Els serveis de seguretat

Diego Torrente

PID_00208837

Universitat Oberta de Catalunya

Índex

Introducció

Aquest mòdul el dedicarem a explicar com es planifiquen i gestionen els serveis de seguretat. Començarem per aclarir que la seguretat i el risc es poden analitzar des de diferents perspectives acadèmiques. Segons la perspectiva que s'adopti, les categories d'anàlisi també són diferents. Tant la seguretat privada com la pública poden analitzar els riscos des de qualsevol d'aquestes perspectives. També poden triar qualsevol tipus d'estratègia de seguretat a l'hora de planificar, gestionar o avaluar la seva activitat. De tota manera, la perspectiva racionalista és la més emprada pel sector privat de la seguretat. També ho són les estratègies preventives. Per tot plegat, dedicarem bona part del mòdul a explicar com s'avaluen riscos o s'elabora un pla de seguretat des d'aquestes òptiques.

Objectius

Els objectius del mòdul són els següents:

1. Conèixer les diferents perspectives en l'anàlisi de riscos.

2. Dominar el procés emprat en l'anàlisi racional de riscos.

3. Conèixer el procés de planificació, gestió i avaluació de la seguretat.

4. Comprendre les diferents estratègies emprades en seguretat.

5. Entendre com influeixen en els serveis les demandes dels clients.

6. Saber quin rol té la tecnologia en els serveis de seguretat.

7. Comprendre la importància del risc com a factor en els serveis.

1. Anàlisi i gestió de la seguretat

Aquesta unitat té l'objectiu de mostrar els fonaments analítics en què recolzen els serveis de seguretat, tant públics com privats. L'apartat planteja tant qüestions teòriques com aplicades. En primer lloc, analitzarem el model d'anàlisi racional de riscos, que és el marc que fa servir més el sector privat, i per això hi dedicarem més atenció.

En segon lloc presentarem altres models d'anàlisi, com el psicològic o el sociològic. En l'apartat següent exposarem la qüestió de la planificació i gestió de la seguretat. Aquestes s'analitzen també des d'una perspectiva sobretot racionalista. Discutirem què és un pla de seguretat i quins elements el formen. Explicarem en què consisteix la gestió de riscos i comentarem breument casos específics com la gestió d'emergències. Finalment, explicarem què és l'avaluació, per a què serveix, de quines modalitats n'hi ha i quins criteris es poden fer servir.

1.1. Anàlisi racional de riscos

El risc es pot definir com la possibilitat o probabilitat que s'esdevingui una situació adversa. Aquesta situació no desitjada es pot desencadenar per una decisió pròpia, una situació de l'entorn o l'acció d'una tercera persona. La idea de *risc* té dos components principals:

- un judici de valor sobre uns resultats que no es desitgen, o que es veuen com a negatius, i l'impacte o dany del qual es calcula;
- l'estimació d'una probabilitat o possibilitat que s'esdevinguin aquests resultats.

Expressat com a fórmula seria de la manera següent:

R = D × P (risc = magnitud del dany × probabilitat que s'esdevingui).

El concepte se sol fer servir en contextos en què hi ha una acció o decisió humana pel mig. Per a designar un esdeveniment desfavorable en què no intervé una decisió humana (un atzar de la naturalesa, un fet no imputable al factor humà), se sol reservar el terme *perill*.

Quan es desconeixen tant els possibles resultats (no se sap si seran positius o negatius) com la probabilitat que s'esdevinguin, es parla d'*incertesa*. La diferència fonamental entre risc i incertesa és que assumim que el risc és calcula-

ble i gestionable, mentre que en la incertesa no es poden fer càlculs i la gestió resulta molt més difícil. En el supòsit més bo, solament podem dibuixar possibles escenaris incerts.

> Això és el que fan, per exemple, els militars quan han d'ocupar un país i no saben ben bé què passarà perquè hi ha centenars de variables en joc. En la vida política s'esdevé una cosa semblant. En aquests casos, no se saben els *outputs* de l'acció (els resultats possibles, tant si són bons com dolents). Això fa molt difícil anticipar els esdeveniments, i les implicacions i conseqüències que tindran. Tampoc no se saben les variables rellevants que influiran en l'acció i que podrien ajudar a prendre una bona decisió. Com que no es poden establir relacions de causa-efecte, és gairebé impossible marcar objectius o prioritzar-los. D'altra banda, no se saben les probabilitats que s'esdevingui alguna cosa. Amb aquestes condicions, gairebé és impossible generar coneixement.

La noció de *risc* forma part de la nostra cultura col·lectiva i de la societat moderna. Pensem i gestionem el món en termes de riscos i oportunitats. L'economia, l'enginyeria, l'arquitectura i altres camps científics fan servir constantment la noció de *risc*. Aquesta idea forma part del paradigma de racionalitat que, segons Weber (1964), és el gran motor d'aquesta societat. Malgrat això, els sociòlegs expliquen que hem passat d'una societat moderna a una societat postmoderna en la qual s'esvaeix el paradigma racional. La ciència perd capacitat de donar resposta als problemes que es presenten. En la societat postmoderna, la incertesa és cada vegada més gran i s'ha d'aprendre a conviure-hi. Hi ha molts aspectes de la vida que cada vegada són més incerts: els mercats laborals, els financers, l'escalfament global, les pandèmies de la grip, la feina, la família, etc. La societat global es converteix així en la societat del risc i, sobretot, de la incertesa (Beck, 1992).

El risc es pot analitzar des de diferents disciplines i, per tant, des de diferents perspectives. La perspectiva dominant en l'anàlisi de riscos és el paradigma racional. És la visió que elabora des de les enginyeries, des del càlcul actuarial i des de moltes altres disciplines tècniques. També és la perspectiva més estesa en el món de la seguretat privada, encara que no l'única. És molt freqüent que les anàlisis de riscos de les consultories de seguretat o de les mateixes empreses del sector es facin des d'aquesta visió. Malgrat això, no hi ha un determinisme, i el sector privat pot arribar a treballar des de qualsevol dels models que comentem en el capítol. El paradigma o model racional parteix d'algunes premisses. La principal és que els riscos es poden analitzar o avaluar objectivament i científicament. Per tant, es pot planificar racionalment la seguretat i prevenir riscos. També s'accepta, de manera més o menys general, que el punt de vista extern de l'expert és més racional que el dels actors implicats.

El concepte d'**anàlisi de riscos**, des d'aquest punt de vista, és el procés pel qual s'identifiquen i avaluen possibles amenaces, els punts vulnerables del sistema que cal protegir, i s'estimen les possibles conseqüències. Aquesta informació es recull en una **avaluació de riscos** (*risk assessment*). Una vegada feta, s'avaluen diferents alternatives o estratègies d'actuació, es tria la millor i es proposen mesures (anomenades també de vegades *contramesures*) per a reduir els riscos a un nivell acceptable. Tota aquesta informació es reflecteix en un **pla de segu-**

retat en què, a més, s'especifica com s'aplicarà, qui en són els responsables (*risk management*), què costarà, com s'avaluarà i quan i, si escau, altres qüestions com la comunicació de riscos a gestors o a la població (*risk communication*).

En l'**anàlisi racional de riscos** hi ha alguns conceptes bàsics. L'*amenaça* es refereix a la possibilitat o probabilitat que una eventualitat concreta (un llamp, una extorsió, un robatori, etc.) es manifesti amb una intensitat, un temps i una localització concrets. La noció de *vulnerabilitat* és, atès el nivell de protecció actual que té, la susceptibilitat d'un bé o una persona a patir un determinat nivell de danys o pèrdues de tota mena a causa de l'acompliment d'una amenaça particular. De vegades, per a referir-se a la pèrdua o repercussió negativa causades per la materialització d'una amenaça es parla d'impacte (estimat o real). El concepte de *mesura* (o *contramesura*) *de seguretat* designa els instruments i mecanismes que miren de reduir riscos actuant sobre els danys potencials o bé sobre la probabilitat d'ocurrència. Hi ha diversos criteris per a classificar-la. Se sol distingir entre mesures preventives, que dissuadeixen o redueixen l'impacte (tanques, càmeres); mesures detectores, que avisen que hi ha alguna cosa que no va bé (alarmes, detectors); mesures correctores, que neutralitzen els problemes identificats (un antivirus); o mesures repressores, que castiguen els infractors (detenció, multes).

L'anàlisi racional de riscos fa servir un protocol bastant establert en què cal seguir uns quants passos (vegeu el quadre 1) (Fisher i Green, 1998).

Quadre 1. Protocol de l'anàlisi racional de riscos

1. Identificar els béns, sistemes o persones que cal protegir. Estimar-ne el valor.
2. Identificar i descriure les amenaces i la probabilitat d'ocurrència.
3. Identificar i avaluar els controls o les contramesures que hi ha.
4. Estimar la vulnerabilitat de béns i sistemes (risc residual).
5. Calcular l'impacte potencial (econòmic o d'altra mena) per a cada zona i tipus de risc.
6. Proposar controls adequats i justificar-los (recomanacions).
7. Recollir tota aquesta informació en una avaluació de riscos.

Font: elaboració pròpia

El primer pas és fixar un objectiu de seguretat. Es tracta d'establir els estàndards de seguretat que es consideren acceptables. El segon és analitzar o avaluar els riscos (amenaces i vulnerabilitats) del sistema que cal protegir. Per a això es fa un inventari de tots els actius i objectes que cal protegir, i s'analitza la importància econòmica i estratègica que té cadascun en el funcionament global de l'entitat. Normalment, aquesta importància s'estima en termes monetaris. Així es calcula en termes de diners les jornades perdudes, la reculada de posició en el mercat, les lesions causades i qualsevol altra situació. D'aquesta manera es pot fer una valoració comparable dels diversos costos que tindria un incident. L'objecte que cal protegir poden ser persones (integritat física, salut, benestar), recursos naturals (aire, aigua, natura), infraestructures, edificis, mercaderies, instal·lacions, equips, informació (financera, comercial, de productes, de clients, de procediments, etc.) i altres objectes intangibles.

L'anàlisi racional de riscos es basa en una metodologia que s'explica en l'informe d'auditoria de riscos, en què es desenvolupa el criteri que se segueix a l'hora d'atribuir un valor econòmic a un determinat objecte. Ha de quedar clar com es calcula el valor dels objectes que cal protegir.

Per exemple, si es calcula el valor econòmic d'una màquina sabotejada, es pot fer respecte al valor de compra o d'amortització, tenint en compte, o no, els costos de reemplaçar-la o el valor del que s'ha deixat de produir com a conseqüència de la paralització.

L'estimació de les amenaces també ha de tenir una base objectiva. A més, s'ha d'explicitar un sistema per a traslladar les diverses mesures de probabilitat a una que hi sigui comparable.

Per exemple, el risc d'inundació es pot apreciar amb dades de pluja a la zona de l'Institut Nacional de Meteorologia expressades en litres per metre quadrat. La probabilitat d'un robatori es pot estimar emprant les estadístiques policials del districte, en nombre d'esdeveniments en un any.

Aquestes dues unitats de mesura no són comparables, i cal reconvertir-les en una mateixa escala que sí que ho sigui. Això permet saber quina de les dues eventualitats representa una amenaça més gran. Quan dany i amenaça són comparables, es poden prendre decisions informades sobre què val més la pena protegir o quina proporció del pressupost és aconsellable invertir. Les metodologies i fonts de dades són diverses. Poden ser sèries estadístiques. Hi poden haver dissenys experimentals naturals o de laboratori en els quals es compara una població sotmesa a certes eventualitats amb una altra de control. Es poden muntar panells Delphi d'experts. Es poden tenir en compte dades qualitatives sobre experiències passades de risc. També hi poden haver tècniques com la de la *tree analysis*, que estudia fallades en sistemes complexos.

Per a cada objecte que cal protegir s'ha de pensar en les repercussions que poden tenir tot tipus d'**amenaces** (inundacions, foc, robatoris, sabotatges, etc.). Per a això es parteix de l'axioma que les amenaces són constants i infinites, encara que la probabilitat i les formes de manifestar-se varien. S'ha de pensar en totes les que són possibles i atribuir a cadascuna una probabilitat en funció de la informació disponible (estadístiques, ocurrències prèvies, estudis). L'estimació del nivell d'amenaça que s'hi atribueix ha d'estar justificada per una metodologia que permeti assignar-hi un valor objectiu, i també fer comparables amenaces molt diferents. Havent vist el valor dels espais que cal protegir, i les amenaces probables, s'han d'analitzar els mitjans de protecció que hi ha actualment i identificar **vulnerabilitats**. Es tracta d'avaluar fins a quant podrien reduir el risc les mesures instal·lades. Per exemple, un detector de fum no evita l'incendi, però escurça el temps de reacció i, per tant, les destrosses causades.

Per això, a la fórmula del risc s'hi afegeix el factor protecció (p):

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

El tipus de danys que pot causar la materialització d'un tipus d'amenaça és molt variable. Cadascun d'aquests danys pot ser de més o menys abast.

> Per exemple, un esdeveniment de robatori pot provocar la desaparició d'un ordinador concret, però també hi poden haver danys materials (a la carcassa), una alteració de l'estat original (ha quedat tacat) una restricció temporal de la capacitat o qualitat del servei (s'ha de reparar), una pèrdua de confidencialitat (han accedit a les dades) i d'altres.

Tot aquest procés d'avaluació de riscos permet, al final, que el client tingui una visió global de tots els riscos de la seva activitat. Aquesta informació està ordenada de més a menys risc. És a dir, se saben des dels elements de més valor i més amenaçats fins als de menys valor i menys amenaçats ($R = D \times P) / p$. Això permetrà al client prendre decisions racionals, com invertir més diners del seu pressupost a protegir els riscos més grans. Quan se sap la distribució de riscos, el tercer i darrer pas de l'avaluador és decidir amb el client si el risc és assumible o no. Si es decideix que no, s'ha de concebre un pla de seguretat, que parteix d'uns objectius que cal aconseguir i de considerar totes les alternatives possibles d'actuació per a aconseguir-los. De cadascuna d'aquestes alternatives se n'han d'avaluar els avantatges i desavantatges. Lògicament, poden ser de diversos tipus. Finalment, s'ha de proposar al client l'opció o opcions que es considerin més bones. L'opció s'ha d'aplicar de manera detallada en el pla de seguretat.

