

# **SECURITATEA REȚELELOR ȘI A SISTEMELOR INFORMATICE**

IMPLEMENTAREA  
DIRECTIVEI NIS ÎN ROMÂNIA



**MARIUS DUMITRESCU**

**DANIELA SIMIONOVICI**

# **SECURITATEA REȚELELOR ȘI A SISTEMELOR INFORMATICE**

**Implementarea Directivei NIS în România**



**EDITURA UNIVERSITARĂ**

**București, 2022**

Colecția Științe juridice

Redactor: Marius George Dumitrescu

Tehnoredactor: Daniela Simionovici

Coperta: Timea Paal

Editură recunoscută de Consiliul Național al Cercetării Științifice (C.N.C.S.) și inclusă de Consiliul Național de Atestare a Titlurilor, Diplomelor și Certificatelor Universitare (C.N.A.T.D.C.U.) în categoria editurilor de prestigiu recunoscut.

**Descrierea CIP a Bibliotecii Naționale a României**

**DUMITRESCU, MARIUS**

**Securitatea rețelelor și a sistemelor informatice : implementarea directivei NIS în România /** Marius Dumitrescu, Daniela Simionovici. -

București : Editura Universitară, 2022-

2 vol.

ISBN 978-606-28-1430-4

**Vol. 1.** - 2022. - Conține bibliografie. - ISBN 978-606-28-1431-1

I. Simionovici, Daniela

004

DOI: (Digital Object Identifier): 10.5682/9786062814311

© Toate drepturile asupra acestei lucrări sunt rezervate, nicio parte din această lucrare nu poate fi copiată fără acordul autorilor

Copyright © 2022

Editura Universitară

Editor: Vasile Muscalu

B-dul. N. Bălcescu nr. 27-33, Sector 1, București

Tel.: 021.315.32.47

[www.editurauniversitara.ro](http://www.editurauniversitara.ro)

e-mail: [redactia@editurauniversitara.ro](mailto:redactia@editurauniversitara.ro)

Distribuție: 0769.041.200  
[comanda@neoprivacy.ro](mailto:comanda@neoprivacy.ro)  
[www.neoprivacy.ro](http://www.neoprivacy.ro)

# DESPRE AUTORI



**MARIUS  
DUMITRESCU**



**DANIELA  
SIMIONOVICI**



**Marius Dumitrescu** este licențiat în Științe Politice, are un master în Marketing și peste 18 ani de experiență în implementarea și gestionarea soluțiilor software medicale și farmaceutice. Din 2018, este fondator și Președinte al Asociației Specialiștilor în Confidențialitate și Protecția Datelor din România (ASCPD), Membru IAPP și IAPP Romania Knowledge Chapter Co-Chair 2022/2023.

A absolvit în 2018 studiile postuniversitare de lungă durată privind protecția datelor la Facultatea de Științe Economice, Drept și Administrație - Centrul pentru Protecția Datelor din Târgu-Mureș, România. Din 2018 este Managing Partner și Data Management and Compliance Solutions Specialist la NeoPrivacy România cu o Certificare PECB DPO. Este director editorial la două publicații online, una pentru profesioniștii din domeniul protecției și securității datelor cu caracter personal ([www.dpo-net.ro](http://www.dpo-net.ro)) și alta adresată comunității medicale și farmaceutice din România ([www.health.ro](http://www.health.ro)). Este autor și coautor a numeroase articole publicate în Revista Română pentru Securitatea și Protecția Datelor cu Caracter Personal (Universul Juridic), Curierul Judiciar și [juridice.ro](http://juridice.ro). Este formator și PECB Certified Trainer, participând la mai multe sesiuni educaționale cu subiecte despre protecția datelor, securitatea datelor, standardele ISO și managementul organizațional. Este implicat activ în organizarea de conferințe naționale și internaționale privind protecția datelor, farmacoconomie și managementul sănătății.

