Cesare Gallotti

con contributi di

Massimo Cottafavi e Stefano Ramacciotti

SICUREZZA DELLE INFORMAZIONI

VALUTAZIONE DEL RISCHIO
I SISTEMI DI GESTIONE
LA NORMA ISO/IEC 27001

Versione Gennaio 2019

Dedicato, come nel 2014, 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 e ringraziamenti

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

Alessandro Manzoni, *I promessi sposi*

La prima versione di questo libro è datata 2002. Negli anni ho fortunatamente incontrato più di 25 persone che l'avevano letto e apprezzato; purtroppo, spesso, l'avevano preso in prestito da una biblioteca e questo non ha aiutato le vendite.

Nel 2014 scrissi una seconda versione 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 era un aggiornamento minore, con qualche nuovo esempio e idea nata durante la partecipazione alla scrittura della ISO/IEC 27003:2017.

Questa quarta versione è anche in lingua inglese. Sono stati aggiunti alcuni esempi e sono stati corretti gli errori evidenziati durante la traduzione.

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, basati sulla ISO/IEC 27002, che utilizzo per le attività di audit e di consulenza.

La quarta parte illustra i requisiti della ISO/IEC 27001:2013 secondo la mia interpretazione maturata durante i lavori di scrittura della norma stessa, i corsi di formazione e le discussioni con i clienti.

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

L'appendice sui Common Criteria e sulle FIPS 140 è un gentile omaggio di Stefano Ramacciotti.

Le successive appendici sulla gestione dei cambiamenti e dei fornitori sono tratte da alcune mie liste di riscontro.

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

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

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

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

Le definizioni sono tratte soprattutto dall'edizione del 2018 dello standard internazionale ISO/IEC 27000. Alcune definizioni sono state lievemente modificate per renderle, a mio parere, più comprensibili. Tra parentesi quadre sono riportate eventuali aggiunte. Le cancellazioni sono evidenziate dal simbolo "[...]".

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

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

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

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

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

Ringrazio anche Franco Ruggieri, Pierfrancesco Maistrello e Francesca Lazzaroni con i quali ho avuto modo di discutere di molte cose in questi anni e che mi hanno fornito preziosi riscontri.

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

Contatti

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

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

Avvertenza

I link riportati in questo libro sono stati verificati l'8 agosto 2018.

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 dei propri clienti, accuratezza di tutti i dati economici e di produzione, disponibilità dei sistemi informatici.

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

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

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

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

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

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

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

Figura 1.0.1: Processi e prodotti

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

Un po' di storia

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

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

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

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

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

2. l'aumento delle persone e dei dispositivi connessi su Internet (a sua volta non progettato per la sicurezza [124]);

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

Figura 1.0.2: L'impresa aperta

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

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

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

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

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

Figura 1.0.3: Nuove minacce

sicurezza delle informazioni (BS 7799 del 1995, di cui si approfondirà la storia nel paragrafo 13.4) e alle metodologie di valutazione del rischio relativo alla sicurezza delle informazioni (CRAMM del 1987, Marion del 1990 e Mehari del 1995) [23].

Parte I

Le basi

Capitolo 2

Sicurezza delle informazioni e organizzazione

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

Thomas Stearns Eliot, *The rock*

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

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

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

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

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

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

2.1 Dati e informazioni

Prima di discutere di dati e informazioni, è opportuno fornirne la definizione, presente in precedenti versioni dello standard ISO/IEC 27000. Nelle ultime versioni dello standard questa definizione non è più riportata, forse perché si preferisce far riferimento ai normali dizionari [97].

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

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

Da questo ragionamento risulta che, quando si parla di *sicurezza delle informazioni*, non ci si limita alla sicurezza informatica, ossia relativa alle informazioni in formato digitale e trattate dai sistemi dell'*Information and communication technology*, ma a tutti i sistemi utilizzati per raccogliere, modificare, conservare, trasmettere e distruggere le informazioni.

[6] www.theguardian.com/uk/2009/apr/09/bob-quick-terror-raids-leak.
[7] punto-informatico.it/3146710/PI/News/aruba-incendio-nella-farm.aspx.
[8] www.bbc.co.uk/news/technology-15287072.
[9] attrition.org/security/rant/sony_aka_sownage.html.
[10] www.pierotaglia.net/facebook-fai-da-te-alpitour-ahi-ahi-ahi-pagine-facebook-hackerate.
[11] www.theregister.co.uk/2013/03/27/spamhaus_ddos_megaflood.

