Cesare Gallotti

Sicurezza delle informazioni

Gestione del rischio
I sistemi di gestione
La ISO/IEC 27001:2022
I controlli della ISO/IEC 27002:2022

Versione Gennaio 2026

Dedicato, come sempre, a, in ordine di apparizione:
Roberto e Mariangela Gallotti;
Clara;
Chiara e Giulia;
Paola Aurora, Alessio e Riccardo;
Juan Andrés e Yeferson, venuti da lontano
direttamente nel nostro cuore.

Indice

Presentazione

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

Alessandro Manzoni, *I promessi sposi*

La prima versione di questo libro è datata 2002. Nel 2014 scrissi una seconda versione (con i moai dell'Isola di Pasqua in copertina) con 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 erano cambiate, grazie ai tanti audit e progetti di consulenza.

La terza versione del 2017 (con il Perito Moreno in copertina) era un aggiornamento minore, con qualche nuovo esempio e idea nata durante la partecipazione alla scrittura della ISO/IEC 27003:2017. Ne ricavai anche una versione in lingua inglese con il supporto di Maël-Sanh Perrier e, grazie ai suoi suggerimenti, colsi l'occasione per introdurre molti miglioramenti.

La quarta versione (con i Giganti della Sila in copertina) nasceva con la disponibilità delle bozze finali delle ISO/IEC 27001:2022 e ISO/IEC 27002:2022 e dalla necessità di aggiornare la descrizione dei controlli di sicurezza. Colsi l'occasione per inserire ulteriori aggiornamenti sulle tecnologie (citando IoT, OT, intelligenza artificiale, eccetera), sulle minacce e gli accreditamenti. Per l'inglese, mi aiutò Simona Cifarelli, che fece un ottimo lavoro, nonostante il poco tempo che le diedi.

Questa quinta edizione, con le Alpi Giulie in copertina, è un aggiornamento dovuto all'entrata in vigore della NIS2, del Regolamento europeo sull'intelligenza artificiale e alla pubblicazione di nuove edizioni di alcune norme ISO.

La prima parte riporta le basi della sicurezza delle informazioni e dei sistemi 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 le minacce e i controlli di sicurezza. È basata sugli appunti, a loro volta 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 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).

Le successive appendici sulla gestione dei cambiamenti e dei fornitori sono tratte da alcune mie liste di riscontro. L'ultima correla i controlli della ISO/IEC 27002:2022 con i paragrafi di questo libro.

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.

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 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.

Alcune definizioni sono state lievemente modificate da quelle ufficiali per renderle, a mio parere, più comprensibili. Tra parentesi quadre sono riportate eventuali aggiunte. Le cancellazioni sono evidenziate dal simbolo "[...]".

Ringraziamenti

Ci tengo a ringraziare alcune persone per l'aiuto dato nella scrittura di questo libro. Sono molto orgoglioso di essere riuscito a rubare loro tempo e energie. 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 un po' di testo da copiare oltre, per ogni edizione, utili idee;
- 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 avrei voluto 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;
- Monica Perego, la prima idraulica della privacy, bravissima e apprezzatissima da chiunque la conosce (e infatti le vendite aumentano ogni volta che cita questo libro); ho l'onore di considerarla mia amica e di ricevere i suoi suggerimenti per migliorare questo libro.

Ringrazio anche Franco Ruggieri, Pierfrancesco Maistrello, Francesca Lazzaroni e gli Idraulici della privacy, che negli hanno hanno contribuito ad alcune idee che trovate in questo libro.

Per l'edizione del 2026, ringrazio Luca Caldarelli, Matteo Celardo, Marco Gemo e Pierluigi Stefli per avermi segnalato errori che ho corretto e Stephen Hanson per il controllo della versione inglese.

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[1] e la mia newsletter mensile: persone preparate, ma consapevoli che la nostra materia è estremamente mutevole e non esiste nessuno più bravo degli altri.

Contatti

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

[1] blog.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 20 dicembre 2025.

Capitolo 1

Introduzione

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

John Niven, *A volte ritorno*

Da sempre l'uomo sente 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 dell'elenco dei propri clienti e partner, 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 a un grosso meteorite.

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 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 [156]);

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. il ricorso a sempre più numerosi fornitori e l'aumento di relazioni con attori esterni.

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

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 sicurezza delle informazioni (BS 7799 del 1995, di cui si approfondirà la storia nel paragrafo 13.5) e alle metodologie di valutazione del rischio relativo alla sicurezza delle informazioni (CRAMM del 1987, Marion del 1990 e Mehari del 1995) [29].

Negli anni 2000, molti Paesi presero consapevolezza dell'importanza della protezione delle reti informatiche e di Internet (rendendo diffusi i termini *cyberspace* e *cybersecurity*). Inizialmente gli USA promossero iniziative legislative (tra cui il Cybersecurity and Infrastructure Security Agency Act del 2018), avviarono agenzie specializzate (nel 2018 fu creata la Cybersecurity & Infrastructure Security Agency, ma già in precedenza operavano il NIST e l'NSA) e programmi per ridurre i rischi informatici delle infrastrutture critiche (nel 2013 iniziarono i lavori per la pubblicazione del NIST Cybersecurity Framework). Successivamente altri Paesi avviarono iniziative simili; tra di essi l'Unione Europea, che aveva già creato nel 2004 ENISA (European Network and Information Security Agency, oggi European Union Agency for Cybersecurity) e poi approvò la Direttiva NIS del 2018 e il Cybersecurity act del 2019, a cui l'Italia affiancò la normativa relativa al "perimetro di sicurezza nazionale cibernetica" nel 2019.

Dall'altra parte furono considerati come sempre più importanti i diritti dei cittadini nell'ambito digitale. Da questo punto di vista, le iniziative furono avviate principalmente dall'Unione europea, con la Direttiva privacy del 1995, seguita dall'importantissimo GDPR del 2016 (vedere il paragrafo 12.15.1.9), imitato da moltissimi Paesi inclusa la Cina. Ma non solo: la UE avviò nel 2018 il programma "New Deal for Consumers", anche per migliorare ulteriormente le normative già attuate e relative al commercio elettronico e alla protezione dei consumatori in generale, dopo aver segnalato le esigenze di sicurezza informatica

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

in numerose altre normative, inclusa quella relativa alla sicurezza dei dispositivi medici e delle macchine in generale.

Queste normative richiedono solitamente alle organizzazioni di valutare il rischio relativo alla sicurezza delle informazioni e di trattarlo con opportuni controlli di sicurezza. Il risultato è un aumento generale della sicurezza delle informazioni, ma anche, in molti casi, degli oneri burocratici per molte organizzazioni.

Un ulteriore fenomeno si è affermato negli stessi anni e ne comprende altri: *Internet of Things* (IoT), *Operational technology* (OT) e domotica. Si tratta dell'informatizzazione e della connessione a Internet di dispositivi e strumenti, sempre più numerosi, con limitate capacità, ma spesso collegati a reti informatiche complesse, con attive anche connessioni wi-fi. Questi dispositivi sono ormai dappertutto: nelle case e negli uffici con le TV smart e gli elettrodomestici "intelligenti", negli impianti anche necessari per la sicurezza delle persone, negli impianti produttivi, nelle reti di distribuzione di gas, energia elettrica e acqua, nei trasporti e nelle infrastrutture ferroviarie e stradali. L'elenco è ormai infinito e include tecnologie molto diverse tra loro. Per la loro facilità di connessione, i loro costi sempre più ridotti e la diversità di tecnologie sono difficilmente controllabili dalle organizzazioni.

