LEGE 362/2018	*Modificat(a)*
Emitent: Parlament **Domenii: Informatica**	**M.O. 21/2019**
Lege privind asigurarea unui nivel comun ridicat de securitate a retelelor si sistemelor informatice	

M.Of.Nr.21 din 9 ianuarie 2019

LEGE Nr. 362
privind asigurarea unui nivel comun ridicat de securitate a retelelor si sistemelor informatice

Parlamentul României adopta prezenta lege.

CAPITOLUL I
Dispozitii generale

SECTIUNEA 1
Obiect si scop

Art. 1. – Prezenta lege stabileste cadrul juridic si institutional, masurile si mecanismele necesare în vederea asigurarii unui nivel comun ridicat de securitate a retelelor si sistemelor informatice si a stimularii cooperarii în domeniu.

Art. 2. – (1) Scopul prezentei legi îl constituie:

a) stabilirea cadrului de cooperare la nivel national si de participare la nivel european si international în domeniul asigurarii securitatii retelelor si sistemelor informatice;

b) desemnarea autoritatii competente la nivel national si a entitatilor de drept public si privat care detin competente si responsabilitati în aplicarea prevederilor prezentei legi, a punctului unic de contact la nivel national si a echipei nationale de interventie în caz de incidente de securitate informatica;

c) stabilirea cerintelor de securitate si notificare pentru operatorii de servicii esentiale si pentru furnizorii de servicii digitale si instituirea mecanismelor de actualizare a acestora în functie de evolutia amenintarilor la adresa securitatii retelelor si sistemelor informatice.

(2) Prezenta lege nu se aplica institutiilor din domeniul apararii, ordinii publice si securitatii nationale, precum si Oficiului Registrului National al Informatiilor Secrete de Stat.

SECTIUNEA a 2-a

Definitii si principii

Art. 3. – În sensul prezentei legi, termenii si expresiile de mai jos au urmatoarea semnificatie:

a) administrarea incidentului – toate procedurile utilizate pentru detectarea, analiza si limitarea unui incident si raspunsul la acesta;

b) domain name system, denumit în continuare DNS – sistem de atribuire de nume distribuite ierarhic într-o retea în care se efectueaza cautari de nume de domenii;

c) furnizor de servicii digitale – orice persoana juridica care furnizeaza un serviciu digital;

d) furnizor de servicii DNS – entitate care furnizeaza servicii DNS pe internet;

e) incident – orice eveniment care are un impact real negativ asupra securitatii retelelor si a sistemelor informatice;

f) internet exchange point, denumit în continuare IXP – facilitate a retelei care permite interconectarea a mai mult de doua sisteme autonome independente, în special în scopul facilitarii schimbului de trafic de internet; IXP furnizeaza interconectare doar pentru sisteme autonome; IXP nu necesita trecerea printr-un al treilea sistem autonom a traficului de internet dintre orice pereche de sisteme autonome participante si nici nu modifica sau interfereaza într-un alt mod cu acest trafic;

g) motor de cautare online – un serviciu digital care permite utilizatorilor sa caute, în principiu, în toate site-urile internet sau site-urile internet într-o anumita limba pe baza unei interogari privind orice subiect sub forma unui cuvânt, a unei fraze sau a unei alte informatii-cheie si care revine cu linkuri în care se pot gasi informatii legate de continutul cautat;

h) operator de servicii esentiale – persoana fizica sau juridica de drept public sau privat de tipul celor prevazute în anexa care face parte integranta din prezenta lege, care furnizeaza un serviciu care îndeplineste conditiile prevazute la art. 6 alin. (1);

i) piata online – serviciu digital care permite consumatorilor si/sau comerciantilor, astfel cum sunt definiti la art. 3 alin. (1) lit. a) si b) din Ordonanta Guvernului nr. 38/2015 privind solutionarea alternativa a litigiilor dintre consumatori si comercianti, cu modificarile ulterioare, sa încheie cu comerciantii vânzari online sau contracte de servicii, fie pe site-ul internet al pietei online, fie pe site-ul internet al unui comerciant care utilizeaza servicii informatice furnizate de piata online;

j) registru de nume de domenii Top-level – entitate care administreaza si opereaza înregistrarea de nume de domenii de internet într-un domeniu Top-level (TLD) specific;

k) reprezentant – orice persoana fizica sau juridica stabilita în Uniunea Europeana desemnata explicit sa actioneze în numele unui furnizor de servicii digitale nestabilit în Uniunea Europeana, careia i se poate adresa autoritatea competenta la nivel national sau echipa de raspuns la incidente de securitate informatica, denumita în continuare echipa CSIRT sau CSIRT, în locul furnizorului de servicii digitale în ceea ce priveste obligatiile furnizorului de servicii digitale în temeiul prezentei legi;

l) retea si sistem informatic:

1. retea de comunicatii electronice în sensul prevederilor art. 4 alin. (1) pct. 6 din Ordonanta de urgenta a Guvernului nr. 111/2011 privind comunicatiile electronice, aprobata cu modificari si completari prin Legea nr. 140/2012, cu modificarile si completarile ulterioare;

2. orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relatie functionala, dintre care unul sau mai multe asigura prelucrarea automata a datelor cu ajutorul unui program informatic;

3. datele digitale stocate, prelucrate, recuperate sau transmise de

elementele prevazute la pct. 1 si 2 în vederea functionarii, utilizarii, protejarii si întretinerii lor;

m) risc – orice circumstanta sau eveniment ce poate fi identificat în mod rezonabil, anterior producerii sale, care are un efect potential negativ asupra securitatii retelelor si a sistemelor informatice;

n) securitatea retelelor si a sistemelor informatice – capacitatea unei retele si a unui sistem informatic de a rezista, la un nivel de încredere dat, oricarei actiuni care compromite disponibilitatea, autenticitatea, integritatea, confidentialitatea sau nonrepudierea datelor stocate ori transmise sau prelucrate ori a serviciilor conexe oferite de reteaua sau de sistemele informatice respective sau accesibile prin intermediul acestora;

o) serviciu digital – serviciu, în sensul prevederilor art. 4 alin. (1) pct. 2 din Hotarârea Guvernului nr. 1.016/2004 privind masurile pentru organizarea si realizarea schimbului de informatii în domeniul standardelor si reglementarilor tehnice, precum si al regulilor referitoare la serviciile societatii informationale între România si statele membre ale Uniunii Europene, precum si Comisia Europeana, cu modificarile si completarile ulterioare si care se încadreaza într-una din categoriile:

1. piata online;
2. motor de cautare online;
3. serviciu de cloud computing;

p) specificatie – specificatie tehnica, în sensul prevederilor art. 2 pct. 4 din Regulamentul (UE) nr. 1.025/2012 al Parlamentului European si al Consiliului din 25 octombrie 2012 privind standardizarea europeana, de modificare a Directivelor 89/686/CEE si 93/15/CEE ale Consiliului si a Directivelor 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE si 2009/105/CE ale Parlamentului European si ale Consiliului si de abrogare a Deciziei 87/95/CEE a Consiliului si a Deciziei nr. 1.673/2006/CE a Parlamentului European si a Consiliului;

q) standard – standard, în sensul prevederilor art. 2 pct. 1 din Regulamentul (UE) nr. 1.025/2012;

r) strategie nationala privind securitatea retelelor si a sistemelor informatice – cadru care furnizeaza obiective si prioritati strategice privind securitatea retelelor si a sistemelor informatice la nivel national;

s) serviciu de cloud computing – serviciu digital care permite accesul la un sistem configurabil de resurse sau servicii informatice care pot fi puse în comun;

s) valoare de prag – valoare minima/maxima, cuantificabila a indicatorilor în baza carora se determina gradul de îndeplinire a unui criteriu.

Art. 4. – Principiile care stau la baza prezentei legi:

a) principiul responsabilitatii si constientizarii – consta în efortul continuu derulat de entitatile de drept public si privat în constientizarea rolului si responsabilitatii individuale pentru atingerea unui nivel comun ridicat de securitate a retelelor si sistemelor informatice;

b) principiul proportionalitatii – consta în asigurarea unui echilibru între riscurile la care retelele si sistemele informatice sunt supuse si cerintele de securitate implementate;

c) principiul cooperarii si coordonarii – consta în realizarea în timp oportun a schimbului de informatii referitoare la riscurile de securitate la adresa retelelor si sistemelor informatice si asigurarea într-o maniera sincronizata a reactiei la producerea incidentelor.

CAPITOLUL II
Domeniul de aplicare

SECTIUNEA 1

Operatorii de servicii esentiale

Art. 5. – În vederea asigurarii unui nivel ridicat de securitate, operatorii de servicii esentiale se identifica si se înscriu în Registrul operatorilor de servicii esentiale.

Art. 6. – (1) Un serviciu este considerat esential daca furnizarea lui îndeplineste cumulativ urmatoarele conditii:

a) serviciul este esential în sustinerea unor activitati societale si/sau economice de cea mai mare importanta;

b) furnizarea sa depinde de o retea sau de un sistem informatic;

c) furnizarea serviciului este perturbata semnificativ în cazul producerii unui incident.

(2) Evaluarea gradului de perturbare a furnizarii serviciului esential se realizeaza în functie de urmatoarele criterii intersectoriale, fara a fi cumulative:

a) numarul de utilizatori care se bazeaza pe serviciul furnizat de entitatea în cauza;

b) dependenta altor sectoare prevazute în anexa la prezenta lege de serviciul furnizat de entitatea în cauza;

c) impactul pe care l-ar putea avea incidentele, în ceea ce priveste intensitatea si durata, asupra activitatilor economice si societale sau asupra sigurantei publice;

d) cota de piata a entitatii în cauza;

e) distributia geografica în ceea ce priveste zona care ar putea fi afectata de un incident;

f) importanta entitatii pentru mentinerea unui nivel suficient al serviciului, tinând cont de disponibilitatea unor mijloace alternative pentru furnizarea serviciului respectiv.

(3) Ministerul Comunicatiilor si Societatii Informationale, denumit în continuare MCSI, la propunerea Centrului National de Raspuns la Incidente de Securitate Cibernetica, denumit în continuare CERT-RO, supune aprobarii prin hotarâre a Guvernului în termen de 5 luni de la data intrarii în vigoare a prezentei legi:

a) valorile de prag pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul retelelor si sistemelor informatice ale operatorilor de servicii esentiale;

b) valorile de prag corespunzatoare criteriilor intersectoriale stabilite potrivit dispozitiilor alin. (2);

c) criteriile sectoriale specifice si valorile de prag corespunzatoare fiecarui sector si subsector de activitate prevazut în anexa;

d) normele tehnice de stabilire a impactului incidentelor.

(4) La nivelul MCSI se înfiinteaza si functioneaza Grupul de lucru interinstitutional pentru determinarea valorilor de prag necesare pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul retelelor si sistemelor informatice ale operatorilor de servicii esentiale, prevazute la alin. (3).

(5) MCSI, la propunerea CERT-RO, în termen de 3 luni de la data intrarii în vigoare a prezentei legi, supune aprobarii prin hotarâre a Guvernului componenta, atributiile si modul de organizare a Grupului de lucru interinstitutional prevazute la alin. (4).

(6) Determinarea valorilor de prag necesare pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul operatorilor de servicii esentiale care furnizeaza servicii din sectorul prevazut la pct. 7 din anexa se realizeaza cu consultarea Autoritatii Nationale pentru Administrare si Reglementare în Comunicatii.

Art. 7. – (1) Registrul prevazut la art. 5 se alcatuieste pentru

sectoarele si subsectoarele prevazute în anexa si raportat la criteriile prevazute la art. 6 si valorile de prag prevazute la art. 6 alin. (3).

(2) Registrul prevazut la alin. (1) se înfiinteaza, se întretine si se actualizeaza periodic, cel putin o data la doi ani de la data intrarii în vigoare a prezentei legi de catre CERT-RO în calitate de autoritate competenta la nivel national.

(3) Registrul prevazut la alin. (1) face parte din categoria documentelor clasificate.

(4) Normele metodologice de organizare si functionare a registrului prevazut la art. 5
se aproba, la propunerea directorului general al CERT-RO, prin ordin al ministrului comunicatiilor si societatii informationale, care se publica în Monitorul Oficial al României, Partea I.

Art. 8. - (1) Entitatile care îndeplinesc conditiile si criteriile prevazute la art. 6
si activeaza într-unul sau mai multe dintre sectoarele sau subsectoarele de activitate prevazute în anexa au obligatia sa notifice CERT-RO în vederea înscrierii în Registrul operatorilor de servicii esentiale.

