SICUREZZA DELLE INFORMAZIONI

VALUTAZIONE DEL RISCHIO

I SISTEMI DI GESTIONE

LA NORMA ISO/IEC 27001:2013

Cesare Gallotti

Versione 15 febbraio 2017

Dedicato, come nel 2014, a, in ordine di apparizione:
Roberto e Mariangela Gallotti;
Clara;
Chiara e Giulia;
Paola Aurora, Alessio e Riccardo:
ad altri che verranno da lontano
ma già nel nostro cuore.

Indice

Presentazione e ringraziamenti

Pensino ora i miei venticinque lettori che impressione dovesse fare sull'animo del poveretto, quello che s'è raccontato.

Alessandro Manzoni, *I promessi sposi*

Nel 2002 scrissi il libro *Sicurezza delle informazioni - Analisi e gestione del rischio* per la FrancoAngeli [33] e mi ero divertito molto a scriverlo. Mi ha fatto anche molto piacere incontrare in questi anni più di 25 persone, che l'avevano letto e apprezzato; purtroppo, spesso, l'avevano preso in prestito da una biblioteca e questo non ha aiutato ad aumentare le vendite.

Va detto che non speravo assolutamente di guadagnare alcunché da quella operazione. Speravo solo di ripagarmi del toner e della carta utilizzati per stampare e correggere le bozze.

Dopo più di dieci anni ho voluto rimettere su carta (elettronica) le idee maturate durante i corsi di formazione, le presentazioni, le discussioni con colleghi e amici, gli incontri a livello nazionale e internazionale per scrivere la ISO/IEC 27001:2013. In alcuni casi, alcune delle convinzioni del 2002 sono cambiate, grazie ai tanti audit e progetti di consulenza fatti in questi anni.

Si tratta quindi più di una raccolta di appunti che di un vero e proprio saggio:

- la prima parte riporta le basi per descrivere la sicurezza delle informazioni e un sistema di gestione per la sicurezza delle informazioni;
- la seconda parte descrive la valutazione del rischio, con un'ampia parte teorica, bilanciata da molti esempi; i calcoli presentati non sono necessari per comprendere appieno i concetti esposti;
- la terza parte descrive i controlli di sicurezza ed è stata ricavata dagli appunti, basati sulla ISO/IEC 27002, che utilizzo per le attività di audit e di consulenza;
- la quarta parte illustra i requisiti della ISO/IEC 27001:2013 secondo la mia interpretazione maturata durante i lavori di scrittura della norma stessa, i corsi di formazione e le discussioni con i clienti;

- le prime tre appendici riportano alcune brevi presentazioni fatte a margine di corsi di formazione (sulla gestione degli auditor e sulla certificazione) o per l'avvio di progetti di certificazione (sui passi per realizzare un SGSI);

- l'appendice sui Common Criteria e sulle FIPS 140 è un gentile omaggio di Stefano Ramacciotti;

- le successive appendici gestione dei cambiamenti, minacce e fornitori sono tratte da alcune mie liste di riscontro utilizzate durante dei progetti.

Ci tengo a precisare che questo testo si basa molto sulla ISO/IEC 27001, ma non è una guida ufficiale alla sua interpretazione: quella è pubblicata come ISO/IEC 27003:2017.

Questo libro è stato scritto per quanti vogliono imparare e approfondire cos'è la sicurezza delle informazioni; ho infatti cercato di rispondere a tutte le domande che mi sono state rivolte in questi anni.

Credo inoltre che alcune riflessioni possano interessare chi conosce già la materia ed essere lo spunto per nuove discussioni. Ciascuno ha i propri punti di vista, anche diversi dai miei, e un confronto potrebbe migliorare le nostre competenze.

Il testo delle norme qui riportato libro non è identico a quello delle traduzioni ufficiali, sia per questioni di diritto d'autore, sia perché, in alcuni casi, volevo rendere il testo più significativo.

Le definizioni sono tratte soprattutto dall'edizione del 2016 dello standard internazionale ISO/IEC 27000. Alcune definizioni sono state lievemente modificate per renderle, a mio parere, più comprensibili. Tra parentesi quadre sono riportate eventuali aggiunte. Le cancellazioni sono evidenziate dal simbolo "[...]".

Ho collaborato in prima persona alla traduzione della ISO/IEC 27001 e 27002 (nel primo caso ero responsabile del progetto, insieme a Fabio Guasconi, Presidente dell'SC 27 di UNINFO). Ciò non ostante, invito chiunque voglia occuparsi di ISO/IEC 27001 a leggere direttamente le norme e preferibilmente in inglese (spesso poco corretto, ma facilmente leggibile). Alcune pubblicazioni italiane sono ottime, ma spesso i testi e gli articoli più aggiornati sono in inglese; si pensi alle linee guida dell'OWASP o del NIST, alcune delle quali segnalate in bibliografia.

Ci tengo a ringraziare tre persone per l'aiuto dato nella scrittura di questo libro, in rigoroso ordine alfabetico:

- Massimo Cottafavi, esperto di Governance, risk and compliance, con cui discuto da tanti anni e che ha letto le bozze e mi ha dato utili idee e un po' di testo da copiare;

- Roberto Gallotti, inflessibile correttore di bozze e fornitore di idee; anche se non può dichiararsi esperto di sicurezza delle informazioni, è un professionista da cui vorrei imparare di più;

- Stefano Ramacciotti, con cui ho discusso di sicurezza delle informazioni in giro per il mondo durante alcuni meeting dell'SC 27 e che ha anche contribuito a delle parti di testo (in particolare, l'appendice sui Common Criteria, l'esempio di Fort Knox e quanto riguarda le tre e le quattro P).

Queste persone sono tra i professionisti più preparati e simpatici che abbia avuto modo di conoscere in questi anni e sono molto orgoglioso di essere riuscito a rubare loro tempo e energie.

Ho sottoposto il libro ad altri amici e molti avrebbero preferito un testo più breve. Nonostante tutto, ho ritenuto opportuno pubblicare quanto fatto.

Infine, ringrazio tutti coloro (clienti, colleghi, concorrenti, partecipanti ai corsi, eccetera) con cui in questi anni mi sono confrontato e che non hanno avuto paura a condividere con me idee e incompetenze reciproche anche attraverso il mio blog blog.cesaregallotti.it e la mia newsletter mensile: persone preparate, ma consapevoli che la nostra materia è estremamente mutevole e non esiste nessuno più bravo degli altri.

Nota alla seconda edizione del 2017

Ho voluto aggiornare, seppure non molto, l'edizione del 2014 includendo alcune riflessioni emerse durante la lavorazione della ISO/IEC 27003:2017 e le esperienze maturate in tre anni di consulenza, audit e formazione sulla ISO/IEC 27001:2013 e la ISO 9001:2015.

Quasi tutti gli aggiornamenti a questo libro sono già apparsi nella mia newsletter e nel mio blog. Qui sono confluiti gli aggiornamenti normativi e alcuni esempi. Oltre a correggere degli errori, ho inserito delle riflessioni sulla *cybersecurity* e sul Regolamento europeo sulla privacy; ho inoltre eliminato alcune considerazioni sulla transizione dalla versione della ISO/IEC 27001 del 2005 a quella del 2013, inclusa un'appendice.

Per questa edizione ringrazio in modo particolare Franco Ruggieri e Pierfrancesco Maistrello con i quali ho avuto modo di discutere di molte cose in questi anni.

Pierfrancesco, insieme a Francesca Lazzaroni, si sono letti le prime bozze di questa seconda edizione e mi hanno fornito preziosi riscontri.

Ancora una volta Stefano Ramacciotti mi ha aiutato molto con la sua disponibilità e competenza. Sarò sempre in debito con lui.

Contatti

Per contattarmi, segnalare errori e proporre miglioramenti, i miei riferimenti sono disponibili su www.cesaregallotti.it.

Invito quanti sono interessati ad abbonarsi alla mia newsletter. Le modalità sono riportare sul mio sito web.

Avvertenza

I link riportati in questo libro sono stati verificati il 24 gennaio 2017.

Capitolo 1

Introduzione

Cosa [...] c'era da interpretare in "Fate i bravi"?

