

ORDIN

pentru aprobarea Normelor privind autorizarea și verificarea furnizorilor de servicii de formare pentru securitate cibernetică

În baza prevederilor art. 20 lit. e) și q), art. 32 alin. (2) lit. e) și art. 33 alin. (2) lit. e) din Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cu modificările și completările ulterioare,

în aplicarea art. 4 lit. f) și art. 5 lit. b) pct. 4 din Ordonanța de urgență a Guvernului nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, aprobată cu modificări și completări prin Legea nr. 11/2022,

în temeiul dispozițiilor art. 7 alin. (3) din Ordonanța de urgență a Guvernului nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, aprobată cu modificări și completări prin Legea nr. 11/2022,

directorul Directoratului Național de Securitate Cibernetică emite prezentul ordin.

Art. 1. – Se aprobă Normele privind autorizarea și verificarea furnizorilor de servicii de formare pentru securitate cibernetică, prevăzute în anexa care face parte integrantă din prezentul ordin.

Art. 2. – Personalul cu atribuții în procesul de autorizare din cadrul Directoratului Național de Securitate Cibernetică va lua măsuri pentru aplicarea prezentului ordin.

Art. 3. – Prezentul ordin se publică în Monitorul Oficial al României, Partea I.

Directorul Directoratului Național de Securitate Cibernetică

Petre-Dan CÎMPEAN

București, 14 octombrie 2022.

Nr. 106.

NORMELE

privind autorizarea și verificarea furnizorilor de servicii de formare pentru securitate cibernetică

CAPITOLUL I

Dispoziții generale

ARTICOLUL 1

Aplicabilitate

- (1) Prezentele norme referitoare la autorizarea furnizorilor de servicii de formare pentru securitate cibernetică, denumite în continuare *norme*, stabilesc cadrul legal privind autorizarea furnizorilor de servicii de formare pentru securitate cibernetică, respectiv pentru formarea auditorilor de securitate cibernetică, a membrilor echipelor CSIRT și/sau a responsabililor cu securitatea rețelelor și sistemelor informatice, în vederea autorizării acestora în condițiile Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cu modificările și completările ulterioare.
- (2) Autorizarea reprezintă procesul în urma căruia furnizorii de servicii de formare pentru securitate cibernetică, pot organiza programe de formare inițială sau continuă în domeniul securității cibernetice, finalizate cu certificate de specializare sau de participare recunoscute de DNSC în calitate de autoritate competentă la nivel național pentru securitatea rețelelor și sistemelor informatice.
- (3) În înțelesul prezentelor norme, furnizorii de servicii de formare pentru securitate cibernetică pot fi persoane juridice înscrise în registrele naționale ale furnizorilor de formare profesională, respectiv *Registrul național al furnizorilor de formare continuă* (gestionat de Ministerul Educației) și/sau *Registrul național al furnizorilor de formare profesională a adulților* (gestionat de Ministerul Muncii și Solidarității Sociale), care dispun de formatori, îndeplinesc cerințele prevăzute în prezentele norme și desfășoară cel puțin o activitate prin care se realizează formarea și/sau instruirea auditorilor de securitate cibernetică, a membrilor echipelor CSIRT sau a responsabililor cu securitatea rețelelor și sistemelor informatice însărcinați cu monitorizarea canalelor de contact, denumiți în continuare *responsabili NIS*.
- (4) Prezentele norme nu se aplică la nivelul instituțiilor din sistemul de apărare, ordine publică și securitate națională, din domeniul protecției infrastructurilor critice și nici la nivelul infrastructurilor cibernetice care vehiculează informații clasificate.
- (5) Formarea profesională specifică pentru securitate cibernetică tratată în prezentele norme, cuprinde:
- a) formarea auditorilor de securitate cibernetică;
 - b) formarea membrilor echipelor CSIRT;
 - c) formarea responsabililor NIS.

ARTICOLUL 2

Termeni, expresii și abrevieri

(1) În cuprinsul prezentelor norme, se utilizează următoarele abrevieri:

- a) *DNSC* – Directoratul Național de Securitate Cibernetică;
- b) *DGRC* – Direcția Generală Reglementare și Control;
- c) *DAA* – Direcția Atestare și Autorizare;
- d) *CSIRT* sau *echipă CSIRT* – echipă de răspuns la incidente de securitate cibernetică;
- e) *RENFOSEC* – Registrul național al furnizorilor de servicii de formare pentru securitate cibernetică.

(2) În cuprinsul prezentelor norme, precum și în activitatea specifică domeniului securității cibernetică se utilizează următoarele concepte:

- a) *autorizație de furnizor de servicii de formare pentru securitate cibernetică* – document emis de autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice pe baza criteriilor de evaluare, cu valabilitate limitată de patru ani, prin care se certifică îndeplinirea condițiilor de către furnizorul de servicii de formare pentru securitate cibernetică privind desfășurarea uneia din activitățile de formare precizate la art. 1 alin. (5);
- b) *centru de formare pentru securitate cibernetică* – mediul fizic sau online, logic și organizațional în care se formează/instruiesc auditorii de securitate cibernetică, membrii echipelor CSIRT și/sau responsabili NIS;
- c) *certificat de specializare auditor de securitate cibernetică* – document eliberat de către DNSC la solicitarea unui furnizor de servicii de formare pentru securitate cibernetică autorizat de autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice, la finalizarea procesului de formare, care certifică specializarea personalului în vederea atestării pentru a desfășura activități de audit de securitate cibernetică;
- d) *certificat de specializare membru echipă CSIRT* – document eliberat de către DNSC la solicitarea unui furnizor de servicii de formare pentru securitate cibernetică autorizat de autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice, la finalizarea procesului de formare, care certifică formarea personalului în vederea autorizării ca membru în cadrul unei echipe CSIRT;
- e) *certificat de specializare responsabil NIS* – document eliberat de către DNSC la solicitarea unui furnizor de servicii de formare pentru securitate cibernetică autorizat de autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice, la finalizarea procesului de formare, care certifică pregătirea personalului în vederea numirii/desemnării ca responsabil cu securitatea rețelelor și sistemelor informatice la nivelul operatorilor economici care furnizează servicii esențiale și/sau digitale;
- f) *certificat evaluare expertiză privind securitatea cibernetică* – document eliberat de către DNSC în calitate de autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice în urma promovării examenului / evaluării expertizei în domeniul auditului de securitate cibernetică, examen desfășurat la sediul DNSC sau într-un centru de formare pentru securitate cibernetică;
- g) *formarea auditorilor de securitate cibernetică* – activitatea prin care se asigură creșterea și diversificarea competențelor profesionale, prin specializare inițială și perfecționarea continuă a auditorilor de securitate cibernetică care urmează a fi

atestați sau reatestați în vederea desfășurării activităților de auditare a rețelelor și sistemelor informatice;

- h) *formarea membrilor echipelor CSIRT* – activitatea prin care se asigură creșterea și diversificarea competențelor profesionale, prin formarea inițială și perfecționarea continuă a membrilor echipelor CSIRT care urmează să facă fie autorizați sau reatestați în vederea participării în echipe CSIRT și furnizării de servicii de tip CSIRT necesare asigurării securității rețelelor și sistemelor informatice ale operatorilor de servicii esențiale și/sau furnizorilor de servicii digitale;
- i) *formarea responsabililor NIS* – activitatea prin care se asigură creșterea și diversificarea competențelor profesionale, prin pregătirea inițierea și perfecționarea continuă a responsabililor NIS care urmează a fi desemnați sau desfășoară activități în vederea elaborării/implementării procedurilor, implementarea cerințelor minime de securitate cibernetică și a măsurilor de protecție ce trebuie implementate la nivelul rețelelor și sistemelor informatice;
- j) *formator pentru securitate cibernetică* – persoană fizică, cu studii superioare, având atribuții de instruire teoretică și/sau practică în cadrul unui furnizor de servicii de formare pentru securitate cibernetică, ce are profil sau specialități corespunzătoare programei de pregătire pentru securitate cibernetică;
- k) *furnizor de servicii de formare pentru securitate cibernetică* – persoană juridică, autorizată de autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice, înscrisă în Registrului național al furnizorilor de servicii de formare pentru securitate cibernetică;
- l) *lista furnizorilor de servicii de formare pentru securitate cibernetică* – cuprinde toți furnizorii de servicii de formare pentru securitate cibernetică valabil autorizați de către autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice și publicată pe site-ul instituției;
- m) *procedura de evaluare și autorizare a furnizorului de servicii de formare pentru securitate cibernetică* – procesul organizat și desfășurat la nivelul autorității competente la nivel național pentru securitatea rețelelor și sistemelor informatice prin care sunt evaluate și analizate, atât documentele care stau la baza solicitării autorizării, cât și experiența formatorilor, finalizat cu emiterea sau nu a autorizației de furnizor de servicii de formare pentru securitate cibernetică;
- n) *Registrul național al furnizorilor de servicii de formare pentru securitate cibernetică* – document constituit, în format electronic, gestionat și administrat la nivelul autorității competente la nivel național pentru securitatea rețelelor și sistemelor informatice care cuprinde evidența cronologică a autorizării, suspendării, revocării și reautorizării activităților furnizorilor de servicii de formare în domeniul securității cibernetică;
- o) *Registrul național de evidență a certificatelor pentru securitate cibernetică* – document constituit, în format electronic, gestionat și administrat la nivelul autorității competente la nivel național pentru securitatea rețelelor și sistemelor informatice care cuprinde evidența tuturor certificatelor menționate la lit. c) - f);
- p) *responsabil NIS* – responsabil cu securitatea rețelelor și sistemelor informatice însărcinat cu monitorizarea canalelor de contact cu autoritatea națională competentă, desemnat/stabilit la nivelul operatorului economic care furnizează servicii esențiale și/sau digitale.

