CUPRINS

Despre autori 5
Cuvânt înainte 15
Mulţumiri 19
Introducere 23

Capitolul I. Considerații generale 27
I.1. Ce este Directiva NIS şi de ce este importantă? 29
I.1.1. Directiva 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora 30
I.1.1.1. Studiu de evaluare a Directivei 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora 32
I.2. De ce este importantă Legea nr. 362/2018 de transpunere a Directivei NIS în România? 41
I.2.1. Transpunerea Directivei în România 42
I.3. Cine este vizat de Legea nr. 362/2018 de transpunere în România a Directivei NIS? ... 46

Capitolul II Directoratul Național de Securitate Cibernetică - DNSC 49
II.1. Responsabilități şi principii ale Directoratului Național de Securitate Cibernetică 52
II.1.1. Responsabilitățile DNSC 52
II.1.2. Principiile DNSC 53
II.2. Obiectivele Directoratului Național de Securitate Cibernetică 54
II.3. Funcțiile şi atribuțiile Directoratului Național de Securitate Cibernetic 55
II.3.a. Strategie şi planificare 55
II.3.b. Funcția de autoritate competentă la nivel național de reglementare, supraveghere şi control 56
II.3.c. Funcția de CSIRT național 56
II.3.d. Funcția de CSIRT guvernamental 57
II.3.e. Funcția de coordonare, implementare, îndrumare şi sprijin a CSIRT-urilor sectoriale 58
II.3.f. Funcția de echipă de răspuns la incidente de securitate cibernetică pentru produse şi servicii informatice utilizate în cadrul sectorului guvernamental 58
II.3.g. Funcția de alertare, prevenire, conştientizare şi instruire 58
II.3.h. Funcția de cooperare şi colaborare 59
II.3.i. Funcția de autoritate națională de certificare privind securitatea cibernetică 60
II.3.j. Funcția de asigurare a conformității şi abordării unitare a securității cibernetice în cadrul infrastructurilor cibernetice 60
II.3.k. Funcția de reprezentare 61
II.3.l. Funcția de cercetare-dezvoltare 61
II.3.m. Funcția de analiză şi prognoză 61
II.3.n. Funcția de identificare, evaluare, monitorizare şi atenuare a riscurilor cibernetice la nivel național 61
II.3.o. Funcția de centru național de gestionare a crizelor de natură cibernetică pe timp de pace 62
II.3.p. Funcția de evaluare a securității cibernetice a noilor tehnologii 62
II.3.q. Funcția de evaluare şi certificare 62
II.3.r. Funcția de educație şi pregătire în domeniul securității cibernetice 63
II.3.s. Funcția de management al proiectelor şi serviciilor 63
II.4. Atribuțiile conducerii Directoratului Național de Securitate Cibernetic 63
II.4.1. Atribuții ale conducerii DNSC 64

II.4.1.1. Atribuțiile directorului DNSC....64
II.4.2. Comitetul director al DNSC....64
II.4.2.1. Atribuțiile și competențele Comitetului director al DNSC....65
II.4.3. Comitetul de reglementare....65
II.4.4. Finanțare....66
II.4.5. Autorizarea laboratoarelor civile....67
II.4.5.1. Activitatea de verificare a laboratoarelor civile....67
II.5. Organizarea Registrului operatorilor de servicii esențiale....69
II.5.1. Constituirea registrului....69
II.5.2. Utilizarea registrului....69
II.5.2.1. Reguli generale privind înscrierea în ROSE, modificarea, radierea și protecția informațiilor înscrise....70

Capitolul III Operatorii de servicii esențiale și furnizorii de servicii digitale....71
III.1. Operatorii de servicii esențiale....73
III.1.1. Înscrierea în Registrul operatorilor de servicii esențiale....74
III.1.2. Radierea din Registrul operatorilor de servicii esențiale....75
III.1.3. Atribuțiile Responsabilului NIS - OSE....75
III.1.4. Obligațiile operatorilor de servicii esențiale....76
III.2. Furnizorii de servicii digitale....77
III.2.1. Obligațiile furnizorilor de servicii digitale....77
III.2.2. Atribuțiile Responsabilului NIS - FSD....79
III.3. Echipele de intervenție în caz de incidente de securitate informatică....79
III.3.1. Obligațiile echipelor de intervenție în caz de incidente de securitate informatică....79

