Lege privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice

CAPITOLUL I - DISPOZIȚII GENERALE

Secțiunea 1 – Obiect și scop

Art. 1. - Prezenta lege stabilește cadrul juridic și instituțional, măsurile și mecanismele necesare în vederea asigurării unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice și a stimulării cooperării în domeniu.

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

a) stabilirea cadrului de cooperare la nivel național și de participare la nivel european și internațional în domeniul asigurării securității rețelelor și sistemelor informatice;

b) desemnarea autorităților și entităților de drept public și privat care dețin competențe și responsabilități în aplicarea prevederilor prezentei legi, a punctului unic de contact la nivel național și a echipei naționale de răspuns la incidente de securitate informatică;

c) stabilirea cerințelor de securitate și notificare pentru operatorii de servicii esențiale și pentru furnizorii de servicii digitale și instituirea mecanismelor de actualizare a acestora în funcție de evoluția amenințărilor la adresa securității rețelelor și sistemelor informatice.

(2) Prezenta lege nu se aplică instituțiilor din domeniul apărării, ordinii publice și securității naționale precum și Oficiului Registrului Național al Informațiilor Secrete de Stat.

Secțiunea a 2 – a – Definiții și principii

Art. 3. - În sensul prezentei legi, termenii şi expresiile de mai jos au următoarea semnificație:

a) *administrarea incidentului* - toate procedurile utilizate pentru detectarea, analiza și limitarea unui incident și răspunsul la acesta;

b) *domain name system, denumit în continuare DNS* - sistem de atribuire de nume distribuite ierarhic într-o rețea în care se efectuează căutări de nume de domenii;

c) *furnizor de servicii digitale* - orice persoană juridică care furnizează un serviciu digital;

d) *furnizor de servicii DNS* - entitate care furnizează servicii DNS pe internet;

e) *incident* - orice eveniment care are un efect real negativ asupra securității rețelelor și a sistemelor informatice;

f) *internet exchange point, denumit în continuare IXP* - facilitate a rețelei care permite interconectarea a mai mult de două sisteme autonome independente, în special în scopul facilitării schimbului de trafic de internet; IXP furnizează interconectare doar pentru sisteme autonome; IXP nu necesită trecerea printr-un al treilea sistem autonom a traficului de internet dintre orice pereche de sisteme autonome participante și nici nu modifică sau interacționează într-un alt mod cu acest trafic;

g) *motor de căutare online* - un serviciu digital care permite utilizatorilor să caute, în principiu, în toate site-urile internet sau site-urile internet într-o anumită limbă pe baza unei interogări privind orice subiect sub forma unui cuvânt, a unei fraze sau a unei alte informații-cheie și care revine cu linkuri în care se pot găsi informații legate de conținutul căutat;

h) *operator de servicii esențiale* - entitate publică sau privată care îndeplinește condițiile prevăzute la art. 6 alin. (1);

i) *piață online* - serviciu digital care permite consumatorilor și/sau comercianților, astfel cum sunt definiți la art. 3 alin. (1) lit. a) și b) din Ordonanța Guvernului nr. 38/2015 privind soluționarea alternativă a litigiilor dintre consumatori și comercianți să încheie online vânzări sau contracte de servicii cu comercianți fie pe site-ul internet al pieței online, fie pe site-ul internet al unui comerciant care utilizează servicii informatice furnizate de piața online;

j) *registru de nume de domenii Top-level* - entitate care administrează și operează înregistrarea de nume de domenii de internet într-un domeniu Top-level (TLD) specific;

k) *reprezentant* - orice persoană fizică sau juridică stabilită în Uniunea Europeană desemnată explicit să acționeze în numele unui furnizor de servicii digitale nestabilit în Uniunea Europeană, căreia i se poate adresa autoritatea competentă națională sau echipa de intervenție în caz de incidente de securitate informatică denumită în continuare echipă CSIRT sau CSIRT, în locul furnizorului de servicii digitale în ceea ce privește obligațiile furnizorului de servicii digitale în temeiul prezentei legi;

l) *rețea și sistem informatic*:

1.rețea de comunicații electronice în sensul prevederilor art. 4 alin. (1) pct. 6 din Ordonanța de urgență a Guvernului nr. 111/2011 privind comunicaţiile electronice, cu modificările și completările ulterioare;

2. orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relație funcțională, dintre care unul sau mai multe asigură prelucrarea automată a datelor cu ajutorul unui program informatic;

3. datele digitale stocate, prelucrate, recuperate sau transmise de elementele prevăzute la punctele 1 și 2 în vederea funcționării, utilizării, protejării și întreținerii lor;

m) *risc* - orice circumstanță sau eveniment ce poate fi identificat în mod rezonabil, anterior producerii sale, care are un efect potențial negativ asupra securității rețelelor și a sistemelor informatice;

n) *securitatea rețelelor și a sistemelor informatice* - capacitatea unei rețele și a unui sistem informatic de a rezista, la un nivel de încredere dat, oricărei acțiuni care compromite disponibilitatea, autenticitatea, integritatea, confidențialitatea sau nonrepudierea datelor stocate ori transmise sau prelucrate ori a serviciilor conexe oferite de rețeaua sau de sistemele informatice respective sau accesibile prin intermediul acestora;

o) *serviciu digital* - serviciu, în sensul prevederilor art. 4 alin. (1) pct. 2 din Hotărârea Guvernului nr. 1016/2004 privind măsurile pentru organizarea şi realizarea schimbului de informaţii în domeniul standardelor şi reglementărilor tehnice, cu modificările și completările ulterioare, precum şi al regulilor referitoare la serviciile societăţii informaționale între România şi statele membre ale Uniunii Europene, precum și Comisia Europeană și care se încadrează într-una din categoriile:

1. Piață online;

2. Motor de căutare online;

3. Serviciu de cloud computing;

p) *specificație* - specificație tehnică, în sensul prevederilor art. 2 pct. 4 din Regulamentul (UE) nr. 1025/2012;

q) *standard* - standard, în sensul prevederilor art. 2 pct. 1 din Regulamentul (UE) nr. 1025/2012 Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului din 25 octombrie 2012 privind standardizarea europeană, de modificare a Directivelor 89/686/CEE și 93/15/CEE ale Consiliului și 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 și 2009/105/CE ale Parlamentului European și ale Consiliului și de abrogare a Deciziei 87/95/CEE a Consiliului și a Deciziei nr. 1673/2006/CE a Parlamentului European și a Consiliului;

r) *strategie națională privind securitatea rețelelor și a sistemelor informatice* - cadru care furnizează obiective și priorități strategice privind securitatea rețelelor și a sistemelor informatice la nivel național;

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;

ș) *valoare de prag* – valoare minimă/maximă, cuantificabilă a indicatorilor în baza cărora se determină gradul de îndeplinire a unui criteriu.

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

a) principiul responsabilității și conștientizării – constă în efortul continuu derulat de entitățile de drept public și privat în conștientizarea rolului și responsabilității individuale pentru atingerea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice

b) principiul proporționalității – constă în asigurarea unui echilibru între riscurile la care rețelele și sistemele informatice sunt supuse și cerințele de securitate implementate

c) principiul cooperării și coordonării – constă în realizarea în timp oportun a schimbului de informații referitoare la riscurile de securitate la adresa rețelelor și sistemelor informatice și asigurarea într-o maniera sincronizată a reacției la producerea incidentelor

CAPITOLUL II – DOMENIUL DE APLICARE

Secțiunea 1 – Operatorii de servicii esențiale

Art. 5. - În vederea asigurării unui nivel ridicat de securitate, entitățile publice sau private care dețin sau administrează rețele și sisteme informatice ce susțin sau furnizează servicii esențiale se identifică și se înscriu în Registrul operatorilor de servicii esențiale.

Art. 6. - (1) Un serviciu este considerat esențial dacă furnizarea lui îndeplinește cumulativ următoarele condiții:

a) serviciul susține activități societale sau economice de cea mai mare importanță;

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

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

(2) Evaluarea gradului de perturbare a furnizării serviciului esențial se realizează în funcție de următoarele criterii, fără a fi cumulative:

a) numărul de utilizatori care se bazează pe serviciul furnizat de entitatea în cauză;

b) dependența altor sectoare prevăzute în Anexă de serviciul furnizat de entitatea în cauză;

c) impactul pe care l-ar putea avea incidentele, în ceea ce privește intensitatea și durata, asupra activităților economice și societale sau asupra siguranței publice;

d) cota de piață a entității în cauză;

e) distribuția geografică în ceea ce privește zona care ar putea fi afectată de un incident;

f) importanța entității pentru menținerea unui nivel suficient al serviciului, ținând cont de disponibilitatea unor mijloace alternative pentru furnizarea serviciului respectiv.

(3) Centrul Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO în calitate de autoritate competentă la nivel național stabilește, după consultarea celorlalte instituții cu responsabilități în domeniul apărării, ordinii publice și securității naționale, actualizează și transmite MCSI Anexa cu valori de prag pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale, ce va include după caz și criteriile și valorile de prag specifice fiecărui sector și subsector de activitate prevăzut în Anexă, în vederea supunerii spre adoptare prin hotărâre a Guvernului.

Art. 7. - (1) Registrul prevăzut la art. 5 se alcătuiește pentru sectoarele și subsectoarele prevăzute în Anexă și raportat la criteriile menționate la art. 6 și valorile de prag menționate la art. 6 alin. (3).

(2) Registrul prevăzut la alin. (1) se întreține și se actualizează periodic, cel puțin o dată la doi ani începând cu data stipulată la art. 51, de către CERT-RO în calitate de autoritate competentă la nivel național.

Art. 8. - (1) Entitățile care îndeplinesc condițiile și criteriile prevăzute la art. 6 și activează într-unul sau mai multe dintre sectoarele sau subsectoarele de activitate prevăzute în Anexă, notifică CERT-RO în vederea înscrierii în Registrul operatorilor de servicii esențiale.

(2) Identificarea operatorilor de servicii esențiale se poate face voluntar în condițiile alin. (1) sau din oficiu de către CERT-RO în temeiul prezentei legi.

(3) Operatorii de servicii esențiale pot solicita asistența CERT-RO în procesul de identificare.

(4) Înscrierea operatorilor de servicii esențiale în Registrul operatorilor de servicii esențiale se realizează în urma depunerii unui raport de audit care atestă îndeplinirea cerințelor minime de securitate și notificare, întocmit de un auditor acreditat în conformitate cu prevederile art.32.

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

(6) Notificarea prevăzută la alin. (1) se realizează în termen de 30 de zile de la data îndeplinirii condițiilor prevăzute la art.6 alin.(1) prin depunerea unei declarații pe propria răspundere.