**Daniela Simionovici** a absolvit cursurile Universității Ștefan cel Mare din Suceava, specializarea Asistență socială și un master în consiliere și administrare resurse umane la aceeași universitate. A absolvit cursul postuniversitar de “Protecția datelor cu caracter personal” organizat de Facultatea de Drept și Științe Administrative ale aceleiași universități sucevene. Este vicepreședinte al Asociației Specialiștilor în Confidențialitate și Protecția Datelor din România - ASCPD, este înregistrată ca PECB Certified DPO și a obținut titlul de „Cel mai bun DPO din Romania” împreună cu Echipa Nord Est DPO România la Târgu Mureș, în iunie 2019. Oferă consultanță în domeniul implementării Regulamentului general privind protecția datelor (GDPR) și oferă și servicii de Responsabil cu protecția datelor personale în regim externalizat (DPO). Este Senior Partner Neoprivacy România și membru al echipei de consultanță și implementare GDPR, ISO, SCIM și NIS. Participă constant la seminare, dezbateri și conferințe dedicate protecției datelor personale și a Directivei NIS și împărtășește din experiența sa scriind articole și cărți dedicate domeniului protecției datelor și NIS din perspectiva practicianului.





## CUPRINS

<b>Despre autori</b> .....	5
<b>Cuvânt înainte</b> .....	15
<b>Mulțumiri</b> .....	19
<b>Introducere</b> .....	23
<b>Capitolul I. Considerații generale</b> .....	27
I.1. Ce este Directiva NIS și 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
<b>Capitolul II</b> <b>Directoratul Național de Securitate Cibernetică - DNSC</b> .....	49
II.1. Responsabilități și 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 și atribuțiile Directoratului Național de Securitate Cibernetic.....	55
II.3.a. Strategie și planificare.....	55
II.3.b. Funcția de autoritate competentă la nivel național de reglementare, supraveghere și 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 și sprijin a CSIRT-urilor sectoriale.....	58
II.3.f. Funcția de echipă de răspuns la incidente de securitate cibernetică pentru produse și servicii informatice utilizate în cadrul sectorului guvernamental .....	58
II.3.g. Funcția de alertare, prevenire, conștientizare și instruire .....	58
II.3.h. Funcția de cooperare și colaborare .....	59
II.3.i. Funcția de autoritate națională de certificare privind securitatea cibernetică .....	60
II.3.j. Funcția de asigurare a conformității și abordării unitare a securității cibernetică în cadrul infrastructurilor cibernetică .....	60
II.3.k. Funcția de reprezentare .....	61
II.3.l. Funcția de cercetare-dezvoltare.....	61
II.3.m. Funcția de analiză și prognoză.....	61
II.3.n. Funcția de identificare, evaluare, monitorizare și atenuare a riscurilor cibernetică 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 cibernetică a noilor tehnologii.....	62
II.3.q. Funcția de evaluare și certificare.....	62
II.3.r. Funcția de educație și pregătire în domeniul securității cibernetică .....	63
II.3.s. Funcția de management al proiectelor și 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
<b>Capitolul III Operatorii de servicii esențiale și furnizorii de servicii digitale .....</b>	<b>71</b>
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
<b>Capitolul IV Etapele implementării prevederilor Legii nr. 362/2018.....</b>	<b>81</b>
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

<b>Capitolul V</b> Măsurile tehnice și organizatorice de securitate.....	117
V.1. Cerințele minime de securitate pentru asigurarea securității rețelelor și 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 și sistemelor informatice aparținând operatorilor de servicii esențiale sau furnizorilor de servicii digitale .....	121
V.1.4. Autorizarea echipelor CSIRT ce deservește rețele și sisteme informatice din categoria serviciilor esențiale și serviciilor digitale .....	122
V.2. Întocmirea și 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
<b>Capitolul VI</b> Controlul îndeplinirii obligațiilor de securitate și aplicarea sancțiunilor .....	133
VI.1. Cerințele minime de asigurare a securității rețelelor și 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
<b>Capitolul VII</b> Propunerea de Directivă NIS 2.0 și 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 și Legea nr. 362/2018 se vor aplica și administrației publice .....	173
<b>Capitolul VIII</b> 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 recunoaștem 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 și raportarea unui incident de securitate .....	182
VIII.2.4.1. Când se consideră că operatorul „a luat la cunoștință” 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 și 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 și externalizarea serviciilor de răspuns la incidente de securitate .....	190
VIII.2.9.3. Documentarea și deschiderea rapoartelor de incident de securitate .....	190

