Manuale di resilienza

di Giancarlo Butti

Manuale di resilienza

EDITORE

ITER Srl – Milano
Via A. Sacchini, 20
20131 Milano (MI)
www.iter.it

ISBN: 9788894441550

STAMPA

Digital Book s.r.l.
Via Karl Marx, 9
06012 Cerbara - Città di Castello (PG)

Prima edizione Aprile 2023

A Carlo, che ha saputo unire genialità, simpatia e altruismo.

Ai nostri piccoli Teddy e Swan

A mia moglie ed a Eros, Chery, Jenny, Hope, Aba

Giancarlo

Giancarlo Butti *(giancarlo.butti@promo.it)*
(LA BS 7799), (LA ISO IEC 27001), CRISC, CDPSE, ISM, DPO, DPO, CBCI, AMBCI

Master in Gestione aziendale e Sviluppo Organizzativo (MIP - Politecnico di Milano).

Referente ESG(*) (Environmental, Social e Governance) e Inclusion del Comitato Scientifico del CLUSIT.

Si occupa di ICT, organizzazione e normativa dai primi anni 80:

- analista di organizzazione, project manager, security manager ed auditor presso gruppi bancari
- consulente in ambito documentale, sicurezza, privacy… presso aziende di diversi settori e dimensioni.

Come divulgatore ha all'attivo:

- oltre 800 articoli su 30 diverse testate
- 26 fra libri e white paper, alcuni dei quali utilizzati come testi universitari
- 27 opere collettive nell'ambito di ABI LAB, Oracle/CLUSIT Community for Security, Rapporto CLUSIT sulla sicurezza ICT in Italia
- relatore in oltre 170 eventi presso ABI, ISACA/AIEA, AIIA, ORACLE, CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF, IKN, TECNA, UNISEF, PARADIGMA…
- già docente del percorso professionalizzante ABI - Privacy Expert e Data Protection Officer
- docente in master e corsi di perfezionamento post-universitario in diversi atenei:
    - Master di II livello in "Data Protection Officer e Diritto della privacy" dell'Università degli Studi Suor Orsola Benincasa - Napoli
    - Corso di Perfezionamento in Data Protection e Data Governance dell'Università degli Studi di Milano
    - Percorso di Alta Formazione Data Protection Officer del Cefriel
    - Master di Specializzazione per Responsabili della Protezione dei Dati Personali dell'UNISEF
    - Percorso DPO e dell'Osservatorio Information Security & Privacy del Politecnico di Milano
    - Analisi e gestione del rischio all'Università Statale di Milano.

Socio di AIEA/ISACA (www.aiea.it – Associazione Italiana Information Systems Auditors), del CLUSIT (www.clusit.it – Associazione Italiana per la Sicurezza Informatica) e di BCI (Business Continuity Institute).

Partecipa a diversi gruppi di lavoro di ABI LAB, di ISACA-AIEA, del CLUSIT…

(*) Già ricercatore nell'ambito delle energie rinnovabili (UNESCO - International directory of new and renewable energy information sources and research centers, 1986)

INDICE

INDICE ..... *v*

PRESENTAZIONE ..... *xv*

Ringraziamenti xv

GUIDA ALLA LETTURA DI QUESTO LIBRO ..... *xvii*

Precedenti pubblicazioni xviii

DEFINIZIONI *1*

Di cosa stiamo parlando 1

Normativa 2

Continuità operativa 2

Resilienza 2

Parametri 3

Standard 4

Continuità operativa 4

Resilienza 4

Parametri 4

Altre definizioni 5

Resilienza 5

Alcuni parametri 8

DORA (Digital Operational Resilience Act) *9*

Perché DORA 9

Aree di intervento 9

Ambito di applicazione 11

Le sanzioni 15

Articolazione della norma 18

LA RACCOLTA DELLE INFORMAZIONI *19*

Tecniche di raccolta dei dati 19

La verifica documentale 20

Fonti dati sulle risorse 21

Le interviste 22

Uso di moduli per la raccolta delle informazioni 22

MISURE DI SICUREZZA DELLA SEDE 24

MISURE DI SICUREZZA DEI LOCALI 26

MISURE DI SICUREZZA DEL CED 28

I RISCHI *31*

Il concetto di rischio 31

Tipologia di rischi 32

Rischi in ambito aziendale....32
Rischi in ambito bancario....33
Rischi di progetto....36
I rischi ICT....37
I rischi di soggetti terzi in carico all'organizzazione....40
Il rischio di terza e quarta parte....41
I limiti del modelli....41
I limiti nella valutazione dell'impatto....43
La valutazione di impatto negli incidenti....43
La valutazione di impatto nella BIA....44
La valutazione di impatto nella analisi dei rischi....44
Documentare le scelte fatte....44
Possibili elementi da considerare nella valutazione di impatto....45