(2) Prin exceptie de la alin. (1) identificarea în vederea înscrierii în Registrul operatorilor de servicii esentiale se poate face si de catre CERT-RO din oficiu în vederea îndeplinirii obligatiilor legale ce îi revin sau în urma unei sesizari privind sustragerea de la obligatia de notificare si înscriere în Registrul operatorilor de servicii esentiale facuta de catre orice persoana interesata, aducând la cunostinta entitatii vizate declansarea procedurii de identificare si comunicând la final operatorului rezultatul acesteia.

(3) Operatorii de servicii esentiale pot solicita asistenta CERT-RO în procesul de identificare.

(4) Înscrierea operatorilor de servicii esentiale în Registrul operatorilor de servicii esentiale se realizeaza prin decizia directorului general al CERT-RO care se comunica operatorului de servicii esentiale în urma depunerii unui raport de audit care atesta îndeplinirea cerintelor minime de securitate si notificare, întocmit de un auditor atestat în conformitate cu prevederile art. 32, si a evaluarii informatiilor si documentatiilor furnizate de operator în cadrul procesului de identificare.

(5) Atunci când o entitate furnizeaza un serviciu dintre cele reglementate la art. 6 alin. (1) lit. a) si în cadrul altor state membre ale Uniunii Europene, CERT-RO se consulta cu autoritatile omologe din statele respective în procesul de identificare înainte de adoptarea unei decizii privind identificarea operatorului.

(6) Notificarea prevazuta la alin. (1) se realizeaza în termen de 30 de zile de la data îndeplinirii conditiilor prevazute la art. 6 alin. (1)prin raportare la criteriile intersectoriale de stabilire a impactului unui incident prevazute la art. 6 alin. (2), respectiv la criteriile sectoriale, precum si la valorile de prag prevazute la art. 6 alin. (3)prin depunerea unei declaratii pe propria raspundere.

(7) Operatorii economici si celelalte entitati care opereaza ori furnizeaza servicii în cadrul sectoarelor si subsectoarelor definite în anexa au obligatia de a pune la dispozitia CERT-RO, la cererea acesteia în calitate de autoritate competenta la nivel national, în termen de 60 de zile de la data primirii solicitarii, documentatiile necesare, inclusiv rapoarte de audit, pentru:

a)stabilirea calitatii de operator de servicii esentiale în conformitate cu prevederile art. 6 si 7;

b)stabilirea masurilor necesare pentru conformarea cu cerintele prezentei legi;

c)stabilirea interdependentei si interconectarii retelelor si sistemelor informatice cu cele ale altor operatori de servicii esentiale ori furnizori de servicii digitale, inclusiv a celor pe care se bazeaza furnizarea serviciilor entitatii în cauza;

d)stabilirea listei de autoritati ale statului pentru care furnizeaza

serviciile definite la art. 6 alin. (1).

(8) Prin exceptie de la termenul general de furnizare a documentatiilor stabilit la alin. (7), termenul de realizare a auditurilor si de depunere a rapoartelor de audit prevazute la alin. (4) si (7) precum si tematica si obiectivele acestora se stabilesc de catre CERT-RO în urma evaluarii celorlalte informatii furnizate în conformitate cu prevederile alin. (7) si curge de la data primirii comunicarii termenului de catre entitatea vizata.

(9) Documentatia prevazuta la alin. (7) si (8) va fi stabilita prin normele metodologice de identificare a operatorilor de servicii esentiale si furnizorilor de servicii digitale, aprobate la propunerea directorului general al CERT-RO, prin ordin al ministrului comunicatiilor si societatii informationale, care se publica în Monitorul Oficial al României, Partea I.

Art. 9. - (1) Entitatile care nu mai îndeplinesc conditiile si criteriile prevazute la art. 6 notifica CERT-RO în vederea radierii din Registrul operatorilor de servicii esentiale si furnizeaza documentatiile relevante în conformitate cu art. 8 alin. (7)lit. a).

(2) CERT-RO dispune, prin decizia directorului general, radierea din Registrul operatorilor de servicii esentiale la cerere sau din oficiu, în urma evaluarii documentatiilor prevazute la alin. (1), si comunica operatorului decizia.

(3) Operatorii de servicii esentiale pot solicita asistenta CERT-RO cu privire la documentatiile prevazute la alin. (1) necesare în procesul de radiere.

(4) Atunci când o entitate furnizeaza un serviciu esential si în cadrul altor state membre ale Uniunii Europene, CERT-RO se consulta cu autoritatile omologe din statele respective înainte de adoptarea unei decizii privind radierea.

(5) Notificarea prevazuta la alin. (1) se realizeaza în termen de 30 de zile de la data la care entitatea nu mai îndeplineste conditiile prevazute la art. 6.

Art. 10. - (1) În scopul asigurarii securitatii retelelor si sistemelor informatice, operatorii de servicii esentiale au urmatoarele obligatii:

a) implementeaza masurile tehnice si organizatorice adecvate si proportionale pentru îndeplinirea cerintelor minime de securitate stabilite în temeiul prevederilor art. 25 alin. (3);

b) implementeaza masuri adecvate pentru a preveni si minimiza impactul incidentelor care afecteaza securitatea retelelor si a sistemelor informatice utilizate pentru furnizarea acestor servicii esentiale, cu scopul de a asigura continuitatea serviciilor respective, stabilite în temeiul prevederilor art. 25 alin. (3);

c) notifica de îndata CERT-RO în calitate de CSIRT national incidentele care au un impact semnificativ asupra continuitatii serviciilor esentiale furnizând cel putin informatiile prevazute la art. 26 alin. (3);

d) pun la dispozitia CERT-RO informatii care sa permita stabilirea impactului transfrontalier al incidentului în conformitate cu prevederile art. 26 alin. (3);

e) se supun controlului desfasurat de catre CERT-RO în vederea stabilirii gradului de respectare a obligatiilor ce le revin în temeiul prezentei legi;

f) stabilesc mijloacele permanente de contact, desemneaza responsabilii cu securitatea retelelor si sistemelor informatice însarcinati cu monitorizarea mijloacelor de contact si comunica CERT-RO în termen de 60 de zile de la înscrierea în Registrul operatorilor de servicii esentiale lista acestora, precum si orice modificari ulterioare de îndata ce au survenit;

g) comunica în termen de maximum 30 de zile catre CERT-RO, în calitate de autoritate competenta la nivel national, orice schimbare survenita în datele furnizate în cadrul procesului de identificare ca operator de servicii esentiale;

h) se interconecteaza în termen de 60 de zile de la înscrierea în Registrul operatorilor de servicii esentiale la serviciul de alertare si cooperare al CERT-RO, asigura monitorizarea permanenta a alertelor si

solicitarilor primite prin acest serviciu ori prin celelalte modalitati de contact si ia în cel mai scurt timp masurile adecvate de raspuns la nivelul retelelor si sistemelor informatice proprii;

i) asigura de îndata raspunsul la incidentele survenite, restabilesc în cel mai scurt timp functionarea serviciului la parametrii dinaintea incidentului si realizeaza auditul de securitate, conform prezentei legi.

(2) Operatorii de servicii esentiale pun la dispozitia CERT-RO în calitate de autoritate competenta la nivel national, la solicitarea acesteia facuta cu mentionarea scopului si precizând informatiile necesare si termenul de furnizare a acestora:

a) informatiile necesare pentru evaluarea securitatii retelelor si a sistemelor informatice vizate de prezenta lege, inclusiv politicile de securitate documentate;

b) rezultatele auditului de securitate realizat la solicitarea CERT-RO, inclusiv informatiile si documentatiile pe care se bazeaza acesta, precum si alte elemente care atesta punerea efectiva în aplicare a cerintelor minime de securitate.

(3) Notificarea de îndata a afectarii serviciilor esentiale prevazuta la alin. (1) lit.

c) se face si în situatia în care afectarea se datoreaza unor incidente care afecteaza un furnizor de servicii digitale de care depinde furnizarea serviciilor esentiale.

(4) Termenul de conformare pentru îndeplinirea obligatiilor prevazute la alin. (1) lit. a) si b) este de 6 luni de la data intrarii în vigoare a normelor tehnice privind cerintele de securitate si notificare ori, dupa caz, de la data înscrierii în Registrul operatorilor de servicii esentiale.

Art. 11. – Operatorii de servicii esentiale au obligatia sa implementeze în termenul de conformare stabilit în conformitate cu dispozitiile art. 37 masurile dispuse de CERT-RO pentru îndeplinirea cerintelor minime de securitate, în vederea remedierii deficientelor constatate cu ocazia controlului exercitat în temeiul art. 35.

SECTIUNEA a 2-a

Furnizorii de servicii digitale

Art. 12. – (1) Furnizorii de servicii digitale au urmatoarele obligatii:

a) implementeaza masurile tehnice si organizatorice adecvate si proportionale pentru îndeplinirea cerintelor minime de securitate a retelelor si sistemelor informatice stabilite în temeiul prevederilor prezentei legi cu privire la serviciile prevazute la art. 3 lit. o) pe care le ofera pe teritoriul Uniunii Europene tinând cont de normele tehnice prevazute la art. 25 alin. (1), în termen de 6 luni de la data intrarii în vigoare a acestora;

b) implementeaza, în termen de 6 luni de la data intrarii în vigoare a normelor tehnice prevazute la art. 25 alin. (1), masuri adecvate pentru a preveni si minimiza impactul incidentelor care afecteaza securitatea retelelor si a sistemelor informatice utilizate pentru furnizarea serviciilor prevazute la lit. a), asigura raspunsul la incidente si continuitatea serviciilor acestora;

c) notifica de îndata CERT-RO în calitate de CSIRT national incidentele care au un impact semnificativ asupra furnizarii serviciilor prevazute la art. 3 lit. o), furnizând cel putin informatiile prevazute la art. 26 alin. (3);

d) pun la dispozitia CERT-RO informatii care sa permita stabilirea impactului transfrontalier al incidentului în conformitate cu prevederile art. 26 alin. (3);

e) stabilesc mijloace permanente de contact, desemneaza responsabilii cu securitatea retelelor si sistemelor informatice însarcinati cu monitorizarea canalelor de contact si comunica CERT-RO, în termen de 60 de zile de la data intrarii în vigoare a prezentei legi, lista acestora, precum si orice modificari ulterioare de îndata ce au survenit;

f) se interconecteaza în termen de 60 de zile de la data intrarii în vigoare a prezentei legi la serviciul de alertare si cooperare al CERT-RO, asigura monitorizarea permanenta a alertelor si solicitarilor primite prin acest serviciu ori prin celelalte modalitati de contact si ia în cel mai scurt timp masurile adecvate de raspuns la nivelul retelelor si sistemelor informatice proprii.

(2) Furnizorii de servicii digitale pun la dispozitia CERT-RO în calitate de autoritate competenta la nivel national, la solicitarea acesteia facuta cu mentionarea scopului si precizând informatiile necesare si termenul de furnizare a acestora:

a) informatiile necesare pentru evaluarea securitatii retelelor si a sistemelor informatice vizate de prezenta lege, inclusiv politicile de securitate documentate;

b) rezultatele auditului de securitate realizat, inclusiv informatiile si documentatiile pe care se bazeaza acesta, precum si alte elemente care atesta punerea efectiva în aplicare a cerintelor minime de securitate.

(3) Obligatia de notificare prevazuta la alin. (1) lit. c) se aplica doar în cazul în care furnizorul de servicii digitale are acces la informatiile necesare pentru evaluarea impactului incidentului prevazute la art. 26 si care sa permita evaluarea prevazuta la art. 28.

(4) Prevederile prezentei legi se aplica furnizorilor de servicii digitale care au stabilit sediul social pe teritoriul României precum si celor din afara Uniunii Europene care stabilesc sediul reprezentantei din Uniune pe teritoriul României.

(5) Prevederile alin. (1)-(4), art. 25 alin. (4), art. 26 alin. (2) din prezenta lege nu se aplica furnizorilor de servicii digitale care se încadreaza în categoria întreprinderilor mici si mijlocii, asa cum sunt definite în Legea nr. 346/2004 privind stimularea înfiintarii si dezvoltarii întreprinderilor mici si mijlocii, cu modificarile si completarile ulterioare.

(6) Operatorii economici, precum si celelalte entitati care furnizeaza servicii digitale au obligatia de a furniza catre CERT-RO, în termen de 60 de zile de la data primirii solicitarii facuta cu mentionarea scopului si precizând informatiile necesare, urmatoarele categorii de documente:

a) documentatiile necesare stabilirii calitatii de furnizor de servicii digitale în sensul prezentei legi;

b) documentatiile necesare stabilirii interdependentei si interconectarii retelelor si sistemelor informatice cu cele ale altor operatori de servicii esentiale ori furnizori de servicii digitale;

c) stabilirea listei de autoritati ale statului pentru care furnizeaza serviciile definite la art. 3 lit. o).