(7) În sensul alin. (2), operatorii economici și celelalte entități care operează ori furnizează servicii în cadrul sectoarelor și subsectoarelor definite în Anexa au obligația de a pune la dispoziția CERT-RO, la cererea acesteia în calitate de autoritate competentă la nivel național, documentațiile necesare, inclusiv rapoarte de audit, pentru:

a) stabilirea calității de operator de servicii esențiale în conformitate cu art. 6 și 7;

b) stabilirea măsurilor necesare pentru conformarea cu cerințele prezentei legi;

c) stabilirea interdependenței și interconectării rețelelor și sistemelor informatice cu cele ale altor operatori de servicii esențiale ori furnizori de servicii digitale, inclusiv a celor pe care se bazează furnizarea serviciilor entității în cauză.

d) stabilirea listei de autorități ale statului deservite.

(8) Termenul de realizare a auditului menționat la alin. (4), tematica și obiectivele acestuia precum și celelalte documentații necesare înscrierii în registru se stabilesc de către CERT-RO în temeiul prezentei legi, în urma evaluării informațiilor furnizate în conformitate cu alin. (7).

Art. 9. - (1) Entitățile care nu mai îndeplinesc condițiile și criteriile prevăzute la art. 6 notifică CERT-RO în vederea radierii din Registrul operatorilor de servicii esențiale.

(2) CERT-RO dispune radierea din Registrul operatorilor de servicii esențiale la cerere sau din oficiu, în urma evaluării documentațiilor menționate la art. 8 alin. (7) lit.a).

(3) Operatorii de servicii esențiale pot solicita asistența autorității competente în procesul de radiere.

(4) Atunci când o entitate furnizează un serviciu esențial și în cadrul altor state membre ale Uniunii Europene, CERT-RO se consultă cu autoritățile omologe din statele respective în procesul de radiere.

(5) Notificarea prevăzută la alin. (1) se realizează în termen de 30 de zile de la data neîndeplinirii condițiilor prevăzute la art.6 alin.(1).

Art. 10. - (1) În scopul asigurării securității rețelelor și sistemelor informatice, operatorii de servicii esențiale au următoarele obligații:

a) implementează măsurile tehnice și organizatorice adecvate și proporționale pentru îndeplinirea cerințelor minime de securitate stabilite în temeiul prevederilor prezentei legi;

b) implementează măsuri adecvate pentru a preveni și minimiza impactul incidentelor care afectează securitatea rețelelor și a sistemelor informatice utilizate pentru furnizarea acestor servicii esențiale, cu scopul de a asigura continuitatea serviciilor respective;

c) notifică deîndată CERT-RO în calitate de CSIRT național incidentele care au un impact semnificativ asupra continuității serviciilor esențiale;

d) pun la dispoziția CERT-RO informații care să permită stabilirea impactului transfrontalier al incidentului;

e) se supun controlului desfășurat de către CERT-RO în scopul determinării măsurii în care se conformează cu dispozițiile prezentei legi.

f) stabilesc canale permanente de contact, desemnează responsabilii cu securitatea rețelelor și sistemelor informatice însărcinați cu monitorizarea canalelor de contact și comunică autorității competente la nivel național lista acestora precum și orice modificări ulterioare deîndată ce au survenit.

g) notifică deîndată CERT-RO în calitate de autoritate competentă la nivel național orice schimbare survenită în datele furnizate în cadrul procesului de identificare ca operator de servicii esențiale.

h) se interconectează la serviciul de alertare și cooperare al CERT-RO, asigură monitorizarea permanentă a alertelor și solicitărilor primite prin acest serviciu ori prin celelalte modalități de contact și ia în cel mai scurt timp măsurile adecvate de răspuns la nivelul rețelelor și sistemelor informatice proprii.

i) restabilesc funcționarea sistemului la parametrii dinaintea incidentului și realizează auditul de securitate, conform prezentei legi.

(2) Operatorii de servicii esențiale pun la dispoziția CERT-RO în calitate de autoritate competentă la nivel național, la solicitarea motivată a acesteia:

a) informațiile necesare pentru evaluarea securității rețelelor și a sistemelor informatice vizate de prezenta lege, inclusiv politicile de securitate documentate;

b) rezultatele auditului de securitate, inclusiv informațiile și documentațiile pe care se bazează acesta, precum și alte elemente care atestă punerea efectivă în aplicare a cerințelor minime de securitate.

(3) Notificarea afectării serviciilor esențiale prevăzută la alin. (1) lit. c) se face și în situația în care afectarea se datorează unor incidente care afectează un furnizor de servicii digitale de care depinde furnizarea serviciilor esențiale.

Art. 11. - Operatorii de servicii esențiale sunt obligați să implementeze măsurile dispuse de CERT-RO pentru îndeplinirea cerințelor minime de securitate, în vederea remedierii deficiențelor constatate cu ocazia controlului exercitat.

Secțiunea a 2-a – Furnizorii de servicii digitale

Art. 12. - (1) Furnizorii de servicii digitale au următoarele obligații:

a) implementează măsurile tehnice și organizatorice adecvate și proporționale pentru îndeplinirea cerințelor minime de securitate a rețelelor și sistemelor informatice stabilite în temeiul prevederilor prezentei legi cu privire la serviciile prevăzute în Art. 3 lit. o) pe care le oferă pe teritoriul Uniunii Europene ținând cont de normele tehnice menționate la art. 25 alin. 4.

b) implementează măsuri adecvate pentru a preveni și minimiza impactul incidentelor care afectează securitatea rețelelor și a sistemelor informatice utilizate pentru furnizarea serviciilor prevăzute la lit. a), cu scopul de a asigura continuitatea serviciilor acestora;

c) notifică deîndată CERT-RO în calitate de CSIRT național incidentele care au impact semnificativ asupra serviciilor prevăzute Art. 3 lit. o);

d) pun la dispoziția echipei CERT-RO informații care să permită stabilirea impactului transfrontalier al incidentului.

e) stabilesc canale permanente de contact, desemnează responsabilii cu securitatea rețelelor și sistemelor informatice însărcinați cu monitorizarea canalelor de contact și comunică autorității competente la nivel național lista acestora precum și orice modificări ulterioare deîndată ce au survenit.

f) se interconectează la serviciul de alertare și cooperare al CERT-RO, asigură monitorizarea permanentă a alertelor și solicitărilor primite prin acest serviciu ori prin celelalte modalități de contact și ia în cel mai scurt timp măsurile adecvate de răspuns la nivelul rețelelor și sistemelor informatice proprii.

(2) Furnizorii de servicii digitale pun la dispoziția CERT-RO în calitate de autoritate competentă la nivel național, la solicitarea motivată a acestuia:

a) informațiile necesare pentru evaluarea securității rețelelor și a sistemelor informatice vizate de prezenta lege, inclusiv politicile de securitate documentate;

b) rezultatele auditului de securitate, inclusiv informațiile și documentațiile pe care se bazează acesta, precum și alte elemente care atestă punerea efectivă în aplicare a cerințelor minime de securitate.

(3) Obligația de notificare prevăzută la alin. (1) lit. c) se aplică doar în cazul în care furnizorul de servicii digitale are acces la informațiile necesare pentru evaluarea impactului incidentului stipulate la art.26 și care să permită evaluarea stipulată la art. 28.

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

(5) Prevederile art. 12, alin (1) lit. a)-d), alin (2)-(4), art. 25 alin,(4), art. 26 alin. (2) din prezenta lege nu se aplică furnizorilor de servicii digitale care se încadrează în categoria întreprinderilor mici și mijlocii, așa cum sunt definite în Legea nr. 346/2004 privind stimularea înființării și dezvoltării întreprinderilor mici și mijlocii, cu modificările și completările ulterioare.

(6) Operatorii economici precum și celelalte entități care furnizează servicii digitale, au obligația de a furniza către CERT-RO, la solicitarea acesteia următoarele categorii de documente:

a) documentațiile necesare stabilirii calității de furnizor de servicii digitale în sensul prezentei legi;

b) documentațiile necesare stabilirii interdependenței și interconectării rețelelor și sistemelor informatice cu cele ale altor operatori de servicii esențiale ori furnizori de servicii digitale.

c) documentațiile necesare stabilirii listei de autorități ale statului deservite.

CAPITOLUL III - ROLURI ȘI RESPONSABILITĂȚI

Secțiunea 1 – Coordonarea la nivel național

Art. 13. - Coordonarea la nivel național a activităților de asigurare a unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice se realizează de Guvern prin Ministerul Comunicațiilor și Societății Informaționale.

Art. 14. - Strategia națională privind asigurarea unui nivel ridicat de securitate a rețelelor și a sistemelor informatice se aprobă prin hotărâre a Guvernului, la propunerea MCSI.

Secțiunea a 2-a – Autorități competente și responsabilități

Art. 15. - (1) Centrul Național de Răspuns la Incidente de Securitate Cibernetică, denumit în continuare CERT-RO, este autoritate competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice care asigură furnizarea serviciilor esențiale ori furnizează serviciile digitale identificate în temeiul prezentei legi.

(2) Pentru asigurarea unui nivel ridicat de securitate a rețelelor și sistemelor informatice, CERT-RO se consultă și cooperează cu:

a) Serviciul Român de Informații, prin Centrul Național Cyberint, pentru securitatea rețelelor și a sistemelor informatice care asigură servicii esențiale a căror afectare aduce atingere securității naționale;

b) Ministerul Apărării Naționale, pentru securitatea rețelelor și a sistemelor informatice care asigură servicii esențiale în sprijinul activităților privind apărarea națională:

c) Ministerul Afacerilor Interne, Oficiul Registrului Național al Informațiilor Secrete de Stat, Serviciul de Informații Externe, Serviciul de Telecomunicații Speciale și, Serviciul de Protecție și Pază, pentru securitatea rețelelor și a sistemelor informatice care asigură servicii esențiale în domeniul lor de activitate și responsabilitate.

Art. 16. - CERT-RO se consultă și cooperează după caz cu organele de urmărire penală și Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal și Autoritatea Națională pentru Administrare și Reglementare în Comunicații în condițiile legii.

Secțiunea a 3-a – Echipele de intervenție în caz de incidente de securitate informatică

Art. 17. - (1) Echipa CSIRT națională definită la Art. 19 alin. (2) lit. b) respectă cerințele de la art. 24 și acoperă sectoarele din Anexa și serviciile menționate la art. 3 lit. o).

(2) Persoanele juridice de drept privat sau persoanele juridice care activează în cadrul aceluiași sector sau subsector de activitate din Anexa la prezenta lege pot constitui echipe CSIRT proprii, sectoriale sau pot achiziționa servicii de specialitate.

(3) Entitățile enumerate la art. 15 alin. (2) pot constitui echipe CSIRT pentru asigurarea securității rețelelor și sistemelor informatice conform domeniului de activitate și responsabilitate.