John Niven, *A volte ritorno*

Da sempre l'uomo ha sentito la necessità di avere le proprie informazioni al sicuro. In particolare, desideriamo che i dati personali (per esempio, il nostro stato di salute e il nostro estratto di conto) siano accessibili solo a poche fidate persone e siano accurati e corretti, che non vengano utilizzati impropriamente per telefonarci a casa o diffamarci pubblicamente sui *social network* e che siano velocemente disponibili, soprattutto su Internet.

Quanto detto riguarda la percezione individuale di cosa si intende per "sicurezza delle informazioni". Anche un'impresa o un qualsiasi ente ha una percezione di cosa si intende per "sicurezza delle informazioni"; per esempio: segretezza dei progetti innovativi e dei propri clienti, accuratezza di tutti i dati economici e di produzione, disponibilità dei sistemi informatici.

Nella prima parte di questo libro sono illustrati i concetti fondamentali relativi alla sicurezza delle informazioni, inclusa la sua stessa definizione.

Il termine *sicurezza*, però, cela in sé una contraddizione. Sicurezza, infatti, fa venire in mente qualcosa di assoluto e incontrovertibile, cioè qualcosa di impossibile nella realtà.

Spesso si dice che Fort Knox, dove si trovano le riserve monetarie degli USA, è uno dei luoghi più sicuri al mondo: sofisticati sensori, barriere perimetrali e allarmi sono tutti ai massimi livelli. Come se non bastassero, è sede di un comando di Marines pronti a intervenire per qualsiasi problema. Fort Knox è riconosciuto come sinonimo di luogo sicuro. Ma come reagirebbe la struttura a un impatto con un meteorite di un chilometro di diametro?

Come si può vedere da questo semplice esempio, non ha senso parlare di sicurezza in senso assoluto, ma solo in senso relativo. Fort Knox non è infatti resistente ad un grosso meteorite. Per questo motivo bisogna diffidare di chiunque offre prodotti o soluzioni sicuri al 100%. Una tale affermazione classifica subito la persona come scarsamente competente o come un imbonitore che vuole vendere qualcosa.

Deve essere individuato il livello *adeguato* di sicurezza che si vuole ottenere attraverso la *valutazione del rischio*. Il livello di sicurezza deve essere raggiunto attraverso opportune azioni di *trattamento*. Nel caso in cui quel livello non possa essere raggiunto, le carenze devono essere analizzate e, se il caso, accettate.

Nel tempo, la valutazione deve essere ripetuta per verificare se il livello di sicurezza desiderato e quello attuato siano ancora validi. Queste attività di valutazione, azione o accettazione e ripetizione costituiscono la *gestione del rischio* (*risk management*), oggetto della seconda parte del libro.

Nella terza parte sono illustrati i *controlli di sicurezza*, ossia le misure utili per garantire la sicurezza delle informazioni. Queste sono soprattutto di tipo organizzativo e non tecnologico. Infatti, buoni processi portano a scegliere buoni e adeguati prodotti e a gestirli correttamente. Non è vero l'inverso: un buon prodotto non conduce ad avere buoni processi.

Figura 1.0.1: Processi e prodotti

La quarta parte tratta dei requisiti della ISO/IEC 27001 per i sistemi di gestione per la sicurezza delle informazioni.

Un po' di storia

Come già accennato, la sicurezza delle informazioni è stata oggetto di attenzione sin dagli albori dell'umanità, basta pensare ai *misteri* collegati a diverse religioni. Per quanto riguarda il passato, Cesare parla di sistemi per evitare l'intercettazione dei messaggi in guerra (al capitolo 48 del libro V del *De bello gallico*); l'utilizzo della partita doppia per garantire l'integrità della contabilità, descritta nel 1494 da Luca Pacioli, è sicuramente precedente al Duecento.

Nelle imprese, fino alla diffusione dell'informatica, la sicurezza delle informazioni si riferiva ai documenti cartacei e alle comunicazioni orali; oggi deve comprendere anche la sicurezza informatica.

Questa, fino agli anni Novanta, era gestita dagli addetti informatici, senza alcun collegamento con la tutela del patrimonio, ossia con la *corporate security*, anche se i rischi di furto di informazioni e di spionaggio erano comunque presi in considerazione.

In quegli anni si verificarono fenomeni importanti relativamente all'informatica e al contesto economico e sociale:

1. la diffusione degli strumenti informatici, grazie ai personal computer e a interfacce sempre più intuitive: Microsoft Windows è del 1985 e Mosaic, il primo *browser* grafico per navigare sul web, è del 1993;

2. l'aumento delle persone e dei dispositivi connessi su Internet (a sua volta non progettato per la sicurezza [115]);

3. l'aumento delle minacce informatiche note al grande pubblico: il primo virus, quello di Morris, è del 1988;
4. la pubblicazione di normative con riferimento alla sicurezza informatica: nel 1993 fu emendato il Codice Penale per includervi i casi di criminalità informatica (Legge 547) e nel 1996 fu emanata la prima versione della Legge sulla privacy (Legge 675) a cui fu affiancato nel 1999 un disciplinare tecnico (DPR 318);
5. l'aumento della conflittualità sociale dovuto alle ristrutturazioni di tante imprese;
6. il ricorso a sempre più numerosi fornitori e l'aumento di relazioni con attori esterni rappresentate in figura 1.0.2.

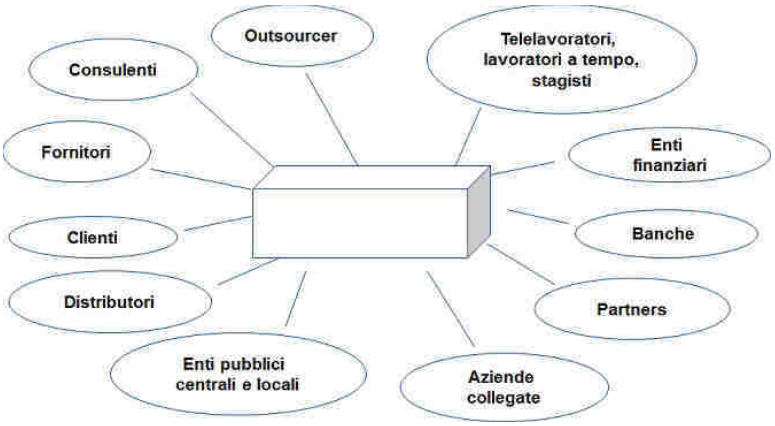

Figura 1.0.2: L'impresa aperta

Tutto questo ha fatto percepire come rilevanti le minacce relative alla sicurezza delle informazioni in generale e informatica in particolare, come illustrato in figura 1.0.3.

Negli anni Novanta cambia anche l'approccio alla sicurezza delle organizzazioni: si specializzano gli ambiti di intervento (informatica, siti fisici, persone) perché richiedono diverse competenze, si stabiliscono delle priorità di intervento sulla base di valutazioni del rischio e, in generale, si percepisce la sicurezza come attività indispensabile per garantire la sostenibilità delle organizzazioni nel tempo.

Negli anni, le esigenze di sicurezza non si sono ridotte. Questo a causa degli eventi più recenti (11 settembre, spionaggio industriale, eccetera), delle evoluzioni normative in materia di sicurezza delle informazioni e della sempre crescente globalizzazione delle imprese.

Per tutti questi motivi sono state introdotte metodologie e pratiche per rendere più strutturate le attività riguardanti la sicurezza delle informazioni. Tra le iniziative più importanti si ricordano quelle relative alla sicurezza dei prodotti e sistemi informatici (TCSEC del 1983, ITSEC del 1991, Common Criteria del 1994 e le Special Publication del NIST[1] emesse dai primi anni Novanta), alla

[1] http://csrc.nist.gov

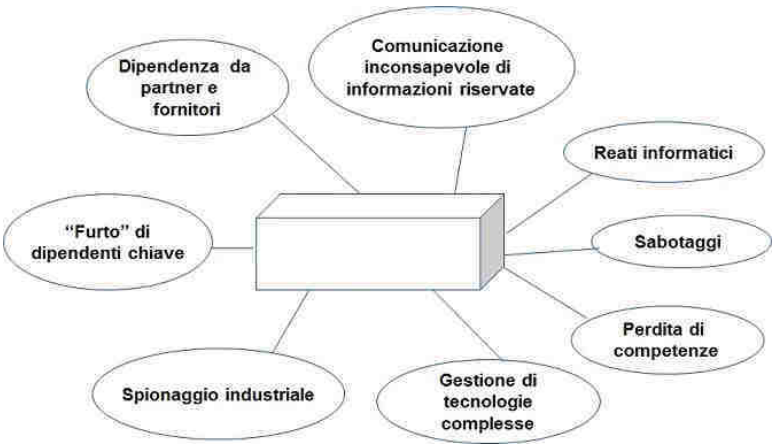

Figura 1.0.3: Nuove minacce

sicurezza delle informazioni (BS 7799 del 1995, di cui si approfondirà la storia nel paragrafo 12.4) e alle metodologie di valutazione del rischio relativo alla sicurezza delle informazioni (CRAMM del 1987, Marion del 1990 e Mehari del 1995) [22].

