ORDONANȚĂ DE URGENȚĂ
privind înființarea Directoratului Național de Securitate Cibernetică și pentru modificarea și completarea unor acte normative

Provocările, riscurile și amenințările de securitate din spațiul cibernetic s-au intensificat în ultimii ani, iar securitatea cibernetică a devenit o necesitate ce implică abordări integrate, cuprinzătoare, adoptarea de strategii de securitate cibernetică, noi și permanente, investiții financiare semnificative și adaptări organizaționale rapide și ambițioase,

având în vedere faptul că amenințările cibernetice nu au o adresă clară (națională) a unui expeditor, nu sunt blocate la granițele statale, au un profund caracter asimetric, întrucât, cu resurse relativ limitate, un individ sau un grup de indivizi, afiliați sau nu cu structuri guvernamentale, pot genera incidente cu efecte perturbatoare semnificative cu impact destabilizator la nivel statal sau al unui sector economic,

ținând cont de faptul că atât statele membre ale Uniunii Europene, cât și multe alte state, inclusiv NATO în anul 2016, au recunoscut spațiul cibernetic ca fiind un spațiu de confruntare și domeniu operațional, alături de domeniile terestru, aerian, cosmic și maritim,

considerând că pentru asigurarea unui nivel ridicat de securitate a rețelelor și sistemelor informatice care stau la baza furnizării serviciilor esențiale la nivelul României ca stat membru al UE, implementarea Directivei (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune este vitală pentru activitățile economice și societale și, în special, pentru funcționarea pieței interne,

urmare a evaluării de către Comisia Europeană a activității de implementare a Directivei (UE) 2016/1148 la nivelul României unde au fost constatate întârzieri și neconformități în abordarea națională,

motivat de faptul că în primul rând transformarea digitală expune statul, societatea, economia și cetățenii unor amenințări și atacuri cibernetice asimetrice caracterizate prin costuri scăzute și prin faptul că atacatorul deține inițial avantaje,

motivat de necesitatea dezvoltării capabilităților de răspuns care trebuie să evolueze în același timp cu atacurile cibernetice, atât prin prevenție, cât și prin reacție și intervenție specializată, de înaltă pregătire și adaptată noilor tipuri de atacuri cibernetice,

motivat de necesitatea creșterii rezilienței cibernetice,

având ca obiectiv gestionarea amenințărilor cibernetice, în măsura în care riscurile asociate sunt foarte reale și semnificative, pentru prevenirea nesiguranței, a pierderilor economice sau a impactului asupra activităților,

mai mult, pentru o prezență mai activă a României pe harta mondială a statelor cu capacități de reacție și intervenție ridicate și, nu în ultimul rând, pentru ca Romania să devina un pol / nod de influență cibernetică regional/global și implicit consolidarea imaginii internaționale a țării,

țintind ca noua instituție să devină o instituție de anvergură internațională care să poziționeze ferm România ca un lider recunoscut în securitatea cibernetică,

apreciind că cele de mai sus constituie premisele unei situații de urgență și extraordinare a căror reglementare nu poate fi amânată,

În temeiul art. 115 alin. (4) din Constituția României, republicată,

Guvernul României adoptă prezenta ordonanță de urgență,

Art. 1 Concepte, definiții și termeni

În înțelesul prezentei ordonanțe de urgență, termenii și expresiile de mai jos au următoarea semnificație:

a) **CSIRT** – echipă de răspuns la incidente de securitate cibernetică – entitate organizațională specializată care dispune de capacitatea necesară pentru prevenirea, analiza, identificarea și reacția la incidentele cibernetice;

b) **comunitatea CSIRT din România** – ansamblul echipelor CSIRT care funcționează în cadrul autorităților și instituțiilor publice ori al altor persoane juridice de drept public sau privat din România și care relaționează cu Directoratul Național de Securitate Cibernetică pe baza unor proceduri și protocoale de cooperare;

c) **spațiul cibernetic național civil** – spațiul cibernetic național care exclude infrastructurile cibernetice aflate, conform prevederilor legale, în administrarea sau responsabilitatea instituțiilor din sistemul național de apărare, ordine publică și securitate națională, precum și cele care vehiculează informații clasificate;

d) **securitate cibernetică** – stare de normalitate, astfel cum este definită în Strategia de securitate cibernetică a României și Planul de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică, aprobat prin Hotărârea Guvernului nr. 271/2013;

e) **amenințare cibernetică** – orice circumstanță, eveniment sau acțiune potențială care ar putea cauza daune sau perturbări la nivelul rețelelor și al sistemelor informatice, precum și la nivelul utilizatorilor unor astfel de sisteme și al altor persoane, sau care poate avea un alt fel de impact negativ asupra acestora.

f) **serviciile publice de tip preventiv** – sunt acele servicii oferite de Directoratul Național de Securitate Cibernetică care constau în:

   1. anunțuri privind evenimente în domeniu;
   2. anunțuri privind amenințări nou-identificate pe plan național și internațional;
   3. cercetare și informare privind noutățile tehnologice în domeniu;
   4. realizarea, la cerere, de auditări și evaluări de securitate sau teste de penetrare;
   5. identificarea vulnerabilităților și punerea la dispoziție de situații actualizate privind încercările de intruziune și servicii de localizare a surselor atacurilor, pe baza informațiilor transmise de furnizorii de rețele și servicii de comunicații electronice;
   6. diseminarea informațiilor de securitate cibernetică.

g) **serviciile publice de tip reactiv** – sunt acele servicii oferite de Directoratul Național de Securitate Cibernetică care constau în:

   1. alerte și atenționări privind apariția unor activități premergătoare atacurilor;
   2. gestiunea incidentelor la nivel național, în cooperare cu celelalte echipe CSIRT;
   3. diseminarea rezultatelor investigațiilor incidentelor de securitate cibernetică, cu respectarea prevederilor acordurilor de cooperare încheiate cu partenerii Directoratului Național de Securitate Cibernetică.

h) **serviciile publice de consultanță pentru managementul serviciilor de securitate cibernetică** – sunt acele servicii oferite de Directoratul Național de Securitate Cibernetică care constau în:

   1. analize de risc aplicate la nivel local și la nivel național privind infrastructurile cibernetice de interes național;
   2. planificarea asigurării funcționării continue și a recuperării în caz de dezastre;
   3. atestarea managementului securității cibernetice și a incidentelor cibernetice;

4. autorizarea echipelor de tip CSIRT și atestarea auditorilor de securitate informatică specifice domeniului securității rețelelor și sistemelor informatice.

i) **sistem de alertă timpurie și informare în timp real privind incidentele cibernetice** – ansamblul de proceduri și sisteme tehnice care au rolul de a identifica premisele de apariție a incidentelor cibernetice și de a avertiza în cazul producerii acestora. Sistemul include și conexiuni de date ce vor transporta informații referitoare la incidentele cibernetice identificate de senzori dedicați, precum și informații statistice referitoare la valorile de trafic înregistrate în nodurile de rețea ale infrastructurilor cibernetice ce asigură funcționalități de utilitate publică ori asigură servicii ale societății informaționale;

j) **criza cibernetică** – o stare de fapt care reprezintă o amenințare reală sau o deteriorare a unei infrastructuri cibernetice, de natură să creeze daune rețelelor și sistemelor informatice care furnizează servicii esențiale, digitale sau de interes național;

k) **produs de securitate cibernetică** - un element sau un grup de elemente care asigură securitatea unei rețele sau a unui sistem informatic;

l) **serviciu de securitate cibernetică** - un serviciu care asigura confidențialitatea, integritatea, disponibilitatea, autenticitatea, non-repudierea unei rețele sau a unui sistem informatic.

Art. 2 Înființarea Directoratului

(1) Se înființează Directoratul Național de Securitate Cibernetică, denumit în continuare DNSC, instituție publică, cu personalitate juridică, în coordonarea Prim-ministrului, finanțată din venituri proprii și subvenții acordate de la bugetul de stat.

(2) Centrul Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO se desființează la momentul intrării in vigoare a prezentei ordonanțe de urgență.

(3) DNSC preia activitățile, atribuțiile și personalul Centrului Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO, cu menținerea drepturilor salariale avute la data preluării.

(4) DNSC are sediul central în municipiul București, strada Italiană, nr. 22, sector 2.

(5) DNSC are calitatea de membru permanent, din Consiliul Operativ de Securitate Cibernetică, denumit în continuare COSC.