Capitolul IV Etapele implementării prevederilor Legii nr. 362/2018....81
IV.1. Principiile Legii nr. 362/2018....83
IV.2. Procesul de identificare a operatorilor de servicii esențiale (OSE)....83
IV.2.1. Etapa 1. Identificarea serviciilor esențiale....85
IV.2.1.1. Pasul 1 - Catalogarea importanței serviciului....86
IV.2.1.2. Pasul 2 - Identificarea modului de furnizare a serviciului....87
IV.2.1.3. Pasul 3 - Stabilirea efectului de perturbare a serviciului în cazul producerii unui incident....88
Faza 1. Evaluarea în funcție de criteriile intersectoriale....90
Concluzii privind evaluarea gradului de perturbare în funcție de criteriile intersectoriale....96
Faza a 2-a. Evaluarea în funcție de criteriile sectoriale și valorile de prag....96
Concluzii privind evaluarea gradului de perturbare în funcție de criteriile sectoriale specifice....107
IV.2.2. Etapa 2. Notificarea DNSC de către operatorii de servicii esențiale....107
IV.2.3. Etapa 3. Evaluarea și înscrierea operatorilor de servicii esențiale....108
IV.3. Procesul de identificare a furnizorilor de servicii digitale (FSD)....109
IV.3.1. Etapa 1. Identificarea serviciilor digitale furnizate....111
IV.3.1.1. Pasul 1 - Stabilirea categoriei organizaționale....111
IV.3.1.2. Pasul 2 - Identificarea serviciului digital furnizat....112
IV.3.1.3. Pasul 3 - Stabilirea categoriei serviciului digital furnizat....113
IV.3.2. Etapa 2. Comunicarea datelor furnizorului de servicii digitale la DNSC....114
IV.3.3. Etapa 3. Evidența furnizorilor de servicii digitale....114
IV.3.3.1. Modificări și completări privind evidența furnizori de servicii digitale....115
IV.3.3.2. Radierea furnizorilor de servicii digitale din evidență....115

Capitolul V Măsuri tehnice şi organizatorice de securitate 117
V.1. Cerințele minime de securitate pentru asigurarea securității rețelelor şi sistemelor informatice 119
V.1.1. Notificarea incidentelor de securitate 119
V.1.1.1. Termenele de notificare 120
V.1.2. Managementul incidentelor de securitate 120
V.1.3. Auditul de securitate a rețelelor şi sistemelor informatice aparținând operatorilor de servicii esențiale sau furnizorilor de servicii digitale 121
V.1.4. Autorizarea echipelor CSIRT ce deservesc rețele şi sisteme informatice din categoria serviciilor esențiale şi serviciilor digitale 122
V.2. Întocmirea şi gestionarea procedurilor documentate 123
V.2.1. Gestionarea procedurilor documentate 123
V.2.2. De ce avem nevoie de proceduri documentate? 126
V.2.3. Cum se realizează o procedură documentată? 126
V.2.4. Stabilirea activităților procedurale 127
V.2.5. Elaborarea procedurilor documentate 128
V.2.5.1. Conținutul propriu-zis al procedurii 128
V.2.5.2. Descrierea procedurii 129
V.2.5.2.1. Recomandări privind descrierea corectă a procedurii 129

Capitolul VI Controlul îndeplinirii obligațiilor de securitate şi aplicarea sancțiunilor 133
VI.1. Cerințele minime de asigurare a securității rețelelor şi sistemelor informatice 135
VI.1.1. Guvernanță 135
VI.1.2. Protecție 139
VI.1.3. Apărare cibernetică 143
VI.1.4. Reziliență 145
VI.2. Aplicarea sancțiunilor 148