È in questo contesto che si è reso necessario un ulteriore allargamento del perimetro della sicurezza, non solo legata alla sicurezza delle informazioni, ma alla sicurezza di tutti gli strumenti attaccabili con dispositivi informatici, importantissimi per la produttività, ma difficilmente configurabili e, anche se sembra paradossale, facili da compromettere. I potenziali impatti non sono più sulle informazioni, ma sulla sicurezza fisica e la salute delle persone, la qualità e disponibilità delle produzioni nel settore manifatturiero e l'affidabilità di innumerevoli servizi.

Dal 2020, con l'aumento del lavoro remoto, le organizzazioni devono anche occuparsi di questo aspetto, che ha impatti non solo sulla sicurezza delle informazioni da un punto di visto tecnologico, ma sulla stessa gestione del lavoro.

Ulteriore fenomeno in crescita riguarda l'intelligenza artificiale, che va progettata in modo da non compromettere le persone e la proprietà e protetta durante il suo funzionamento, ma che può anche essere usata come strumento di difesa e di attacco.

Negli anni 2020, in Europa sono diventate applicabili numerose normative, sulla scia del GDPR del 2016. Si citano il Data Act, la NIS2, la CER e l'AI Act. A livello italiano sono state ulteriormente promulgate altre normative come quella relativa al PSNC e la Legge 90 del 2024. Le autorità di controllo (in Italia soprattutto il Garante per la protezione dei dati personali e ACN) a loro volta regolamentano e sanzionano alcune volte in modo pasticciato. Gli organismi di standardizzazione continuano a pubblicare standard (uno degli ultimi è la ISO 56001 sull'innovazione, quasi un ossimoro).

Alcuni criticano questo approccio perché blocca l'innovazione; altri lo supportano perché tutela i consumatori e le nazioni. Le organizzazioni, in tutto questo, devono trovare il modo di monitorare le richieste e renderne efficiente e il più possibile utile l'adozione di norme e standard.

Da segnalare che l'ipertrofia normativa ha richiesto, a chi deve adeguarsi e a chi deve verificare, la disponibilità di numerose competenze, spesso mancanti. Questo sta portando ulteriori inefficienze che si spera verranno risolte nel prossimo futuro.

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 2007 alcuni disegni della F2007 della Ferrari entrarono in possesso della sua concorrente McLaren[4];
- 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[5];

[1] http://it.wikipedia.org/wiki/Biblioteca_di_Alessandria.
[2] https://contribuenti.it/cartelle-pazze.
[3] www.repubblica.it/2003/i/sezioni/cronaca/blackitalia/blackitalia/blackitalia.html.
[4] news.bbc.co.uk/sport2/hi/motorsport/formula_one/6994416.stm.
[5] www.theguardian.com/uk/2009/apr/09/bob-quick-terror-raids-leak.

- a settembre 2013, i *social network* di Alpitour furono violati e alcuni link modificati per indirizzare a siti web malevoli[6];
- a inizio 2013, i servizi di antispamming della Spamhaus furono bloccati da un attacco[7];
- a fine 2019, un'organizzazione, a causa di un colpo di vento, si vide volare numerosi documenti cartacei per strada[8];
- nel maggio 2020, EasyJet fu attaccata da malintenzionati che rubarono i dati dei passeggeri, inclusi numeri di carte di credito[9];
- nel marzo 2021, il data centre di OVH a Strasburgo andò a fuoco e molti sistemi rimasero indisponibili[10];
- nell'agosto 2021, i sistemi informatici per la prenotazione delle vaccinazioni COVID-19 della Regione Lazio rimasero indisponibili per quattro giorni a causa di un ransomware[11];
- a ottobre 2021 Facebook, WhatsApp e Instagram rimasero rimasti bloccati per 6 ore a causa di un errore di configurazione[12].

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 [121].

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

Le informazioni sono archiviate e trasmesse su *supporti*. Essi possono essere *analogici* o *non digitali* come la carta, le fotografie e 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.

[6] www.pierotaglia.net/facebook-fai-da-te-alpitour-ahi-ahi-ahi-pagine-facebook-hackerate.
[7] www.theregister.co.uk/2013/03/27/spamhaus_ddos_megaflood.
[8] https://www.key4biz.it/idiot-wind-bob-dylan-puo-aiutare-nella-valutazione-del-rischio-aziendale/307656/.
[9] https://www.bbc.com/news/technology-52722626.
[10] https://www.wired.it/internet/web/2021/03/10/incendio-data-center-ovh-strasburgo/.
[11] https://www.cybersecurity360.it/nuove-minacce/regione-lazio-vaccini-bloccati-poco-pronta-contro-il-ranwomare-ecco-perche/.
[12] https://www.corriere.it/esteri/21_ottobre_05/facebook-instagram-whatsapp-down-costa-zuckerberg-6-miliardi-dollari-d6f5c632-2586-11ec-9c26-509de9bc1f2d.shtml.

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 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, i *dati* sono elementi o numeri grezzi, simboli o fatti che acquistano significato solo quando sono elaborati o interpretati. Le *informazioni* sono dati in un contesto, organizzati in modo da dare loro importanza e valore.

Questa distinzione si ritrova anche nelle quattro tipologie di rappresentazione della conoscenza [110]:

- *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 [86] 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.

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" [30]. È evidente che questo approccio non considera la disponibilità delle informazioni.

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 2.2.1. 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 a 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 2.2.2. 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.

Alcuni preferiscono usare il termine *confidenzialità* perché il termine *riservatezza* potrebbe essere confuso con quello delle classifiche di segretezza nell'ambito della sicurezza dello Stato; da notare che altri, per esempio nei Paesi anglosassoni, sono meno precisi, visto che usano sempre il termine "confidential", sia nell'ambito delle classifiche di segretezza, sia in altri contesti.

2.2.2 Integrità

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

Esempio 2.2.3. 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 2.2.4. 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.

La disponibilità può avere impatti sulla riservatezza o l'integrità. È compito della Direzione stabilire a quali parametri dare maggiore importanza e comunicare questa scelta nella politica di sicurezza delle informazioni (paragrafo 12.2).

Esempio 2.2.5. I backup migliorano la disponibilità dei dati, ma aumentano i rischi di perdita di riservatezza a causa della duplicazione dei dati e della possibilità che possano essere rubati.

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, tracciabilità e la possibilità di assicurare il diritto all'oblio.

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

La proprietà di *completezza* di un'informazione richiede che non abbia carenze. Una carenza è equivalente a 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.

La *tracciabilità* , che fornisce prove di responsabilità o, in inglese, *accountability*, è la possibilità di sapere chi ha o avuto accesso a un'informazione e chi l'ha modificata. È possibile osservare che i dati necessari per tracciare l'informazione devono far parte dell'informazione stessa e quindi anche la tracciabilità può essere visto come caso particolare di quello di integrità,

La normativa in materia di privacy ha evidenziato il *diritto alla cancellazione*, diventato noto come *diritto all'oblio*. Questo prevede che le informazioni relative a una persona fisica siano eliminate quando dichiarato in fase di raccolta dei dati o, in certe condizioni, e se non in contrasto con la normativa vigente, quando richiesto dalla persona stessa. La necessità di soddisfare questa proprietà richiede di predisporre archivi e sistemi informatici in modo da soddisfare le richieste[13].