Art. 18. - (1) Echipele CSIRT proprii, sectoriale sau serviciile de specialitate stipulate la art. 17 alin. (2) care deservesc operatori de servicii esențiale și furnizori de servicii digitale au în principal următoarele obligații:

a) să se autorizeze în temeiul prezentei legi;

b) să asigure compatibilitatea și interoperabilitatea sistemelor, procedurilor și metodelor utilizate cu cele ale echipei CSIRT naționale din cadrul CERT-RO;

c) să furnizeze cel puțin setul minim de servicii de tip CSIRT necesar asigurării la nivel național a unei protecții unitare a operatorilor și furnizorilor ce fac obiectul prezentei legi;

d) să utilizeze în cadrul echipelor cel puțin o persoană calificată în conformitate cu prevederile prezentei legi;

e) să se interconecteze la serviciul de alertă, monitorizare și cooperare al CERT-RO și să asigure un răspuns prompt la alertele și solicitările transmise de echipa CSIRT națională.

(2) normele privind compatibilitatea și interoperabilitatea menționate la alin. (1) lit. b) precum și setul minim de servicii menționat la alin. (1) lit. c) se stabilesc prin normele tehnice emise de CERT-RO în calitate de autoritate competentă la nivel național în temeiul art. 20 alin. (1) lit. e).

Secțiunea a 4-a – Autoritatea competentă la nivel național – CERT-RO

Art. 19. - (1) CERT-RO își desfășoară activitatea în baza prevederilor prezentei legi și a legislației proprii de organizare și funcționare.

(2) În cadrul CERT-RO se organizează și funcționează:

a) Punctul unic de contact la nivel național;

b) Echipa de intervenție în caz de incidente de securitate informatică la nivel național, denumită în continuare echipa CSIRT națională sau CSIRT național.

Art. 20. - (1) CERT-RO în calitate de autoritate competentă la nivel național are următoarele atribuții generale:

a) identifică, cu consultarea autorităților și entităților de reglementare și administrare a sectoarelor și subsectoarelor prevăzute în Anexă, operatorii de servicii esențiale care au sediul social, filială, sucursală sau punct de lucru pe teritoriul României;

b) elaborează și actualizează normele tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice;

c) elaborează și actualizează normele tehnice privind îndeplinirea obligațiilor de notificare a incidentelor de securitate de către operatorii și furnizorii prevăzuți de prezenta lege;

d) propune și actualizează valorile de prag necesare pentru stabilirea importanței impactului unui incident, după consultarea cu autoritățile și entitățile de reglementare și administrare menționate la litera a);

e) elaborează și actualizează, după consultarea celorlalte instituții cu responsabilități în domeniul apărării, ordinii publice și securității naționale, normele tehnice și regulamentele privind cerințele referitoare la înființarea și funcționarea echipelor CSIRT, precum și cele referitoare la atestarea auditorilor calificați cu competențe în domeniul securității serviciilor esențiale și ține evidența acestora;

f) elaborează și promovează practici comune pentru administrarea incidentelor și a riscurilor și pentru sistemele de clasificare a incidentelor, riscurilor și informațiilor;

g) participă, prin reprezentant, la Grupul de cooperare la nivelul Uniunii Europene, în vederea adoptării soluțiilor optime pentru atingerea obiectivului de securitate și a schimbului de informații între statele membre;

h) permite echipelor CSIRT, acces la datele privind incidentele notificate de operatorii de servicii esențiale sau de furnizorii de servicii digitale, în măsura necesară pentru a-și îndeplini atribuțiile;

i) verifică în condițiile art. 35-43 respectarea de către operatorii de servicii esențiale și furnizorii de servicii digitale a obligațiilor ce le revin conform prezentei legi;

j) emite dispoziții cu caracter obligatoriu pentru operatorii de servicii esențiale în vederea conformării și remedierii deficiențelor constatate și stabilește termenul până la care aceștia trebuie să se conformeze;

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

l) primește sesizări cu privire la neîndeplinirea obligațiilor operatorilor și furnizorilor prevăzuți de prezenta lege;

m) cooperează cu autoritățile competente din celelalte state și oferă asistență acestora, prin schimbul de informații, transmiterea de solicitări și sesizări, efectuarea controlului ori luarea de măsuri de supraveghere și remediere a deficiențelor constatate, în cazul operatorilor și furnizorilor prevăzuți de prezenta lege care își au sediul principal în România ori care, deși au sediul principal stabilit în alt stat membru, rețelele sau sistemele informatice acestora sunt situate și pe teritoriul României;

n) monitorizează aplicarea prevederilor prezentei legi;

o) autorizează, revocă sau reînnoiește autorizarea echipelor CSIRT ce deservesc operatori de servicii esențiale ori furnizori de servicii digitale.

p) eliberează, revocă sau reînnoiește atestatele auditorilor de securitate informatică care pot efectua audit în cadrul rețelelor și sistemelor informatice ce susțin servicii esențiale ori furnizează servicii digitale în condițiile prezentei legi.

q) acreditează, revocă sau reînnoiește acreditarea formatorilor și furnizorilor de servicii de formare în domeniile menționate la literele o) și p).

r) alcătuiește și actualizează periodic, cel puțin o dată la doi ani, lista serviciilor esențiale care îndeplinesc condițiile de la art. 6 alin. (1) cu consultarea autorităților și entităților menționate la alin. (1) precum și a celor menționate la art. 15 alin. (2) și o înaintează MCSI spre a fi supusă aprobării Guvernului.

Art. 21. - În calitate de Punct național unic de contact, CERT-RO are următoarele atribuții:

a) exercită o funcție de legătură între autoritățile statului și autoritățile similare din alte state, Grupul de cooperare și rețeaua CSIRT;

b) elaborează și transmite Grupului de cooperare rapoarte de sinteză privind notificările primite și acțiunile întreprinse ;

c) transmite la cererea autorităților sau a echipelor CSIRT, către punctele unice de contact din celelalte state membre, notificările și solicitările privind incidentele ce

afectează funcționarea serviciilor esențiale și a celor digitale de pe teritoriul respectivelor state;

d) transmite autorităților prevăzute la art. 15 alin. (2) și art. 16 notificările și cererile primite din alte state membre, potrivit domeniului de activitate și responsabilitate.

Art. 22. - În calitate de CSIRT național, CERT-RO are următoarele atribuții:

a) monitorizează incidentele de securitate a rețelelor și sistemelor informatice la nivel național;

b) emite avertizări timpurii, alerte și anunțuri și diseminează informațiile privind riscurile și incidentele către autoritățile prevăzute la art. 15 alin. (2), precum și orice entitate de drept public sau privat căreia îi poate fi afectată securitatea rețelelor și sistemelor informatice;

c) primește notificări privind incidentele care afectează rețelele și sistemele operatorilor de servicii esențiale ori ale furnizorilor de servicii digitale;

d) furnizează operatorului de servicii esențiale care a făcut notificarea, în măsura posibilităților, informații relevante în ceea ce privește acțiunile ulterioare notificării;

e) stabilește, în baza notificărilor primite, impactul la nivel național și transfrontalier al incidentelor și informează autoritățile relevante la nivel național precum și autoritățile similare din alte state potențial afectate;

f) poate informa publicul în condițiile prezentei legi;

g) asigură răspunsul la incidente, potrivit ariei de competență și responsabilitate;

h) elaborează analize dinamice de risc și de incident și sensibilizare situațională;

i) cooperează, la nivel național, cu echipele CSIRT în cadrul unei platforme de management al incidentelor și pentru schimbul de informații;

j) participă la acțiunile comune în cadrul rețelei CSIRT la nivel european, precum și, după necesități, la acțiunile solicitate în cadrul rețelelor internaționale de cooperare;.

k) poate solicita asistența Ageniției Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor - ENISA pentru aducerea la îndeplinire a atribuțiilor sale.

l) înființează, întreține și operează serviciul de alertare și cooperare cu operatorii de servicii esențiale și furnizorii de servicii digitale menționat la art. 10 alin. (1) lit. h) și art. 12 alin. (1) lit. f).

(2) Echipele CSIRT se conectează și realizează schimbul de informații cu echipa CSIRT națională din cadrul CERT-RO prin intermediul platformei de management a incidentelor, menționată la alin.(1), lit. i).

Art. 23. - (1) În scopul cooperării operaționale, Echipa CSIRT națională din cadrul CERT-RO participă la Rețeaua CSIRT compusă din reprezentanți ai echipelor CSIRT naționale ale statelor membre din Uniunea Europeană și cea a CERT-UE.

(2) Cooperarea prevăzută la alin. (1) se realizează prin:

a) schimbul de informații privind serviciile, operațiunile și posibilitățile de cooperare;

b) schimbul și analiza informațiilor fără caracter comercial referitoare la incidentele ce afectează un stat membru;

c) schimbul de informații fără caracter confidențial privind incidente individuale;

d) participa la elaborarea unui răspuns coordonat al Rețelei CSIRT, pentru managementul unui incident identificat pe teritoriul unui alt stat membru;

e) acordarea de sprijin voluntar în abordarea incidentelor transfrontaliere;

f) analiza și identificarea de noi forme de cooperare operațională în cadrul Rețelei CSIRT;

g) participarea la elaborarea de orientări și practici unitare în domeniul cooperării operaționale;

h) solicitarea Rețelei CSIRT de a asigura un răspuns coordonat la un incident identificat la nivel național.

(3) Fac excepție de la schimbul de informații prevăzut la alin. (2) lit. c) situațiile în care schimbul ar periclita investigarea incidentului.

(4) Echipa CSIRT participă și la alte rețele internaționale de cooperare, după necesități.

Art. 24. - (1) În vederea îndeplinirii atribuțiilor ce îi revin în calitate de autoritate competentă la nivel național în temeiul art. 20, CERT-RO va beneficia prin finanțare de la bugetul de stat de resurse materiale, financiare și umane suficiente pentru:

a) desfășurarea activităților de normare prevăzute la art. 20 alin. (1) lit. a)-f) și r);

b) primirea sesizărilor, efectuarea controlului, verificărilor și supravegherilor prevăzute la art. 20 alin. (1) lit. i)-l) precum și pentru asigurarea punerii în aplicare a deciziilor și sancțiunilor, rezolvării contestațiilor și reprezentarea în contencios administrativ.

c) desfășurarea activităților de cooperare prevăzute la art. 20 alin. (1) lit. g), h) și m)

d) înființarea, administrarea și funcționarea registrelor și evidențelor prevăzute de art. 20 alin. (1) lit. o)-r) precum și a registrului operatorilor de servicii esențiale prevăzut la art. 7.

e) desfășurarea activităților de autorizare și acreditare prevăzute la art. 20 alin. (1) lit. o)-q).

f) luarea măsurilor cu caracter excepțional prevăzute la art. 42.