(7) Documentatia prevazuta la alin. (6) va fi stabilita prin normele metodologice prevazute la art. 8 alin. (9).

CAPITOLUL III
Roluri si responsabilitati

SECTIUNEA 1
Coordonarea strategica la nivel national

Art. 13. - Coordonarea strategica la nivel national a activitatilor de asigurare a unui nivel comun ridicat de securitate a retelelor si

sistemelor informatice se realizeaza de catre Guvern prin Ministerul Comunicatiilor si Societatii Informationale sub aspectul politicilor publice si al initiativei legislative în domeniu.

Art. 14. – Strategia nationala privind securitatea retelelor si a sistemelor informatice se aproba prin hotarâre a Guvernului, la propunerea MCSI în termen de 6 luni de la data intrarii în vigoare a prezentei legi.

SECTIUNEA a 2-a

Autoritati competente si responsabilitati

Art. 15. – (1) CERT-RO este autoritate competenta la nivel national pentru securitatea retelelor si a sistemelor informatice care asigura furnizarea serviciilor esentiale ori furnizeaza serviciile digitale identificate în temeiul prezentei legi.

(2) Pentru asigurarea unui nivel ridicat de securitate a retelelor si sistemelor informatice, CERT-RO se consulta si coopereaza cu:

a) Serviciul Român de Informatii, pentru securitatea retelelor si a sistemelor informatice care asigura servicii esentiale a caror afectare aduce atingere securitatii nationale;

b) Ministerul Apararii Nationale, pentru securitatea retelelor si a sistemelor informatice care asigura servicii esentiale în sprijinul activitatilor privind apararea nationala;

c) Ministerul Afacerilor Interne, Oficiul Registrului National al Informatiilor Secrete de Stat, Serviciul de Informatii Externe, Serviciul de Telecomunicatii Speciale si Serviciul de Protectie si Paza, pentru securitatea retelelor si a sistemelor informatice care asigura servicii esentiale în domeniul lor de activitate si responsabilitate.

Art. 16. – CERT-RO se consulta si coopereaza, dupa caz, cu:

a) organele de urmarire penala;

b) Autoritatea Nationala pentru Administrare si Reglementare în Comunicatii, atunci când incidentele au ca rezultat afectarea securitatii ori functionarii retelelor publice de comunicatii electronice ori când pentru administrarea unui incident sunt necesare masuri ce intra în aria de activitate si responsabilitate a acesteia;

c) Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal în cazul incidentelor care au ca rezultat încalcarea securitatii datelor cu caracter personal, în conditiile legii.

SECTIUNEA a 3-a

Echipele de interventie în caz de incidente de securitate informatica

Art. 17. – (1) Echipa CSIRT definita la art. 19 lit. b) respecta cerintele de la art. 24 si acopera sectoarele din anexa si serviciile prevazute la art. 3 lit. o).

(2) Persoanele juridice care activeaza în cadrul aceluiasi sector sau subsector de activitate din anexa la prezenta lege pot constitui echipe CSIRT proprii sau sectoriale ori pot achizitiona servicii de specialitate de tip CSIRT.

(3) Entitatile prevazute la art. 15 alin. (2) si art. 16 lit. b) pot constitui echipe CSIRT pentru asigurarea securitatii retelelor si sistemelor informatice conform domeniului de activitate si

responsabilitate.

(4) Echipele CSIRT sectoriale se autorizeaza si se desemneaza de catre CERT-RO în urma evaluarii îndeplinirii conditiilor specifice de autorizare a acestui tip de echipe elaborate în conformitate cu prevederile art. 20 lit. e).

Art. 18. - (1) Echipele CSIRT proprii, sectoriale sau serviciile de specialitate prevazute la art. 17 alin. (2) care deservesc operatori de servicii esentiale si furnizori de servicii digitale au urmatoarele obligatii:

a) sa fie autorizate de catre CERT-RO în temeiul prezentei legi;

b) sa asigure compatibilitatea si interoperabilitatea sistemelor, procedurilor si metodelor utilizate cu cele ale echipei CSIRT nationale din cadrul CERT-RO;

c) sa furnizeze cel putin setul minim de servicii de tip CSIRT necesar asigurarii la nivel national a unei protectii unitare a operatorilor si furnizorilor ce fac obiectul prezentei legi;

d) sa utilizeze în cadrul echipelor un numar corespunzator de persoane calificate în conformitate cu prezenta lege;

e) sa se interconecteze la serviciul de alerta, monitorizare si cooperare al CERT-RO si sa asigure un raspuns prompt la alertele si solicitarile transmise de echipa CSIRT nationala.

(2) Normele tehnice privind compatibilitatea si interoperabilitatea prevazute la alin. (1) lit. b), setul minim de servicii mentionat la alin. (1) lit. c) si criteriile de stabilire a numarului de persoane calificate prevazute la alin. (1) lit. d) se aproba, la propunerea directorului general al CERT-RO, prin ordin al ministrului comunicatiilor si societatii informationale, care se publica în Monitorul Oficial al României, Partea I.

SECTIUNEA a 4-a

Autoritatea competenta la nivel national - CERT-RO

Art. 19. - În cadrul CERT-RO se organizeaza si functioneaza si:

a) punctul unic de contact la nivel national;

b) echipa de raspuns la incidente de securitate informatica la nivel national, denumita în continuare echipa CSIRT nationala sau CSIRT national.

Art. 20. - CERT-RO, în calitate de autoritate competenta la nivel national, are urmatoarele atributii generale:

a) identifica, cu consultarea autoritatilor si entitatilor de reglementare si administrare a sectoarelor si subsectoarelor prevazute în anexa, operatorii de servicii esentiale care au sediul social, filiala, sucursala sau punct de lucru pe teritoriul României;

b) elaboreaza si actualizeaza normele tehnice privind cerintele minime de asigurare a securitatii retelelor si sistemelor informatice;

c) elaboreaza si actualizeaza normele tehnice privind îndeplinirea obligatiilor de notificare a incidentelor de securitate de catre operatorii si furnizorii prevazuti de prezenta lege;

d) coordoneaza activitatea Grupului de lucru interinstitutional mentionat la art. 6 alin. (4);

e) elaboreaza si actualizeaza, dupa consultarea celorlalte institutii cu responsabilitati în domeniul apararii, ordinii publice si securitatii nationale, precum si a altor institutii si autoritati, dupa caz, normele metodologice, tehnice, precum si regulamentele privind cerintele referitoare la înfiintarea, autorizarea si functionarea echipelor CSIRT, desemnarea echipelor CSIRT sectoriale, cele referitoare la atestarea auditorilor calificati cu competente în domeniul securitatii serviciilor esentiale si a serviciilor digitale, precum si normele referitoare la autorizarea formatorilor si furnizorilor de servicii de formare pentru

activitatile prevazute la lit. o) si p);

f)elaboreaza si promoveaza practici comune pentru administrarea incidentelor si a riscurilor si pentru sistemele de clasificare a incidentelor, riscurilor si informatiilor;

g)participa, prin reprezentanti, la Grupul de cooperare la nivelul Uniunii Europene constituit pentru a facilita cooperarea strategica si schimbul de informatii între statele membre, pentru a consolida încrederea si în vederea obtinerii unui nivel comun ridicat de securitate a retelelor si a sistemelor informatice în Uniunea Europeana si compus din reprezentanti ai statelor membre, ai Comisiei Europene si ai Agentiei Uniunii Europene pentru Securitatea Retelelor si a Informatiilor - ENISA, în vederea adoptarii solutiilor optime pentru atingerea obiectivului de securitate si a schimbului de informatii între statele membre, respectiv:

(i)dupa caz, participa la schimbul de experienta privind aspecte legate de securitatea retelelor si a sistemelor informatice cu institutii, organe, oficii si agentii relevante ale Uniunii Europene;

(ii)participa la dezbateri privind standardele si specificatiile prevazute la art. 25 alin. (6) cu reprezentanti ai organizatiilor de standardizare europene relevante;

(iii)colecteaza exemple de bune practici privind riscurile si incidentele;

h)permite echipelor CSIRT acces la datele privind incidentele notificate de operatorii de servicii esentiale sau de furnizorii de servicii digitale, în masura necesara pentru a-si îndeplini atributiile, cu respectarea legii;

i)verifica în conditiile art. 35-42 respectarea de catre operatorii de servicii esentiale si furnizorii de servicii digitale a obligatiilor ce le revin conform prezentei legi;

j)emite în temeiul art. 37 dispozitii cu caracter obligatoriu pentru operatorii de servicii esentiale în vederea conformarii si remedierii deficientelor constatate si stabileste termenul pâna la care acestia trebuie sa se conformeze;

k)instituie masuri de supraveghere ex post pentru furnizorii de servicii digitale cu privire la neîndeplinirea obligatiilor ce le revin conform prevederilor prezentei legi;

l)primeste sesizari cu privire la neîndeplinirea obligatiilor operatorilor si furnizorilor prevazuti de prezenta lege;

m)coopereaza cu autoritatile competente din celelalte state si ofera asistenta acestora, prin schimbul de informatii, transmiterea de solicitari si sesizari, efectuarea controlului ori luarea de masuri de supraveghere si remediere a deficientelor constatate, în cazul operatorilor si furnizorilor prevazuti de prezenta lege care îsi au sediul principal în România ori care, desi au sediul principal stabilit în alt stat membru, retelele sau sistemele informatice ale acestora sunt situate si pe teritoriul României;

n)monitorizeaza aplicarea prevederilor prezentei legi;

o)autorizeaza, revoca sau reînnoieste autorizarea echipelor CSIRT ce deservesc operatori de servicii esentiale ori furnizori de servicii digitale;

p)elibereaza, revoca sau reînnoieste atestatele auditorilor de securitate informatica care pot efectua audit în cadrul retelelor si sistemelor informatice ce sustin servicii esentiale ori furnizeaza servicii digitale în conditiile prezentei legi;

q)autorizeaza, revoca sau reînnoieste autorizarea formatorilor si furnizorilor de servicii de formare pentru activitatile prevazute la lit. o) si p);

r)alcatuieste si actualizeaza periodic, cel putin o data la doi ani, începând cu data intrarii în vigoare a prezentei legi, lista serviciilor esentiale care îndeplinesc conditiile de la art. 6 alin. (1), cu consultarea autoritatilor si entitatilor prevazute la lit. a), precum si a celor prevazute la art. 15 alin. (2), si o înainteaza MCSI spre a fi supusa aprobarii prin hotarâre a Guvernului. Prima lista se supune aprobarii Guvernului în termen de 6 luni de la data intrarii în vigoare a prezentei

legi;

s)propune spre aprobare MCSI normele tehnice, metodologice si regulamentele prevazute de prezenta lege, în termen de 6 luni de la data intrarii în vigoare a acesteia.

Art. 21. – În calitate de punct national unic de contact, CERT-RO are urmatoarele atributii:

a)exercita o functie de legatura între autoritatile statului si autoritatile similare din alte state, Grupul de cooperare si reteaua echipelor de raspuns la incidentele de securitate informatica, denumita în continuare reteaua CSIRT;

b)elaboreaza si transmite Grupului de cooperare rapoarte de sinteza privind notificarile primite si actiunile întreprinse;

c)transmite, la cererea autoritatilor sau a echipelor CSIRT, catre punctele unice de contact din celelalte state membre notificarile si solicitarile privind incidentele ce afecteaza functionarea serviciilor esentiale si a celor digitale de pe teritoriul respectivelor state;

d)transmite autoritatilor prevazute la art. 15 alin. (2) si art. 16 notificarile si cererile primite din alte state membre, potrivit ariei de responsabilitate.