2.2.5 Gli impatti sui parametri RID

Ciascun evento può avere impatti su uno o più parametri RID.

Esempio 2.2.6. Possiamo considerare alcuni eventi riportati 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: in caso di furto delle password, come accadde alla Sony nel 2011[14], 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 dovette 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.

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 Sicurezza informatica e cybersecurity

Si parla di *sicurezza informatica* quando ci si limita alla sicurezza delle informazioni sui sistemi informatici. A rigore, alcuni sistemi informatici (per

[13] https://www.garanteprivacy.it/i-miei-diritti/diritti/oblio.
[14] attrition.org/security/rant/sony_aka_sownage.html.

esempio quelli industriali) potrebbero non essere considerati come pertinenti le informazioni.

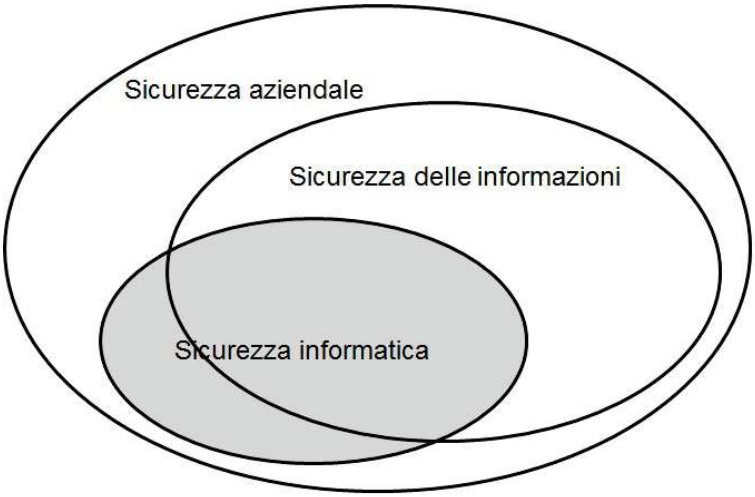

Figura 2.3.1: Sicurezza delle informazioni e sicurezza informatica

Esempio 2.3.1. Nel 2016 alcuni appartamenti in Finlandia rimasero senza acqua calda per una settimana perché il sistema di riscaldamento fu oggetto di attacco informatico[15].

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

Esempio 2.3.2. Nel 2021 uno sconosciuto riuscì ad accedere ai sistemi informatici di un impianto di trattamento dell'acqua in Florida (USA) e modificò alcuni dosaggi[16].

Alcuni classificano questo attacco come relativo agli impianti industriali e non alle informazioni.

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

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

[16] https://www.zdnet.com/article/following-oldsmar-attack-fbi-warns-about-using-teamviewer-and-windows-7/

o rigorosa e, anzi, creando confusione e false aspettative. È importante capire il punto chiave della questione: sicuramente la *cybersecurity* riguarda sistemi informatici, ma non solo quelli che trattano informazioni vere e proprie (ossia documenti e tabelle), bensì anche parametri di configurazione, comunque essenziali per il funzionamento di molte infrastrutture come reti di distribuzione di gas ed elettricità, impianti di riscaldamento e raffreddamento, sistemi industriali e domotici, eccetera.

Una buona definizione è la seguente[17]:

> *cybersecurity*: la capacità di rendere sicuri gli oggetti vulnerabili attraverso l'informatica.

Questo esclude dalla cybersecurity la sicurezza fisica e ambientale dei sistemi informatici.

La definizione del NIST, che è l'ente che ha reso popolare il termine con il suo *Cybersecurity framework* o CSF [115], è troppo generica: "Il processo di protezione delle informazioni attraverso la prevenzione, rilevazione e risposta agli attacchi". Va anche detto che le misure di sicurezza proposte dal CSF sono normali misure di sicurezza informatica.

La cybersecurity include la sicurezza di:

- *Internet of things* (IoT), inclusi i dispositivi usati in ambito industriale (*Industrial IoT* o IIoT) e domotico;
- *Operational technology*, che a sua volta include i sistemi industriali (*industrial control systems* o ICS), che a loro volta includono le reti *supervisory control and data acquisition* (SCADA) che controllano le reti di distribuzione di gas, elettricità, acqua, eccetera;
- sistemi di domotica.

In questi ambiti si usa preferibilmente il termine *resilienza*, per molti versi simile a quello di *disponibilità*, però meno legato alle informazioni in senso stretto.

C'è anche chi usa il termine *cybersecurity* 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 e non riflettendo sul fatto che in inglese non si usa l'espressione *cybernetics security*.

Con il DL 82 del 2021, convertito con la Legge 109 del 2021, è stata fornita una definizione italiana alla *cybersicurezza*: "l'insieme delle attività necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico".

Qui è chiaro che si limita la materia alla sicurezza dei sistemi informatici, escludendo le informazioni su altri supporti e includendo sistemi che non trattano propriamente informazioni, ma solo parametri di configurazione, comunque essenziali per il funzionamento di molte infrastrutture: reti di distribuzione di gas ed elettricità, impianti di riscaldamento e raffreddamento, sistemi industriali e domotici, eccetera.

[17] https://www.cisoplatform.com/profiles/blogs/understanding-difference-between-cyber-security-information.

2.4 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.

2.4.1 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 trasforma elementi in ingresso (*input*) in elementi in uscita (*output*).

Apparentemente banale, nasconde diverse complessità.

Esempio 2.4.1. 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 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 degli 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 al fornitore, raccolta e 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 [74]:

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

Esempio 2.4.2. 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 elementi in ingresso (*input*), provenienti da funzioni interne o entità esterne, come clienti, fornitori e partner;
- per ogni attività del processo sono utilizzati strumenti (i moduli e i mezzi di comunicazione per le attività burocratiche; le macchine e gli impianti per le attività manifatturiere; i programmi software per i sistemi informatici);
- per ogni attività sono indicati i responsabili e gli esecutori;
- sono stabilite le modalità per tenere sotto controllo il processo;
- ogni processo ha elementi in uscita (*output*) e 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.

2.4.2 Le funzioni

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

I *processi* descrivono come le funzioni interagiscono tra loro o al loro interno, come schematizzato in figura 2.4.1.

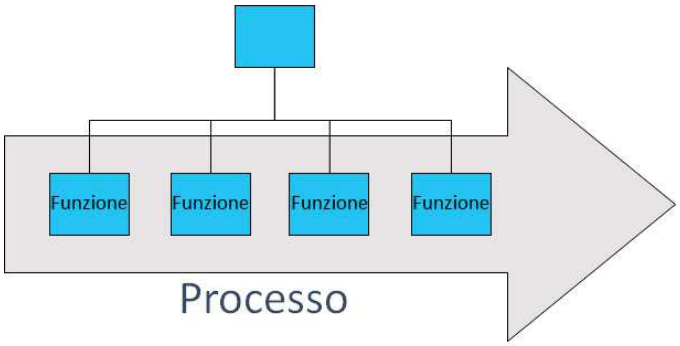

Figura 2.4.1: Processo e funzioni

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

Esempio 2.4.3. 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.