Com es pot apreciar, en general, les anàlisis de riscos tenen una gran complexitat si es fan bé. També són cares fer, en particular si el sistema que cal protegir és gran i ric en processos. A la pràctica, les empreses de seguretat ho simplifiquen emprant un **qüestionari de vulnerabilitat** (*security survey*) o bé **matrius de vulnerabilitat**, en què es recullen, de manera esquemàtica i reglada, una sèrie d'informacions clau sobre els objectes (espais, béns) que cal protegir, les rutines de funcionament, les amenaces (tipus i probabilitat) i els controls i recursos que hi ha. Hi sol haver models predissenyats per a cada tipus d'activitat dels clients. Aquests instruments acostumen a estar centrats en els riscos objectius més que no pas en els subjectius. La informació s'acostuma a recollir per observació i es complementa, sovint, amb alguna entrevista.

El **quadre 2** mostra el tipus d'informació que se sol recollir en els models protocol·litzats d'avaluació de riscos en el cas de magatzems de mercaderies. Encara que no hi ha dos magatzems iguals, aquest tipus de documents serveixen de guia de referència, a la qual, després, es pot afegir algun element específic.

Quadre 2. Informacions freqüents en els formularis estandarditzats emprats en l'avaluació de riscos en magatzems

- Perímetre (tanques, accessos, il·luminació, vies subterrànies)
- Pàrquing (identificació, vehicles, horaris, vigilància)
- Entrades (identificació, control de visites i treballadors, camions, horaris)
- Control de claus (nombre de còpies, custòdia)
- Finestres (alçària, reixes, conductes de ventilació, claraboies)
- Mercaderies (perillositat, manipulació, emmagatzematge, inventari)
- Valors (caixes fortes, qui hi accedeix, quants diners hi ha)
- Ordinadors (tipus d'informació, nivell crític, accés, protecció)
- Alarmes (tipus, localització de detectors, circuit tancat de televisió, manteniment)
- Foc (sortides, extintors, ruixadors automàtics o *sprinklers*, inflamables, evacuació)
- Guardes (quants n'hi ha, horaris, rutes i patrulles, missió)

Font: elaboració pròpia

El model racional es fa servir de manera generalitzada. Malgrat això, té límits. En relació amb l'anàlisi de riscos, la racionalitat d'aquest model és limitada.

> Per exemple, no sempre es consideren totes les amenaces que hi ha; de vegades no es poden quantificar; de vegades la qualitat de les dades disponibles és dolenta; de vegades no hi ha prou temps per a fer una anàlisi conscienciosa o surt massa cara, de manera que es redueix tot a un mer sistema estàndard d'indicadors.

Un altre problema habitual és la propensió de considerar solament els riscos objectius, i de descurar els subjectius, o bé la tolerància a aquests riscos. D'altra banda, el model racionalista funciona més bé en sistemes amb riscos simples o on no hi ha gaire intervenció humana en el sistema. A més, des d'aquesta perspectiva, es tendeix a no tenir en compte els actors (les preferències de risc, motivacions, confiança, etc., de les persones afectades), i no se'ls sol permetre participar en la presa de decisions. En relació amb la planificació de la seguretat, el paradigma també presenta problemes. Planificar és condició necessària, però no suficient, per a l'èxit. L'ideal és prevenir, però la prevenció també té costos de tota mena que varien segons el mètode triat.

La segona perspectiva d'anàlisi és l'econòmica. Es pot dir que, en realitat, és una extensió de la perspectiva racionalista. L'economia estudia les formes en què s'assignen recursos escassos. Aquí, l'anàlisi parteix de la premissa que l'home és un ésser racional que vol maximitzar els beneficis –o les oportunitats– i minimitzar els riscos. Oportunitat i risc són els dos extrems d'un mateix eix. Qualsevol decisió comporta costos i beneficis que poden ser calculats. Estenent aquest argument, es poden calcular els costos que implica que es materialitzi un risc i també els costos que té crear una estructura de seguretat que miri de minimitzar o impedir que arribi a esdevenir-se. La seguretat i el risc s'han d'administrar amb criteris d'eficàcia i eficiència.

Un objectiu de l'anàlisi econòmica de riscos és saber i comparar els costos d'una eventualitat (un accident, un incident) i els beneficis derivats de prevenir-la. D'això se'n diu *anàlisi de cost-benefici*. Tots dos paràmetres s'expressen en termes monetaris. Es poden estudiar, per exemple, els costos que tenen els accidents de trànsit i l'estalvi que representa tenir un programa de vigilància policial a la carretera que n'eviti alguns –una vegada deduïts els costos d'aquest

programa. Així es poden comparar costos de diversos programes de prevenció i identificar el més eficient. Un altre tipus d'objectiu és comparar l'eficàcia de dos programes en relació amb el cost que tenen. L'anàlisi de cost-efectivitat expressa els costos en termes monetaris i els èxits en unitats diverses, com ara detinguts, accidents o anys de vida.

Les metodologies són una mica complexes. Quan es comptabilitzen costos s'ha de distingir entre aquells de què es fa càrrec la víctima directament, o terceres persones (la seva família, per exemple), o la societat (mitjançant l'Estat). Se'n diu *costos personals, externs i socials*. Els personals se centren en les víctimes (o en els transgressors, si escau). Els externs afecten terceres persones que paguen sense haver-ho decidit voluntàriament. Els socials comporten despeses que paguen tots els contribuents i que redueixen la qualitat de vida agregada de la societat. D'altra banda, hi ha diversos tipus de costos-beneficis: fixos o marginals, d'oportunitat, tangibles o intangibles, a curt o llarg termini, etc. El mètode de càlcul pot ser directe, si s'estima per fonts primàries, o indirecte, si es fa per fonts secundàries. De vegades cal determinar el valor d'intangibles com la salut, la seguretat, la tranquil·litat o la vida humana. En aquest cas es pot estimar per mitjà del que se sol pagar en indemnitzacions o bé del mètode anomenat *de disposició al pagament*. De vegades cal calcular el benefici que comporta un programa o acció determinat. La dificultat és saber quina part de la variació en la realitat és atribuïble al programa i quina a altres circumstàncies.

L'anàlisi econòmica no està exempta de dificultats. Hi ha, per exemple, controvèrsies per a decidir quines partides s'han de comptabilitzar en les estimacions de costos o de beneficis i com s'ha de fer. D'altra banda, hi ha determinats riscos dels quals no se sap prou bé l'extensió i abast. Uns exemples d'això són la delinqüència organitzada transnacional i els anomenats *delictes fiscals*. A més, els valors realment importants per a les persones són difícils de mesurar, encara que siguin tractats d'intangibles i s'hi atribueixi un valor arbitrari. L'anàlisi econòmica també se centra molt en el risc objectiu i passa per alt les qüestions del risc percebut i tolerable. Potser la crítica més de fons, però, és que l'eficiència, al voltant de la qual gira sobretot aquesta perspectiva, no és l'únic objectiu de les polítiques públiques, ni tampoc de les de seguretat.

1.2. Altres models d'anàlisi

Un tercer paradigma d'anàlisi és el **psicològic**. Aquest model parteix de la idea que les percepcions, actituds i coneixements que tenen les persones són clau a l'hora de definir, avaluar i prendre decisions de risc. Per tant, amb aquesta mena d'anàlisi, l'important és com es perceben els riscos (coneixement, percepció), les predisposicions o preferències davant el risc (actituds) i els factors que influeixen sobre aquestes percepcions i preferències. Aquestes qüestions tenen una aplicació pràctica en la gestió de la inseguretat, la comunicació de riscos, el disseny ambiental i altres camps. Hi ha una àmplia producció científica que analitza els factors que expliquen la percepció de risc, la sensació

d'inseguretat o la por. Se sap que la gent pren decisions d'assumir, o no, riscos i modela la conducta, l'opinió o, fins i tot, el vot portada, sobretot, per aquestes percepcions. Per això aquesta perspectiva té ressò en molts plantejaments de les polítiques públiques de seguretat. Tanmateix, l'ús que en fa la seguretat privada és limitat. Potser la raó més important que ho explica és la gran influència que té la perspectiva racionalista en un sector basat molt en la tecnologia i en la vigilància dissuasiva (Gabrosky, 1998).

La percepció d'inseguretat ciutadana o la por del delicte és dels temes més estudiats. Hi ha principalment **tres grans grups de factors** que expliquen aquesta por.

1) El primer grup és el grau de vulnerabilitat o protecció. Hi ha certs col·lectius (pobres, marginats, dones, gent gran, immigrants, turistes) que poden viure situacions de més desprotecció per diverses raons. Les conseqüències d'una victimització poden ser més impactants o doloroses perquè no tenen tants instruments per a respondre-hi o refer-se'n. La sensació de por augmenta si no hi ha confiança en la policia o en el sistema penal. Sovint es veuen a si mateixos com a col·lectius de risc, com a víctimes tipus.

2) El segon grup són factors que actuen de protectors davant la sensació d'inseguretat. Els qui tenen més capital social, una xarxa de suport sòlida, se solen sentir més segurs i protegits.

3) El tercer grup té a veure amb les condicions de l'entorn. La brutícia al carrer, les pintades, l'abandó dels espais, el trencament de mobiliari públic són interpretats per la població com a signes de descontrol. Aquests espais es viuen com a "amenaçadors". Es pot esdevenir el mateix si el desordre és social. Per exemple, la presència de colles juvenils, gent sense llar, esvalots o baralles s'associen amb degradació, desordre i imprevisibilitat (Wilson i Kelling, 1982).

En la mesura que se sap que hi ha factors que hi influeixen, una idea que se'n deriva és que la por es pot gestionar (Moore i Trojanowicz, 1988). Hi ha diverses estratègies. Una consisteix a cuidar la informació a una comunitat. És aconsellable donar informació objectiva, realista i útil sobre la inseguretat.

> Per exemple, donar dades sobre el perfil dels delinqüents, sobre el nivell de risc real de la zona, sobre el tipus de víctimes més freqüents, sobre la manera de millorar la seguretat pròpia.

El risc real i el percebut tendeixen a coincidir com més experiència o informació hi ha. Els riscos s'han de comunicar amb coherència, transparència, puntualitat i sinceritat. Una informació de qualitat i útil comporta una tasca policial prèvia d'investigació i intel·ligència basada a analitzar riscos, a entendre la lògica dels incidents o a dissenyar actuacions transversals. També es pot incidir

en la por mitjançant l'educació i la formació. És útil i efectiu ensenyar hàbits segurs. Es tracta que el ciutadà també assumeixi protagonisme o responsabilitat en la seguretat pròpia. Això li dóna més confiança.

Tant per a saber l'abast de la sensació d'inseguretat com per a gestionar-la, cal poder-la mesurar. Una via que es fa servir molt són les **enquestes de victimització** (Sabaté, Aragay i Torrelles, 1999; Thomé i Torrente, 2003). Una dificultat que té l'anàlisi de la percepció d'inseguretat és que un mateix risc pot desencadenar molts estats emocionals d'intensitat desigual, les fronteres dels quals, però, costen de precisar. Algunes d'aquestes fronteres són precaució, inseguretat, por, ansietat i pànic. La por es pot entendre com una reacció emocional defensiva, i no sempre proporcional, davant una amenaça reconeguda. És un mecanisme natural de protecció. El contrari és la ràbia. El qui respon a una enquesta, però, pot confondre por amb precaució, que és una resposta racional davant una amenaça (real o percebuda). Tampoc no és clara la frontera amb la idea d'*inseguretat*, entesa com un sentiment d'incertesa davant de situacions futures. La noció d'*ansietat* és el sentiment vague d'angoixa davant d'amenaces que no es poden definir clarament. Pot comportar quadres neuròtics. En l'extrem final de l'escala hi ha la sensació de pànic, és a dir, una reacció emocional molt intensa que, a més, comporta pensaments i actes irracionals i disfuncionals. Es manifesta al costat de símptomes físics.

La **por** no és un problema menor o una mera qüestió subjectiva. És clar que la por té **conseqüències** serioses que no són desitjables ni des d'un punt de vista personal ni col·lectiu. Se sap, per exemple, que els qui tenen por del delicte tendeixen a aïllar-se més. Redueixen les trobades, eviten llocs i situacions que perceben com de risc. En fer-ho augmenten la neurosi que tenen. Això també els porta a canviar hàbits quotidians de consum, oci, transport i d'altres. Tot plegat, acompanyat, de vegades, d'un augment en les mesures de protecció. En l'àmbit col·lectiu, els qui s'estan en veïnats on es viu amb por tendeixen a reduir les sortides, de manera que redueixen també el contacte entre la gent del barri i les activitats comunitàries. El barri comença a perdre cohesió social i llavors augmenten les actituds intolerants. Des d'un punt de vista de l'espai, com que aquestes persones se'n desvinculen afectivament i no se'n cuiden, el barri es deteriora físicament i en l'àmbit de neteja. Com que això fa que no convidi gaire a viure-hi, doncs, en aquestes àrees es redueix la presència de vianants i, fins i tot, es mira de no passar-hi. Queden buides i anònimes, de manera que atreuen conductes desordenades i fins i tot delictives. La falta de compromís i identificació amb l'espai, llavors, entra en una espiral ascendent.

Arribats a cert punt, es produeix una devaluació social i econòmica de determinats llocs. Els veïns ja no volen viure al barri i augmenten les migracions. Es desaccelera l'economia, tanquen alguns comerços i cau el preu dels habitatges. Des del punt de vista polític, la por fa que es deslegitimi la política i es desconfiï de les institucions. En les zones amb problemes d'inseguretat, augmenta el descontentament i el desinterès per la política. Això afavoreix els partits

i opcions polítics més demagògics i reaccionaris. D'altra banda, augmenta la pressió envers l'augment de la despesa pública en seguretat i envers l'adopció de polítiques més dures.

Un altre exemple de la contribució de la perspectiva psicològica són els estudis sobre les **actituds davant el risc**. Amb relativa independència del tipus de riscos de què es tracti, la gent té una inclinació a assumir-los o a evitar-los. De vegades se'n diu *preferències* o *gustos* davant el risc. La idea és que dues persones, amb la mateixa informació, prenen decisions diferents. Hi ha gent que té aversió al risc i posa l'èmfasi en la possibilitat que s'esdevingui una adversitat, mentre que n'hi ha d'altra que cerca –i hi pensa més– la possibilitat d'èxit. També hi ha actituds passives, de manera que la gent ni cerca ni evita el risc. Les motivacions per assumir-lo són diverses. Poden respondre a una decisió raonada o deliberada (càlcul, astúcia), a una predisposició (personalitat, actituds, creences, valors) o a pressions socials (influència del grup, valors socials, compromisos). La motivació és més gran si aquests tres factors van en la mateixa direcció. L'actitud o predisposició és més decisiva en la mesura que la informació sobre un risc és ambigua o incerta. Per regla general, la gent reacciona més davant les amenaces que davant les oportunitats. Per exemple, a la majoria de gent els preocupa més evitar pèrdues que tenir beneficis econòmics.

