de un servicio de seguridad?

7. ¿Qué factores influyen en que un servicio de seguridad se conciba y se organice de una determinada manera?

8. Explicad algún rol de los que cumple la tecnología en la seguridad privada

9. ¿Qué tipo de barreras puede tener una empresa de seguridad para trabajar en delitos de cuello blanco?

10. ¿Cuál suele ser el planteamiento de las empresas de seguridad frente al riesgo alto en sus servicios?

Solucionario

Ejercicios de autoevaluación

1. Proceso por el que se identifican y evalúan posibles amenazas, los puntos vulnerables del sistema a proteger, y se estiman las posibles consecuencias. Esa información se recoge en un informe de riesgos.

2. La noción de "vulnerabilidad" es, dado su nivel de protección actual, la susceptibilidad de un bien o persona a sufrir un determinado nivel de daños o pérdidas de todo tipo, debido a la realización de una amenaza particular.

3. La planificación de la seguridad es un proceso por el que, tras analizar los riesgos, se fijan unos objetivos de seguridad, se elige una estrategia que se despliega a través de toda una serie de actuaciones. Además, se prevén los recursos necesarios, se establece una organización de las tareas con sus procedimientos y controles, y se fijan las responsabilidades correspondientes. Suele incluirse, además, un protocolo de seguridad que define las reglas y procedimientos que sirven para coordinar las respuestas para diversos tipos de eventualidades, o aspectos concretos como las comunicaciones, por ejemplo. Se planifican todas las necesidades de formación o reciclaje del personal. Se prevén futuras evaluaciones y criterios para modificar o corregir el propio plan

4. El plan sirve a un doble propósito de ayudar a vender el servicio y, una vez ha sido comprado, es una guía del trabajo a desarrollar. Con relación a lo primero, a través del plan, el cliente también puede estudiar la propuesta de seguridad que se le hace y su coste. Es decir, va a poder apreciar la calidad de la propuesta y lo que incluye. El plan también ayuda a que en el proceso de negociación entre proveedor y cliente sea más ordenado y concreto. Durante la ejecución, también sirve para proteger al proveedor de seguridad de posibles exigencias del cliente que no se habían incluido, ni presupuestado, en el plan.

5. Las estadísticas miden el delito denunciado; las encuestas el percibido como tal por la población. Ofrecen una información cuantitativa y representativa de la delincuencia sufrida, aunque no se haya denunciado. Tienen la ventaja de que los resultados se pueden extrapolar a la población. Además permiten conocer una gran cantidad de información de la víctima y de sus actitudes y opiniones. Sin embargo, solo permiten conocer los datos del delincuente o determinados detalles del delito si esta los conoce. Las encuestas no son capaces de recoger todos los delitos ya que dependen de que estos tengan una víctima individual, que pueda responder, que sea consciente de serlo, y conozca los detalles del delito. Eso no ocurre con los delitos de víctima colectiva, o la mayoría de los de cuello blanco, o delincuencia organizada.

6. Un objeto a proteger, una amenaza del que protegerlo, y una estrategia para hacerlo.

7. La forma en que los servicios de seguridad son diseñados, vendidos, llevados a cabo y evaluados depende de las condiciones del entorno de las empresas. Algunos de ellos son el marco legal, el mercado laboral, el accionariado, o las presiones de la competencia, entre otros. Sin embargo existen tres relevantes que son las necesidades y prioridades del cliente, la tecnología y el nivel de riesgo de determinados servicios o clientes.

8. La innovación y la tecnología permiten ampliar y renovar la oferta de productos y servicios, y también dinamizar la demanda. Permiten ahorrar costes. Pero también producen cambios en la forma de trabajar y de organizar el trabajo. Incluso llevan a la integración de los sectores.

9. La principal barrera es una contradicción de intereses. Pero también pueden existir barreras relacionadas con el acceso a información relevante y desbalances de poder.

10. Realizan valoraciones de beneficio-riesgo. Pero si estos son altos, intentan evitar o minimizar riesgos.

Bibliografía

Broder, James F.; Tucker, Eugene G. (2011). *Risk Analysis and the Security Survey*. Oxford: Elsevier.

International Organization for Standardization (2009). *Risk management - Principles and guidelines*. ISO 31000:2009.

International Organization for Standardization (2009). *Risk assessment techniques*. ISO 31000.

Merkelbach, M.; Daudin, P. (2011). *From Security Management to Risk Management: Critical Reflections on Aid Agency Security Management and the ISO Risk Management Guidelines*. http://www.securitymanagementinitiative.org/index.php?option=com_docman& task=cat_view&gid=22&Itemid=32&lang=en