2.5 Processi, prodotti e persone

La sicurezza delle informazioni non dipende solo dalla tecnologia, ma anche da processi, prodotti e persone. Processi ben definiti guidano i comportamenti, appropriati prodotti supportano i processi e persone competenti assicurano che questi siano efficaci. Vanno anche coinvolti fornitori qualificati. Si parla quindi delle 4 P: processi (o procedure), persone, prodotti e partner.

Esempio 2.5.1. Un'auto da corsa data in mano a 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 a un bravo pilota, otterrebbe quasi certamente risultati superiori, grazie alla maggiore preparazione e 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.

Nessuna delle quattro P è la più importante: 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, la persona addetta alla sua installazione e configurazione e il fornitore che ne garantisce il supporto.

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 e fornitori.

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 3.0.1. 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 3.0.2. Tornando all'esempio dei tornelli, si vede facilmente come più processi interagiscano tra loro: analisi dei rischi per valutare le necessità, gestione degli acquisti e formazione.

A tornelli attivi, sono coinvolti ulteriori processi: controllo degli accessi,

gestione del personale (per stabilire chi è autorizzato ad accedere), gestione dei fornitori (per gli addetti alla manutenzione), gestione degli incidenti (da attivare in caso di guasto o allarme); 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 o interagenti di un'organizzazione per stabilire politiche e obiettivi e processi [a loro volta interrelati o 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 impatti su molte aree dell'organizzazione e sui clienti, fornitori e partner, 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 deriva la seguente definizione dalla ISO 9000.

> *Sistema di gestione per la sicurezza delle informazioni (SGSI):* parte di un sistema di gestione che riguarda la 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 a 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, alla protezione dell'ambiente 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.

Per un SGSI è importantissimo il ruolo della Direzione, che ne è la proprietaria. La Direzione deve dimostrare impegno nell'attuazione del SGSI, usarlo come strumento per controllarne gli elementi interrelati e interagenti e assicurare che sia efficace (ossia che soddisfi gli obiettivi di sicurezza delle informazioni).

3.3 Le certificazioni

Come essere sicuri che siano stati adottati i processi adeguati, che il personale sia preparato e che i prodotti e servizi 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 a 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 [87] di cui si tratta più diffusamente in appendice C), dei prodotti (il più importante è quello basato sulla ISO/IEC 15408 [76, 77, 78], detti anche *Common criteria*, dei servizi e delle persone [58, 159].

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 o i processi siano stati a loro volta verificati con esito positivo.

Solo attraverso la misura della fiducia che si può riporre in un prodotto, in un servizio, in una persona o in un processo, 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 a 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 Townshend (The Who),
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* e dal suo monitoraggio. L'insieme di queste fasi costituisce la *gestione 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.
>
> Note: I rischi sono spesso riferiti come eventi potenziali e conseguenze o una loro combinazione.

Il rischio non è necessariamente negativo perché può essere originato da minacce e opportunità.

Nella sicurezza delle informazioni, i rischi riguardano la possibilità che la riservatezza, l'integrità o la disponibilità siano compromesse. Comprendere questi rischi aiuta le organizzazioni a determinare i controlli appropriati.

L'incertezza è dovuta ad *eventi*, che possono avere *effetti* negativi o positivi.

Gli effetti immediati, corrispondenti ai costi diretti, sono detti *impatti*) e saranno approfonditi più avanti (paragrafo 7.2.1); quelli a breve, medio e lungo termine sono detti *conseguenze*. Nella valutazione del rischio si preferisce valutare le conseguenze. Esse possono essere positive o negative.

Sin da ora è necessario chiarire 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, pertinenti e riferibili.

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 o di liquidità economica a causa della difettosità dei prodotti e dei servizi.

I rischi possono avere conseguenze positive. Gli eventi che li generano sono indicati con il termine di *opportunità*. Conseguenze positive 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 conseguenze positive, soprattutto sul fatturato, oppure conseguenze negative 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 conseguenze positive se apprezzate dai clienti, oppure conseguenze negative 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 15.6.

4.1.2 Il livello di rischio

Per comprendere come agire di fronte a 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 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.

L'assegnazione di livelli di rischio permette di scegliere le azioni di trattamento appropriate e assegnare loro la corretta priorità.

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.

[1] https://www.money.it/imprese-fallite-stato-non-paga-crediti-commerciali.

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 alle sue conseguenze i (si osservi che tradizionalmente si usa la i di *impatti*):

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

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 le conseguenze saranno diverse. 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 alla conseguenza $i(m, a)$ 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 le conseguenze (per esempio, se si stipula una polizza di assicurazione). Probabilità e conseguenze sono quindi dipendenti da c e la formula 4.1.3 può essere riscritta così:

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

Un controllo carente rappresenta una vulnerabilità. Per questo si possono sostituire 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 dipendono le *conseguenze*;
- 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 conseguenze diverse a seconda della valigia coinvolta. Quindi "il" rischio relativo al bagaglio è composto da più rischi "singoli" dovuti alle diverse minacce e alle loro conseguenze 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 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* le potenziali conseguenze del furto e imbarcare solo parte del bagaglio;
- *evitare* il rischio di furto del bagaglio all'aeroporto e prendere il treno;
- *eliminare* il rischio e viaggiare senza bagaglio (ipotesi molto difficile da realizzare);
- *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 alla 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 finalità di una valutazione del rischio è capire dove l'organizzazione è esposta e determinare quali rischi richiedono di essere mitigati. Fornisce un approccio strutturato per prendere le corrette decisioni e supporta la conformità, la resilienza operativa e un'efficace allocazione di risorse.

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 [134], sulla privacy, 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.

Per questo si riporta in figura 4.2.1 la rappresentazione di un'organizzazione attraverso la piramide di Anthony [152] (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 a 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. Per esempio, è necessario valutare il rischio per identificare: come strutturare i processi di sicurezza delle informazioni, gli impegni da richiedere al personale, le modalità di uso delle utenze privilegiate e il livello di robustezza delle credenziali, quali trasmissioni cifrare, quali canali di comunicazione usare in caso di emergenze, eventuali software per cui non è necessario condurre test preventivi, le modalità con cui conservare i log.

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 per la valutazione del rischio, 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, *smartphone* e tablet), aree o servizi, per i quali adottare metodi di analisi più accurati. Tra questi metodi vi sono i *vulnerability assessment* (paragrafo 12.15.4) e le *gap analysis* rispetto a *best practice*. Si osservi che questi metodi non sono valutazioni del rischio poiché evidenziano solo vulnerabilità.

Esempio 4.2.2. In una grande organizzazione si decise di raccogliere i dati necessari a identificare il rischio di ciascuna funzione organizzativa. Ciò permise di raccogliere molte informazioni utili, ma si rivelarono eccessivamente numerose. Inoltre, la diversa sensibilità dei rappresentanti delle

funzioni organizzative comportò una forte disomogeneità tra i risultati.

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

Con un altro approccio, adottato in un secondo tempo e più utile, si individuarono inizialmente 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 analizzarono i rischi delle entità più critiche e relativi alle minacce e vulnerabilità non adeguatamente affrontate nella prima fase; infine si analizzarono 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 [103] 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.