(2) În vederea îndeplinirii atribuțiilor ce îi revin în calitate de Punct unic de contact la nivel național, CERT-RO beneficiază prin finanțare de la bugetul de stat de resurse materiale, financiare și umane suficiente pentru asigurarea în regim permanent a funcției de legătură, primire și retransmitere a cererilor și solicitărilor prevăzute la art. 21 lit. a), c) și d).

(3) În vederea îndeplinirii atribuțiilor ce îi revin în calitate de echipă CSIRT națională conform art. 22 și 23, CERT-RO beneficiază prin finanțare de la bugetul de stat de resurse materiale, financiare și umane suficiente pentru:

a) monitorizarea în regim permanent a incidentelor și primirea notificărilor și alertelor specificate la art. 22 lit. a) și c)

b) emiterea avertizărilor, contactarea și alertarea altor entități și diseminarea de informații relevante în temeiul art. 22 lit. b), d), e), f) și l).

c) asigurarea răspunsului, intervenției și cooperării în temeiul art. 22 lit. g), i), j), k), l)

d) stabilirea impactului incidentelor și analiza acestora în temeiul art. 22 lit. e) și h)

(4) Resursele alocate conform alin (1)-(3) vor asigura:

a) continuitatea activităților și disponibilitatea permanentă a serviciilor;

b) participarea la Grupul de cooperare prevăzut de art. 20;

c) un sistem adecvat de gestionare și transmitere a cererilor;

d) o infrastructură adecvată prevăzută cu sisteme redundante;

e) spațiu de lucru de rezervă în amplasamente securizate;

f) disponibilitatea ridicată a serviciilor de comunicații prin mijloace multiple de contact, capacitatea de a contacta alte entități în orice moment și evitarea punctelor unice de defecțiune;

g) amplasamente securizate a sediilor echipei CSIRT naționale din cadrul CERT-RO și a sistemelor informatice de suport;

h) mijloacele necesare asigurării controlului punerii în aplicare a dispozițiilor prezentei legi și aplicării de sancțiuni precum și pentru îndeplinirea celorlalte obligații ce îi revin conform legii.

(5) Resursele financiare necesare pentru funcționarea CERT-RO se asigură de la bugetul de stat precum și din venituri proprii.

(6) Veniturile proprii ale CERT-RO se constituie din următoarele categorii:

a) sumele provenite din activitățile prevăzute la art. 20 alin. (1) lit. o) – q);

b) sumele provenite din amenzile administrative aplicate în temeiul art. 41;

c) sumele provenite din furnizarea serviciului prevăzut de art. 22 alin. (1) lit. l);

d) alte venituri proprii în conformitate cu prevederile legale pentru instituțiile finanțate parțial din venituri proprii.

(7) Tarifele pentru serviciile menționate la alin. (6) lit. a) și c) se stabilesc prin decizia directorului general al CERT-RO și se publică în Monitorul Oficial al României, Partea I.

(8) Sumele care constituie venituri proprii ale CERT-RO se evidențiază separat în cadrul bugetului MCSI și se regăsesc permanent la dispoziția CERT-RO.

(9) Sumele care constituie venituri proprii ale CERT-RO pot fi utilizate în condițiile legii, după necesități, pentru:

a) achiziționarea de servicii de specialitate;

b) închirierea, achiziționarea sau construcția de imobile în vederea desfășurării activității;

c) achiziția de echipamente și software, inclusiv software dezvoltat la comandă;

d) afilierea la rețele și organizații internaționale de profil și participarea prin reprezentanți la lucrările acestora precum și la alte evenimente de profil;

e) cursuri de formare și perfecționare precum și certificări ale personalului propriu;

f) editarea de publicații, ghiduri de specialitate, clipuri video de conștientizare;

g) organizarea de conferințe seminarii și alte evenimente de profil;

h) efectuarea de studiii statistice și finanțarea de activități de cercetare;

i) constituirea unui fond de urgență pentru intervenții ale echipei CSIRT naționale;

j) renovări și îmbunătățiri ale sediilor și locațiilor de desfășurare a activității.

k) finanțarea altor activități în vederea îndeplinirii atribuțiilor ce îi revin, în condițiile legii;

(10) CERT-RO poate folosi pentru desfășurarea activității bunuri materiale şi fonduri băneşti primite de la persoanele juridice şi fizice, sub forma de donaţii şi sponsorizări, cu respectarea dispoziţiilor legale.

(11) CERT-RO poate înființa birouri și sedii la nivel local și regional în vederea asigurării activităților și reprezentării adecvate pentru îndeplinirea obligațiilor ce îi revin în temeiul prezentei legi.

CAPITOLUL IV - ASIGURAREA SECURITĂȚII REȚELELOR ȘI SISTEMELOR INFORMATICE

Secțiunea 1 – Cerințele minime de securitate

Art. 25. - (1) În vederea asigurării unui nivel comun de securitate a rețelelor și sistemelor informatice, operatorii de servicii esențiale și furnizorii de servicii digitale au obligația de a respecta normele tehnice emise CERT-RO în temeiul prevederilor art. 20 alin. (1) lit. b).

(2) CERT-RO elaborează cu consultarea autorităților care reglementează sectoarele și subsectoarele prevăzute în Anexă ghiduri în sprijinul implementării măsurilor minime de securitate pentru operatorii și furnizorii prevăzuți în prezenta lege.

(3) Normele tehnice prevăzute la alin. (1) aplicabile operatorilor de servicii esențiale se stabilesc în baza cel puțin a următoarelor categorii de activități de asigurare a securității rețelelor și sistemelor informatice:

a) managementul drepturilor de acces;

b) conștientizarea și instruirea utilizatorilor;

c) jurnalizarea și asigurarea trasabilității activităților în cadrul rețelelor și sistemelor informatice;

d) testarea și evaluarea securității rețelelor și sistemelor informatice;

e) managementul configurațiilor rețelelor și sistemelor informatice;

f) asigurarea disponibilității serviciului esențial și a funcționării rețelelor și sistemelor informatice;

g) managementul continuității funcționării serviciului esențial;

h) managementul identificării și autentificării utilizatorilor;

i) răspunsul la incidente;

j) mentenanța rețelelor și sistemelor informatice;

k) managementul suporturilor de memorie externă;

l) asigurarea protecției fizice a rețelelor și sistemelor informatice;

m) realizarea planurilor de securitate;

n) asigurarea securității personalului;

o) analizarea și evaluarea riscurilor ;

p) asigurarea protecției produselor și serviciilor aferente rețelelor și sistemelor informatice;

q) managementul vulnerabilităților și alertelor de securitate

(4) Normele tehnice prevăzute la alin. (1) aplicabile furnizorilor de servicii digitale se stabilesc în baza următoarelor categorii de activități de asigurare a securității rețelelor și sistemelor informatice:

a) securitatea sistemelor și a instalațiilor;

b) gestionarea incidentelor;

c) gestionarea continuității activității;

d) monitorizarea, auditarea și testarea;

e) conformitatea cu standardele europene și internaționale.

(5) În implementarea măsurilor de la alin. (1) operatorii de servicii esențiale:

a) identifică rețelele și sistemele informatice care susțin furnizarea de servicii esențiale;

b) elaborează și implementează politici și planuri proprii de securitate a rețelelor și sistemelor informatice;

c) asigură managementul incidentelor care afectează securitatea rețelelor și sistemelor informatice ;

d) previn accesul neautorizat la rețelele și sistemele informatice;

e) previn diseminarea datelor deținute la nivelul rețelelor și sistemelor informatice către alte persoane decât cele autorizate să cunoască conținutul acestora.

f) implementează un sistem de management al riscului;

g) implementează planuri de acțiune pe niveluri de alertă de securitate a rețelelor și sistemelor informatice;

h) asigură continuitatea serviciilor;

(6) Normele tehnice prevăzute la alin.(1) se emit cu luarea în considerare a cerințelor și standardelor europene și internaționale fără a impune sau a discrimina în favoarea utilizării unui anumit tip de tehnologie.

Secțiunea a 2-a – Notificarea incidentelor de securitate

Art. 26. - (1) Notificările efectuate de operatorii de servicii esențiale în temeiul art. 10 alin. (1) lit. c) și f) trebuie să îndeplinească condițiile și să conțină informațiile prevăzute în normele tehnice prevăzute la art. 20 alin. (1) lit. c).

(2) Notificările efectuate de furnizorii de servicii digitale în temeiul art. 12 alin. (1) lit. c) trebuie să îndeplinească condițiile și să conțină informațiile prevăzute în normele tehnice menționate la art. 20 alin. (1) lit. c)

(3) Notificarea incidentelor conține, în mod obligatoriu, următoarele elemente:

a) elementele de identificare ale infrastructurii și operatorului sau furnizorului în cauză;

b) descrierea incidentului;

c) perioada de desfăşurare a incidentului;

d) impactul estimat al incidentului;

e) măsuri preliminare adoptate;

f) lista de autorități ale statului afectate de incident;

g) întinderea geografică potențială a incidentului;

h) date despre efecte potențial transfrontaliere ale incidentului;

(4) Notificarea prevăzută la alin. (1) și (2) nu va conține:

a) informații clasificate;

b) date care pot aduce atingere drepturilor şi libertăţilor cetăţeneşti ori intereselor legitime ale unor terţe entităţi implicate, în condițiile legii.

(5) CERT-RO în calitate de autoritate competentă la nivel național va elabora și publica ghiduri de notificare și formularele necesare.

(6) CERT-RO în calitate de CSIRT național va stabili și va aduce la cunoștința publicului precum și operatorilor și furnizorilor menționați în prezenta lege, canalele de comunicare pentru efectuarea notificărilor cerute prin prezenta lege.

(7) Notificările privind incidentele ce fac obiectul prezentei legi pot fi făcute și de către echipele CSIRT ale entităților de drept public sau privat ori care deservesc un anumit sector de activitate, ori de către furnizorii de servicii de securitate aflați în relație contractuală, conform atribuțiilor ce le revin în baza actului de înființare ori a contractului de prestări servicii, după caz.

(8) Notificarea făcută de o echipă CSIRT în temeiul alin. (7) echivalează cu notificarea făcută de operatorul sau furnizorul afectat, acesta purtând întreaga răspundere pentru conținutul notificării și îndeplinirea celorlalte obligații ce îi revin conform prezentei legi.

(9) Obligația de a notifica un incident de către furnizorii de servicii digitale se aplică doar în cazul în care aceștia au acces la informațiile necesare pentru a evalua impactul unui incident asupra parametrilor menționați la art. 25, alin. (4).