ASSET - PROCESSI - SERVIZI....47

Normativa....47
Gli asset dal punto di vista dell'azienda....49
I beni materiali....50
I beni immateriali....51
La conoscenza....52
Il capitale intellettuale....53
La classificazione delle informazioni....55
Requisiti di sicurezza....56
Rilevanza complessiva....58
I documenti....59
Elementi di un documento....59
I documenti elettronici....59
Il sistema informativo....60
Il ciclo di vita delle informazioni....61
Il capitale umano....62
Competenze/Conoscenze....63
I cataloghi delle competenze....64
Altri asset immateriali....69
La collocazione degli asset aziendali....69
Correlazione fra gli asset....70
Struttura gerarchica....71
Categorizzazione degli asset....71
Cataloghi di asset....76
Le informazioni da raccogliere in ambito ICT....76
Mappatura del sistema informativo....77
Le applicazioni sviluppate dagli utenti (End User Computing)....79
Shadow IT....79
Il livello di analiticità nella mappatura degli asset....79
I servizi....80

I processi 81
I componenti dei processi 82
Le attività 83
I ruoli nei processi e la tabella RACI 84
Le interazioni fra processi 84
Esempi e schede di rilevazione di un processo in ambito servizi 85
Il diagramma SIPOC 87
Il livello di analiticità nella mappatura dei processi 87
Cataloghi di processi 88
Le finalità di trattamento 90
Cataloghi delle finalità 90
Il DPS come strumento di mappatura 93
La rilevazione dei flussi documentali 101
Strumenti 104

LE MINACCE E LE VULNERABILITÀ 107

Gli eventi di minaccia 107
Classificazione delle fonti di minacce 111
Minacce ambientali 111
Minacce industriali 111
Minacce - Guasti 112
Minacce comportamentali 112
Minacce correlate al personale 113
Minacce e requisiti di sicurezza 115
Evoluzione delle minacce 115
Le Vulnerabilità 117
Cataloghi delle minacce e delle vulnerabilità 119
IT - Grundschutz catalogues 120
ENISA - Threat taxonomy 121
NIST 122

GLI SCENARI DI RISCHIO PER LA CONTINUITÀ OPERATIVA 125

Normativa banche 125
Normativa pubblica amministrazione 128
Esempi di scenari, eventi ed asset coinvolti 129
Nuovi rischi - i rischi climatici 131
Esempio di soluzioni 134
Effetti sul modello di continuità operativa 135

LA GESTIONE DEL RISCHIO 137

Standard per la gestione del rischio 137
I principi 138
Il framework 138
Il processo per la gestione dei rischi 139
Metodologie per la gestione del rischio 139

I ruoli nella gestione dei rischi 141

LA VALUTAZIONE DEGLI IMPATTI 143

Correlazione fra impatti 143
I costi di ripristino 146
Valutazione dell'impatto 147
Parametri utili alla valutazione degli impatti 148
Esempi di scale di impatto 149

LA BIA (BUSINESS IMPACT ANALYSIS) 155

Definizione della metodologia con cui eseguire una BIA 162
Modalità di valorizzazione 162
Perimetro 163
Le funzioni operative importanti 164
Periodicità di revisione 167
Modalità di raccolta delle informazioni 167
La conduzione della BIA 168
Individuare gli asset che supportano i processi 169
Definire i parametri di valutazione quali/quantitativi 170
Determinazione del tempo massimo di indisponibilità (MTPD) 174
Processi svolti da diverse unità organizzative 174
Determinazione dell'RTO 175
Punti di attenzione 175
Individuare gli asset minimi necessari a erogare un processo 177
La valutazione delle correlazioni 178
La classificazione dei processi 179
La valutazione dell'RPO 180
Punti di attenzione 180
La valutazione di altri parametri significativi 181
Punti di attenzione 181
Analisi del rischio e bia 182