Com es pot comprovar, el model psicològic d'anàlisi de riscos és fructífer pel que fa a idees i té una llarga trajectòria empírica. Malgrat això, també té límits. Un d'aquests límits és que coneixements, percepcions o actituds no són trets solament individuals. Estan afectats per factors de grup, socials, culturals, o polítics. La persona i els seus atributs psicològics no es pot aïllar fàcilment del seu context vital. És més fàcil que les polítiques puguin incidir en els contextos que no pas directament en les persones agafades de manera individual.

El quart gran paradigma en l'anàlisi de riscos és l'**organitzatiu**. La premissa de partida és que la seguretat són productes i serveis que es venen i compren. Aquests productes i serveis els ideen i els duen a terme empreses o institucions. Aquestes empreses treballen en entorns que les condicionen. L'entorn d'una organització està format pels clients, els proveïdors, el marc legal, els accionistes, el mercat laboral i de matèries primeres, la tecnologia i altres forces externes. L'entorn pressiona i influeix en la presa de decisions, en les estratègies d'empresa, en les seves activitats i també en els seus productes i serveis. L'entorn afecta la capacitat d'una empresa de definir, organitzar, gestionar i avaluar els seus productes i serveis de seguretat.

> Per exemple, una empresa de vigilància que, en un context d'alta competència i escassetat de vigilants, vol reduir els costos de personal pot oferir serveis d'acudir i custòdia de claus que no requereixen tanta plantilla.

Aquesta perspectiva d'anàlisi planteja que es poden explicar els objectius, les estratègies o els productes i serveis d'una empresa (variable dependent) en funció de l'entorn (variable independent). Com més poder relatiu té algun d'aquests elements de l'entorn, més capacitat té d'influir en les decisions, es-

tratègies, polítiques o productes d'una firma determinada. La unitat 2 d'aquest mòdul, per exemple, mira d'explicar els serveis de seguretat en funció de la demanda dels clients i la tecnologia.

Un dels grans avantatges i aportacions d'aquesta perspectiva és que mostra que els productes i serveis de seguretat, fins i tot el concepte mateix, són el resultat de molts factors; no són una cosa estàtica o invariable. El disseny d'un producte o l'organització d'un servei tenen a veure amb les necessitats dels clients, l'estat actual de la tecnologia, el grau de competència en l'oferta, el nivell de risc del servei i altres variables, totes de l'entorn de les organitzacions. De factors n'hi ha molts. Encara hi ha altres raons. Cadascuna el porta a formular un tipus de demanda diferent i a valorar el servei rebut amb diferents criteris.

> Per exemple, un client pot tenir punts de vista diferents del que implica per a ell la seguretat. Les seves motivacions per contractar un servei també poden ser molt diverses. Pot voler contractar seguretat únicament per complir la normativa –sia per obligació o convenciment–, per prevenir danys materials o pèrdues econòmiques, per prevenir responsabilitats civils o penals, o per evitar danys o agressions personals. També ho pot fer per rebaixar la prima d'una assegurança o contractar-la, per abaratir els costos de producció, per augmentar la qualitat o valor afegit de productes o serveis, per aconseguir informació o coneixements valuosos, per transmetre o fomentar una imatge pública determinada, per atendre expectatives o demandes de clients o treballadors (o ciutadans), per contribuir a controlar o disminuir la delinqüència, o per obtenir un servei auxiliar a la seva activitat a baix cost.

La cinquena perspectiva és la **sociològica**. La sociologia estudia la lògica de les regularitats que s'observen en la vida social. Les premisses de l'anàlisi parteixen de la idea que els riscos tenen causes o conseqüències socials (Beck, 1995). A més, aquests riscos estan distribuïts socialment de manera desigual. D'altra banda, els riscos no són una qüestió del tot objectiva sinó que també estan construïts socialment, políticament i culturalment (Foucault, 1992; Douglas, 1996). Hi ha nombroses raons per a pensar que aquesta perspectiva sociològica és raonable. Per exemple, ni tan sols els riscos meteorològics o els geològics són completament "naturals". Les conseqüències nocives d'una inundació es produeixen sobretot perquè hi va haver la decisió humana de construir a la vora del riu. Pot ser que un terratrèmol de la mateixa escala gairebé no destrueixi res al Japó i sigui devastador a Haití. El que és definit com a segur o arriscat varia en l'espai i en el temps. La seguretat i el risc no són qüestions neutres i sempre estan envoltades de conflictes. La seguretat d'uns pot ser la inseguretat d'altres.

Els plantejaments sociològics lliguen la noció de *risc* amb processos socials i polítics. Sostenen, per exemple, que les cultures defineixen com a risc allò que amenaça l'ordre social (Douglas, 1996); o que el poder defineix riscos a fi de disciplinar, governar i perpetuar-se (Foucault, 1990). De la mateixa manera, els lliguen amb processos de desigualtat i consideren que la posició davant els riscos és un indicador important d'estratificació social. Els factors importants de vulnerabilitat tenen a veure amb la desigualtat socioeconòmica, la discriminació i l'exclusió social. Per això, és important analitzar quins grups estan subjectes a una exposició més gran a certs riscos, quins són més vulnerables a aquests riscos o quins no tenen el poder i la capacitat de decidir sobre aquests

riscos. Actualment, la visió sociològica del tema és dominada per la teoria de la societat del risc (Beck, 1992; Luckman, 1991), segons la qual, en un món global i molt interconnectat, les situacions de risc es propaguen ràpidament, de manera que aquests riscos cada vegada tendeixen a ser més seriosos pel que fa a les conseqüències, més universals pel que fa a l'extensió i més indiscriminats pel que fa a l'escala social.

Molt vinculada al paradigma sociològic hi ha l'**anàlisi política** de riscos. Sota aquesta perspectiva, el risc i la seguretat són qüestions molt vinculades a l'exercici del poder. S'entén per *poder* la capacitat d'influir sobre altres persones o grups, i també la d'assegurar-se per a un mateix recursos valuosos que també volen d'altres. La idea de *política* cal veure-la com el joc dirigit a guanyar quotes de poder i, així, estar en més bones condicions d'influenciar en prioritats, objectius o decisions públics. Les *polítiques* són el conjunt de decisions i actuacions impulsades des del govern amb la finalitat de respondre a un problema públic. La premissa de partida és que els problemes de seguretat són, primer de tot, construccions socials i polítiques. Hi ha diferents actors polítics (govern, partits, sindicats, grups d'interessos, mitjans, població, etc.) que influeixen, segons el seu grau de poder, en la definició, gestió i percepció social dels riscos. Els governs plantegen polítiques i plans de seguretat en funció dels interessos propis i d'altres actors amb capacitat d'influència. Les polítiques, però, solament són el reflex directe de la voluntat dels poderosos. També hi influeixen, entre altres factors, les ideologies polítiques, el coneixement científic, la situació econòmica, els models d'altres països que s'imiten, el marc legal i les estructures burocràtiques.

El model s'aplica perfectament a la seguretat, que cada vegada es converteix en un camp de confrontació política més central. Protegir el ciutadà és una missió central de l'estat i una font de la seva legitimitat, però aquest estat cada dia està en més males condicions de garantir-la (Mir, 1999). Les polítiques de seguretat pública es veuen en la necessitat de tenir nous aliats o cercar noves estratègies. La seguretat privada és un d'aquests possibles aliats. Una política de seguretat és el conjunt de principis, objectius i mesures orientats a protegir la població davant un risc o conjunt de riscos. La qualitat d'una política de seguretat depèn del fet que persegueixi l'interès general, sigui efectiva i eficient, i també tan universal, equitativa i socialment justa com sigui possible. A més, ha de ser democràtica i participativa, i els seus responsables n'han de retre comptes (*accountability*) als organismes representatius. Ningú no demana a un pla de seguretat privat que compleixi uns requisits semblants. Únicament se li demana que defensi bé els interessos del seu client i que, defensant-los, no contravingui les lleis vigents.

Des d'un punt de vista de l'anàlisi política, és important comprendre els mecanismes que té l'estat per a incidir en la realitat. Els governs fan polítiques de seguretat mitjançant una sèrie d'instruments. El primer són les sancions o multes. L'objectiu d'aquest instrument és evitar o corregir conductes amb l'amenaça d'una sanció. La regulació pot definir conductes desitjables o inde-

sitjables, estàndards que cal complir i un sistema de sancions. La mateixa Llei de seguretat privada n'és un exemple. Les multes tenen l'avantatge que disposen del suport d'una llei i hi ha institucions que les apliquen. Malgrat això, hi ha uns quants inconvenients. El primer és que, sovint, vigilar certs àmbits i obtenir certa informació és laboriós, i mantenir els controls surt car. Les regles solen ser complexes. També es critica la rigidesa dels estàndards i l'alt nivell d'intervencionisme.

Un altre instrument de les polítiques són els incentius econòmics. L'objectiu és estimular conductes de prevenció de riscos premiant-les econòmicament. Això es pot fer abaixant impostos (per exemple, no pagant tants impostos per la benzina sense plom) o a còpia de subvencions (per exemple, subvencionant la producció de biodièsel). L'avantatge d'aquestes pràctiques és que no interfereixen gaire en el mercat i que els costos de gestió són baixos. El desavantatge és que hi pot haver algú que s'estimi més pagar i continuar una mala pràctica. És allò de "jo contamino, jo pago". L'autoregulació és un instrument que té l'objectiu d'incentivar que els qui produeixen riscos s'autocontrolin. L'avantatge és que no és una mesura imposada. Els implicats mateixos són els que, des del coneixement i l'experiència que tenen en el sector, decideixen fins a on volen arribar. Per a l'Administració, el cost d'informació i seguiment és baix. El desavantatge és que les decisions no les pren un òrgan independent, sinó organitzacions que tenen uns interessos creats. Com que són entitats privades, la rendició de comptes es fa més limitada.

Una altra alternativa política és concedir franquícies, atorgar contractes o donar llicències. En aquest cas es vol que els creadors de riscos puguin operar sota certes condicions i per un període. L'avantatge és que aquest mecanisme permet tenir control sobre l'acompliment i, si escau, es pot decidir no renovar-los si hi ha cap incompliment. El desavantatge, una altra vegada, és que el control de les condicions de concessió pot ser dificultós i sortir car. A més, les condicions imposades poden treure flexibilitat al mercat. Un altre problema és que les empreses poden acabar repercutint l'augment dels costos en el consumidor. Una estratègia diferent és donar publicitat als riscos. L'objectiu, en aquest cas, és obligar els proveïdors de productes o serveis de risc a donar informació al consumidor sobre aquests productes o serveis (en l'etiquetatge, els prospectes, els catàlegs). L'avantatge és que el consumidor decideix si assumeix el risc o no, i a quin preu. Tot plegat comporta poc intervencionisme de l'Administració. La informació donada, però, pot tenir errors o ser inintel·ligible, manipuladora o incompleta. A més, el consumidor pot assumir riscos excessius perquè el preu és barat. Finalment, es pot recórrer a les assegurances. En aquest cas, les asseguradores (públiques o privades) imposen condicions variables en les pòlisses segons el tipus de mesures de control i prevenció que adopta l'assegurat. Mitjançant l'incentiu de rebaixar les primes es volen fer millorar les condicions de seguretat. Aquesta mesura comporta poc o gens d'intervencionisme de

l'Administració, ja que es tracta d'un pacte lliure entre les parts. El problema és que el fet mateix que hi hagi una assegurança pot fer baixar la vigilància preventiva a l'assegurat.

Cada model d'anàlisi de riscos s'emmarca en el context d'una disciplina i una tradició acadèmica. Cada disciplina científica es defineix perquè té unes categories i perspectives d'anàlisi més o menys pròpies amb les quals mira la realitat. Els problemes i la realitat, però, no pertanyen a cap disciplina, ni es reparteixen entre aquestes disciplines. A la pràctica, qualsevol fenomen es pot explicar des de diverses perspectives. Un exemple gràfic d'això és la gran varietat de factors que incideixen en cadascuna de les tres dimensions del risc (real, percebut i tolerable). Els paràgrafs següents fan un repàs d'aquesta qüestió. El **risc real** deriva d'una situació o decisió. És inevitable per complet (sempre hi ha algun risc) i se sap *a posteriori*. Els factors que causen situacions de risc són incomptables i varien segons l'àrea (riscos infecciosos, financers, laborals, etc.). En el cas de la delinqüència, la criminologia aporta una gran varietat de teories i variables explicatives que inclouen factors sociològics (privació relativa, anomia, tensió de valors, etiquetatge, subcultura), polítics (criminologia crítica), demogràfics (estructura d'edats de la població), psicològics (trastorns de personalitat, impulsivitat) o genètics (Downes i Rock, 1995).

El **risc percebut** és el que s'atribueix subjectivament a una situació o conducta. Generalment no coincideix amb el real per una sèrie de raons (es parla llavors d'infrarepresentació o sobrerepresentació). Entre aquestes raons hi ha la falta o distorsió d'informació, i també factors psicològics com el caràcter (introversió), la personalitat i d'altres que en condicionen la percepció. La por també sembla que respon a imatges primàries de les coses (Sjöberg, 2000). És més gran davant allò que és desconegut (Fischoff i altres, 1978). El condicionament, però, no solament és psicològic, sinó que també és social. Determinades variables com el gènere, l'edat, el sistema de valors, la ideologia política, el nivell de salut, l'existència de grups de suport, l'aïllament social i la solitud, la situació socioeconòmica, la incertesa econòmica, el nivell educatiu o les pautes de socialització influeixen en els nivells de por.

El **risc acceptable o tolerable** és el nivell que una persona, o un grup, considera acceptable o assumible. De fet, definim la seguretat com el nivell de risc que una persona (o comunitat) considera acceptable. Aquesta dimensió és diferent del risc real o del percebut. La tolerància està connectada directament a la presa de decisions. Si es considera que un risc és acceptable o tolerable, hi haurà una conducta. Si no, n'hi haurà una altra. Aquí intervenen diverses qüestions. La primera és que la decisió d'acceptar-lo o no és fruit d'un balanç de costos i beneficis esperats.

> Conduir un cotxe, per exemple, pot ser valorat com a perillós, però la percepció de risc es contrasta amb els beneficis que comporta fer-ho. Segons com es plantegi aquest balanç, es prendrà una decisió o una altra.