(10) Entitățile care nu au fost identificate drept operatori de servicii esențiale și nu sunt furnizori de servicii digitale pot notifica voluntar CERT-RO în calitate de CSIRT național incidentele care au un impact semnificativ asupra continuității serviciilor pe care le furnizează.

(11) CERT-RO tratează notificările obligatorii cu prioritate față de notificările voluntare.

(12) Notificările voluntare se tratează doar atunci când această prelucrare nu împiedică îndeplinirea celorlalte obligații ce îi revin autorității competente la nivel național și în limita resurselor existente.

(13) Notificarea voluntară nu impune entității notificatoare nicio obligație care nu i-ar fi revenit dacă nu ar fi făcut notificarea.

(14) Notificările prevăzute la alin (1) și (2) nu expun entitățile care notifică unei răspunderi sporite.

Secțiunea a 3-a – Managementul incidentelor

Art. 27. - (1) După primirea notificării, CERT-RO în calitate de CSIRT național:

a) evaluează preliminar impactul incidentului la nivel național și alertează, sau după caz, poate solicita operatorului sau furnizorului să alerteze alte entități afectate precum și autoritățile cu responsabilități în prevenirea, limitarea și combaterea efectelor incidentului potrivit legii;

b) poate solicita informații suplimentare operatorului sau furnizorului care a făcut notificarea în vederea îndeplinirii obligațiilor ce îi revin;

c) oferă operatorului sau furnizorului care a făcut notificarea, atunci când circumstanțele o permit, informații care ar putea sprijini administrarea incidentului;

d) în calitate de Punct unic de contact informează celelalte state membre sau partenere afectate dacă incidentul are un impact semnificativ asupra continuității serviciilor esențiale ori a serviciilor digitale în statele respective;

e) în urma analizei incidentelor, poate declanșa după caz acțiune de control pentru verificarea respectării cerințelor prezentei legi;

f) poate lua măsurile stipulate la art. 42;

g) coordonează la nivel național răspunsul la incident în colaborare cu celelalte autorități și entități publice sau private, conform domeniului de activitate și responsabilitate.

Art. 28. - Impactul unui incident se determină ținând cont cel puțin de următorii parametri:

(1) În cazul operatorilor de servicii esențiale:

a) numărul de utilizatori afectați de perturbarea serviciului esențial;

b) durata incidentului;

c) distribuția geografică în ceea ce privește zona afectată de incident.

(2) În cazul furnizorilor de servicii digitale:

a) numărul de utilizatori afectați de incident, în special utilizatori care se bazează pe serviciu pentru furnizarea propriilor servicii;

b) durata incidentului;

c) distribuția geografică în ceea ce privește zona afectată de incident;

d) amploarea perturbării funcționării serviciului;

e) amploarea impactului asupra activităților economice și societale.(3) CERT-RO în calitate de autoritate competentă la nivel național elaborează și actualizează normele tehnice de stabilire a impactului pentru categoriile de operatori și furnizori.

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

(2) Pentru incidentele care afectează un operator de servicii esențiale sau un furnizor de servicii digitale informarea menționată la alin. (1) se realizează după consultarea prealabilă a acestuia asupra conținutului înștiințării.

(3) În cazul furnizorior de servicii digitale, informarea publicului specificată la alin (1) poate fi făcută și direct de către aceștia la solicitarea CERT-RO ori a autorităților sau echipelor CSIRT ale altor state membre afectate.

Art. 30. - (1) În activitatea de primire a notificărilor și de management al incidentelor desfășurată în baza prezentei legi, CERT-RO protejează interesele de securitate și comerciale ale operatorului de servicii esențiale și ale furnizorului de servicii digitale, precum și confidențialitatea informațiilor furnizate în notificare, în conformitate cu legislația în vigoare.

(2) Informațiile prelucrate în sensul îndeplinirii obligațiilor de la alin. (1) nu fac parte din categoria informațiilor de interes public așa cum acestea sunt reglementate în legea 544/2002 cu modificările și completările ulterioare.

(3) Informațiile confidențiale conform legislației naționale și normelor Uniunii Europene, precum cele privind secretul comercial, fac obiectul schimbului de informații cu Comisia și cu alte autorități numai dacă acest lucru este necesar pentru aplicarea prezentei legi.

(4) Informațiile care fac obiectul schimbului se limitează la informații relevante și proporționale cu scopul urmărit.

(5) Schimbul de informații se va face cu garantarea păstrării confidențialității informațiilor și protejarea securității și intereselor comerciale ale operatorilor de servicii esențiale și ale furnizorilor de servicii digitale.

(6) Prelucrarea datelor cu caracter personal se efectuează în conformitate cu legislația în vigoare.

CAPITOLUL V – AUDIT ȘI AUTORIZARE

Secțiunea 1 – Auditul de securitate a rețelelor și sistemelor informatice aparținând operatorilor de servicii esențiale sau furnizorilor de servicii digitale

Art. 31. - Poate fi auditor de securitate a rețelelor și sistemelor informatice - persoana fizică autorizată sau persoana juridică ce realizează, audit de securitate a rețelelor și sistemelor informatice, adică desfășoară acea activitate prin care se realizează o evaluare sistematică a tuturor politicilor, procedurilor și măsurilor de

protecţie implementate la nivelul rețelelor și sistemelor informatice, în vederea identificării disfuncţiilor şi vulnerabilităţilor şi a furnizării unor soluţii de remediere a acestora.

Art. 32. - (1) Auditul de securitate specificat la art. 8 alin. (4), respectiv art. 10 alin. (2) lit. b) și art. 12 alin. (2) lit. b) se realizează de către auditorii de securitate informatică ce dețin atestat valabil eliberat de către CERT-RO pentru a audita rețele și sisteme informatice ce deservesc servicii esențiale sau servicii digitale.

(2) În acest sens CERT-RO:

a) întreține și actualizează Registrul auditorilor menționați la alin. (1);

b) elaborează şi aprobă, prin ordinul directorului general al CERT-RO, regulamentul pentru atestarea şi verificarea auditorilor de securitate informatică pentru rețelele și sistemele informatice aparținând operatorilor de servicii esențiale sau furnizorilor de servicii digitale și stabilește condițiile de valabilitate pentru atestatele acordate;

c) acordă, prelungește, suspendă sau retrage atestarea pentru auditorii de securitate informatică pentru rețelele și sistemele informatice aparținând operatorilor de servicii esențiale sau furnizorilor de servicii digitale, în conformitate cu prevederile regulamentului prevăzut la lit. b)

d) verifică în urma sesizărilor sau din oficiu în conformitate cu prevederile art. 35-43 îndeplinirea de către auditori autorizați în temeiul prezentei legi a obligațiilor legale ce le revin.

e) stabilește tematicile pentru specializarea auditorilor în vederea atestării menționate la lit. c) și acreditează, verifică, suspendă sau retrage autorizarea formatorilor din domeniul auditului de securitate informatică pentru rețelele și sistemele informatice ale operatorilor de servicii esențiale și 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 atestați care asigură în mod curent servicii de securitate informatică ori servicii de tip CSRIT operatorului de servicii esențiale sau furnizorul de servicii digitale, ori sunt angajați ai acestora.

b) auditorul care are un contract de prestări servicii pentru rețeaua și sistemul supus auditului aflat în desfășurare la momentul la care se efectuează auditul sau într-un termen mai mic de un an.

c) auditorul care a mai efectuat 3 audituri consecutive la același operator de servicii esențiale

(4) Activitatea de audit se efectuează potrivit standardelor și specificațiilor europene și internaționale aplicabile în domeniu.

(5) Tematicile de audit vor ține seama de normele tehnice în vigoare emise de către CERT-RO privind securitatea rețelelor și sistemelor informatice ale operatorilor de servicii esențiale și a furnizorilor de servicii digitale.

(6) Atestatele au o valabilitate de 3 ani.

(7) Sumele percepute ca tarife pentru serviciile de la alin. (2) lit. c) și e) constituie venituri la bugetul CERT-RO.

(8) Constituie excepţie de la prevederile alin. (1) auditul de securitate realizat la nivelul instituţiilor cu responsabilităţi în domeniul apărării, ordinii publice şi securităţii naţionale

Secțiunea a 2-a Autorizarea echipelor CSIRT ce deservesc rețele și sisteme informatice din categoria serviciilor esențiale și serviciilor digitale

Art. 33. - (1) Echipele CSIRT care deservesc operatori de servicii esențiale ori furnizori de servicii digitale se autorizează de către CERT-RO în calitate de autoritate competentă la nivel național.

(2) În acest sens CERT-RO:

a) întreține și actualizează Registrul echipelor CSIRT menționate la alin. (1);

b) elaborează şi aprobă, prin ordinul directorului general al CERT-RO, regulamentul pentru autorizarea şi verificarea echipelor CSIRT care deservesc operatorii de servicii esențiale sau furnizorii de servicii digitale și stabilește condițiile de valabilitate pentru autorizațiile acordate;

c) acordă, prelungește, suspendă sau retrage autorizarea pentru echipele CSIRT, în conformitate cu prevederile regulamentului prevăzut la lit. b)

d) verifică în urma sesizărilor sau din oficiu în conformitate cu prevederile art. 35-43 îndeplinirea de către echipele CSIRT acreditate în temeiul prezentei legi a obligațiilor legale ce le revin.

e) stabilește tematicile pentru formarea membrilor echipelor CSIRT în vederea autorizării menționate la lit. c) și acreditează, verifică, suspendă sau retrage autorizarea formatorilor din domeniul asigurării de servicii de tip CSIRT pentru rețelele și sistemele informatice ale operatorilor de servicii esențiale și furnizorilor de servicii digitale.

(3) În vederea autorizării echipa CSIRT trebuie să îndeplinească condițiile prevăzute în normele tehnice elaborate în temeiul art. 20 alin. (1) lit. e).

(4) Autoritzațiile au o valabilitate de 3 ani.

(5) Sumele percepute ca tarife pentru serviciile de la alin. (2) lit. c) și e) constituie venituri la bugetul CERT-RO.

CAPITOLUL VI – COOPERARE

Art. 34. - (1) Autoritățile și entitățile care reglementează sectoarele și subsectoarele de activitate specificate în Anexă au obligația de a coopera și sprijini CERT-RO în calitate de autoritate competentă la nivel național și de a răspunde solicitărilor acesteia, potrivit domeniilor de activitate și responsabilitate pentru:

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

b) identificarea operatorilor de servicii esențiale în sensul prezentei legi și actualizarea listei acestora;

c) identificarea cerințelor de securitate și notificare existente în cadrul sectorului sau subsectorului respectiv, în vederea determinării nivelului de securitate asigurat de acestea.

d) stabilirea cerințelor specifice de asigurare a securității rețelelor și sistemelor informatice și de notificare a incidentelor survenite pentru sectoarele și subsectoarele prevăzute în Anexa.

e) armonizarea cerințelor specifice menționate la punctele anterioare cu cerințele de securitate și notificare prevăzute de prezenta lege.

f) luarea măsurilor cu caracter excepțional stipulate la art. 42

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

(2) Cerințele specifice de securitate impuse operatorilor de servicii esențiale sau furnizorilor de servicii digitale prin acte juridice europene transpuse la nivel național care reglementează respectivul sector de activitate se aplică doar în măsura în care nivelul de securitate asigurat este cel puțin echivalent cu obligațiile prevăzute în prezenta lege.

