Indice

Indice....3

Introduzione e riconoscimenti....11

1.
La Governance della Sicurezza....13
La società del rischio....13
Il concetto di sicurezza applicata alle aziende e alle organizzazioni....15
La sicurezza come processo aziendale....15

2.
Il panorama legislativo....17
Considerazioni introduttive....17
Sicurezza e responsabilità amministrativa degli enti....19
Il Decreto Legislativo 231/2001....19
Progettazione e implementazione del sistema di deleghe aziendali....26
La sicurezza e i "computer crimes"....30
La Legge 23 dicembre 1993 n. 547....30
La legge 18 marzo 2008 n. 48 "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001 e norme di adeguamento all'ordinamento interno"....37
La tutela dei dati aziendali tramite l'attuazione della normativa in tema di Privacy....39
Il Decreto legislativo 30 giugno 2003, n. 196 (Codice della Privacy)....39
L'attuazione della normativa sul documento informatico e sulle firme elettroniche....46
Premesse....46
La normativa in vigore....48
Il D.Lgs. 61/2011 e le Infrastrutture Critiche Europee....52
L'attuazione della normativa sulla "disciplina del segreto"....57
La sicurezza aziendale tra aspetti logici e fisici....60
Aspetti conclusivi....62

3.
Certificazione e "standard" relativi....65
Il concetto di certificazione....65
Dall'"Orange Book" ad ITSEC fino ai Common Criteria....68
I "Common Criteria"....74

Il Target Of Evaluation (TOE)....78
Il Security Target (ST)....79
Requisiti di sicurezza....80
Requisiti di sicurezza funzionali (SFR)....81
Requisiti di sicurezza di garanzia (SAR)....83
Livelli EAL....84
Classi di garanzia (SAR)....86
Protection Profile (PP)....88
Lo standard ISO/IEC 27001(ex BS7799)....88
Il concetto di "Information Security Management System"....92
Definizione della politica di sicurezza di alto livello (Define the policy)....92
Gestione del rischio (Manage the risk)....94
Definizione delle contromisure (Select control objectives and controls to be implemented)....94
Analisi dell'applicabilità delle contromisure (Prepare a statement of applicability) 94
I controlli previsti dall'ISO/IEC 27002....94
1 - Politica di sicurezza (Security policy)....95
2 - Organizzazione della sicurezza (Security organisation)....95
3 - Classificazione e controllo dei beni (Asset classification and control)....95
4 - Gestione del personale (Personnel security)....96
5 - Sicurezza fisica e ambientale (Physical and environmental security)....96
6 - Gestione dei sistemi (Communications and operations management)....97
7 - Controllo accessi (Access control)....98
8 - Sviluppo e manutenzione dei sistemi (Systems development and manteinance). 99
9 - Business continuity (Business continuity management)....99
10 - Conformità (Compliance)....100
Considerazioni....100
Altri standard....101
BS 25999 e BS 25777 101
ITIL v3 104
ISO 20000....105
ISO/IEC 21827:2008 (SSE-CMM®) 105
COBIT....106
L'infrastruttura della certificazione....107

4.
L'analisi e la gestione del rischio....109
Premessa....109
Il modello complessivo....110
Modello generale e terminologia....111
Concetti e termini....111
Schema sinottico (modello)....113
Aspetti di metrica....114
Il "motore"....116
La "Base di conoscenza"....116

MIGRA....117
Premesse e generalità....117
I "Componenti"....117
Classificazione della "criticità" dei componenti....119
Componenti a vocazione fisica....120
Responsabilità della compilazione del questionario....122
Componenti a vocazione logica....122
Costruzione e utilizzo del questionario....124
Responsabilità della compilazione del questionario....125
"Minaccia" e "Attacco"....125
"Contromisure"....126
Specifica funzionale....126
Specifica attuativa....127
La metodologia in funzione....128
Appendice al capitolo....133
GLOSSARIO....133

5.
Le contromisure "fisiche"....137
Premesse....137
Centrali di governo e controllo....138
Dispositivi antintrusione....140
Sistemi di protezione perimetrale....141
Sistemi di protezione passiva....141
Reti di recinzione....141
Sistemi antiscavalcamento....142
Sistemi di protezione attiva....142
Cavo con sensori inerziali....143
Fili tesi....143
Tappeti sensibili....143
Sistemi antitaglio/antiscavalcamento....143
Campo elettrostatico....143
Barriera a infrarossi....143
Barriera a microonde....144
Sistemi di protezione periferica....144
Finestre antisfondamento....144
Sistemi fisici di protezione finestrature....145
Porte blindate....145
Serrature....145
Rilevatori di vibrazione....146
Rilevatori a battente....146
Barriera a microonde....146
Barriera ad infrarossi....147
Sistemi di protezione volumetrica....147
Sistemi a raggi infrarossi....147
Sistemi acustici (rottura vetro)....147
Microonde ed ultrasuoni....148
Sistemi a doppia tecnologia....148
Componenti di segnalazione e supporto....148
Combinatori telefonici....148