(6) DNSC are responsabilități privind securitatea cibernetică a spațiului cibernetic național civil.

(7) DNSC are în structura internă compartimente funcționale precum și alte structuri în subordinea sa, cu sau fără personalitate juridică.

Art. 3 Responsabilități și principii

(1) Principala responsabilitate a DNSC este asigurarea securității cibernetice a spațiului cibernetic național civil, în colaborare cu instituțiile și autoritățile competente.

(2) DNSC este autoritatea competentă la nivel național pentru spațiul cibernetic național civil, inclusiv pentru securitatea rețelelor și sistemelor informatice care asigură furnizarea de servicii esențiale ori furnizează servicii digitale, identificate în temeiul Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cu modificările și completările ulterioare, precum și pentru gestionarea riscurilor și a incidentelor cibernetice.

(3) În exercitarea calității de autoritate competentă la nivel național, DNSC se consultă și cooperează cu:

a) Serviciul Român de Informații – privind securitatea rețelelor și a sistemelor informatice care asigură servicii esențiale, precum și a produselor și serviciilor informatice utilizate în cadrul sectorului guvernamental, a căror afectare aduce atingere securității naționale.

b) Ministerul Apărării Naționale – privind securitatea rețelelor și a sistemelor informatice care asigură servicii esențiale în sprijinul activităților privind apărarea țării.

c) Ministerul Afacerilor Interne, Serviciul de Informații Externe, Serviciul de Telecomunicații Speciale și Serviciul de Protecție și Pază – privind securitatea rețelelor și a sistemelor informatice care asigură servicii esențiale în domeniul lor de activitate și responsabilitate.

d) Administrația Prezidențială - privind securitatea rețelelor și serviciilor de comunicații și tehnologia informației din domeniul propriu de activitate și responsabilitate, precum și pentru cele destinate Consiliului Suprem de Apărare a Țării, denumit în continuare CSAT, administrate conform hotărârilor adoptate de acesta în condițiile legii.

(4) Pentru îndeplinirea responsabilităților sale, DNSC se consultă și cooperează, după caz, cu:

a) instituțiile publice prevăzute la alin. (3).

b) Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, în cazul incidentelor care au ca rezultat încălcarea securității datelor cu caracter personal, în condițiile legii.

c) Autoritatea Națională pentru Administrare și Reglementare în Comunicații, atunci când incidentele au ca rezultat afectarea securității ori funcționării rețelelor publice de comunicații electronice ori când pentru administrarea unui incident sunt necesare măsuri ce intră în aria de activitate și responsabilitate a acesteia.

d) Oficiul Registrului National al Informațiilor Secrete de Stat, în cazul incidentelor și atacurilor cibernetice asupra sistemelor informatice și de comunicații care vehiculează informații clasificate.

e) Ministerul Afacerilor Externe, în cazul unor incidente și atacuri cibernetice care afectează interese pe plan extern ale României.

f) organele de urmărire penală, în condițiile legii.

(5) În vederea atingerii obiectivelor și funcțiilor, DNSC aplică următoarele principii:

a) **principiul legalității** – atât DNSC, cât și personalul instituției acționează cu respectarea prevederilor legale în vigoare și a tratatelor și a convențiilor internaționale la care România este parte.

b) **principiul egalității** – beneficiarii activităților desfășurate de către DNSC vor fi tratați în mod egal, într-o manieră nediscriminatorie, corelativ cu obligația DNSC de autoritate națională, de a trata în mod egal pe toți beneficiarii, fără discriminare, pe criteriile prevăzute de legislația în domeniul de competență.

c) **principiul transparenței** – în procesul elaborării de propuneri de acte normative, DNSC va informa și va supune consultării și dezbaterii publice proiectele de acte normative și va permite accesul persoanelor juridice și fizice la datele și informațiile de interes public, în condițiile Legii nr. 544/2001 privind liberul acces la informațiile de interes public. În același timp, beneficiarii DNSC au dreptul de a obține informații de la instituție, iar instituția are obligația de a pune la dispoziția beneficiarilor informații din oficiu sau la cerere, în limitele legii.

d) **principiul proporționalității** – formele de activitate ale DNSC trebuie să fie corespunzătoare cu legislația națională și să satisfacă interesul public, precum și echilibrate din punctul de vedere al efectelor asupra persoanelor fizice și juridice.

e) **principiul imparțialității** – personalul DNSC își exercită atribuțiile legale fără subiectivism, indiferent de propriile convingeri sau interese.

f) **principiul continuității** – activitatea DNSC se exercită fără întreruperi, cu respectarea prevederilor legale.

g) **principiul neutralității tehnologice** – în activitatea specifică de reglementare, testare și evaluare, DNSC nu favorizează o anumită marcă sau tehnologie și nu impune sau discriminează în favoarea utilizării unui anumit tip de tehnologie.

h) **principiul solidarității internaționale** – în relațiile cu partenerii din Uniunea Europeană și celelalte state sau organizații, DNSC promovează cooperarea între state în vederea rezolvării cât mai eficiente a provocărilor globale în domeniul securității cibernetice.

i) **principiului sincronizării** – măsurile și cerințele de securitate impuse de DNSC vor ține cont de evoluția fenomenului securității cibernetice la nivelul Uniunii Europene.

j) **principiul satisfacerii interesului public** – DNSC, precum și personalul instituției urmăresc satisfacerea interesului public înaintea celui individual sau de grup. Interesul public național este prioritar față de interesul public local.

k) **principiul conștientizării** – în activitatea sa de informare a persoanelor fizice și juridice, precum și a cetățenilor, DNSC prezintă noi cunoștințe și informații cu privire la vulnerabilitățile, riscurile și atacurile cibernetice, pe înțelesul tuturor, folosind diverse metode de atragere a interesului grupurilor țintă.

(6) În îndeplinirea atribuțiilor sale, DNSC urmărește atingerea obiectivelor luând în acest sens măsuri rezonabile, cu respectarea principiilor prevăzute la alin. (5).

(7) Responsabilitățile DNSC nu aduc atingere legislației în vigoare referitoare la sistemul național de apărare, ordine publică și securitate națională, la infrastructurile critice naționale și la informațiile clasificate.

Art. 4 Obiective

Principalele obiective ale DNSC sunt:

a) asigurarea securității, confidențialității, integrității, disponibilității, rezilienței elementelor din spațiul cibernetic național civil, în cooperare cu instituțiile care au competențe și atribuții în domeniu.

b) asigurarea cadrului de strategii, politici și reglementări care să susțină implementarea viziunii naționale în domeniul securității cibernetice.

c) crearea cadrului național de cooperare între instituții din domeniul public, privat, de educație și cercetare, pentru asigurarea unei viziuni și abordări realiste, comune și coerente privitor la securitatea cibernetică a României.

d) crearea și operarea unei platforme naționale de colaborare care să permită schimbul de informații între constituenți, instituții ale statului, mediul academic și mediul privat în domeniul incidentelor, vulnerabilităților și crizelor de natură cibernetică.

e) crearea cadrului național de certificare în domeniul securității cibernetice, în cooperare cu instituțiile care au competențe și atribuții în domeniu.

f) crearea cadrului național de instruire în domeniul securității cibernetice, în cooperare cu instituțiile care au competențe și atribuții în domeniu.

g) promovarea și susținerea pe plan internațional a strategiei naționale în domeniul securității cibernetice.

h) crearea cadrului național destinat evaluării noilor tehnologii și impactului acestora asupra securității cibernetice a României.

i) dezvoltarea capacității de atragere de fonduri de finanțare pentru realizarea obiectivelor instituționale.

j) elaborarea și coordonarea planului de management al crizelor de securitate cibernetică la nivel național, în cooperare cu instituțiile care au competențe și atribuții în domeniul managementului crizelor și sub autoritatea COSC.

