

Cesare Gallotti

con contributi di

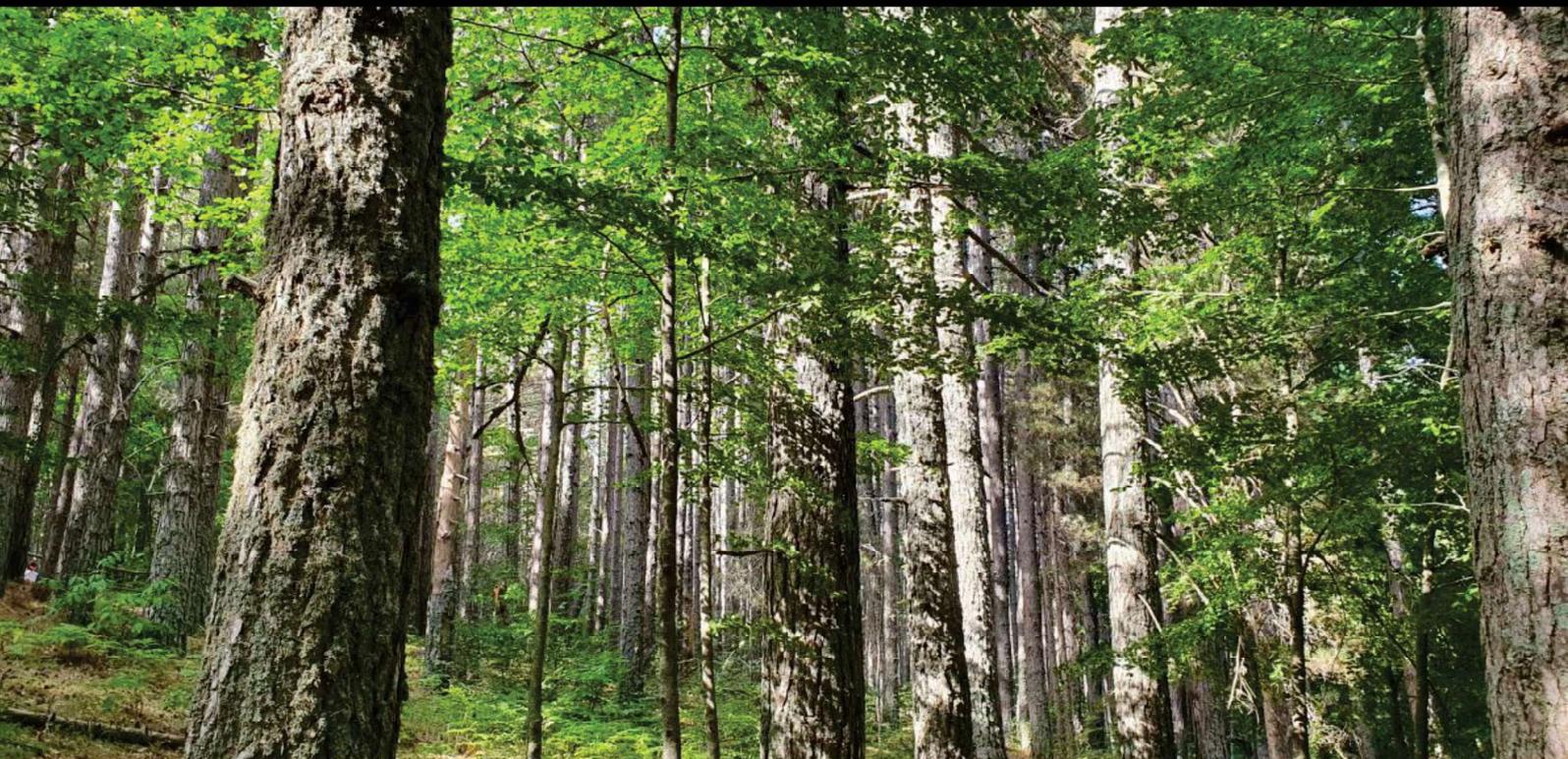
Massimo Cottafavi e Stefano Ramacciotti

.....

S I C U R E Z Z A  
D E L L E  
I N F O R M A Z I O N I

.....

GESTIONE DEL RISCHIO  
I SISTEMI DI GESTIONE  
LA ISO/IEC 27001:2022  
I CONTROLLI DELLA ISO/IEC 27002:2022



Versione Gennaio 2022



CESARE GALLOTTI  
CON IL CONTRIBUTO DI  
MASSIMO COTTAFIVI E STEFANO RAMACCIOTTI

## SICUREZZA DELLE INFORMAZIONI

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

Versione Gennaio 2022

©2022 Cesare Gallotti

Tutti i diritti riservati

Ovviamente non è difficile copiare questo libro tutto o in parte, ma devo offrire una pizza a chi mi ha aiutato a farlo (vedere nei ringraziamenti), quindi vi prego di non farlo.