Art. 22. – (1) În calitate de CSIRT national, CERT-RO are urmatoarele atributii:

a)monitorizeaza incidentele de securitate a retelelor si sistemelor informatice la nivel national;

b)emite avertizari timpurii, alerte si anunturi si dissemineaza informatiile privind riscurile si incidentele catre autoritatile prevazute la art. 15 alin. (2), precum si orice entitate de drept public sau privat careia îi poate fi afectata securitatea retelelor si sistemelor informatice;

c)primeste notificari privind incidentele care afecteaza retelele si sistemele operatorilor de servicii esentiale ori ale furnizorilor de servicii digitale;

d)furnizeaza operatorului de servicii esentiale care a facut notificarea, în masura posibilitatilor, informatii relevante în ceea ce priveste actiunile ulterioare notificarii;

e)stabileste, în baza notificarilor primite, impactul la nivel national si transfrontalier al incidentelor si informeaza autoritatile relevante la nivel national, precum si autoritatile similare din alte state potential afectate;

f)aduce la cunostinta publicului periodic si ori de câte ori este necesar avertizari, alerte si informari privind riscuri si amenintari, posibile masuri de prevenire si contracarare, în scopul cunoasterii de catre public a acestora si al luarii masurilor adecvate, si publica statistici privitoare la incidentele identificate la nivel national, cu respectarea conditiilor prezentei legi;

g)asigura raspunsul la incidente în limitele prezentei legi;

h)elaboreaza analize dinamice de risc si de incident;

i)coopereaza, la nivel national, cu echipele CSIRT în cadrul unei platforme de management al incidentelor si pentru schimbul de informatii;

j)participa la actiunile comune în cadrul retelei CSIRT la nivel european, precum si, dupa necesitati, la actiunile solicitate în cadrul retelelor internationale de cooperare;

k)poate solicita asistenta ENISA pentru ducerea la îndeplinire a atributiilor sale;

l)înfiinteaza, întretine si opereaza serviciul de alertare si cooperare cu operatorii de servicii esentiale si furnizorii de servicii digitale mentionat la art. 10 alin. (1)lit. h) si art. 12 alin. (1)lit. f).

(2) Echipele CSIRT se conecteaza si realizeaza schimbul de informatii cu echipa CSIRT nationala aflata în cadrul CERT-RO prin intermediul platformei de management al incidentelor, mentionata la alin. (1) lit. i).

(3) În vederea administrarii adecvate a incidentelor majore la nivel national ori pentru administrarea unor incidente care necesita înalta

specializare si pregatire tehnica de specialitate, CERT-RO poate dezvolta parteneriate si alcatui echipe mixte compuse din specialisti proprii si specialisti proveniti de la alte institutii ori entitati din mediul privat, cu respectarea legii si asigurarea conditiilor privind confidentialitatea si accesul la informatii în limitele legii si cu acordul partilor implicate în incident.

Art. 23. - (1) În scopul cooperarii operationale, echipa CSIRT nationala care functioneaza în cadrul CERT-RO participa la reteaua CSIRT compusa din reprezentanti ai echipelor CSIRT nationale ale statelor membre din Uniunea Europeana si cea a CERT-UE.

(2) Cooperarea prevazuta la alin. (1) se realizeaza prin:

a) schimbul de informatii privind serviciile, operatiunile si posibilitatile de cooperare;

b) schimbul si analiza informatiilor fara caracter comercial referitoare la incidentele ce afecteaza un stat membru;

c) schimbul de informatii fara caracter confidential privind incidente individuale;

d) participarea la elaborarea unui raspuns coordonat al Retelei CSIRT, pentru managementul unui incident identificat pe teritoriul unui alt stat membru;

e) acordarea de sprijin voluntar în abordarea incidentelor transfrontaliere;

f) analiza si identificarea de noi forme de cooperare operationala în cadrul retelei CSIRT;

g) participarea la elaborarea de orientari si practici unitare în domeniul cooperarii operationale;

h) solicitarea retelei CSIRT de a asigura un raspuns coordonat la un incident identificat la nivel national.

(3) Fac exceptie de la schimbul de informatii prevazut la alin. (2) lit. c) situatiile în care schimbul ar periclita investigarea incidentului.

(4) Echipa CSIRT participa si la alte retele internationale de cooperare, dupa necesitati.

Art. 24. - (1) În vederea îndeplinirii atributiilor ce îi revin în calitate de autoritate competenta la nivel national în temeiul art. 20, din bugetul CERT-RO se asigura resursele materiale, financiare si umane suficiente pentru:

a) desfasurarea activitatilor de normare prevazute la art. 20 lit. a)-f) si r);

b) primirea sesizarilor, efectuarea controlului, verificarilor si supravegherilor prevazute la art. 20 lit. i)-l), precum si pentru asigurarea punerii în aplicare a deciziilor si sanctiunilor, rezolvarii contestatiilor si reprezentarea în contencios administrativ;

c) desfasurarea activitatilor de cooperare prevazute la art. 20 lit. g), h) si m), înfiintarea, administrarea si functionarea registrelor si evidentelor prevazute de art. 20 lit. o)-r), precum si a Registrului operatorilor de servicii esentiale prevazut la art. 5;

d) desfasurarea activitatilor de autorizare si acreditare prevazute la art. 20 lit. o)-q);

e) luarea masurilor cu caracter exceptional prevazute la art. 41.

(2) În vederea îndeplinirii atributiilor ce îi revin în calitate de punct unic de contact la nivel national, din bugetul CERT-RO se asigura resursele materiale, financiare si umane suficiente pentru asigurarea în regim permanent a functiei de legatura, primire si retransmitere a cererilor si solicitarilor prevazute la art. 21 lit. a), c) si d).

(3) În vederea îndeplinirii atributiilor ce îi revin în calitate de echipa CSIRT nationala conform prevederilor art. 22 si 23, din bugetul CERT-RO se asigura resursele materiale, financiare si umane suficiente pentru:

a) alertele prevazute la art. 22 alin. (1) lit. a) si c);

b) emiterea avertizarilor, contactarea si alertarea altor entitati si diseminarea de informatii relevante în temeiul art. 22 alin. (1) lit. b),

d)-f) si l);
c) asigurarea raspunsului, interventiei si cooperarii în temeiul art. 22 alin. (1) lit. g), i)-l);
d) stabilirea impactului incidentelor si analiza acestora în temeiul art. 22 alin. (1) lit. e) si h).
(4) Resursele financiare, materiale si umane alocate CERT-RO vor asigura:
a) continuitatea activitatilor si disponibilitatea permanenta a serviciilor;
b) participarea la Grupul de cooperare prevazut de art. 20 lit. g);
c) un sistem adecvat de gestionare si transmitere a cererilor;
d) o infrastructura adecvata prevazuta cu sisteme redundante;
e) spatiu de lucru de rezerva în amplasamente securizate;
f) disponibilitatea ridicata a serviciilor de comunicatii prin mijloace multiple de contact, capacitatea de a contacta alte entitati în orice moment si evitarea punctelor unice de defectiune;
g) amplasamente securizate ale sediilor echipei CSIRT nationale din cadrul CERT-RO si ale sistemelor informatice de suport;
h) mijloacele necesare asigurarii controlului punerii în aplicare a dispozitiilor prezentei legi si aplicarii de sanctiuni precum si pentru îndeplinirea celorlalte obligatii ce îi revin conform legii;
i) personalul adecvat, inclusiv din punctul de vedere al competentelor.
(5) Începând cu 1 ianuarie 2019, resursele financiare necesare pentru functionarea CERT-RO se asigura din venituri proprii prevazute la alin. (6) si în completare din subventii de la bugetul de stat prin bugetul MCSI.
(6) Începând cu 1 ianuarie 2019, CERT-RO poate retine si utiliza urmatoarele categorii de venituri proprii:
a) sumele provenite din activitatile prevazute la art. 32 alin. (2) lit. c) si e), respectiv activitatile prevazute la art. 33 alin. (2) lit. c) si e);
b) sumele provenite din furnizarea serviciului prevazut la art. 22 alin. (1) lit. l).
(7) Cuantumul tarifului pentru serviciile prevazute la alin. (6) se stabileste prin ordin al ministrului comunicatiilor si societatii informationale, la propunerea directorului general al CERT-RO, si se publica în Monitorul Oficial al României, Partea I.
(8) Din bugetul CERT-RO se asigura, cu respectarea prevederilor legale în vigoare, si urmatoarele categorii de cheltuieli:
a) achizitionarea de servicii de specialitate;
b) închirierea, achizitionarea sau constructia de imobile în vederea desfasurarii activitatii;
c) achizitia de echipamente si software, inclusiv software dezvoltat la comanda;
d) afilierea la retele si organizatii internationale de profil si participarea prin reprezentanti la lucrarile acestora precum si la alte evenimente de profil;
e) cursuri de formare si perfectionare precum si certificari ale personalului propriu;
f) editarea de publicatii, ghiduri de specialitate, clipuri video de constientizare;
g) organizarea de conferinte, seminare si alte evenimente de profil;
h) efectuarea de studii statistice si activitati de cercetare;
i) renovari si îmbunatatiri ale sediilor si locatiilor de desfasurare a activitatii.
(9) CERT-RO poate folosi pentru desfasurarea activitatii bunuri materiale si fonduri banesti primite de la persoanele juridice si fizice, sub forma de donatii si sponsorizari, cu respectarea dispozitiilor legale si asigurarea transparentei privind donatiile, sponsorizarile si sursa acestora.
(10) CERT-RO poate înfiinta birouri si sedii la nivel local în vederea asigurarii activitatilor si reprezentarii adecvate pentru îndeplinirea

obligatiilor ce îi revin în temeiul prezentei legi.

CAPITOLUL IV
Asigurarea securitatii retelelor si sistemelor informatice

SECTIUNEA 1
Cerintele minime de securitate

Art. 25. – (1) În vederea asigurarii unui nivel comun de securitate a retelelor si sistemelor informatice, operatorii de servicii esentiale si furnizorii de servicii digitale au obligatia de a respecta normele tehnice elaborate de CERT-RO în temeiul prevederilor art. 20 lit. b).

(2) CERT-RO elaboreaza, cu consultarea autoritatilor care reglementeaza sectoarele si subsectoarele prevazute în anexa, ghiduri în sprijinul implementarii masurilor minime de securitate pentru operatorii si furnizorii prevazuti în prezenta lege.

(3) Normele tehnice prevazute la alin. (1) aplicabile operatorilor de servicii esentiale se stabilesc în baza cel putin a urmatoarelor categorii de activitati de asigurare a securitatii retelelor si sistemelor informatice:

a) managementul drepturilor de acces;
b) constientizarea si instruirea utilizatorilor;
c) jurnalizarea si asigurarea trasabilitatii activitatilor în cadrul retelelor si sistemelor informatice;
d) testarea si evaluarea securitatii retelelor si sistemelor informatice;
e) managementul configuratiilor retelelor si sistemelor informatice;
f) asigurarea disponibilitatii serviciului esential si a functionarii retelelor si sistemelor informatice;
g) managementul continuitatii functionarii serviciului esential;
h) managementul identificarii si autentificarii utilizatorilor;
i) raspunsul la incidente;
j) mentenanta retelelor si sistemelor informatice;
k) managementul suporturilor de memorie externa;
l) asigurarea protectiei fizice a retelelor si sistemelor informatice;
m) realizarea planurilor de securitate;
n) asigurarea securitatii personalului;
o) analizarea si evaluarea riscurilor;
p) asigurarea protectiei produselor si serviciilor aferente retelelor si sistemelor informatice;
q) managementul vulnerabilitatilor si alertelor de securitate.

(4) Normele tehnice prevazute la alin. (1) aplicabile furnizorilor de servicii digitale se stabilesc în baza urmatoarelor categorii de activitati de asigurare a securitatii retelelor si sistemelor informatice:

a) securitatea sistemelor si a instalatiilor;
b) gestionarea incidentelor;
c) gestionarea continuitatii activitatii;
d) monitorizarea, auditarea si testarea;
e) conformitatea cu standardele europene si internationale.

(5) În implementarea masurilor de la alin. (1) operatorii de servicii esentiale:

a) identifica retelele si sistemele informatice care sustin furnizarea de servicii esentiale;
b) elaboreaza si implementeaza politici si planuri proprii de securitate a retelelor si sistemelor informatice;
c) asigura managementul incidentelor care afecteaza securitatea retelelor

si sistemelor informatice;
d) previn accesul neautorizat la retelele si sistemele informatice;
e) previn diseminarea datelor detinute la nivelul retelelor si sistemelor informatice catre alte persoane decât cele autorizate sa cunoasca continutul acestora;
f) implementeaza un sistem de management al riscului;
g) implementeaza planuri de actiune pe niveluri de alerta de securitate a retelelor si sistemelor informatice;
h) asigura continuitatea serviciilor.
(6) Normele tehnice prevazute la alin. (1) se emit cu luarea în considerare a cerintelor si standardelor europene si internationale fara a impune sau a discrimina în favoarea utilizarii unui anumit tip de tehnologie.