ARTICOLUL 3

Autoritatea competentă la nivel național

- (1) Pentru eliberarea, revocarea sau reînnoirea autorizațiilor furnizorilor de servicii de formare pentru securitate cibernetică ce desfășoară programe de pregătire/specializare pentru auditorii de securitate cibernetică, pentru membrii echipelor CSIRT și/sau pentru responsabili NIS, Directoratul Național de Securitate Cibernetică este autoritatea competentă la nivel național în conformitate cu prevederile art. 15 alin. (1) coroborat cu art. 20 lit. q) din Legea nr. 362/2018, cu modificările și completările ulterioare.
- (2) Directoratul Național de Securitate Cibernetică, în calitate de autoritate competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice, coordonează procesul de autorizare și verificare a furnizorilor de servicii de formare pentru securitate cibernetică.
- (3) Organizarea și gestionarea activității sunt asigurate de Direcția atestare și autorizare din cadrul Direcției generale reglementare și control.
- (4) Verificarea și controlul activității desfășurate de furnizorii de servicii de formare pentru securitate cibernetică sunt asigurate de Direcția verificare și control din cadrul Direcției generale reglementare și control.
- (5) Autorizarea reprezintă un proces desfășurat de către personalul Direcției atestare și autorizare ce presupune analiza și evaluarea documentației depuse de furnizorii de formare și are ca rezultat eliberarea autorizației de furnizor de servicii de formare pentru securitate cibernetică în baza căreia se pot furniza servicii de formare și/sau instruire în domeniul securității cibernetice. Modelul autorizației este prezentat în anexa nr. 1.
- (6) Soluționarea cererilor de autorizare se face în termen de 60 de zile de la data înregistrării.
- (7) Directoratul Național de Securitate Cibernetică, în calitate de autoritate competentă la nivel național, asigură:
 - a) menținerea și actualizarea permanentă a Registrului național al furnizorilor de servicii de formare pentru securitate cibernetică;
 - b) acordarea, prelungirea, suspendarea sau retragerea autorizațiilor furnizorilor de servicii de formare pentru securitate cibernetică;
 - c) evaluarea procesului de pregătire/specializare a auditorilor în vederea atestării ca auditori de securitate cibernetică, a membrilor echipelor CSIRT și/sau a responsabililor NIS atât prin verificarea și actualizarea tematicilor elaborate, aprobarea programelor de pregătire, cât și prin comisiile de examen/evaluare de securitate și eliberarea certificatelor de specialitate/ evaluare.

ARTICOLUL 4

Condiții privind eliberarea autorizației pentru furnizorii de servicii de formare

- (1) Pentru a se supune autorizării în vederea furnizării de servicii de formare pentru securitate cibernetică, furnizorii de servicii de formare profesională stabiliți în România trebuie să îndeplinească următoarele condiții de eligibilitate:
 - a) să fie legal constituiți;
 - b) să aibă prevăzute în statut sau, după caz, în actul de înființare activități de formare profesională;

- c) să își îndeplinească obligațiile de plată a impozitelor, taxelor și contribuțiilor datorate, potrivit legislației în vigoare.
- (2) Pentru a deveni furnizor de servicii de formare pentru securitate cibernetică și a fi înscris în Registrul național al furnizorilor de servicii de formare pentru securitate cibernetică, solicitantul trebuie să parcurgă următorul proces:
 - a) să solicite, în scris, printr-o cerere autorizarea ca furnizor de servicii de formare pentru securitate cibernetică;
 - b) să fie înscris într-unul din registrele naționale specificate la art. 1 alin. (3);
 - c) să dispună de formatori cu experiență în domeniul securității cibernetice pentru desfășurarea procesului de pregătire/instruire a auditorilor de securitate cibernetică, a membrilor echipelor CSIRT și/sau a responsabililor NIS.
- (3) În procesul de autorizare sunt autorizați furnizorii de servicii de formare pentru securitate cibernetică, și nu formatorii pentru securitate cibernetică.
- (4) Un formator nu poate solicita autorizare pentru desfășurarea uneia dintre activitățile de formare precizate la art. 1 alin. (5), ci numai un furnizor de servicii de formare legal constituit.
- (5) Un furnizor de servicii de formare pentru securitate cibernetică nu poate solicita autorizarea ca furnizor de servicii de formare fără a deține o listă de formatori de cel puțin două persoane fizice.
- (6) Autorizația de furnizor de servicii de formare pentru securitate cibernetică se eliberează pentru fiecare dintre categoriile de pregătire pentru care furnizorul de servicii de formare pentru securitate cibernetică organizează programe de formare profesională.

ARTICOLUL 5

Criteriile de evaluare a furnizorilor de servicii de formare pentru securitate cibernetică în vederea autorizării

- (1) Criteriile de evaluare a furnizorilor de servicii de formare pentru securitate cibernetică au în vedere următoarele elemente:
 - a) programul de formare profesională pentru cel puțin o activitate de formare din cele prevăzute la art. 1 alin. (5);
 - b) experiența furnizorilor de formare profesională și rezultatele activității lor anterioare obținerii autorizării sau în alte programe de formare profesională pe care le-au realizat, dacă este cazul;
 - c) capacitatea furnizorului de servicii de formare de a asigura resursele umane, materiale și financiare, necesare pentru elaborarea, susținerea și desfășurarea programului de formare;
 - d) autorizațiile și avizele necesare desfășurării programelor de formare profesională, după caz.
- (2) În vederea autorizării, furnizorii de servicii de formare pentru securitate cibernetică trebuie să facă dovada că realizează programele de formare profesională cu formatori care au profiluri sau specialități corespunzătoare programei de pregătire, respectiv care au pregătirea specifică educației adulților conform standardelor ocupaționale.
- (3) La analizarea programei de pregătire, specialiștii Direcției atestare și autorizare din cadrul Direcției generale reglementare și control au în vedere dacă:
 - a) structura programei de pregătire este în concordanță cu prezentele norme;

- b) fiecare modul, respectiv pentru auditorii de securitate cibernetică, membrii echipelor CSIRT și responsabili NIS, permite dobândirea cunoștințelor necesare desfășurării activităților;
 - c) obiectivele generale ale programului sunt formulate în conformitate cu tipul formării auditorilor de securitate cibernetică, membrilor echipelor CSIRT și responsabililor NIS;
 - d) conținutul tematic:
 - (i). este adecvat nivelului de pregătire al participanților;
 - (ii). este formulat în concordanță cu terminologia și legislația în vigoare;
 - (iii). respectă tematicile de specializare a auditorilor de securitate cibernetică, a membrilor echipelor CSIRT și a responsabililor NIS, aprobate prin decizia directorului DNSC și publicată în Monitorul Oficial al României, Partea I;
 - e) metodele/formele de activitate sunt adecvate procesului de formare și sunt stabilite în concordanță cu conținutul tematic;
 - f) mijloacele de instruire și materialele de învățare sunt corespunzătoare pentru atingerea obiectivelor de referință, respectiv pentru dobândirea competențelor specifice;
 - g) criteriile de evaluare asigură cuantificarea rezultatelor obținute în urma desfășurării procesului de pregătire.
- (4) În procesul de evaluare și autorizare, autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice colaborează cu instituții cu responsabilități în domeniul apărării, ordinii publice și securității naționale, cu alte instituții și autorități, după caz, precum și cu instituții cu responsabilități în aplicarea legii în vederea evaluării înscrisurilor trimise de către solicitant.
- (5) Criteriile care stau la baza autorizării furnizorilor de servicii de formare pentru securitate cibernetică stau și la baza monitorizării și verificării acestora.
- (6) Neîndeplinirea criteriilor de autorizare determină neacordarea sau, după caz, retragerea autorizației.
- (7) Rezultatul activității de evaluare/autorizare se concretizează, după caz, în:
- a) emiterea autorizației în vederea furnizării de servicii de formare pentru securitate cibernetică, când sunt îndeplinite toate condițiile prevăzute în prezentele norme;
 - b) respingerea cererii de autorizare.
- (8) Autorizația de furnizor de servicii de formare pentru securitate cibernetică se semnează de directorul DNSC și se avizează de adjunctul directorului DNSC care coordonează activitatea de reglementare și control, managerul superior al DGRC și managerul DAA.
- (9) În cazul respingerii eliberării autorizației, în adresa de răspuns se vor consemna motivele care au stat la baza acesteia.

