INDICE SOMMARIO

Prefazione 11

CAPITOLO 1
LE CLASSIFICAZIONI PREVISTE DAL DECRETO LEGISLATIVO N. 138/2024

1. Cenni introduttivi 15
2. Ambito di applicazione 19
3. Criteri di inclusione 20
4. Segue. La differenza tra soggetti essenziali e importanti 21
5. Criteri principali 22
6. La classificazione dei soggetti e i parametri dimensionali 23
7. Imprese associate, collegate 24
8. Attività e servizi intragruppo 26
9. Inclusione automatica di organizzazioni appartenenti a gruppi di imprese (art. 3, comma 10, del decreto NIS) 26
10. Calcolo delle soglie 27
11. La clausola di salvaguardia 30
12. Criteri per il calcolo delle dimensioni aziendali 31
13. Pubbliche amministrazioni 32
14. Organizzazioni estere (UE ed extra-UE) 34

CAPITOLO 2
LA CATENA DI APPROVVIGIONAMENTO E LA SICUREZZA NELLA *SUPPLY CHAIN*

1. Cenni introduttivi 37
2. L'importanza della sicurezza nella supply chain 38
3. Gestione operativa della supply chain 38
4. Gestione del rischio nella catena di approvvigionamento: linee guida operative 39
5. Focus operativo sui fornitori critici 40
6. Soluzioni integrate per la gestione dei rischi 41

CAPITOLO 3

LA RESPONSABILITÀ DEGLI ORGANI DI AMMINISTRAZIONE E DIRETTIVI NELLA CIBERSICUREZZA

1. Cenni introduttivi 43
2. Il nuovo paradigma della governance nella cibersicurezza 44
2.1. La responsabilità degli organi di gestione 44
2.2. Responsabilità specifiche degli organi di governance 44
2.3. Implementazione delle misure di sicurezza 45
3. Formazione e cultura della sicurezza 45
3.1. Requisiti formativi 45
3.2. Modalità formative 46
3.3. Promozione di una cultura della sicurezza 46
4. Gestione operativa della sicurezza 46
5. La colpa di organizzazione 47
5.1. Premesse 47
5.2. La colpa di organizzazione nel contesto della sicurezza informatica 47
5.3. Cibersicurezza come strumento di prevenzione e valorizzazione aziendale 48
6. Responsabilità degli organi apicali per il difetto di adeguata organizzazione 48
6.1. Chi impersonifica l'imprenditore nelle imprese collettive 48
6.2. Le conseguenze civili della colpa di organizzazione 49
6.3. Azioni di Responsabilità 51
6.4. Impatti sul Patrimonio Sociale 51
6.5. Conseguenze amministrative della colpa di organizzazione 52
6.6. Conseguenze penali della colpa di organizzazione 53

CAPITOLO 4

L'AGENZIA PER LA Cibersicurezza NAZIONALE, IL SERVIZIO REGOLAZIONE, IL CSIRT

1. L'Agenzia per la Cibersicurezza Nazionale 55
1.1. Profilo dell'Agenzia 55
1.2. Funzioni e competenze 56
1.3. Certificazione e standard 56
1.4. Il modello collaborativo ACN-imprese 56
2. Il Servizio Regolazione 57

2.1. Premesse 57
2.2. Funzioni principali 57
2.3. Interazione con i soggetti regolati 57
2.4. Impatto e risultati 58
3. Il CSIRT 58
3.1. Premesse 58
3.2. Monitoraggio e prevenzione 58
3.3. Gestione degli incidenti e risposta 58
3.4. Cooperazione e sensibilizzazione 59

CAPITOLO 5

LA PIATTAFORMA ACN E I RUOLI NIS: POC, SOSTITUTO, SEGRETERIA E OBBLIGHI DEGLI ORGANI DIRETTIVI

1. Portale ACN e Servizi NIS 61
2. Il Punto di Contatto (POC) 62
3. Il Sostituto Punto di Contatto 63
4. La Segreteria 64
5. Il Referente CSIRT 65
6. Il Rappresentante NIS nell'Unione 67
7. Gli Obblighi degli Organi di Amministrazione e Direttivi 68
8. Cesnimento e associazione delle utenze 69
9. Registrazione dei Soggetti NIS 70
10. Verifiche e Clausola di Salvaguardia 72
11. Elaborazione dell'Elenco dei Soggetti NIS 73
12. Aggiornamento Annuale (15 aprile - 31 maggio) 74
13. Elenco degli Organi di Amministrazione e Direttivi 74
14. Aggiornamento Continuo 75

CAPITOLO 6

ANALISI DEL RISCHIO - COME VALUTARE LE VULNERABILITÀ AZIENDALI

1. Cenni introduttivi 77
2. L'analisi del rischio 78
3. I principi dell'analisi del rischio 78
4. Fasi dell'analisi del rischio 79
5. Il processo di gestione del rischio: identificazione, valutazione, trattamento 80
6. Monitoraggio e revisione continua 81

CAPITOLO 7

LE MISURE DI SICUREZZA NELLA DIRETTIVA NIS2

1. Requisiti orizzontali 83
2. Requisiti settoriali 85
3. I dieci ambiti di intervento 87
3.1 Gestione del rischio 87
3.2 Gestione degli incidenti 88
3.3 Continuità operativa, disaster recovery e gestione delle crisi 89
3.4 Sicurezza della supply chain 90
3.5 Sicurezza dei sistemi ICT 90
3.6 Gestione delle vulnerabilità 91
3.7 Fattore umano e consapevolezza 93
3.8La crittografia 93
3.9 Sicurezza delle risorse umane 94
3.10 Autenticazione forte e gestione degli accessi 95
4. Attuazione e obblighi di base 97
4.1 Premessa sull'attuazione delle misure di sicurezza di base 97
4.2 Soggetti obbligati all'adozione delle misure di sicurezza di base 97
4.3 Le misure da adottare 98
4.4 Termini per l'adozione delle misure 98
4.5 La natura "di base" delle misure di sicurezza 99
4.6 Struttura delle misure di sicurezza 99
4.7 – Verso l'attuazione operativa delle misure 92

