EXPUNERE DE MOTIVE

Secţiunea 1 Titlul proiectului de act normativ **Lege privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice**	
Secţiunea a 2-a Motivul emiterii actului normativ	
1. Descrierea situaţiei actuale	**Cadrul normativ european** În iulie 2016 a fost adoptată *Directiva (UE) 2016/1148*[1] *privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune*, aceasta fiind primul act legislativ al Uniunii Europene privind securitatea rețelelor și sistemelor informatice, menit să transpună obiectivele Strategiei Europene de securitate cibernetică stabilite pentru pilonul NIS. Directiva creează structurile necesare pentru cooperarea strategică și operațională între statele membre și pentru creșterea nivelului de reziliență al rețelelor și al sistemelor informatice de pe teritoriul UE. Constatând faptul că amploarea, frecvența și impactul incidentelor de securitate este în creștere, reprezentând o amenințare gravă pentru funcționarea rețelelor și a sistemelor informatice, fapt ce poate împiedica desfășurarea activităților economice și genera pierderi financiare substanțiale subminând încrederea utilizatorilor și provocând pagube majore economiei Uniunii, Directiva impune o abordare globală la nivelul Uniunii, care să includă cerințe comune privind crearea capacităților minime și planificarea, schimb de informații, cooperare și cerințe comune de securitate pentru operatorii de servicii esențiale și furnizorii de servicii digitale, fără a-i împiedica pe aceștia să adopte măsuri de securitate mai stricte decât cele prevăzute de Directivă. Directiva stabilește data de 9 mai 2018 ca moment până la

1 Jurnalul Oficial al Uniunii Europene L 194/1, 19.7.2016

	care statele membre trebuie să transpună și să adopte în legislația națională actele normative cu putere de lege și actele administrative de transpunere și punere în aplicare. În luna mai 2017, *Evaluarea la jumătatea perioadei a punerii în aplicare a strategiei privind piața unică digitală - O piață unică digitală conectată pentru toți*[2], făcută de Comisia Europeană, la punctul 3 - A*sigurarea unui mediu digital echitabil, deschis și sigur*, reține ca necesară extinderea Strategiei privind piața unică digitală, pentru a ține pasul cu tendințele și provocările care apar, precum cele legate de platformele online, de economia datelor și de securitatea cibernetică, susținând la subpunctul 3.3 *Încurajarea unui ecosistem cibernetic de încredere: Abordarea în comun a provocărilor legate de securitatea cibernetică* și constatând necesitatea revizuirii Strategiei de securitate cibernetică a UE raportat la contextul semnificativ diferit al amenințărilor față de anul 2013. **Cadrul normativ național** La nivel național, în domeniul securităţii, există deja în vigoare o serie de reglementări, acte normative cu caracter primar sau secundar, cum ar fi: Ordonanţa de urgenţă a Guvernului nr.98/2010 privind identificarea, desemnarea şi protecţia infrastructurilor critice, care stabileşte cadrul legal privind identificarea, desemnarea infrastructurilor critice naţionale/europene şi evaluarea necesităţii de a îmbunătăţi protecţia acestora, în scopul creşterii capacităţii de asigurare a stabilităţii, securităţii şi siguranţei sistemelor economico-sociale şi protecţiei persoanelor. Actul normativ defineşte infrastructura critică naţională, denumită ICN ca fiind un element, un sistem sau o componentă a acestuia, aflat pe teritoriul naţional, care este esenţial pentru menţinerea funcţiilor vitale ale societăţii, a sănătăţii, siguranţei, securităţii, bunăstării sociale ori economice a persoanelor şi a cărui perturbare sau distrugere ar avea un impact semnificativ la nivel naţional ca urmare a incapacităţii de a menţine respectivele funcţii. Actul normativ stabileşte criteriile intersectoriale de identificare a ICN urmând ca autorităţile publice responsabile să identifice potenţialele

2 Comunicare a comisiei către parlamentul european, consiliu, comitetul economic și social european și comitetul regiunilor, Evaluarea la jumătatea perioadei a punerii în aplicare a strategiei privind piața unică digitală - O piață unică digitală conectată pentru toți, COM(2017) 228 final, Bruxelles, 10.5.2017