CAPITOLUL II

AUTORIZAREA FURNIZORILOR DE SERVICII DE FORMARE PENTRU SECURITATE CIBERNETICĂ

SECȚIUNEA 1

Autorizarea furnizorilor de servicii de formare

ARTICOLUL 6

Documente necesare pentru autorizare

- (1) Autorizația de furnizor de servicii de formare pentru securitate cibernetică se obține în baza cererii de autorizare și a dosarului pentru emiterea autorizației de furnizor de servicii de formare pentru securitate cibernetică. Modelul de cerere este prevăzut în anexa nr. 2.
- (2) Dosarul pentru emiterea autorizației de furnizor de servicii de formare pentru securitate cibernetică trebuie să cuprindă următoarele documente:
 - a) documentul de înființare/înregistrare al persoanei juridice, respectiv certificat de înregistrare în registrele naționale, după caz, Registrul comerțului, Registrul asociațiilor și fundațiilor, Registrul federațiilor etc.;
 - b) certificat constatator emis de instituția care gestionează registrul în care se ține evidența înființării persoanei juridice, cu starea la zi a persoanei juridice, nu mai vechi de 30 de zile;
 - c) codul unic de înregistrare/cod de înregistrare fiscal;
 - d) autorizația de furnizor de formare profesională, prin care se confirmă înscrierea în Registrul național al furnizorilor de formare continuă (gestionat de Ministerul Educației) și/sau Registrul național al furnizorilor de formare profesională a adulților (gestionat de Ministerul Muncii și Solidarității Sociale);
 - e) lista formatorilor care vor participa la desfășurarea programului de formare și temele alocate acestora;
 - f) documente specifice pentru fiecare formator, stabilite la alin. (3);
 - g) programa de formare specifică pentru fiecare categorie în parte, respectiv pentru formarea auditorilor de securitate cibernetică, membrilor echipelor CSIRT și responsabililor NIS (programa de pregătire, întocmită în conformitate cu standardele de pregătire profesională, aprobate în condițiile reglementărilor în vigoare);
 - h) lista dotărilor utilizate în realizarea pregătirii teoretice și practice, corelată cu dotările prevăzute în programa de pregătire;
 - i) dovada achitării tarifului de evaluare și procesare în vederea autorizării ca furnizor de servicii de formare pentru securitate cibernetică, pentru fiecare tip de formare stabilite la art. 1 alin. (5).
- (3) Documentele specifice pentru formatori sunt:
 - a) actul de identitate, în copie;
 - b) certificatul de absolvire curs de formatori sau dovada pentru profesare în funcție didactică în învățământul superior sau expert în securitate cibernetică;
 - c) curriculum vitae – model europass, cu detalierea secțiunii „experiență profesională” ce va conține justificarea privind experiența în domeniu, respectiv cele stabilite la art. 19 alin. (3);
 - d) diplomă studii superioare, respectiv licență, master etc.;
 - e) certificate, brevete, adeverințe sau alte documente care fac dovada îndeplinirii de către formatori a criteriilor privind deținerea unui nivel minim de experiență de cinci ani în domeniul securității cibernetică.

ARTICOLUL 7

Transmitere documente pentru autorizare

- (1) Dosarul pentru emiterea autorizației de furnizor de servicii de formare pentru securitate cibernetică se constituie și se transmite, în format electronic, împreună cu cererea de autorizare, sub semnătură electronică sau olografă (scanate), la autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice, prin email la **dgrc-autorizare@dnsc.ro**.
- (2) Documentația va fi în limba română, paginată și însoțită de un opis.
- (3) Autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice va confirma primirea documentelor/înscrierilor.
- (4) Orice modificare ulterioară a documentelor prevăzute la art. 6 alin. (2) și (3) va fi transmisă, în format electronic, la autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice în termen de maximum 15 zile de la data producerii acesteia, folosind procedura stabilită la alin. (1).

ARTICOLUL 8

Inițierea procedurii de evaluare și autorizare

- (1) După confirmarea primirii documentației, autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice procedează la inițierea procedurii de evaluare și autorizare a furnizorului de servicii de formare pentru securitate cibernetică.
- (2) Procedura de evaluare și autorizare presupune parcurgerea a patru etape procedurale, respectiv: evaluarea documentației de autorizare; evaluarea expertizei formatorilor; evidența furnizorului de servicii; finalizarea procedurii de autorizare.
- (3) În cazul în care autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice constată că pentru finalizarea procedurii de evaluare și autorizare sunt necesare înscrieri suplimentare și/sau expertize ori constată că anumite documente depuse nu îndeplinesc condițiile legale de fond sau de formă ori că lipsesc anumite documente doveditoare sau nu au fost achitate taxele legale, solicită noi informații/ documente și acordă un termen de până la 30 zile pentru furnizarea acestora.
- (4) Neprezentarea completărilor în termenul precizat la alin. (3), conduce la întreruperea procedurii de evaluare și autorizare, restituirea dosarului și informarea solicitantului cu privire la refuzul eliberării autorizației de furnizor de servicii de formare pentru securitate cibernetică.
- (5) Procedura de evaluare și autorizare, respectiv luarea în evidență a furnizorului de servicii de formare pentru securitate cibernetică sau refuzul privind autorizarea, se finalizează la nivelul autorității competente la nivel național pentru securitatea rețelelor și a sistemelor informatice, în termen de maximum 60 de zile de la primirea documentației complete de la solicitant.

ARTICOLUL 9

Evaluarea documentației de autorizare

- (1) Autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice constituie mapa furnizorului de servicii de formare pentru securitate cibernetică, evaluează documentele transmise de către solicitant, solicită date, informații sau înscrieri suplimentare, dacă e cazul, și în funcție de situație dispune continuarea sau întreruperea procedurii de evaluare și autorizare.

- (2) Mapa furnizorului de servicii de formare pentru securitate cibernetică ce cuprinde cererea solicitantului, dosarul pentru emiterea autorizației, alte informații/înscrisuri suplimentare, dacă e cazul, și informații cu privire la etapele procedurale aplicate se păstrează la autoritatea competentă la nivel național, în format electronic.

ARTICOLUL 10

Evaluarea expertizei formatorilor

- (1) Autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice analizează/evaluează valabilitatea documentelor specifice și certificărilor profesionale pentru fiecare formator în conformitate cu art. 6 alin. (3).
- (2) În urma evaluării expertizei formatorilor, autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice dispune continuarea sau întreruperea procedurii de evaluare și autorizare.

ARTICOLUL 11

Evidența furnizorului de servicii

- (1) Direcția atestare și autorizare din cadrul Direcției generale reglementare și control întocmește raportul final de evaluare și autorizare prin care se propune emiterea autorizației de furnizor de servicii de formare pentru securitate cibernetică sau restituirea dosarului.
- (2) În baza raportului final de evaluare și autorizare, autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice emite autorizația de furnizor de servicii de formare pentru securitate cibernetică, ia în evidență furnizorul de servicii de formare pentru securitate cibernetică și actualizează lista furnizorilor de servicii de formare pentru securitate cibernetică.
- (3) Lista furnizorilor de servicii de formare pentru securitate cibernetică se publică pe site-ul instituției.
- (4) Evidența furnizorilor de servicii de formare pentru securitate cibernetică se ține de către autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice, în format electronic, pe baza registrului național al furnizorilor de servicii de formare pentru securitate cibernetică.

ARTICOLUL 12

Finalizarea procedurii de autorizare

- (1) Autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice transmite solicitantului autorizația de furnizor de servicii de formare pentru securitate cibernetică.
- (2) Autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice actualizează bazele de date specifice și trece la monitorizarea respectării aplicării Legii nr. 362/2018 de către furnizorul de servicii de formare pentru securitate cibernetică.
- (3) În termen de 10 zile de la primirea autorizației de furnizor de servicii de formare pentru securitate cibernetică, persoana juridică, va efectua plata tarifului de autorizare furnizori de servicii de formare în conformitate cu *Decizia directorului Directoratului Național de Securitate Cibernetică nr. 301/2021 pentru aprobarea listei cuantumului tarifelor pentru servicii din activitățile prevăzute la art. 22 alin.(1) lit. l), art. 32 alin. (2) lit. c) și e) și la art.*

33 alin. (2) lit. c) și e) din Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice.

- (4) Neachitarea taxei duce la revocarea autorizației și radierea furnizorului de servicii de formare pentru securitate cibernetică din evidențele autorității competente la nivel național pentru securitatea rețelelor și a sistemelor informatice.
- (5) Dosarele solicitanților care nu se încadrează în prevederile prezentelor norme, precum și dosarele incomplete ale solicitanților care nu au fost completate în termenul stabilit la art. 8 alin. (3) se restituie acestora, fiind însoțite de o adresă de informare cu privire la restituire. Taxa de evaluare și procesare în vederea autorizării ca furnizor de servicii de formare nu se restituie.

SECȚIUNEA a 2-a

Revocarea autorizației de furnizor de servicii de formare

ARTICOLUL 13

Revocarea autorizației

- (1) Directoratul Național de Securitate Cibernetică, în calitate de autoritate competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice, dispune revocarea autorizației de furnizor de servicii de formare pentru securitate cibernetică în următoarele situații:
 - a) neîndeplinirea criteriilor de autorizare determină neacordarea sau, după caz, retragerea autorizației;
 - b) nerespectarea în procesul de pregătire a programei, a tematicii sau a standardelor și specificațiilor europene și internaționale;
 - c) nerespectarea în întocmirea programelor de pregătire a tematicilor pentru fiecare activitate de formare elaborate de autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice;
 - d) neachitarea tarifelor de furnizor de servicii de formare pentru securitate cibernetică sau de reînnoire autorizație;
 - e) neachitarea amenzilor contravenționale stabilite de personalul de control din cadrul autorității competente la nivel național pentru securitatea rețelelor și a sistemelor informatice în urma controalelor impuse de sesizările primite, din oficiu sau în urma autosesizării ori încălcării de către furnizorul de servicii de formare pentru securitate cibernetică a obligațiilor ce îi revin în temeiul Legii nr. 362/2018, cu modificările și completările ulterioare;
 - f) suspendarea de trei ori consecutiv a autorizației de furnizor de servicii de formare pentru securitate cibernetică în timpul unei perioade de valabilitate a acesteia;
 - g) comiterea de infracțiuni în domeniul securității cibernetică;
 - h) în cazul unui program, dacă la două serii consecutive se constată că rata de promovare este mai mică de 70% sau rata de abandon este mai mare de 50%, se face o reevaluare a furnizorului de servicii de formare pentru securitate cibernetică și, dacă este cazul, i se retrage autorizația.
- (2) La cererea expresă a furnizorului de servicii de formare pentru securitate cibernetică privind renunțarea la autorizație, autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice dispune revocarea autorizației și radierea furnizorului de servicii de formare pentru securitate cibernetică din registrul național. Modelul de cerere este prezentat în anexa nr. 3.