Per descomptat, cada persona fa el seu propi balanç. Hi ha una gran quantitat de variables que es prenen en compte. Per exemple, els riscos semblen més assumibles si es presenten com a justos o si sintonitzen amb certs valors (justícia, equitat, ètica, consens). Podem estar disposats a assumir els riscos que assumim voluntàriament, però, en general, costa més assumir riscos per coacció. Els perills naturals (inundacions, terratrèmols, llamps) sembla que es justifiquen més bé que no pas els que construeix l'home. Les situacions de risc més familiars (per exemple, els accidents domèstics) semblen més assumibles que no pas les estranyes. Una persona pot acceptar més riscos si manté un nivell d'adhesió o compromís amb certs grups o institucions. El balanç de costos i beneficis pot ser diferent pel que fa a una decisió en funció de si la informació disponible és completa, esbiaixada o comprensible. A la pràctica, les informacions rigoroses i objectives que té la gent són limitades, i aquesta gent pren decisions depenent de les seves percepcions. Finalment, però, el contingut d'aquestes informacions i les percepcions que té un subjecte estan influïts per variables socials i polítiques.

En relació amb la manera en què la gent avala els riscos i pren decisions, se sap que hi influeixen factors contextuals. Per exemple, com més gran és la "visibilitat" del risc i més cert, immediat o irreversible es veu el dany, o més incert el resultat final, més gran es percep aquest risc. Se sap també que els factors culturals (valors, expectatives i preferències) modelen la percepció, definició i acceptabilitat dels riscos. Se sap que els factors psicològics (cognitius, afectivomotivacionals o de personalitat) tenen un rol més important en l'avaluació de riscos en la mesura que hi ha més incertesa. Com més incertesa hi ha, més importants són. En la valoració de riscos també funcionen certs biaixos heurístics (principis per a reduir la complexitat real). Així, es destaquen certes propietats de la realitat i se n'ignoren d'altres. Se sap també que l'efecte de les dinàmiques dels grups i organitzacions afecten de manera important les percepcions i decisions de risc. Un grup pot extremar tant l'acceptació com l'evitació individual de riscos.

La **confiança** és un factor fonamental tant per a avaluar riscos com per a acceptar-los. Té una importància creixent en una societat postmoderna i global en què la incertesa és gran i les anàlisis racionals de riscos són fràgils (Sjöberg, 1987). A més, la confiança és una condició clau per a les relacions econòmiques i per a les humanes en general. En seguretat, crear confiança és clau. Aquesta confiança, però, és fràgil, de manera que és més fàcil de destruir que de construir. La gent que se sent manipulada pel que fa a la confiança triga a recuperar-la. Una de les raons d'això és perquè la desconfiança es reforça a si mateixa una vegada desencadenada. A més, es produeix asimetria en la seva percepció. Això vol dir que, per exemple, els esdeveniments negatius (errors, mentides, accidents) hi impacten més que no pas els positius. De la mateixa manera, les notícies negatives tendeixen a tenir-hi més efecte que no pas les positives.

1.3. Planificació i gestió

Aquest apartat explica com es planifica i gestiona la seguretat seguint un esquema racionalista. Des d'aquesta perspectiva, cal entendre la **gestió de la seguretat** com un procés continuat i proactiu per a establir i mantenir uns nivells de risc acceptables o dins el que s'ha convingut amb el client. El procés és retroalimentat i inclou tot el cicle, que comença amb l'anàlisi (o auditoria) de riscos i l'elaboració del pla de seguretat, continua amb l'aplicació i control de funcionament del pla de seguretat i l'avaluació de la consecució dels objectius d'aquest pla i la presa de mesures correctives, i s'acaba amb la reanàlisi de riscos i reelaboració del pla de seguretat també.

Un gestor de riscos ha de ser capaç de prendre decisions en qualsevol d'aquestes fases. Cal fer-ho, ja que les condicions de l'entorn canvien constantment i això acaba afectant la seguretat.

> Per exemple, una empresa pot començar una nova línia de productes que implica emmagatzemar matèries primeres inflamables que no es tenien quan es va dissenyar el pla original de seguretat.

Davant un risc qualsevol, hi ha diverses possibilitats bàsiques d'actuació. La consideració d'aquestes alternatives és una qüestió prèvia al procés mateix de planificació. Una opció és assumir-lo i acceptar-ne les conseqüències potencials. Una altra possibilitat és evitar-lo; és a dir, sabent que hi és, apartar-se'n o no prendre decisions arriscades. També es pot intentar controlar-lo, cosa que implica identificar-lo i vigilar els elements vulnerables. Reduir-lo és una alternativa que fa que calgui posar contramesures que redueixin el dany potencial o la probabilitat d'ocurrència. Es pot optar per dispersar-lo repartint els punts vulnerables. També es poden transferir els riscos de manera que passin a d'altres o bé es comparteixin. Finalment, es poden compensar contractant una assegurança o amb altres fórmules. Quan s'ha decidit donar una resposta proactiva al risc és quan comença realment el procés de planificació o gestió.

Per a planificar, es parteix de l'anàlisi de riscos o bé de recerques que aporten informació sobre les característiques dels factors que incideixen en el problema que cal tractar. Els estudis que inclouen factors explicatius són els idonis perquè faciliten la presa de decisions posterior. No sempre es pot partir d'un bon estudi previ. Sense les dades adequades, però, no es poden prendre decisions informades. En el pitjor dels casos es pot recórrer a estudis sobre problemes semblants o en contextos semblants. A més, s'ha de fer una tasca de documentació per a obtenir la màxima informació possible sobre el fenomen local (fonts secundàries, estadístiques, entrevistes, etc.). Es tracta d'obtenir tot el coneixement que es pugui sobre el risc.

El pas següent és plantejar-se diverses **estratègies de seguretat** i triar-ne una. N'hi ha unes quantes. Una de possible és prevenir evitant o pal·liant danys o pèrdues. Això es pot fer de maneres diverses, tal com veurem tot seguit. Per a prevenir cal entendre aquesta lògica dels fenòmens. També es pot reparar o

compensar amb assegurances o altres mecanismes. Una estratègia diferent és actuar sobre possibles transgressors a partir de saber els perfils de risc habituals. Una altra opció és castigar els delinqüents amb la via penal (Foucault, 1990). També es pot provar de reintegrar aquests delinqüents a la societat amb programes de reinserció. En comptes d'actuar sobre els transgressors, es pot actuar sobre les víctimes. Per exemple, educant-les en una cultura de l'autoprotecció. Es pot estudiar el perfil d'aquestes víctimes amb la idea d'identificar-les i actuar-hi. Es pot millorar la seguretat col·lectiva amb programes de prevenció comunitària o amb polítiques socials. Una altra possibilitat és actuar solament en l'àmbit de la seguretat percebuda gestionant la millora de la sensació de seguretat. També es pot millorar la seguretat millorant la tolerància davant els riscos. Totes aquestes estratègies són d'acció. El sector privat tendeix a fer servir més les preventives, i el públic, les reactives.

Potser les estratègies que desperten més atenció són la de **prevenció** (Hughes, 1998). La gestió de la seguretat implica, sovint, fer prevenció. Per *prevenció* s'hi entén qualsevol acció proactiva (no reactiva) adreçada a evitar que es produeixi cap tipus de dany o pèrdua, o bé a pal·liar-ne la gravetat. Prevenir és fonamental, ja que, en seguretat, prevenció és, gairebé sempre, sinònim d'eficàcia i eficiència. La prevenció implica planificació. Diverses de les estratègies esmentades en el paràgraf anterior es consideren de prevenció. Els manuals les solen classificar segons diferents criteris. Un d'aquests criteris és el mecanisme que actua. D'aquesta manera, hi ha una prevenció de base social (polítiques educatives o d'igualtat d'oportunitats, subsidis d'atur, etc.). El pressupòsit és que, com més igualtat social, menys delicte. Una altra estratègia és la comunitària. Aquí el mecanisme que actua és enfortir els llaços de cohesió social i solidaritat a escala local i de barri. Hi ha una prevenció basada a incidir en els transgressors que ja ho són. En alguns casos vol evitar la reincidència, reinserir la persona a la societat o bé mantenir certa vigilància dissuasiva. La prevenció centrada en transgressors potencials es basa a identificar poblacions de risc i incidir-hi per la via educativa, per la d'ajudes específiques o per altres maneres. També es pot basar en les víctimes potencials i actuar sobre aquestes víctimes, per exemple, mitjançant l'educació per a la prevenció de riscos. La prevenció situacional es basa a incidir sobre la vigilància i els objectius de la transgressió o el delicte.

La prevenció és una estratègia per a combatre la inseguretat objectiva, però també es pot prevenir la inseguretat percebuda. De fet, hi ha actuacions en el primer terreny que també tenen efecte en el segon. Així, la prevenció de base social millora la vida del barri, i augmentar la confiança i cohesió veïnal. Aquesta cohesió reforça tant la seguretat real com la percebuda. La situacional –basada en l'urbanisme, en el disseny d'objectes o en les tecnologies de seguretat– sol sortir més barata que la social, i la relació cost-eficàcia és bona. Si aquestes accions milloren la sensació d'ordre, la por descendeix una mica. Una altra estratègia per a combatre la inseguretat és la mera vigilància. La visibilitat de la policia, o fins i tot de la seguretat privada, és un factor tranquil·litzador. Un element que rep una atenció creixent són les condicions de l'entorn, tant

socials com físiques. La sensació de seguretat millora quan ho fa el civisme, la convivència i l'ordre social. El desordre crida més desordre, i més desordre crida el petit delicte (Wilson i Kelling, 1982). No permetre la conducta desordenada de certs col·lectius millora la seguretat real i percebuda. L'ordre físic i la neteja tenen una gran importància per a crear entorns segurs que es percebin a més com a tals. Per mitjà de l'arquitectura i l'urbanisme es poden crear espais més segurs.

Per exemple, augmentant els espais urbans de trobada, afavorint la vigilància mútua, eliminant barreres o reduint la dimensió dels blocs de pisos.

La por millora substancialment si a la comunitat hi ha solidaritat i llaços comunitaris. Poden ser xarxes de mútua vigilància, suport o ajuda. També són efectius els programes de reparació, mediació, arbitratge. Finalment, la justícia social té un paper en la seguretat fent més equitatiu el repartiment de beneficis i riscos de tota mena.

La planificació i gestió de la seguretat implica tenir informació sobre els riscos. En el cas concret de les dades sobre delinqüència, hi ha tres **proveïdors bàsics d'informació**: controladors (policia, jutjats, presó, inspeccions, tècnics), víctimes i transgressors. Les **estadístiques policials** són l'instrument més comú en el primer cas. El problema és que solament recullen els delictes que es denuncien, i que la probabilitat que ho siguin varia segons el tipus de què es tracti. Les **enquestes de victimització** són la tècnica de recol·lecció de dades més emprada en el segon cas. Consisteixen a demanar a una mostra representativa de la població els delictes que patit durant un període de referència, i també altres qüestions que hi estan relacionades. Tenen l'avantatge que els resultats es poden extrapolar a la població. A més, permeten conèixer una gran quantitat d'informació de la víctima i de les seves actituds i opinions. Malgrat això, solament permeten saber les dades del delinqüent o determinats detalls del delicte si el delinqüent els sap. Les enquestes no són capaces de recollir tots els delictes, ja que depenen del fet que aquests delictes tinguin una víctima individual, que pugui respondre, que sigui conscient de ser-ho i que sàpiga els detalls del delicte. Això no s'esdevé en els delictes de víctima col·lectiva, o en la majoria dels delictes fiscals, o en la delinqüència organitzada.

Els anomenats *autoinformes* o *enquestes d'autoinculpació* segueixen el mateix mètode que els de victimització, però en aquest cas demanen les conductes delictives que ha comès l'enquestat durant un període de referència, i també altres qüestions que hi estan relacionades. Aquesta tècnica permet recollir potencialment més quantitat i varietat de dades que cap altra. Permet estudiar la prevalença i incidència. A més, es redueixen biaixos de gènere, edat o classe presents en altres fonts, com les estadístiques policials. És capaç de proporcionar una gran quantitat de dades sobre el perfil del delinqüent, els seus valors, les actituds, l'entorn vital, les tècniques, la presa de decisions, la neutralització de la reacció social, els hàbits, les xarxes socials, els contactes amb agències de control o altres conductes de risc (consum de drogues, per exemple). El

problema és que solen tenir quotes altes de no-resposta. La taxa de resposta varia segons la mostra (adults, delinqüents, minories). Així i tot, funcionen prou bé amb poblacions joves. Per això es fan servir sobretot en estudis de delinqüència juvenil.

La **planificació de la seguretat** és un procés pel qual, després d'analitzar els riscos, es fixen uns objectius de seguretat i es tria una estratègia que es desplega mitjançant tot un seguit d'actuacions. A més, es preveuen els recursos necessaris, s'estableix una organització de les tasques amb els procediments i controls que fan falta i es fixen les responsabilitats corresponents. S'hi sol incloure, a més, un protocol de seguretat que defineix les regles i procediments que serveixen per a coordinar les respostes per a diversos tipus d'eventualitats, o aspectes concrets com les comunicacions, per exemple. Es planifiquen totes les necessitats de formació o reciclatge del personal. Es preveuen futures avaluacions i criteris per a modificar o corregir el pla mateix. En definitiva, es tracta de crear un sistema ordenat que garanteixi que s'aconseguiran els objectius proposats. En el sector de la seguretat privada, les avaluacions de riscos i els plans de seguretat els poden fer les empreses consultores o bé les proveïdores de serveis.

El **pla de seguretat** és el document en què es recullen de manera ordenada totes aquestes informacions (vegeu el quadre 3). El pla serveix per a un doble propòsit: ajuda a vendre el servei i, quan ha estat comprat, és una guia de la feina que cal fer. En aquest sentit, equival al pla i a la memòria d'un arquitecte, o al projecte de recerca d'un científic, per posar dos exemples.