Parte I

Le basi

Capitolo 2

Sicurezza delle informazioni e organizzazione

Where is the Life we have lost in living?
Where is the wisdom we have lost in knowledge?
Where is the knowledge we have lost in information?

Thomas Stearns Eliot, *The rock*

In questo capitolo sono fornite le definizioni di base della *sicurezza delle informazioni*. Nel capitolo successivo è specificato cos'è un *sistema di gestione per la sicurezza delle informazioni*.

Può essere interessante svolgere un piccolo esercizio: elencare i casi di notizie lette sul giornale o di eventi di cui siamo stati testimoni o vittime, collegati alla sicurezza delle informazioni. Ad esempio:

- nel 48 p.e.v. la biblioteca di Alessandria fu incendiata con la conseguente distruzione del patrimonio librario[1];
- nel 1998, il Ministero delle Finanze inviò milioni di cartelle esattoriali sbagliate ai contribuenti[2];
- nel 2003 l'Italia sperimentò un blackout dovuto a un albero caduto sulla linea dell'alta tensione in Svizzera e che in alcune zone durò anche più di 24 ore[3] rendendo indisponibili, tra gli altri, servizi informatici e di comunicazione;
- nel febbraio 2006, i sistemi informatici del Comune di Milano si bloccarono per una settimana a causa di un virus[4];
- nel 2007 alcuni disegni della F2007 della Ferrari entrarono in possesso della sua concorrente McLaren[5];

[1] http://it.wikipedia.org/wiki/Biblioteca_di_Alessandria.
[2] www.contribuenti.it/cartellepazze/cartellepazze1.asp.
[3] www.repubblica.it/2003/i/sezioni/cronaca/blackitalia/blackitalia/blackitalia.html.
[4] attivissimo.blogspot.it/2006/02/milano-ancora-ko-da-ks.html.
[5] news.bbc.co.uk/sport2/hi/motorsport/formula_one/6994416.stm.

- nel 2010, il capo dell'antiterrorismo di Scotland Yard dovette rassegnare le dimissioni perché fotografato con un documento classificato "secret" sotto braccio e in bella vista[6];
- nell'aprile 2011, alcuni servizi informatici di Aruba rimasero indisponibili per un incendio originato dal sistema UPS[7];
- a ottobre 2011 la rete Blackberry rimase bloccata per 3 giorni a causa di un errato aggiornamento dei sistemi[8];
- nel 2011, il servizio informatico PSN della Sony fu attaccato da malintenzionati che rubarono dati sugli utenti, incluse le loro password; la Sony bloccò il servizio per mesi[9];
- a settembre 2013, i *social network* di Alpitour furono violati e alcuni link modificati per indirizzare a siti web malevoli[10];
- a inizio 2013, i servizi di antispamming della Spamhaus sono stati bloccati da un attacco[11].

Questi esempi illustrano come la sicurezza delle informazioni debba occuparsi di molti potenziali eventi negativi: incendi, eventi naturali, guasti di apparecchiature e impianti, errori umani, attacchi di malintenzionati, eccetera.

2.1 Dati e informazioni

Prima di discutere di dati e informazioni, è opportuno fornirne la definizione, presente in precedenti versioni dello standard ISO/IEC 27000. Nelle ultime versioni dello standard questa definizione non è più riportata, forse perché si preferisce far riferimento ai normali dizionari [89].

> *Informazione (Information data)*: conoscenza o insieme di dati che hanno valore per un individuo o un'organizzazione.

Le informazioni sono archiviate e trasmesse su dei *supporti*. Essi possono essere *analogici* o *non digitali* come la carta, le fotografie o i film su pellicola, o *digitali* come i computer e le memorie rimovibili (per esempio: chiavi USB, CD e DVD). Un caso particolare di supporto non digitale è l'essere umano, che nella sua mente conserva informazioni. Per la trasmissione si possono usare: posta tradizionale, telefono (ormai basato su tecnologia mista), reti informatiche e, sempre considerando il caso particolare degli esseri umani, conversazioni tra persone.

Da questo ragionamento risulta che, quando si parla di *sicurezza delle informazioni*, non ci si limita alla sicurezza informatica, ossia relativa alle informazioni in formato digitale e trattate dai sistemi dell'*Information and communication*

[6] www.corriere.it/esteri/09_aprile_10/cavalera_dossier_segreti_dimissioni_quick_41e477fe-2595-11de-bdf0-00144f02aabc.shtml.
[7] punto-informatico.it/3146710/PI/News/aruba-incendio-nella-farm.aspx.
[8] www.bbc.co.uk/news/technology-15287072.
[9] attrition.org/security/rant/sony_aka_sownage.html.
[10] www.pierotaglia.net/facebook-fai-da-te-alpitour-ahi-ahi-ahi-pagine-facebook-hackerate.
[11] www.theregister.co.uk/2013/03/27/spamhaus_ddos_megaflood.

technology, ma a tutti i sistemi utilizzati per raccogliere, modificare, conservare, trasmettere e distruggere le informazioni.

Questo è uno dei motivi per cui si preferisce parlare di "informazioni" e non di "dati": il termine, intuitivamente, ha una valenza più ampia.

Più rigorosamente, la sicurezza delle informazioni include quella dei dati, come si deduce dalle quattro tipologie di rappresentazione della conoscenza [62, 77]:

- *dati*: insieme di singoli fatti, immagini e impressioni;
- *informazioni*: dati organizzati e significativi;
- *conoscenza*: informazioni recepite e comprese da un singolo individuo;
- *sapienza*: conoscenze tra loro connesse che permettono di prendere decisioni.

Per completezza è necessario ricordare che il termine inglese *information* è un *mass noun* e quindi in italiano va tradotto al plurale.

2.2 Sicurezza delle informazioni

La ISO/IEC 27000 definisce:

> *Sicurezza delle informazioni (Information security)*: preservazione della riservatezza, integrità e disponibilità delle informazioni.

È quindi necessario definire le tre proprietà sopra riportate (tra parentesi quadre vi sono delle aggiunte rispetto alla ISO/IEC 27000).

> *Riservatezza (Confidentiality)*: proprietà di un'informazione di non essere disponibile o rivelata a individui, entità o processi non autorizzati;
>
> *Integrità (Integrity)*: proprietà di accuratezza e completezza;
>
> *Disponibilità (Availability)*: proprietà di essere accessibile e utilizzabile [entro i tempi previsti] su richiesta di un'entità autorizzata.

Ci si riferisce spesso a queste proprietà come *parametri RID* e nel seguito sono descritte più approfonditamente.

Si parla di *sicurezza informatica* quando ci si limita alla sicurezza delle informazioni sui sistemi informatici. A rigore, alcuni sistemi informatici (per esempio quelli industriali) potrebbero non essere considerati come pertinenti le informazioni.

Esempio 2.2.1. Nel 2016 degli appartamenti in Finlandia sono rimasti senza acqua calda per una settimana perché il sistema di riscaldamento è stato oggetto di attacco informatico[12].

Questo non è propriamente un attacco con impatto sulle informazioni, ma è sicuramente un incidente di sicurezza informatica.