(3) Aplicarea actelor juridice europene menționate la alin. (2) nu derogă de la celelalte obligații care revin operatorilor de servicii esențiale și furnizorilor de servicii digitale conform prezentei legi.

CAPITOLUL VII - SUPRAVEGHERE, CONTROL, SANCȚIONARE

Secțiunea 1 – Activitatea de control

Art. 35. - (1) Controlul respectării prevederilor prezentei legi, ale legislației speciale din domeniul asigurării securității rețelelor și sistemelor informatice şi ale actelor normative sau individuale emise de CERT-RO în calitate de autoritate competentă la nivel național în conformitate cu dispoziţiile prezentei legi ori ale legislaţiei speciale din domeniul asigurării securității rețelelor și sistemelor informatice pentru care CERT-RO are calitatea de autoritate competentă la nivel național, precum şi al respectării obligaţiilor operatorilor de servicii esențiale și ale furnizorilor de servicii digitale definiți în prezenta lege care decurg din regulamentele Uniunii Europene, acolo unde se stabileşte competenţa de monitorizare sau de verificare a respectării acestor obligaţii de către CERT-RO în calitate de autoritate competentă la nivel național, revine CERT-RO, care acţionează prin personalul de specialitate împuternicit în acest scop, denumit în continuare personal de control.

(2) Personalul de control, precum şi atribuţiile acestuia se stabilesc prin decizie a directorului CERT-RO.

Art. 36. - (1) Personalul de control poate să efectueze acţiuni de control, inclusiv inopinate, în cadrul cărora poate să solicite, menţionând temeiul legal şi scopul solicitării, orice documente necesare pentru efectuarea controlului, să ridice copii de

pe orice registre, acte financiar-contabile şi comerciale ori alte acte sau documente, cu respectarea prevederilor legale în vigoare.

(2) În cadrul acţiunilor de control, personalul de control poate să solicite şi să primească, la faţa locului sau la termenul solicitat, orice informaţii necesare pentru efectuarea controlului şi poate stabili termene până la care aceste informaţii să îi fie furnizate, sub sancţiunea prevăzută la art. 41 alin. (1) lit. c), cu respectarea prevederilor legale în vigoare.

(3) Rezultatul acţiunilor de control va fi consemnat într-o notă de control.

Art. 37. - (1) În cazul descoperirii nerespectării de către un furnizor de servicii digitale sau operator de servicii esențiale a unei obligaţii prevăzute în prezenta lege sau în legislaţia specială din domeniul asigurării securității rețelelor și sistemelor informatice şi ale actelor normative sau individuale emise de CERT-RO în calitate de autoritate competentă la nivel național în conformitate cu dispoziţiile prezentei legi ori ale legislaţiei speciale din domeniul asigurării securității rețelelor și sistemelor informatice pentru care CERT-RO are calitatea de autoritate competentă la nivel național ori a unei obligaţii care decurge din regulamentele Uniunii Europene, atunci când competenţa de monitorizare şi verificare a acestei obligaţii aparţine autorităţii competente la nivel național, înainte de aplicarea sancţiunii, CERT-RO va transmite entității în cauză o notificare prin care îi va aduce la cunoştinţă încălcarea constatată şi sancţiunea aplicabilă, acordându-i un termen în vederea formulării unui punct de vedere.

Art. 38. - Următoarele fapte constituie contravenţii:

1. încălcarea obligației prevăzută la art. 8 alin. (1).

2. nerespectarea termenului prevăzut la art. 8 alin. (6).

3. nefurnizarea în termenul specificat de CERT-RO în calitate de autoritate competentă la nivel național a informațiilor și documentațiilor solicitate în temeiul art. 8 alin. (7).

4. nedepunerea raportului de audit specificat la art. 8 alin. (4).

5. nerespectarea termenului prevăzut la art. 9 alin. (6).

6. încălcarea obligațiilor prevăzute la art. 10 alin. (1) lit. a)-h).

7. nefurnizarea în termenul specificat de CERT-RO în calitate de autoritate competentă la nivel național a informațiilor și documentațiilor solicitate în temeiul art. 10 alin. (2) lit. a) și b)

8. încălcarea obligației prevăzută la art. 10 alin. (3).

9. neîndeplinirea obligației prevăzute la art. 11 în termenul specificat de CERT-RO în calitate de autoritate competentă la nivel național.

10. neîndeplinirea obligațiilor prevăzute la art. 12 alin. (1) lit. a)-d).

11. nefurnizarea în termenul specificat de CERT-RO în calitate de autoritate competentă la nivel național a informațiilor și documentațiilor solicitate în temeiul art. 12 alin. (2) lit. a) și b)

12. nefurnizarea în termenul specificat de CERT-RO în calitate de autoritate competentă la nivel național a informațiilor și documentațiilor solicitate în temeiul art. 12 alin. (6).

13. neîndeplinirea obligațiilor stipulate la art. 18 alin (1).

14. nerespectarea de către furnizorii de servicii digitale a măsurilor instituite în temeiul art. 20 alin. (1) lit. k).

15. nerespectarea normelor tehnice stipulate la art. 25 alin. (1).

16. neîndeplinirea obligațiilor stipulate la art. 26 alin. (1)-(3).

17. nefurnizarea informațiilor suplimentare solicitate de CERT-RO în temeiul art. 27 alin. (1) lit. b).

18. neconformarea la obligația de a se supune verificărilor stipulate la art. 27 alin. (1) lit. e).

19. nefurnizarea în notificarea privind incidentele de securitate a informațiilor care să permită CERT-RO să stabilească impactul incidentului în conformitate cu parametrii prevăzuți la art. 28 alin. (1) și (2) și cu normele tehnice de stabilire a impactului stipulate la art. 28 alin. (3).

20. încălcarea de către auditorii specificați la art. 32 alin. (1) a normelor privind incompatibilitatea, stipulate la art. 32 alin. (3).

21. furnizarea de rapoarte de audit de securitate dintre cele specificate la art. 8 alin. (4), art. 9 alin. (4), respectiv art. 10 alin. (2) lit. b) și art. 12 alin. (2) lit. b) realizate de către auditori fără atestat valabil eliberat de CERT-RO în temeiul art. 32 alin. (1)

și (2) lit. c) ori aflați într-una din stările de incompatibilitate stipulate la art. 32 alin. (3).

22. asigurarea de servicii de tip echipă CSIRT către operatorii de servicii esențiale ori furnizorii de servicii digitale de către entități care nu dețin autorizație valabilă, eliberată în temeiul art. 33 alin. (1) de către CERT-RO în calitate de autoritate competentă la nivel național.

23. neîndeplinirea de către autoritățile și entitățile de reglementare pentru sectoarele și subsectoarele de activitate specificate în Anexă a obligațiilor stipulate la art. 34 alin. (1) precum și neparticiparea în procesul de stabilire a nivelului de securitate menționat la art. 34 alin. (2).

24. neîndeplinirea ori îndeplinirea cu rea credință a obligaților stipulate la art. 44.

Art. 39. - (1) Contravenţiile prevăzute la art. 38 se sancţionează astfel:

a) cu amendă de la 3.000 lei la 50.000 lei, iar, în cazul unor încălcări repetate, cu amendă în cuantum de până la 100.000 lei;

b) prin derogare de la dispoziţiile art. 8 alin. (2) lit. a) din Ordonanţa Guvernului nr. 2/2001 privind regimul juridic al contravenţiilor, aprobată cu modificări şi completări prin Legea nr. 180/2002, cu modificările şi completările ulterioare, pentru persoanele cu o cifră de afaceri de peste 2.000.000 lei, cu amendă în cuantum de până la 2% din cifra de afaceri, iar, în cazul unor încălcări repetate, cu amendă în cuantum de până la 5% din cifra de afaceri.

(2) În vederea individualizării sancţiunii, CERT-RO va lua în considerare gradul de pericol social concret al faptei, perioada de timp în care obligaţia legală a fost încălcată, precum şi, dacă este cazul, consecinţele încălcării.

(3) Cifra de afaceri este cea prevăzută în ultima situaţie financiară anuală raportată de operatorul economic.

(4) Pentru persoanele fizice autorizate, întreprinderile individuale şi întreprinderile familiale, cifrei de afaceri prevăzute la alin. (1) lit. b) îi corespunde totalitatea veniturilor brute realizate de respectivii operatori economici.

(5) În măsura în care prezenta lege nu prevede altfel, contravenţiilor prevăzute la art. 38 li se aplică dispoziţiile Ordonanţei Guvernului nr. 2/2001, aprobată cu modificări şi completări prin Legea nr. 180/2002, cu modificările şi completările ulterioare.

Art. 40. - (1) Contravenţiile prevăzute la art. 38 se constată de către personalul de control din cadrul CERT-RO prin procesul-verbal de constatare a contravenţiei şi de aplicare a sancţiunii.

(2) Sancţiunea pentru contravenţiile prevăzute la alin. (1) se aplică, prin rezoluţie scrisă, de către directorul CERT-RO.

Art. 41. - (1) CERT-RO poate aplica amenzi administrative în cuantum de până la 30.000 lei pentru fiecare zi de întârziere, stabilind totodată şi data de la care acestea se calculează în cazul:

a) nerespectării termenului de furnizare a informaţiilor solicitate de CERT-RO în conformitate cu dispoziţiile prezentei legi sau ale legislaţiei speciale din domeniul asigurării securității rețelelor și sistemelor informatice pentru care rolul de autoritate competentă la nivel național revine CERT-RO, precum şi a informaţiilor stabilite prin actele normative ori individuale emise de CERT-RO în conformitate cu dispoziţiile prezentei legi sau ale legislaţiei speciale din domeniul comunicaţiilor electronice;

b) nerespectării obligaţiilor prevăzute la art. 10 alin. (1) lit. a)-h) și art. 12 alin. (1) lit. a)-f);

c) refuzului de a se supune controlului ori de a efectua auditul de securitate prevăzut la art. 10 alin. (2) lit. a) și b) și art. 12 alin. (2) lit. a) și b) sau transmiterea rezultatelor auditului;

(2) Decizia directorului CERT-RO prin care se aplică sancţiunile prevăzute la alin. (1) constituie titlu executoriu, fără vreo altă formalitate.