*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

<b>Presentazione e ringraziamenti</b>	<b>ix</b>
<b>1 Introduzione</b>	<b>1</b>
<b>I Le basi</b>	<b>7</b>
<b>2 Sicurezza delle informazioni e organizzazione</b>	<b>9</b>
2.1 Dati e informazioni . . . . .	10
2.2 Sicurezza delle informazioni . . . . .	11
2.2.1 Riservatezza . . . . .	11
2.2.2 Integrità . . . . .	12
2.2.3 Disponibilità . . . . .	12
2.2.4 Altre proprietà di sicurezza . . . . .	13
2.2.5 Gli impatti sui parametri RID . . . . .	14
2.3 Sicurezza informatica e cybersecurity . . . . .	14
2.4 Organizzazione, processi e funzioni . . . . .	17
2.4.1 I processi . . . . .	17
2.4.2 Le funzioni . . . . .	18
2.5 Processi, prodotti e persone . . . . .	19
<b>3 Sistema di gestione per la sicurezza delle informazioni</b>	<b>21</b>
3.1 Sistema di gestione . . . . .	22
3.2 Sistema di gestione per la sicurezza . . . . .	22
3.3 Le certificazioni . . . . .	23
<b>II La gestione del rischio</b>	<b>25</b>
<b>4 Rischio e valutazione del rischio</b>	<b>27</b>
4.1 Cos'è il rischio . . . . .	28
4.1.1 I rischi positivi e negativi . . . . .	28
4.1.2 Il livello di rischio . . . . .	29
4.2 Cos'è la valutazione del rischio . . . . .	31
4.3 I metodi per valutare il rischio . . . . .	34
4.3.1 I programmi software per la valutazione del rischio . . . . .	34
4.3.2 Avvertenza . . . . .	36
4.4 Chi coinvolgere . . . . .	36
4.4.1 I responsabili del rischio . . . . .	37

4.4.2	I facilitatori . . . . .	37
4.5	I documenti di gestione del rischio . . . . .	38
<b>5</b>	<b>Il contesto e l'ambito</b>	<b>39</b>
5.1	Il contesto . . . . .	39
5.2	L'ambito . . . . .	43
<b>6</b>	<b>Identificazione del rischio</b>	<b>45</b>
6.1	Gli asset . . . . .	45
6.1.1	Informazioni . . . . .	46
6.1.2	Gli altri asset . . . . .	47
6.1.3	Chi identifica gli asset . . . . .	49
6.2	Le minacce . . . . .	50
6.2.1	Gli agenti di minaccia . . . . .	51
6.2.2	Tecniche di minaccia . . . . .	54
6.2.3	Le minacce e il rischio privacy . . . . .	54
6.2.4	Chi individua le minacce . . . . .	55
6.3	Associare le minacce agli asset . . . . .	55
6.4	Collegare le minacce alle conseguenze . . . . .	56
6.5	Le vulnerabilità e i controlli di sicurezza . . . . .	56
6.6	Correlare le vulnerabilità agli asset . . . . .	57
6.7	Correlare vulnerabilità e minacce . . . . .	58
6.7.1	Controlli alternativi, compensativi, complementari e correlati . . . . .	59
6.7.2	Controlli di prevenzione, recupero e rilevazione . . . . .	60
6.8	Conclusione . . . . .	60
<b>7</b>	<b>Analisi del rischio</b>	<b>61</b>
7.1	Metodi di analisi . . . . .	62
7.1.1	Metodi quantitativi . . . . .	62
7.1.2	Metodi qualitativi . . . . .	63
7.2	Il valore degli asset . . . . .	63
7.2.1	Valutare le informazioni . . . . .	64
7.2.2	Il rischio privacy . . . . .	66
7.2.3	Chi assegna i valori alle informazioni . . . . .	66
7.2.4	Valutare gli altri asset . . . . .	67
7.2.5	Valutare gli asset IoT e industriali . . . . .	69
7.3	Valutare la verosimiglianza delle minacce . . . . .	69
7.3.1	Quali valori assegnare alle minacce . . . . .	69
7.3.2	Chi assegna i valori alle minacce . . . . .	72
7.4	Il rischio intrinseco . . . . .	72
7.4.1	Rischio intrinseco quantitativo . . . . .	72
7.4.2	Rischio intrinseco qualitativo . . . . .	74
7.5	Valutare le vulnerabilità e i controlli . . . . .	75
7.5.1	Identificare i controlli ideali . . . . .	76
7.5.2	Quali valori assegnare ai controlli . . . . .	78
7.5.3	Chi assegna i valori ai controlli . . . . .	82
7.6	Il livello di rischio . . . . .	83
7.6.1	Livello di rischio quantitativo . . . . .	83
7.6.2	Livello di rischio qualitativo . . . . .	84