	ICN care corespund criteriilor definite. În aplicarea ordonanţei de urgenţă, Guvernul a emis Hotărârea nr.718/2011, prin care aprobă Strategia naţională privind protecţia infrastructurilor critice. Hotărârea Guvernului nr.494/2011, reglementează înfiinţarea ca instituţie publică cu personalitate juridică, în coordonarea Ministerului Comunicațiilor şi Societății Informaţionale, a Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO, structură independentă de expertiză şi cercetare-dezvoltare în domeniul protecţiei infrastructurilor cibernetice, definind totodată termeni şi expresii precum infrastructură cibernetică, spaţiu cibernetic, securitate cibernetică, atac cibernetic, incident cibernetic etc. Un alt act normativ emis în domeniul securităţii naţionale îl constituie Hotărârea Guvernului nr. 271/2013, pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică. Strategia de securitate cibernetică prezintă obiectivele, principiile şi direcţiile majore de acţiune pentru cunoaşterea, prevenirea şi contracararea ameninţărilor, vulnerabilităţilor şi riscurilor la adresa securităţii cibernetice a României şi pentru promovarea intereselor, valorilor şi obiectivelor naţionale în spaţiul cibernetic. Prin H.G. 494/2011 Centrul național de răspuns la incidente de securitate cibernetică - CERT-RO are o serie de atribuții similare celor din Directiva 1148/2016 fiind Centru Național de Răspuns la Incidente de Securitate Cibernetică cu atribuții si de punct de contact cu celelalte echipe CERT. Cu toate acestea, nu există prevederi unitare în legislația națională privitoare la notificarea în sensul Directivei NIS a incidentelor de securitate a rețelelor și sistemelor informatice. O situație similară se constată și în privința cerințelor de securitate a rețelelor și sistemelor informatice, la nivel național existând doar cerințe specifice derivate din transpunerea unor acte normative europene care reglementează anumite sectoare de activitate.

	În conformitate cu art. 25 alin. (1) din directiva 1148/2016 (NIS) România are obligația, în calitate de stat membru al Uniunii Europene, de a asigura transpunerea Directivei în legislația națională până cel târziu la data de 9 mai 2018, toate actele normative cu putere de lege precum și cele administrative necesare trebuind să producă efecte începând cu data de 10 mai 2018.
2. Schimbări preconizate	Pentru transpunerea prevederilor Directivei 1148/2016 (NIS) în legislația națională este necesară elaborarea unui act normativ cu putere de lege precum și asigurarea prin acte normative și administrative subsecvente a cadrului legal necesar aplicării acestuia. În acest scop, prin prezentul proiect de act normativ se propune adoptarea unui set de norme coerente, clare și transparente, menite să instituie un cadru național unitar de asigurare a securității informatice și a răspunsului la incidentele de securitate survenite la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale și ale furnizorilor de servicii digitale în conformitate cu cerințele Directivei 1148/2016. Prezentul proiect de act normativ reglementează: • cadrul de cooperare la nivel național și de participare la nivel european și internațional în domeniul asigurării securității rețelelor și sistemelor informatice • autoritățile și entitățile de drept public și privat care dețin competențe și responsabilități în aplicarea prevederilor prezentei legi, a punctului unic de contact la nivel național și a echipei naționale de răspuns la incidente de securitate informatică • cerințele de securitate și de notificare pentru operatorii de servicii esențiale și pentru furnizorii de servicii digitale precum și instituirea mecanismelor de actualizare a acestora în funcție de evoluția amenințărilor la adresa securității rețelelor și sistemelor informatice În vederea delimitării sferei de aplicabilitate a proiectului de act normativ de aria mai largă a securității cibernetice - așa cum este definită în actele normative la nivel național și care cuprinde și activitățile din domeniile securitate națională și apărare – proiectul preia și utilizează terminologia din Directiva 1148/2016 referindu-se la