ARTICOLUL 14

Finalizarea procedurii de revocare a autorizației

- (1) După revocarea autorizației de furnizor de servicii de formare pentru securitate cibernetică, autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice informează persoana în cauză, radiază furnizorul de servicii de formare pentru securitate cibernetică din evidențele autorității, respectiv Registrul național al furnizorilor de servicii de formare pentru securitate cibernetică și actualizează lista furnizorilor de servicii de formare pentru securitate cibernetică de pe site-ul instituției.
- (2) Furnizorul de servicii de formare pentru securitate cibernetică căruia i-a fost revocată autorizația, poate solicita o nouă autorizație după intrarea în legalitate, dar nu mai devreme de un an.

Secțiunea a 3-a

Reînnoirea autorizației de furnizor de servicii de formare

ARTICOLUL 15

Reînnoirea autorizației

- (1) Cu 60 de zile înainte de expirarea termenului de valabilitate a autorizației, furnizorul de servicii de formare pentru securitate cibernetică va solicita Directoratului Național de Securitate Cibernetică reînnoirea autorizației prin completarea și transmiterea unei cereri de reînnoire a autorizației, însoțită de dosarul pentru reînnoirea autorizației de furnizor de servicii de formare pentru securitate cibernetică. Modelul de cerere este prezentat în anexa nr. 4.
- (2) Dosarul pentru reînnoirea autorizației de furnizor de servicii de formare pentru securitate cibernetică va cuprinde următoarele documente:
 - a) documentele stabilite la art. 6 alin. (2), actualizate la zi;
 - b) documentele stabilite la art. 6 alin. (3) pentru fiecare formator;
 - c) tariful de evaluare și procesare în vederea reînnoirii autorizării ca furnizor de servicii de formare pentru securitate cibernetică (același cu cel pentru autorizarea inițială);
 - d) lista programelor de pregătire desfășurate pe perioada de valabilitate a autorizației, conform modelului prezentat în Anexa nr. 5.
- (3) În procedura de evaluare și reînnoire a autorizației de furnizor de servicii de formare pentru securitate cibernetică, autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice aplică prevederile de la capitolul II secțiunea 1.
- (4) În termen de 10 zile de la primirea autorizației de furnizor de servicii de formare pentru securitate cibernetică, furnizorul va efectua plata tarifului de autorizare furnizori de servicii de formare în conformitate cu *Decizia directorului Directoratului Național de Securitate Cibernetică nr. 301/2021 pentru aprobarea listei cuantumului tarifelor pentru servicii din activitățile prevăzute la art. 22 alin. (1) lit. l), art. 32 alin. (2) lit. c) și e) și la art. 33 alin. (2) lit. c) și e) din Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice*.
- (5) Neachitarea tarifului precizat la alin. (4) duce la revocarea autorizației și radierea furnizorului de servicii de formare pentru securitate cibernetică din registrul național.

SECȚIUNEA a 4-a

Suspendarea autorizației de furnizor de servicii de formare

ARTICOLUL 16

Suspendarea autorizației

- (1) Autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice poate dispune suspendarea autorizației de furnizor de servicii de formare pentru securitate cibernetică, pentru o perioadă stabilită de autoritate, în următoarele situații:
 - a) în cazul descoperirii de către autoritatea competentă la nivel național a nerespectării de către un furnizor de servicii de formare pentru securitate cibernetică a unei obligații prevăzute de Legea nr. 362/2018, cu modificările și completările ulterioare, sau prezentele norme sau de un act emis de autoritatea competentă la nivel național în baza Legii nr. 362/2018, cu modificările și completările ulterioare – până la remedierea deficiențelor constatate și conformare cu Legea nr. 362/2018, cu modificările și completările ulterioare;
 - b) în cazul procedurii de reînnoire a autorizației pentru nerespectarea termenului stabilit la art. 8 alin. (3) – de la a 31-a zi de la data efectuării modificării și până la îndeplinirea cerinței stabilite, dar nu mai mult de 60 zile.
- (2) În cazul suspendării autorizației de furnizor de servicii pentru securitate cibernetică, furnizorul de servicii de formare căruia i s-a suspendat autorizația nu va mai putea desfășura activități de formare pentru securitate cibernetică în condițiile Legii nr. 362/2018, cu modificările și completările ulterioare, și nici să emită certificate de specialitate până la remedierea neregulilor și intrarea în legalitate.
- (3) Modelul deciziei de suspendare a autorizației de furnizor de servicii de formare pentru securitate cibernetică este prezentat în anexa nr. 6.

SECȚIUNEA a 5-a

Registrul național al furnizorilor de servicii de formare pentru securitate cibernetică

ARTICOLUL 17

Constituirea, întreținerea și actualizarea registrului

- (1) Directoratul Național de Securitate Cibernetică constituie, la nivelul Direcției atestare și autorizare din cadrul Direcției generale reglementare și control, Registrul național al furnizorilor de servicii de formare pentru securitate cibernetică (RENFOSEC), ce este întreținut și actualizat în permanență.
- (2) Registrul se constituie în format electronic pe activități de formare pentru securitate cibernetică prezentate la art. 1 alin. (5) și cuprinde date și informații cu privire la furnizorii de servicii de formare pentru securitate cibernetică supuși procesului de autorizare, revocare sau suspendare a autorizației de furnizor de servicii de formare pentru securitate cibernetică.
- (3) Modelul registrului este prezentat în anexa nr. 7.
- (4) Pentru informarea publică, respectiv a operatorilor de servicii esențiale, furnizorilor de servicii digitale, auditorilor de securitate cibernetică și echipelor CSIRT, inclusiv a solicitanților de atestate sau autorizatii, în baza Registrului național al furnizorilor de servicii de formare pentru securitate cibernetică, autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice elaborează, actualizează în

permanență și publică pe site-ul instituției lista furnizorilor de servicii de formare pentru securitate cibernetică.

- (5) Eliberarea, revocarea și reînnoirea autorizațiilor de furnizor de servicii de formare pentru securitate cibernetică se consemnează de către autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice în evidențele proprii.

CAPITOLUL III

Formarea și furnizarea serviciilor de formare pentru securitate cibernetică

ARTICOLUL 18

Furnizorul de servicii de formare pentru securitate cibernetică

- (1) Furnizor de servicii de formare pentru securitate cibernetică poate fi orice persoană juridică ce realizează pe teritoriul României activități de formare profesională ce îndeplinește condițiile stabilite în prezentele norme și care asigură pregătire/specializarea auditorilor de securitate cibernetică, membrilor echipelor CSIRT și/sau responsabililor NIS.
- (2) Furnizorii de servicii de formare pentru securitate cibernetică își desfășoară activitatea în centre de formare, on-line sau on-site, prin personal de specialitate (formatori pentru securitate cibernetică) și realizează activități de pregătire/specializare în domeniul securității ciberetice.
- (3) Furnizorii de servicii de formare pentru securitate cibernetică sunt autorizați de autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice, iar evidența acestora este ținută în Registrul național al furnizorilor de servicii de formare pentru securitate cibernetică.
- (4) Calitatea de furnizor de servicii de formare pentru securitate cibernetică se dovedește prin autorizația de furnizor de servicii de formare pentru securitate cibernetică eliberată de către Directoratul Național de Securitate Cibernetică în calitate de autoritate competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice.
- (5) Autorizația de furnizor de servicii de formare pentru securitate cibernetică este nominală, netransmisibilă și are valabilitate trei ani de la data emiterii.

ARTICOLUL 19

Formatorul pentru securitate cibernetică

- (1) Formator pentru securitate cibernetică poate fi orice persoană fizică, calificată, cu atribuții de instruire teoretică și practică, cu profiluri sau specialități corespunzătoare programei de pregătire pentru securitate cibernetică.
- (2) Formatorul pentru securitate cibernetică deține specializări corespunzătoare programei de pregătire.
- (3) Formatorul pentru securitate cibernetică trebuie să îndeplinească cumulativ următoarele:
 - a) să fi absolvit un curs de formare cu certificat de absolvire sub antetul Autorității Naționale pentru Calificări sau să dețină dovada pentru profesare în funcție didactică în învățământul superior sau pentru profesare ca expert în securitate cibernetică;
 - b) nivelul studiilor: studii superioare absolvite cu diplomă;

- c) să aibă experiență de minim cinci ani în domeniul securității cibernetice.

ARTICOLUL 20

Activități de formare pentru securitate cibernetică

- (1) Activitățile de formare pentru securitate cibernetică sunt:
 - a) formarea auditorilor de securitate cibernetică;
 - b) formarea membrilor echipelor CSIRT;
 - c) formarea responsabililor NIS.
- (2) Formarea pentru securitate cibernetică cuprinde formarea inițială și formarea continuă organizate prin alte forme decât cele specifice sistemului național de învățământ.
- (3) Formarea inițială asigură pregătirea necesară pentru dobândirea competențelor minime necesare pentru a putea desfășura activități specifice, respectiv auditor de securitate cibernetică, membru al unei echipe CSIRT sau responsabil NIS.
- (4) Formarea continuă este ulterioară formării inițiale și asigură personalului angrenat în activități specifice Legii nr. 362/2018, cu modificările și completările ulterioare, fie dezvoltarea competențelor profesionale deja dobândite, fie dobândirea de noi competențe.

