

SICUREZZA DELLE INFORMAZIONI

VALUTAZIONE DEL RISCHIO
I SISTEMI DI GESTIONE
LA NORMA ISO/IEC 27001:2013

Cesare Gallotti



Versione 10 giugno 2014

Indice

Presentazione e ringraziamenti	ix
1 Introduzione	1
I Le basi	5
2 Sicurezza delle informazioni e organizzazione	7
2.1 Dati e informazioni	8
2.2 Sicurezza delle informazioni	9
2.2.1 Riservatezza	10
2.2.2 Integrità	10
2.2.3 Disponibilità	11
2.2.4 Altre proprietà di sicurezza	11
2.3 Organizzazione, processi e funzioni	12
2.3.1 I processi	12
2.3.2 Le funzioni	14
2.4 Processi, prodotti e persone	15
3 Sistema di gestione per la sicurezza delle informazioni	17
3.1 Sistema di gestione	18
3.2 Sistema di gestione per la sicurezza...	19
3.3 Le certificazioni	19
II La gestione del rischio	21
4 Rischio e valutazione del rischio	23
4.1 Cos'è il rischio	24
4.1.1 I rischi positivi e negativi	24
4.1.2 Il livello di rischio	25
4.2 Cos'è la valutazione del rischio	27
4.3 I metodi per valutare il rischio	30
4.3.1 I programmi software per la valutazione del rischio	31
4.4 Chi coinvolgere	33

4.4.1	I responsabili del rischio	33
4.4.2	I facilitatori	34
5	Il contesto e l'ambito	35
5.1	Il contesto	35
5.2	L'ambito	39
6	Identificazione del rischio	41
6.1	Gli asset	41
6.1.1	Information asset	42
6.1.2	Gli altri asset	42
6.1.3	Chi identifica gli asset	44
6.2	Le minacce	45
6.2.1	Gli agenti di minaccia	47
6.2.2	Tecniche di minaccia	49
6.2.3	Chi individua le minacce	50
6.3	Associare le minacce agli asset	50
6.4	Collegare le minacce alle conseguenze	52
6.5	Le vulnerabilità e i controlli di sicurezza	53
6.6	Correlare le vulnerabilità agli asset	53
6.7	Correlare vulnerabilità e minacce	54
6.7.1	Controlli alternativi, compensativi, complementari e correlati	55
6.7.2	Controlli di prevenzione, recupero e rilevazione	56
6.8	Conclusione	56
7	Analisi del rischio	59
7.1	Metodi di analisi	60
7.1.1	Metodi quantitativi	60
7.1.2	Metodi qualitativi	61
7.2	Il valore degli asset	61
7.2.1	Valutare le informazioni	62
7.2.2	Quali valori assegnare alle informazioni	62
7.2.3	Chi assegna i valori alle informazioni	64
7.2.4	Valutare gli altri asset	65
7.3	Valutare la verosimiglianza delle minacce	67
7.3.1	Quali valori assegnare alle minacce	67
7.3.2	Chi assegna i valori alle minacce	69
7.4	Il rischio intrinseco	70
7.4.1	Rischio intrinseco quantitativo	70
7.4.2	Rischio intrinseco qualitativo	71
7.5	Valutare le vulnerabilità e i controlli	73
7.5.1	Identificare i controlli ideali	74
7.5.2	Quali valori assegnare ai controlli	76
7.5.3	Chi assegna i valori ai controlli	80
7.6	Il livello di rischio	81

7.6.1	Livello di rischio quantitativo	82
7.6.2	Livello di rischio qualitativo	83
7.6.3	Conclusioni	85
7.7	Ulteriori riflessioni sulle aggregazioni	86
8	Ponderazione del rischio	87
9	Trattamento del rischio	91
9.1	Le opzioni di trattamento del rischio	92
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)	95
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	100
9.3.3	Efficacia delle azioni	101
9.3.4	Tenuta sotto controllo del piano di azioni	101
10	Monitoraggio e riesame del rischio	103
III	I controlli di sicurezza	105
11	I controlli di sicurezza	107
11.1	Documenti	108
11.1.1	Tipi di documenti	108
11.1.2	Come scrivere i documenti	111
11.1.3	Approvazione e distribuzione	112
11.1.4	Archiviazione delle registrazioni	113
11.1.5	Tempo di conservazione	113
11.1.6	Verifica e manutenzione dei documenti	114
11.1.7	Documenti di origine esterna	114
11.2	Politiche di sicurezza delle informazioni	114
11.3	Organizzazione per la sicurezza delle informazioni	116
11.3.1	La Direzione	117
11.3.2	Governance e management	117
11.3.3	Il responsabile della sicurezza	118
11.3.4	Altri ruoli e responsabilità	118
11.3.5	Coordinamento	119
11.3.6	Gestione dei progetti	119
11.3.7	Separazione dei ruoli	120
11.3.8	Rapporti con le autorità	122