Altri tipi di valutazione del rischio, richiesti anche da alcuni riferimenti autorevoli, richiedono un approccio più operativo, diverso da quello esposto in questa parte del libro. Per esempio:

- per valutare il rischio delle vulnerabilità tecnologiche identificate puntualmente con un *vulnerability assessment* o dalle segnalazioni della *threat intelligence*, è necessario valutarne la possibilità che vengano sfruttate, e quindi la verosimiglianza e le conseguenze di un attacco riuscito, per ottenere un livello di rischio e l'urgenza di applicazione degli aggiornamenti, delle patch o dei workaround;

- per valutare il rischio relativo all'approvvigionamento, va identificata la criticità delle singole forniture e i possibili eventi negativi che possono impattarle, per identificare le caratteristiche che devono avere i fornitori, le condizioni contrattuali da imporre e le verifiche iniziali e periodiche ai fornitori e alle forniture.

4.3 I metodi per valutare il rischio

In questo libro viene proposto un approccio alla valutazione del rischio, basato su asset, minacce e vulnerabilità (o contromisure), come è evidente dalle formule del paragrafo 4.1.2. Questo è comune a molti approcci (per esempio Octave [5] e Mehari[2]).

Questo perché è comodo didatticamente e richiesto, anche se obsoleto, da alcuni enti di controllo.

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*) e punti di partenza diversi: il metodo classico parte dagli asset per individuare le minacce e le vulnerabilità, mentre il metodo "basato

[2] https://clusif.fr/services/management-des-risques/.

sugli eventi"parte dalle minacce per poi individuare gli asset che potrebbero danneggiare.

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 vulnerabilità inaccettabili. In altre parole, ancora una volta si valutano *asset*, minacce e contromisure.

Il metodo classico nella sua forma più pura, che porta ad analizzare il rischio per ciascun asset, è peculiare della sicurezza delle informazioni ed è in uso, almeno, dalla fine degli anni Ottanta, quando la sicurezza delle informazioni era decisamente diversa da quella attuale. Per questo motivo qui non se ne raccomanda l'adozione.

In questo libro viene presentato un metodo simile a quello classico, che però prevede una valutazione quasi indipendente di asset e minacce.

Oggi, per una valutazione del rischio a livello strategico e tattico, e considerando che le organizzazioni tendono a gestire i sistemi informatici e i processi centralmente, può essere utile considerare l'organizzazione come un unico asset. A questo approccio va sempre affiancata, a livello operativo, una conoscenza di dettaglio dell'infrastruttura informatica e degli strumenti usati per gestirla, come illustrato nel seguito.

4.3.1 Validità dell'approccio

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.

L'approccio dovrebbe quindi essere abbastanza semplice per essere utilizzato efficacemente e abbastanza robuto per supportare conclusioni significative.

4.3.2 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, di inserire tutti i dati raccolti. Sono utili 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 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 due progetti: uno di introduzione di tornelli all'ingresso e uno di riesame e aggiornamento 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 alla sede o alle utenze.

La valutazione del rischio era stata condotta raccogliendo molti dati precisi, come richiesto dal programma prescelto, e aveva richiesto alcuni mesi di lavoro. Nonostante ciò, evidentemente, non era riuscita a fornire risultati utili a giustificare i progetti avviati.

Il secondo difetto, comune a molti prodotti, consiste nella segretezza dell'algoritmo di calcolo. In questo modo, a fronte di risultati non accettabili, non ne è possibile comprendere l'origine per correggerla o per convincersi della validità dei risultati.

Il terzo difetto consiste nella configurazione iniziale del prodotto. Spesso i questionari e le misure di sicurezza sono impostati considerando un'organizzazione "tipo". Il più famoso software per la valutazione del rischio, ossia il CRAMM, negli anni Novanta era parametrizzato secondo le medie imprese commerciali inglesi (infatti i questionari riportano le Sterline); molti altri sono configurati considerando organizzazioni grandi o grandissime. Spesso la configurazione è inadeguata al contesto in cui si vuole valutare il rischio.

Il quarto difetto è la difficoltà di riconfigurazione di questi strumenti. Questo si verifica in particolare quando si vogliono modificare i parametri di riferimento o aggiungere nuove minacce o nuove vulnerabilità.

Esempio 4.3.3. In molte banche si effettuano valutazioni del rischio relativo all'*Internet banking*. Molto spesso la minaccia di *phishing* non è prevista dai prodotti commerciali e, per quanto sia importantissima nel contesto di riferimento, non può essere censita a causa delle rigidità del prodotto usato per la valutazione del rischio.

Il quinto difetto è che gli utilizzatori di un software commerciale tendono ad adottarlo in modo meccanico, quando invece dovrebbero adattare il metodo al proprio contesto. Gli strumenti non dovrebbero sostituire le analisi professionali e il valore della valutazione del rischio risiede nella discussione, nella comprensione reciproca e nelle decisioni informate.

Ulteriore difetto, soprattutto dei software "per la compliance" (GRC, *Governance, risk and compliance*, sempre più diffusi dagli anni Duemilaventi, è che spesso si riducono alla compilazione di liste di controlli di sicurezza.

È evidente quanto un programma software possa essere utile per raccogliere i dati ed effettuare i calcoli necessari. Un foglio di calcolo può essere sufficiente ed essere configurato facilmente secondo le necessità.

4.3.3 Avvertenza

Quanto segue si basa su teorie consolidate nel tempo in merito all'analisi del rischio, non sempre relativo alla sicurezza delle informazioni. Infatti gli approcci più diffusi e propagandati in materia di valutazione del rischio relativo alla sicurezza delle informazioni prevedono analisi molto accurate e di dettaglio, preferibilmente aiutate da software commerciali venduti da consulenti-venditori.

Per quanto riguarda le metodologie qualitative presentate nel seguito, alcune delle idee sono state tratte dall'esperienza maturata facendo uso di un semplice foglio di calcolo disponibile liberamente sul web [56, 57].

Ciò non ostante si raccomanda lo studio di diversi metodi per poi decidere quale utilizzare o svilupparne uno nuovo, adeguato alle proprie necessità. Sono disponibili alcuni cataloghi di metodi in pubblicazioni [97, 46]. Alcuni di questi metodi non sono relativi alla sicurezza delle informazioni, ma possono fornire idee utili a chi voglia approfondire l'argomento e sviluppare nuove soluzioni. Quelli relativi alla sicurezza delle informazioni presentano tutti i passi descritti in questo libro, anche se talvolta utilizzano termini alternativi, aggregano alcune fasi o propongono algoritmi di calcolo diversi.

Esempio 4.3.4. Un esempio di metodo alternativo ("basato sugli eventi") si basa sulla variante della *fault tree analysis* e prevede di analizzare le minacce e le loro conseguenze senza apparentemente identificare gli *asset* nel dettaglio.

Nella realtà, per identificare le minacce è necessario sapere quali elementi (asset) possono sfruttare (un'intrusione ai sistemi informatici può avvenire attraverso una wi-fi pubblica, un'applicazione web, una rete informatica esposta su Internet) e quali controlli di sicurezza, necessariamente collegati a degli *asset*, la contrastano.