7.6.3	Conclusioni . . . . .	86
7.7	Ulteriori riflessioni sulle aggregazioni . . . . .	87
<b>8</b>	<b>Ponderazione del rischio</b>	<b>89</b>
<b>9</b>	<b>Trattamento del rischio</b>	<b>91</b>
9.1	Le opzioni di trattamento del rischio . . . . .	91
9.1.1	Evitare o eliminare il rischio . . . . .	92
9.1.2	Aumentare il rischio . . . . .	93
9.1.3	Modificare la probabilità della minaccia (Prevenire) . . . . .	94
9.1.4	Modificare le conseguenze (Recuperare) . . . . .	94
9.1.5	Condividere il rischio . . . . .	95
9.1.6	Mantenere il rischio (Accettare) . . . . .	95
9.2	Piano di trattamento del rischio . . . . .	96
9.3	Scelta e attuazione delle azioni di riduzione . . . . .	96
9.3.1	Riesaminare il piano delle azioni . . . . .	97
9.3.2	Il piano delle azioni . . . . .	99
9.3.3	Efficacia delle azioni . . . . .	100
9.3.4	Tenuta sotto controllo del piano di azioni . . . . .	100
<b>10</b>	<b>Monitoraggio e riesame del rischio</b>	<b>103</b>
10.1	Analisi del rischio operativo . . . . .	104
10.2	L'integrazione delle analisi del rischio . . . . .	104
<b>III</b>	<b>Minacce e controlli di sicurezza delle informazioni</b>	<b>107</b>
<b>11</b>	<b>Tecniche di minaccia</b>	<b>109</b>
11.1	Intrusione nella sede o nei locali da parte di malintenzionati . . . . .	109
11.2	Intrusione nei sistemi informatici . . . . .	110
11.3	Social engineering e frodi . . . . .	112
11.4	Furto d'identità . . . . .	114
11.5	Danneggiamento di apparecchiature fisiche . . . . .	114
11.6	Danneggiamenti dei programmi informatici . . . . .	116
11.7	Furto di apparecchiature IT o di impianti . . . . .	116
11.8	Furto di documenti fisici . . . . .	117
11.9	Intercettazioni di emissioni elettromagnetiche . . . . .	118
11.10	Interferenze da emissioni elettromagnetiche . . . . .	118
11.11	Lettura e copia di documenti IT . . . . .	119
11.12	Modifica di documenti informatici . . . . .	120
11.13	Trattamento scorretto delle informazioni . . . . .	120
11.14	Malware . . . . .	122
11.15	Copia e uso illegale di software . . . . .	123
11.16	Uso non autorizzato di servizi IT esterni . . . . .	124
11.17	Uso non autorizzato di sistemi e servizi informatici offerti dall'organizzazione . . . . .	124
11.18	Recupero di informazioni . . . . .	124
11.19	Esaurimento o riduzione delle risorse . . . . .	125
11.20	Intercettazione delle comunicazioni . . . . .	127
11.21	Invio di dati a persone non autorizzate . . . . .	127