(3) Sumele rezultate din încasarea amenzilor administrative stabilite la alin. (1) se reţin integral ca venituri proprii, cu titlu permanent, la dispoziţia CERT-RO şi vor fi folosite în conformitate cu prevederile bugetului de venituri şi cheltuieli aprobat potrivit legii.

Art. 42. - (1) În cazul constatării unei contravenții în conformitate cu art. 38, CERT-RO poate dispune încetarea încălcării dispozițiilor respective fie imediat, fie într-un termen rezonabil, precum și orice măsuri necesare pentru a asigura încetarea încălcării și remedierea situației produse. Măsurile vor fi adecvate și proporționale cu

încălcarea săvârșită și vor prevedea un termen în care operatorul de servicii esențiale ori furnizorul de servicii digitale trebuie să se conformeze acestora;

(2) În cazul în care nerespectarea de către operatori sau furnizori a obligaţiilor din prezenta lege poate crea probleme grave de natură economică sau operaţională altor operatori sau furnizori, CERT-RO poate lua măsuri urgente cu caracter provizoriu pentru remedierea situaţiei.

(3) În cazul în care nerespectarea de către operatori sau furnizori a obligaţiilor prevăzute de prezenta lege prezintă un pericol grav şi iminent la adresa apărării naţionale, ordinii publice, securităţii naţionale sau sănătăţii publice, CERT-RO va înştiinţa şi, dacă este necesar, va coopera cu organele judiciare, precum şi cu instituţiile competente din domeniul apărării şi securităţii naţionale, ordinii publice sau sănătăţii publice, în vederea remedierii situației constatate și asigurării legalității condițiilor operării de servicii esențiale sau furnizării de servicii digitale. CERT-RO poate lua măsuri urgente, proporţionale şi cu caracter provizoriu pentru remedierea situaţiei, cu consultarea sau la solicitarea motivată a acestor instituţii, după caz.

(4) Atunci când apreciază că este necesar, CERT-RO poate menţine măsurile dispuse conform alin. (2) şi (3) pentru o perioadă de cel mult 90 de zile. În cazul în care punerea în executare a acestora necesită o durată mai mare de timp, CERT-RO poate dispune prelungirea aplicabilităţii pentru o perioadă suplimentară de cel mult 90 de zile. Operatorului sau furnizorului în cauză i se va acorda posibilitatea de a-şi prezenta punctul de vedere şi de a propune soluţii pentru remedierea definitivă a situaţiei create.

(5) Măsurile prevăzute la alin. (2) şi (3) se dispun prin decizie a directorului CERT-RO.

(6) Măsurile prevăzute de alin (2) se pot dispune de către CERT-RO cu titlu excepțional și în situația administrării unor incidente de natură să prezinte pericolele ori să aibă urmările prevăzute la alin. (3) cu consultarea precum și la solicitarea motivată a instituțiilor menționate la aliniatul respectiv.

Art. 43. - (1) În exercitarea atribuţiilor ce îi revin potrivit actelor normative în vigoare, CERT-RO va fi sprijinită operativ, la cerere, de către autorităţile administraţiei publice locale, de organele de poliţie ori de alte autorităţi publice, în vederea identificării şi localizării persoanelor fizice sau juridice care săvârşesc fapte de natură contravenţională.

(2) Orice decizie a CERT-RO prin care se vatămă drepturile unei persoane fizice sau juridice, recunoscute de prezenta lege, 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, fără parcurgerea procedurii prealabile prevăzute de art. 7 din Legea contenciosului administrativ nr. 554/2004, cu modificările și completările ulterioare. Deciziile cu caracter individual pot fi atacate în termen de 30 de zile de la comunicare.

DISPOZIȚII TRANZITORII

Art. 44. - Înscrierea în Registrul prevăzut de art.8, în primii 2 ani de la data intrării în vigoare a prezentei legi, se face prin depunerea unei declarații pe propria răspundere însoțită de o documentație de autoevaluare a îndeplinirii cerințelor minime de securitate și notificare.

DISPOZIȚII FINALE

Art. 45. - Până la 9 august 2018 și, ulterior, în fiecare an, CERT-RO în calitate de punct unic de contact transmite grupului de cooperare un raport de sinteză privind notificările primite, care include numărul de notificări și natura incidentelor notificate, precum și acțiunile întreprinse în conformitate cu art. l0 alin. (1) lit. c) , art. 12 alin. (1) lit. c) coroborate cu art. 27 alin. (1) lit. d).

Art. 46. - (1) În scopul asigurării unui nivel ridicat de securitate a rețelelor și a sistemelor informatice, Guvernul României va adopta strategia națională privind securitatea rețelelor și a sistemelor informatice stipulată la art. 14 și care va acoperi cel puțin următoarele elemente:

(a) obiectivele și prioritățile strategiei naționale privind securitatea rețelelor și a sistemelor informatice;

(b) un cadru de guvernanță pentru realizarea obiectivelor și a priorităților strategiei naționale privind securitatea rețelelor și a sistemelor informatice, care să includă rolurile și responsabilitățile organismelor guvernamentale și ale altor actori relevanți;

(c) identificarea măsurilor referitoare la gradul de pregătire, răspuns și redresare, inclusiv cooperarea dintre sectorul public și cel privat;

(d) indicarea programelor de instruire, sensibilizare și formare legate de strategia națională privind securitatea rețelelor și a sistemelor informatice;

(e) indicarea planurilor de cercetare și dezvoltare legate de strategia națională privind securitatea rețelelor și a sistemelor informatice;

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

(g) o listă a diferiților actori implicați în punerea în aplicare a strategiei naționale privind securitatea rețelelor și a sistemelor informatice.

(2) În elaborarea strategiei, Guvernul României poate solicita asistența ENISA.

(3) În termen de 3 luni de la adoptare, Guvernul României transmite Comisiei comunică Comisiei strategia adoptată în temeiul alin (1).

(4) Comunicarea de la alin (3) nu va conține elementele care au legătură cu securitatea națională.

Art. 47. - CERT-RO identifică și stabilește documentele și detaliile tehnice necesare pentru evaluarea inițială a securității infrastructurilor care urmează să se declare operator de servicii esențiale.

Art. 48. - Cerințele de securitate și notificare prevăzute de Capitolul IV nu se aplică:

a) furnizorilor de rețele publice de comunicaţii electronice şi furnizorilor de servicii de comunicaţii electronice destinate publicului, care beneficiază de drepturi speciale sau exclusive pentru prestarea serviciilor în alte sectoare ale economiei, în România sau într-un alt stat membru al Uniunii Europene.

b) prestatorilor de servicii de încredere calificați și necalificați care fac obiectul art. 19 din Regulamentul (UE) nr. 910/2014.

Art. 49. - (1) Până la 9 noiembrie 2018, pentru fiecare sector și subsector menționat în Anexa, CERT-RO identifică operatorii de servicii esențiale care au sediul social, filială, sucursală, punct de lucru sau altă formă de reprezentare legal stabilită pe teritoriul României.

(2) Până la 9 mai 2018 Guvernul României notifică Comisiei Europene regimul sancționator aplicabil în temeiul prezentei legi precum și orice modificare ulterioară a acestuia.

(3) În termenul prevăzut la alin. (1) și ulterior la fiecare doi ani, CERT-RO transmite Comisiei Europene următoarele informații în vederea evaluării aplicării prezentei legi:

(a) lista măsurilor care permit identificarea operatorilor de servicii esențiale;

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

(c) numărul operatorilor de servicii esențiale identificați pentru fiecare sector menționat în Anexa și o indicație a importanței lor în legătură cu sectorul respectiv;

(d) limite, atunci când acestea există, pentru determinarea nivelului relevant de furnizare, în raport cu numărul de utilizatori care se bazează pe serviciul respectiv sau cu importanța operatorului de servicii esențiale.

Art. 50. - Prezenta lege nu aduce atingere :

a)OUG 98/2011 privind identificarea, desemnarea și protecția infrastructurilor critice, cu modificările și completările ulterioare,

b)Legilor de transpunere a Directivei 2011/93/UE privind combaterea abuzului sexual asupra copiilor, a exploatării sexuale a copiilor și a pornografiei infantile și de înlocuire a Deciziei-cadru 2004/68/JAI a Consiliului, respectiv :

1. Ordonanța de urgență nr. 18/2016 pentru modificarea și completarea Legii nr. 286/2009 privind Codul penal, Legii nr. 135/2010 privind Codul de procedură penală, precum și pentru completarea art. 31 alin. (1) din Legea nr. 304/2004 privind organizarea judiciară

2. Legea nr. 304/2004 privind organizarea judiciară, republicată, cu modificările și completările ulterioare.

3. Legea nr. 287/2009 privind Codul civil – republicată

4. Legea nr. 63/2012 pentru modificarea și completarea Codului penal al României și a Legii nr. 286/2009 privind Codul penal

5. Hotărâre pentru aprobarea Metodologiei-cadru privind prevenirea și intervenția în echipă multidisciplinară și în rețea în situațiile de violență asupra copilului și de violență în familie și a Metodologiei de intervenție multidisciplinară și

interinstituţională privind copiii exploataţi şi aflaţi în situaţii de risc de exploatare prin muncă, copiii victime ale traficului de persoane, precum şi copiii români migranţi victime ale altor forme de violenţă pe teritoriul altor state

6. Lege pentru modificarea şi completarea Legii nr. 678/2001 privind prevenirea şi combaterea traficului de persoane

7. Lege privind unele măsuri pentru asigurarea protecţiei victimelor infracţiunilor

8. Lege pentru modificarea şi completarea Legii nr. 302/2004 privind cooperarea judiciară internaţională în materie penală

9. Lege pentru punerea în aplicare a Legii nr. 135/2010 privind Codul de procedură penală şi pentru modificarea şi completarea unor acte normative care cuprind dispoziţii procesual penale

10. Lege privind executarea pedepselor şi a măsurilor privative de libertate dispuse de organele judiciare în cursul procesului penal

11. Lege privind organizarea şi funcţionarea sistemului de probaţiune

12. Lege privind ratificarea Convenţiei Consiliului Europei pentru protecţia copiilor împotriva exploatării sexuale şi a abuzurilor sexuale, adoptată la Lanzarote la 25 octombrie 2007 şi semnată de România la Lanzarote la 25 octombrie 2007

13. Lege pentru punerea în aplicare a Legii nr. 286/2009 privind Codul penal

14. Lege privind prevenirea şi combaterea traficului de personae

15. Legea nr. 365/2002 privind comerţul electronic – republicată, cu modificările și completările ulterioare

16. Legea nr. 217/2003 pentru prevenirea şi combaterea violenţei în familie – republicată

17. Legea nr. 272/2004 privind protecţia şi promovarea drepturilor copilului – republicată,cu modificările și completările ulterioare