ARTICOLUL 21

Programa de formare pentru securitate cibernetică

- (1) Programa de formare pentru securitate cibernetică cuprinde, fără a se limita la acestea, următoarele elemente:
 - a) obiectivele programului de formare exprimate în competențele profesionale ce urmează să fie dobândite de fiecare persoană fizică ce urmează programul;
 - b) durata de pregătire pentru realizarea obiectivelor propuse;
 - c) numărul minim și maxim de participanți pentru un ciclu sau o serie de pregătire;
 - d) locul de desfășurare;
 - e) calificarea persoanelor cu atribuții de instruire teoretică și practică, respectiv a formatorilor;
 - f) programa de pregătire, conform anexei nr. 8;
 - g) mijloacele și metodele prin care se asigură transmiterea și asimilarea cunoștințelor și formarea deprinderilor practice necesare desfășurării activităților pentru care se desfășoară programul;
 - h) dotările, echipamentele și materialele necesare formării;
 - i) procedura de evaluare în conformitate cu obiectivele specifice programului de formare profesională.
- (2) Programa de formare este aprobată la nivel național de Directoratul Național de Securitate Cibernetică, odată cu autorizarea furnizorului de servicii de formare pentru securitate cibernetică și se adresează numai absolvenților de studii superioare.
- (3) Tematicile pentru specializarea auditorilor de securitate cibernetică, a membrilor echipelor CSIRT și a responsabililor NIS se elaborează la nivelul autorității competente naționale, se aprobă prin decizia directorului DNSC și se publică în Monitorul Oficial al României, Partea I.
- (4) Durata minimă a programului de formare pentru securitate cibernetică, exprimată în ore de pregătire, pentru pregătirea teoretică și practică, pentru care se eliberează certificatul de specializare sau certificatul de participare este de:
 - a) 30 ore – formă inițială;

- b) 20 credite/an – formă continuă.
- (5) Creditele de la alin. (4) lit. b) pot fi realizate prin participarea la conferințe, simpozioane, sesiuni de pregătire tehnică, exerciții, cursuri sau alte forme de pregătire, care vor fi atestate prin documente justificative privind participarea la acestea.
- (6) Stabilirea creditelor pentru activitățile de la alin. (5) se va face prin decizie a directorului DNSC care va fi publicată pe site-ul instituției.
- (7) Echivalarea nivelului continuu de specializare se realizează de către autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice cu ocazia reînnoirii atestării sau autorizării.
- (8) Timpul alocat programului de formare pentru securitate cibernetică va fi corelat cu scopul, obiectivele, conținuturile și strategiile de realizare.
- (9) Activităților practice li se alocă cel mult jumătate și nu mai puțin de o treime din durata totală a programului de formare.

ARTICOLUL 22

Certificate de pregătire

- (1) Programul de formare pentru securitate cibernetică se finalizează printr-un examen.
- (2) Din comisia de examen poate face parte și un reprezentant al autorității competente la nivel național pentru securitatea rețelelor și a sistemelor informatice.
- (3) În vederea stabilirii datelor, premergător examenului de finalizare a programului de formare, furnizorul de servicii de formare pentru securitate cibernetică organizator va informa autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice despre activitate, respectiv perioada/data de desfășurare, locul și numărul de cursanți. Autoritatea competentă la nivel național va înștiința, după caz, de participare sau nu, inclusiv persoana nominalizată în comisia de examen și rolul acesteia.
- (4) Informarea autorității competente la nivel național pentru securitatea rețelelor și a sistemelor informatice se face cel mai târziu în prima zi a modului de pregătire din programul de formare, prin informare electronică, prin email la **dgrc-autorizare@dnsc.ro**.
- (5) După finalizarea examenului/programului, furnizorul de servicii de formare pentru securitate cibernetică transmite tabelul cu absolvenții, rezultatele și documentele aferente programului de formare la autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice.
- (6) După finalizarea programului de formare pentru securitate cibernetică se eliberează:
 - a) certificat de specializare – pentru pregătirea inițială;
 - b) certificat de participare – pentru pregătirea continuă.
- (7) Certificatul de specializare este emis de autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice pe baza documentelor aferente programului de formare specificate la alin. (3). Modelul de certificat de specializare se găsește în anexa nr. 9.
- (8) Evidența certificatelor de specializare se ține la nivelul Direcției atestare și autorizare pe baza Registrului național de evidență a certificatelor pentru securitate cibernetică (RENECSC). Modelul registrului se identifică în anexa nr. 10.
- (9) Certificatul de participare este eliberat de furnizorul de servicii de formare pentru securitate cibernetică sau de organizatorii activităților stabilite la art. 21 alin. (5).

- (10) Certificatele de specializare și de participare sunt utilizate în procesul de atestare ca auditor de securitate cibernetică, autorizare echipe CSIRT și/sau desfășurarea activitate ca responsabil NIS la nivelul operatorilor de servicii esențiale sau furnizori de servicii digitale și sunt recunoscute de autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice.

CAPITOLUL IV

Verificarea activității furnizorilor de servicii de formare pentru securitate cibernetică

ARTICOLUL 23

Verificarea activității furnizorilor de servicii de formare

- (1) Directoratul Național de Securitate Cibernetică în calitate de autoritate competentă la nivel național, prin Direcția verificare și control din cadrul Direcției generale reglementare și control, verifică modul de îndeplinire a activității de către furnizorii de servicii de formare pentru securitate cibernetică, în baza planului de control anual, a sesizărilor primite sau a activității de monitorizare a aplicării prevederilor Legii nr. 362/2018, cu modificările și completările ulterioare, la nivelul României.
- (2) În cazul în care, în urma verificărilor, se constată nerespectarea prevederilor prezentelor norme sau a Legii nr. 362/2018, cu modificările și completările ulterioare, autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice poate dispune suspendarea pe o perioadă de timp stabilită în vederea remedierii sau revocarea autorizației de furnizor de servicii de formare pentru securitate cibernetică.
- (3) Direcția verificare și control din cadrul Direcției generale reglementare și control verifică, în urma sesizărilor sau din oficiu, în conformitate cu prevederile art. 35 – 42 din Legea nr. 362/2018, cu modificările și completările ulterioare, îndeplinirea de către furnizorii de servicii de formare pentru securitate cibernetică a obligațiilor legale ce le revin și dispune, după caz, măsuri de remediere, suspendarea activității pe o perioadă specificată sau revocarea autorizației de furnizor de servicii de formare pentru securitate cibernetică.
- (4) Anual, în primul trimestru, furnizorii de servicii de formare pentru securitate cibernetică vor transmite la Directoratul Național de Securitate Cibernetică la Direcția verificare și control, în format electronic, la adresa de email **dgrc-control@dnsc.ro**, o situație a programelor de formare pentru securitate cibernetică, pe activități de formare și niveluri de specializare, desfășurate în anul calendaristic precedent, respectiv numărul, beneficiarii programelor, perioadele, neregulile constatate și dificultăți întâmpinate. Modelul de situație se regăsește în anexa nr. 11.

CAPITOLUL V

Organizarea și desfășurarea examenului/evaluării în domeniul auditului de securitate cibernetică

ARTICOLUL 24

Organizarea examinării/evaluării pentru auditori de securitate cibernetică

- (1) În aplicarea art. 25 din Regulamentul pentru atestarea și verificarea auditorilor de securitate cibernetică, aprobat prin Ordinul secretarului general al Guvernului nr. 559/2021, la nivelul Directoratului Național de Securitate Cibernetică sau centrelor de formare pentru securitate cibernetică se organizează activități de examinare/evaluare în domeniul auditului de securitate cibernetică.
- (2) Activitatea de examinare/evaluare se desfășoară la datele stabilite de către autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice.
- (3) Coordonarea întregii activități de examinare/evaluare revine Directoratului Național de Securitate Cibernetică în calitate de autoritate competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice.

ARTICOLUL 25

Participanți și taxă de participare

- (1) La activitatea de examinare/evaluare în domeniul auditului de securitate cibernetică pot participa absolvenți de studii superioare cu experiență în domeniul securității cibernetice și care nu dețin certificări profesionale pentru atestare în vederea desfășurării activității de auditor de securitate cibernetică.
- (2) Pentru a participa la examinare/evaluare solicitantul va completa și înainta o cerere de solicitare la autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice, în format electronic, la adresa **dgrc-autorizare@dnsc.ro**. Modelul de cerere se identifică în anexa nr. 12.
- (3) Cererea de solicitare va fi însoțită de dosarul de participare, în format electronic, compus din următoarele documente, în copie:
 - a) actul de identitate;
 - b) document de atestare a pregătirii de bază (studii superioare absolvite);
 - c) curriculum vitae – model europass;
 - d) dovada achitării taxei de evaluare participare la examen – 300 lei, plătită on-line, în contul Directoratului Național de Securitate Cibernetică.

ARTICOLUL 26

Desfășurarea examinării/evaluării pentru auditori de securitate cibernetică

- (1) În funcție de numărul solicitanților, autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice va stabili locul și data desfășurării examinării/evaluării și va publica pe site-ul instituției tematica, precum și datele de organizare a activității.
- (2) Participanții se vor prezenta la locația precizată, la data și ora stabilite, iar accesul la examinare/evaluare se va face pe bază de carte de identitate.
- (3) Examenul/Evaluarea se susține în fața unei comisii de evaluare.
- (4) Comisia de evaluare este desemnată de către Directoratul Național de Securitate Cibernetică, prin decizia directorului DNSC la propunerea managerului superior securitate cibernetică al DGRC și cu avizul adjunctului directorului DNSC coordonator al activității de reglementare și control.
- (5) Compunerea comisiei de evaluare:

- a) președinte – un reprezentant al autorității competente la nivel național pentru securitatea rețelelor și a sistemelor informatice;
 - b) membri – un reprezentant din cadrul DNSC; un reprezentant din instituțiile membre Consiliului Operativ de Securitate Cibernetică (COSC); un reprezentant din mediul academic;
 - c) secretar – un reprezentant din cadrul Direcției atestare și autorizare sau un reprezentant din cadrul centrului de formare pentru securitate cibernetică, când activitatea se desfășoară la sediul acestuia.
- (6) Examinarea/Evaluarea se realizează pe cele două tipuri principale de activități de audit, respectiv special și comun.
- (7) Examinarea/Evaluarea presupune desfășurarea unui test de evaluare, practic și teoretic, care presupune:
- a) la proba teoretică: test grilă;
 - b) la proba practică: identificarea unor vulnerabilități și stabilirea de recomandări pentru limitarea riscurilor de securitate; implementarea și evaluarea cerințelor minime de securitate cibernetică.