11.22	Invio e ricezione di dati non accurati . . . . .	129
11.23	Ripudio di invio da parte del mittente . . . . .	130
11.24	IoT, OT, IIOT . . . . .	130
11.25	Intelligenza artificiale . . . . .	131
<b>12</b>	<b>I controlli di sicurezza</b>	<b>133</b>
12.1	Documenti . . . . .	134
12.1.1	Tipi di documenti . . . . .	134
12.1.2	Come scrivere i documenti . . . . .	137
12.1.3	Approvazione e distribuzione . . . . .	138
12.1.4	Archiviazione delle registrazioni . . . . .	139
12.1.5	Tempo di conservazione . . . . .	140
12.1.6	Verifica e manutenzione dei documenti . . . . .	140
12.1.7	Documenti di origine esterna . . . . .	140
12.2	Politiche di sicurezza delle informazioni . . . . .	140
12.3	Organizzazione per la sicurezza delle informazioni . . . . .	143
12.3.1	Organizzazione . . . . .	143
12.3.2	Separazione dei ruoli . . . . .	146
12.3.3	Gestione dei progetti . . . . .	147
12.3.4	Rapporti con le autorità . . . . .	148
12.3.5	Monitoraggio delle minacce . . . . .	149
12.4	Gestione del personale . . . . .	150
12.4.1	Inserimento del personale . . . . .	150
12.4.2	Uscita del personale e cambiamenti di posizione . . . . .	151
12.4.3	Competenze e sensibilizzazione . . . . .	151
12.4.4	Lavoro fuori sede . . . . .	154
12.5	Gestione degli asset . . . . .	155
12.5.1	Informazioni . . . . .	155
12.5.2	Identificazione, censimento e proprietà degli asset . . . . .	159
12.6	Controllo degli accessi . . . . .	161
12.6.1	Credenziali e identificazione . . . . .	161
12.6.2	Autenticazione . . . . .	162
12.6.3	Autorizzazioni . . . . .	168
12.7	Crittografia . . . . .	174
12.7.1	Algoritmi simmetrici e asimmetrici . . . . .	175
12.7.2	Le funzioni hash . . . . .	176
12.7.3	Protocolli crittografici . . . . .	176
12.7.4	Chiavi crittografiche . . . . .	177
12.7.5	Servizi fiduciari . . . . .	177
12.7.6	Normativa applicabile alla crittografia . . . . .	178
12.8	Sicurezza fisica . . . . .	178
12.8.1	Sicurezza della sede . . . . .	178
12.8.2	Sicurezza delle apparecchiature . . . . .	182
12.8.3	Archivi fisici . . . . .	186
12.9	Conduzione dei sistemi informatici . . . . .	187
12.9.1	Documentazione . . . . .	188
12.9.2	Configurazione dei dispositivi e dei sistemi informatici . . . . .	188
12.9.3	Gestione dei cambiamenti . . . . .	190
12.9.4	Malware . . . . .	202
12.9.5	Backup . . . . .	203

12.9.6	Logging e monitoraggio . . . . .	205
12.9.7	Gestione della capacità . . . . .	209
12.9.8	Dispositivi portatili e personali . . . . .	209
12.9.9	Cancellazione dei dati . . . . .	212
12.10	Sicurezza delle comunicazioni . . . . .	212
12.10.1	Servizi autorizzati . . . . .	212
12.10.2	Segmentazione della rete . . . . .	215
12.10.3	Sicurezza della rete . . . . .	218
12.10.4	Scambi di informazioni . . . . .	220
12.11	Acquisizione, sviluppo e manutenzione . . . . .	225
12.11.1	Acquisizione dei sistemi IT . . . . .	225
12.11.2	Internet of things . . . . .	226
12.11.3	Intelligenza artificiale . . . . .	227
12.12	Gestione dei fornitori . . . . .	227
12.12.1	Gli accordi e i contratti con i fornitori . . . . .	228
12.12.2	Selezione dei fornitori . . . . .	230
12.12.3	Monitoraggio dei fornitori . . . . .	231
12.12.4	Cloud computing e fornitori . . . . .	231
12.12.5	L'acquisizione di prodotti informatici e lo sviluppo affidato all'esterno . . . . .	232
12.12.6	Le assicurazioni . . . . .	233
12.13	Gestione degli incidenti . . . . .	234
12.13.1	Ruoli e procedure . . . . .	235
12.13.2	Processo di gestione degli incidenti . . . . .	235
12.13.3	Controllo delle vulnerabilità . . . . .	238
12.13.4	Gestione dei problemi . . . . .	241
12.13.5	Gestione delle crisi . . . . .	242
12.13.6	Digital forensics . . . . .	243
12.14	Continuità operativa (Business continuity) . . . . .	244
12.14.1	La business impact analysis (BIA) . . . . .	245
12.14.2	Valutazione del rischio per la continuità operativa . . . . .	247
12.14.3	Obiettivi e strategie di ripristino . . . . .	247
12.14.4	I piani di continuità . . . . .	251
12.14.5	Test e manutenzione . . . . .	253
12.15	Conformità . . . . .	254
12.15.1	Normativa vigente . . . . .	254
12.15.2	Contratti . . . . .	262
12.15.3	Audit . . . . .	263
12.15.4	Vulnerability assessment . . . . .	264
12.15.5	Il riesame del sistema di gestione . . . . .	266

## **IV I requisiti di un sistema di gestione per la sicurezza delle informazioni 267**

<b>13</b>	<b>Le norme ISO e l'HLS</b>	<b>269</b>
13.1	Specifiche e linee guida . . . . .	269
13.2	Le norme della famiglia ISO/IEC 27000 . . . . .	270
13.3	ISO/IEC 27701 . . . . .	271
13.4	L'HLS . . . . .	271