	securitatea rețelelor și sistemelor informatice. În același sens, proiectul delimitează explicit activitățile reglementate de cele ale instituțiilor din domeniile apărare și securitate națională prevăzând mecanisme de cooperare în situațiile în care un incident aduce atingere activităților acelor instituții ori prin amploarea sa afectează apărarea sau securitatea națională. În privința autorității competente la nivel național, a punctului unic și a echipei CSIRT naționale proiectul propune dezvoltarea acestora în cadrul aceleiași instituții, respectiv a Centrului Național de Răspuns la Incidente de Securitate - CERT-RO care îndeplinește în prezent rolul de CSIRT/CERT național, reprezintă România în grupul de cooperare și este punct unic de contact cu celelalte echipe CERT la nivel național și internațional. Pentru definirea transparentă și cu claritate a domeniului de aplicare, proiectul reglementează operatorii de servicii esențiale raportat la anexa care cuprinde sectoare și subsectoare de activitate și definirea serviciilor esențiale respectiv modalitatea de analiza a gradului de perturbare a furnizării unui serviciu esențial, enunțând criteriile trans-sectoriale de analiză, urmând a fi emise prin hotărâre de guvern valorile de prag și criteriile specifice fiecărui sector de activitate. Proiectul propune alcătuirea unui Registru al operatorilor de servicii esențiale, înscrierea în acesta putându-se face fie voluntar prin notificarea transmisă de operator autorității competente la nivel național – CERT-RO, fie din oficiu în urma verificărilor efectuate de către CERT-RO. În privința furnizorilor de servicii digitale, proiectul nu prevede alcătuirea unui registru al acestora, însă permite autorității identificarea acestora în vederea stabilirii îndeplinirii cerințelor de securitate și notificare, proiectul preluând excepțiile de la aplicare și cerințele mai reduse ce se aplică acestora, conform Directivei. În vederea coordonării la nivel național în managementul incidentelor, proiectul de act normativ prevede furnizarea de către CERT-RO a unui serviciu de alertare și cooperare la care se vor interconecta operatorii și furnizorii prevăzuți de prezentul proiect de act normativ, stabilind totodată obligația acestora de a monitoriza alertele primite și a

	asigura răspunsul prompt în caz de necesitate. Sub aspectul cerințelor de securitate și notificare, proiectul prevede cerințele și capitolele minimale, instituind mecanismul de actualizare și publicare a acestora de către autoritatea competentă la nivel național în urma consultărilor cu celelalte autorități, astfel încât cerințele să poată evolua în pas cu evoluția amenințărilor cât și a tehnologiilor. Proiectul statuează utilizarea standardelor internaționale, cu respectarea principiului neutralității tehnologice în soluțiile impuse. Proiectul de act normativ își propune stimularea dezvoltării pieței de securitate informatică. În acest sens sunt definite măsurile care privesc piața de audit de securitate pentru rețelele și sistemele operatorilor și furnizorilor vizați cât și piața de servicii de securitate informatică de tip CSIRT, respectiv: • realizarea auditurilor de către auditori independenți, prevăzând un mecanism pentru atestarea acestora care să asigure menținerea unui nivel al auditului corespunzător cu evoluția amenințărilor și tehnologiilor. • reglementarea unui sistem de autorizare a echipelor CSIRT care deservesc operatorii de servicii esențiale și furnizorii de servicii digitale precum și a echipelor CSIRT sectoriale, • reglementarea unui sistem de acreditare a formatorilor și furnizorilor de servicii de formare pentru auditorii și echipele CSIRT vizate, în vederea stimulării furnizării de servicii de formare în concordanță cu evoluția amenințărilor și tehnologiilor, Sub aspectul regimului sancționator, proiectul oferă autorității competente la nivel național – CERT-RO dreptul de realizare a controlului implementării cerințelor de securitate și notificare, precum și de îndeplinire a obligațiilor de către celelalte entități vizate de proiect, definind un set de contravenții și sancțiuni în linie cu cerințele directivei și oferind un set de garanții în privința contestării acestora. Pentru a îndeplini rolul multiplu de autoritate competentă la