Quadre 3. Estructura i contingut d'un pla de seguretat tipus

Portada (nom del pla, autors, client i data)
Índex
Resum (o resum executiu)
Presentació (propòsit de l'informe, abast, rellevància, antecedents)
Anàlisi o auditoria de riscos (s'hi sol incloure; es treu de l'avaluació de riscos)
- Metodologia (tipus de dades emprades, recol·lecció i anàlisi)
- Objectes que cal protegir (cost, sensibilitat i posició crítica)
- Amenaces (tipus i probabilitat d'ocurrència)
- Vulnerabilitat (mesures existents, àrees vulnerables)
- Impacte (valorat en termes econòmics o d'altres)

Objectius i prioritats (prioritzats i justificats)
Estratègia de seguretat
- Justificació de l'estratègia (per exemple, anàlisi de cost-benefici)
- Línies estratègiques i actuacions que hi estan vinculades

Actuacions
- Accions, procediments, protocols (rutinaris i d'emergència)
- Contramesures (necessàries i opcionals)
- Controls (equip, personal, procediments)

Organització i gestió
- Recursos propis i aliens (humans i materials)
- Organització i atribució de comeses
- Responsabilitat i jerarquies
- Selecció i formació de personal
- Comunicació de riscos (població, altres agències)

Avaluació
- Criteris d'avaluació
- Pla d'auditories de seguretat (periodicitat, responsabilitat)

Pressupost
Bibliografia
Apèndixs (el contingut varia)
- Legislació aplicable
- Protocols o procediments d'actuació (activació, avís, evacuació, etc.)
- Convenis i contractes
- Documents de suport (telèfons del personal o d'institucions, mapes, recursos)

Font: elaboració pròpia

En relació amb el primer propòsit, el pla, que inclou l'anàlisi de riscos, serveix perquè el client tingui presents les seves vulnerabilitats, i l'impacte econòmic que poden tenir per a ell les possibles incidències. Amb això es fan visibles les seves necessitats de seguretat. Gràcies al pla, el client també pot estudiar la proposta de seguretat que li fan i el cost que té. És a dir, podrà apreciar la qualitat de la proposta i el que inclou. A l'hora de prendre decisions, inevitablement comparará els costos que poden tenir els potencials incidents amb els costos del servei de seguretat. Per això és important que tota la informació que apareix sigui clara i quantificable perquè l'ajudi a decidir. El pla també ajuda a fer que el procés de negociació entre proveïdor i client sigui més ordenat i concret. Durant l'execució, també serveix per a protegir el proveïdor de seguretat de possibles exigències del client que no s'havien inclòs ni pressupostat en el pla. A la pràctica, els plans que es cobren al client solen ser més detallats, mentre que els que no es cobren i serveixen sobretot d'argument de venda no ho solen ser tant.

El procés de redacció d'un pla de seguretat parteix de l'anàlisi de riscos. El pas següent és identificar objectius i decidir estratègies, activitats, organització i altres elements esmentats. En el pla hi apareixen tots. Si aquest pla implica la col·laboració d'altres organitzacions externes (sien públiques o privades), cal entaular-hi negociacions i signar convenis de col·laboració o contractes que detallin el contingut, les condicions i els costos de l'assistència. Les negociacions han de tenir lloc abans de donar per definitiu el pla. Finalment, tenim l'aprovació formal del pla i la distribució als responsables i actors implicats. De vegades, el personal encarregat de dur-lo a terme no està prou preparat, i cal establir un programa de formació i aprenentatge (*training*) abans d'engegar-lo.

Hi ha unes preguntes fonamentals que s'ha de fer el qui dissenyi un pla de seguretat. La primera és per què s'ha de controlar; és a dir, quins són els objectius de seguretat que es volen aconseguir. Això implica plantejar els estàndards que són desitjables o acceptables. La segona qüestió és què s'ha de protegir o a qui. D'això se n'ha dit *objecte que cal protegir*. Després hi ha les qüestions de com s'ha de controlar (l'estratègia), amb què (mitjans) i quan (seqüenciació).

La planificació s'ha de fer d'acord amb uns **principis** que es consideren més o menys universals i que, segons com, mostren la bondat d'aquesta planificació. Un d'aquests principis és el d'eficàcia; és a dir, màxima consecució dels objectius de seguretat. Eficiència, o màxima protecció al cost més baix que sigui possible. Respecte pels drets i llibertats de la gent. Participació de tota la gent que n'està concernida. Igualtat o equitat en la protecció. En el cas de les empreses, s'hi afegeixen altres qüestions com la mínima interferència en els processos o en la vida quotidiana de l'organització. Integració o coordinació entre els objectius, estratègies i controls de diferents àrees de seguretat (per exemple, laboral i mediambiental). Finalment, hi ha la simplificació en els controls i contramesures que s'instal·lin. Hi ha més principis, però aquests són els més comuns.

A part dels principis generals orientadors esmentats, hi ha **axiomes pràctics** que s'accepten de manera general. El primer és que, en el procés de planificació, cal preveure totes les amenaces, encara que després la probabilitat que es materialitzin sigui baixa. Els sistemes més crítics s'han de protegir primer, més i més bé. Cada contramesura concreta que s'instal·la té nivells d'eficàcia i costos diferents.

El planificador ha de saber les possibilitats i límits que té cada tecnologia en relació amb un problema concret. Alguns controls (o contramesures) no alteren la probabilitat que s'esdevingui un incident, sinó que solament redueixen la vulnerabilitat i l'impacte potencial. Per exemple, un sistema d'extinció automàtica de foc no evitarà l'incendi, però si funciona bé reduirà els danys causats perquè l'extingirà en poca estona.

Hi ha mesures que poden alterar la probabilitat perquè tenen un efecte dissuasiu. Per exemple, una càmera de seguretat. En qualsevol cas, l'axioma és que no la invulnerabilitat absoluta no existeix. Els controls tenen nivells de vulnerabilitat en si mateixos. Sempre hi ha un risc residual, que ha de ser acceptable.

En funció de l'àrea, hi ha diverses modalitats de plans de seguretat especialitzats. Hi ha plans d'emergències, de seguretat local, de protecció civil i de seguretat laboral, entre molts altres. També hi ha subplans dins un pla general complex. Per exemple, hi pot haver un pla de comunicació de riscos o d'evacuació en el marc d'un altre de més gran. L'estructura bàsica de qualsevol pla és la mateixa, encara que hi poden haver matisos.

> Per exemple, els continguts dels plans de protecció civil solen incloure un inventari de riscos, un catàleg de recursos mobilitzables, una estructura operativa i de comandament, els criteris de mobilització i coordinació de recursos i les directrius de funcionament.

Hi ha dos tipus de plans de protecció civil: els territorials (per zones geogràfiques) i els especials (per sectors d'activitat o riscos específics).

Normalment, tot el procés de planificació de la seguretat és a càrrec d'un especialista. Si el sistema que cal protegir és complex, hi pot participar un grup petit d'especialistes al costat d'alguns responsables de diferents departaments d'una empresa, per exemple. Malgrat això, elaborar un pla de protecció civil o un pla de seguretat local o autonòmic és una tasca complexa que abasta molts objectes que cal protegir i molts riscos que cal considerar.

En aquests casos, el procés comença amb l'organització d'un equip encarregat de la planificació. Val més formar un equip transversal, ja que es guanya en coresponsabilitat, amplitud de mires i implicació política. La mida depèn, en part, dels recursos disponibles i de la complexitat de la feina que s'ha de fer.

> Per exemple, per a un pla de protecció civil, l'equip pot procedir d'àrees tan diverses com la resposta a l'emergència (operativa, sanitat, medi ambient), comunicacions (relacions públiques, premsa), comunitat (relacions amb altres agències), recursos humans (funcionaris, voluntaris, sindicats) o serveis de suport (jurídics, compres, manteniment, informàtica).

En l'equip de planificació cal establir unes línies d'autoritat. S'ha de trobar un equilibri entre jerarquia (emergències) i participació (ordenació o *planning*). Una vegada establert aquest equilibri, s'han de fixar les missions, determinar els objectius i repartir les responsabilitats. Establir un calendari de treball en què es fixin dates límit. Per a dur a terme les tasques, abans cal tenir un pressupost detallat per partides. Fer una anàlisi de riscos a gran escala (local o regional) és molt complex. Cal considerar factors històrics, geogràfics, tecnològics, i assentaments i activitats humanes. Per exemple, per a dissenyar un pla de protecció civil s'ha de començar per l'estudi de les vulnerabilitats. L'esquema general és el mateix. S'ha de fer un inventari exhaustiu de punts especialment sensibles que cal protegir i de les activitats de risc a l'àrea. S'ha d'estimar la probabilitat d'ocurrència d'eventualitats meteorològiques, riscos industrials, accidents en transport de mercaderies perilloses, etc. Aquestes apreciacions es

basen en estadístiques, estudis, enquestes i altres fonts. S'han d'avalar possibles impactes humans, materials o econòmics. S'ha de fer un inventari de tots els mitjans públics i privats disponibles. S'ha de calcular el factor de protecció assignant un valor a la disponibilitat i adequació dels recursos a cada risc particular. Una vegada identificats els punts vulnerables, s'ha de redactar el pla.

Els plans de protecció civil (i tots els altres) es poden dissenyar *ex novo* o poden ser revisions dels que ja hi ha. De fet, gairebé sempre hi solen haver estructures mínimes de protecció, encara que no estiguin coordinades en un pla. Per això cal analitzar la situació actual. Això implica fer una avaluació que inclou revisar els plans i polítiques de protecció que ja hi ha i identificar la legislació que els afecta. Distingir els recursos interns i externs (personal, equip, serveis, organitzacions, transports i comunicacions) que hi ha compromesos en el pla actual. També cal identificar les activitats, els serveis o les operacions crítiques que duen a terme (comunicacions, subministraments, empreses vitals, etc.) i revisar la cobertura de les assegurances. Tot això comporta recaptar una gran quantitat d'informació i fer moltes reunions amb responsables dels bombers, seguretat pública i privada, Creu Roja, meteorologia, sanitat, subministraments, etc.

Un aspecte especial de la gestió del risc és la gestió de situacions d'emergència o crisi. Aquest concepte designa el procés per a prevenir aquestes situacions, respondre-hi i refer-se'n. Tècnicament parlant, es fan les mateixes tasques que en qualsevol tipus de gestió (planificació, formació, direcció, comunicació, coordinació o avaluació). Malgrat això, el context d'emergència o crisi requereix que la gestió dels recursos humans i materials, l'anàlisi d'informació i la presa de decisions sigui més ràpida i crítica. Hi ha determinades àrees de la gestió, com la direcció i control, la logística, les comunicacions, el salvament, les relacions amb la comunitat, la protecció de propietats, la gestió política i mediàtica de la crisi, o la recuperació de la crisi i la restauració de la normalitat, que cobren una importància clau.

L'organització de resposta a situacions d'emergència o crisi la dirigeix l'Autoritat de Protecció Civil (més en l'àmbit institucional i polític), i té, a més, un cap operatiu i un equip de gestió de l'emergència. En contextos d'emergència o crisi, és important tenir un comandament únic i executiu que prengui decisions ràpides. No obstant això, l'envergadura d'algun d'aquests contextos i la diversitat de temes afectats (sanitaris, arquitectònics, mediambientals, etc.) demana també certa multidisciplinarietat, participació i coordinació. Per això cobra tanta importància l'equip de gestió d'emergències. Aquest equip dóna suport a la direcció operativa ocupant-se dels molts aspectes col·laterals a l'incident, com ara la comunicació amb la premsa, l'assegurament dels recursos materials necessaris, la relació amb col·laboradors, hospitals, etc., o l'assegurament que les comunicacions funcionen.

La direcció operativa s'encarrega del comandament de les persones i dels mitjans emprats en l'incident. Dóna ordres, avalua la situació, fixa estratègies, aplica el pla, activa recursos, requereix la col·laboració externa, ordena evacuacions, supervisa la resposta i dóna per acabada l'emergència. Depèn directament de l'Autoritat de Protecció Civil. Entre les funcions crítiques que fan hi ha la de mobilitzar i coordinar el personal d'emergències, informar i aconsellar la població afectada sobre el risc i donar explicacions a l'opinió pública (mitjans de comunicació). En relació amb el primer aspecte, en situacions de crisi les comunicacions són vitals, ja que cal coordinar un gran nombre de persones. El pla d'emergències ha de preveure alternatives en cas d'una fallada, ha de preveure totes les línies possibles de comunicació i separar els canals de comunicació operativa i els de suport. En relació amb el darrer aspecte, és molt important la claredat, coherència i consistència dels missatges. Per això s'aconsella designar un únic portaveu i canal oficial. La informació ha de ser completa, exacta i aprovada. S'ha de donar el mateix accés a la informació a tots els mitjans de comunicació, i s'han d'evitar les especulacions i els portaveus no autoritzats.

1.4. Avaluació de la seguretat

Avaluar és emetre un judici de valor sobre la necessitat, disseny, implementació, eficàcia, impacte o eficiència d'un programa o actuació basant-se en l'anàlisi d'informació empírica recollida de manera sistemàtica.

L'avaluació s'ha d'entendre com un procés continuat que facilita millorar constantment. Els resultats de l'avaluació serveixen, si escau, per a modificar i enriquir el pla que s'avalua. Hi ha diversos tipus d'avaluació. El més conegut és la que se centra a mesurar fins a quin punt s'han complert els objectius d'un pla o programa. Malgrat això, la mera resposta a aquesta qüestió no proporciona informació útil sobre si el programa estava ben dissenyat, sobre quines fases o activitats no van sortir bé i, sobretot, per què han fallat.

Per tot plegat, les preguntes d'avaluació s'han anat ampliant. Es poden plantejar qüestions com les següents:

- Fa falta una actuació?
- Està ben definit el programa?
- És avaluable?
- S'ha aplicat adequadament?
- Quins efectes ha tingut?
- Ha estat eficient?

Normalment es distingeix entre avaluacions prèvies al programa, avaluacions que es fan durant l'aplicació del programa i avaluacions sobre els resultats del programa. D'altra banda, hi ha la qüestió de qui participa en l'avaluació. Tradicionalment, tant l'elaboració com l'avaluació de programes es plantegen des del poder i es conceben com un procés vertical. Malgrat això, en l'execució dels programes hi participen molts actors i les conseqüències d'aquesta execució n'afecten molts altres. L'èxit d'un programa depèn del fet que tothom s'hi senti implicat. Això és més fàcil d'aconseguir si la gent ha participat en la definició i elaboració.

Per tant, hi ha diversos tipus d'avaluacions i tots són aplicables a la seguretat.

L'**avaluació de necessitats** és prèvia al programa. Consisteix a saber quines són les característiques del problema que es vol solucionar i l'abast que té. Es tracta d'avaluar les necessitats que hi ha, i veient la distància que existeix entre el que hi ha i el que hauria de ser d'acord amb el que s'esdevé en altres llocs, allò que diu la llei, els experts aconsellen o, senzillament, les persones o clients demanen. Una modalitat d'aquesta avaluació és la de riscos.

L'**avaluació del disseny de programa** es fa sobre el paper i consisteix a veure la consistència lògica que té en relació amb el problema que es vol solucionar. Entre moltes altres qüestions, s'analitza si els objectius i les accions previstes són coherents i segueixen una seqüència lògica, si el model d'intervenció està contrastat o si el pressupost és suficient.