Le valutazioni del rischio possono diventare burocratiche se sono troppo complesse o non considerano le attività operative. Le organizzazioni dovrebbero evitare un livello di dettaglio eccessivo perché rende difficile prendere decisioni. È opportuno ricercare la chiarezza e la praticità.

4.4 Chi coinvolgere

Una valutazione del rischio significativa richiede la partecipazione di quanti permettono di comprendere le attività, i sistemi e il contesto dell'organizzazione. Tutte le parti interessate dovrebbero quindi essere coinvolte nella valutazione del rischio: personale interno, inclusi i responsabili di funzione, clienti, fornitori e partner.

Nei capitoli successivi sono indicate altre figure da coinvolgere.

Ovviamente a ciascuno deve essere comunicato solo quanto necessario affinché possa contribuire alle diverse fasi.

Il coinvolgimento del personale, dei clienti, dei fornitori e partner può essere utile a:

- identificare il rischio (ossia gli asset, le minacce e le vulnerabilità);
- valutare il rischio, grazie alla condivisione del loro punto di vista e delle loro percezioni;
- ponderare il rischio;
- stabilire il piano di trattamento del rischio, perché devono contribuire alla pianificazione e attuazione delle azioni;
- ridurre le incomprensioni in merito alle azioni da attuare;
- ridurre le resistenze al cambiamento;
- avere conseguenze positive sull'immagine dell'organizzazione percepita dai propri clienti, fornitori e partner e dal personale.

Quando si coinvolgono le persone, è necessario prestare attenzione all'*effetto Dunning-Kruger*, per cui individui poco esperti e poco competenti in un campo tendono a sovrastimare la propria preparazione giudicandola, a torto, superiore alla media. Da aggiungere anche quanto riguarda individui esperti in un campo [65]: "La competenza in un campo non si estende in altri campi. Ma spesso gli esperti la pensano così. Più il loro campo di competenza è ristretto, e più è probabile che la pensino così".

Da prestare attenzione anche al *argumentum ad vercundiam* (appello alla modestia), ossia all'accettazione di un'opinione perché proposta da un esperto, anche se di altro campo, come se la sua conoscenza si estendesse in altri ambiti della conoscenza.

I successivi paragrafi riguardano due ruoli particolari (i proprietari del rischio e i facilitatori), che meritano un approfondimento e sono richiamati nel seguito.

4.4.1 I responsabili del rischio

Una figura richiesta dalla ISO/IEC 27001 è quella di *responsabile del rischio*, la cui definizione è fornita dalla ISO/IEC 27000.

> *Responsabile del rischio* (*risk owner*): persona o entità con la responsabilità e con il potere per gestire un rischio.

In altre parole, i responsabili del rischio assicurano che siano definiti, implementati e monitorati gli appropriati controlli.

Il termine "responsabile del rischio"è usato dalla ISO/IEC 27001 per allineamento alla ISO 31000, che non usa il termine "Direzione". Il ruolo di responsabile del rischio, poiché deve avere potere di spesa, coincide spesso con quello della Direzione (paragrafo 12.3.1.1). Essa può delegare altre funzioni affinché facciano delle proposte in merito alla gestione del rischio e alle spese corrispondenti e coordinino le attività relative. La Direzione è sempre e comunque il responsabile ultimo del rischio.

In tutti i casi, i responsabili del rischio devono essere individuati a un livello gerarchico con adeguati poteri decisionali e di spesa, poiché devono decidere quali controlli di sicurezza attuare e mantenere.

Se le informazioni sono conservate, archiviate, comunicate o elaborate da fornitori, outsourcer o da altre entità, il responsabile del rischio deve essere comunque una persona interna all'organizzazione e può coincidere con il referente dei rapporti con queste entità esterne.

Se un rischio riguarda più aree dell'organizzazione, occorre stabilire come concordare le decisioni pertinenti, oppure se attribuire la responsabilità a un livello gerarchico superiore comune.

4.4.2 I facilitatori

I *facilitatori* guidano il processo, conducono gli incontri tra le parti interessate e assicurano che le discussioni rimangano strutturate, obiettive e allineate con l'approccio scelto. Essi aiutano a chiarire i termini usati e i presupposti. Alcuni approcci [5] invitano espliciamente ad avvalersi di facilitatori per coordinare le diverse attività di descrizione del contesto, individuazione dell'ambito, identificazione, analisi, ponderazione e trattamento del rischio.

Spesso questo ruolo è ricoperto da uno o più consulenti esterni. Persone interne, con adeguate competenze, potrebbero ricoprirlo validamente, favoriti anche dalla più precisa conoscenza dell'organizzazione.

4.5 I documenti di gestione del rischio

Per la gestione del rischio, come si vedrà nel seguito, sono prodotti alcuni documenti. Questi documenti forniscono elementi per gli audit, supportano le decisioni e favoriscono il miglioramento continuo.

Alcuni di essi riportano anche carenze e vulnerabilità e pertanto vanno mantenuti riservati. Si deve anche ricordare che questi documenti possono essere scambiati tra più persone.

Vanno quindi applicati opportuni controlli di sicurezza, soprattutto di controllo degli accessi (paragrafo 12.6) e sugli scambi di informazioni (paragrafo 12.10.4).

Capitolo 5

Il contesto e l'ambito

JAQUES. All the world's a stage,
And all the men and women merely players.

William Shakespeare, *As you like it*, Atto II, Scena VII.

In questo capitolo si descrivono le fasi preliminari alla valutazione del rischio. Queste prevedono un'analisi del contesto in cui si vuole operare in modo da decidere in quale ambito valutare il rischio.

Si potrà decidere di valutare il rischio per tutta l'organizzazione, di estendere l'attività anche a parti esterne o di ridurla a un perimetro più limitato (per esempio, ai soli servizi offerti ai clienti).

5.1 Il contesto

La definizione della ISO 9000:2015 fornisce una prima indicazione.

> *Contesto di un'organizzazione*: combinazione di fattori interni ed esterni che possono avere degli effetti sullo sviluppo e raggiungimento degli obiettivi di un'organizzazione.

Comprendere il contesto organizzativo è essenziale per stabilire un sistema di gestione per la sicurezza delle informazioni efficace perché permette di stabilire obiettivi e controlli adeguati, proporzionati e allineati alle necessità dell'organizzazione.

È utile presentare l'elenco degli elementi da includere nella descrizione del contesto [96]. Questi elementi si dividono in *fattori* (*issues*) *interni* ed *esterni*. Tra i fattori interni vi sono:

- le strategie attuali e future e le relative priorità;
- il livello di innovazione, attuale e prevista;
- le caratteristiche delle attività principali svolte in termini di servizi e prodotti offerti e le modifiche previste al portafoglio dei prodotti e servizi offerti;

- la struttura organizzativa, inclusi i fornitori principali e i processi affidati all'esterno (in *outsourcing* o *esternalizzati*);
- le caratteristiche delle sedi;
- le tipologie di informazioni trattate;
- le caratteristiche principali del sistema informativo dell'organizzazione, tra cui:
  - i principali servizi informatici e le relative tecnologie infrastrutturali e applicative;
  - il tipo di dispositivi portatili in uso, se presenti, tra cui cellulari, *smartphone* e tablet;
  - gli archivi non informatici come quelli cartacei;
  - i luoghi dove sono collocati i sistemi informatici e gli archivi non informatici, inclusi quelli gestiti da fornitori;
  - quali sistemi informatici sono *condivisi* con altre entità (clienti, fornitori, partner e altri soggetti esterni) e chi ne ha la proprietà (un'organizzazione può usare alcuni sistemi dei clienti, fornitori o partner per comunicare con loro);
- i rapporti con il personale interno (indipendentemente dalla tipologia di contratto tra le parti) e le loro competenze informatiche;
- le aspettative delle parti interne interessate (vedere 5.2).