Art. 5 Funcții și atribuții

În îndeplinirea obiectivelor, DNSC exercită următoarele funcții și atribuții:

a) **Strategie și planificare**

1. Realizează politica Guvernului în domeniul securității cibernetice și stabilește la nivel național strategiile și politicile publice în domeniul securității cibernetice.
2. Asigură elaborarea și diseminarea politicilor publice de prevenire și contracarare a incidentelor din cadrul infrastructurilor cibernetice din spațiul cibernetic civil național.
3. Participă la elaborarea strategiei naționale de securitate cibernetică în cooperare cu instituțiile din Sistemul Național de Apărare, Ordine Publică și Securitate Națională, denumit în continuare SNAOPSN, cu competențe în domeniu, și coordonează implementarea acesteia, asigurând inclusiv monitorizarea acțiunilor întreprinse, a măsurilor implementate și evaluarea rezultatelor obținute.
4. Elaborează și coordonează aplicarea planului de management al crizelor de securitate cibernetică la nivel național pe timp de pace, în cooperare cu instituțiile care au competențe și atribuții în domeniul managementului crizelor.
5. Elaborează și coordonează implementarea strategiei naționale de instruire în domeniul securității cibernetice, în cooperare cu instituțiile care au competențe și atribuții în domeniu.
6. Elaborează și coordonează implementarea strategiei naționale de cooperare între instituții din domeniul public, privat, de educație și cercetare, pentru asigurarea unei viziuni și abordări realiste, comune și coerente privitor la securitatea cibernetică a României, inclusiv din perspectiva pregătirii și menținerii resursei umane în România.
7. Elaborează propuneri privind modificarea cadrului legislativ în domeniul securității cibernetice, pe care le înaintează către Guvernul României.
8. Asigură sprijin autorităților publice în elaborarea și implementarea strategiilor naționale sectoriale, care includ componente de securitate cibernetică.
9. Sprijină participarea instituțiilor statului român și a altor părți interesate în proiecte naționale și internaționale din domeniul securității cibernetice, în vederea îndeplinirii obiectivelor strategiei naționale de securitate cibernetică.

b) **Funcția de autoritate competentă la nivel național de reglementare, supraveghere și control** – asigură reglementarea și gestionarea securității cibernetice a României și a spațiului cibernetic național civil, astfel:

1. Monitorizează implementarea strategiei și politicilor naționale și sectoriale în domeniul securității cibernetice.
2. Elaborează cadrul normativ și instituțional în domeniul securității cibernetice, inițiază și respectiv avizează proiecte de acte normative în domeniul său de competență, pe care le supune spre aprobare, în condițiile legii.
3. Exercită atribuțiile stabilite prin Legea nr. 362/2018.
4. Elaborează regulamente, norme, cerințe, ghiduri și recomandări, în domeniul de competență, care se aprobă prin decizia directorului DNSC și se publică, după caz, în Monitorul Oficial al României sau pe site-ul instituției.
5. Îndeplinește atribuțiile de autoritate națională pentru furnizorii de servicii de găzduire/hosting.
6. Stabilește standardele și reglementările în domeniul securității cibernetice la nivel național, cu excepția celor prevăzute la art. 20 alin. (1), care devin obligatorii odată cu publicarea în Monitorul Oficial al României, Partea I, și verifică implementarea acestora prin acțiuni de control.
7. Gestionează și administrează evidențe privind persoanele fizice și juridice care intră sub incidența actelor normative care reglementează domeniul securității cibernetice, conform atribuțiilor instituției.

c) **Funcția de CSIRT național**

1. Asigură coordonarea activităților la nivel național de detecție, protecție și răspuns la atacuri cibernetice, precum și desfășurarea de activități de supraveghere, monitorizare, identificare, analiză, investigare și de răspuns la incidente de securitate cibernetică, prin echipa CSIRT națională, pentru infrastructurile cibernetice aflate în domeniul de competență, așa cum vor fi definite prin regulamentul de organizare și funcționare al DNSC.
2. Exercită și atribuțiile de CSIRT național stabilite prin Legea nr. 362/2018.
3. Coordonează răspunsul la incidente de securitate cibernetice la nivel național pentru domeniul său de competență.
4. Monitorizează, identifică, analizează și răspunde la amenințările de securitate cibernetică din spațiul cibernetic național civil.
5. Derulează activități de investigare a incidentelor cibernetice care vizează sau utilizează spațiul cibernetic național civil, în conformitate cu competențele legale, utilizând după caz metode tehnice care presupun inclusiv analiza metadatelor corespunzătoare conexiunilor de rețea puse la dispoziția DNSC de către posesorii acestora.
6. Evaluează riscurile de securitate cibernetică la nivel național și emite avertizări, buletine de informare și de prognoză.
7. Derulează activități de identificare și analiză a amenințărilor, inclusiv în cooperare cu mediul public, privat și academic, în scopul implementării unui nivel ridicat de securitate cibernetică.
8. Derulează activități tehnice specifice de identificare a vulnerabilităților site-urilor cu conținut în limba română și emite avertizări de securitate.
9. Dezvoltă sisteme și instrumente de identificare, analiză și prognoză privind incidentele cibernetice, în baza cărora stabilește impactul la nivel național și transfrontalier al incidentelor și informează autoritățile relevante la nivel național, precum și autoritățile similare din alte state potențial afectate. În acest sens, DNSC cooperează cu instituțiile din sistemul național de apărare, ordine publică și securitate națională, precum și cu mediul privat și mediul academic.
10. Asigură colectarea, în condițiile legii, analiza și schimbul de informații privind riscurile și vulnerabilitățile de securitate ale rețelelor și sistemelor informatice, precum și ale produselor și serviciilor de securitate cibernetică.
11. Oferă servicii publice de tip preventiv, de tip reactiv și de consultanță.
12. Implementează, gestionează și coordonează Platforma Națională pentru Raportarea Incidentelor de Securitate Cibernetică, denumită în continuare *PNRISC*.

d) **Funcția de CSIRT guvernamental**

1. Monitorizează implementarea măsurilor de securitate cibernetică la nivelul instituțiilor Guvernului României, în colaborare și coordonare cu instituțiile statului care au competențe și atribuții în domeniu.
2. Sprijină instituțiile statului care au competențe și atribuții în domeniu în exercitarea atribuțiilor legate de securitatea cibernetică.

e) **Funcția de coordonare, implementare, îndrumare și sprijin a CSIRT-urilor sectoriale**

1. Asigură sau participă la asigurarea funcției de CSIRT sectorial pentru toate sectoarele specificate de Legea nr. 362/2018, în colaborare și coordonare cu instituțiile statului care au competențe și atribuții în domeniu și cu autoritățile de reglementare din sectoarele implicate.
2. În cooperare cu instituțiile care coordonează și/sau reglementează domenii de activitate ce pot fi afectate de incidente de securitate cibernetică, dezvoltă echipe CSIRT sectoriale, comerciale sau participă la completarea capabilităților echipelor constituite la nivel sectorial, subsectorial ori al operatorilor economici.

f) **Funcția de echipă de răspuns la incidente de securitate cibernetică pentru produse și servicii informatice utilizate în cadrul sectorului guvernamental**

1. Asigură identificarea, evaluarea și gestionarea riscurilor asociate vulnerabilităților de securitate cibernetică din produsele, soluțiile, componentele și/sau serviciile informatice ale sectorului guvernamental.
2. Asigură infrastructura și procesele necesare pentru primirea, investigarea și raportarea, publică sau către instituțiile statului care au competențe și atribuții în domeniu, informațiilor privind vulnerabilitățile de securitate cibernetică ale produselor, soluțiilor, componentelor și/sau serviciilor informatice ale sectorului guvernamental.

g) **Funcția de alertare, prevenire, conștientizare și instruire**

1. Asigură informarea și pregătirea la nivel național a populației precum și a tuturor entităților care fac parte din spațiul cibernetic civil național, inclusiv a operatorilor economici din sectoarele stabilite în baza Legii nr. 362/2018 și din sectorul public cu privire la riscurile de securitate din spațiul cibernetic civil.
2. Promovează dezvoltarea unui comportament adecvat în spațiul cibernetic național civil pentru persoanele fizice și juridice prin conștientizarea efectelor consecințelor atacurilor cibernetice și a modalității de semnalare a acestora.
3. Emite informări privind obligațiile care derivă din calitate de administrator, furnizor sau utilizator al rețelelor și sistemelor informatice, privind atitudinea în fața unor posibile atacuri cibernetice, privind conștientizarea cetățenilor și instituțiilor publice și private, despre necesitatea semnalării/notificării atacurilor cibernetice.
4. Dezvoltă cadrul național de conștientizare a populației în cooperare cu mediul public, privat și academic în scopul asigurării unei abordări eficiente a pregătirii populației privind modalitățile de comportament, reacție și reziliență cibernetică în mediul online.
5. Desfășoară și participă la campanii/acțiuni de prevenire și conștientizare a cauzelor și consecințelor atacurilor cibernetice asupra rețelelor și sistemelor informatice civile, la nivel internațional, național și regional.