L'**avaluació de l'avaluabilitat** consisteix a veure si el programa, tal com està dissenyat, es podrà avaluar. L'avaluació de l'aplicació es fa quan el programa ja funciona. Consisteix a detectar discrepàncies o desviacions entre el que s'ha previst i la realitat. Per exemple, actuacions que no es duen a terme o resistències dels professionals o dels destinataris.

L'**avaluació de la cobertura** consisteix a veure si el programa arriba a tota la població objecte i si hi ha barreres d'accés al programa. El monitoratge o seguiment de programes comporta una avaluació continuada dels programes el desenvolupament dels quals es perllonga. Es basa a dissenyar uns indicadors de funcionament i recollir periòdicament informació partint d'aquests indicadors.

L'**avaluació de resultats** consisteix a mesurar fins a quin punt s'han complert els objectius en la població diana. També s'analitza si hi ha efectes no volguts.

L'**avaluació de l'impacte** és el mateix, però sobre la resta de la població no objecte del programa.

Hi ha una avaluació econòmica que analitza el cost-benefici del programa, o el cost-eficàcia, entre altres paràmetres.

Si avaluar consisteix a jutjar el valor d'una cosa, aquest judici s'ha de fer partint d'uns criteris, o preguntes d'avaluació, que han de ser justificables i s'han de concretar en una sèrie d'indicadors amb els quals es puguin mesurar. Així, els criteris per a avaluar l'eficàcia s'han de justificar partint dels objectius concrets de seguretat que es volen aconseguir. Si es vol veure, per exemple, fins a quin punt en una botiga de roba de marca ha millorat la seguretat després d'instal·lar un sistema de seguretat per a prevenir robatoris, cal explicitar quins indicadors es fan servir. El lloc per a fer-ho és el pla de seguretat. Aquests indicadors poden ser diversos: el nombre robatoris de gènere, la quantia del que s'ha robat, els robatoris que s'han evitat perquè ha sonat el detector de pinces d'alarma, el volum de vendes, la sensació de seguretat dels clients i dels treballadors, etc. A més, essent rigorosos, s'ha de poder atribuir una eventual millora a l'efecte del sistema i no pas al d'altres factors.

De vegades es parla d'**avaluació de la qualitat**. El concepte de *qualitat*, però, pot significar moltes coses i tenir molts indicadors. El sector privat sol fer servir una varietat de **criteris** per a aproximar-se al concepte de *qualitat de la seguretat*. Un primer criteri són els **danys o pèrdues humanes o materials evitats**. Seria un criteri adequat per a mesurar l'eficàcia, però la mesura és complexa perquè implica calcular el que s'ha previngut. L'ideal és fer-ho per mitjà d'un mètode experimental amb un grup de control (sense seguretat) i un altre d'experimental (amb seguretat). Això, però, no és possible sempre. Com a alternativa es pot comparar amb anys anteriors o altres llocs controlant l'efecte de terceres variables.

Un altre criteri freqüent és l'**absència d'errors i incidències en els serveis o els equips**. Aquí es canvien els indicadors de resultats pels de funcionament. El pressupòsit és que els sistemes compliran la funció si funcionen bé. Com a mesura d'eficàcia és inadequada. Un altre criteri que es fa servir és la **capacitat de resposta tècnica a les demandes** o necessitats. Aquí s'introdueix el criteri de capacitat de servei. Una altra aproximació és la satisfacció subjectiva del client (o del ciutadà, en el cas de la seguretat pública). Es vol que sigui un indicador de qualitat del servei, però és indirecte. També s'ha fet servir com a criteri el **canvi d'actituds** i conductes del client envers la seguretat, el qual deixa de veure-la com una despesa per a veure-la com una inversió. Malgrat això, es mesura més la persuasió que no pas una altra cosa. Finalment, hi ha empreses que fan servir la motivació del seu personal de seguretat com un criteri. Aquest criteri, però, mesura la qualitat del servei que presten massa indirectament i incertament.

La seguretat és un bé intangible. Hi ha un estudi que fa servir els criteris esmentats per a estudiar com entenen la qualitat un grup de directius d'empreses espanyoles (Torrente, 2006). El criteri més referit és la capacitat de l'empresa de respondre a les necessitats i demandes del client. En el segon lloc hi figura el grau d'absència d'errors o incidències en els serveis. En el tercer lloc s'esmenta la satisfacció del client. En el quart, la importància dels danys o pèrdues evitats amb el servei. En el cinquè, la capacitat d'influir en el client o educar-lo. Fi-

nalment, hi ha el grau en què l'empresa és capaç de motivar el personal. Com que la seguretat és una activitat de serveis, la capacitat d'atendre qualsevol eventualitat del client és vista com a molt important, sobretot pel subsector de base tecnològica (seguretat contra incendis, sistemes electrònics). Aquest subsector coincideix amb el de la vigilància a destacar la importància de l'absència d'incidències en els serveis i, encara que no tant, la satisfacció del client. Crida l'atenció que no es parli gaire d'un criteri centrat més en els resultats com és ara la quantia de danys o pèrdues evitats. Una explicació possible és la dificultat a l'hora de mesurar-lo. En general, hi ha un desacord notori en els criteris de qualitat. En qualsevol cas, els més esmentats són la capacitat de resposta, l'absència d'incidències i la satisfacció del client. L'accent en aquest tipus de criteris revela que el sector espanyol dóna més importància al servei mateix que no pas a l'eficàcia. Si un indicador del grau de desenvolupament d'un sector és el consens a l'hora de definir la qualitat i l'excel·lència en els seus serveis, segons l'estudi esmentat, a Espanya queda terreny per recórrer.

Resumint les idees del capítol, un risc és bàsicament un esdeveniment no desitjat al qual s'associa una probabilitat. Per tant, n'hi ha una gran diversitat (mediambientals, delictius, laborals, mèdics, etc.). Els riscos es poden analitzar des de diferents perspectives. La més emprada i simple és la racionalista. El sector de la seguretat privada la fa servir molt. La raó és que tendeix a definir la seguretat com l'evitació de danys i pèrdues, i a plantejar-se estratègies de vigilància i prevenció situacional. Per tant, l'objectiu i el camí són clars i, normalment, no hi ha gaire complexitat en l'entorn. El model racional encaixa perfectament amb aquestes condicions. Altres models d'anàlisi de riscos són més complexos perquè involucren processos psicològics, socials o polítics.

2. Disseny dels serveis

Aquesta unitat mira d'explicar la lògica que hi ha al darrere dels serveis de seguretat privada. L'anàlisi parteix de la idea, vista en la unitat anterior, que hi ha moltes estratègies per a respondre als problemes de seguretat. Aquestes estratègies es concreten en determinats productes i serveis que comercialitza el sector. La manera en què aquests productes i serveis són dissenyats, venuts, duts a terme i avaluats depèn de determinats factors que discutirem en aquest capítol. En primer lloc estudiarem les necessitats i prioritats del client. En segon lloc analitzarem el paper que té la tecnologia en desenvolupament de productes i serveis. En tercer lloc discutirem com influeix el nivell de risc de determinats serveis o clients. A més, hi ha altres factors de l'entorn de les empreses que afecten els seus serveis, com el marc legal, el mercat laboral, els accionistes i les pressions de la competència. Tots plegats acaben configurant l'oferta de serveis de seguretat privada.

2.1. Estratègies i serveis de seguretat

La seguretat consisteix bàsicament a situar les situacions de risc en límits acceptables. Aquestes situacions poden ser diverses, però també hi ha moltes possibilitats de donar-hi resposta; és a dir, diverses maneres de gestionar-les.

> Les estratègies de seguretat es poden entendre com un conjunt coherent i anticipat d'accions orientades a un objectiu. Una estratègia és, per tant, una combinació més o menys ordenada de respostes i objectius.

Hi ha diverses estratègies per a crear o potenciar la seguretat. Aquestes estratègies es poden classificar de diferents maneres. Horwitz (1990) distingeix quatre **estils de control social**:

- El penal implica castigar les persones que es desvien. Hi ha diversos criteris i consideracions a l'hora de triar i escalar un càstig.
- El compensatori consisteix en el fet que els transgressors recompensen econòmicament les seves víctimes.
- El conciliatori consisteix en la negociació conjunta de les parts, sia amb mediador o sense, per a cercar una solució conjunta al greuge.
- El terapèutic comporta el tractament expert de les persones que es desvien amb l'ànim de reintegrar-les a la normalitat.

Totes les estratègies esmentades són reactives. És a dir, s'engeguen com a resposta a un fet que ja s'ha produït. Malgrat això, també hi ha estratègies preventives que miren d'evitar que es produeixi un fet no desitjat o, en tot cas, minimitzar-ne les conseqüències negatives.

La seguretat té tres dimensions: l'objectiva, la subjectiva i la tolerable. Per tant, una manera de produir-la és gestionar la percepció d'inseguretat (o por). Se sap que hi ha diferents factors que afecten aquesta percepció (informacions distorsionades, entorns bruts i desordenats, poca confiança en les institucions de seguretat, etc.). Es tracta, llavors, d'actuar-hi. Una altra estratègia de seguretat consisteix a aconseguir que la població sigui més tolerant a certs actes desviats o a determinats col·lectius.

La naturalesa mateixa dels riscos no determina completament les estratègies per a donar-hi resposta. Aquestes estratègies més aviat són el fruit d'una decisió política i social. Les institucions poden fer servir diferents estratègies en funció del moment històric o de les circumstàncies. També en poden combinar diverses de diferents. Les estratègies institucionals no són inamovibles. La policia, per exemple, està condicionada pel marc de l'estat de dret i del sistema penal en què està immersa. Això fa que elabori una estratègia penal predominant en les seves respostes. Malgrat això, la policia ha anat incorporant estratègies de mediació, de prevenció situacional o comunitària, educatives, etc., en funció dels condicionants que troba. Tampoc no s'ha de pensar que la seguretat privada està abocada a fer servir sempre les mateixes estratègies. De fet, la seguretat privada es caracteritza per la flexibilitat d'adaptar-se a les necessitats dels seus clients.

> Així, per exemple, una empresa que col·labora estretament amb la policia tendeix a mimetitzar les seves respostes penals. No obstant això, aquesta mateixa empresa pot emprar estratègies de prevenció situacional amb un altre client.

Per tant, en la protecció dels clients, les empreses de seguretat fan servir diverses estratègies. En uns casos, la seguretat es basa a obtenir informació rellevant (detectius privats). En d'altres, l'accent recau en la prevenció de danys, sien personals o econòmics (vigilància, videovigilància, sensors, dissuasió per mitjà de gossos). La reparació de danys i pèrdues és una altra opció (assegurances). També ho és traslladar un cas al sistema penal (denúncia). La recopilació i anàlisi d'informació es dóna en el sector dels serveis (asseguradores, sobretot) i entre els particulars que recorren a detectius privats. Es pot optar per crear sensació de seguretat millorant la il·luminació o esborrant grafits. En general, **la seguretat privada segueix una estratègia preventiva** més que no pas reactiva. Dit d'una altra manera, la seguretat privada ven prevenció de danys i pèrdues materials i personals. És una prevenció vinculada més a la vigilància i la dissuasió que no pas a atacar les causes dels problemes. En bona mesura juga també amb la creació de sensació de seguretat. De respostes reactives, com denunciar delictes, n'hi ha, però no són tan freqüents com en

la seguretat pública. La idea important en tot això és que **les estratègies de seguretat són contingents**; no són intrínsecament privades o públiques. La qüestió rellevant és saber quins factors expliquen la tria d'una o altra.

Un servei de seguretat té, bàsicament, tres components:

- un objecte que cal protegir,
- un risc o amenaça del qual protegir aquest objecte, i
- una estratègia per a fer-ho.

L'objectiu final sol ser evitar o minimitzar el dany o la pèrdua. De les estratègies de seguretat ja n'hem parlat.

En relació amb el primer aspecte, l'**objecte que cal protegir**, els clients de la seguretat privada poden voler protegir persones, instal·lacions o béns materials. Tots són elements tangibles. També podrien voler evitar, però, altres conseqüències negatives, com incórrer en responsabilitats per incompliment de normes, accidents o incidents, perdre reputació, encarir les assegurances. Fins i tot, poden voler protegir aspectes interns, com els seus processos de producció, o externs, com la seva posició en el mercat.

Les possibles **amenaces** són incomptables. Poden provenir de fenòmens naturals, inundacions, llamps, terratrèmols i altres meteors. Poden tenir origen en accidents o incidents que es produeixen en el transcurs normal de l'activitat dels clients, com incendis, curtcircuits, caigudes de mercaderies, relliscades de treballadors o atropellaments. Poden ser el resultat de conductes deliberades i malintencionades, com sabotatges, intrusions, robatoris, segrestos o extorsions. Els riscos no són tots iguals. Si s'analitza la història d'una companyia o es fan estudis, es veu que cada risc està associat a una probabilitat o possibilitat que s'esdevingui. Les conseqüències tampoc no són les mateixes. El dany potencial que produeix una inundació a la sala on hi ha els servidors informàtics de l'empresa és molt més gran que l'efecte que tindrà als vestidors. Al seu torn, les conseqüències negatives són molt diverses: pèrdues de jornades laborals, de producte acabat, d'informació, d'imatge corporativa, de posicions en el mercat, etc. En darrera instància, tots aquests danys i pèrdues es poden estimar en termes monetaris. Com s'aprecia, tant els objectes que cal protegir com els riscos de protegir-los, són molts i diversos. Tot això ofereix a la indústria de la seguretat un enorme camp d'activitat i d'especialització (De Waard, 1999).

Cada client centra la demanda (i la despesa) a protegir els elements que tenen una importància estratègica en la seva activitat. De la mateixa manera, mira de protegir-se de les eventualitats més probables. De fet, l'anàlisi de riscos consisteix precisament a identificar aquests elements, valorar el grau d'exposició que tenen i calcular les conseqüències que tindria per al client que es materialitzés una eventualitat. Hi ha diferents activitats que poden ser sensibles a amenaces de procedència molt diferent: pèrdues d'inventari, absentisme de treba-

lladors, accidents, inundacions, interrupcions en el subministrament elèctric, plagis, responsabilitats civils o penals, agressions contra els directius, filtració d'informació a la competència.

> Per a una multinacional farmacèutica és crucial impedir l'accés als ordinadors de recerca. Per a una marca, una filtració sobre el darrer model de cotxe pot ser catastròfica. Per a l'estat és vital protegir instal·lacions crítiques, o els seus líders polítics, entre altres elements. Per a una cadena de supermercats és important mantenir l'activitat de la línia de caixes. Si el client és un particular, probablement protegirà les seves propietats o el seu patrimoni.