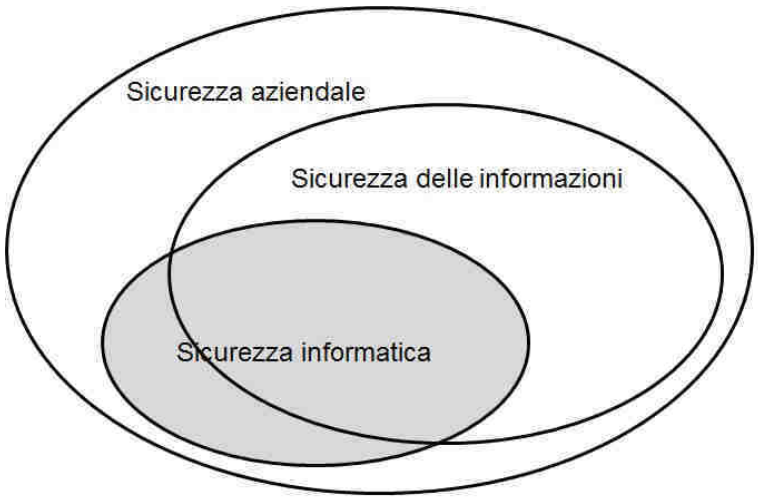

Figura 2.2.1: Sicurezza delle informazioni e sicurezza informatica

In questo libro non si usa il termine *cybersecurity* in quanto si tratta della stessa sicurezza informatica, solo con un nome ritenuto più suggestivo. Esso è tratto dal termine *cyberspace*, inventato da William Gibson nel 1986 nell'ambito della letteratura cyberpunk forse perché il termine "Internet"non era abbastanza diffuso. Lo stesso Gibson ha ammesso di avere usato il termine greco "cyber"(timone, da cui sono anche tratti i termini "governo"e "cibernetica") senza saperne il significato ma solo perchè interessante.

Negli anni in molti hanno cercato di giustificare l'uso dei termini *cybersecurity* e *cyberspace* in ambito scientifico, ma senza trovare una soluzione condivisa o rigorosa e, anzi, creando confusione e false aspettative. Per esempio c'è chi usa il termine intendendo qualcosa di più o di meno della sicurezza informatica e c'è chi lo usa per indicare la sicurezza di Internet includendo fenomeni come il bullismo online (*cyberbullismo*). In Italia, regnando la confusione, c'è chi ha tradotto "cybersecurity"con "sicurezza cibernetica", non sapendo evidentemente cosa sia la cibernetica.

2.2.1 Riservatezza

Alcuni riducono la sicurezza delle informazioni a questo parametro, ma si tratta di un approccio riduttivo.

In ambito informatico si estremizza dicendo che "il computer sicuro è il computer spento o, meglio, rotto", oppure che "l'unico sistema realmente sicuro è un sistema spento, affogato in un blocco di cemento, sigillato in una stanza con pareti schermate col piombo e protetto da guardie armate; e anche in questo caso, si potrebbero avere dei dubbi" [23]. È evidente che questo approccio non considera la disponibilità delle informazioni.

[12] http://www.theregister.co.uk/2016/11/09/finns_chilling_as_ddos_knocks_out_building_control_system/

La riservatezza è spesso associata alla segretezza, però la necessità di mantenere riservate le informazioni non implica la necessità di non rivelarle ad alcuno, ma di stabilire chi ha il diritto ad accedervi.

Non è semplice stabilire le caratteristiche di riservatezza di ogni informazione e chi può accedervi, come dimostra l'esempio seguente.

Esempio 2.2.2. In un'azienda italiana, i dati sul personale sono sicuramente riservati, ma persone diverse devono accedervi: il medico competente, l'amministrazione, i dirigenti, certi uffici pubblici, il commercialista e l'ufficio legale.

Ciascuno non dovrebbe accedere a tutti i dati, ma solo ad una parte di essi: l'amministrazione alla sola busta paga, il medico ai soli dati sanitari, eccetera.

Il livello di riservatezza di un'informazione può variare nel tempo. Il caso più rappresentativo di questo concetto è il *Freedom of Information Act* statunitense che prevede la *declassifica* (ossia la rimozione dei vincoli di segretezza) delle informazioni governative non oltre i 50 anni dalla loro creazione.

Esempio 2.2.3. Le caratteristiche di un nuovo modello di automobile vanno tenute riservate. In fase di progettazione devono essere disponibili ai soli progettisti, in fase di produzione anche agli operai, ma in fase di commercializzazione devono, seppur parzialmente, essere disponibili al pubblico.

2.2.2 Integrità

Se un dato è scorretto o alterato in modo non autorizzato, vuol dire che non è sicuro.

Esempio 2.2.4. Richard Pryor, in Superman III del 1983, riesce a rubare soldi alla propria azienda dopo averne alterato il sistema di contabilità.

Senz'altro era autorizzato ad accedere al sistema e a vedere le informazioni registrate, dato che lavorava nell'ufficio della contabilità, ma non avrebbe dovuto alterarlo senza autorizzazione.

La cancellazione di un'informazione è una forma estrema di alterazione e, pertanto, riguarda l'integrità.

2.2.3 Disponibilità

La maggior parte delle persone, come già detto, intende la sicurezza delle informazioni come mantenimento della loro riservatezza. Molti informatici, per contro, soprattutto se impiegati in aziende commerciali, intendono la sicurezza delle informazioni come la capacità di renderle immediatamente disponibili a chi le richiede. Non è però possibile pretendere l'immediatezza in tutte le occasioni e quindi la proprietà di disponibilità può essere riformulata così: "le informazioni devono essere disponibili entro i tempi stabiliti a coloro che le richiedono e ne hanno il diritto".

Esempio 2.2.5. I "tempi stabiliti" dipendono da vari fattori: nel contesto della borsa azionaria si tratta di qualche millisecondo, nel contesto di un sito web di commercio elettronico pochi secondi, in un'agenzia bancaria pochi minuti.

2.2.4 Altre proprietà di sicurezza

Le tre proprietà sopra descritte costituiscono la definizione classica di *sicurezza delle informazioni*. Alcuni preferiscono aggiungerne altre: autenticità, completezza, non ripudiabilità.

Le informazioni sono *autentiche* quando attestano la verità. Questa proprietà è caso particolare di integrità: un'informazione non autentica equivale ad un'informazione modificata senza autorizzazione.

La proprietà di *completezza* di un'informazione richiede che non abbia carenze. Una carenza è equivalente ad una cancellazione, totale o parziale, non autorizzata di dati e quindi è un caso particolare di integrità.

Un'informazione corretta, ma successivamente smentita dal suo autore è un'informazione *ripudiata*. È facile capire quanto sia importante avere informazioni *non ripudiabili*: le promesse sono mantenute e i debiti pagati nei tempi stabiliti.

Un'informazione non ripudiabile, per esempio, è quella riportata da un documento firmato dal suo autore. In altre parole, un'informazione è non ripudiabile se è completa di firma o di un suo equivalente; quindi anche questa proprietà può essere vista come caso particolare dell'integrità.

Esempio 2.2.6. Ciascun evento può avere impatti su uno o più parametri RID. Ad essi si possono quindi associare gli esempi riportati in apertura del capitolo, come nella successiva tabella 2.2.1.

Alcune attribuzioni non sono condivisibili da tutti. Una delle ragioni è che bisogna stabilire se un parametro vada assegnato considerando l'effetto diretto dell'evento o anche quello indiretto: nel caso del furto delle password della Sony, il danno diretto riguarda strettamente la riservatezza, ma poi potrebbe riguardare l'integrità (se quelle password sono usate per alterare dei dati) e la disponibilità (la Sony ha dovuto bloccare il sito per più mesi).

L'incendio viene associato all'integrità e alla disponibilità, ma potrebbe essere associato anche alla riservatezza se l'evacuazione di un edificio consente l'accesso a persone non autorizzate oppure comporta la dispersione fuori sede di documenti cartacei riservati.

Ulteriore elemento, dettato dalla normativa in materia di privacy, è il *diritto all'oblio*, ossia la necessità di eliminare le informazioni, quando possibile, per assicurare i diritti delle persone interessate[13].

[13] http://www.repubblica.it/tecnologia/2014/05/13/news/causa_contro_google_corte_ue_motore_di_ricerca_responsabile_dati-85985943/.

Esempio di incidente	**R**	**I**	**D**
Incendio		x	x
Cartelle esattoriali sbagliate		x	
Blackout			x
Virus blocca i sistemi informatici	x	x	x
Furto disegni industriali	x		
Diffusione documenti	x		
Guasto impianto			x
Modifica scorretta sistema IT	x	x	x
Furto di password da parte di esterni	x	x	x
Modifica non autorizzata di informazioni		x	x
Attacchi di *Denial of Service*			x

Tabella 2.2.1: Esempio eventi e parametri RID

2.3 Organizzazione, processi e funzioni

In conformità con le norme ISO è qui adottato il termine *organizzazione* per indicare ogni forma di impresa, azienda, ente, associazione, agenzia, eccetera.