h) **Funcția de cooperare și colaborare**

1. Asigură cadrul de cooperare în vederea derulării de activități specifice asigurării securității cibernetice, cercetării, schimbului de informații, instruirii, educației, conștientizării, elaborării de proiecte, precum și a oricăror altor activități necesare pentru asigurarea securității cibernetice a României, conform competențelor legale.
2. Asigură reprezentarea României în formatele de cooperare internațională pe domeniile de competență, în cooperare cu alte autorități competente ale statului, în interesul asigurării cooperării inter-instituționale, informării reciproce și susținerii unei poziții unitare la nivel internațional.
3. Sprijină efortul național și inițiativele de cooperare în cadrul organizațiilor internaționale din care România face parte – în special în cadrul Uniunii Europene (UE), al Organizației Națiunilor Unite (ONU), a Organizației pentru Securitate și Cooperare în Europa (OSCE) și a Organizației Tratatului Atlanticului de Nord (NATO).
4. În colaborare cu alte autorități competente, universități, centre de cercetare și operatori economici participă la dezvoltare de soluții tehnologice de securitate cibernetică de interes, care pot avea o dublă utilizare civilă și militară.
5. Înființează, coordonează și gestionează Platforma Națională de Cooperare în Domeniul Securității Cibernetice, denumită în continuare *PNCDSC*, între instituțiile de stat, mediul privat, mediul academic și organizații non-guvernamentale, în scopul asigurării unui cadru național unitar de expertiză, cercetare, informare și orice alte acțiuni conexe domeniului de competență.
6. Participă în grupuri de cooperare, de lucru sau de specialitate și în rețele de cooperare, forumuri și organizații din domeniul securității cibernetice constituite la nivel național, european și internațional.

7. Dezvoltă relații de parteneriat cu alte structuri naționale sau internaționale cu competențe și responsabilități în domeniul securității cibernetice, în acest sens încheind memorandumuri și protocoale de cooperare cu persoane de drept public sau privat, naționale sau străine.
8. Cooperează cu instituțiile din SNAOPSN, precum și din COSC în vederea asigurării securității cibernetice la nivelul României.
9. Sprijină participarea instituțiilor statului român și a altor părți interesate în proiecte naționale și internaționale din domeniul securității cibernetice.

i) **Funcția de autoritate națională de certificare privind securitatea cibernetică** – are calitatea de organism național și asigură mecanismele naționale privind evaluarea, certificarea și acreditarea produselor, serviciilor și proceselor în domeniul securității cibernetice.

1. DNSC este autoritate națională de certificare în domeniul securității cibernetice pentru spațiul cibernetic civil. În această calitate, certifică din punct de vedere al securității cibernetice atât produse și servicii de securitate cibernetică, cât și produse și servicii de tehnologia informației și comunicațiilor.
2. Înființează și gestionează Registrul Național al Activelor, Produselor și Serviciilor De Securitate Cibernetică, denumit în continuare RNAPSSC.
3. Autorizează laboratoarele civile de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor care sunt utilizate în cadrul rețelelor și sistemelor informatice.
4. Cooperează cu instituțiile naționale și internaționale în domeniul standardizării și acreditarii produselor, serviciilor și proceselor în domeniul securității cibernetice.

j) **Funcția de asigurare a conformității și abordării unitare a securității cibernetice în cadrul infrastructurilor cibernetice** – avizează din punct de vedere al conformității proiecte care implică sisteme și rețele informatice, altele decât cele ce urmează a fi implementate în infrastructurile instituțiilor din SNAOPSN, cu cerințele și normele tehnice din domeniul securității cibernetice impuse la nivel național și internațional.

k) **Funcția de reprezentare** – asigură, în numele României, reprezentarea în organismele și organizațiile naționale, regionale, europene și internaționale, ca autoritate națională pentru domeniul său de activitate, în conformitate cu cadrul normativ în vigoare.

l) **Funcția de cercetare-dezvoltare**

1. Consolidează, sprijină și promovează potențialul național de cercetare, dezvoltare și inovare al activităților, proceselor și tehnologiilor de vârf de securitate cibernetică, pe baza capacităților individuale și colective ale sectorului public și privat, ale mediului academic și ale industriei.
2. Desfășoară și participă la activități de cercetare-dezvoltare în domeniul securității cibernetice și elaborează proceduri și recomandări privind securitatea cibernetică, potrivit prevederilor legale privind cercetarea științifică și dezvoltarea tehnologică.
3. Elaborează studii și cercetări privind problematica securității cibernetice a produselor, serviciilor și infrastructurilor cibernetice.
4. Elaborează și actualizează cadrul metodologic, procedural și de bune practici cu privire la activitatea de cercetare științifică în domeniul securității cibernetice, prin consultare cu instituțiile care au atribuții și competențe în domeniu.
5. Planifică și desfășoară activități de cercetare științifică în domeniile de competență, cooperând la nivel central și teritorial cu instituții din mediul public, privat și academic, precum și cu persoane fizice.
6. Dezvoltă relații pe linie de cercetare științifică cu universități, institute de cercetare, edituri, biblioteci și specialiști în domeniu din țară și din străinătate.
7. Promovează inițiativa științifică, dezvoltarea și inovarea în domenii specifice securității cibernetice, cu scopul de a sprijini și proteja interesele naționale în acest domeniu.

m) **Funcția de analiză și prognoză** – evaluează și analizează evoluțiile din domeniul securității cibernetice și emite avertizări, analize, buletine de informare și de prognoză.

n) **Funcția de identificare, evaluare, monitorizare și atenuare a riscurilor cibernetice la nivel național**.

o) **Funcția de centru național de gestionare a crizelor de natură cibernetică pe timp de pace**

1. La nivelul DNSC se constituie Centrul Național de Gestionare a Crizelor Cibernetice, denumit în continuare CNGCC, din care fac parte reprezentanți din cadrul instituțiilor și autorităților competente, cu responsabilități în domeniul securității cibernetice.
2. Împreună cu instituțiile din SNAOPSN, CNGCC asigură procesarea și analiza datelor și informațiilor referitoare la atacurile cibernetice care vizează spațiul național cu potențial impact major în sfera rețelelor și sistemelor informatice, prin produse analitice, destinate fundamentării deciziei de nivel strategic sau care să constituie suportul operațional pentru managementul crizelor cibernetice.
3. Sub autoritatea COSC, CNGCC asigură managementul crizelor cibernetice cauzate de atacuri cibernetice, în colaborare cu instituțiile statului care au competențe și atribuții în domeniul de gestionare a crizelor care afectează buna funcționare a statului.

p) **Funcția de evaluare a securității cibernetice a noilor tehnologii**

1. Evaluează din punct de vedere al securității cibernetice noile tehnologii, sisteme informatice și rețele complexe respectiv sistemele de control industrial, IoT (internet of things), tehnologii smart, cloud, tehnologii biometrice, 5G, realitatea virtuală, inteligența artificială, precum și alte noi tehnologii.
2. Identifică vulnerabilități de securitate cibernetică a produselor și serviciilor din domeniul noilor tehnologii, sisteme informatice și rețele complexe și evaluează riscurile și impactul acestora asupra securității cibernetice a României.

q) **Funcția de evaluare și certificare**

1. Avizează din punct de vedere al securității cibernetice și al conformității cu obiectivele din Strategia Națională de Securitate Cibernetică a României toate proiectele care conțin componente și soluții din domeniul tehnologiei informației și comunicațiilor pentru care se solicită garanții guvernamentale și/sau care sunt inițiate de instituțiile publice, astfel cum sunt definite de Legea nr. 500/2002 privind finanțele publice, cu modificările și completările ulterioare, precum și de companiile/societățile naționale sau societățile reglementate de Legea societăților nr. 31/1990 republicată, cu modificările și completările ulterioare, și de regii autonome care sunt înființate în baza Legii nr. 15/1990 privind reorganizarea unităților economice de stat ca regii autonome și societăți comerciale, cu modificările și completările ulterioare, la care statul este acționar unic ori majoritar.
2. Evaluează, testează și certifică produse și servicii de securitate cibernetică, pentru nevoi proprii sau la solicitarea instituțiilor din SNAOPSN și/sau Guvernului.
3. Stabilește reguli, prescripții sau caracteristici pentru activități sau pentru rezultatele acestora din domeniul securității cibernetice, pentru asigurarea unei abordări unitare la nivel național în scopul realizării unui nivel ridicat al securității cibernetice.
4. În colaborare cu organismele specializate participă la elaborarea, aprobarea și adoptarea de standarde în domeniul de competență, pe care le pune la dispoziția publicului.
5. Participă la lucrările comitetelor tehnice naționale și internaționale pentru punerea în aplicare a standardelor și specificațiilor tehnice acceptate la nivel internațional, aplicabile securității rețelelor și a sistemelor informatice, fără a impune sau discrimina în favoarea utilizării unui anumit tip de tehnologie.