Vist des d'una perspectiva empresarial, la seguretat és un actiu econòmic: ajuda a mantenir o millorar la qualitat, la quantitat o el valor afegit de la producció.

Per tant, cada tipus de client té un perfil diferent d'objectes que cal protegir. La protecció de béns i instal·lacions afecta tota mena de clients, encara que una mica més el sector industrial, la construcció i l'Administració pública. També les empreses que provenen de sectors subjectes a una regulació intensa i a un sistema de responsabilitat com el sector industrial, la banca, l'Administració pública o alguns serveis que contracten seguretat privada, a més d'altres motius, per a evitar sancions o no incórrer en responsabilitats. El sector espanyol de la seguretat gira molt al voltant de la protecció d'instal·lacions i béns. Malgrat això, no s'assumeix tant la protecció d'altres elements que impliquen més especialització, o s'acaben derivant a empreses fora del sector. Un d'aquests elements és la protecció de la posició en el mercat. Aquesta posició es pot veure amenaçada per diverses causes (per exemple, filtració de patents, problemes en la producció, desfasament tecnològic, ús d'informació inadequada o falsejada). La seguretat té aquí aspectes d'intel·ligència organitzacional, d'espionatge industrial o de protecció de la propietat intel·lectual, entre d'altres.

La demanda de serveis de seguretat corporativa cada vegada adquireix més complexitat i entronca amb altres activitats especialitzades de consultoria de negocis o enginyeria industrial. S'esdevé el mateix amb la seguretat dels processos de producció, que es connecta amb aspectes d'organització de la feina, seguretat laboral o control de la qualitat. La informació és un bé estratègic en la societat del coneixement. De manera creixent, així ho entenen moltes empreses i despatxos que ofereixen serveis de seguretat informàtica, protecció de bases de dades, contraespionatge, investigació comercial o investigació privada. El client és molt transversal i prové de qualsevol activitat, encara que potser una mica més els serveis públics i privats. Aquests exemples fan pensar que hi ha certes activitats de seguretat molt qualificades que encara no han aconseguit tot el seu desenvolupament potencial a Espanya, si bé es troben a faltar estudis comparatius.

2.2. Demandes de clients

L'oferta de productes i serveis de seguretat està condicionada en bona mesura per la demanda del client, i aquesta demanda, per la manera en què aquest client identifica, conceptualitza i prioritza les seves necessitats de seguretat

(Torrente, 2006). Les empreses, com la gent, fan les seves pròpies anàlisis de riscos. De vegades es basen en les percepcions subjectives dels seus responsables, de vegades són estudis que elaboren els directors de seguretat, els gabinets especialitzats o els proveïdors de serveis. De manera més o menys informada, les empreses mantenen concepcions sobre quins objectes caldria protegir, de quins riscos, de quina manera i quants diners s'està disposat a invertir en això. La demanda que fa finalment el client depèn de com avalua aquests elements, però també de si concep la seguretat com una despesa o una inversió.

La seguretat té una dificultat intrínseca per superar per a poder vendre's. Aquesta dificultat consisteix en el fet que allò que és normal és que no passi res. Per a les persones o empreses que tenen aquest pensament, pot ser que pagar un servei de seguretat no tingui sentit o no sigui una prioritat. En aquests casos, la percepció del **valor afegit** de la seguretat no és gaire. Llavors, probablement, no hi haurà demanda tret que estiguin obligades per la legislació o les condicions de l'assegurança a adoptar certes mesures de seguretat. Per contra, hi ha altres empreses que perceben la seguretat com una inversió. El seu objectiu quan contracten un servei de seguretat és prevenir els costos econòmics importants que comportaria la materialització de certs riscos als quals estan exposades. D'altra banda, també poden valorar altres beneficis, com oferir una imatge de seguretat o de prestigi social als clients, transmetre missatges dissuasius a potencials transgressors, donar suport als directius preocupant-se de la seva integritat física, abaratir la prima d'assegurança o protegir-se d'eventuals sancions i reclamacions.

Segons els directius de les empreses de seguretat espanyoles (Torrente, 2006), la motivació principal dels clients per demandar seguretat és prevenir danys i pèrdues directes, o evitar sancions perquè no compleixen la normativa. La demanda de seguretat no està gaire associada a qüestions d'imatge (excepte potser en alguns serveis de cara al públic), protecció personal o suport als processos productius, o com a manera d'abaratir les primes de les assegurances. Potser per això les empreses de seguretat es veuen a si mateixes més com a proveïdores de serveis de prevenció de danys i costos que no pas com a col·laboradores en el funcionament de l'activitat dels clients. Tendeixen a pensar que bona part de les demandes que reben, incloent-hi les del sector públic, conceben la seguretat més com una despesa que no pas com una inversió. Fins a cert punt, tampoc no es veuen a si mateixes com a reforçadores de la seguretat pública.

El tipus de demanda varia segons el **tipus de clients**. Per exemple, entre els clients del sector industrial, els riscos solen ser explícits i estar vinculats al tipus de matèries primeres amb què treballen o als seus processos de producció. En les grans firmes industrials, els responsables de riscos laborals, industrials o de manteniment o els directors de seguretat tenen un protagonisme a l'hora de definir necessitats de seguretat. Per això, les exigències als proveïdors d'aquesta veta de mercat solen ser més grans que no pas en el sector dels serveis privats o públics, i les discussions es tornen més tècniques. A les companyies grans hi sol haver un responsable o director de seguretat; a les més petites aquestes

funcions, de vegades, les fan els encarregats de manteniment. Com a conseqüència de tot això, el sector industrial valora la capacitat de servei i tècnica dels proveïdors de seguretat.

El **volum de l'empresa** de seguretat es relaciona, en part, amb el tipus i caràcter dels serveis que ofereix (Torrente, 2006). Ho fa, però, en bona mesura, perquè tenen clients diferents. Les empreses de seguretat molt grans ofereixen uns serveis més diversificats i generalistes –encara que amb un pes important de la vigilància–, mentre que les empreses mitjanes i petites ofereixen serveis més especialitzats. Els clients importants del sector solen consumir molts serveis de vigilància, mentre que el muntatge i manteniment d'equips té una importància relativa més gran entre els clients mitjans i petits. D'altra banda, a mesura que augmenta el volum de l'empresa de seguretat, els serveis que es venen posen més l'accent en la planificació. A la pràctica, això vol dir que van més acompanyats d'estudis previs de riscos. Aquest fet s'esdevé sobretot a les empreses de força volum, que són les que solen tenir clients importants i amb necessitats complexes que cal analitzar i planificar bé. Aquesta anàlisi es fa en col·laboració amb els directors de seguretat, que són una figura present, sobretot, en les grans firmes. En aquest sentit, es pot dir que la capacitat del proveïdor de definir el servei de seguretat és més petita quan el client és una empresa gran o una multinacional. Les negociacions amb aquest tipus de clients solen ser dures. Per contra, les empreses de seguretat més petites solen tenir també clients més petits, amb els quals es dóna més confiança i proximitat. Malgrat això, els clients multinacionals ofereixen al sector un gran volum de facturació. A més, permeten als proveïdors de seguretat expandir-se per altres països o beneficiar-se de la seva gran xarxa social.

2.3. Rol de la tecnologia

La innovació i el desenvolupament tecnològic tenen incidència no solament en l'oferta de productes i serveis, sinó també en la dinamització de la demanda. La innovació comprèn nous conceptes de seguretat, maneres d'organitzar-la i aplicacions tècniques. Més que no pas tecnologies de la seguretat, hi ha tecnologies aplicades a la seguretat (Gabrosky, 1998). L'evolució d'aquestes tecnologies és molt ràpida. Malgrat això, el rol que té en el sector és més complex del que se sol pensar. Un primer debat és si les tecnologies de la seguretat, cada vegada més fiables i barates, supleixen el factor humà, cada vegada més escàs i car. Probablement hi ha certes tasques clau en seguretat que fa un vigilant (intervenir, tranquil·litzar o, fins i tot, dissuadir) que no es poden mecanitzar. N'hi ha d'altres, però, que potser sí. En el fons, la qüestió central és quins avantatges i límits té la tecnologia respecte als serveis de base humana. D'altra banda, no totes les tecnologies són iguals en eficàcia i en capacitat de generar vendes (Gabrosky, 1998).

Els directius de les empreses de seguretat espanyoles valoren més la inversió per a desenvolupar productes o processos nous, fins i tot per a millorar l'organització (Torrente, 2006). No obstant això, la inversió per al desenvolu-

pament de coneixement bàsic, compra de patents, es valora com a menys important. D'altra banda, les raons declarades per les quals val la pena invertir en recerca i desenvolupament són mantenir o augmentar la quota de mercat i formar o capacitar el personal. Curiosament, la recerca bàsica o la compra de patents no es vincula a aquestes finalitats. Els directius mantenen diferències de percepció sobre la importància de la tecnologia en els serveis segons el volum o l'activitat de l'empresa. Els d'empreses petites subratllen la importància que té conèixer de prop les necessitats del client i el tracte personal; els de les mitjanes posen èmfasi en la capacitat d'oferir un bon servei, i els de les grans s'estimen més un equilibri entre professionalització i tecnologia.

Hi ha certs segments, com la prevenció d'incendis, en què dominen els sistemes basats en la tecnologia. En aquest cas, però, es tracta solament d'activar automàticament l'extinció davant l'indici de foc. En el sector de la seguretat (*security*), però, sempre fa falta, davant un avís d'emergència, que hi hagi algú que prengui la decisió sobre la manera com s'ha d'actuar. El dubte és si el decisor ha de fer també la tasca de vigilància. En qualsevol cas, els directius del sector coincideixen en el fet que la tendència és a tenir menys vigilants, però més especialitzats i preparats. Per a això, però, cal que el client també concebi la seguretat com un servei especialitzat i d'alt valor afegit.

Una de les tendències en el desenvolupament tecnològic és cap a la confluència i **integració de diferents tecnologies** (Gabrosky, 1998). Això fa que hi hagi més convergència entre branques diferents de la seguretat (incendis, intrusió, vigilància, etc.). Hi ha nombrosos exemples en què la domòtica, les tecnologies informàtiques o les de comunicacions s'han integrat. En fer-ho, les organitzacions han d'entrar en àrees de negoci noves. Normalment, la innovació és més fàcil en empreses petites i flexibles. Una altra possibilitat és la col·laboració estratègica entre companyies amb una tecnologia que tendeix a convergir. Una altra tendència és a anar cap a sistemes més **intel·ligents** i **interactius**. Els sistemes no solament detecten amb sensors, sinó que aquests sensors estan connectats a sistemes informàtics. El resultat és que són capaços de cercar, analitzar i comunicar informació en temps real. Aquesta integració entre les tecnologies sensorials (detectors, escàners, càmeres), de la informació (bases de dades, computadors) i de les comunicacions (telefonia digital, satèl·lits) ofereix unes possibilitats enormes en el camp.

Les noves tecnologies produeixen certs canvis en la manera de treballar (Gabrosky, 1998). Un exemple d'això és l'efecte d'Internet en la investigació privada. La feina del detectiu privat consisteix a proporcionar informació al client. Aquesta informació ha de ser rellevant i presentar-se de la manera adequada segons la finalitat. Poden ser proves per a un judici, informes comercials tècnics, proves de conductes, dades personals reservades o dades financeres sobre empreses. És a dir, es demana informació que ajudi a prendre decisions. Normalment es tracta d'informacions que aquest detectiu no pot aconseguir fàcilment, ni són públiques o accessibles. Hi ha certes informacions que les obté amb seguiments, perquisicions, simulacions o gràcies a contactes en de-

terminades institucions. En alguns casos hi ha acords informals de reciprocitat entre despatxos o detectius. Els despatxos més grans mantenen relacions amb altres gabinets estrangers que els posen en contacte amb bufets d'advocats o institucions d'altres països. Internet canvia la feina del detectiu perquè permet obtenir una bona quantitat d'informació de les xarxes socials o de molts altres llocs virtuals. També perquè facilita i agilita l'intercanvi d'informació entre col·legues o entre despatxos. Malgrat això, les noves tecnologies no desplacen del tot els mètodes tradicionals. La professió de detectiu continua fent servir les xarxes de contactes que faciliten l'accés a determinades informacions.

La innovació i la tecnologia també introdueixen canvis en l'organització dels serveis (Fisher i Green, 1998; Gabrosky, 1998). Un exemple d'això són els serveis de vigilància, que cada vegada són més tecnificats i tenen menys personal. La mecanització completa de la vigilància és difícil perquè, com hem indicat, en els moments crítics cal tenir algú al lloc i moment just perquè avaluï la situació i prengui decisions. L'existència d'alarmes connectades a centrals receptores i als mòbils dels propietaris permet innovar en els serveis.

> Un exemple d'això són els serveis dits *d'acudir*, que miren de racionalitzar l'ús del vigilant, que acudeix sol a l'espai protegit quan es produeix una alarma i que hi entra amb la clau que li ha deixat abans el propietari. Un altre canvi que permet la tecnologia és fer copartícip el client en la presa de decisions quan hi ha una situació d'alarma. El senyal d'alarma en un habitatge s'envia, juntament amb imatges i sons en temps real, al telèfon mòbil del propietari i a la central de la companyia de seguretat. La central d'alarmes entra en contacte amb el propietari i valoren plegats si es tracta d'una vertadera situació d'alarma o no.

Els canvis tecnològics produeixen, sovint, desajustos entre la realitat del mercat i la seva regulació (Rubise, 1994). La innovació en el sector va molt de pressa i la innovació legislativa és més lenta. Un exemple gràfic d'això és la tendència a integrar sistemes. Així, els nous sistemes domòtics integren i gestionen sistemes diferents d'una casa, com ara la temperatura, la il·luminació, la videosupervisió de nens, el monitoratge de gent gran o malalts, o l'alarma antirobatori. La informació que processen pot tenir moltes aplicacions en seguretat, oci, medicina o assistència social. Aquests sistemes són capaços de comunicar-se amb centrals d'alarma que, al seu torn, poden rebre i gestionar informació procedent de diverses fonts (per exemple, senyals telefònics i imatges digitals, senyals de GPS o informació d'Internet). El problema es planteja quan, en contra de la tendència a la integració de sistemes i funcions, la legislació de seguretat privada insisteix a separar les funcions de seguretat d'altres funcions. Això dificulta l'acompliment de serveis integrals a la casa.