Capitolul VII Propunerea de Directivă NIS 2.0 şi implicațiile ei majore 169
VII.1. Obligația de independență instituțională a DNSC față de entitățile stabilite prin Directiva NIS 2.0 171
VII.2. Modificările aduse de Directiva NIS 2.0 172
VII.2.1. Directiva NIS 2.0 şi Legea nr. 362/2018 se vor aplica şi administrației publice 173
Capitolul VIII Planul de răspuns la incidente de securitate 177
VIII.1. Considerații generale 179
VIII.2. Etapele unui plan de răspuns la incidente de securitate 179
VIII.2.1. Cum recunoaştem un incident de securitate? 180
VIII.2.2. Echipa de management a incidentelor de securitate 180
VIII.2.3. Cronologia evenimentelor în cazul unui incident de securitate 181
VIII.2.4. Descoperirea şi raportarea unui incident de securitate 182
VII.2.4.1. Când se consideră că operatorul „a luat la cunoştință" despre producerea unui incident de securitate? 182
VIII.2.5. Tipuri de incidente care ar trebui raportate 183
VIII.2.6. Identificarea incidentelor de securitate 185
VIII.2.7. Implicarea departamentelor de management şi IT / conformitate 185
VIII.2.8. Notificările în regim de urgență 188
VIII.2.9. Activități inițiale 188
VIII.2.9.1. Izolarea incidentului de securitate 189
VIII.2.9.2. Cyber Asigurări şi externalizarea serviciilor de răspuns la incidente de securitate 190
VIII.2.9.3. Documentarea şi deschiderea rapoartelor de incident de securitate 190

VIII.2.9.4. Înființarea echipei de management a incidentului şi analiza planurilor alternative ... 190
VIII.2.10. Activitățile post incident ... 191
VIII.2.10.1. Analiza şi planificarea ... 191
VIII.2.10.2. Investigația ... 192
VIII.2.10.3. Reducerea riscurilor şi adoptarea măsurilor corective ... 193
VIII.2.10.4. Notificarea ... 194
VIII.2.10.5. Închiderea dosarului deschis pentru incidentul de securitate ... 194
VIII.2.10.6. Raportarea ... 195

Capitolul IX Studiu de caz - Identificarea ca OSE şi SE conform Legii NIS ... 197
IX.1. Considerații generale ... 199
IX.1.1. Entitatea activează într-unul sau mai multe dintre sectoarele/subsectoarele prevăzute în Anexa la Legea NIS? ... 199
Lista sectoarelor şi subsectoarelor care intră sub incidența Legii NIS ... 199
Fişa de evaluare primară ... 200
Lista tipurilor de entități care intră sub incidența Legii NIS ... 200
IX.1.2. Este aplicabilă o lege specială (lex specialis)? ... 207
Inventar legislativ ... 207
Inventar legislativ special ... 207
IX.1.3. Furnizează operatorul un „serviciu esențial" în sensul Directivei NIS? ... 208
Analiza internă a importanței serviciului oferit ... 210
IX.1.4. Depinde serviciul de o rețea şi de sisteme informatice? ... 212
Analiza internă a dependenței serviciilor de o rețea şi de sisteme informatice ... 212
IX.1.5. Un incident de securitate ar avea un efect perturbator semnificativ? ... 214
IX.1.5.1. Evaluarea gradului de perturbare a furnizării SENIS în funcție de criteriile intersectoriale ... 214
Numărul de utilizatori care se bazează pe servicii ... 215
Dependența altor sectoare de serviciul furnizat ... 217
Impactul pe care l-ar putea avea incidentele asupra activităților economice şi societale sau a siguranței publice ... 222
Cota de piață ... 224
Distribuția geografică în ceea ce priveşte zona care ar putea fi afectată de un incident . 226
Importanța entității pentru menținerea unui nivel suficient al serviciului, ținând cont de disponibilitatea unor mijloace alternative pentru furnizarea serviciului ... 228
IX.1.5.2. Evaluarea gradului de perturbare a furnizării SENIS în funcție de criteriile *sectoriale* şi *valorile de prag* ... 229
Sectorul Energie – A÷C ... 230
În tabelul de mai jos am inclus doar codurile sectoriale pentru care sunt prevăzute valori de prag explicite: ... 230
Sectorul Transport – D÷G ... 232
Sectorul Bancar – H ... 236
Sectorul Infrastructuri ale pieței financiare – I ... 237
Sectorul Sănătății – J ... 238
Sectorul furnizarea şi distribuirea de apă potabilă – K ... 238
Sectorul Infrastructură digitală – L ... 240
ANEXE ... 243
Anexa 1. Sectoare de activitate şi tipuri de entități ... 245
Anexa 2. Diagrama Procesului de identificare a operatorilor de servicii esențiale ... 249
Anexa 3. Lista Serviciilor Esențiale aprobată prin Hotărâre nr. 963 din 5 noiembrie 2020 251
Anexa 4. Criterii şi valori de prag, intersectoriale şi sectoriale ... 259