SECTIUNEA a 2-a
Notificarea incidentelor de securitate

Art. 26. - (1) Notificarile efectuate de operatorii de servicii esentiale în temeiul art. 10 alin. (1) lit. c) trebuie sa îndeplineasca conditiile si sa contina informatiile prevazute în normele tehnice prevazute la art. 20 lit. c).
(2) Notificarile efectuate de furnizorii de servicii digitale în temeiul prevederilor art. 12 alin. (1) lit. c) trebuie sa îndeplineasca conditiile si sa contina informatiile prevazute în normele tehnice prevazute la art. 20 lit. c).
(3) Notificarea incidentelor contine, în mod obligatoriu, urmatoarele informatii:
a) elementele de identificare ale infrastructurii si operatorului sau furnizorului în cauza;
b) descrierea incidentului;
c) perioada de desfasurare a incidentului;
d) impactul estimat al incidentului;
e) masuri preliminare adoptate;
f) lista de autoritati ale statului afectate de incident;
g) întinderea geografica potentiala a incidentului;
h) date despre efecte potential transfrontaliere ale incidentului.
(4) Notificarea prevazuta la alin. (1) si (2) nu va contine:
a) informatii clasificate;
b) date care pot aduce atingere drepturilor si libertatilor cetatenesti ori intereselor legitime ale unor terte entitati implicate în incident, în conditiile legii.
(5) CERT-RO, în calitate de autoritate competenta la nivel national, elaboreaza si actualizeaza, prin decizie a directorului general publicata în Monitorul Oficial al României, Partea I, formularele necesare notificarilor de incident efectuate în temeiul prezentului articol, detaliind informatiile si documentatiile necesar a fi furnizate.
(6) CERT-RO, în calitate de CSIRT national, va stabili si va aduce la cunostinta publicului, precum si operatorilor si furnizorilor mentionati în prezenta lege mijloacele de comunicare pentru efectuarea notificarilor cerute prin prezenta lege.
(7) Notificarile privind incidentele ce fac obiectul prezentei legi pot fi facute si de catre echipele CSIRT ale entitatilor de drept public sau privat ori care deservesc un anumit sector de activitate ori de catre furnizorii de servicii de securitate aflati în relatie contractuala, conform atributiilor ce le revin în baza actului de înfiintare ori a contractului de prestari servicii, dupa caz.
(8) Notificarea facuta de o echipa CSIRT în temeiul alin. (7)

echivaleaza cu notificarea facuta de operatorul sau furnizorul afectat, acesta purtând întreaga raspundere pentru continutul notificarii si îndeplinirea celorlalte obligatii ce îi revin conform prezentei legi.

(9) Obligatia de a notifica un incident de catre furnizorii de servicii digitale se aplica doar în cazul în care acestia au acces la informatiile necesare pentru a evalua impactul unui incident asupra parametrilor mentionati la art. 28 alin. (2).

(10) Entitatile care nu au fost identificate drept operatori de servicii esentiale si nu sunt furnizori de servicii digitale pot notifica voluntar CERT-RO, în calitate de CSIRT national, furnizând cel putin informatiile prevazute la alin. (3), incidentele care au un impact semnificativ asupra continuitatii serviciilor pe care le furnizeaza.

(11) CERT-RO trateaza notificarile obligatorii cu prioritate fata de notificarile voluntare.

(12) Notificarile voluntare se trateaza doar atunci când aceasta prelucrare nu împiedica îndeplinirea celorlalte obligatii ce îi revin autoritatii competente la nivel national si în limita resurselor existente.

(13) Notificarea voluntara nu impune entitatii notificatoare nicio obligatie care nu i-ar fi revenit daca nu ar fi facut notificarea.

(14) Notificarile prevazute la alin. (1) si (2) nu atrag raspunderea pentru entitatile care notifica, în conditiile respectarii obligatiilor prevazute de prezenta lege.

SECTIUNEA a 3-a

Managementul incidentelor

Art. 27. - Dupa primirea notificarii, CERT-RO, în calitate de CSIRT national:

a) evalueaza preliminar impactul incidentului la nivel national si alerteaza, sesizeaza ori notifica sau, dupa caz, poate solicita operatorului sau furnizorului sa alerteze alte entitati afectate precum si autoritatile cu responsabilitati în prevenirea, limitarea si combaterea efectelor incidentului, precum si autoritatile prevazute la art. 16, potrivit legii;

b) poate solicita informatii suplimentare operatorului sau furnizorului care a facut notificarea în vederea îndeplinirii obligatiilor ce îi revin, mentionând termenul de furnizare a acestora;

c) ofera operatorului sau furnizorului care a facut notificarea, atunci când circumstantele o permit, informatii care ar putea sprijini administrarea incidentului;

d) în calitate de punct unic de contact, informeaza celelalte state membre sau partenere afectate daca incidentul are un impact semnificativ asupra continuitatii serviciilor esentiale ori a serviciilor digitale în statele respective;

e) în urma analizei incidentelor, poate, dupa caz, declansa actiune de control pentru verificarea respectarii cerintelor prezentei legi;

f) poate lua masurile prevazute la art. 41;

g) coordoneaza la nivel national raspunsul la incident în colaborare cu celelalte autoritati si entitati publice sau private, conform domeniului de activitate si responsabilitate.

Art. 28. - (1) Impactul unui incident se determina tinând cont cel putin de urmatorii parametri:

(i) în cazul operatorilor de servicii esentiale:

a) numarul de utilizatori afectati de perturbarea serviciului esential;

b) durata incidentului;

c) distributia geografica în ceea ce priveste zona afectata de incident;

(ii) în cazul furnizorilor de servicii digitale:

a) numarul de utilizatori afectati de incident, în special utilizatori care se bazeaza pe serviciul pentru furnizarea propriilor servicii;
b) durata incidentului;
c) distributia geografica în ceea ce priveste zona afectata de incident;
d) amploarea perturbarii functionarii serviciului;
e) amploarea impactului asupra activitatilor economice si societale.

(2) Grupul de lucru interinstitutional prevazut la art. 6 alin. (4) elaboreaza si actualizeaza normele tehnice de stabilire a impactului pentru categoriile de operatori si furnizori prevazuti de prezenta lege.

(3) Criteriile prevazute la pct. 2. se aplica si notificarilor voluntare efectuate în temeiul prevederilor art. 26 alin. (10).

Art. 29. – (1) CERT-RO poate înstiinta publicul, atunci când informarea este necesara pentru a preveni un incident sau pentru a se administra un incident în curs.

(2) Pentru incidentele care afecteaza un operator de servicii esentiale sau un furnizor de servicii digitale, informarea mentionata la alin. (1) se realizeaza dupa consultarea prealabila a acestuia asupra continutului înstiintarii.

(3) În cazul furnizorilor de servicii digitale, informarea publicului specificata la alin. (1) poate fi facuta si direct de catre acestia la solicitarea CERT-RO ori a autoritatilor sau echipelor CSIRT ale altor state membre afectate.

Art. 30. – (1) În activitatile de identificare a operatorilor de servicii esentiale si furnizorilor de servicii digitale, de control, de primire a notificarilor privitoare la incidente si de management al acestora desfasurate în baza prezentei legi, precum si în procesele interne, CERT-RO protejeaza interesele de securitate si comerciale ale operatorului de servicii esentiale si ale furnizorului de servicii digitale, precum si confidentialitatea informatiilor furnizate.

(2) Cu exceptia informatiilor necesare înstiintarii de la art. 29 alin. (1), informatiile prelucrate în sensul îndeplinirii obligatiilor de la alin. (1) nu fac parte din categoria informatiilor de interes public asa cum acestea sunt reglementate în Legea nr. 544/2001 privind liberul acces la informatiile de interes public, cu modificarile si completarile ulterioare.

(3) Informatiile confidentiale conform legislatiei nationale si normelor Uniunii Europene, precum cele privind secretul comercial, fac obiectul schimbului de informatii cu Comisia Europeana si cu alte autoritati numai daca acest lucru este necesar pentru aplicarea prezentei legi.

(4) Informatiile care fac obiectul schimbului mentionat la alin. (3) se limiteaza la informatii relevante si proportionale cu scopul urmarit.

(5) Schimbul de informatii mentionat la alin. (3) se va face cu garantarea pastrarii confidentialitatii informatiilor si protejarea securitatii si intereselor comerciale ale operatorilor de servicii esentiale si ale furnizorilor de servicii digitale.

(6) Prelucrarile de date cu caracter personal ce intra sub incidenta prezentei legi se efectueaza cu respectarea reglementarilor legale privind protectia persoanelor fizice în ceea ce priveste prelucrarea datelor cu caracter personal.

(7) Notificarile realizate în temeiul prezentei legi nu afecteaza obligatiile operatorilor de date cu caracter personal stabilite potrivit art. 33 si 34 din Regulamentul (UE) 2016/679 al Parlamentului European si al Consiliului din 27 aprilie 2016 privind protectia persoanelor fizice în ceea ce priveste prelucrarea datelor cu caracter personal si privind libera circulatie a acestor date si de abrogare a Directivei 95/46/CE.

(8) În scopul îndeplinirii atributiilor ori furnizarii serviciilor prevazute de prezenta lege, precum si în scopul prevenirii si raspunsului la incidentele de securitate informatica ori al cooperarii la nivel national, comunitar si international în prevenirea si raspunsul la incidentele de securitate informatica, CERT-RO colecteaza, primeste, prelucreaza si transmite date si informatii ce pot constitui sau pot

contine date cu caracter personal, în limitele legislatiei aplicabile, cu asigurarea respectarii prevederilor alin. (6).

CAPITOLUL V
Audit si autorizare

SECTIUNEA 1
Auditul de securitate a retelelor si sistemelor informatice apartinând operatorilor de servicii esentiale sau furnizorilor de servicii digitale

Art. 31. – Poate fi auditor de securitate a retelelor si sistemelor informatice persoana fizica sau persoana juridica ce realizeaza audit de securitate a retelelor si sistemelor
informatice, adica desfasoara acea activitate prin care se realizeaza o evaluare sistematica a tuturor politicilor, procedurilor si masurilor de protectie implementate la nivelul retelelor si sistemelor informatice, în vederea identificarii disfunctiilor si vulnerabilitatilor si a furnizarii unor solutii de remediere a acestora.

Art. 32. – (1) Auditul de securitate specificat la art. 8 alin. (4), respectiv art. 10 alin. (2)lit. b) si art. 12 alin. (2)lit. b) se realizeaza de catre auditorii de securitate informatica ce detin atestat valabil eliberat de catre CERT-RO pentru a audita retele si sisteme informatice ce deservesc servicii esentiale sau servicii digitale în sensul prezentei legi.

(2) În acest sens CERT-RO:

a)întretine si actualizeaza Registrul auditorilor mentionati la alin. (1);

b)elaboreaza si transmite spre aprobare MCSI, în conformitate cu prevederile art. 20 lit. e) si s), regulamentul pentru atestarea si verificarea auditorilor de securitate informatica pentru retelele si sistemele informatice apartinând operatorilor de servicii esentiale sau furnizorilor de servicii digitale si stabileste conditiile de valabilitate pentru atestatele acordate;

c)acorda, prelungeste, suspenda sau retrage atestarea pentru auditorii de securitate informatica pentru retelele si sistemele informatice apartinând operatorilor de servicii esentiale sau furnizorilor de servicii digitale, în conformitate cu prevederile regulamentului prevazut la lit. b);

d)verifica în urma sesizarilor sau din oficiu, în conformitate cu prevederile art. 35-42, îndeplinirea de catre auditorii atestati în temeiul prezentei legi a obligatiilor legale ce le revin;

e)elaboreaza si aproba, prin decizie a directorului general publicata în Monitorul Oficial al României, Partea I, tematicile pentru specializarea auditorilor în vederea atestarii prevazute la lit. c) si autorizeaza, verifica, suspenda sau retrage autorizarea formatorilor din domeniul auditului de securitate informatica pentru retelele si sistemele informatice ale operatorilor de servicii esentiale si furnizorilor de servicii digitale.

(3) Nu pot realiza auditul solicitat la art. 10 alin. (2) lit. b), respectiv art. 12 alin. (2)lit. b):

a)auditorii atestati care asigura în mod curent servicii de securitate informatica ori servicii de tip CSRIT operatorului de servicii esentiale sau furnizorului de servicii digitale ori sunt angajati ai acestora;

b)auditorul care are un contract de prestari servicii pentru reteaua si sistemul supus auditului aflat în desfasurare la momentul la care se efectueaza auditul sau într-un termen mai mic de un an;

c)auditorul care a mai efectuat 3 audituri consecutive la acelasi operator de servicii esentiale sau furnizor de servicii digitale.

(4) Activitatea de audit se efectueaza potrivit standardelor si specificatiilor europene si internationale aplicabile în domeniu.