Sirene di allarme da interno....*148*
Lampeggiatori....*148*
Sirene di allarme da esterno....*149*
Dispositivi per la sorveglianza di oggetto....149
Dispositivi resistenti....*149*
Casseforti....**149**
Armadi di sicurezza....**150**
Rilevatori....150
Rilevatori sismici....*150*
Rilevatori volumetrici capacitivi....*150*
Rilevatori microfonici....*150*
Illuminazione e TVCC....151
Illuminazione perimetrale e periferica....*151*
Illuminazione volumetrica....*151*
Sistema televisivo a circuito chiuso (TVCC)....*151*
Apparati e tecnologie complementari....156
Motion detector digitale....*156*
Visualizzazione plurischermo....*156*
Selettore ciclico....*156*
Stampanti video....*156*
Controllo degli accessi e rilevazione presenze....157
Tornelli....*158*
Barriere motorizzate....*158*
Badge....*158*
Scrittori/trascrittori di badge....*159*
Lettori di badge....*159*
Derivato esterno videocitofonico....*159*
Derivato esterno citofonico....*159*
Il sistema antincendio....160
La rilevazione dell'incendio....*161*
L'estinzione dell'incendio....162
Estintori a mano....*163*
Estintori carrellati....*163*
Manichette per acqua e lance idriche....*164*
Schiumogeni con monitore....*164*
Idranti e naspi....*164*
Impianti a getti d'acqua suddivisa....*165*
Impianti a schiuma....*165*
Sistemi ad anidride carbonica....*165*
Sistemi a saturazione totale....*166*
Sistemi di tipo misto....*166*
Sistemi a polvere chimica....*166*
Evacuatori di fumo e calore....*167*
Isolatori del loop....*167*
Dispositivi complementari....167

Rilevatore antiallagamento.....*167*
Rilevatore di gas.....*167*
Sistemi di supporto alla sorveglianza.....*168*

6.
Le contromisure "logiche".....169
Premesse.....169
Crittografia.....170
Terminologia.....171
Precedenti storici e cifrari classici.....173
Cifrari simmetrici moderni.....177
Le funzioni hash.....183
Il problema dello scambio delle chiavi, la crittografia a chiave pubblica e la firma digitale.....185
Diffie-Hellman.....*185*
L'idea della crittografia a chiave pubblica.....*187*
RSA.....*188*
Utilizzo pratico degli algoritmi di cifratura a chiave pubblica.....*188*
La firma digitale.....*189*
Problematiche relative alla lunghezza delle chiavi.....*190*
Problematiche relative all'utilizzo della crittografia a chiave pubblica.....*191*
Applicazioni avanzate diverse.....192
Tecnologie diverse per la sicurezza logica.....195
Il firewall.....196
Generalità.....*196*
Packet filtering.....*197*
Circuit level gateway.....*200*
Application proxy.....*201*
Architetture complesse.....*201*
Considerazioni generali sulla realizzazione dei firewall.....*205*
Quanto è sicuro un firewall?.....*206*
La difesa in profondità: Intrusion Detection, Network Access Control, data Loss Prevention.....207
IDS.....*207*
Network Access Control.....*209*
Data Loss Prevention.....*209*
Tunnel e VPN.....210
IPSec.....*211*
Transport Layer Security e SSH.....*212*
DTLS.....*212*
SSTP.....*212*
OpenVPN.....*213*
Identity management.....213
Autentificazione forte.....216
Procedimenti operativi.....216

Back-up....*216*
Network security auditing....217
Gestione degli aggiornamenti....218
Vulnerability assessment....219
Penetration testing....220
Modalità di valutazione....221

7.
L'infrastruttura organizzativa....223
Premesse....223
La struttura organizzativa della sicurezza....223
Normative legali e standard di certificazione....225
Metodologie di analisi dei rischi....225
Aspetti sociali e di intelligence, promozione e comunicazione della sicurezza....226
Tecnologie informatiche, crittografia....227
Tecnologie fisiche....228
Redazione delle procedure per la sicurezza....228
Le situazioni di outsourcing....229
I ruoli e le responsabilità....230

8.
La gestione dell'emergenza....233
Premesse....233
Disaster Recovery Plan e Business Continuity Plan....234
Business Impact Analysis e Piano operativo....235
La"Business Impact Analysis"....236
Criticità dei processi aziendali....237
Classificazione delle applicazioni....240
Calcolo del peso delle applicazioni....242
Correlazione tra processi e applicazioni....243
Criticità delle applicazioni....244
La progettazione del PDR....245
Fasi di realizzazione di un PDR....246
FASE 0 - Definizione dei parametri di PDR....*247*
FASE 1 - Definizione dei requisiti del Piano di Disaster Recovery....*251*
CED ridondato....**252**
Hot site aziendale....**252**
Altro CED aziendale....**252**
Centro servizi....**252**
Empty shell....**252**
Coordinamento della riattivazione....**256**
Team di riattivazione....**257**
Team di help-desk....**257**
Team di rientro....**257**
FASE 2 - Progettazione di dettaglio del Piano....*257*
FASE 3 - Implementazione del Piano....*261*

FASE 4 - Test preoperativo....263
FASE 5 - Test operativi e adeguamento periodici....265
Tecnologie moderne e PDR....266

9.
Prospettive e futuro....269
Le condizioni al contorno....269
Il costo dello storage e della banda tendono a zero....269
La mobilità....270
La tendenza alla digitalizzazione di tutto....271
I social network e l'interazione a 360°....272
L'"Internet of Things"....273
La privacy in un mondo che non dimentica nulla....273
Il perimetro non esiste (quasi) più....274
Il rischio insider....275
I rischi della nuvola....276
L'evoluzione delle minacce alla sicurezza: il malware dalla devianza alle operazioni militari....276

TCP/IP....289

Cyber-bibliografia....297
Libri....297
Periodici a stampa....298
Siti Web....298

Indice analitico....301