LA VALUTAZIONE DELLA PROBABILITÀ 185

Metodologie per la valutazione della probabilità 186
Determinazione della probabilità di un evento 186
Correlazione fra probabilità 191
Le possibili fonti dati per la valutazione della probabilità 192
Uso di dati storici e loro profondità 195
Altri fattori 196

L'ANALISI DEI RISCHI 199

Un approccio all'analisi del rischio a più livelli 199
Terminologia dell'analisi dei rischi 202
Metodologie per l'analisi dei rischi 204
Un confronto tra i 2 approcci 206

Aspetti trasversali nella analisi dei rischi 207
Documentare l'analisi dei rischi 207
Sinergie 208
Fasi dell'analisi dei rischi 209
Rischio: correlazione fra impatti e probabilità 211
La raccolta dei dati 212
Scale qualitative 212
Scale quantitative 214
Il problema della rappresentazione dei valori stimati 214
Calcolo del rischio quantitativo 215
Somma o moltiplicazione? 217
Conclusioni 218
Evoluzione da qualitativo a quantitativo 218
Da IT Security a Cybersecurity: standard ISO/IEC 27032:2012 219
Misura del rischio Cybersecurity 221
Concetto di misura 221
Definizione di misura 221
Oggetto della misura 221
I metodi di misura 222
Il rilievo statistico dei dati raccolti 223
Da Qualitativo a Quantitativo: sostituzione uno-a-uno 224
L'esperto come strumento della valutazione 224
La matematica dell'incertezza: il metodo Monte Carlo 225
Loss exceedance curve 228
Visualizzare il rischio 228
La tolleranza al rischio: come descriverla in termini statistici 228
Supporto alle decisioni: ROSI 229
Come migliorare le stime 229
La stima dell'impatto 229
La taratura delle stime di probabilità 230
Riduzione dell'incertezza con metodi statistici 231
Set di utility fogli di calcolo personalizzate 233
Analisi dei rischi dal punto di vista del GDPR 234
La granularità dell'analisi 235
La valutazione della probabilità 236
La valutazione dell'impatto 238
Valutazione dell'impatto complessivo 239
La valutazione del rischio 240
Determinazione analitica della valutazione di impatto 241
Il contesto del trattamento 241
Facilità di identificazione 242
Circostanza della violazione 243
Analisi dei rischi in base agli artt. 24 e 25 243
L' analisi del rischio dal punto di vista dell'organizzazione 244

Il rischio risarcitorio....245
Il rischio sanzionatorio....247
Il trattamento del rischio dal punto di vista del GDPR....251

AGGREGAZIONI E CORRELAZIONI DEI RISCHI....253

Somma dei rischi e calcolo della rischiosità totale....253
Rischi indipendenti....254
Rischi correlati....254
Perché un approccio "rischio totale"....255
Riduzione dei rischi per le categorie di minacce....255
Evoluzione rischio per categoria....257
Diagramma di Pareto....257

IL TRATTAMENTO DEL RISCHIO....259

L'attivazione delle contromisure....261
Il trasferimento del rischio....263
Il ciclo dell'analisi del rischio....264

LE MISURE DI SICUREZZA....265

Normativa....265
Classificazione delle misure di sicurezza....271
Ciclo di vita delle misure di sicurezza....272
Coerenza nelle contromisure....273
Differenza nelle contromisure....275
Framework di sicurezza....276
Cataloghi delle misure di sicurezza....291
MISURE DI CARATTERE GENERALE....291
RAPPORTI CON IL PERSONALE....292
RAPPORTI CON ESTERNI (fornitori/outsourcer)....293
GESTIONE DELLA SICUREZZA....295
GESTIONE DEGLI ACCESSI FISICI/LOGICI AGLI ASSET....295
SICUREZZA FISICA....297
VIDEOSORVEGLIANZA....300
SICUREZZA LOGICA....302
GESTIONE DEI DOCUMENTI....312
Architettura zero trust....313
Risorse esterne....314
ENISA - Handbook on Security of Personal Data Processing....315
CyberSecurity Framework Nazionale....316
IT - Grundschutz catalogues....318
NIST Special Publication 800-53 (Rev. 4)....319
NIST 800 53 REV. 5....321
Misure di sicurezza - Policy e Procedure....322
AUSTRALIAN GOVERNMENT INFORMATION SECURITY MANUAL....322
SANS INSTITUTE....326