(5) Tematicile de audit vor tine seama de normele tehnice în vigoare privind securitatea retelelor si sistemelor informatice ale operatorilor de servicii esentiale si ale furnizorilor de servicii digitale elaborate în temeiul prezentei legi.

(6) Atestatele au o valabilitate de 3 ani.

(7) Constituie exceptie de la prevederile alin. (1) auditul de securitate realizat la nivelul institutiilor cu responsabilitati în domeniul apararii, ordinii publice si securitatii nationale, precum si pentru serviciile puse la dispozitie de catre acestea.

(8) Lista standardelor si specificatiilor europene si internationale prevazute la alin. (4) se elaboreaza si se aproba prin decizie a directorului general al CERT-RO, se actualizeaza periodic si se publica în Monitorul Oficial al României, Partea I.

SECTIUNEA a 2-a

Autorizarea echipelor CSIRT ce deservesc retele si sisteme informatice din categoria serviciilor esentiale si serviciilor digitale

Art. 33. - (1) Echipele CSIRT care deservesc operatori de servicii esentiale ori furnizori de servicii digitale se autorizeaza de catre CERT-RO în calitate de autoritate competenta la nivel national.

(2) În acest sens CERT-RO:

a)întretine si actualizeaza Registrul echipelor CSIRT prevazute la alin. (1);

b)elaboreaza si transmite spre aprobare MCSI, în conformitate cu prevederile art. 20 lit. e) si s), regulamentul pentru autorizarea si verificarea echipelor CSIRT care deservesc operatorii de servicii esentiale sau furnizorii de servicii digitale si stabileste conditiile de valabilitate pentru autorizatiile acordate;

c)acorda, prelungeste, suspenda sau retrage autorizarea pentru echipele CSIRT, în conformitate cu prevederile regulamentului prevazut la lit. b);

d)verifica în urma sesizarilor sau din oficiu, în conformitate cu prevederile art. 35-42, îndeplinirea de catre echipele CSIRT autorizate în temeiul prezentei legi a obligatiilor legale ce le revin;

e)elaboreaza tematicile pentru formarea membrilor echipelor CSIRT în vederea autorizarii prevazute la lit. c) si autorizeaza, verifica, suspenda sau retrage autorizarea formatorilor din domeniul asigurarii de servicii de tip CSIRT pentru retelele si sistemele informatice ale operatorilor de servicii esentiale si furnizorilor de servicii digitale.

(3) În vederea autorizarii, echipa CSIRT trebuie sa îndeplineasca conditiile prevazute în normele tehnice elaborate în temeiul prevederilor art. 20 lit. e).

(4) Autorizatiile au o valabilitate de 3 ani.

CAPITOLUL VI
Cooperare

Art. 34. – (1) Autoritatile si entitatile care reglementeaza sectoarele si subsectoarele de activitate prevazute în anexa au obligatia de a coopera si sprijini CERT-RO în calitate de autoritate competenta la nivel national si de a raspunde solicitarilor acesteia, potrivit domeniilor de activitate si responsabilitate, pentru:

a) identificarea serviciilor esentiale din sectoarele de activitate reglementate de acestea;

b) identificarea operatorilor de servicii esentiale în sensul prezentei legi si actualizarea listei acestora;

c) identificarea cerintelor de securitate si notificare existente în cadrul sectorului sau subsectorului respectiv, în vederea determinarii nivelului de securitate asigurat de acestea;

d) stabilirea cerintelor specifice de asigurare a securitatii retelelor si sistemelor informatice si de notificare a incidentelor survenite pentru sectoarele si subsectoarele prevazute în anexa;

e) armonizarea cerintelor specifice prevazute la punctele anterioare cu cerintele de securitate si notificare prevazute de prezenta lege;

f) luarea masurilor cu caracter exceptional prevazute la art. 41;

g) stabilirea criteriilor si valorilor de prag specifice, necesare pentru determinarea impactului unui incident la nivelul sectorului sau subsectorului respectiv;

h) armonizarea reglementarilor emise de acestea la nivel de sector cu cerintele prezentei legi.

(2) Cerintele specifice de securitate impuse operatorilor de servicii esentiale sau furnizorilor de servicii digitale prin acte juridice ale Uniunii Europene de directa aplicare sau prin acte juridice ale Uniunii Europene transpuse la nivel national care reglementeaza respectivul sector de activitate se aplica doar în masura în care nivelul de securitate asigurat este cel putin echivalent cu obligatiile prevazute în prezenta lege.

(3) Aplicarea actelor juridice ale Uniunii Europene prevazute la alin. (2) nu deroga de la celelalte obligatii care revin operatorilor de servicii esentiale si furnizorilor de servicii digitale conform prezentei legi.

CAPITOLUL VII
Supraveghere, control, sanctionare

SECTIUNEA 1
Activitatea de control

Art. 35. – (1) CERT-RO exercita controlul respectarii prevederilor prezentei legi, a obligatiilor impuse prin actele emise de CERT-RO în aplicarea prezentei legi, în limitele competentelor legale de monitorizare sau de verificare.

(2) În vederea efectuarii controlului prevazut la alin. (1), directorul general al CERT-RO, prin decizie, desemneaza personalul de specialitate împuternicit sa efectueze controlul si stabileste atributiile acestuia.

(3) Normele de aplicare a dispozitiilor privind controlul îndeplinirii obligatiilor de securitate si notificare de catre operatorii de servicii

esentiale si furnizorii de servicii digitale si controlul îndeplinirii obligatiilor de catre auditorii de securitate informatica atestati ori de catre echipele CSIRT autorizate sa deserveasca operatori de servicii esentiale si furnizori de servicii digitale se aproba, la propunerea CERT-RO, prin ordin al ministrului comunicatiilor si societatii informationale care se publica în Monitorul Oficial al României, Partea I.

Art. 36. – (1) În urma sesizarilor primite, din oficiu sau în urma autosesizarii în temeiul art. 27 lit. e), precum si în situatia existentei unor indicii temeinice privind sustragerea unui operator sau furnizor de la obligatiile ce îi revin în temeiul prezentei legi ori încalcarea de catre un auditor, echipa CSIRT sau furnizor de formare autorizat a obligatiilor ce le revin în temeiul prezentei legi, personalul de control poate sa efectueze actiuni de control, în cadrul carora poate sa solicite, mentionând temeiul legal si scopul solicitarii, documentele necesare pentru efectuarea controlului, sa ridice copii de pe registre ori alte acte sau documente, în conditiile legii, inclusiv prevederilor referitoare la pastrarea confidentialitatii tuturor documentelor si informatiilor primite.

(2) În cadrul actiunilor de control, personalul de control poate sa solicite si sa primeasca, la fata locului sau la termenul solicitat, informatiile necesare pentru efectuarea controlului si poate stabili termene pâna la care aceste informatii sa îi fie furnizate, în conditiile legii, inclusiv prevederilor referitoare la pastrarea confidentialitatii tuturor documentelor si informatiilor primite.

(3) Rezultatul actiunilor de control va fi consemnat într-o nota de control.

Art. 37. – (1) Înainte de aplicarea unei sanctiuni, în cazul descoperirii nerespectarii de catre un furnizor de servicii digitale sau operator de servicii esentiale a unei obligatii prevazute de prezenta lege sau de un act emis de CERT-RO în baza prezentei legi, CERT-RO va transmite entitatii în cauza o notificare prin care îi va aduce la cunostinta încalcarea constatata, masurile cu caracter obligatoriu ce trebuie luate în vederea remedierii deficientelor constatate si stabileste termenul de conformare precum si sanctiunea aplicabila.

(2) Termenul de conformare se calculeaza începând cu data comunicarii notificarii prevazute la alin. (1).

Art. 38. – Urmatoarele fapte constituie contraventii daca nu au fost savârsite în astfel de conditii încât sa fie considerate potrivit legii infractiuni:

1. neîndeplinirea obligatiei de notificare în vederea înscrierii în Registrul operatorilor de servicii esentiale, prevazuta la art. 8 alin. (1), în termenul prevazut la art. 8 alin. (6);
2. neîndeplinirea în termenul prevazut a obligatiei de furnizare a informatiilor solicitate de catre CERT-RO în temeiul art. 8 alin. (7) lit. a);
3. neîndeplinirea în termenul prevazut a obligatiei de furnizare a informatiilor solicitate de catre CERT-RO în temeiul art. 8 alin. (7)lit. b);
4. neîndeplinirea în termenul prevazut a obligatiei de furnizare a informatiilor solicitate de catre CERT-RO în temeiul art. 8 alin. (7)lit. c);
5. neîndeplinirea în termenul prevazut a obligatiei de furnizare a informatiilor solicitate de catre CERT-RO în temeiul art. 8 alin. (7)lit. d);
6. nedepunerea raportului de audit specificat la art. 8 alin. (4)si (7) în termenul comunicat de catre CERT-RO persoanei juridice în temeiul art. 8 alin. (8);
7. neîndeplinirea obligatiei prevazute la art. 9 alin. (1)în termenul prevazut la art. 9 alin. (5);
8. neducerea la îndeplinire a masurilor dispuse de CERT-RO prin notificarea transmisa în urma controlului, pentru remedierea deficientelor constatate, în termenul de conformare stabilit în conformitate cu

prevederile art. 37;

9. neîndeplinirea de catre operatorii de servicii esentiale a obligatiei de implementare a masurilor pentru îndeplinirea cerintelor minime de securitate în conformitate cu art. 10 alin. (1) lit. a) în termenul stabilit la art. 10 alin. (4);

10. neîndeplinirea de catre operatorii de servicii esentiale a obligatiei de implementare a masurilor adecvate pentru a preveni si minimiza impactul incidentelor în conformitate cu art. 10 alin. (1) lit. b) în termenul stabilit la art. 10 alin. (4);

11. încalcarea de catre operatorii de servicii esentiale a obligatiei stabilite la art. 10 alin. (1)lit. c) de a notifica incidentul de securitate ori notificarea acestuia cu o întârziere mai mare de 12 ore de la data constatarii acestuia;

12. încalcarea obligatiei stabilite la art. 10 alin. (1)lit. d) prin nefurnizarea în cadrul notificarii privitoare la incidentul de securitate a informatiilor care sa permita
stabilirea impactului transfrontalier al acestuia;

13. nerespectarea prevederilor art. 10 alin. (1)lit. e) în termen de 48 de ore de la data comunicarii de catre CERT-RO a ordinului de începere a controlului;

14. necomunicarea catre CERT-RO a informatiilor si mijloacelor permanente de contact ori a actualizarilor acestora în termenele stabilite la art. 10 alin. (1)lit. f);

15. neîndeplinirea obligatiei de comunicare prevazute la art. 10 alin. (1) lit. g) în termen de 30 de zile;

16. neîndeplinirea obligatiei de interconectare prevazute la art. 10 alin. (1) lit. h) în termen de 60 de zile;

17. neluarea de catre operatorul de servicii esentiale a masurilor adecvate de raspuns în termen de 12 ore de la primirea prin serviciul de alertare si cooperare al CERT-RO mentionat la art. 10 alin. (1)lit. h) ori prin celelalte mijloace de contact a alertelor si solicitarilor privitoare la incidente;

18. neîndeplinirea de îndata a obligatiei de a asigura raspunsul la incidentele survenite stabilite la art. 10 alin. (1)lit. i) ori îndeplinirea acesteia cu o întârziere mai mare de 12 ore de la data constatarii incidentului;

19. neîndeplinirea obligatiei stabilite la art. 10 alin. (1) lit. i) de a restabili functionarea serviciului esential afectat de incident la parametrii dinaintea incidentului ori întârzierea nejustificata a restabilirii functionarii acestuia;

20. neîndeplinirea în urma raspunsului la incident a obligatiei stabilite la art. 10 alin. (1) lit. i) de a efectua auditul de securitate a retelelor si sistemelor informatice afectate;

21. nefurnizarea în termenul stabilit de CERT-RO a informatiilor si documentatiilor solicitate în temeiul art. 10 alin. (2)lit. a);

22. neefectuarea auditului de securitate si netransmiterea rezultatelor acestuia si a datelor necesare în termenul stabilit de CERT-RO în urma solicitarii facute în temeiul prevederilor art. 10 alin. (2)lit. b);

23. încalcarea cumulativa a obligatiilor prevazute la art. 10 alin. (3)si art. 26 alin. (1)-(3) într-un termen de 12 ore de la
data constatarii incidentului de catre operatorul de servicii esentiale.