Altra definizione da segnalare è quella di *business*: molte norme distinguono tra attività di *business*, ossia quelle principali di un'organizzazione, e quelle *di supporto*. In alcuni testi con il termine *business* si intendono le persone non coinvolte nelle attività di gestione dei sistemi informatici.

Questa differenziazione potrebbe invitare a vedere l'informatica come estranea alle altre attività dell'organizzazione e pertanto in questo libro non si utilizza quel termine.

Nel seguito è descritto come si compone un'organizzazione, ossia in processi e funzioni.

2.3.1 I processi

La definizione di *processo* fornita dalla ISO/IEC 27000 è la seguente.

> *Processo:* insieme di attività fra di loro interrelate o interagenti che trasformano elementi in ingresso (*input*) in elementi in uscita (*output*).

Apparentemente banale, nasconde diverse complessità.

Esempio 2.3.1. Si consideri il processo di gestione della formazione del personale. Gli *input* sono le esigenze di formazione e l'*output* è il miglioramento delle competenze delle persone coinvolte.

Ma non è così semplice: gli *input* comprendono anche i costi, il budget, le date in cui tenere il corso, la disponibilità (se il caso) dell'aula, le eventuali offerte e fatture dei fornitori, le giornate in cui il docente e il personale sono disponibili. Tra gli *output* vi sono: la valutazione dei costi rispetto al budget, la scelta del metodo di formazione, le richieste di offerta, gli ordini e i pagamenti ai fornitori, la convocazione al corso, i risultati di eventuali esami.

Le attività sono numerose: raccolta delle esigenze di formazione, verifica dei costi e comparazione con il budget, scelta dei corsi da erogare e delle date, dei partecipanti prescelti e delle sedi, convocazione dei partecipanti, conferma al fornitore, pagamento del fornitore, raccolta ed invio dei risultati degli esami e così via.

Ciascuna di queste attività può essere svolta con diversi strumenti (informatici o non informatici).

Una caratteristica dei processi, implicita nella definizione, è che devono essere *tenuti sotto controllo*, in modo che forniscano gli output previsti e si possano prevenire o rilevare scostamenti da quanto previsto.

Il controllo può essere esercitato quotidianamente dai singoli operatori e dai loro responsabili e periodicamente dal personale addetto alle verifiche o con misurazioni di efficacia ed efficienza, dove, usando la ISO 9000:2015:

Efficacia: grado rispetto al quale le attività pianificate sono realizzate e i risultati pianificati raggiunti.
Efficienza: relazione tra risultati ottenuti e risorse utilizzate.

Esempio 2.3.2. Per misurare il processo di gestione della formazione è possibile elaborare dati sui risultati dei test sostenuti, sui costi e sulla soddisfazione dei responsabili delle persone da formare e dei partecipanti alla formazione.

Ecco quindi di seguito le caratteristiche di ogni processo:

- ogni processo ha degli elementi in ingresso (*input*), provenienti da funzioni interne o entità esterne, come clienti e fornitori;
- per ogni attività del processo sono utilizzati degli strumenti (i moduli e i mezzi di comunicazione per le attività burocratiche; le macchine per le attività manifatturiere; i programmi software per i sistemi informatici);
- per ogni attività sono indicati dei responsabili;
- sono stabilite le modalità per tenere sotto controllo il processo;
- ogni processo ha degli elementi in uscita (*output*) e dei destinatari, ossia funzioni interne o esterne.

È necessario conoscere due termini: si *mappano* i processi così come sono e si *modellano* così come si desidera modificarli.

Nel mapparli o modellarli bisogna evitare di descrivere ogni possibile dettaglio: la vita reale è sempre più complicata di ogni sua possibile descrizione. L'importante è disporre di descrizioni sufficienti per tenere sotto controllo il processo, illustrarlo alle parti interessate (compresi coloro che devono attuarlo) e migliorarlo.

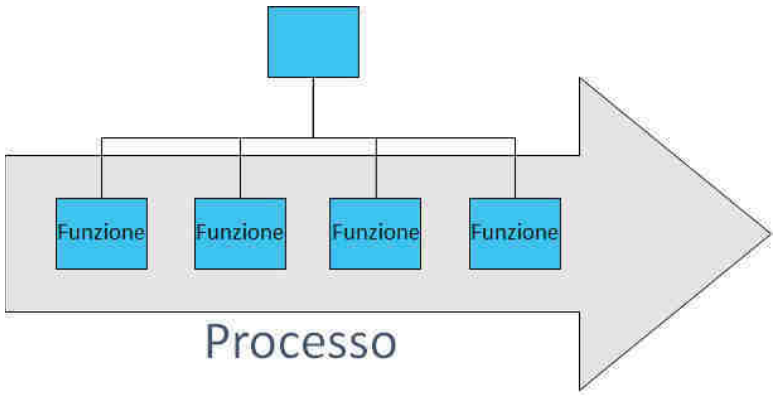

Figura 2.3.1: Processo e funzioni

2.3.2 Le funzioni

Un'organizzazione è strutturata in *funzioni*, ossia gruppi di persone corrispondenti alle caselle degli uffici riportati in un organigramma.

I *processi* descrivono come le funzioni interagiscono tra loro o al loro interno, come schematizzato in figura: 2.3.1.

Le comunicazioni, all'interno delle stesse funzioni o tra funzioni distinte, devono avvenire con modalità concordate.

Esempio 2.3.3. Per il processo di formazione, potrebbero essere coinvolti, oltre al responsabile delle persone da formare, l'ufficio personale, l'amministrazione e l'ufficio acquisti.

Queste *funzioni* possono comunicare tra loro via e-mail, applicazioni informatiche, moduli cartacei o oralmente.

2.4 Processi, prodotti e persone

È stata sottolineata l'importanza dei processi per la realizzazione di un sistema di gestione per la sicurezza delle informazioni, ma questi non sono certamente sufficienti. Sono fondamentali anche le persone e i prodotti.

È infatti necessario avvalersi di persone qualificate, in grado di comprendere e conseguire la sicurezza delle informazioni, attraverso l'applicazione di giusti processi e l'impiego di prodotti idonei. Si parla quindi delle 3 P: processi (o procedure), persone e prodotti. In appendice B è introdotta una quarta P, relativa ai fornitori (partner).

Esempio 2.4.1. Un'auto da corsa data in mano ad un neo-patentato presumibilmente non vincerebbe alcun premio e il pilota metterebbe a repentaglio la sua vita, anche per la scarsa conoscenza delle procedure, inesperienza alla guida e probabile sopravvalutazione delle sue capacità.

Un'auto meno impegnativa, data in mano ad un bravo pilota, otterrebbe quasi certamente risultati superiori, grazie alla maggiore preparazione ed alle migliori conoscenze sia teoriche che pratiche. Solo però una corretta combinazione di auto, pilota (con il suo team di meccanici) e procedure porta a raggiungere i migliori risultati e vincere la gara.

Quale delle tre P è la più importante? Nessuna: tutte devono partecipare in modo bilanciato al conseguimento dell'impresa.

Trattando di sicurezza delle informazioni, l'antivirus è sicuramente un prodotto importante, ma lo sono anche la procedura per tenerlo aggiornato e la persona addetta alla sua installazione e configurazione.

Quando si parla di persone, è sempre opportuno intendere una pluralità di soggetti con compiti differenti. Esattamente come nella Formula Uno, dove ci sono meccanici, ingegneri e persone specializzate, addestrate e controllate anche per cambiare il bullone della ruota ai pit stop. Il mondo della sicurezza delle informazioni è ormai un campo così complicato che non si può parlare di uno, ma di molti specialisti che si occupano di alcuni processi e impiegano più prodotti.

Per esempio sono necessari: lo specialista della gestione sicura delle informazioni, strettamente collegato con il responsabile dei sistemi informativi, dal quale dipendono gli specialisti dei vari apparati di rete, dei server, dei dispositivi personali e dei software applicativi.

Capitolo 3

Sistema di gestione per la sicurezza delle informazioni

Comme de longs échos qui de loin se confondent
Dans une ténébreuse et profonde unité,
Vaste comme la nuit et comme la clarté,
Les parfums, les couleurs et les sons se répondent

Charles Baudelaire, *Correspondances*

La sicurezza delle informazioni si può raggiungere attraverso idonei processi organizzativi. Sono infatti necessari processi per stabilire qual è il livello di sicurezza adeguato, individuare le carenze, decidere come colmarle e con quali prodotti, programmare i tempi e i responsabili delle attività di adeguamento, formare il personale e mantenere le soluzioni adottate.