MISURARE 329
Normativa 329
Come quantificare l'efficacia di un Framework di Controlli di Cybersecurity 330
Un'utile analogia 331
Ontologia FAIR con i fattori di rischio 332
Alcune osservazioni sulle tipologie di controllo 334
Panoramica del modello CAM 335
Come procedere 337
Conclusione e passi successivi 338
Risorse aggiuntive 339
Metriche e misure e loro caratteristiche 339
Tipologia di misure di sicurezza 342
Implementation Measures 342
Effectiveness/efficiency measures 342
Impact Measures 343
Lead e Lag indicators 343
Metriche di resilienza 344
Fase di preparazione 345
Fase di erogazione del servizio: 348
Fase di recupero 348
Misurare i processi ICT 349
Cataloghi di misure in ambito sicurezza 350
DiSIEM 350
Diversity-enhancements for SIEMs D3.1 Security Metrics and Measurements 350
NIST Special Publication 800-55 Revision 1 - Performance Measurement Guide for Information Security 351
Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring 354
Software Engineering Institute 355
Annex B: Board IT metrics which are applicable to cyber-resilience (estratto) 358
Annex C: Cyber-resilience metrics 360
Service level agreement 361
Gestione impiantistica industriale – parte elettrica 361
Gestione Sicurezza Fisica 361
Security maturity model 362
Building Security In Maturity Model (BSIMM) Version 7 362
Cyber Security Capability Maturity Model (CMM) – V1.2 363
Cyber resilience oversight expectations for financial market infrastructures 365

INCIDENTI 367
Normativa 367
Gli incidenti nell'ambito della resilienza operativa 375
Esempi di incidenti 376
Incidenti in ambito ICT 377

Soggetti che possono segnalare un incidente (o permettere di prevenirlo) 380
Canali di segnalazione 381
L'individuazione di segnali da strumenti 382
I livelli di valutazione degli incidenti, i criteri e le metriche 383
Escalation di incidenti che coinvolgono processi critici 384
Procedura di gestione degli incidenti 390
I ruoli nella gestione degli incidenti 390
Composizione dei vari team 392
Livello di maturità nella gestione degli incidenti 393

IL PIANO DI BC 395

Normativa 395
I contenuti del piano 402
Intervallo temporale di riferimento 403
Piani alternativi 404
L'organizzazione della documentazione a supporto del piano 404
Piani settoriali e documenti operativi 404
La gestione dei documenti del piano di BC 406
L'aggiornamento del piano di BC 407
Resilienza by design 408
Disponibilità della documentazione in caso di crisi 408
Punti di attenzione: BC 409
Rischi residui 410
Esempi di indici di piani 410
Esempio di piano di DR 411
I piani settoriali 413
I piani per l'indisponibilità del sistema informativo 415
I ruoli della continuità operativa 416
Il coinvolgimento del personale 420
Le comunicazioni 421

LA GESTIONE DELLA CRISI 423

Dall'incidente alla gestione della emergenza e della crisi 424
Lo stato di crisi 427

LE SOLUZIONI PER IL SISTEMA INFORMATIVO 429

Normativa 429
Indisponibilità del sistema informativo 434
Alcuni parametri utili a predisporre le soluzioni 437
Reliability (affidabilità) 437
Availability (disponibilità) 437
Esempi di applicazione 438
Punti di attenzione 442
Alta affidabilità (alta disponibilità) 443
Punti di attenzione 444

Alta affidabilità (alta disponibilità) 444
Soluzioni di Disaster Recovery 446
Punti di attenzione: DR 449
Possibili requisiti del sito di DR 451
Attacco cyber 454
Normativa 454
Effetti di un attacco ransomware 456
Fasi di un attacco ransomware 458
Azioni di mitigazione preventive e successive ad un attacco 461
Azioni preventive 461
Interventi dopo un attacco 462
Riepilogo di possibili misure preventive e di recovery 464
Policy per il backup 465