24. neîndeplinirea de catre operatorii de servicii esentiale a obligatiei prevazute la art. 11 în termenele stabilite de CERT-RO prin actul de control comunicat operatorului de servicii esentiale;

25. neducerea la îndeplinire de catre furnizorul de servicii digitale a masurilor dispuse de CERT-RO prin notificarea transmisa în urma controlului, pentru remedierea deficientelor constatate în aplicarea prevederilor art. 12 alin. (1)lit. a) si b) în termenul de conformare stabilit în conformitate cu prevederile art. 37;

26. neîndeplinirea de catre furnizorii de servicii digitale, în termenul stabilit, a obligatiei de implementare a masurilor pentru respectarea

cerintelor minime de securitate în conformitate cu prevederile art. 12 alin. (1)lit. a);

27. neîndeplinirea de catre furnizorii de servicii digitale a obligatiei de implementare, în termenul stabilit, a masurilor adecvate pentru a preveni si minimiza impactul incidentelor în conformitate cu prevederile art. 12 alin. (1)lit. b);

28. încalcarea de catre furnizorii de servicii digitale a obligatiei stabilite la art. 12 alin. (1)lit. c) de a notifica incidentul de securitate ori notificarea acestuia cu o întârziere mai mare de 12 ore de la data constatarii acestuia;

29. încalcarea obligatiei stabilite la art. 12 alin. (1)lit. d) prin nefurnizarea în cadrul notificarii privitoare la incidentul de securitate a informatiilor care sa permita stabilirea impactului transfrontalier al acestuia;

30. necomunicarea catre CERT-RO a informatiilor si mijloacelor permanente de contact în termenul stabilit la art. 12 alin. (1)lit. e);

31. neîndeplinirea obligatiei de comunicare a modificarilor survenite în datele de contact prevazute la art. 12 alin. (1)lit. e) în termen de 30 de zile;

32. neîndeplinirea obligatiei de interconectare prevazute la art. 12 alin. (1)lit. f) în termen de 60 de zile;

33. neluarea de catre furnizorul de servicii digitale a masurilor adecvate de raspuns în termen de 12 ore de la primirea prin serviciul de alertare si cooperare al CERT-RO mentionat la art. 12 alin. (1)lit. f) ori prin celelalte mijloace de contact a alertelor si solicitarilor privitoare la incidente;

34. neîndeplinirea obligatiei de a asigura raspunsul la incidentele de securitate si de a asigura continuitatea serviciilor stabilite la art. 12 alin. (1)lit. b) ori îndeplinirea acesteia cu o întârziere mai mare de 12 ore de la data constatarii incidentului;

35. nefurnizarea în termenul stabilit de CERT-RO a informatiilor si documentatiilor solicitate în temeiul art. 12 alin. (2)lit. a);

36. neefectuarea auditului de securitate si netransmiterea rezultatelor acestuia si a datelor necesare în termenul stabilit de CERT-RO în urma solicitarii facute în temeiul art. 12 alin. (2)lit. b);

37. neîndeplinirea în termenul prevazut a obligatiei de furnizare a informatiilor solicitate de catre CERT-RO în temeiul art. 12 alin. (6)lit. a);

38. neîndeplinirea în termenul prevazut a obligatiei de furnizare a informatiilor solicitate de catre CERT-RO în temeiul art. 12 alin. (6)lit. b);

39. neîndeplinirea în termenul prevazut a obligatiei de furnizare a informatiilor solicitate de catre CERT-RO în temeiul art. 12 alin. (6)lit. c);

40. neducerea la îndeplinire a masurilor instituite de CERT-RO în temeiul art. 20 lit. k), în termen de 60 de zile de la data comunicarii;

41. neconformarea cu normele tehnice prevazute la art. 25 alin. (1);

42. neconformarea operatorilor de servicii esentiale cu normele tehnice privitoare la notificarea incidentelor de securitate prevazute la art. 26 alin. (1);

43. neconformarea furnizorilor de servicii digitale cu normele tehnice privitoare la notificarea incidentelor de securitate prevazute la art. 26 alin. (2);

44. nefurnizarea de catre operatorul de servicii esentiale ori furnizorul de servicii digitale în termenul stabilit de CERT-RO a informatiilor suplimentare solicitate de CERT-RO în temeiul art. 27 lit. b);

45. încalcarea de catre auditorii specificati la art. 32 alin. (1)a normelor privind incompatibilitatea, prevazute la art. 32 alin. (3);

46. furnizarea de rapoarte de audit de securitate dintre cele prevazute la art. 8 alin. (4), respectiv art. 10 alin. (2)lit. b) si art. 12 alin.

(2)lit. b), realizate de catre auditori fara atestat valabil eliberat de CERT-RO în temeiul art. 32 alin. (1) si (2) lit. c) ori aflati într-una din starile de incompatibilitate prevazute la art. 32 alin. (3);

47. asigurarea de servicii de tip echipa CSIRT catre operatorii de servicii esentiale ori furnizorii de servicii digitale de catre entitati care nu detin autorizatie valabila, eliberata în temeiul art. 33 alin. (1)de catre CERT-RO în calitate de autoritate competenta la nivel national;

48. neîndeplinirea de catre autoritatile si entitatile de reglementare pentru sectoarele si subsectoarele de activitate prevazute în anexa a obligatiilor prevazute la art. 34 alin. (1), precum si neparticiparea în procesul de stabilire a nivelului de securitate mentionat la art. 34 alin. (2);

49. refuzul de a se supune controlului declansat de CERT-RO în temeiul prevederilor art. 36 ori întârzierea în furnizarea informatiilor si documentelor solicitate în cadrul activitatilor de control în temeiul prevederilor art. 37.

Art. 39. - (1) Contraventiile prevazute la art. 38 se sanctioneaza astfel:

a)cu amenda de la 3.000 lei la 50.000 lei, iar în cazul constatarii unor încalcari repetate limita maxima a amenzii este de 100.000 lei;

b)prin derogare de la dispozitiile art. 8 alin. (2) lit. a) din Ordonanta Guvernului nr. 2/2001 privind regimul juridic al contraventiilor, aprobata cu modificari si completari prin Legea nr. 180/2002, cu modificarile si completarile ulterioare, pentru persoanele cu o cifra de afaceri de peste 2.000.000 lei, cu amenda în cuantum de la 0,5% la 2% din cifra de afaceri, iar, în cazul unor încalcari repetate, limita maxima a amenzii este de 5% din cifra de afaceri.

(2) În vederea individualizarii sanctiunii, CERT-RO va lua în considerare gradul de pericol social concret al faptei, perioada de timp în care obligatia legala a fost încalcata, precum si, daca este cazul, consecintele încalcarii.

(3) Cifra de afaceri este cea prevazuta în ultima situatie financiara anuala raportata de operatorul economic.

(4) Pentru persoanele fizice autorizate, întreprinderile individuale si întreprinderile familiale, cifrei de afaceri prevazute la alin. (1) lit. b) îi corespunde totalitatea veniturilor brute, astfel cum sunt definite de Legea nr. 227/2015 privind Codul fiscal, cu modificarile si completarile ulterioare, realizate de respectivele entitati.

(5) Prin exceptie de la prevederile alin. (3) si (4), în cazul în care, în anul financiar anterior sanctionarii, întreprinderea nu a înregistrat cifra de afaceri sau cifra de afaceri nu poate fi determinata, va fi luata în considerare cea aferenta anului financiar în care entitatea a înregistrat cifra de afaceri, an imediat anterior anului de referinta pentru calcularea cifrei de afaceri în vederea aplicarii sanctiunii. În ipoteza în care nici în anul anterior anului de referinta pentru calcularea cifrei de afaceri în vederea aplicarii sanctiunii entitatea nu a realizat cifra de afaceri, va fi luata în calcul ultima cifra de afaceri înregistrata de entitate.

(6) Pentru entitatile nou-înfiintate si care nu au înregistrat cifra de afaceri în anul anterior sanctionarii, amenda prevazuta la alin. (1) se stabileste în cuantum de minimum unu si maximum 25 de salarii minime brute pe economie.

(7) În masura în care prezenta lege nu prevede altfel, contraventiilor prevazute la art. 38 li se aplica dispozitiile Ordonantei Guvernului nr. 2/2001, aprobata cu modificari si completari prin Legea nr. 180/2002, cu modificarile si completarile ulterioare.

Art. 40. - (1) Contraventiile prevazute la art. 38 se constata de catre personalul de control din cadrul CERT-RO prin procesul-verbal de constatare a contraventiei si de aplicare a sanctiunii, semnat de catre personalul care efectueaza controlul si de catre reprezentantul operatorului sau furnizorului prezent la momentul încheierii procesului-verbal, caruia i se

va înmâna o copie a procesului-verbal.

(2) Sanctiunea pentru contraventiile prevazute la alin. (1) se aplica de catre personalul de control care a facut constatarea.

Art. 41. – (1) În cazul constatarii unei contraventii în conformitate cu prevederile art. 38, CERT-RO dispune încetarea încalcarii dispozitiilor respective fie imediat, fie într-un termen rezonabil, precum si orice masuri necesare pentru a asigura încetarea încalcarii si remedierea situatiei produse. Masurile vor fi adecvate si proportionale cu încalcarea savârsita si vor prevedea un termen în care operatorul de servicii esentiale ori furnizorul de servicii digitale trebuie sa se conformeze acestora.

(2) În cazul în care nerespectarea de catre operatori sau furnizori a obligatiilor din prezenta lege poate crea probleme grave de natura economica sau operationala altor operatori sau furnizori, CERT-RO poate lua masuri urgente cu caracter provizoriu pentru remedierea situatiei.

(3) În cazul în care nerespectarea de catre operatori sau furnizori a obligatiilor prevazute de prezenta lege prezinta un pericol grav si iminent la adresa apararii nationale, ordinii publice, securitatii nationale sau sanatatii publice, CERT-RO va informa organele judiciare si va notifica institutiile competente din domeniul apararii si securitatii nationale, ordinii publice sau sanatatii publice.

(4) Atunci când apreciaza ca este necesar, CERT-RO poate mentine masurile dispuse conform prevederilor alin. (2) pentru o perioada de cel mult 90 de zile. În cazul în care punerea în executare a acestora necesita o durata mai mare de timp, CERT-RO poate dispune prelungirea aplicabilitatii pentru o perioada suplimentara de cel mult 90 de zile. Operatorului sau furnizorului în cauza i se va acorda posibilitatea de a-si prezenta punctul de vedere si de a propune solutii pentru remedierea definitiva a situatiei create.

(5) Masurile prevazute la alin. (2) se dispun prin decizie a directorului general al CERT-RO, ce poate fi atacata cu plângere în termen de 30 zile de la comunicare.

(6) Masurile prevazute la alin. (2) se pot dispune de catre CERT-RO cu titlu exceptional si în situatia administrarii unor incidente de natura sa prezinte pericolele ori sa aiba urmarile prevazute la alin. (3), cu consultarea, precum si la solicitarea motivata a institutiilor prevazute la alineatul respectiv.

Art. 42. – (1) În exercitarea atributiilor ce îi revin potrivit actelor normative în vigoare, CERT-RO va fi sprijinita operativ, la cerere, de catre autoritatile publice, precum si de catre organele de politie în cazuri temeinic justificate, în vederea identificarii si localizarii persoanelor fizice sau juridice care savârsesc fapte de natura contraventionala.

(2) Orice decizie a CERT-RO prin care se vatama drepturile unei persoane fizice sau juridice ori refuzul nejustificat al CERT-RO de a-i procesa cererea referitoare la un drept recunoscut de prezenta lege pot fi atacate în contencios administrativ.

CAPITOLUL VIII
Dispozitii tranzitorii

Art. 43. – Înscrierea în registrul prevazut la art. 8, în primii 2 ani de la data intrarii în vigoare a prezentei legi, se face prin depunerea unei declaratii pe propria raspundere însotite de o documentatie de autoevaluare a îndeplinirii cerintelor minime de securitate si notificare.

CAPITOLUL IX
Dispozitii finale

Art. 44. – Până la 9 august 2018 si, ulterior, în fiecare an, CERT-RO, în calitate de punct unic de contact, transmite Grupului de cooperare un raport de sinteza privind notificarile primite, care include numarul de notificari si natura incidentelor notificate, precum si actiunile întreprinse în conformitate cu prevederile art. 10 alin. (1)lit. c) si art. 12 alin. (1)lit. c) coroborate cu art. 27 lit. d).