18. Legea nr. 196/2003 privind prevenirea şi combaterea pornografiei - republicată

c)Legilor de transpunere a Directivei 2013/40/UE privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului:

1. Ordin nr.4520/C/2014 pentru modificarea şi completarea Regulamentului de organizare şi funcţionare a Direcţiei de Investigare a Infracţiunilor de Criminalitate

Organizată şi Terorism, aprobat prin Ordinul ministrului justiţiei şi libertăţilor cetăţeneşti nr. 1.226/C/2009

2. Ordin nr.4682/C/2016 pentru aprobarea Regulamentului de organizare şi funcţionare a Direcţiei de Investigare a Infracţiunilor de Criminalitate Organizată şi Terorism

3. Lege nr.218/2002 privind organizarea şi funcţionarea Poliţiei Române, republicată, cu modificările și completările ulterioare

4. Lege nr.255/2013 pentru punerea în aplicare a Legii nr.135/2010 privind Codul de procedură penală şi pentru modificarea şi completarea unor acte normative care cuprind dispoziţii procesual penale, cu modificările și completările ulterioare

5. Lege nr.39/2003 privind prevenirea şi combaterea criminalităţii organizate, cu modificările și completările ulterioare

6. Lege nr.135/2010 privind Codul de procedură penală, cu modificările și completările ulterioare

7. Lege nr.64/2004 pentru ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23 noiembrie 2001

8. Lege nr.187/2012 pentru punerea în aplicare a Legii nr.286/2009 privind Codul penal, cu modificările și completările ulterioare

9. Lege nr.286/2009 privind Codul penal, cu modificările și completările ulterioare

10. Lege nr.161/2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei, cu modificările și completările ulterioare

d)Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, cu modificările și completările ulterioare precum și celor ale Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, cu modificările și completările ulterioare.

e) Legea nr. 182/2002 privind protecția informațiilor clasificate, cu modificările și completările ulterioare, precum și a actelor normative subsecvente.

Art. 51. - Prezenta lege intră în vigoare începând cu data de 9 mai 2018, cu excepția prevederilor art. 52, care intră în vigoare la 3 zile de la publicare.

Art. 52. - În termenul prevăzut la art. 51, MCSI la propunerea CERT-RO supune aprobării Guvernului anexa cu valori de prag pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale prevăzută la art. 6 alin. (3);

Art. 53. - (1) În termenul prevăzut la art. 51, se aprobă prin decizie a directorului CERT-RO normele tehnice prevăzute la art. 20 lit. b), c) și f) și se publică în Monitorul Oficial.

(2) Normele tehnice prevăzute la art. 20 lit. b), c) și f) se actualizează ori de câte ori este necesar, conform evoluției amenințărilor la adresa securității rețelelor și sistemelor informatice și au caracter obligatoriu pentru operatorii de servicii esențiale și furnizorii de servicii digitale.

Art. 54. - (1) MCSI va notifica Comisia în termen de 30 zile de la publicarea în Monitorul Oficial a prezentei legi cu privire la desemnarea autorității competente, a punctului unic de contact și atribuțiilor acestora.

(2) MCSI va notifica Comisia în termen de 30 zile de la publicarea în Monitorul Oficial orice modificare a actelor prevăzute la alin. (1).

(3) MCSI va notifica Comisia în termen de 30 zile de la publicarea în Monitorul Oficial a prezentei legi cu privire la misiunea, precum și la principalele elemente ale procedurilor de administrare a incidentelor folosite de echipa CSIRT națională.

Art. 55. – Prezenta lege transpune Directiva Parlamentului European și a Consiliului nr. 1148/2016 din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, publicată în Jurnalul Oficial al Uniunii Europene nr. L194/2016.

ANEXA - SECTOARE DE ACTIVITATE ȘI TIPURI DE ENTITĂȚI

Sectorul	Subsectorul	Tipul de entitate
1. Energie	a) Electricitate	– Furnizori și producători de energie electrică, așa cum sunt definiti la art. 3 din Legea energiei electrice şi a gazelor naturale nr. 123/2012, republicată cu modificările și completările ulterioare
		–Operatori de distribuție, astfel cum sunt definiți la articolul 3 din Legea energiei electrice și a gazelor naturale nr. 123/2012, cu modificările și completările ulterioare
		–Operatori de transport și de sistem, astfel cum sunt definiți la articolul 3 din Legea nr. 123/2012, a energiei electrice şi a gazelor naturale, cu modificările și completările ulterioare
	(b) Petrol	–Operatori de conducte de transport al petrolului
		–Operatori ai instalațiilor de producție, de rafinare și de tratare a petrolului, de depozitare și de transport
	(c)Gaze naturale	–Întreprinderi de furnizare, astfel cum sunt definite la articolul 100 din Legea nr. 123/2012, a energiei electrice şi a gazelor naturale, cu modificările și completările ulterioare

		—Operatori de distribuție, astfel cum sunt definiți la articolul 100 din Legea nr. 123/2012, a energiei electrice și a gazelor naturale, cu modificările și completările ulterioare
		—Operatori de transport și de sistem, astfel cum sunt definiți la articolul 100 din Legea nr. 123/2012, a energiei electrice și a gazelor naturale, cu modificările și completările ulterioare
		—Operatori de înmagazinare, astfel cum sunt definiți la articolul 100 din Legea nr. 123/2012, a energiei electrice și a gazelor naturale, cu modificările și completările ulterioare
		—Operatori de sistem GNL, astfel cum este definit la articolul 100 din Legea nr. 123/2012, a energiei electrice și a gazelor naturale, cu modificările și completările ulterioare
		—Întreprinderi din sectorul gazelor naturale, astfel cum este definit la articolul 100 din Legea nr. 123/2012, a energiei electrice și a gazelor natural, cu modificările și completările ulterioare
		—Operatori de instalație de rafinare și de tratare a gazelor naturale
2. Transport	(a) Transport aerian	—Transportatori aerieni, astfel cum sunt

	Hotărârea nr. 455/2011 privind tarifele de aeroport – Art.4	– Organe de administrare a aeroportului, astfel cum sunt definite la articolul 4 din Hotărârea nr. 455/2011 privind tarifele de aeroport, aeroporturi astfel cum sunt definite la art. 2 pct. 1 al Directivei 2009/12/CE, inclusiv aeroporturile principale enumerate în secțiunea 2 din anexa II la Regulamentul (UE) nr. 1315/2013 al Parlamentului European și al Consiliului, precum și entități care operează instalații auxiliare în cadrul aeroporturilor.
	Regulamentul (UE) nr. 1315/2013	– Operatori de control al gestionării traficului care prestează servicii de control al traficului aerian (ATC), astfel cum sunt definite la articolul 2 punctul 1 din Regulamentul (CE) nr. 549/2004 al Parlamentului European și al Consiliului
	(b) Transport feroviar Legea nr. 202/2016 privind integrarea sistemului feroviar din România în spaţiul feroviar unic național **Art.3**	– Administratori de infrastructuri, astfel cum sunt definiți la articolul 3 din Legea nr. 202/2016 privind integrarea sistemului feroviar din România în spaţiul feroviar unic european
		– Întreprinderi feroviare, astfel cum sunt definite la articolul 3 din Legea nr. 202/2016 privind integrarea sistemului feroviar din România în spaţiul feroviar unic european
	I Transport pe apă	– Companii de transport de mărfuri și pasageri pe ape interioare, maritime și de coastă, astfel cum sunt definite pentru transportul maritim în anexa I la Regulamentul (CE) nr. 725/2004 al Parlamentului European și al Consiliului, fără a include navele individuale

		operate de companiile respective
	Ordinul nr. 290/2007 pentru introducerea măsurilor de întărire a securității portuare – art.3 Hotărârea nr. 1016/2010 pentru stabilirea Sistemului de informare şi monitorizare a traficului navelor maritime care intră/ies în/din apele naţionale navigabile ale României – art 3	—Organe de gestionare a porturilor, astfel cum sunt definite la articolul 3 din Ordinul nr. 290/2007 pentru introducerea măsurilor de întărire a securității portuare, inclusiv instalațiile portuare ale acestora, astfel cum sunt definite la articolul 2 punctul 11 din Regulamentul (CE) nr. 725/2004 și entitățile care operează lucrări și echipamente în cadrul porturilor
		—Operatori de servicii de trafic naval, astfel cum sunt definiti la articolul 3 din Hotărârea nr. 1016/2010 pentru stabilirea Sistemului de informare şi monitorizare a traficului navelor maritime care intră/ies în/din apele naţionale navigabile ale României, cu modificările și completările ulterioare
	(d) Transport rutier Ordonanţa nr. 7/2012 privind implementarea sistemelor de transport inteligente în domeniul transportului rutier şi pentru realizarea interfeţelor cu alte moduri de transport- art.4	—Autorități rutiere, astfel cum sunt definite la articolul 2 punctul 12 din Regulamentul ational (UE) 2015/962 al Comisiei responsabile pentru controlul gestionării traficului
		—Operatori de sisteme de transport inteligente, astfel cum sunt definiti la articolul 4 din Ordonanţa nr. 7/2012 privind implementarea sistemelor de transport inteligente în domeniul transportului rutier şi pentru realizarea interfeţelor cu alte moduri de transport
3 Sectorul		Instituții de credit, astfel cum sunt definite la articolul 4 punctul 1 din Regulamentul (UE)

. bancar		nr. 575/2013 al Parlamentului European și al Consiliului
4 . Infrastructuri ale pieței financiare	Nu exista notificare privind transpunerea	– Operatori de locuri de tranzacționare, astfel cum sunt definite la articolul 4 punctul 24 din Directiva 2014/65/UE a Parlamentului European și a Consiliului_
		– Contrapartide centrale, astfel cum sunt definite la articolul 2 punctul 1 din Regulamentul (UE) nr. 648/2012 al Parlamentului European și al Consiliului
5 . Sectorul sănătății	Instituții de asistență medicală (inclusiv spitale și clinici private)	Furnizori de servicii medicale, astfel cum sunt definiți la articolul 3 litera (g) din Directiva 2011/24/UE a Parlamentului European și a Consiliului
6 . Furnizarea și distribuirea de apă potabilă Legea nr. 458/2002 privind calitatea apei potabile- art. 2		Furnizori și distribuitori de „apă destinată consumului uman”, astfel cum sunt definiti la articolul 2 alin. (1) din Legea nr. 458/2002 privind calitatea apei potabile, co modificările și completările ulterioare, excluzând distribuitorii pentru care distribuția de apă destinată consumului uman reprezintă doar o parte din activitatea lor generală de distribuire a altor produse de bază și produs care nu sunt considerate servicii esențiale.
7 . Infrastructură digitală		– IXP
		– DNS
		– TLD