VIII.2.9.4. Înființarea echipei de management a incidentului și analiza planurilor alternative.....	190
VIII.2.10. Activitățile post incident.....	191
VIII.2.10.1. Analiza și planificarea .....	191
VIII.2.10.2. Investigația .....	192
VIII.2.10.3. Reducerea riscurilor și 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
<b>Capitolul IX</b> Studiu de caz - Identificarea ca OSE și 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 și subsectoarelor care intră sub incidența Legii NIS.....	199
Fișa 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 și de sisteme informatice?.....	212
Analiza internă a dependenței serviciilor de o rețea și 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 și societale sau a siguranței publice .....	222
Cota de piață.....	224
Distribuția geografică în ceea ce privește 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 și 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 și distribuirea de apă potabilă – K.....	238
Sectorul Infrastructură digitală – L.....	240
<b>ANEXE</b> .....	243
Anexa 1. Sectoare de activitate și 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 și valori de prag, intersectoriale și sectoriale .....	259

Valorile de prag corespunzătoare criteriilor intersectoriale .....	260
Criterii și 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 și clinici private). Cod sectorial/subsectorial: J.....	271
Sector: Furnizare și 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 și 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
<b>Glosar de termeni și abrevieri .....</b>	<b>405</b>
<b>Bibliografie.....</b>	<b>441</b>



# CUVÂNT ÎNAINTE







La mai mult de patru ani de la intrarea în vigoare a Directivei UE nr. 2016/1148 (Directiva NIS) și la peste trei ani de la transpunerea acesteia prin Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, România a făcut progrese tangibile în procesul de implementare.

Însă, succesul implementării nu depinde doar de noile reglementări legislative ci și de abilitatea efectivă a operatorilor de servicii esențiale, a furnizorilor de servicii digitale și a responsabililor cu implementarea NIS la nivelul entităților vizate de a înțelege, interpreta și a aplica prevederile legale, normele tehnice și metodologice aferente. Mai mult, este important ca specialiștii să poată aprecia corect și implicațiile aplicării acestor prevederi, prin prisma altor acte normative relevante.

Pentru aceasta, este nevoie de o analiză aprofundată, de obținerea unor noi competențe și cunoștințe specifice privind modalitatea de implementare a Directivei NIS în România și de o schimbare culturală profundă din partea fiecăruia. Practic, este nevoie să studiem din nou, să avem acces la studii de caz detaliate și la cunoștințele aprofundate ale unor experți recunoscuți în domeniu.

Scrisă sub forma unui ghid detaliat și pragmatic, acest superb material de implementare a Directivei NIS elaborează pe cuprinsul a sute de pagini foarte bine scrise experiența concretă în domeniu a celor doi autori.

Într-o formă clară și foarte bine prezentată, lucrarea pune la dispoziție o varietate de explicații, îndrumări, recomandări, dar și materiale de suport fiind una din publicațiile extrem de necesare azi tuturor celor implicați în implementarea Directivei NIS.

Sunt surprins în mod plăcut de nivelul tehnic, pragmatismul ideilor și recomandărilor exprimate în materialul publicat. Materialul ne explică în detaliu și cu exemple practice elemente cheie ale responsabilităților ce revin operatorilor de servicii esențiale și furnizorilor de servicii digitale, dar și detalii privind etapele implementării Legii nr. 362/2018 de către aceștia sau măsurile tehnice și organizatorice de securitate ce trebuie aplicate. Efectiv, fiecare capitol ne oferă posibilitatea de a aplica și implementa în practică prevederile directivei.

Mai mult, lucrarea acoperă și o serie de elemente privind Directiva NIS 2.0, cu obiectivul de a anticipa și pregăti cititorul pentru noile obligații ce derivă din evoluția naturală a directivei.

Consider că ”Securitatea rețelelor și a sistemelor informatice - Implementarea Directivei NIS în România” este unul din instrumentele esențiale pentru specialiștii în domeniu, pe care îl recomand cu căldură a fi utilizat începând chiar de azi.