r) **Funcția de educație și pregătire în domeniul securității cibernetice**

1. Dezvoltă parteneriate cu ministere de resort, cu școli, licee/colegii și universități, cu mediul privat, precum și cu parteneri internaționali, în scopul creării cadrului național de educație și pregătire în domeniul securității cibernetice care să ofere resursa umană necesară statului român pentru asigurarea securității cibernetice.
2. Promovează școlarizarea, educarea și formarea profesională a elevilor și studenților cu privire la securitatea cibernetică în vederea asigurării implementării și utilizării noilor tehnologii în viața de zi cu zi.
3. Desfășoară acțiuni, exerciții și colocvii de pregătire și instruire.
4. Inițiază și coordonează, în colaborare cu reprezentanți ai mediului public, privat și academic, înființarea și dezvoltarea de centre de excelență în domeniul securității cibernetice, centrale și regionale, având ca scop pregătirea resursei umane calificate pentru nevoile naționale, desfășurarea de activități de cercetare-dezvoltare în domeniul securității cibernetice, precum și orice alte activități necesare asigurării unui nivel ridicat de securitate cibernetică în România. Aceste activități pot include, fără a se limita la, pregătirea resursei umane din alte state.
5. Certifică, la cerere, centre de excelență, programe de școlarizare, educare și formare profesională în domeniul securității cibernetice.

s) **Funcția de management al proiectelor și serviciilor pentru activități** se realizează fără a aduce atingere activităților incluse în art. 5 lit. b) și lit. q) după cum urmează:

1. DNSC participă la identificarea, coordonarea și implementarea de proiecte de interes comun, atât pe cont propriu, cât și în parteneriat și facilitează accesul instituțiilor, operatorilor economici și persoanelor abilitate la aceste proiecte.
2. DNSC întocmește, conduce, execută și participă la proiecte cu finanțare internă și externă pentru asigurarea unui nivel ridicat de securitate a rețelelor și sistemelor informatice.
3. DNSC produce și valorifică soluții de securitate, aplicații informatice și produse pentru asigurarea unui nivel ridicat de securitate cibernetică a rețelelor și sistemelor informatice.
4. DNSC asigură asistență de specialitate, participă în echipe de intervenții / monitorizare și furnizează servicii în domeniul de competență pentru asigurarea securității cibernetice.
5. DNSC valorifică rezultatele cercetărilor realizate la nivelul instituției.
6. DNSC poate crea sau participa în structuri cu sau fără personalitate juridică, departamente, secții, laboratoare ori alte structuri legale sau organizatorice necesare realizării unora din activitățile din obiectul său de activitate, cu respectarea prevederilor legale in vigoare.

t) **Funcția de management al organizării și asocierii în societăți** se realizează fără a aduce atingere activităților incluse în art. 5 lit. b) și lit. q) după cum urmează:

1. DNSC poate înființa, în condițiile legii, în numele statului, societăți cu capital de stat în România și în străinătate. De asemenea, DNSC poate participa, cu respectarea cadrului legal în vigoare din domeniul societar la majorarea capitalului social al societăților la care exercită, în numele statului, calitatea de acționar.
2. Decizia privind înființarea de societăți sau majorarea capitalului social are ca temei o analiză economico-financiară, tehnică, juridică și de oportunitate care se fundamentează pe următoarele principii:
    i. promovare a concurenței între operatorii economici;
    ii. garantarea tratamentului egal și nediscriminatoriu al acestora;
    iii. asigurarea transparenței fondurilor publice alocate și utilizarea eficientă a acestora;
    iv. dezvoltarea regională fundamentată pe considerente sociale, economice și de mediu;
    v. evitarea apariției unor situații de natură să determine conflicte sociale ori manifestare a concurenței neloiale

3. Drepturile și obligațiile statului rezultând din calitatea de acționar/asociat la societățile înființate potrivit lit. t) pct. 1. vor fi exercitate de către DNSC prin directorul DNSC și cei doi adjuncți ai directorului DNSC.
4. Exercitarea drepturilor și îndeplinirea obligațiilor statului prevăzute la lit. t) pct. 3. de către DNSC prin alte instituții publice se stabilesc prin hotărâre a Guvernului.
5. Orice proiect de hotărâre prevăzut la lit. t) pct. 4. trebuie să fie însoțit de un memorandum aprobat prealabil de Guvern, privind oportunitatea promovării operațiunii și încadrarea în politicile economico-bugetare și financiare ale Guvernului. Memorandumul este supus aprobării Guvernului după obținerea avizului Consiliul Concurenței.

Art. 6 Conducere

(1) Conducerea DNSC este asigurată de directorul DNSC și doi adjuncți ai directorului DNSC, care au rang de secretar de stat, respectiv subsecretari de stat.

(2) Directorul DNSC și cei doi adjuncți ai directorului DNSC sunt numiți și eliberați din funcție prin decizie a prim-ministrului României, cu avizul CSAT.

(3) Directorului DNSC și celor doi adjuncți ai directorului DNSC le sunt aplicabile regimul incompatibilităților și al conflictului de interese aplicabil funcțiilor de secretar de stat și subsecretar de stat, astfel cum este prevăzut de cartea I titlul IV din Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției, cu modificările și completările ulterioare.

(4) Durata mandatului directorului DNSC este de 5 ani, cu posibilitatea prelungirii o singură dată, nu mai mult de 5 ani.

(5) Mandatul directorului DNSC încetează în următoarele situații:

a) în situația imposibilității de a-și îndeplini mandatul mai mult de 120 de zile calendaristice consecutive dintr-un interval de 140 de zile;

b) în caz de condamnare penală prin hotărâre judecătorească definitivă, pentru care nu a intervenit reabilitarea;

c) în situația retragerii avizului CSAT ca urmare a constatării unor abateri grave care afectează buna funcționare a DNSC, securitatea națională sau interesele naționale;

d) prin demisie;

e) prin deces;

f) la expirarea perioadei mandatului.

(6) Dacă funcția de director DNSC devine vacantă, în condițiile alin. (5) lit. a) - e) se procedează la numirea unei noi persoane pentru această funcție pentru durata rămasă din mandat, în condițiile prevederilor alin. (3).

(7) În caz de vacanță a funcției de director DNSC, până la desemnarea și numirea, în condițiile legii, a unui nou director, pentru durata rămasă din mandat, interimatul va fi asigurat de unul din directorii adjuncți.

Art. 7 Reprezentare

(1) Directorul DNSC reprezintă instituția în raporturile cu alte autorități și instituții publice, organizații non-guvernamentale, precum și cu orice persoane juridice și fizice din țară și din străinătate.

(2) Directorul DNSC este ordonator principal de credite în condițiile legii.

(3) În exercitarea atribuțiilor sale, directorul DNSC emite decizii și ordine.

(4) Deciziile și ordinele cu caracter normativ se publică în Monitorul Oficial al României, Partea I.

(5) Deciziile și ordinele adoptate în exercitarea atribuțiilor prevăzute de lege, inclusiv cele adoptate în conformitate cu prevederile Legii nr. 362/2018, pot fi atacate în contencios administrativ, în condițiile legii.

(6) DNSC transmite Comisiei Europene informații cu privire la implementarea normativelor europene ce intră în domeniile de competență ale instituției, conform termenelor stabilite sau la solicitarea expresă a Comisiei Europene.

Art. 8 Atribuții ale conducerii DNSC

(1) Directorul DNSC are următoarele atribuții principale:

a) Supune spre aprobare prim-ministrului, cu avizul CSAT strategia de dezvoltare instituțională a DNSC, programe de activitate și cooperare și planul anual de activitate ale DNSC.

b) Supune spre avizarea CSAT proiectul de buget anual al DNSC.

c) Aprobă planurile de investiții ale DNSC.

d) Convoacă și prezidează reuniunile Comitetului Director al DNSC.

e) Stabilește amplasarea sediilor structurilor teritoriale ale DNSC.

f) Stabilește, prin decizie internă, atribuțiile specifice fiecărui compartiment funcțional din cadrul DNSC.

g) Aprobă regulamentul intern al DNSC.

h) Aprobă, în condițiile legii, încadrarea, promovarea, precum și modificarea sau încetarea raporturilor de muncă ale personalului DNSC.

i) Prezintă anual în CSAT raportul de activitate al DNSC.

j) Supune spre aprobare CSAT, actele de organizare ale DNSC, respectiv statul de funcții, structura organizatorică și regulamentul de organizare și funcționare, precum și orice modificare a acestora.