ARTICOLUL 27

Finalizarea examinării/evaluării pentru auditori de securitate cibernetică

- (1) La finalul procesului de examinare/evaluare, autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice va emite un certificat de evaluare a expertizei privind securitatea cibernetică, document care ține locul de certificare profesională și este recunoscut numai la nivelul autorității competente la nivel național pentru securitatea rețelelor și a sistemelor informatice. Modelul de certificat este prezentat în anexa nr. 13.
- (2) Evidența emiterii certificatelor de evaluare a expertizei se ține la nivelul Direcției atestare și autorizare din cadrul Direcției generale reglementare și control pe baza Registrului național de evidență a certificatelor pentru securitate cibernetică (RENECSC).
- (3) Taxa de examinare/evaluare și emiterie certificat, în valoare de 700 lei, se plătește on-line, în contul DNSC. După confirmarea plății taxei autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice va elibera certificatul și îl va transmite solicitantului.
- (4) Neplata taxei duce la imposibilitatea eliberării certificatului.

CAPITOLUL VI

Dispoziții finale

ARTICOLUL 28

Modificări condiții de funcționare

- (1) Orice schimbare în statutul și activitatea furnizorului de servicii de formare pentru securitate cibernetică, care modifică condițiile în care a fost autorizat, vor fi aduse la cunoștința autorității competente la nivel național pentru securitatea rețelelor și a sistemelor informatice, electronic, la adresa **dgrc-autorizare@dnsc.ro**, în cel mult 15 zile de la data producerii schimbărilor.

- (2) În cazul în care furnizorul de servicii de formare pentru securitate cibernetică nu mai deține formatori autorizați, autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice dispune suspendarea până la dovedirea îndeplinirii condiției de la art. 4 alin. (5), dar nu mai târziu de 60 zile.
- (3) În cazul în care furnizorul de servicii de formare pentru securitate cibernetică nu mai este înscris într-unul din registrele naționale ale furnizorilor de formare profesională, respectiv Registrul național al furnizorilor de formare continuă (gestionat de Ministerul Educației) sau Registrul național al furnizorilor de formare profesională a adulților (gestionat de Ministerul Muncii și Solidarității Sociale), autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice dispune revocarea autorizației de furnizor de servicii de formare pentru securitate cibernetică și radierea din Registrul național al furnizorilor de servicii de formare pentru securitate cibernetică.

ARTICOLUL 29

Condiții particulare privind formarea de securitate cibernetică

- (1) În aplicarea art. 36 alin. (1) din Regulamentul pentru atestarea și verificarea auditorilor de securitate cibernetică, aprobat prin Ordinul secretarului general al Guvernului nr. 559/2021, în primele șase luni de la intrarea în vigoare a prezentelor norme, auditorii de securitate cibernetică, persoane fizice, au obligația de a finaliza un curs de specializare auditor la unul dintre furnizorii de servicii de formare autorizați de către autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice.
- (2) Pregătirea inițială la un furnizor de servicii de formare ne autorizat de autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice nu este recunoscută de către autoritatea competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice în aplicarea Legii nr. 362/2018, cu modificările și completările ulterioare.

ARTICOLUL 30

Anexe

Anexele nr. 1 - 13 fac parte integrantă din prezentele norme.



DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ
DIRECȚIA GENERALĂ REGLEMENTARE ȘI CONTROL
DIRECȚIA ATESTARE ȘI AUTORIZARE

AUTORIZAȚIE

**FURNIZOR DE SERVICII DE FORMARE PENTRU
SECURITATE CIBERNETICĂ**

seria nr. din

TIP AUTORIZAȚIE DE FORMARE:

☐ Auditori securitate cibernetică / ☐ Membri CSIRT / ☐ Responsabili NIS

În aplicarea dispozițiilor art. 20 lit. q) din *Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice*, cu modificările și completările ulterioare,

În temeiul prevederilor art. 3 alin. (4) din *Normele privind autorizarea formatorilor și furnizorilor de servicii de formare pentru securitate cibernetică*, aprobate prin Ordinul directorului Directoratului Național de Securitate Cibernetică nr. 106/2022,

În baza *Raportului final de evaluare și autorizare*, nr. / /, întocmit de Direcția atestare și autorizare din cadrul Direcției generale reglementare și control,

Directoratul Național de Securitate Cibernetică, în calitate de autoritate competentă la nivel național pentru securitatea rețelelor și sistemelor informatice, autorizează:

.....

cu sediul în; CUI/CIF:

**FURNIZOR DE SERVICII DE FORMARE PENTRU SECURITATE
CIBERNETICĂ**

Cod unic identificare IDFSF: **QE**-.....

Înscris în **Registrul național al furnizorilor de servicii de formare pentru securitate cibernetică**.

Perioada de valabilitate: / / – / /

.....
Directorul DNSC

QR

(Verso Autorizație)

AVIZE

.....

Adjunctul directorului DNSC

.....

Managerul superior DGRC

.....

Managerul DAA

Autorizația a fost emisă la data de și a fost înscrisă în RENFOSEC la poziția ...

CERERE DE AUTORIZARE
furnizor de servicii de formare pentru securitate cibernetică

A. DATE DE IDENTIFICARE SOLICITANT**Denumirea:**

Forma de organizare sau statutul juridic

Sediul:

Strada:

Nr. Bl./Clădir Sc. Ap./Cam.
e

Localitatea:

Cod poștal:

Județul/Municipiul:

Sector:

Nr. telefon fix

Nr. mobil

E-mail:

Pagina internet:

Date identificare comercială/fiscalăNr. înregistrare RN¹:

CUI/CIF:

Localitatea:

Cod poștal:

Județul/Municipiul:

Sector:

Adresă corespondență

Strada:

Nr. Bl./Clădir Sc. Ap./Cam.
e

Localitatea:

Cod poștal:

Județul/Municipiul:

Sector:

Reprezentant legal

Prenumele

Numele

CNP

Funcția

B. SOLICITARE

În temeiul *Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice*, cu modificările și completările ulterioare,

În baza Normelor privind autorizarea furnizorilor de servicii de formare pentru securitate cibernetică, aprobate prin Ordinul directorului Directoratului Național de Securitate Cibernetică nr. 106/2022,

solicit eliberarea autorizației de furnizor de servicii de formare pentru securitate cibernetică ☐

Tipul de program de formare de reînnoit:

¹ Registrul comerțului; Registrul asociațiilor și fundațiilor; Registrul federațiilor etc.

Auditori de securitate cibernetică ☐	Membrii echipelor CSIRT ☐	Responsabili NIS ☐
Denumirea programului de formare		
C. ACORD PRELUCRARE DATE²		
Îmi exprim acordul cu privire la prelucrarea datelor cu caracter personal și procesarea electronică a datelor de către DNSC, în calitate de autoritate competentă la nivel național pentru securitatea rețelilor și sistemelor informatice, în procesul de implementare și monitorizare a Legii nr. 362/2018, cu modificările și completările ulterioare, ☐ Da		
D. CONFORMITATEA CU ORIGINALUL A DOCUMENTELOR FURNIZATE		
Confirm că toate documentele furnizate, în copie, sunt „conform cu originalul” . ☐ Da		
Anexe: Dosarul de autorizare ...		

Semnătură/Reprezentant legal

Nume și prenume:

Data:

Semnătura:

² În procesele interne, DNSC protejează interesele de securitate și comerciale ale furnizorilor de servicii de formare pentru securitate cibernetică, precum și confidențialitatea informațiilor furnizate de către aceștia.

Informațiile prelucrate în sensul îndeplinirii obligațiilor de la art. 32 și art. 33 din Legea nr. 362/2018, cu modificările și completările ulterioare, nu fac parte din categoria informațiilor de interes public așa cum acestea sunt reglementate în Legea nr. 544/2001 privind liberul acces la informațiile de interes public, cu modificările și completările ulterioare.