13.5	Storia della ISO/IEC 27001 . . . . .	272
13.6	Come funziona la normazione . . . . .	274
<b>14</b>	<b>Il miglioramento continuo e il ciclo PDCA</b>	<b>277</b>
14.1	Il miglioramento continuo . . . . .	277
14.2	Il ciclo PDCA . . . . .	278
14.2.1	Pianificare . . . . .	279
14.2.2	Fare . . . . .	280
14.2.3	Verificare . . . . .	280
14.2.4	Intervenire . . . . .	281
14.2.5	La natura frattale del ciclo PDCA . . . . .	282
<b>15</b>	<b>I requisiti di sistema</b>	<b>285</b>
15.1	Ambito di applicazione dello standard . . . . .	285
15.2	Riferimenti normativi della ISO/IEC 27001 . . . . .	286
15.3	Termini e definizioni della ISO/IEC 27001 . . . . .	286
15.4	Contesto dell'organizzazione e ambito del SGSI . . . . .	286
15.4.1	Il contesto dell'organizzazione . . . . .	286
15.4.2	L'ambito del SGSI . . . . .	287
15.4.3	Sistema di gestione per la sicurezza delle informazioni . . . . .	288
15.5	Leadership . . . . .	288
15.5.1	Politica per la sicurezza delle informazioni . . . . .	289
15.5.2	Ruoli e responsabilità . . . . .	289
15.6	Pianificazione . . . . .	290
15.6.1	I rischi relativi all'efficacia del sistema di gestione . . . . .	290
15.6.2	Valutazione del rischio relativo alla sicurezza delle informazioni . . . . .	293
15.6.3	Il trattamento del rischio relativo alla sicurezza delle informazioni . . . . .	294
15.6.4	Le azioni . . . . .	296
15.6.5	Obiettivi . . . . .	298
15.7	Processi di supporto . . . . .	305
15.7.1	Risorse . . . . .	305
15.7.2	Competenze e consapevolezza . . . . .	305
15.7.3	Comunicazione . . . . .	306
15.7.4	Informazioni documentate . . . . .	307
15.8	Attività operative . . . . .	308
15.8.1	La pianificazione e il controllo dei processi operativi . . . . .	308
15.8.2	Valutazione e trattamento del rischio relativo alla sicurezza delle informazioni . . . . .	308
15.9	Valutazione delle prestazioni . . . . .	309
15.9.1	Monitoraggio, misurazione, analisi, valutazione . . . . .	309
15.9.2	Audit interni . . . . .	314
15.9.3	Riesami di Direzione . . . . .	318
15.10	Miglioramento . . . . .	320
15.10.1	Non conformità . . . . .	320
15.10.2	Azioni correttive . . . . .	323
15.10.3	Azioni preventive . . . . .	323
15.10.4	Miglioramento continuo . . . . .	324
15.11	Appendice A della ISO/IEC 27001 . . . . .	324

15.12Bibliografia della ISO/IEC 27001 . . . . .	325
<b>V Appendici</b>	<b>327</b>
<b>A Gestire gli auditor</b>	<b>329</b>
A.1 L'auditor è un ospite . . . . .	330
A.2 L'auditor è un partner . . . . .	331
A.3 L'auditor è un fornitore . . . . .	332
A.4 L'auditor è un auditor . . . . .	333
<b>B I primi passi per realizzare un SGSI</b>	<b>335</b>
B.1 Individuare l'ambito . . . . .	335
B.2 Coinvolgere i manager . . . . .	336
B.3 Gestire i documenti . . . . .	336
B.4 Miglioramento . . . . .	336
B.5 Formare il personale . . . . .	336
B.6 Gap analysis . . . . .	337
B.7 Realizzare il sistema di gestione . . . . .	337
<b>C La certificazione di un sistema di gestione</b>	<b>339</b>
C.1 Gli attori . . . . .	339
C.2 Il percorso di certificazione . . . . .	340
C.2.1 Il contratto . . . . .	340
C.2.2 L'audit di certificazione . . . . .	341
C.2.3 Raccomandazione ed emissione del certificato . . . . .	341
C.2.4 Audit straordinario . . . . .	341
C.2.5 Audit periodici . . . . .	341
C.2.6 Audit di ricertificazione . . . . .	342
C.3 I bandi di gara . . . . .	342
C.4 Standard e certificazioni per settori specifici . . . . .	343
C.5 Accredитamento . . . . .	343
C.5.1 Accredитamento per la certificazione dei sistemi di gestione	343
C.5.2 Certificazione e accredитamento dei laboratori . . . . .	345
C.5.3 Certificazione dei prodotti, servizi e processi . . . . .	345
C.5.4 Certificazione della sicurezza informatica, Common Cri- teria e Cybersecurity Act . . . . .	346
C.5.5 Certificazione e perimetro di sicurezza nazionale . . . . .	347
C.5.6 Certificazione di processo e il GDPR . . . . .	347
C.6 I falsi miti della certificazione . . . . .	348
<b>D Common Criteria (ISO/IEC 15408) e FIPS 140-3</b>	<b>349</b>
<small>DI STEFANO RAMACCIOTTI</small>	
D.1 Common Criteria (ISO/IEC 15408) . . . . .	349
D.1.1 Generalità . . . . .	349
D.1.2 Tecnica della valutazione . . . . .	350
D.1.3 Problemi dovuti a una scarsa conoscenza dei Common Criteria . . . . .	352
D.2 FIPS 140-3 . . . . .	355
D.2.1 Generalità . . . . .	355