Tra i fattori esterni che potrebbero avere impatti sulla sicurezza delle informazioni vi sono:

- i concorrenti e i potenziali concorrenti;
- la normativa applicabile e se ne sono previste modifiche nel medio periodo;
- la situazione economica attuale e prevista nelle zone in cui opera l'organizzazione;
- il clima politico e sociale nelle zone in cui opera l'organizzazione;
- la disponibilità sul mercato e i costi delle risorse utili all'organizzazione;
- le strategie di mercato, attuali e previste, dei clienti, fornitori e partner attuali e potenziali;
- le aspettative delle parti esterne interessate (vedere 5.2).

Quando si descrive il contesto non è necessario descrivere tutti i punti sopra elencati, ma solo quelli significativi per la sicurezza delle informazioni.

Esempio 5.1.1. La descrizione del contesto di un'azienda casearia potrebbe essere il seguente.

Caratteristiche dei servizi e prodotti. L'azienda si occupa di produzione e vendita di prodotti caseari. Essa ha un fatturato annuo di circa 10 milioni di Euro.

Struttura organizzativa. La struttura organizzativa è descritta nell'organigramma (figura 5.1.1). Ulteriori fornitori, oltre al commercialista e agli agenti commerciali, sono: lo sviluppatore del CRM, un operatore di telecomunicazioni, una società di vigilanza e un'impresa di pulizie.

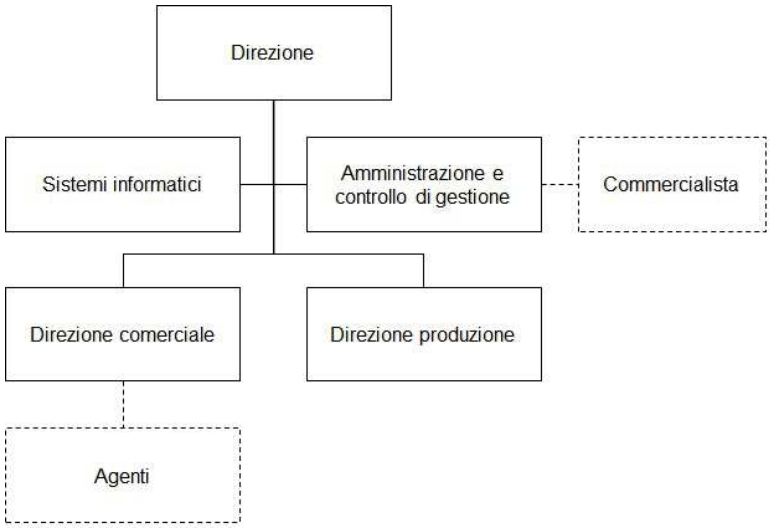

Figura 5.1.1: Esempio di organigramma

Ubicazioni fisiche. L'azienda ha sede in una cascina di proprietà, non condivisa con altre organizzazioni, nel comune di Basilio (MI).

Informazioni trattate. Le informazioni trattate sono quelle relative ai clienti, ai fornitori, ai partner, al personale e ai prodotti (le ricette e le verifiche di qualità). Per evitare di avvantaggiare la concorrenza, è molto importante garantire la riservatezza delle informazioni sui clienti, sui fornitori e sui partner; per il rispetto della normativa vigente in materia di privacy è importante trattare correttamente i dati del personale e, per salvaguardare il patrimonio di conoscenze aziendali, è necessario garantire la riservatezza e integrità delle ricette e dei verbali di verifica.

Sistema informatico. Da un punto di vista sistemistico, l'architettura si basa su sistemi Microsoft Windows per i server e i PC. Le applicazioni e i servizi più importanti sono: sistema di posta elettronica, file server, CRM (*customer relationship management*) e un sistema sviluppato internamente per il controllo del magazzino e della produzione. Gli agenti possono accedere al CRM e quindi all'anagrafica clienti e allo stato degli ordini da qualsiasi strumento dotato di *web browser*.

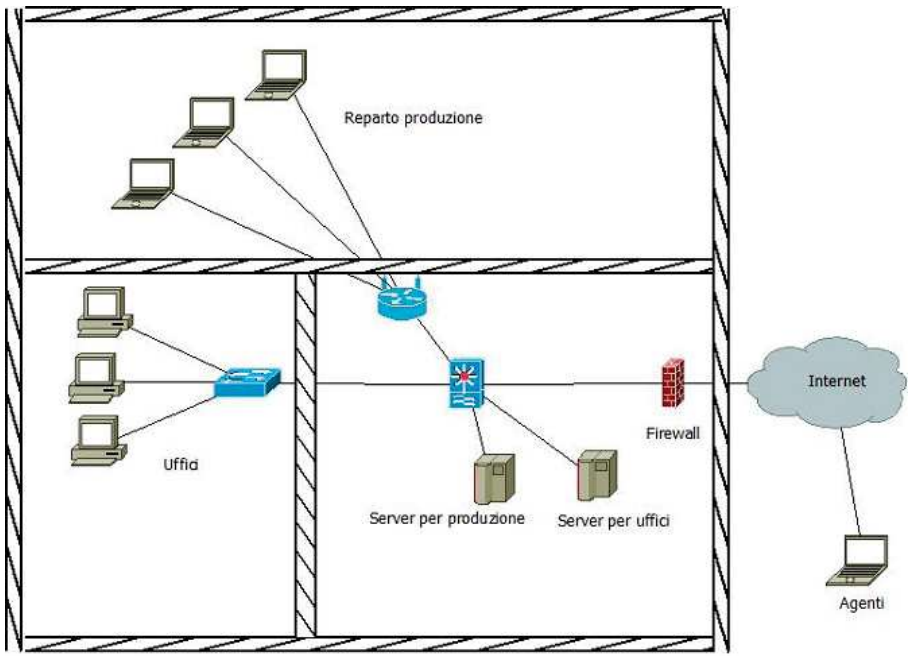

Figura 5.1.2: Esempio di rete IT

Archivi cartacei. Tutti i dati possono essere anche in copie cartacee, archiviate in sede in appositi archivi o, limitatamente ai dati di tipo contabile e amministrativo, nello studio del commercialista.

Normativa vigente. La normativa richiede estrema cura nel mantenimento delle informazioni sui prodotti immessi sul mercato e per questo è vitale garantire l'integrità dei dati relativi alla produzione. Non sono previste modifiche di rilievo nel lungo periodo, ma occorre tenerla sotto controllo.

Livello di innovazione. Le innovazioni sono necessarie per mantenere la competitività sul mercato (informatizzazione del magazzino, comunicazioni con i fornitori via strumenti elettronici, eccetera).

5.2 Le parti interessate

La definizione di *parte interessata* della ISO/IEC 27000:2015 è la seguente.