CERERE DE RENUNȚARE

la autorizația de furnizor de servicii de formare pentru securitate cibernetică

A. DATE DE IDENTIFICARE FURNIZOR DE SERVICII DE FORMARE:																						
DENUMIREA: 																						
Cod unic identificare (IDFSF) <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 10%;">Q</td> <td style="width: 10%;">E</td> <td style="width: 10%;">-</td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> </tr> </table>					Q	E	-															
Q	E	-																				
Adresă corespondență <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 60%; border-bottom: 1px solid black;">Strada:</td> <td style="width: 10%; border-bottom: 1px solid black;">Nr.</td> <td style="width: 15%; border-bottom: 1px solid black;">Bl./Clădire</td> <td style="width: 10%; border-bottom: 1px solid black;">Sc.</td> <td style="width: 5%; border-bottom: 1px solid black;">Ap./Cam.</td> </tr> <tr> <td style="border: 1px solid black; height: 20px;"></td> <td style="border: 1px solid black; width: 10%;"></td> <td style="border: 1px solid black; width: 15%;"></td> <td style="border: 1px solid black; width: 10%;"></td> <td style="border: 1px solid black; width: 5%;"></td> </tr> </table> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 40%; border-bottom: 1px solid black;">Localitatea:</td> <td style="width: 15%; border-bottom: 1px solid black;">Cod poștal:</td> <td style="width: 25%; border-bottom: 1px solid black;">Județul/Municipiul:</td> <td style="width: 20%; border-bottom: 1px solid black;">Sector:</td> </tr> <tr> <td style="border: 1px solid black; height: 20px;"></td> <td style="border: 1px solid black; width: 15%;"></td> <td style="border: 1px solid black; width: 25%;"></td> <td style="border: 1px solid black; width: 20%;"></td> </tr> </table> E-mail: 					Strada:	Nr.	Bl./Clădire	Sc.	Ap./Cam.						Localitatea:	Cod poștal:	Județul/Municipiul:	Sector:				
Strada:	Nr.	Bl./Clădire	Sc.	Ap./Cam.																		
Localitatea:	Cod poștal:	Județul/Municipiul:	Sector:																			
B. SOLICITARE																						
În temeiul <i>Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice</i> , cu modificările și completările ulterioare, În baza Normelor privind autorizarea furnizorilor de servicii de formare pentru securitate cibernetică, aprobate prin Ordinul directorului Directoratului Național de Securitate Cibernetică nr. 106/2022, Solicit renunțarea la autorizația de furnizor de servicii de formare pentru securitate cibernetică ☐																						
Tipul de program de formare de reînnoit: <table style="width: 100%;"> <tr> <td style="width: 33%;">Auditori de securitate cibernetică ☐</td> <td style="width: 33%;">Membrii echipelor CSIRT ☐</td> <td style="width: 33%;">Responsabili NIS ☐</td> </tr> </table>					Auditori de securitate cibernetică ☐	Membrii echipelor CSIRT ☐	Responsabili NIS ☐															
Auditori de securitate cibernetică ☐	Membrii echipelor CSIRT ☐	Responsabili NIS ☐																				
C. ACORD PRELUCRARE DATE³																						
Îmi exprim acordul cu privire la prelucrarea datelor cu caracter personal și procesarea electronică a datelor de către DNSC, în calitate de autoritate competentă la nivel național pentru securitatea rețelelor și sistemelor informatice, în procesul de implementare și monitorizare a Legii nr. 362/2018, cu modificările și completările ulterioare. ☐ Da																						
D. CONFORMITATEA CU ORIGINALUL A DOCUMENTELOR FURNIZATE																						
Confirm că toate documentele furnizate, în copie, sunt „conform cu originalul” . ☐ Da																						
Anexe:																						

Semnătură/Reprezentant legal

Nume și prenume:

Data:

Semnătura:

³ În procesele interne, DNSC protejează interesele de securitate și comerciale ale furnizorilor de servicii de formare pentru securitate cibernetică, precum și confidențialitatea informațiilor furnizate de către aceștia.

Informațiile prelucrate în sensul îndeplinirii obligațiilor de la art. 32 și art. 33 din Legea nr. 362/2018, cu modificările și completările ulterioare, nu fac parte din categoria informațiilor de interes public așa cum acestea sunt reglementate în Legea nr. 544/2001 privind liberul acces la informațiile de interes public, cu modificările și completările ulterioare.

CERERE DE REÎNNOIRE
autorizație furnizor de servicii de formare pentru securitate cibernetică

A. DATE DE IDENTIFICARE FURNIZOR DE SERVICII DE FORMARE:															
DENUMIREA: 															
Cod unic identificare (IDFSF) <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 10%;">Q</td> <td style="width: 10%;">E</td> <td style="width: 10%;">-</td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> <td style="width: 10%;"></td> </tr> </table>					Q	E	-								
Q	E	-													
Adresă corespondență Strada: Nr. Bl./Clădire Sc. Ap./Cam. 															
Localitatea: Cod poștal: Județul/Municipiul: Sector: 															
E-mail: 															
B. SOLICITARE															
În temeiul <i>Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice</i> , cu modificările și completările ulterioare, În baza Normelor privind autorizarea furnizorilor de servicii de formare pentru securitate cibernetică, aprobate prin Ordinul directorului DNSC nr. R/106/2022, Solicit reînnoirea autorizației de furnizor de servicii de formare pentru securitate cibernetică ☐															
Tipul de program de formare de reînnoit: Auditori de securitate cibernetică ☐ Membrii echipelor CSIRT ☐ Responsabili NIS ☐															
C. ACORD PRELUCRARE DATE⁴															
Îmi exprim acordul cu privire la prelucrarea datelor cu caracter personal și procesarea electronică a datelor de către DNSC, în calitate de autoritate competentă la nivel național pentru securitatea rețelelor și sistemelor informatice, în procesul de implementare și monitorizare a Legii nr. 362/2018, cu modificările și completările ulterioare. ☐ Da															
D. CONFORMITATEA CU ORIGINALUL A DOCUMENTELOR FURNIZATE															
Confirm că toate documentele furnizate, în copie, sunt „conform cu originalul” . ☐ Da															
Anexe: Dosarul de reautorizare.															

Semnătură/Reprezentant legal

Nume și prenume:

Data:

Semnătura:

⁴ În procesele interne, DNSC protejează interesele de securitate și comerciale ale furnizorilor de servicii de formare pentru securitate cibernetică, precum și confidențialitatea informațiilor furnizate de către aceștia. Informațiile prelucrate în sensul îndeplinirii obligațiilor de la art. 32 și art. 33 din Legea nr. 362/2018 nu fac parte din categoria informațiilor de interes public așa cum acestea sunt reglementate în Legea nr. 544/2001 privind liberul acces la informațiile de interes public, cu modificările și completările ulterioare.

LISTA

Programelor de formare pentru securitate cibernetică desfășurate pe perioada de valabilitate a autorizației⁵

Activitate de formare desfășurată: ☐ [ASC] / ☐ [CSIRT] / ☐ [NIS]

Perioada – de la data de:/...../20....

la data de:/...../20....

Secțiunea 1. Furnizorul de servicii de formare

1. Furnizor servicii de formare: / IDFSF:
(denumire PJ)

Nr. crt.	Forma de pregătire	Anul	Perioadă		Participanți		Activități de formare		
			Zile	Ore	Înscriși	Absolvenți	ASC	CSIRT	NIS
0	1	2	3	4	5	6	7	8	9
1.	Programe de formare inițială	20...	21	168	200	179	x	x	x
2.	Programe de formare continuă		10	20	57	57		x	
Subtotal Anul 20...			$\sum_{i=1}^n (Ca3)$	$\sum_{i=1}^n (Ca4)$	$\sum_{i=1}^n (Ca5)$	$\sum_{i=1}^n (Ca6)$			
1.	Programe de formare inițială	20...	21	168	200	179	x	x	x
2.	Programe de formare continuă		10	20	57	57	x	x	
Subtotal Anul 20...			$\sum_{i=1}^n (Cb3)$	$\sum_{i=1}^n (Cb4)$	$\sum_{i=1}^n (Cb5)$	$\sum_{i=1}^n (Cb6)$			
1.	Programe de formare inițială								
2.	Programe de formare continuă								
TOTAL GENERAL		-	$\sum_{i=1}^n (C.3)$	$\sum_{i=1}^n (C.4)$	$\sum_{i=1}^n (C.5)$	$\sum_{i=1}^n (C.6)$			

Secțiunea 2. Formatori⁶

1. Formator:
(numele/prenumele)

Nr. crt.	Forma de pregătire	Teme/programe		Activități de formare		
		Număr	Ore	ASC	CSIRT	NIS
0	1	3	4	7	8	9
1.	Programe de formare inițială	7	14	x	x	x
2.	Programe de formare continuă	3	6		x	
SITUAȚIE GENERALĂ		$\sum_{i=1}^n (Cf3)$	$\sum_{i=1}^n (Cf4)$			

⁵ Perioada de valabilitate a autorizației – perioada cuprinsă între data emiterii autorizației și până la data solicitării reînnoirii autorizației.

⁶ Se completează pentru fiecare formator – câte un tabel.



DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ
DIRECȚIA GENERALĂ REGLEMENTARE ȘI CONTROL
DIRECȚIA ATESTARE ȘI AUTORIZARE

DECIZIE DE SUSPENDARE

a autorizației de furnizare de servicii de formare pentru securitate cibernetică
 nr. / din

În aplicarea dispozițiilor art. 32 alin. (2) lit. e) și art. 33 alin. (2) lit. e) din Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cu modificările și completările ulterioare,

în temeiul prevederilor art. 16 din Normele privind autorizarea formatorilor și furnizorilor de servicii de formare pentru securitate cibernetică, aprobate prin Ordinul directorului Directoratului Național de Securitate Cibernetică nr. 106/2022,

în baza Notei de constatare/control nr. ... / / întocmită de Direcția verificare și control din cadrul Direcției generale reglementare și control,

Directoratul Național de Securitate Cibernetică, în calitate de autoritate competentă la nivel național pentru securitatea rețelelor și sistemelor informatice, emite următoarea decizie de suspendare.

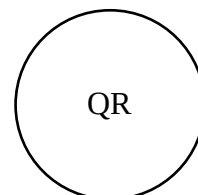
Art. 1. – Începând cu data de / / se suspendă autorizația de furnizare de servicii de formare pentru securitate cibernetică seria nr. din ... / / emisă pentru: – cu sediul în localitatea, județul, str., nr., CP; CUI/CIF:; cod unic de identificare IDFSF: QE-.....

Art. 2. – Perioada de suspendare este de o lună de la data emiterii deciziei, cu excepția cazului în care furnizorul de servicii de formare pentru securitate cibernetică a remediat deficiențele constatate și validate de către DNSC dată de la care autorizația redevine valabilă.

Art. 3. – Suspendarea autorizației se înscrie în Registrul național al furnizorilor de servicii de formare pentru securitate cibernetică, se actualizează lista furnizorilor de servicii de formare pentru securitate cibernetică și se publică pe site-ul instituției.

Art. 4. – Decizia se comunică furnizorului de servicii de formare pentru securitate cibernetică.