LE SOLUZIONI 469

Normativa 469
Le soluzioni per essere resilienti 474
Responsabilità e rispetto delle normative 478
Gli aspetti finanziari 479

FORNITORI E OUTSOURCER 481

Normativa 481
Azioni da svolgere nella relazione con i fornitori 491
La criticità di un fornitore 492
I rischi dei fornitori 493
La scelta del fornitore 498
La valutazione puntuale del fornitore 503
AGID - Linee guida - La sicurezza nel procurement ICT 504
Gli aspetti contrattuali 505
CONSIP - Contratto Quadro - Clausole contrattuali 513
CONSIP – Contratto quadro 514
I termini di un contratto 515
Monitoraggio degli SLA e della sicurezza 521
Exit Strategy ed Exit Plan 524
I fornitori in ambito cloud 528
Ripartizione di responsabilità cliente - fornitore nei modelli Cloud 530
La valutazione del fornitore da parte di enti Ufficiali 532
CIRCOLARE N. 2 2018 533
Criteri per la qualificazione dei Cloud Service Provider per la PA 533
FedRAMP High Readiness Assessment Report (RAR) Template 534
I market place 537
La valutazione volontaria 538
Gli schemi SOC 539
Lo schema C5 539

VERIFICHE ***541***
I test di resilienza 541
Tipologie di test di resilienza 552
Test e verifiche della continuità operativa 553
Tipologie delle verifiche teoriche e pratiche 557
Verifica teorica 558
Walk-through strutturato 558
Tattico 558
Simulazione 558
I test degli impianti 558
I componenti del sistema informativo 560
I Ced 561
Alta affidabilità 562
Disaster Recovery 563
Attacco cyber 565
Malfunzionamenti 565
Indisponibilità degli asset essenziali 566
Test dei Fornitori e degli Outsourcer 567
Punti di attenzione 568
Guida all'esecuzione dei test 569
Check list di spunta dei test 569
Revisione degli esiti dei test 570
La pianificazione dei test 570
Le verifiche delle strutture di controllo 571

LA FORMAZIONE ***575***
Normativa 575
Formazione e consapevolezza 579
La formazione in ambito sicurezza 581
Norme di comportamento 582

GLI STANDARD ***591***
ISO Sicurezza 593

LE NORMATIVE ***599***

ARTICOLI ***601***
cybersecurity360 (www.cybersecurity360.it) 601
ISCOMM – MISE (atc.mise.gov.it) 602
sicurezzanazionale.gov.it 602
rivista cybersecurity trends (cybertrends.it) 602

PRESENTAZIONE

Quest'ultima opera di Giancarlo Butti è sicuramente una delle più complete sui temi della resilienza e della continuità operativa, in particolare in ambito finanziario.

Ancora una volta Giancarlo, che recentemente è entrato nel comitato scientifico del Clusit, ha dato alla luce un manuale particolarmente utile per la gestione dei rischi, in linea con il **Digital Operational Resilience Act** (DORA) e il testo costituisce una buona base per la sua corretta implementazione, anche per le parti della normativa non ancora pubblicate.

Paolo Giudice
Fondatore e Segretario Generale del Clusit
(Associazione Italiana per la Sicurezza Informatica)

RINGRAZIAMENTI

Un ringraziamento va a Paolo per la sua presentazione, ad Alberto, per aver contribuito ancora una volta ad una mia pubblicazione e a Daliso, business continuity manager con cui abbiamo condiviso lunghi anni di esperienza nella gestione, test e verifiche negli ambiti della continuità operativa.

GUIDA ALLA LETTURA DI QUESTO LIBRO

La finalità di questo libro è quella di dare una visione il più possibile complessiva dei temi trattati, con particolare riferimento alla resilienza ed alla continuità operativa.

L'obiettivo è quello di fornire al lettore tutti gli strumenti che possano consentire ad una organizzazione di:

- gestire i propri rischi
- gestire i rischi di soggetti terzi derivanti dall'attività dell'organizzazione (ad esempio gli interessati di cui l'organizzazione tratta i dati)
- gestire i rischi derivanti da terze e quarte parti
- individuare e implementare adeguate misure tecnico/organizzative per la mitigazione dei rischi e per rendere un'organizzazione sempre più resiliente
- gestire la continuità operativa.