11.4 Gestione del personale	122
11.4.1 Inserimento del personale	122
11.4.2 Competenze	123
11.4.3 Consapevolezza e sensibilizzazione	124
11.4.4 Lavoro fuori sede	126
11.5 Gestione degli asset	126
11.5.1 Informazioni	126
11.5.2 Identificazione e censimento degli asset	128
11.6 Controllo degli accessi	130
11.6.1 Credenziali	130
11.6.2 Autorizzazioni	135
11.7 Crittografia	140
11.7.1 Algoritmi simmetrici e asimmetrici	141
11.7.2 Protocolli crittografici	142
11.7.3 Normativa applicabile alla crittografia	143
11.8 Sicurezza fisica	143
11.8.1 Sicurezza della sede	143
11.8.2 Sicurezza delle apparecchiature	146
11.8.3 Archivi fisici	148
11.9 Conduzione dei sistemi informatici	149
11.9.1 Documentazione	149
11.9.2 Gestione dei cambiamenti	150
11.9.3 Malware	160
11.9.4 Backup	161
11.9.5 Monitoraggio e logging	163
11.9.6 Dispositivi portatili e personali	166
11.10 Sicurezza delle comunicazioni	168
11.10.1 Servizi autorizzati	168
11.10.2 Segmentazione della rete	170
11.10.3 Protezione degli apparati di rete	172
11.10.4 Scambi di informazioni	173
11.11 Acquisizione, sviluppo e manutenzione	177
11.12 Gestione dei fornitori	178
11.12.1 Gli accordi e i contratti con i fornitori	179
11.12.2 Selezione dei fornitori	181
11.12.3 Monitoraggio dei fornitori	181
11.12.4 Due parole sul <i>cloud</i>	182
11.13 Gestione degli incidenti	182
11.13.1 Processo di gestione degli incidenti	183
11.13.2 Controllo delle vulnerabilità	187
11.13.3 Gestione dei problemi	189
11.13.4 Gestione delle crisi	190
11.13.5 Digital forensics	191
11.14 Continuità operativa (Business continuity)	192
11.14.1 La business impact analysis	194
11.14.2 Valutazione del rischio per la continuità operativa	195

11.14.3 Obiettivi e strategie di ripristino	196
11.14.4 I piani di continuità	200
11.14.5 Test e manutenzione	201
11.15 Conformità	202
11.15.1 Normativa vigente	202
11.15.2 Audit	208
11.15.3 Vulnerability assessment	209

IV I requisiti di un sistema di gestione per la sicurezza delle informazioni 211

12 Il miglioramento continuo e il ciclo PDCA 213	
12.1 Il miglioramento continuo	213
12.2 Il ciclo PDCA	214
12.2.1 Pianificare	215
12.2.2 Fare	215
12.2.3 Verificare	216
12.2.4 Intervenire	217
12.2.5 La natura frattale del ciclo PDCA	218
13 Le norme ISO e l'HLS 221	
13.1 Specifiche e linee guida	221
13.2 Le norme della famiglia ISO/IEC 27000	222
13.3 L'HLS	223
13.4 Storia della ISO/IEC 27001	223
13.5 Come funziona la normazione	226
14 I requisiti di sistema 229	
14.1 Ambito di applicazione dello standard	229
14.2 Riferimenti normativi della ISO/IEC 27001	230
14.3 Termini e definizioni della ISO/IEC 27001	230
14.4 Contesto dell'organizzazione e ambito del SGSI	230
14.4.1 Il contesto dell'organizzazione	231
14.4.2 L'ambito del SGSI	231
14.4.3 Sistema di gestione per la sicurezza delle informazioni	232
14.5 Leadership	233
14.5.1 Politica per la sicurezza delle informazioni	233
14.5.2 Ruoli e responsabilità	234
14.6 Pianificazione	234
14.6.1 I rischi relativi al sistema di gestione	235
14.6.2 Valutazione del rischio relativo alla sicurezza delle informazioni	238
14.6.3 Il trattamento del rischio relativo alla sicurezza delle informazioni	239
14.6.4 Le azioni	241

14.6.5	Obiettivi	243
14.7	Processi di supporto	250
14.7.1	Risorse	250
14.7.2	Competenze e consapevolezza	251
14.7.3	Comunicazione	252
14.7.4	Informazioni documentate	252
14.8	Attività operative	253
14.8.1	La pianificazione e il controllo dei processi operativi	253
14.8.2	Valutazione e trattamento del rischio relativo alla sicurezza delle informazioni	254
14.9	Valutazione delle prestazioni	254
14.9.1	Monitoraggio, misurazione, analisi, valutazione	254
14.9.2	Audit interni	259
14.9.3	Riesami di Direzione	264
14.10	Miglioramento	265
14.10.1	Non conformità	265
14.10.2	Azioni correttive	269
14.10.3	Azioni preventive	269
14.10.4	Miglioramento continuo	270
14.11	Appendice A della ISO/IEC 27001	270
14.12	Bibliografia della ISO/IEC 27001	271
V	Appendici	273
A	Gestire gli auditor	275
A.1	L'auditor è un ospite	276
A.2	L'auditor è un partner	277
A.3	L'auditor è un fornitore	278
A.4	L'auditor è un auditor	279
B	I primi passi per realizzare un SGSI	281
B.1	Individuare l'ambito	281
B.2	Coinvolgere i manager	282
B.3	Gestire i documenti	282
B.4	Miglioramento	282
B.5	Formare il personale	283
B.6	Gap analysis	283
B.7	Realizzare il sistema di gestione	284
C	La certificazione di un sistema di gestione	285
C.1	Gli attori	285
C.2	Il percorso di certificazione	286
C.2.1	Il contratto	287
C.2.2	L'audit di certificazione	287
C.2.3	Raccomandazione ed emissione del certificato	287