D.2.2	Tecnica della valutazione . . . . .	357
D.2.3	Problemi dovuti all'impiego della FIPS 140-3 . . . . .	359
<b>E</b>	<b>Requisiti per i cambiamenti</b>	<b>361</b>
E.1	Requisiti funzionali di controllo accessi . . . . .	361
E.2	Requisiti sulla connettività . . . . .	362
E.3	Requisiti funzionali relativi alla crittografia . . . . .	362
E.4	Requisiti di monitoraggio . . . . .	363
E.5	Requisiti di capacità . . . . .	363
E.6	Requisiti architetturali . . . . .	363
E.7	Requisiti applicativi . . . . .	364
E.8	Requisiti di servizio . . . . .	364
<b>F</b>	<b>Requisiti per contratti e accordi con i fornitori</b>	<b>365</b>
F.1	Requisiti per i fornitori di prodotti . . . . .	365
F.2	Requisiti per i fornitori di servizi non informatici . . . . .	366
F.3	Requisiti per i fornitori di servizi informatici . . . . .	367
<b>G</b>	<b>I controlli della ISO/IEC 27002:2022</b>	<b>371</b>
	<b>Bibliografia</b>	<b>379</b>

# 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 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.

Questa quarta versione (con i Giganti della Sila in copertina) nasce 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. Ho colto l'occasione per inserire ulteriori aggiornamenti sulle tecnologie (citando IoT, OT, intelligenza artificiale, eccetera), sulle minacce e gli accreditamenti. Questa volta, per l'inglese, mi ha aiutato Simona Cifarelli, che ha fatto un ottimo lavoro, nonostante il poco tempo che le ho dato.

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).

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. 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 27003:2017.

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.

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 "[...]".

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 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 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, aggiornata a ogni edizione, l'esempio di Fort Knox e quanto riguarda le tre e le quattro P);
- 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 avuto l'onore di considerarla mia amica e di ricevere i suoi suggerimenti per migliorare questo libro.

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 Lazaroni con i quali ho avuto modo di discutere di molte cose in questi anni e che mi hanno fornito preziosi riscontri. Ringrazio anche gli Idraulici della privacy, che mi hanno permesso di migliorare le mie conoscenze in ambito privacy e con i quali ho pubblicato un libro [65] il cui ricavato va in beneficenza.

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](http://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](http://www.cesaregallotti.it).

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

## Avvertenza

I link riportati in questo libro sono stati verificati il 22 dicembre 2021.



# 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. 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 [148]);
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.

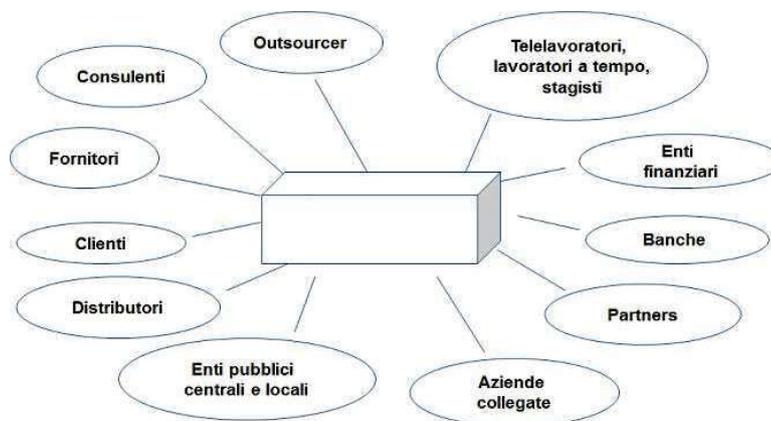


Figura 1.0.2: L'impresa aperta

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.