> *Parte interessata* o *stakeholder*: persona fisica o organizzazione che può influenza, essere influenzata o percepirsi influenzata da una decisione o attività.

Le parti interessate hanno requisiti, ossia aspettative, relativamente al sistema di gestione per la sicurezza delle informazioni. Tali requisiti devono essere considerati dall'organizzazione.

Le *parti interne interessate* sono il personale, gli azionisti e i soci. Le loro aspettative includono il rispetto dei contratti e degli accordi e la buona qualità dell'ambiente di lavoro.

Le *parti esterne interessate* includono i clienti, i fornitori e i partner attuali e potenziali, le società dello stesso gruppo dell'organizzazione e gli enti normativi e di controllo. Tra le loro aspettative vi è il rispetto dei contratti e degli accordi, degli accordi intra-gruppo e della normativa vigente.

Esempio 5.2.1. La parti interessate dell'azienda casearia potrebbero essere le seguenti.

Concorrenti. La concorrenza è molto sentita nel settore, ma non è tale da far temere attività di spionaggio industriale.

Clienti. I clienti richiedono il rispetto delle scadenze e la qualità dei prodotti, in linea con i contratti stipulati e la normativa vigente.

Fornitori. Oltre agli agenti, i fornitori principali sono quelli di materie prime e imballi e si attendono di veder apprezzati i loro sforzi per soddisfare le richieste dell'azienda e di essere pagati secondo le scadenze pattuite.

Personale interno. Composto da 13 persone tra impiegati e operai, con istruzione e formazione non elevata e senza competenze specifiche sull'uso dei sistemi informatici, tranne i due addetti al loro sviluppo e manutenzione. Si aspettano di lavorare in un buon posto di lavoro, rispettoso della normativa vigente (tra cui lo Statuto dei lavoratori e la privacy) e delle scadenze dei pagamenti. Il clima aziendale è buono e non si sono registrate contestazioni significative negli ultimi venti anni.

L'organizzazione non deve necessariamente considerare tutti i requisiti delle parti interessate, deve però identificarli e determinare quali il sistema di gestione per la sicurezza delle informazioni intende affrontare.

Esempio 5.2.2. I clienti di un servizio di infrastruttura cloud (IaaS) potrebbero richiedere l'esecuzione del backup da parte del fornitore del servizio. Questo potrebbe essere offerto come servizio opzionale o incluso automaticamente nell'offerta. Gli stessi clienti potrebbero desiderare, in caso di incidente, dei tempi massimi di interruzione del servizio, mentre il fornitore potrebbe assicurarne di diversi.

Da un punto di vista più gestionale, i clienti potrebbero desiderare che il fornitore rispetti determinate normative o standard non obbligatori nel Paese dove opera il fornitore (p.e. l'HIPAA statunitense). Il fornitore potrebbe prendere in carico tali requisiti o no.

Deve essere assicurato il rispetto della normativa vigente e degli accordi sottoscritti con il personale, i fornitori e i clienti.

5.3 L'ambito

Dopo aver individuato il contesto, è possibile decidere l'*ambito* (in inglese *scope*) in cui effettuare la valutazione del rischio relativo alla sicurezza delle informazioni. Esso può comprendere tutta l'organizzazione o una parte di essa.

Spesso il fattore relativo alla percezione dei clienti è ritenuto così importante che si riduce l'ambito ai soli servizi loro offerti.

Esempio 5.3.1. L'azienda casearia potrebbe decidere di valutare il rischio relativo alla sicurezza delle informazioni per tutta l'organizzazione perché ogni area ha impatti sui tre fattori ritenuti fondamentali dalla Direzione: rapporti con i clienti, qualità del prodotto e soddisfazione del personale.

La stessa azienda potrebbe limitare l'ambito alla produzione, sia a causa degli impatti sui clienti, sia perché richiesto dalla normativa vigente nel campo alimentare.

L'ambito potrebbe essere esteso anche ai fornitori, nel caso in cui trattino dati dell'organizzazione o forniscano prodotti critici.

Alcuni processi non possono essere completamente esclusi dall'ambito, in particolare se la finalità della valutazione del rischio è la certificazione del sistema di gestione per la sicurezza delle informazioni.

Esempio 5.3.2. Se l'azienda casearia decidesse di valutare i rischi relativi alla sicurezza delle informazioni solo nell'ambito della produzione, dovrebbe comunque considerare alcuni processi apparentemente esterni a essa. Per esempio, la gestione del personale è esterna alla produzione, ma molto importante per la sicurezza delle informazioni (paragrafo 12.4). Per questo deve, almeno parzialmente, essere inclusa nell'ambito.

Se l'azienda casearia ha un fornitore di servizi informatici, anch'esso deve essere incluso.

Quando si stabilisce l'ambito, ne devono essere analizzati i confini.

Esempio 5.3.3. Quando si stabilisce l'ambito dell'azienda casearia, è necessario rilevare che i suoi sistemi informatici sono connessi a internet, che il CRM è accessibile via web da qualsiasi PC e che alcuni dati sono accessibili agli agenti esterni.

L'ambito dovrebbe quindi essere descritto riportando:

- le tipologie di informazioni che si vogliono proteggere;
- le caratteristiche dei servizi erogati o dei prodotti realizzati dall'organizzazione e pertinenti le informazioni da proteggere;
- la struttura organizzativa coinvolta nelle attività comprese nell'ambito e i suoi rapporti con la parte di organizzazione esclusa dall'ambito;
- la tecnologia adottata, uno schema della rete informatica e una descrizione delle sue interfacce con altri sistemi informatici dell'organizzazione o dei fornitori esclusi dall'ambito;

- le sedi e i locali dove sono trattate le informazioni oggetto dell'ambito e dove sono collocati gli archivi e i sistemi informatici compresi nell'ambito, inclusi quelli presso fornitori o altre parti esterne;
- i fornitori più importanti coinvolti nella sicurezza delle informazioni, inclusi quelli che sviluppano o conducono i sistemi informatici dell'organizzazione.

Capitolo 6

Identificazione del rischio

Sarebbe un inutile sfoggio di potenza.
(That's much too vulgar a display of power).

Dal film *L'esorcista*

Iniziamo dalla definizione della ISO/IEC 27000.

> *Identificazione del rischio*: processo di individuazione, riconoscimento e descrizione del rischio.

Nel capitolo 4 abbiamo già visto che questo processo richiede l'identificazione di:

- asset;
- minacce;
- vulnerabilità e controlli di sicurezza;
- relazioni tra asset, minacce e vulnerabilità.

6.1 Gli asset

Gli asset sono elementi che permettono all'organizzazione di operare e raggiungere i propri obiettivi. Per la sicurezza delle informazioni, tra gli asset ci sono le informazioni stesse, i sistemi, le persone e i processi coinvolti nella loro elaborazione.

Cominciamo con il riportare la definizione ora non più presente nella ISO/IEC 27000, ma sempre utile.

> *Asset* (*bene*): qualsiasi cosa cha abbia valore per l'organizzazione.
>
> Nota: esistono molti tipi di asset, tra cui: informazioni, software e programmi per computer, elementi fisici (per esempio i computer), servizi, persone e le loro qualifiche, competenze ed esperienze, reputazione e immagine dell'organizzazione.