(2) Directorul DNSC poate delega adjuncților directorului DNSC exercitarea atribuțiilor prevăzute la alin. (1).

(3) În lipsa directorului DNSC, atribuțiile sale se exercită de către adjunctul directorului DNSC desemnat prin decizie a directorului DNSC.

(4) Dacă atât directorul DNSC, cât și adjuncții directorului DNSC sunt absenți sau în imposibilitate temporară de a-și exercita prerogativele, reprezentarea DNSC se asigură de către o persoană cu funcție de conducere desemnată prin decizie a directorului DNSC.

Art. 9 Comitetul Director

(1) În activitatea sa, conducerea DNSC este sprijinită de Comitetul Director al DNSC, ce funcționează în baza unui statut elaborat de către DNSC, aprobat de prim-ministru, cu avizul CSAT.

(2) Comitetul Director este format din reprezentanți ai:

a) Administrației Prezidențiale;

b) Prim-ministrului;

c) CIO-ului Guvernamental;

d) Ministerului Afacerilor Interne;

e) Ministerului Apărării Naționale;

f) Serviciului Român de Informații;

g) Serviciului de Informații Externe;

h) Serviciului de Telecomunicații Speciale;

i) Serviciului de Protecție și Pază.

(3) Membrii Comitetului Director sunt desemnați de către conducerea instituțiilor menționate la alin. (2).

(4) Directorul DNSC și directorii adjuncți ai DNSC sunt membri de drept ai Comitetului Director.

(5) Comitetul Director are următoarele atribuții și competențe:

a) Avizează strategiile de dezvoltare ale DNSC și propunerile de politici publice elaborate de DNSC, destinate prevenirii și contracarării incidentelor din cadrul infrastructurilor cibernetice.

b) Avizează bugetul anual, planul anual de activitate și raportul anual de activitate ale DNSC.

c) Urmărește desfășurarea în condiții de eficiență economică și performanță profesională a activității DNSC.

d) Formulează recomandări privind obiectivele din planul anual de activitate al DNSC.

e) Formulează recomandări privind punctele de vedere naționale ce trebuie susținute de reprezentanții DNSC în formatele de cooperare internațională.

f) Analizează activitatea DNSC pe baza rapoartelor de activitate prezentate de către directorul DNSC.

g) Avizează actele de organizare ale DNSC, precum și orice modificare a acestora, respectiv statul de funcții, structura organizatorică și regulamentul de organizare și funcționare.

h) Sprijină conducerea DNSC în îndeplinirea obiectivelor instituționale asumate prin prezentul act normativ și prin regulamentul de organizare și funcționare.

(6) Comitetul Director își desfășoară activitatea în cadrul unor întâlniri trimestriale, în ședințe ordinare, sau ori de câte ori este nevoie, în ședințe extraordinare.

(7) În exercitarea atribuțiilor sale Comitetul Director emite avize și recomandări, care se adoptă cu votul majorității simple a membrilor prezenți la ședință.

(8) Secretariatul Comitetului Director este asigurat de către DNSC.

Art. 10 Comitetul de Reglementare

(1) Se înființează Comitetul de Reglementare cu rol de garant al obiectivității, transparenței, neutralității, echidistanței, nediscriminării și legalității activităților de reglementare desfășurate de DNSC acordând, în acest scop, sprijin de specialitate, prin îndrumări și recomandări în ceea ce privește asigurarea respectării principiilor obiectivității, transparenței, neutralității, echidistanței, nediscriminării și legalității în activitatea de reglementare a DNSC.

(2) Comitetul de Reglementare are un rol consultativ și are următoarea componență:

a) trei membri din cadrul DNSC, desemnați prin decizie a Directorului DNSC.

b) câte un membru din instituțiile prevăzute la art. 9 alin. (2) precum și de la Oficiul Registrului Național al Informațiilor Secrete de Stat (ORNISS);

(3) Numirea și revocarea membrilor Comitetului de Reglementare se face de către Comitetul Director la propunerea instituțiilor menționate la alin. (2).

(4) Conducătorul compartimentului funcțional care gestionează activitatea de reglementare din cadrul DNSC este membru de drept al Comitetului de Reglementare, convoacă și prezidează reuniunile acestuia.

(5) Membrii Comitetului de Reglementare trebuie să îndeplinească următoarele condiții:

a) să fie cetățeni români, cu domiciliul stabil în România, cu o bună reputație etică și profesională.

b) să fie absolvenți de studii superioare și cu pregătire profesională în domeniul tehnic, economic sau juridic, având o vechime în muncă de minimum 10 ani.

c) să aibă o experiență de minimum 5 ani în funcții de conducere în domeniul securității cibernetice, rețelelor și sistemelor informatice sau din SNAOPSN.

(6) Durata mandatului membrilor Comitetului de Reglementare este de 3 ani.

(7) În cazul imposibilității definitive de exercitare a mandatului de către unul dintre membri, instituțiile menționate la alin. (2) desemnează o nouă persoană în condițiile alin. (3) și (5) pentru perioada rămasă din mandat.

(8) Se consideră imposibilitate definitivă de exercitare a mandatului orice împrejurare care creează o indisponibilizare cu o durată mai mare de 90 de zile consecutive.

(9) Activitatea Comitetului de Reglementare se desfășoară în baza statutului Comitetului de Reglementare, elaborat de către DNSC cu avizul CSAT.

(10) Secretariatul Comitetului de Reglementare este asigurat de DNSC prin compartimentul funcțional care gestionează activitatea de reglementare.

Art. 11 Finanțare

(1) Finanțarea cheltuielilor curente și de capital ale DNSC se asigură din venituri proprii și subvenții acordate de la bugetul de stat.

(2) Veniturile proprii provin din:

a) Venituri din funcția de autoritate:

1. tarife pentru servicii prevăzute la art. 24 alin. (6^1) din Legea nr. 362/2018, stabilite prin decizie a Directorului DNSC care se publică în Monitorul Oficial al României, Partea I;
2. tarife pentru înscrierea în Registrul național al activelor, produselor și serviciilor de securitate cibernetică;
3. tarife pentru autorizarea laboratoarelor civile de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor care sunt utilizate în cadrul rețelelor și sistemelor informatice;
4. tarife pentru avizarea conformității privind securitatea cibernetică;
5. tarife pentru certificarea securității cibernetice a soluțiilor, produselor și serviciilor de tehnologia informației și comunicațiilor, inclusiv a noilor tehnologii;

b) Venituri din surse altele decât cele provenite din funcția de autoritate:

1. servicii de specialitate, audit, investigații cibernetice, consultanță de specialitate, școlarizare și educație privind securitatea cibernetică și managementul riscurilor cibernetice;
2. furnizare de produse și servicii de securitate cibernetică;
3. încasări din drepturi de proprietate intelectuală și licențe;
4. donații, legate și sponsorizări în condițiile legii;
5. credite interne și externe contractate în condițiile legii;
6. proiecte, fonduri, granturi și alte instrumente de finanțare pentru care DNSC este eligibil;
7. comisioane pentru parteneriate și proiecte;
8. alte venituri ce se pot realiza în condițiile legii.

(3) Sumele încasate din sursele prevăzute la alin. (2) se rețin integral ca venituri proprii.

(4) Bugetul anual de venituri și cheltuieli al DNSC se aprobă, în condițiile legii, cu avizul CSAT.

Art. 12 Analiza activității DNSC

(1) Activitatea DNSC este analizată de CSAT pe baza raportului anual, care se prezintă pentru anul anterior, precum și a rapoartelor specifice întocmite la solicitarea CSAT.

(2) Raportul anual de activitate se depune la CSAT, până la data de 31 martie, după avizare de către Comitetul Director.

(3) DNSC elaborează rapoarte, analize și informări cu privire la securitatea cibernetică a spațiului cibernetic național, a infrastructurilor cibernetice de interes național, a rețelelor și sistemelor informatice din domeniile de competență pe care le prezintă prim-ministrului, președintelui, CSAT, COSC și instituțiilor cu atribuții în SNAOPSN, precum și Comitetului Director.