Figura 1.0.3: Nuove minacce

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<sup>1</sup> 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) [27].

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),

<sup>1</sup><http://csrc.nist.gov>.

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 comunque segnalato le esigenze di sicurezza informatica in numerose altre normative, inclusa quella relativa alla sicurezza dei dispositivi medici.

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 fu 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.

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.



**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<sup>1</sup>;
- nel 1998, il Ministero delle Finanze inviò milioni di cartelle esattoriali sbagliate ai contribuenti<sup>2</sup>;
- 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<sup>3</sup> 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<sup>4</sup>;
- 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<sup>5</sup>;

---

<sup>1</sup>[http://it.wikipedia.org/wiki/Biblioteca\\_di\\_Alessandria](http://it.wikipedia.org/wiki/Biblioteca_di_Alessandria).

<sup>2</sup>[www.contribuenti.it/cartellepazze/cartellepazze1.asp](http://www.contribuenti.it/cartellepazze/cartellepazze1.asp).

<sup>3</sup>[www.repubblica.it/2003/i/sezioni/cronaca/blackitalia/blackitalia/blackitalia.html](http://www.repubblica.it/2003/i/sezioni/cronaca/blackitalia/blackitalia/blackitalia.html).

<sup>4</sup>[news.bbc.co.uk/sport2/hi/motorsport/formula\\_one/6994416.stm](http://news.bbc.co.uk/sport2/hi/motorsport/formula_one/6994416.stm).

<sup>5</sup>[www.theguardian.com/uk/2009/apr/09/bob-quick-terror-raids-leak](http://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<sup>6</sup>;
- a inizio 2013, i servizi di antispamming della Spamhaus furono bloccati da un attacco<sup>7</sup>;
- a fine 2019, un'organizzazione, a causa di un colpo di vento, si vide volare numerosi documenti cartacei per strada<sup>8</sup>;
- nel maggio 2020, EasyJet fu attaccata da malintenzionati che rubarono i dati dei passeggeri, inclusi numeri di carte di credito<sup>9</sup>;
- nel marzo 2021, il data centre di OVH a Strasburgo andò a fuoco e molti sistemi rimasero indisponibili<sup>10</sup>;
- nell'agosto 2021, i sistemi informatici per la prenotazione dei vaccini COVID-19 della Regione Lazio rimasero indisponibili per quattro giorni a causa di un ransomware<sup>11</sup>;
- a ottobre 2021 Facebook, WhatsApp e Instagram rimasero rimasti bloccati per 6 ore a causa di un errore di configurazione<sup>12</sup>.

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 [118].

*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.

<sup>6</sup>[www.pierotaglia.net/facebook-fai-da-te-alpitour-ahi-ahi-ahi-pagine-facebook-hackerate](http://www.pierotaglia.net/facebook-fai-da-te-alpitour-ahi-ahi-ahi-pagine-facebook-hackerate).

<sup>7</sup>[www.theregister.co.uk/2013/03/27/spamhaus\\_ddos\\_megafood](http://www.theregister.co.uk/2013/03/27/spamhaus_ddos_megafood).

<sup>8</sup><https://www.key4biz.it/idiot-wind-bob-dylan-puo-aiutare-nella-valutazione-del-rischio-aziendale/307656/>.

<sup>9</sup><https://www.bbc.com/news/technology-52722626>.

<sup>10</sup><https://www.wired.it/internet/web/2021/03/10/incendio-data-center-ovh-strasburgo/>.

<sup>11</sup><https://www.cybersecurity360.it/nuove-minacce/regione-lazio-vaccini-bloccati-poco-pronta-contro-il-ranwomare-ecco-perche/>.

<sup>12</sup>[https://www.corriere.it/esteri/21\\_ottobre\\_05/facebook-instagram-whatsapp-down-costa-zuckerberg-6-miliardi-dollari-d6f5c632-2586-11ec-9c26-509de9bc1f2d.shtml](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, la sicurezza delle informazioni include quella dei dati, come si deduce dalle quattro tipologie di rappresentazione della conoscenza [107]:

- *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 [83] 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” [28]. 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.

## 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 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<sup>13</sup>.

<sup>13</sup>[http://www.repubblica.it/tecnologia/2014/05/13/news/causa\\_contro\\_google\\_corte\\_ue\\_motore\\_di\\_ricerca\\_responsabile\\_dati-85985943/](http://www.repubblica.it/tecnologia/2014/05/13/news/causa_contro_google_corte_ue_motore_di_ricerca_responsabile_dati-85985943/).