CAPITOLO 8

LE LINEE GUIDA ACN DI SETTEMBRE 2025: DAL QUADRO TEORICO ALL'ATTUAZIONE OPERATIVA

1. Quadro generale 102
2. Ambito di applicazione 102
3. L'approccio basato sul rischio 102
4. Per almeno i sistemi informativi e di rete rilevanti 103
4.1 In accordo agli esiti della valutazione del rischio (ID.RA-05) 103
4.2 Fatte salve motivate e documentate ragioni normative e tecniche 104
4.3 Forniture con potenziali impatti sulla sicurezza 104
4.4 Un sistema proporzionato e dimostrabile 105

5. Tipologia dei requisiti 105
6. Evidenze documentali 106
6.1 Elenchi 106
6.2 Inventari 106
6.3 Piani 107
6.4 Politiche 107
6.5 Procedure 108
6.6 REgistri 108
6.7 Approvazione e aggiornamento 108
6.8 La funzione strategica della documentazione 109
7. Modalità di attuazione 109
8. Un processo di miglioramento continuo 110

CAPITOLO 9

MISURE DI SICUREZZA DI BASE PER I SOGGETTI IMPORTANTI

1. Governo (Govern) 113
2. Identificazione (Identify) 119
3. Protezione (Protect) 124
4. Rilevamento (Detect) 130
5. Risposta (Respond) 131
6. Ripristino (Recover) 133

CAPITOLO 10

MISURE DI SICUREZZA DI BASE PER I SOGGETTI ESSENZIALI

1. Governo (Govern) 136
2. Identificazione (Identify) 144
3. Protezione (Protect) 150
4. Rilevamento (Detect) 159
5. Risposta (Respond) 160
6. Ripristino (Recover) 162

CAPITOLO 11

LA SEGNALAZIONE DEGLI INCIDENTI SIGNIFICATIVI

1. Quadro generale 163
1.1 Cenni introduttivi 163
2. Definizione di incidente significativo 164
3. Quadro normativo di riferimento 164
4. Tipologie di incidenti significativi 165
5. Evidenza dell'incidente 166
6. Tempistiche e fasi di comunicazione 166
6.1 Aggiornamento continuo 167
6.2 Conferma di ricezione 167
7. Quasi incidenti (near miss) e notifiche volontarie 168
7.1 Procedura per le notifiche volontarie 168
7.2 Incentivi alla segnalazione volontaria 168
7.3 Obblighi organizzativi 169
8. Referente CIRST e sostituto 169
9. Coordinamento con la protezione dei dati personali 169
10. Responsabilità e conservazione delle evidenze 170
11. Sintesi operativa 170

CAPITOLO 12

D.LGS. 138 DEL 2024 ED IL RAPPORTO CON IL REGOLAMENTO UE 2016/679 (GDPR)

1. Cenni introduttivi 174
2. Le connessioni tra GDPR e NIS2 174
3. Implicazioni pratiche per le organizzazioni 175
4. Il DPO nel contesto del D.lgs. 138/2024 175

CAPITOLO 13

SANZIONI AMMINISTRATIVE E REPUTAZIONALI

1. Cenni introduttivi 179
2. Sanzioni per imprese ed enti 179
2.1 Imprese 179
2.2. Enti pubblici 180

3. La responsabilità erariale nel contesto NIS 2 181
4. Responsabilità civile 182
4.1. Premesse 182
4.2 Responsabilità civile delle imprese 182
4.3. Responsabilità civile degli enti pubblici 183
5. Conseguenze reputazionali e operative 183
6. Obbligo di segnalazione e rischi di crisi aziendale 184
7. Reputazione aziendale e implicazioni del decreto NIS 2 184
7.1 Inquadramento 184
7.2. Impatti per le imprese 184
7.3. Impatti sugli enti pubblici 185

CAPITOLO 14

LA TIMELINE DI RECEPIMENTO E ATTUAZIONE DELLA NIS 2

1. Cenni introduttivi 187
2. Recepimento 187
3. Prima Fase Attuativa 188
4. Seconda Fase Attuativa 189
5. Terza Fase Attuativa 189

CAPITOLO 15

REGOLAMENTO (UE) 2022/2554 – DORA

1. Cenni introduttivi 191
2. La funzione di controllo dei rischi ICT 192
3. Comunicazione all'autorità competente per l'utilizzo di servizi ICT a supporto di funzioni essenziali o importanti 193
4. Segnalazione dei gravi incidenti ICT e delle minacce informatiche significative 194
5. *Test* avanzati di penetrazione basati sulle minacce 195

MODELLI DOCUMENTALI

1. Verbale CdA per rec Piattaforma ACN 197
2. Verbale CdA per Azienda fuori perimetro 201
3. Supply Chain - Clausole Contrattuali 205
4. Richiesta Compliance NIS2 210
5. Attestazione Compliance 213
6. Verbale CdA 217
7. Organigramma NIS - Media Impresa 221
8. Funzionigramma NIS2 - Media Impresa Soggetta 225
9. Verbale di Costituzione del Team di Risposta alle Crisi 231
10. Denuncia degli Incidenti di Sicurezza Informatica 235
11. Politica di Analisi dei Rischi e di Sicurezza 241
12. Atto di Delega 253
13. Verbale CdA - DPO 259

Q-Check List **263**