Art. 13 Personalul instituției

(1) Personalul DNSC este format din personal contractual propriu și personal detașat din SNAOPSN, încadrat pe funcții conform statului de funcții al DNSC.

(2) Statul de funcții, structura organizatorică și regulamentul de organizare și funcționare al DNSC precum și orice modificare a acestora se aprobă de către CSAT. Statul de funcții cuprinde și funcțiile prevăzute a se încadra cu personal provenit inclusiv din SNAOPSN.

(3) Numărul maxim de posturi este de 1250.

(4) Statul de funcții al DNSC conține funcții specifice de conducere și de execuție după cum urmează:

a) Funcții de conducere: Manager superior securitate cibernetică, Manager securitate cibernetică, Coordonator superior securitate cibernetică, Coordonator securitate cibernetică.

b) Funcții de execuție (studii superioare): Expert securitate cibernetică, Expert preluare, analiză primară și răspuns la incidente securitate cibernetică, Expert investigații digitale și analiză malware, Expert dezvoltare, implementare și administrare infrastructuri securitate cibernetică, Expert analiză surse deschise, riscuri și amenințări securitate cibernetică, Expert accesare fonduri, implementare și administrare proiecte securitate cibernetică, Expert legal politici, standardizare de securitate cibernetică, Expert evaluare și impact financiar securitate cibernetică, Expert politici, strategii și cooperare securitate cibernetică, Expert dezvoltare competențe, aptitudini și cunoștințe specifice de securitate cibernetică.

c) Funcții de execuție (studii medii): Asistent securitate cibernetică, Asistent preluare, analiză primară și răspuns la incidente securitate cibernetică, Asistent investigații digitale și analiză malware, Asistent dezvoltare, implementare și administrare infrastructuri securitate cibernetică, Asistent analiză surse deschise, riscuri și amenințări securitate cibernetică, Asistent accesare fonduri, implementare și administrare proiecte securitate cibernetică, Asistent legal politici, standardizare de securitate cibernetică, Asistent evaluare și impact financiar securitate cibernetică, Asistent politici, strategii și cooperare securitate cibernetică, Asistent dezvoltare competențe, aptitudini și cunoștințe specifice de securitate cibernetică.

Art. 14 Încadrarea și promovarea personalului

Personalul DNSC este angajat pe bază de concurs sau examen organizat în condițiile legii, în conformitate cu structura organizatorică, iar salarizarea personalului se face potrivit prevederilor legale în vigoare privind salarizarea personalului plătit din fonduri publice.

Art. 15 Patrimoniu

(1) DNSC preia patrimoniul, arhiva și creditele bugetare angajate, inclusiv pe întreg anul în curs, ale Centrului Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO, care se desființează.

(2) DNSC se subrogă în toate drepturile și obligațiile, Centrului Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO inclusiv în litigiile aflate pe rolul instanțelor judecătorești și dobândește calitatea procesuală a acestuia.

(3) Predarea-preluarea patrimoniului se efectuează în baza situațiilor financiare întocmite potrivit prevederilor art. 28 alin. (1^1) din Legea contabilității nr. 82/1991 republicată, cu modificările și completările ulterioare, și a protocolului de predare-preluare întocmit în termen de 30 de zile de la data

intrării în vigoare a prezentei ordonanțe de urgență. Protocolul de predare-preluare cuprinde și creditele bugetare și execuția bugetară pe anul în curs pe care DNSC o preia de la Centrul Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO.

Art. 16 Cooperare

(1) DNSC cooperează cu organizații și organisme internaționale pe domeniile sale de competență.

(2) DNSC reprezintă România la nivelul instituțiilor Uniunii Europene și la nivelul altor foruri internaționale pentru domeniile de competență.

(3) Pentru asigurarea unei capacități adecvate de identificare, evaluare și adoptarea unor măsuri de management al riscului și/sau de răspuns la incidente și atacuri cibernetice, DNSC dezvoltă schimburi de informații și transfer de expertiză cu instituțiile și autoritățile cu responsabilități în domeniu, promovează și susține cooperarea între sectorul public și cel privat, precum și cooperarea cu mediile neguvernamentale și comunitatea academică.

(4) DNSC poate face parte ca membru cotizant în organizații și organisme naționale și internaționale, pe domeniile sale de competență.

Art. 17 Atribuții în situații de criză cibernetică pe timp de pace

(1) Atribuțiile specifice, modul de organizare și funcționare a CNGCC se stabilesc prin Regulamentul de Organizare și Funcționare a CNGCC, care se elaborează de către DNSC în termen de 6 luni de la intrarea în vigoare a prezentei Ordonanțe de Urgență și se aprobă de către Directorul DNSC, cu avizul COSC.

(2) Conducerea DNSC va dispune măsurile necesare pentru asigurarea capacității operaționale a instituției, inclusiv a CNGCC pentru gestionarea de criză cibernetică.

Art. 18 Autorizarea laboratoarelor civile

(1) În implementarea Regulamentului (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică), produsele și serviciile de securitate cibernetică utilizate în cadrul rețelelor și sistemelor informatice sunt testate, evaluate și certificate de operatori economici care au calitatea de laboratoare civile autorizate. Funcționarea laboratoarelor civile autorizate ce efectuează activități de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor care sunt utilizate în cadrul rețelelor și sistemelor informatice, este condiționată de obținerea unei autorizații prealabile din partea DNSC.

(2) Acordarea, prelungirea, suspendarea sau retragerea autorizației prevăzută la alin. (1) se efectuează, în baza regulamentului de autorizare și verificare a laboratoarelor civile de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor care sunt utilizate în cadrul rețelelor și sistemelor informatice, elaborat de DNSC și aprobat prin hotărâre a Guvernului. Valabilitatea autorizației este de maximum 3 ani.

(3) Cererea pentru obținerea autorizației de funcționare a laboratoarelor civile prevăzute la alin. (1) însoțită de documentația stabilită prin regulamentul prevăzut la alin. (2) se transmite către DNSC în format fizic sau prin mijloace electronice.

(4) În termen de 10 zile de la primirea cererii solicitantului, DNSC îl informează pe acesta dacă documentația este completă sau solicită informații suplimentare relevante.

(5) În termen de maxim 60 de zile de la data primirii tuturor informațiilor solicitate, DNSC eliberează autorizația de funcționare a laboratorului de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor care sunt utilizate în cadrul rețelelor și sistemelor informatice sau informează solicitantul asupra deciziei sale negative.

(6) DNSC justifică în mod corespunzător orice decizie prin care refuză autorizația de funcționare a laboratorului de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor care sunt utilizate în cadrul rețelelor și sistemelor informatice.

Art. 19 Activitatea de verificare a laboratoarelor civile

(1) DNSC exercită controlul activității desfășurate de către laboratoarele civile de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor care sunt utilizate în cadrul rețelelor și sistemelor informatice.

(2) Activitatea de verificare a îndeplinirii obligațiilor de către laboratoarele civile se desfășoară în baza regulamentului de autorizare și verificare a laboratoarelor civile prevăzut la art. 18 alin. (2).

(3) Următoarele fapte constituie contravenții dacă nu au fost săvârșite în astfel de condiții încât să fie considerate infracțiuni potrivit legii:

a) nerespectarea condițiilor prevăzute în autorizația de funcționare a laboratorului civil;

b) încălcarea de către laboratorul civil a normelor stabilite în regulamentul prevăzut la art. 18 alin. (2).

c) furnizarea de rapoarte sau certificate de testare, evaluare sau certificare de către laboratoare civile neautorizate sau fără autorizație valabilă;

d) refuzul laboratorului civil de a se supune controlului declanșat de DNSC ori întârzierea nejustificată în furnizarea informațiilor și documentelor solicitate în cadrul activităților de control în temeiul prezentei ordonanțe de urgență.

(4) Contravențiile prevăzute la alin. (3) se sancționează astfel:

a) cu amendă de la 5.000 lei la 50.000 lei, iar în cazul săvârșirii unei noi contravenții în termen de 6 luni, de la data săvârșirii primei contravenții, limita maximă a amenzii este de 200.000 lei;

b) prin derogare de la dispozițiile art. 8 alin. (2) lit. a) din Ordonanța Guvernului nr. 2/2001 privind regimul juridic al contravențiilor, aprobată cu modificări și completări prin Legea nr. 180/2002, cu modificările și completările ulterioare, pentru operatorii economici cu o cifră de afaceri de peste 1.000.000 lei, cu amendă în cuantum de până la 5% din cifra de afaceri, iar, în cazul săvârșirii unei noi contravenții, în termen de 6 luni, de la data săvârșirii primei contravenții, limita maximă a amenzii este de 10% din cifra de afaceri.