	nivel național având și atribuții de autorizare a celorlalte echipe CSIRT private și sectoriale, cât și de echipă CSIRT națională, CERT-RO nu va asigura prin echipa CSIRT națională servicii de asigurare a securității rețelelor și sistemelor informatice pentru operatorii și furnizorii vizați, având în vedere că în sarcina CSIRT-ului național revine doar coordonarea la nivel național a incidentelor (primirea notificărilor, evaluarea impactului, alertarea precum și oferirea de ghidaj). Până la 9 noiembrie 2018, statele membre identifică operatorii de servicii esențiale care au un sediu pe teritoriul lor. Sectoarele vizate pentru identificarea serviciilor esențiale și a operatorilor de servicii esențiale cuprind: energia, transporturile, sectorul bancar, infrastructuri ale pieței financiare, sănătate, furnizarea și distribuirea de apă potabilă, infrastructura digitală.
Secţiunea a 3-a Impactul socioeconomic al proiectului de act normativ	
1. Impactul macroeconomic	Actul normativ propus are impact asupra sectoarelor vizate în Anexa: energia, transporturile, sectorul bancar, infrastructuri ale pieței financiare, sănătate, furnizarea și distribuirea de apă potabilă, infrastructura digitală.
1^1. Impactul asupra mediului concurenţial şi domeniului ajutoarelor de stat	Proiectul de act normativ nu se referă la acest subiect
2. Impactul asupra mediului de afaceri	Directiva 1148/2016 și pe cale de consecință și proiectul impune cerințe de securitate operatorilor de servicii esențiale și furnizorilor de servicii digitale, cerințe care se reflectă în costuri de implementare.
3. Impactul social	Constituind cadrul legal care reglementează securitatea rețelelor și sistemelor informatice ce susțin servicii esențiale din domenii cheie la nivel social, este de așteptat o creștere a rezilienței acestor servicii și respectiv o reducere a riscurilor la nivel social asociate cu atacurile cibernetice. Indirect va duce pe termen lung la o creștere a încrederii în serviciile societății digitale și o dezvoltare a serviciilor de securitate informatică.
4. Impactul asupra mediului	Proiectul de act normativ nu se referă la acest subiect
5. Alte informaţii	Nu au fost identificate
Secţiunea a 4-a Impactul financiar asupra bugetului general consolidat, atât pe termen scurt, pentru anul curent, cât şi pe termen lung (pe 5 ani)	

Având în vedere că proiectul de act normativ prevedere finanţarea activităţii autorităţii competente la nivel naţional – CERT-RO pentru dezvoltarea capacităţilor la nivelul cerut de Directiva 1148/2016 atât sub aspect financiar cât şi al resurselor umane, proiectul de act normativ poate avea un impact asupra bugetului general consolidat, cel mai devreme pentru anul 2018.

- mii lei -

Indicatori	Anul curent	Următorii 4 ani				Media pe 5 ani
1	2	3	4	5	6	7
1. Modificări ale veniturilor bugetare, plus/minus, din care:						
a) buget de stat, din acesta:						
(i) impozit pe profit						
(ii) impozit pe venit						
b) bugete locale:						
(i) impozit pe profit						
c) bugetul asigurărilor sociale de stat:						
(i) contribuţii de asigurări						
2. Modificări ale cheltuielilor bugetare, minus, din care:						
a) buget de stat, din acesta:						
(i) cheltuieli de personal						
(ii) bunuri si servicii						
b) bugete locale:						
(i) cheltuieli de personal						
(ii) bunuri şi servicii						
c) bugetul asigurărilor sociale de stat:						
(i) cheltuieli de personal						
(ii) bunuri si servicii						
3. Impact financiar, plus/minus, din care:						
a) buget de stat						
b) bugete locale						
4. Propuneri pentru acoperirea creşterii cheltuielilor bugetare						
5. Propuneri pentru a compensa reducerea veniturilor bugetare						
6. Calcule detaliate privind fundamentarea modificărilor						

veniturilor						
si/sau cheltuielilor bugetare						
7. Alte informaţii						

Secţiunea a 5-a
Efectele proiectului de act normativ asupra legislaţiei în vigoare