Esempio 3.0.2. Si consideri il sistema di tornelli per accedere agli uffici. Bisogna stabilire se offre il livello di sicurezza desiderato, quali tecnologie adottare anche considerando le normative vigenti, quale fornitore incaricare dell'installazione, quali contratti stipulare per la manutenzione, come abilitare e disabilitare gli utenti per l'accesso, come agire in caso di guasto.

Non è ovviamente vero l'inverso: buoni prodotti di sicurezza non garantiscono il raggiungimento dei risultati desiderati. Sono numerosi i casi di acquisto di strumenti rimasti inutilizzati perché non integrabili con i sistemi già in uso o perché nessuno ha ricevuto l'adeguata formazione per installarli e mantenerli.

I processi non sono tra loro isolati e indipendenti, ma correlati e interagenti.

Esempio 3.0.3. Tornando all'esempio dei tornelli, si vede facilmente come più processi interagiscano tra loro: di analisi dei rischi per valutare le necessità, di gestione degli acquisti e di formazione.

A tornelli attivi, sono coinvolti ulteriori processi: di controllo degli ac-

cessi, di gestione del personale (per stabilire chi è autorizzato ad accedere), di gestione dei fornitori (per gli addetti alla manutenzione), di gestione degli incidenti (da attivare in caso di guasto o allarme); di verifica periodica dell'adeguatezza dei tornelli.

In questo capitolo si definiscono quindi i *sistemi di gestione* e i *sistemi di gestione per la sicurezza delle informazioni*. Si fanno anche delle considerazioni sulla loro pianificazione e attuazione.

3.1 Sistema di gestione

Come già detto in precedenza, i processi sono tra loro interrelati e interagenti. Può quindi risultare chiara la seguente definizione, fornita dalla ISO/IEC 27000.

> *Sistema di gestione (management system)*: Insieme di elementi interrelati e interagenti di un'organizzazione per stabilire politiche e obiettivi e [insieme di] processi [interrelati e interagenti] per raggiungere tali obiettivi.

La definizione prevede di stabilire politiche, obiettivi e processi e poi fare in modo che gli obiettivi siano raggiunti. Non è quindi previsto che siano date politiche, obiettivi e processi e poi ci si disinteressi del loro funzionamento e della loro realizzabilità.

In sintesi, sacrificando la teoria e tornando alla pratica, possiamo dire che:

- ogni organizzazione ha uno scopo (*missione*);
- il sistema di gestione di un'organizzazione è il suo insieme di pratiche organizzative (processi) e di strumenti atti a raggiungere il suo scopo;
- tali processi e strumenti sono tra loro interrelati;
- ciascun cambiamento organizzativo, anche se potenzialmente piccolo, può avere degli impatti su molte aree dell'organizzazione e sui clienti e fornitori, derivanti delle interrelazioni dei processi;
- quando si operano cambiamenti va prestata attenzione ai loro impatti sin da quando sono pianificati.

3.2 Sistema di gestione per la sicurezza delle informazioni

In un'organizzazione non tutte le attività sono dedicate o coinvolte nella sicurezza delle informazioni. Difatti si ha la seguente definizione dalla ISO 9000:2015.

> *Sistema di gestione per la sicurezza delle informazioni (SGSI):* la parte del sistema di gestione di un'organizzazione che si occupa della sicurezza delle informazioni.

Per indicare il sistema di gestione per la sicurezza delle informazioni si usa spesso il suo acronimo (*SGSI*) o la dicitura inglese *information security management system* (*ISMS*).

Altre parti del sistema di gestione di un'organizzazione possono riguardare: la qualità, l'ambiente, la sicurezza e la salute dei lavoratori.

È importante distinguere gli ambiti di ciascun sistema di gestione, le loro interrelazioni e le loro sovrapposizioni, per evitare di trattare materie estranee ad una disciplina o moltiplicare inutilmente gli sforzi.

Esempio 3.2.1. La sicurezza delle informazioni non si occupa, se non marginalmente, di rischio di credito, di protezione del brand aziendale e della sicurezza fisica e igiene dei lavoratori: sono altre discipline, che richiedono competenze diverse e sono trattate da altri sistemi di gestione.

La prevenzione degli incendi è materia comune alla sicurezza delle informazioni, alla sicurezza fisica e alla sicurezza e salute del personale. Deve quindi essere affrontata in modo da evitare inutili sovrapposizioni e garantire l'adeguamento delle misure intraprese alle esigenze di tutti.

3.3 Le certificazioni relative alla sicurezza delle informazioni

Come essere sicuri che siano stati adottati i processi adeguati, che il personale sia preparato e che i prodotti utilizzati siano affidabili? Occorre effettuare delle valutazioni condotte da un ente "terzo" e indipendente, a sua volta controllato da appositi organismi.

Le valutazioni prevedono la raccolta e l'analisi degli elementi di prova secondo criteri stabiliti, in modo da valutarli obiettivamente e nel rispetto delle norme. Il risultato finale può dare luogo ad una certificazione.

Nell'ambito della sicurezza delle informazioni esistono schemi per la certificazione dei processi (il più importante è quello basato sulla ISO/IEC 27001 di cui si tratta più diffusamente in appendice C), dei prodotti (il più importante è quello basato sulla ISO/IEC 15408, detti anche *Common criteria* e di cui si tratta più diffusamente in appendice D) e delle persone [36].

La certificazione serve a dare una ragionevole fiducia che:

- le decisioni siano prese da persone competenti;
- le persone impieghino prodotti a loro volta verificati e ritenuti affidabili;
- le procedure impiegate siano state a loro volta verificate con esito positivo.

Solo attraverso la misura della fiducia che si può riporre in un prodotto, in una persona o in una procedura, si ha la ragionevole certezza che le cose vadano nella giusta direzione.

Il sistema di certificazione ha anch'esso dei difetti, il primo dei quali è che gli organismi di certificazione sono pagati dalle stesse entità che richiedono la certificazione. Ciò non toglie che questi meccanismi contribuiscano ad una maggiore sicurezza.

Parte II

La gestione del rischio

Capitolo 4

Rischio e valutazione del rischio

I'd call that a bargain
the best I ever had.

Pete Townshened,
Bargain

Nei paragrafi e capitoli seguenti è spiegato cos'è il *rischio* e come valutarlo, in modo da decidere come trattarlo. Le fasi della *valutazione del rischio* (*risk assessment*) sono riportate in figura 4.0.1 e sono:

1. identificazione del rischio,
2. analisi del rischio,
3. ponderazione del rischio.

Queste fasi devono essere precedute da una comprensione del *contesto* e dell'*ambito* in cui si valuta il rischio e seguite dal *trattamento del rischio*. A ciascuna di queste fasi sono dedicati i capitoli da 5 a 9.

Figura 4.0.1: Le fasi della gestione del rischio

L'ultimo capitolo di questa parte si occupa del monitoraggio e della rivalutazione del rischio, attività necessarie perché il rischio venga gestito nel tempo.

4.1 Cos'è il rischio

Per parlare di *valutazione* e *trattamento del rischio*, bisogna innanzitutto definire il *rischio*, utilizzando la ISO/IEC 27000.

> *Rischio*: effetto dell'incertezza sugli obiettivi.

L'incertezza è dovuta a degli *eventi*, che possono avere degli *effetti* o *conseguenze* o *impatti*, negativi o positivi.

Sin da ora è necessario evidenziare che non si può identificare il *rischio reale*, ma solo quello *percepito* e le valutazioni sono sempre soggettive. Le tecniche di identificazione, analisi e ponderazione del rischio non devono quindi avere la pretesa di rappresentare una realtà oggettiva, ma di guidare verso risultati il più possibile completi e pertinenti.

4.1.1 I rischi positivi e negativi

I rischi possono generare effetti negativi, come per esempio:

- danno di immagine a causa di eventi negativi e di dominio pubblico;
- perdita di quote di mercato a causa delle azioni dei concorrenti, incluse quelle di riduzione dei prezzi, innovazione e spionaggio;
- perdita di competitività a causa dell'aumento del costo delle materie prime;
- rallentamenti della produzione a causa della chiusura di un fornitore;
- riduzione della liquidità per difficoltà di recupero crediti verso i clienti;
- costi di adeguamento a nuovi dispositivi normativi;
- perdite economiche a causa di scioperi, atti di sabotaggio o di terrorismo derivanti dal clima sociale e politico;
- perdita di reputazione, di clienti e di liquidità economica a causa della difettosità dei prodotti e dei servizi.