Art. 45. – (1) Strategia nationala prevazuta la art. 14 va acoperi cel putin urmatoarele elemente:

a)obiectivele si prioritatile strategiei nationale privind securitatea retelelor si a sistemelor informatice;

b)un cadru de guvernanta pentru realizarea obiectivelor si a prioritatilor strategiei nationale privind securitatea retelelor si a sistemelor informatice, care sa includa rolurile si responsabilitatile organismelor guvernamentale si ale altor actori relevanti;

c)identificarea masurilor referitoare la gradul de pregatire, raspuns si redresare, inclusiv cooperarea dintre sectorul public si cel privat;

d)indicarea programelor de instruire, sensibilizare si formare legate de strategia nationala privind securitatea retelelor si a sistemelor informatice;

e)indicarea planurilor de cercetare si dezvoltare legate de strategia nationala privind securitatea retelelor si a sistemelor informatice;

f)un plan de evaluare a riscurilor pentru identificarea riscurilor;

g)o lista a diferitilor actori implicati în punerea în aplicare a strategiei nationale privind securitatea retelelor si a sistemelor informatice.

(2) În elaborarea strategiei, MCSI poate solicita asistenta ENISA.

(3) În termen de 3 luni de la data intrarii în vigoare a prezentei legi, MCSI transmite Comisiei Europene strategia adoptata în temeiul art. 14.

(4) Comunicarea de la alin. (3) nu va contine elementele care au legatura cu securitatea nationala.

Art. 46. – CERT-RO identifica si stabileste documentele si detaliile tehnice necesare pentru evaluarea initiala a securitatii entitatilor care urmeaza sa se declare operatorii de servicii esentiale.

Art. 47. – Cerintele de securitate si notificare prevazute la cap. IV nu se aplica:

a)furnizorilor de retele publice de comunicatii electronice si furnizorilor de servicii de comunicatii electronice destinate publicului;

b)prestatorilor de servicii de încredere calificati si necalificati care fac obiectul art. 19 din Regulamentul (UE) nr. 910/2014 al Parlamentului European si al Consiliului din 23 iulie 2014 privind identificarea electronica si serviciile de încredere pentru tranzactiile electronice pe piata interna si de abrogare a Directivei 1999/93/CE.

Art. 48. – (1) Până la 9 noiembrie 2018, pentru fiecare sector si subsector mentionat în anexa, pe lânga primirea de notificari în vederea înscrierii în Registrul operatorilor de servicii esentiale conform art. 8 alin. (1), CERT-RO identifica operatorii de servicii esentiale care au sediul social, filiala, sucursala, punct de lucru sau alta forma de reprezentare legal stabilita pe teritoriul României.

(2) În termen de 30 de zile de la data intrarii în vigoare a prezentei legi, MCSI notifica Comisiei Europene regimul sanctionator aplicabil în temeiul prezentei legi, precum si orice modificare ulterioara a acestuia.

(3) În termenul prevazut la alin. (1) si ulterior la fiecare doi ani,

CERT-RO transmite Comisiei Europene urmatoarele informatii în vederea evaluarii aplicarii prezentei legi:

a) lista masurilor care permit identificarea operatorilor de servicii esentiale;

b) lista serviciilor prevazute la art. 6 alin. (1) lit. a);

c) numarul operatorilor de servicii esentiale identificati pentru fiecare sector mentionat în anexa si o indicatie a importantei lor în legatura cu sectorul respectiv;

d) limite, atunci când acestea exista, pentru determinarea nivelului relevant de furnizare, în raport cu numarul de utilizatori care se bazeaza pe serviciul respectiv sau cu importanta operatorului de servicii esentiale.

Art. 49. - (1) MCSI va notifica Comisia Europeana în termen de 30 de zile de la publicarea în Monitorul Oficial al României, Partea I, a prezentei legi cu privire la desemnarea autoritatii competente, a punctului unic de contact si atributiilor acestora.

(2) MCSI va notifica Comisia Europeana în termen de 30 de zile de la publicarea în Monitorul Oficial al României, Partea I, orice modificare a actelor normative în baza carora a fost facuta desemnarea de la alin. (1).

(3) MCSI va notifica Comisia Europeana în termen de 30 de zile de la publicarea în Monitorul Oficial al României, Partea I, a prezentei legi cu privire la misiunea, precum si la principalele elemente ale procedurilor de administrare a incidentelor folosite de echipa CSIRT nationala.

Art. 50. - CERT-RO îsi desfasoara activitatea în baza prevederilor prezentei legi si a Hotarârii Guvernului nr. 494/2011 privind înfiintarea Centrului National de Raspuns la Incidente de Securitate Cibernetica - CERT-RO, care va fi modificata si completata corespunzator prevederilor prezentei legi.

*

Prezenta lege transpune în totalitate Directiva (UE) 2016/1.148 a Parlamentului European si a Consiliului din 6 iulie 2016 privind masuri pentru un nivel comun ridicat de securitate a retelelor si a sistemelor informatice în Uniune, publicata în Jurnalul Oficial al Uniunii Europene, seria L, nr. 194 din 19 iulie 2016.

Aceasta lege a fost adoptata de Parlamentul României, în conditiile art. 147 alin. (2), cu respectarea prevederilor art. 75 si ale art. 76 alin. (2) din Constitutia României, republicata.

p. PRESEDINTELE CAMEREI DEPUTATILOR,
FLORIN IORDACHE
PRESEDINTELE SENATULUI
CALIN-CONSTANTIN-ANTON POPESCU-TARICEANU

Bucuresti, 28 decembrie 2018.
Nr. 362.

ANEXA

Sectoare de activitate si tipuri de entitati

Sectorul	Subsectorul	Tipul de entitate
1. Energie	a) electricitate	- operatori economici din domeniul energiei electrice, astfel cum sunt definiti la art. 3 pct. 42 din Legea energiei electrice si a gazelor naturale nr. 123/2012 , cu modificarile si completarile ulterioare;
		- operatori de distributie, astfel cum sunt definiti la art. 3 pct. 39 din Legea nr. 123/2012 , cu modificarile si completarile ulterioare;
		- operatori de transport si de sistem, astfel cum sunt definiti la art. 3 pct. 40 din Legea nr. 123/2012 , cu modificarile si completarile ulterioare;
	b) petrol	- operatori de conducte de transport al petrolului;
		- operatori ai instalatiilor de productie, de rafinare si de tratare a petrolului, de depozitare si de transport;
	c) gaze naturale	- furnizori persoane fizice sau juridice, astfel cum sunt definiti la art. 100 pct. 44 din Legea nr. 123/2012 , cu modificarile si completarile ulterioare;
		- operatori de distributie, astfel cum sunt definiti la art. 100 pct. 63 din Legea nr. 123/2012 , cu modificarile si completarile ulterioare;
		- operatori de transport si de sistem, astfel cum sunt definiti la art. 100 pct. 65 din Legea nr. 123/2012 , cu modificarile si completarile ulterioare;
		- operatori de înmagazinare, astfel cum sunt definiti la art. 100 pct. 64 din Legea nr. 123/2012 , cu modificarile si completarile ulterioare;
		- operatori ai terminalelor GNL, astfel cum sunt definiti la art. 100 pct. 60 din Legea nr. 123/2012 , cu modificarile si completarile ulterioare;
		- operatori economici din sectorul gazelor naturale, astfel cum sunt definiti la art. 100 pct. 67 din Legea nr. 123/2012 , cu modificarile si completarile ulterioare;
		- operatori de instalatie de rafinare si de tratare a gazelor naturale
2. Transport	a) transport aerian	- transportatori aerieni, astfel cum sunt definiti la art. 3 pct. 4 din Regulamentul (CE) nr. 300/2008 al Parlamentului European si al Consiliului din 11 martie 2008 privind norme comune în domeniul securitatii aviatiei civile si de abrogare a Regulamentului (CE) nr. 2.320/2002;
		- organe de administrare a aeroportului, astfel cum sunt definite la art. 4 din Hotarârea Guvernului nr. 455/2011 privind tarifele de aeroport, inclusiv aeroporturile principale enumerate în sectiunea 2 din anexa II la Regulamentul (UE) nr. 1.315/2013 al Parlamentului European si al Consiliului din 11 decembrie 2013 privind orientarile Uniunii pentru dezvoltarea retelei transeuropene de transport si de abrogare a Deciziei nr. 661/2010/UE, precum si entitati care opereaza instalatii auxiliare în cadrul aeroporturilor;
		- operatori de control al gestionarii traficului care presteaza servicii de control al traficului aerian (ATC), astfel cum sunt definite la art. 2 pct. 1 din Regulamentul (CE) nr. 549/2004 al Parlamentului European si al Consiliului din 10 martie 2004 de stabilire a cadrului pentru crearea cerului unic European (regulament-cadru);
	b) transport feroviar	- administratori de infrastructuri, astfel cum sunt definiti la art. 3 pct. 3 din Legea nr. 202/2016 privind integrarea sistemului feroviar din România în spatiul feroviar unic european;
		- întreprinderi feroviare, astfel cum sunt definite la art. 3 pct. 3 din Legea nr. 202/2016 privind integrarea sistemului feroviar din România în spatiul feroviar unic european;
	c) transport pe apa	- companii de transport de marfuri si pasageri pe ape interioare, maritime si de coasta, astfel cum sunt definite pentru transportul maritim în anexa I la Regulamentul (CE) nr. 725/2004 al Parlamentului European si al Consiliului din 31 martie 2004 privind consolidarea securitatii navelor si a instalatiilor portuare, fara a include navele individuale operate de companiile respective;

		- organe de gestionare a porturilor, astfel cum sunt definite la art. 3 din Ordinul ministrului transporturilor nr. 290/2007 pentru introducerea masurilor de întarire a securitatii portuare, inclusiv instalatiile portuare ale acestora, astfel cum sunt definite la art. 2 pct. 11 din Regulamentul (CE) nr. 725/2004, si entitatile care opereaza lucrari si echipamente în cadrul porturilor;
		- operatori de servicii de trafic naval, astfel cum sunt definiti la art. 3 din Hotarârea Guvernului nr. 1.016/2010 pentru stabilirea Sistemului de informare si monitorizare a traficului navelor maritime care intra/ies în/din apele nationale navigabile ale României, cu modificarile si completarile ulterioare;
	d) transport rutier	- autoritati rutiere, astfel cum sunt definite la art. 2 pct. 12 din Regulamentul delegat (UE) 2015/962 al Comisiei din 18 decembrie 2014 de completare a Directivei 2010/40/UE a Parlamentului European si a Consiliului în ceea ce priveste prestarea la nivelul UE a unor servicii de informare în timp real cu privire la trafic, responsabile pentru controlul gestionarii traficului;
		- operatori de sisteme de transport inteligente, astfel cum sunt definiti la art. 4 din Ordonanta Guvernului nr. 7/2012 privind implementarea sistemelor de transport inteligente în domeniul transportului rutier si pentru realizarea interfetelor cu alte moduri de transport, aprobata prin Legea nr. 221/2012
3. Sectorul bancar		- institutii de credit, astfel cum sunt definite la art. 4 pct. 1 din Regulamentul (UE) nr. 575/2013 al Parlamentului European si al Consiliului din 26 iunie 2013 privind cerintele prudentiale pentru institutiile de credit si societatile de investitii si de modificare a Regulamentului (UE) nr. 648/2012
4. Infrastructuri ale pietei financiare		- operatori de locuri de tranzactionare, astfel cum sunt definite la art. 4 pct. 24 din Directiva 2014/65/UE a Parlamentului European si a Consiliului din 15 mai 2014 privind pietele instrumentelor financiare si de modificare a Directivei 2002/92/CE si a Directivei 2011/61/UE;
		- contrapartide centrale, astfel cum sunt definite la art. 2 pct. 1 din Regulamentul (UE) nr. 648/2012 al Parlamentului European si al Consiliului din 4 iulie 2012 privind instrumentele financiare derivate extrabursiere, contrapartile centrale si registrele centrale de tranzactii
5. Sectorul sanatatii	institutii de asistenta medicala (inclusiv spitale si clinici private)	- furnizori de servicii medicale, astfel cum sunt definiti în Hotarârea Guvernului nr. 304/2014 pentru aprobarea Normelor metodologice privind asistenta medicala transfrontaliera, cu modificarile ulterioare
Sectorul	Subsectorul	Tipul de entitate
6. Furnizarea si distribuirea de apa potabila		- furnizori si distribuitori de apa destinata consumului uman, astfel cum sunt definiti la art. 2 din Legea nr. 458/2002 privind calitatea apei potabile, republicata, cu modificarile si completarile ulterioare, excluzând distribuitorii pentru care distributia de apa destinata consumului uman reprezinta doar o parte din activitatea lor generala de distribuire a altor produse de baza si produse care nu sunt considerate servicii esentiale
7. Infrastructura digitala		- IXP;
		- DNS;
		- TLD