1. Măsuri normative necesare pentru aplicarea prevederilor proiectului de act normativ: a) acte normative în vigoare ce vor fi modificate sau abrogate, ca urmare a intrării în vigoare a proiectului de act normativ; b) acte normative ce urmează a fi elaborate în vederea implementării noilor dispoziţii.	In aplicarea proiectului, vor fi emise: 1. hotărâre a Guvernului care să publice Anexa cu valori de prag pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale. 2. hotărâre a Guvernului care să stabilească organizarea și funcționarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică CERT-RO și să înlocuiască H.G. 494/2011. 3. Norme tehnice și regulamente emise prin decizia Directorului CERT-RO și publicate în Monitorul Oficial astfel: a. normele tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice b. normele tehnice privind îndeplinirea obligațiilor de notificare a incidentelor de securitate de către operatorii și furnizorii c. norme tehnice și valorile de prag pentru stabilirea impactului incidentelor de securitate la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale și furnizorilor de servicii digitale. d. normele tehnice și regulamentele privind cerințele referitoare la înființarea și funcționarea echipelor CSIRT e. normele tehnice și regulamentele privind cerințele referitoare la atestarea auditorilor calificați cu competențe în domeniul securității serviciilor esențiale f. Lista serviciilor esențiale pentru fiecare sector și subsector din anexa la lege. Conform prevederilor art 25 alin (1) din Directiva 1148/2016, toate actele normative cu putere de lege care transpun directiva precum și actele administrative de punere în aplicare a transpunerii trebuie să producă efecte începând cu data de 10 mai 2018.

2. Conformitatea proiectului de act normativ cu legislaţia comunitară în cazul proiectelor ce transpun prevederi comunitare	Proiectul de lege transpune: - Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune
3 Măsuri normative necesare aplicării directe a actelor normative comunitare	Proiectul de act normativ nu se referă la acest subiect
4. Hotărâri ale Curţii de Justiţie a Uniunii Europene	Proiectul de act normativ se conformează prevederilor cuprinse în legislaţia UE menţionată la punctul 2.
5. Alte acte normative şi/sau documente internaţionale din care decurg angajamente	Proiectul de act normativ nu se referă la acest subiect.
6. Alte informaţii	Nu au fost identificate.
Secţiunea a 6-a Consultările efectuate în vederea elaborării proiectului de act normative	
1. Informaţii privind procesul de consultare cu organizaţii neguvernamentale, institute de cercetare şi alte organisme implicate 2. Fundamentarea alegerii organizaţiilor cu care a avut loc consultarea, precum şi a modului în care activitatea acestor organizaţii este legată de obiectul proiectului de act normative	Proiectul de act normativ nu se referă la acest subiect
3. Consultările organizate cu autorităţile administraţiei publice locale, în situaţia în care proiectul de act normativ are ca obiect activităţi ale acestor autorităţi, în condiţiile Hotărârii Guvernului nr. 521/2005 privind procedura de consultare a structurilor asociative ale autorităţilor administraţiei publice locale la elaborarea proiectelor de acte normative	Proiectul de act normativ nu se referă la acest subiect
4. Consultările desfăşurate în cadrul consiliilor interministeriale, în conformitate cu prevederile Hotărârii Guvernului nr. 750/2005	Proiectul de act normativ nu se referă la acest subiect

privind constituirea consiliilor interministeriale permanente	
5. Informaţii privind avizarea de către: a) Consiliul Legislativ b) Consiliul Suprem de Apărare a Ţării c) Consiliul Economic şi Social d) Consiliul Concurenţei e) Curtea de Conturi	Proiectul necesită avizul Consiliului Legislativ. Proiectul necesită avizul Consiliului Concurenţei Proiectul necesită avizul Consiliului Suprem de Apărare a Ţării
6. Alte informaţii	
Secţiunea a 7-a Activităţi de informare publică privind elaborarea si implementarea proiectului de act normative	
1. Informarea societăţii civile cu privire la necesitatea elaborării proiectului de act normativ	Proiectul se publică pe site-ul MCSI
2. Informarea societăţii civile cu privire la eventualul impact asupra mediului în urma implementării proiectului de act normativ, precum şi efectele asupra sănătăţii şi securităţii cetăţenilor sau diversităţii biologice	Proiectul de act normativ nu se referă la acest subiect
3. Alte informaţii	Nu au fost identificate
Secţiunea a 8-a Măsuri de implementare	
1. Măsurile de punere în aplicare a proiectului de act normativ de către autorităţile administraţiei publice centrale şi/sau locale - înfiinţarea unor noi organisme sau extinderea competentelor instituţiilor existente.	a) instituţii ce urmează a fi înfiinţate, reorganizate sau desfiinţate – proiectul de act normativ nu se referă la acest subiect; b) rezultatul se poate obţine cu instituţiile existente; c) sursa de finanţare a instituţiilor ce urmează a fi înfiinţate - proiectul de act normativ nu se referă la acest subiect.
2. Alte informaţii	Nu au fost identificate