I rischi possono avere impatti positivi. Gli eventi che li generano sono indicati con il termine di *opportunità*. Impatti positivi e relative opportunità possono essere:

- miglioramento dell'immagine per il tempestivo adeguamento a nuovi dispositivi normativi;
- aumento della clientela grazie all'elevata innovazione;
- miglioramento della reputazione e della produttività grazie alla buona gestione del personale.

Alcuni rischi potrebbero essere sia positivi sia negativi. Per esempio:

- un nuovo cliente può avere impatti positivi, soprattutto sul fatturato, oppure impatti negativi se risulta essere un cattivo pagatore (la Pubblica amministrazione italiana è nota per i suoi ritardi nei pagamenti e molte imprese sono fallite per questo[1]);
- un'innovazione o l'apertura di una nuova sede o l'aggiunta di una nuova linea di produzione possono avere impatti positivi se apprezzate dai clienti, oppure impatti negativi se non generano guadagni tali da coprire i costi sostenuti per realizzarle;
- ogni cambiamento e riorganizzazione possono migliorare l'efficacia e l'efficienza dei processi, ma possono anche peggiorarle o scontentare il personale.

La sicurezza delle informazioni si occupa solo dei rischi con effetti negativi, oggetto di questo e dei prossimi capitoli. Delle opportunità relative al sistema di gestione si discuterà nel paragrafo 14.6.

4.1.2 Il livello di rischio

Per comprendere come agire di fronte ad un rischio, è opportuno stabilirne il *livello*, ossia una misura di grandezza. Sempre dalla ISO/IEC 27000 si ha la definizione seguente.

> *Livello di rischio*: grandezza di un rischio espresso come combinazione delle sue conseguenze e della loro verosimiglianza.

Anche intuitivamente:

- più sono elevate le conseguenze (o gli impatti) di un possibile evento, più alto è percepito il rischio;
- più è *verosimile* o *probabile* che si verifichi un evento negativo, più alto è percepito il rischio.

La ISO/IEC 27001 utilizza il termine *verosimiglianza* e non *probabilità* per evitare che venga interpretato come richiesta di calcolare il rischio in termini quantitativi (paragrafo 7.1). In questo libro, per contro, lo si utilizzerà spesso perché ritenuto più intuitivo.

Si consideri, come esempio, nel *contesto* dei viaggi aerei, l'imbarco del bagaglio su un aereo: il rischio relativo al furto è più elevato quanto più gli oggetti nel bagaglio hanno valore e quanto più la compagnia aerea o gli aeroporti dove si transita sono noti per l'elevato numero di furti avvenuti.

Si può rappresentare questa relazione con una formula matematica, dove il rischio r è direttamente proporzionale alla probabilità p di accadimento di un evento e al suo impatto i:

$$r \propto p \cdot i \tag{4.1.1}$$

Quando si imbarca un bagaglio, i rischi non si riducono a quelli collegati al furto, ma anche ad altri, come quelli collegati alla perdita o al ritardo nel riceverlo; in questo caso le probabilità di accadimento e gli impatti saranno

[1] Solo a titolo di esempio, si segnala questo comunicato del 3 aprile 2013: http://www.cgiamestre.com/articoli/12470.

diversi. Quindi, il rischio dipende dall'evento o *minaccia* m e la formula 4.1.1 andrebbe più correttamente riscritta così:

$$r(m) \propto p(m) \cdot i(m) \tag{4.1.2}$$

Più valore ha il bagaglio, più il rischio è elevato e quindi il rischio aumenta se aumenta il *valore* degli oggetti su cui agisce la minaccia. Questi oggetti, la cui definizione ufficiale è al paragrafo 6.1, sono detti *asset* e indicati con la lettera a. Il rischio che il bagaglio sia rubato (minaccia) è direttamente proporzionale alla probabilità del furto $p(m)$ e dall'impatto $i(m, a)$ del furto m sull'asset a. La formula 4.1.2 va quindi riscritta così:

$$r(m, a) \propto p(m) \cdot i(m, a) \tag{4.1.3}$$

Se il bagaglio non ha serratura, è più vulnerabile e il rischio aumenta. Il rischio dipende quindi anche dalle vulnerabilità v e dalla loro gravità $g(v)$. Più le vulnerabilità sono elevate, più il rischio è alto. La formula 4.1.3 può essere quindi scritta anche così:

$$r(m, a, v) \propto p(m) \cdot i(m, a) \cdot g(v) \tag{4.1.4}$$

Se si applicano misure o *controlli di sicurezza* c al bagaglio (per esempio, l'aggiunta di un lucchetto o la stipula di una polizza assicurativa), il rischio relativo al furto diminuisce. Si può vedere la *robustezza* dei controlli di sicurezza $r(c)$ come l'inverso delle vulnerabilità (se il bagaglio è munito di serratura, è meno vulnerabile) e ottenere la seguente formula:

$$r(m, a, c) \propto \frac{p(m) \cdot i(m, a)}{r(c)}. \tag{4.1.5}$$

I controlli possono modificare la probabilità di riuscita di una minaccia (se si usa un lucchetto) o gli impatti conseguenti (per esempio, se si stipula una polizza di assicurazione). Probabilità e impatti sono quindi dipendenti da c e la formula 4.1.4 può essere riscritta così:

$$r(m, a, c) \propto p(m, c) \cdot i(m, a, c) \tag{4.1.6}$$

Sostituendo i controlli c con le vulnerabilità v, si ottiene questa formula:

$$r(m, a, v) \propto p(m, v) \cdot i(m, a, v) \tag{4.1.7}$$

Da quanto detto, è possibile elencare i parametri di valutazione del rischio:

- il *contesto*;
- l'*asset* e il suo *valore*, da cui dipende l'*impatto*;
- la *minaccia* e la sua *verosimiglianza* o *probabilità*;
- le *vulnerabilità* e la loro *gravità* o i *controlli di sicurezza* e la loro *robustezza*.

Il bagaglio può essere rubato o perso, danneggiato o arrivare in ritardo; inoltre, se il bagaglio è composto da più valige, queste minacce possono avere impatti diversi a seconda della valigia coinvolta. Quindi "il" rischio relativo al bagaglio è composto da più rischi "singoli" dovuti alle diverse minacce e ai loro impatti sull'insieme degli asset. È per questo che alcuni usano l'espressione *mappa del rischio*.

Una volta calcolato il livello di rischio, è necessario prendere delle decisioni per affrontarlo o *trattarlo*. Utilizzando ancora l'esempio del furto dei bagagli, le possibili decisioni sono:

- *prevenire* il furto e non imbarcare il bagaglio;
- *ridurre* il potenziale impatto del furto e imbarcare solo parte del bagaglio;
- *evitare* il rischio di furto del bagaglio all'aeroporto e prendere il treno;
- *condividere* il rischio con una compagnia di assicurazioni e stipulare una polizza;
- *accettare* il rischio e imbarcare il bagaglio.

L'accettazione o non accettazione del rischio dipendono dal *livello di accettabilità* stabilito da ciascuno: c'è chi imbarca sempre tutto il bagaglio e c'è chi cerca di portare quanto più bagaglio a mano possibile.

Ciascuna scelta non elimina il rischio, ma ne può introdurre di nuovi: il bagaglio a mano può essere anch'esso rubato, in treno si verificano ugualmente furti di bagagli e la compagnia di assicurazione potrebbe fallire e non pagare quanto dovuto.

Più avanti tutti questi concetti sono descritti compiutamente e in relazione con la sicurezza delle informazioni.

4.2 Cos'è la valutazione del rischio

Prima di tutto, è necessario fornire la definizione ufficiale della ISO/IEC 27000.

> *Valutazione del rischio* (*risk assessment*): processo complessivo di identificazione, analisi e ponderazione del rischio.

In parole più semplici, la valutazione del rischio è un insieme di attività volte a identificare i rischi (ossia gli asset, le minacce e le vulnerabilità), calcolarne il livello e decidere se sono accettabili.