**Dan Cîmpean**  
**Director General al**  
**Directoratului Național de Securitate Cibernetică - DNSC**  
**București, 2021**



# MUȚUMIRI

An aerial, high-angle photograph of a city street, likely in Bucharest, Romania. The image is heavily stylized with a cyan/blue color palette. The street is filled with light trails from moving vehicles, creating a sense of motion and time-lapse. On the right side, a large, ornate, multi-story building with classical architectural features, including domes and arched windows, is prominent. The background shows a dense urban landscape with various buildings and structures. The overall composition is dynamic and visually striking.



*Autorii mulțumesc familiilor, prietenilor, colegilor și  
tuturor colaboratorilor care au făcut posibil acest proiect*



# INTRODUCERE







Adoptarea, în iulie 2016, a Directivei UE nr. 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniunea Europeană (Directiva NIS), confirmă preocupările constante din ultimii ani ale forurilor comunitare pe linia creșterii rezilienței infrastructurilor IT&C aparținând operatorilor de servicii esențiale și furnizorilor de servicii digitale din statele membre. Această Directivă prevede măsuri unitare pentru atingerea unui nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune și noi mecanisme de cooperare la nivel european.

***Nu este o nouă lege a securității cibernetice!  
Nu vizează apărarea și securitatea națională.  
Vizează piața și serviciile!***

În esență, Legea NIS impune niște obligații celor vizați în vederea implementării unor cerințe minime de securitate a sistemelor și rețelelor informatice, în așa fel încât să se asigure continuitatea activităților economice și să prevină perturbarea acestora.

În timp ce Regulamentul UE nr. 2016/679 (GDPR) este preocupat de protecția datelor cu caracter personal, Directiva NIS se concentrează asupra menținerii funcționării serviciilor esențiale.

Să presupunem că un furnizor este afectat de un atac cibernetic și datele personale nu sunt compromise, dar serviciul furnizat devine inutilizabil pentru o zi întreagă. Deși nu există nicio obligație de a raporta incidentul conform prevederilor GDPR, compania dvs. aproape sigur că va trebui să notifice autoritatea de reglementare în conformitate cu Directiva NIS. Dar, să presupunem că există o întrerupere a serviciului care are drept consecință negativă și pierderea datelor cu caracter personal. Compania se va confrunta cu cerințe distincte de raportare, atât în conformitate cu Directiva NIS, cât și cu GDPR. După cum afirmă autoritatea britanică de reglementare, *“cerințele fiecărei legislații ar trebui să fie respectate în termenii săi”*. Acest lucru presupune obligativitatea de a prezenta două rapoarte autorităților de reglementare pentru același incident!

În acest context, statele membre aveau obligația să adopte și să publice până în 9 mai 2018 actele administrative și legislative necesare transpunerii acestei Directive, pe care să le comunice Comisiei Europene, iar, până la 9 noiembrie 2018 să identifice operatorii de servicii esențiale aflați pe teritoriul lor.

Totodată, Directiva NIS presupune elaborarea de către statele membre UE a unei Strategii naționale privind securitatea rețelelor și sistemelor informatice, care să definească obiectivele strategice și măsurile de reglementare adecvate, în vederea creșterii nivelului securității acestor sisteme.

Prezenta lucrare se adresează operatorilor de servicii esențiale, furnizorilor de servicii digitale și responsabililor cu implementarea NIS la nivelul entităților vizate de prevederile Directivei.

Scopul prezentei lucrări este de a-i ajuta pe cei vizați nu doar să implementeze prevederile Directivei, ci să înțeleagă importanța acesteia și, mai ales, faptul că serviciile esențiale pe care le furnizează au nevoie de o protecție deosebită nu pentru faptul că nerespectarea Directivei ar atrage după sine amenzi, ci pentru faptul că orice perturbare în furnizarea serviciilor esențiale se poate traduce în disfuncționalități grave la nivel comunitar și chiar societal.

În baza legislației în vigoare și a documentelor și ghidurilor de sprijin puse la dispoziția celor interesați, pe parcursul lucrării vom oferi explicații, îndrumări, recomandări, dar și materiale de suport pentru ca implementarea Directivei în organizațiile operatorilor de servicii esențiale / furnizorilor de servicii digitale să se poată realiza *de facto* și nu doar de formă.