.....
Directorul DNSC



(Verso Decizie)

AVIZE

.....

Adjunctul directorului DNSC

.....

Managerul superior DGRC

.....

Managerul DAA

Decizia a fost emisă la data de și a fost înscrisă în RENFOSEC la poziția ...

ANEXA nr. 7 la norme

Registrul național al furnizorilor de servicii de formare pentru securitate cibernetică (RENFOSEC)

Nr. crt.	Date despre furnizorul de servicii de formare						Programul de formare			Date autorizare DNSC				Observații
	Date identificare				Reprezentant legal		Auditori	CSIRT	Responsabili NIS	Date autorizație				
	Denumire	CUI	Adresa	IDFSF	Nume și prenume	Funcția				Seria	Număr	Valabilitatea	Stare	
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1														
...														

PROGRAMA DE PREGĂTIRETIP DE FORMARE: ☐ Auditori securitate cibernetică / ☐ Membri CSIRT / ☐ Responsabili NIS

Durata de pregătire (în ore):

Total, din care: - instruire practică
 - instruire teoretică

Nr. crt.	Nivel de specializare	Competențe specifice	Conținut tematic	Metode/ forme de activitate	Mijloace de instruire, materiale de învățare	Criterii de performanță
1	2	3	4	5	6	7

LISTA TEMELOR

Nr. crt.	Titlu temă	Metoda de predare	Durata [ore]	Mijloace de instruire, materiale de învățare	Formator
1	2	3	4	5	6
1	Noțiuni introductive ...	Teoretică	2		

TEMELE

TEMA NR.

Durata (în ore):

Obiective generale:

Tipul temei:

Conținutul temei: **Tema1.pdf** (se atașează la Programa de pregătire)



DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ
DIRECȚIA GENERALĂ REGLEMENTARE ȘI CONTROL
DIRECȚIA ATESTARE ȘI AUTORIZARE

CERTIFICAT DE SPECIALIZARE
PENTRU SECURITATE CIBERNETICĂ
seria nr. din

TIP PROGRAM DE FORMARE:

☐ *Auditori securitate cibernetică* / ☐ *Membri CSIRT* / ☐ *Responsabili NIS*

DI./Dna

CNP, născut (ă) în anul luna ziua, în localitatea, județul

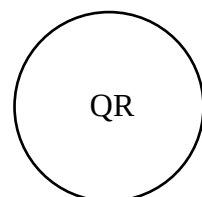
a participat la programul de formare inițială pentru securitate cibernetică
desfășurat în perioada, cu durata de ore, organizat de,
cu sediul în localitatea, județul, înscris în Registrul național al
furnizorilor de servicii de formare pentru securitate cibernetică / IDFSF: QE-.....,

a promovat examenul de finalizare în anul luna ziua, cu media,
obținând recunoașterea și specializarea de a profesa ca

Prezentul certificat se eliberează în baza Normelor privind autorizarea furnizorilor de servicii
de formare pentru securitate cibernetică, aprobate prin Ordinul directorului Directoratului
Național de Securitate Cibernetică nr. 106/2022.

Certificatul se utilizează în condițiile Legii nr. 362/2018 privind asigurarea unui nivel comun
ridicat de securitate a rețelelor și sistemelor informatice, cu modificările și completările
ulterioare, și a actelor subsecvente acesteia.

.....
Directorul DNSC



(Verso Certificat)

AVIZE

.....
Adjunctul directorului DNSC

.....
Managerul superior DGRC

.....
Managerul DAA

.....
Reprezentantul legal FSF

.....
Președintele Comisiei de examen

.....
Secretarul Comisiei de examen

Certificatul a fost emis la data de și a fost înscris în Registrul electronic național de evidență a certificatelor pentru securitate cibernetică (RENECSC) a poziția ...

**Registrul național de evidență a certificatelor pentru securitate cibernetică
(RENECSC)**

Nr. crt.	Date posesor			Date certificat						Organizator (IDFSF)	Obs.
	Nume	Prenume	CNP	Seria	Număr	Tip	Data emiterii	Stare	Activitate evaluată		
0	1	2	3	4	5	6	7	8	9	10	11
1											
...											

SITUAȚIA

programelor de formare pentru securitate cibernetică desfășurate în anul ...

Activitate de formare desfășurată⁷: ☐ [ASC] / ☐ [CSIRT] / ☐ [NIS]

Furnizor de servicii de formare: / IDFSF:
.....

(Denumire PJ)

Tabel 1. Nivel de specializare⁸: ☐ [pregătire inițială] / ☐ [pregătire continuă]

Nr. crt.	Programul	Perioada	Zile / ore	Taxă școlarizare (mii lei)	Date participanți			Probleme/Nereguli constatate
					Inițial	Absolvit	Procent	
0	1	2	3	4	5	6	7	8
1.	Pregătire inițială ASC	10.03.2022 – 14.03.2022	5/ 20	10	15	12	80%	1).. 2)...
...	...							
n.	...							
Situație centralizatoare								
TOTAL		-	$\sum_{i=1}^n (C3)$	$\sum_{i=1}^n (C4)$	$\sum_{i=1}^n (C5)$	$\sum_{i=1}^n (C6)$	...%	-

⁷ Se va întocmi câte o situație pentru fiecare activitate de formare, respectiv pentru formarea auditorilor de securitate cibernetică, formarea membrilor echipelor CSIRT și formarea responsabililor NIS.

⁸ Se va întocmi câte un tabel, individual, pentru fiecare nivel de specializare (inițială sau continuă).

CERERE SOLICITARE
participare la examinare/evaluare în domeniul auditului de securitate cibernetică

A. DATE DE IDENTIFICARE SOLICITANT**Date personale solicitant**

Prenumele

Numele

CNP

Domiciliu

Strada:

Nr.

Bl./Clădire

Sc.

Ap./Cam.

Localitatea:

Cod poștal:

Județul/Municipiul:

Sector:

Nr. telefon fix

Nr. mobil

E-mail:

Adresă corespondență⁹

Strada:

Nr.

Bl./Clădire

Sc.

Ap./Cam.

Localitatea:

Cod poștal:

Județul/Municipiul:

Sector:

B. SOLICITARE

În temeiul *Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice*, cu modificările și completările ulterioare,

în baza Normelor privind autorizarea furnizorilor de servicii de formare pentru securitate cibernetică, aprobate prin Ordinul directorului Directoratului Național de Securitate Cibernetică nr. 106/2022,

solicit participare la examinare/evaluare în domeniul auditului de securitate cibernetică ☐

Tipul activității pentru care se solicită examinarea/evaluareaActivități speciale ☐Activități comune ☐**C. ACORD PRELUCRARE DATE¹⁰**

Îmi exprim acordul cu privire la prelucrarea datelor cu caracter personal și procesarea electronică a datelor de către DNSC, în calitate de autoritate competentă la nivel național pentru securitatea rețelelor și sistemelor informatice, în procesul de implementare și monitorizare a Legii nr. 362/2018, cu modificările și completările ulterioare,

☐ Da

⁹ Se va completa numai dacă diferă de domiciliu solicitantului.

¹⁰ În procesele interne, DNSC protejează interesele de securitate ale persoanelor care solicită participarea la examinare/evaluare, precum și confidențialitatea informațiilor furnizate de către aceștia.

Informațiile prelucrate în sensul îndeplinirii obligațiilor de la art. 32 și art. 33 din Legea nr. 362/2018, cu modificările și completările ulterioare, nu fac parte din categoria informațiilor de interes public așa cum acestea sunt reglementate în Legea nr. 544/2001 privind liberul acces la informațiile de interes public, cu modificările și completările ulterioare.

D. CONFORMITATEA CU ORIGINALUL A DOCUMENTELOR FURNIZATE

Confirm că toate documentele furnizate, în copie, sunt „conform cu originalul” .

☐ Da

Anexe:

... (documentele precizate la art. 25 alin. (3) din Normele privind autorizarea și verificarea furnizorilor de servicii de formare pentru securitate cibernetică, aprobate prin Ordinul directorului Directoratului Național de Securitate Cibernetică nr. 106/2022)

Semnătură/Solicitant

Nume și prenume:

Data:

Semnătura:



DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ
DIRECȚIA GENERALĂ REGLEMENTARE ȘI CONTROL
DIRECȚIA ATESTARE ȘI AUTORIZARE

CERTIFICAT DE EVALUARE
EXPERTIZĂ PRIVIND SECURITATEA CIBERNETICĂ

seria nr. din

DI./Dna,

CNP, născut (ă) în anul luna ziua, în localitatea, județul,

a participat la activitatea de examinare/evaluare în domeniul auditului de securitate cibernetică, organizată de Directoratul Național de Securitate Cibernetică,

a promovat examenul în anul luna ziua, cu media,

obținând certificarea în vederea atestării ca auditor de securitate cibernetică.

Prezentul certificat se eliberează în baza Normelor privind autorizarea furnizorilor de servicii de formare pentru securitate cibernetică, aprobate prin Ordinul directorului Directoratului Național de Securitate Cibernetică nr. 106/2022.

Certificatul se utilizează în condițiile Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cu modificările și completările ulterioare, și a actelor subsecvente acestora. Documentul ține locul de certificare profesională și este recunoscut numai la nivelul autorității competente la nivel național.

.....
Directorul DNSC

QR

(Verso Certificat)

AVIZE

.....
Adjunctul directorului DNSC

.....
Managerul superior DGRC

.....
Managerul DAA

.....
Reprezentantul legal FSF

.....
Președintele Comisiei de
examen

.....
Secretarul Comisiei de examen

*Certificatul a fost emis la data de și a fost înscris în Registrul național de evidență a
certificatelor pentru securitate cibernetică (RENECSC) a poziția ...*