### 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<sup>14</sup>, 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 <i>Denial of Service</i>			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 esempio quelli industriali) potrebbero non essere considerati come pertinenti le informazioni.

**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<sup>15</sup>.

<sup>14</sup>[attribution.org/security/rant/sony\\_aka\\_sownage.html](http://attribution.org/security/rant/sony_aka_sownage.html).

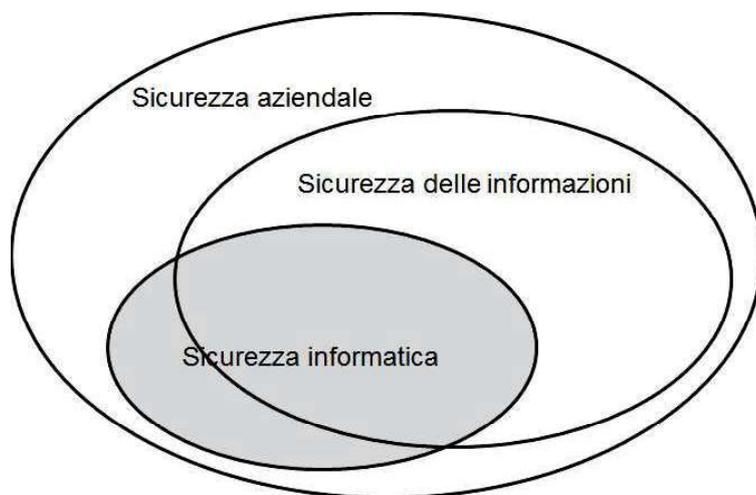


Figura 2.3.1: Sicurezza delle informazioni e sicurezza informatica

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<sup>15</sup>.

Questo attacco, anche se ha avuto impatti sulle informazioni dei dosaggi, è visto da alcuni come relativo agli impianti industriali e non alla sicurezza delle 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 perché 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. 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

<sup>15</sup>[http://www.theregister.co.uk/2016/11/09/finns\\_chilling\\_as\\_ddos\\_knocks\\_out\\_building\\_control\\_system/](http://www.theregister.co.uk/2016/11/09/finns_chilling_as_ddos_knocks_out_building_control_system/)

<sup>16</sup><https://www.zdnet.com/article/following-olddsmar-attack-fbi-warns-about-using-teamviewer-and-windows-7/>

gas ed elettricità, impianti di riscaldamento e raffreddamento, sistemi industriali e domotici, eccetera.

Una buona definizione è la seguente<sup>17</sup>:

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

Questa vuol dire che essa 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.

Vuole anche dire che è esclusa dalla *cybersecurity* la sicurezza fisica e ambientale dei sistemi informatici.

C'è anche chi usa il termine *cybersecurity* per indicare la sicurezza di Internet includendo fenomeni come il bullismo online (*cyberbullismo*).

La definizione del NIST, che è l'ente che ha reso popolare il termine con il suo *Cybersecurity framework* o CSF [113], 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.

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 quindi le informazioni su altri supporti, ma 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.

Nella definizione italiana il termine *confidenzialità* è usato al posto di *riservatezza* perché quest'ultimo può 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

<sup>17</sup><https://www.cisoplatfrom.com/profiles/blogs/understanding-difference-between-cybersecurity-information>.

termine “confidential”, sia nell’ambito delle classifiche di segretezza, sia in altri contesti<sup>18</sup>.

## 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.

---

<sup>18</sup>Si preferisce non ribadire i commenti sull’uso del termine “cibernetico”.

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 [70]:

*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.

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.

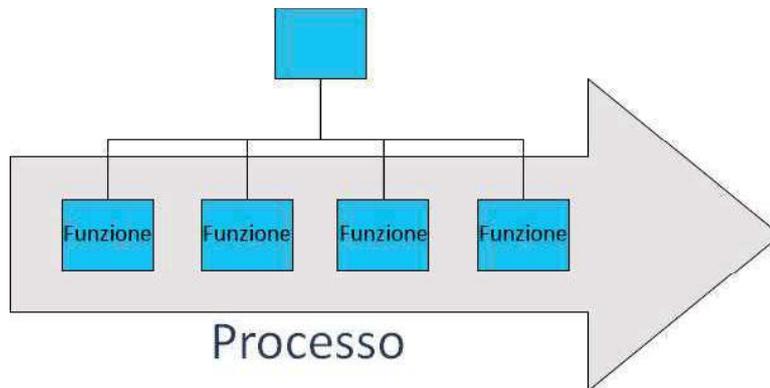


Figura 2.4.1: Processo e funzioni

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

## 2.5 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 2.5.1.** 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.

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.