Valorile de prag corespunzătoare criteriilor intersectoriale 260
Criterii şi valori de prag sectoriale 261
Sector: Energie. Subsector: Electricitate. Cod sectorial/subsectorial: A 261
Sector: Energie. Subsector: Petrol. Cod sectorial/subsectorial: B 262
Sector: Energie. Subsector: Gaze naturale. Cod sectorial/subsectorial: C 263
Sector: Transport. Subsector: Transport aerian. Cod sectorial/subsectorial: D 265
Sector: Transport. Subsector: Transport feroviar. Cod sectorial/subsectorial: E 266
Sector: Transport. Subsector: Transport pe apă. Cod sectorial/subsectorial: F 267
Sector: Transport. Subsector: Transport rutier. Cod sectorial/subsectorial: G 269
Sector: Bancar. Subsector: -. Cod sectorial/subsectorial: H 270
Sector: Infrastructuri ale pieței financiare. Subsector: -. Cod sectorial/subsectorial: I 271
Sector: Sănătate. Subsector: Instituții de asistență medicală (inclusiv spitale şi clinici private). Cod sectorial/subsectorial: J 271
Sector: Furnizare şi distribuire de apă potabilă. Subsector: -. Cod sectorial/subsectorial: K 272
Sector: Infrastructură digitală. Subsector: -. Cod sectorial/subsectorial: L 273
Anexa 5. Lista orientativă OSE / SE pentru valori de prag "0" 275
Anexa 6. Lista celor mai frecvente amenințări la securitatea cibernetică 319
Anexa 7. Lista tipurilor de entități care intră sub incidența Legii NIS 322
Anexa 8. Formulare utilizate în relația cu DNSC 329
ANEXA nr. 2 la norme: Formular de asistență pentru identificarea operatorilor de servicii esențiale 330
ANEXA nr. 3 la norme: Formular de asistență pentru procesul de radiere a operatorului de servicii esențiale 332
ANEXA nr. 4 la norme: Notificare privind înscrierea în Registrul operatorilor de servicii esențiale 333
ANEXA nr. 5 la norme: Notificare privind modificarea/completarea datelor din Registrul operatorilor de servicii esențiale 335
ANEXA nr. 6 la norme: Notificare privind radierea din Registrul operatorilor de servicii esențiale 337
ANEXA nr. 7 la norme: Declarație pe propria răspundere privind îndeplinirea cerințelor minime de securitate pentru înscrierea în Registrul operatorilor de servicii esențiale 339
ANEXA nr. 11 la norme: Comunicare privind datele furnizorului de servicii digitale şi listă responsabili NIS 340
ANEXA nr. 12 la norme: Comunicare privind modificarea/completarea datelor furnizorilor de servicii digitale 342
ANEXA nr. 13 la norme: Comunicare privind radierea furnizorului de servicii digitale 344
DAICMS (Documentația de autoevaluare a îndeplinirii cerințelor minime de securitate) 346
Anexa 9. Lista orientativă a procedurilor privind securitatea informatică 350
Anexa 10. Model de "Procedura de răspuns în cazul unui incident de securitate" 354
Anexa 11. Cele mai frecvente riscuri privind securitatea cibernetică 368
Anexa 12. Indicii privind o posibilă infectare a calculatorului / laptopului 374
Anexa 13. Model - Analiza de risc pentru autoevaluarea îndeplinirii cerințelor minime de securitate 376
Anexa 14. Model - Decizie de numire Responsabil NIS 384
Anexa 15. Check-list de autoevaluare inițială a entităților sub aspect NIS 385

Glosar de termeni şi abrevieri 405
Bibliografie 441