C.2.4	Audit straordinario	288
C.2.5	Audit periodici	288
C.2.6	Audit di ricertificazione	288
C.3	I bandi di gara	288
C.4	I falsi miti della certificazione	289
D	Common Criteria (ISO/IEC 15408) e FIPS 140-2	291
D.1	Diffusione dei Common Criteria	293
D.2	FIPS 140-2	295
D.3	Altre certificazioni di prodotto	300
E	Requisiti per i cambiamenti	301
E.1	Requisiti funzionali di controllo accessi	301
E.2	Requisiti sulla connettività	302
E.3	Requisiti funzionali relativi alla crittografia	302
E.4	Requisiti di monitoraggio	303
E.5	Requisiti di capacità	303
E.6	Requisiti architetturali	303
E.7	Requisiti applicativi	303
E.8	Requisiti di servizio	304
F	Tecniche di minaccia	305
F.1	Intrusione nella sede o nei locali da parte di malintenzionati	305
F.2	Intrusione nei sistemi informatici	306
F.3	Social engineering	308
F.4	Furto d'identità	309
F.5	Danneggiamento di apparecchiature fisiche	309
F.6	Danneggiamenti dei programmi informatici	311
F.7	Furto di apparecchiature IT o di impianti	312
F.8	Lettura, furto, copia o alterazione di documenti in formato fisico	312
F.9	Intercettazioni di emissioni elettromagnetiche	313
F.10	Interferenze da emissioni elettromagnetiche	313
F.11	Lettura e copia di documenti IT	314
F.12	Modifica non autorizzata di documenti informatici	315
F.13	Trattamento scorretto delle informazioni	315
F.14	Malware	316
F.15	Copia e uso illegale di software	317
F.16	Uso non autorizzato di servizi IT esterni	318
F.17	Uso non autorizzato di sistemi e servizi informatici offerti dall'organizzazione	318
F.18	Recupero di informazioni	319
F.19	Esaurimento o riduzione delle risorse	319
F.20	Intercettazione delle comunicazioni	321
F.21	Invio di dati a persone non autorizzate	322
F.22	Invio e ricezione di dati non accurati	323
F.23	Ripudio di invio di messaggi e documenti da parte del mittente	324

G Requisiti per contratti e accordi con i fornitori	325
G.1 Requisiti per i fornitori di prodotti	325
G.2 Requisiti per i fornitori di servizi non informatici	326
G.3 Requisiti per i fornitori di servizi informatici	327
H Dalla ISO/IEC 27001:2005 alla ISO/IEC 27001:2013	331
H.1 I cambiamenti ai requisiti di sistema	331
H.1.1 Il contesto e l'ambito	331
H.1.2 Leadership	332
H.1.3 Pianificazione	332
H.1.4 Supporto	333
H.1.5 Valutazione delle prestazioni	334
H.1.6 Miglioramento	335
H.2 Controlli di sicurezza	336
H.2.1 Terminologia	336
H.2.2 Controlli spostati	337
H.2.3 Controlli integrati in altri	337
H.2.4 Nuovi controlli	338
Bibliografia	339

Presentazione e ringraziamenti

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

Alessandro Manzoni, *I promessi sposi*

Nel 2002 scrissi il libro *Sicurezza delle informazioni - Analisi e gestione del rischio* per la FrancoAngeli [28] e mi ero divertito molto a scriverlo. Mi ha fatto anche molto piacere incontrare in questi anni più di 25 persone, che l'avevano letto e apprezzato; purtroppo, spesso, l'avevano preso in prestito da una biblioteca e questo non ha aiutato ad aumentare le vendite.

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

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

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

- la prima parte riporta le basi per descrivere la sicurezza delle informazioni e un sistema di gestione per la sicurezza delle informazioni;
- la seconda parte descrive la valutazione del rischio, con un'ampia parte teorica, bilanciata da molti esempi; i calcoli presentati non sono necessari per comprendere appieno i concetti esposti;
- la terza parte descrive i controlli di sicurezza ed è stata ricavata dagli appunti, basati sulla ISO/IEC 27002, che utilizzo per le attività di audit e di consulenza;