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

(6) Cifrei de afaceri prevăzute la alin. (4) lit. b) îi corespunde totalitatea veniturilor brute realizate de respectivii operatori economici în anul anterior sancționării.

(7) Pentru entitățile nou-înființate și pentru entitățile care nu au înregistrat cifra de afaceri în anul anterior sancționării, amenda prevăzută la alin. (4) se stabilește în cuantum de minim unu și maxim 25 de salarii minime brute pe economie.

(8) În măsura în care prezenta ordonanță de urgență nu prevede altfel, contravențiilor prevăzute la alin. (3) li se aplică dispozițiile Ordonanței Guvernului nr.2/2001 privind regimul juridic al contravențiilor, aprobată cu modificări și completări prin Legea nr.180/2002, cu modificările și completările ulterioare.

(9) Constatarea contravențiilor prevăzute la alin. (3) se realizează de către personalul de control din cadrul DNSC, iar aplicarea sancțiunii corespunzătoare se fac prin decizia directorului DNSC.

(10) Decizia prevăzută la alin. (9) trebuie să cuprindă următoarele elemente: datele de identificare ale contravenientului, data săvârșirii faptei, descrierea faptei contravenționale și a împrejurărilor care au fost avute în vedere la individualizarea sancțiunii, indicarea temeiului legal potrivit căruia se stabilește și se sancționează contravenția, sancțiunea aplicată, termenul și modalitatea de plată a amenzii, termenul de exercitare a căii de atac și instanța de judecată competentă.

(11) În vederea individualizării sancțiunii, directorul DNSC va lua în considerare gradul de pericol social concret al faptei, perioada de timp în care obligația legală a fost încălcată, precum și, dacă este cazul, consecințele încălcării asupra concurenței.

(12) Prin derogare de la prevederile art. 13 din Ordonanța Guvernului nr. 2/2001, aprobată cu modificări și completări prin Legea nr. 180/2002, cu modificările și completările ulterioare, aplicarea sancțiunii potrivit alin. (4) se prescrie în termen de un an de la data săvârșirii faptei. În cazul încălcărilor care durează în timp sau al celor constând în săvârșirea, în baza aceleiași rezoluții, la intervale diferite de timp, a mai multor acțiuni sau inacțiuni, care prezintă, fiecare în parte, conținutul aceleiași contravenții, prescripția începe să curgă de la data constatării sau de la data încetării ultimului act ori fapt săvârșit, dacă acest moment intervine anterior constatării.

(13) Decizia prevăzută la alin. (9) se comunică contravenientului în termen de 15 zile de la data constatării contravenției.

(14) Odată cu decizia prevăzută la alin. (9), contravenientului i se comunică și înștiințarea de plată, care conține mențiunea privind obligativitatea achitării amenzii în termen de 30 de zile de la data comunicării deciziei.

(15) Decizia prevăzută la alin. (9) constituie titlu executoriu, fără vreo altă formalitate. Acțiunea în contencios administrativ în condițiile alin. (17) suspendă executarea numai în ceea ce privește achitarea amenzii, până la pronunțarea de către instanța de judecată a unei hotărâri definitive.

(16) Sumele provenite din amenzile aplicate în conformitate cu dispozițiile prezentului articol se fac venit integral la bugetul de stat. Executarea se realizează în conformitate cu dispozițiile legale privind executarea silită a creanțelor fiscale. În vederea punerii în executare a sancțiunii, DNSC comunică din oficiu organelor de specialitate ale Agenției Naționale de Administrare Fiscală decizia prevăzută la alin. (9), după expirarea termenului prevăzut în înștiințarea de plată sau după rămânerea definitivă a hotărârii judecătorești prin care s-a soluționat acțiunea în contencios administrativ.

(17) Prin derogare de la prevederile art. 7 din Legea contenciosului administrativ nr. 554/2004, cu modificările și completările ulterioare, deciziile adoptate potrivit prezentei ordonanțe de urgență pot fi atacate în contencios administrativ la Curtea de Apel București, fără parcurgerea procedurii prealabile, în termen de 30 de zile de la comunicarea acestora.

Art. 20 Dispoziții finale și tranzitorii

(1) Prezenta ordonanță de urgență nu se aplică domeniilor din responsabilitatea instituțiilor de apărare, ordine publică și securitate națională, infrastructurilor critice naționale și infrastructurilor ce vehiculează informații clasificate.

(2) Lista bunurilor proprietate publică a statului, precum și lista bunurilor imobile proprietate privată a statului, preluate în administrare de către DNSC, se vor aproba prin hotărâre a Guvernului României, în termen de 30 de zile de la data intrării în vigoare a prezentei ordonanțe de urgență.

(3) Reîncadrarea personalului preluat potrivit art. 2 alin. (3) în structura organizatorică a DNSC se realizează în termenele și cu procedura prevăzute de lege.

(4) De la data aprobării de către CSAT a statului de funcții, organigramei și regulamentului de organizare și funcționare DNSC, se va demara procedura de ocupare a posturilor vacante în noua structură organizatorică.

(5) În termen de 180 de zile de la data intrării în vigoare a prezentei ordonanțe de urgență se va aproba, prin hotărâre a Guvernului, regulamentul de autorizare și verificare a laboratoarelor civile de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor care sunt utilizate în cadrul rețelelor și sistemelor informatice.

(6) Prin derogare de la dispozițiile art. 27 alin. (3) din Legea nr. 55/2020 privind unele măsuri pentru prevenirea și combaterea efectelor pandemiei de COVID-19, cu modificările și completările ulterioare, pe durata stării de alertă se pot desfășura și concursuri sau examene pentru ocuparea posturilor vacante sau temporar vacante din structura organizatorică a DNSC.

(7) Se autorizează Ministerul Finanțelor Publice să introducă modificările în structura bugetului de stat și în volumul și structura bugetelor ordonatorilor principali de credite, corespunzător prevederilor

prezentei ordonanțe de urgență, după caz, la propunerea ordonatorilor principali de credite, pe bază de protocoale de predare-preluare.

(8) În termen de 5 zile de la aprobarea modificărilor prevăzute la alin. (7) se autorizează Secretariatul General al Guvernului să introducă modificările corespunzătoare în bugetul propriu și în anexele la acesta și să le comunice Ministerului Finanțelor Publice.

(9) Până la încheierea protocoalelor prevăzute la alin. (7), finanțarea cheltuielilor curente și de capital ale DNSC se asigură din bugetul Secretariatul General al Guvernului.

(10) La data intrării în vigoare a prezentei ordonanțe de urgență se abrogă Hotărârea Guvernului nr. 494/2011 privind înființarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO, publicată în Monitorul Oficial al României, Partea I, nr. 388 din 2 iunie 2011, cu modificările și completările ulterioare.

Art. 21 Modificarea și completarea unor acte normative

(1) În tot cuprinsul Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice cu modificările și completările ulterioare, publicată în Monitorul Oficial al României, Partea I, nr. 21 din 9 ianuarie 2019, sintagma "Centrul Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO" și sintagma "Secretariatul General al Guvernului" se înlocuiesc cu sintagma "Directoratul Național de Securitate Cibernetică", sintagma "CERT-RO" se înlocuiește cu sintagma "DNSC", iar sintagma "Secretarul General al Guvernului" se înlocuiește cu sintagma "Directorul DNSC".

(2) La data intrării în vigoare a prezentei ordonanțe de urgență se abrogă art. II din Ordonanța de urgență nr.4/2020 privind stabilirea unor măsuri la nivelul administrației publice centrale și pentru modificarea unor acte normative, publicată în Monitorul Oficial al României, Partea I, nr. 38 din 20 ianuarie 2020.

(3) La anexa nr. VIII la Legea-cadru nr. 153/2017 privind salarizarea personalului plătit din fonduri publice, publicată în Monitorul Oficial al României, Partea I, nr. 492 din 28 iunie 2017, cu modificările și completările ulterioare, la capitolul II litera A punctul I, după nota 6 se introduce o nouă notă, nota 7, cu următorul cuprins:

"7. Prevederile pct. 3 și 4 se aplică în mod corespunzător și personalului din cadrul Directoratului Național de Securitate Cibernetică."

PRIM-MINISTRU

LUDOVIC ORBAN