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

Più rigorosamente, la sicurezza delle informazioni include quella dei dati, come si deduce dalle quattro tipologie di rappresentazione della conoscenza [71, 86]:

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

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

2.2 Sicurezza delle informazioni

La ISO/IEC 27000 definisce:

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

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

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

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

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

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

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

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

Figura 2.2.1: Sicurezza delle informazioni e sicurezza informatica

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

Negli anni in molti hanno cercato di giustificare l'uso dei termini *cybersecurity* e *cyberspace* in ambito scientifico, ma senza trovare una soluzione condivisa o rigorosa e, anzi, creando confusione e false aspettative. Per esempio c'è chi usa il termine intendendo qualcosa di più o di meno della sicurezza informatica. Alcuni escludono dalla sicurezza informatica la sicurezza dell'*Internet of things* (IoT) o la sicurezza dell'*Operational technology* (OT), che include la sicurezza dei sistemi industriali (*industrial control systems* o *ICS*), che include la sicurezza delle reti *supervisory control and data acquisition* ($SCADA$); altri escludono dalla *cybersecurity* la sicurezza fisica e ambientale dei sistemi informatici. C'è 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.

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" [24]. 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 2.2.2. In un'azienda italiana, i dati sul personale sono sicuramente riservati, ma persone diverse devono accedervi: il medico competente, l'amministrazione, i dirigenti, certi uffici pubblici, il commercialista e l'ufficio legale.

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

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

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

2.2.2 Integrità

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

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

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

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

2.2.3 Disponibilità

La maggior parte delle persone, come già detto, intende la sicurezza delle informazioni come mantenimento della loro riservatezza. Molti informatici, per contro, soprattutto se impiegati in aziende commerciali, intendono la sicurezza delle informazioni come la capacità di renderle immediatamente disponibili a chi le richiede. Non è però possibile pretendere l'immediatezza in tutte le occasioni

e quindi la proprietà di disponibilità può essere riformulata così: "le informazioni devono essere disponibili entro i tempi stabiliti a coloro che le richiedono e ne hanno il diritto".

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

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 2.2.6. 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.

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

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

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

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

Esempio 2.2.7. Ciascun evento può avere impatti su uno o più parametri RID. Ad essi si possono quindi associare gli esempi riportati in apertura del capitolo, come nella successiva tabella 2.2.1.

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

L'incendio viene associato all'integrità e alla disponibilità, ma potrebbe

essere associato anche alla riservatezza se l'evacuazione di un edificio consente l'accesso a persone non autorizzate oppure comporta la dispersione fuori sede di documenti cartacei riservati.

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

Ulteriore elemento, dettato dalla normativa in materia di privacy, è il cosiddetto *diritto all'oblio*. Questo prevede che le informazioni relative ad 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].

2.3 Organizzazione, processi e funzioni

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

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

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

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

2.3.1 I processi

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

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

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

Apparentemente banale, nasconde diverse complessità.

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

Ma non è così semplice: gli *input* comprendono anche i costi, il budget, le date in cui tenere il corso, la disponibilità (se il caso) dell'aula, le 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 ed invio dei risultati degli esami e così via.

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

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

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

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

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

Ecco quindi di seguito le caratteristiche di ogni processo:

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

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

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

2.3.2 Le funzioni

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

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

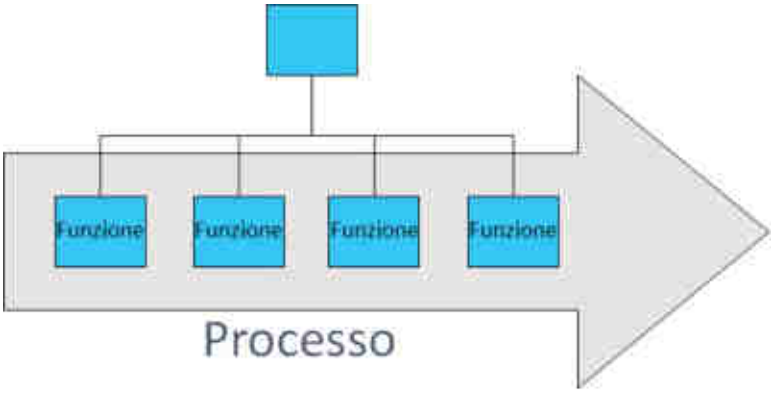

Figura 2.3.1: Processo e funzioni

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

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

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

2.4 Processi, prodotti e persone

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

È infatti necessario avvalersi di persone qualificate, in grado di comprendere e conseguire la sicurezza delle informazioni, attraverso l'applicazione di giusti processi e l'impiego di prodotti idonei. Si parla quindi delle 3 P: processi (o

procedure), persone e prodotti. In appendice B è introdotta una quarta P, per i fornitori (partner).

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

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

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

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

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

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