2.4. Control del risc

El sector de la seguretat treballa amb el risc. Malgrat això, com que hi estan sobreexposats, tenen la necessitat de valorar-los bé i saber evitar els més seriosos o, almenys, mantenir-los sota control. De fet, la clau del seu negoci es assumir tan pocs riscos com sigui possible com a empresa. Això mateix s'esdevé en altres activitats relacionades amb la seguretat (i amb totes en general). Així, el

primer que aprèn un policia és a gestionar les situacions conflictives i a no exposar-se. Les companyies d'assegurances fan càlculs actuarials constantment amb l'objectiu de no assumir massa riscos financers.

Els experts en risc ho són perquè saben controlar-lo. Protegint la seguretat dels seus clients, el sector de la seguretat es pot veure exposat també a riscos per als seus treballadors, els seus equips o l'empresa mateixa (riscos financers, responsabilitats penals i civils, entre d'altres). Les fonts són molt diverses: riscos tecnològics (informàtics, de les comunicacions), industrials (accidents nuclears o químics), naturals (inundacions, terratrèmols, tempestes), financers, de mercat (espionatge industrial, fugida de cervells), petita delinqüència (robatoris, furts, violència), delinqüència organitzada (terrorisme, tràfic il·legítim de mercaderies), delinqüència de les organitzacions (fraus en productes, publicitat falsa, contaminació), etc.

Per tant, no hi ha ningú que valori tant la seguretat com una empresa de seguretat (o d'assegurances). La seva continuïtat depèn de controlar el risc. Els riscos que assumeix el sector varien, en part, segons l'activitat del client. Per això, el client ideal seria el que valora la seguretat com un valor afegit, es deixa assessorar, té una capacitat de compra alta i un potencial d'expansió en les compres, i no presenta riscos o problemes extraordinaris, o si en presenta cap, no ho fa de manera continuada. La preferència llavors és assumir serveis de risc moderat i derivar a altres actors o a l'estat els serveis de més risc. L'empresa de seguretat també ha de tenir un entorn relativament segur per a dur a terme l'activitat econòmica. El garant últim d'aquest entorn és l'estat. Això planteja el debat teòric de si s'està produint una divisió de funcions en la qual el sector privat assumeix els casos de baix risc i l'estat els d'alt risc (Becker, 1974).

Davant un risc destacat, l'empresa pot decidir assumir-lo pactant tot un seguit de salvaguardes amb el client, apujant el preu, contractant assegurances addicionals, subcontractant altres companyies per a determinades tasques, o modificant el format o organització dels serveis de seguretat. El risc es converteix així en un element més que influeix en el disseny dels productes i l'organització dels serveis de seguretat.

> Per exemple, l'ús de vidres blindats en bancs, benzineres, administracions de loteria, etc., sorgeix en una època de gran auge de l'heroïna i en la qual es produeixen molts assalts lligats al consum d'aquesta droga.

També pot decidir no assumir el risc i no treballar-hi. Sempre és interessant analitzar els tipus de riscos que no assumeix la indústria de la seguretat i les raons que hi ha per a fer-ho. La decisió de rebutjar un servei se sol produir quan els possibles riscos no compensen la rendibilitat d'aquest servei.

A Espanya gairebé no hi ha estudis sobre el tipus de **situacions o problemes** que es detecten en els serveis de les empreses de seguretat. Un estudi diu que es donen tres grups de situacions (Torrente i altres, 2005).

- En el primer grup hi ha les situacions més nombroses, que tenen a veure amb la propietat, i dins aquestes situacions, els petits robatoris i, encara que no tant, el vandalisme. Crida l'atenció que, des del món privat, també s'observen situacions que es poden relacionar amb la delinqüència organitzada o, almenys, amb delictes de grup (robatoris en polígons industrials o xalets a càrrec de bandes, sabotatges sofisticats, tràfic de drogues, amenaces terroristes, etc.).

- En el segon grup hi ha les situacions més relacionades amb els conflictes de convivència, violència quotidiana i medi ambient (conflictes, baralles, etc.).

- En el tercer grup hi ha una diversitat de situacions contra l'empresa (com ara atacs a la seguretat informàtica) o d'altres que tenen a veure amb determinades males pràctiques de la mateixa organització a la qual serveixen.

La seguretat privada pot ser un observador privilegiat d'aquestes situacions. Malgrat això, segons aquest estudi, els delictes contra el medi ambient, el blanqueig de diner o el mal ús de fons públics no es detecten. L'autor conclou que, en general, la seguretat privada espanyola assumeix riscos moderats, i que els camps de més risc o conflictivitat queden relativament fora dels seus serveis.

El sector de la seguretat privada detecta de manera creixent riscos derivats d'una nova delinqüència global o, almenys, transnacional. Són incidents que impliquen xarxes o bandes internacionals de delinqüents, atacs informàtics, terrorisme internacional o accidents a gran escala. L'extensió de l'amenaça, les conseqüències greus que pot tenir, el poder dels grups, la sofisticació d'aquesta amenaça o els limitats instruments per a fer-hi front fa que hi hagi firmes que es replantegin alguns serveis. Un exemple d'això és l'impacte que van tenir entre les companyies asseguradores i de seguretat els atemptats de l'11 de setembre de 2001 als Estats Units i l'11 de març de 2004 a Espanya.

El fet de responsabilitzar-se de la seguretat d'un gran aeroport o assegurar-lo va deixar de ser un negoci atractiu. El problema no es resol adoptant noves mesures de seguretat o fent que siguin més sofisticades. No es tracta de cercar noves vies per a treure profit de la tradicional carrera entre el món de la seguretat i el del delicte. El problema és respondre a les enormes conseqüències i responsabilitats per la fallida de la seguretat.

Davant aquests nous riscos globals hi ha la necessitat de disposar d'informació adequada sobre les xarxes de delinqüència, les seves estratègies o les seves activitats. Malgrat que les grans companyies poden obtenir i analitzar informacions procedents de les seves seus centrals, la informació més bona està en mans de la policia i de les xarxes de col·laboració policial internacional. La intel·ligència policial és clau per a combatre-les. Aquest fet és un al·licient perquè el sector privat cerqui la col·laboració i ajuda del sector públic. D'altra banda, però, les grans multinacionals de la seguretat podrien ajudar molt perquè

tenen presència en molts països i recullen una bona quantitat d'informació en la tasca diària de protegir els seus clients. Tot això planteja el debat sobre les possibilitats d'una cooperació davant aquest tipus d'amenaces.

Una de les incerteses més importants per al sector són les conseqüències financeres que es deriven de les grans catàstrofes naturals, de la delinqüència global o dels actes del terrorisme internacional. Això està alterant les regles de joc en el sector. Les companyies d'assegurances i de seguretat cada vegada són més reticents a acceptar els riscos de protegir determinades instal·lacions. Fins i tot hi ha estats que fixen sostres en la seva responsabilitat. D'altra banda, però, en alguns sectors, concretament en els de transports i comunicacions, els atemptats terroristes de Nova York i Washington han provocat un augment de la demanda de seguretat. En general, i excepte en aquests sectors econòmics concrets, l'impacte dels atemptats no ha estat palpable, però així i tot s'aprecia un canvi de sensibilitat general envers els temes de seguretat. En països com França, les companyies d'assegurances i les de seguretat es coordinen tant en el mercat com en les seves accions de *lobby* per a reformes legislatives. És lògic si es pensa que el risc depèn de la probabilitat que s'esdevingui un incident multiplicat per la gravetat potencial de les conseqüències que pot tenir. Les empreses de seguretat incideixen en la probabilitat d'aquestes conseqüències, i les d'assegurances, a compensar els costos d'aquestes conseqüències també. A Espanya no n'hi ha tanta tradició, però tenint en compte les dinàmiques assenyalades, la tendència és a anar cap a una coordinació més gran.

En teoria, el sector privat pot assumir qualsevol tipus de serveis de seguretat. Malgrat això, hi ha determinats tipus de delictes crucials per a la seguretat dels països, com el terrorisme internacional, el tràfic de drogues a gran escala o el tràfic d'immigrants il·legals, que no generen una demanda des del mercat. Aquesta demanda únicament és capaç de generar-la l'estat. Si hi ha aquesta demanda pública, el sector privat pot col·laborar. No obstant això, hi ha un altre tipus de límits. Un principi bàsic de les empreses de seguretat (i de totes les altres) és no entrar en col·lisió amb les activitats ni els interessos dels seus clients. Per això es diu que una limitació del sector privat a l'hora d'assumir qualsevol tipus de serveis és que, en funció de la composició dels seus clients principals, poden entrar en contradicció.

> Per exemple, difícilment una empresa que presta serveis a un banc estarà interessada a investigar el blanqueig de capital, sobretot si és un bon client.

Una empresa de seguretat pot servir alhora, i sense conflicte, dos clients que competeixen en el mercat. Malgrat això, és difícil traslladar al sector privat potencials demandes de l'estat en la seva lluita contra la delinqüència de les organitzacions (Mir, 1999). Hi ha tot un debat sobre la relació entre estat i mercat de la seguretat que analitzem en la primera unitat del mòdul "La seguretat privada a Espanya".

Activitats

1. Cerqueu un informe de seguretat a Internet i mireu-ne primer l'estructura (l'índex) i el contingut. Compareu l'estructura amb el model que apareix en el quadre 3.

2. Busqueu un qüestionari de seguretat o una matriu de riscos a Internet. Estudieu-la i expliqueu a un company com funciona.

3. Trieu un magatzem d'un familiar, una botiga que conegueu, la vostra empresa (si és petita) o qualsevol altre espai al qual us sigui fàcil d'accedir. Feu l'avaluació de riscos i escriviu els resultats en un document amb l'estructura adequada.

4. Trieu cinc articles de revistes que tractin sobre una realitat delictiva. Digueu quins d'aquests articles tenen un enfocament descriptiu o explicatiu.

Exercicis d'autoavaluació

Unitat 1

1. Què és l'anàlisi de riscos?

2. Doneu una definició de *vulnerabilitat*.

3. Expliqueu en què consisteix la planificació de la seguretat.

4. Quina utilitat pràctica té un pla de seguretat?

5. Quins avantatges tenen les enquestes de victimització sobre les estadístiques policials com a fotografies de la realitat delictiva?

Unitat 2

6. Quins són els tres components bàsics d'un servei de seguretat?

7. Quins factors influeixen en el fet que un servei de seguretat es concebi i s'organitzi d'una determinada manera?

8. Expliqueu algun dels rols que té la tecnologia en la seguretat privada.

9. Quin tipus de barreres pot tenir una empresa de seguretat per a treballar en delictes fiscals?

10. Quin sol ser el plantejament de les empreses de seguretat davant el risc alt en els seus serveis?

Solucionari

Exercicis d'autoavaluació

1. L'anàlisi de riscos és el procés pel qual s'identifiquen i avaluen possibles amenaces i els punts vulnerables del sistema que cal protegir, i s'estimen les possibles conseqüències. Aquesta informació es recull en una avaluació de riscos.

2. La noció de *vulnerabilitat* és, atès el nivell de protecció actual que té, la susceptibilitat d'un bé o una persona de patir un determinat nivell de danys o pèrdues de tota mena, a causa de la materialització d'una amenaça particular.

3. La planificació de la seguretat és un procés pel qual, després d'analitzar els riscos, es fixen uns objectius de seguretat i es tria una estratègia que es desplega mitjançant tot un seguit de actuacions. A més, es preveuen els recursos necessaris, s'estableix una organització de les tasques amb els procediments i controls que fan falta i es fixen les responsabilitats corresponents. S'hi sol incloure, a més, un protocol de seguretat que defineix les regles i procediments que serveixen per a coordinar les respostes per a diversos tipus d'eventualitats, o aspectes concrets com les comunicacions, per exemple. Es planifiquen totes les necessitats de formació o reciclatge del personal. Es preveuen futures avaluacions i criteris per a modificar o corregir el pla mateix.

4. El pla de seguretat serveix a un doble propòsit: ajuda a vendre el servei i, quan ha estat comprat, és una guia de la feina que cal fer. En relació amb el primer propòsit, per mitjà del pla, el client també pot estudiar la proposta de seguretat que li fan i el cost que té. És a dir, podrà apreciar la qualitat de la proposta i el que inclou. El pla també ajuda a fer que el procés de negociació entre proveïdor i client sigui més ordenat i concret. Durant l'execució, també serveix per a protegir el proveïdor de seguretat de possibles exigències del client que no s'havien inclòs, ni pressupostat, en el pla.

5. Les estadístiques mesuren el delicte denunciat; les enquestes, el delicte percebut com a tal per la població. Ofereixen una informació quantitativa i representativa de la delinqüència que s'ha patit, encara que no s'hagi denunciat. Tenen l'avantatge que els resultats es poden extrapolar a la població. A més, permeten conèixer una gran quantitat d'informació de la víctima i de les seves actituds i opinions. Malgrat això, solament permeten saber les dades del delinqüent o determinats detalls del delicte si el delinqüent els sap. Les enquestes no són capaces de recollir tots els delictes, ja que depenen del fet que aquests delictes tinguin una víctima individual, que pugui respondre, que sigui conscient de ser-ho i que sàpiga els detalls del delicte. Això no s'esdevé en els delictes de víctima col·lectiva, o en la majoria dels delictes fiscals, o en la delinqüència organitzada.

6. Els tres components bàsics d'un servei de seguretat són un objecte que cal protegir, una amenaça de la qual protegir-lo i una estratègia per a fer-ho.

7. La manera en què els serveis de seguretat són dissenyats, venuts, duts a terme i avaluats depèn de les condicions de l'entorn de les empreses. Alguns d'aquests factors són el marc legal, el mercat laboral, els accionistes i les pressions de la competència. Malgrat això, n'hi ha tres de rellevants, que són les necessitats i prioritats del client, la tecnologia i el nivell de risc de determinats serveis o clients.

8. La innovació i la tecnologia permeten ampliar i renovar l'oferta de productes i serveis, i també dinamitzar la demanda. Permeten estalviar costos. També, però, produeixen canvis en la manera de treballar i d'organitzar la feina. Fins i tot fan que els sectors s'integrin.

9. La principal barrera és una contradicció d'interessos. També hi poden haver, però, barreres relacionades amb l'accés a informació rellevant i desbalanços de poder.

10. Les empreses de seguretat fan valoracions de benefici-risc. Si són alts, però, miren d'evitar o minimitzar riscos.

Bibliografia

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

International Organization for Standardization (2009). *Risk Assessment Techniques*. ISO: 31000.

International Organization for Standardization (2009). *Risk Management - Principles and Guidelines*. 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* [en línia]. http://www.securitymanagementinitiative.org/index.php?option=com_docman&task=cat_view&gid=22&Itemid=32&lang=en