La definizione non riguarda solo la valutazione del rischio per la sicurezza delle informazioni, ma è generale e potrebbe essere applicata anche all'analisi dei rischi strategici, finanziari, sulla sicurezza dei lavoratori, di progetto [97], sulla privacy[2], eccetera.

Nel nostro caso è corretto utilizzare la dicitura *valutazione del rischio relativo alla sicurezza delle informazioni*, anche se spesso, per brevità e quando non ci possono essere confusioni, in questo libro si usa solo la dicitura *valutazione del rischio*.

Bisogna avere chiara la finalità della valutazione del rischio in modo da individuare i metodi adeguati.

[2] http://europrivacy.info/2015/07/21/pia-concept-directive-9546-current-draft-eu-part-1/

Per questo si riporta in figura 4.2.1 la rappresentazione di un'organizzazione attraverso la piramide di Anthony [112] (si osservi che in altri contesti, per esempio militari, i termini hanno significato diverso).

Figura 4.2.1: La piramide di Anthony

- A *livello strategico* sono richiesti dati stimati e approssimati, utili per dare indirizzi con prospettive a lungo termine (qualche anno);
- a *livello tattico* sono richiesti dati consuntivi, arrotondati e abbastanza tempestivi, utili per avere indicazioni sull'andamento delle attività operative e prendere decisioni con prospettive a medio termine (qualche mese);
- a *livello operativo* i dati devono essere esatti e in tempo reale, poiché servono ad effettuare e tenere sotto controllo le attività in corso.

Per realizzare un sistema di gestione per la sicurezza delle informazioni è necessario individuarne gli elementi, in particolare i processi e le loro interrelazioni, e prendere decisioni in merito alle misure di sicurezza da adottare. Questo riguarda i livelli strategici e tattici, che hanno bisogno di dati aggregati e non particolarmente accurati. Parafrasando il principio del rasoio di Occam, per prendere una decisione è inutile avere più dati di quelli strettamente necessari.

Di conseguenza il livello di dettaglio e di approfondimento necessario alla valutazione del rischio deve essere basso, anche quando il valore delle informazioni che si vogliono proteggere è alto: analisi del rischio molto dettagliate forniscono troppi dettagli inutili per prendere delle decisioni a livello strategico e tattico.

Avere la pretesa di descrivere completamente la realtà e identificare nel dettaglio ogni asset, minaccia e vulnerabilità sarebbe un inutile spreco di lavoro: l'identificazione del rischio, per quanto accurata, permetterà solo di avere un modello della realtà, e mai potrà rappresentarla correttamente e in ogni suo dettaglio. Per illustrare questo concetto, Korzybski (anche se in altro contesto) diceva che la mappa non è il territorio e Magritte che il disegno di una pipa non è una pipa.

Esempio 4.2.1. In un'organizzazione, dopo 6 mesi di raccolta di dati molto accurati, il responsabile della sicurezza si accorse che l'organizzazione aveva subito tanti cambiamenti da richiedere una nuova esecuzione del lavoro.

I cambiamenti, peraltro, erano stati condotti senza considerare i rischi relativi alla sicurezza delle informazioni, dimostrando ulteriormente quanto poco utile era stato considerato il lavoro svolto.

Chi vuol fare un "lavoro accurato" confonde la finalità (avere elementi per decidere) con il suo mezzo (avere un'accurata analisi del rischio).

È quindi opportuno iniziare da un'analisi non troppo accurata di livello tattico. Questa potrebbe evidenziare la necessità di analizzare a livello operativo e con maggior dettaglio alcuni sistemi informatici (server, apparati di rete, applicazioni, pc, dispositivi portatili come cellulari e tablet), aree o servizi, per i quali adottare metodi di analisi più accurati. Tra questi metodi vi sono i *vulnerability assessment* (paragrafo 11.15.3) e le *gap analysis* rispetto a delle best practice. Si osservi che questi metodi non sono delle valutazioni del rischio poiché evidenziano solo le vulnerabilità.

Esempio 4.2.2. In una grande organizzazione si era deciso di raccogliere i dati necessari ad identificare il rischio a livello di ciascuna funzione organizzativa. Ciò ha permesso di raccogliere molte informazioni utili, ma si sono rilevate eccessivamente numerose. Inoltre, la diversa sensibilità dei rappresentanti delle funzioni organizzative ha comportato una forte disomogeneità tra i risultati.

L'analisi non ha neanche permesso di rilevare le carenze a livello tattico, come la mancanza di regole per la gestione delle chiavi fisiche, di un approccio comune per l'archiviazione delle informazioni, per l'esecuzione dei backup e dei test di continuità operativa.

Con un altro approccio, adottato in un secondo tempo e più utile, si sono inizialmente individuati i rischi dovuti a carenze nelle regole generali in modo da rendere le procedure adottate da ciascuna entità omogenee alle altre e in linea con il livello di sicurezza desiderato per l'azienda nel suo complesso; successivamente si sono analizzati i rischi delle entità più critiche e relativi alle minacce e vulnerabilità non adeguatamente affrontate nella prima fase; infine si sono analizzate le restanti aree privilegiando il metodo di *gap analysis*, ossia analizzando se in esse erano attuate le misure stabilite per l'insieme dell'organizzazione e intervenendo quando necessario.

Alcuni studi [69] dicono che analisi meno accurate portano a risultati altrettanto significativi di quelle più accurate ma meno ottimistiche e dunque più prudenti, il che non è certamente un male quando si parla di sicurezza.

4.3 I metodi per valutare il rischio

In questo libro viene proposto un approccio "classico" alla valutazione del rischio, basato su asset, minacce e vulnerabilità (o contromisure), come è evidente dalle formule del paragrafo 4.1.2.

Altri propongono metodi apparentemente non allineati a questo approccio. Se però si analizzano attentamente, questi metodi sono sempre riconducibili a quello classico, anche se usano termini diversi (per esempio, *scenari* al posto di *asset* o *aggregazioni di asset*, oppure *eventi* o *scenari di rischio* o *casi di errore* al posto di *minacce*).

Esempio 4.3.1. Molte organizzazioni adottano un approccio basato sull'importanza delle informazioni da cui derivano le scelte per tutelarle, indipendentemente dagli asset in cui sono contenute.

Se si analizza da vicino questo metodo, si osserva che sono analizzate le informazioni (ossia gli *asset*) e le minacce per calcolare il livello di *rischio intrinseco* (paragrafo 7.4) e sono successivamente individuate delle misure di sicurezza da applicare per evitare che vi siano delle vulnerabilità inaccettabili. In altre parole, ancora una volta si valutano *asset*, minacce e contromisure.

Un metodo *valido* di valutazione del rischio deve avere le seguenti caratteristiche:

- *completezza:* devono essere considerati, al giusto livello di sintesi, tutti gli asset, tutte le minacce e tutte le vulnerabilità;
- *ripetibilità:* valutazioni condotte nello stesso contesto e nelle stesse condizioni devono dare gli stessi risultati;
- *comparabilità:* valutazioni condotte in tempi diversi nello stesso contesto devono permettere di comprendere se il rischio è cambiato e come;
- *coerenza:* a fronte di valori di asset, minacce e vulnerabilità più elevati di altri, il livello di rischio deve essere più elevato.

4.3.1 I programmi software per la valutazione del rischio

Si trovano in commercio molti programmi software per effettuare valutazioni del rischio. Essi presentano un percorso guidato per censire gli asset, le minacce e le vulnerabilità, assegnare loro dei valori ed elaborare dei prospetti sul livello di rischio.

Questi programmi possono essere utili in organizzazioni molto grandi perché permettono di organizzare le attività delle persone interessate e di inserire tutti i dati raccolti. Lo sono anche quando le persone coinvolte nella valutazione del rischio (compresi i consulenti) non sono particolarmente esperte e hanno bisogno di uno strumento che li guidi passo dopo passo.

Purtroppo questi programmi hanno dei difetti che è opportuno conoscere.

Il primo difetto consiste nella quantità di dati da inserire: spesso sono moltissimi e richiedono molto tempo. Questo non garantisce affatto risultati precisi, utili o validi.

Esempio 4.3.2. In un'organizzazione erano in corso dei progetti per l'introduzione di tornelli all'ingresso e di bonifica delle utenze di un'applicazione. Nonostante ciò, i risultati della valutazione del rischio evidenziavano solo la scarsa consapevolezza del personale e non problemi relativi all'accesso