Il tipo di approccio è molto pratico e parte dagli elementi base, quali l'individuazione degli asset che sono da supporto ai processi ed ai servizi erogati dalla organizzazione, nonché delle correlazioni esistenti fra tutti questi elementi.

Vengono poi analizzati il concetto di rischio e gli elementi che entrano in gioco nella valutazione dei rischi (minacce, vulnerabilità…), i criteri con cui determinare impatti e probabilità e le diverse metodologie qualitative e quantitative per la sua determinazione, nonché i limiti di tali metodologie.

Per ogni elemento considerato vengono presentati elenchi specifici, sia interni al libro, sia rimandando a pubblicazioni esterne, facilmente reperibili e consultabili.

Analogamente vengono presentate metriche e criteri di misura.

Nell'ambito della gestione della continuità operativa capitoli specifici sono dedicati alla gestione degli incidenti ed alla BIA, agli scenari di rischio che è opportuno considerare e alle relative soluzioni, alla redazione del Piano di continuità operativa, ai relativi test ed alla gestione della crisi.

Tutti gli argomenti trattati sono in linea con le specifiche richieste formulate nel nuovo regolamento sulla resilienza operativa, il **Digital Operational Resilience Act,** nel resto del testo **DORA** e quindi il testo costituisce una base per la sua corretta implementazione anche per le parti della normativa non ancora pubblicata.

Il testo analizza infatti gli attuali standard, buone pratiche e normative che trattano gli argomenti per i quali **DORA** rimanda a documenti tecnici non ancora formalizzati.

La maggior parte dei capitoli del testo parte con una serie di richiami normativi, nella totalità dei casi dedicati al mondo finanziario.

Questa scelta è legata a 2 diversi fattori.

Il primo è che il mondo finanziario è uno di quelli maggiormente regolamentati in questo ambito e di conseguenza è ricco di normative che dai primi anni duemila forniscono indicazioni ai soggetti vigilati.

Il secondo aspetto, più rilevante, è che tali normative entrano anche in dettagli molto analitici e quindi forniscono delle indicazioni pratiche applicabili in qualunque settore.

I testi delle normative sono presentati evidenziando gli aspetti più salienti in modo tale da facilitare il lettore nella loro lettura e comprensione; preferisco da sempre questo tipo di approccio rispetto ad una estrapolazione dei contenuti, in quanto tale pratica rischia molto spesso di decontestualizzare un concetto, falsandone l'interpretazione.

Non necessariamente sono presentati i testi più recenti delle normative; la loro scelta è funzionale alle finalità del libro e non a rappresentare una situazione normativa aggiornata, che diventerebbe rapidamente obsoleta, in considerazione della frequenza con cui i vari enti preposti rilasciano nuove normative.

Si è prestata cura nel riportare il testo delle normative, ma al riguardo quanto riportato non ha alcun valore ufficiale; per una corretta ed esaustiva rappresentazione dei testi è necessario consultare i documenti ufficiali.

Per motivi di riservatezza e rispetto dei soggetti coinvolti il testo non contiene volutamente riferimenti a casi pratici vissuti in prima persona, ma è grazie all'esperienza così maturata che nascono i contenuti di questo libro.

Personalmente mi occupo di privacy e sicurezza da oltre 25 anni e di business continuity da quando Banca d'Italia ha pubblicato la sua prima circolare circa 20 anni fa.

Partecipo inoltre all'Osservatorio sulla business continuity di ABI LAB praticamente dalla sua costituzione.

PRECEDENTI PUBBLICAZIONI

Questo libro è basato sulle mie precedenti pubblicazioni:

- Sicurezza totale
- Sicurezza totale 4.0 - L'ABC sulla Physical Cyber Security per i DPO e le PMI (e non solo)
- Governance del rischio - Dall'analisi al reporting e la sintesi per la Direzione
- Dalla carta alle nuvole

Tutti editi dalla ITER.

Alcuni paragrafi sono tratti dai miei articoli su Toolnews, e di questo ringrazio Alessandro Giacchino.

Le parti dedicate alle valutazioni del rischio quantitativo e alla metodologia FAIR sono state sviluppate principalmente da Alberto Piamonte.

La parte dedicata alla formazione è stata sviluppata con il contributo di Daliso Gobbetti.