



Responsabil cu Securitatea Rețelelor și Sistemelor Informatice (Responsabil NIS)

Autorizat D.N.S.C.

Curs autorizat de Directoratul Național de Securitate Cibernetică (D.N.S.C.), desfășurat online, prin intermediul aplicației **Zoom**



Examinarea se va desfășura online și va consta într-un test grilă (derulat pe platforma de e-Learning APSAP) și o probă practică (pregătire + prezentare proiect)



Cerință obligatorie pentru a primi Certificatul de Specializare emis de DNSC: Studii medii, cu sau fără Diplomă de Bacalaureat



Grupul țintă vizat: Profesioniști sau persoane care aspiră să se angajeze în domeniu, fiind oferită o bază solidă de cunoștințe și competențe practice



După finalizarea cursului, participanții care îndeplinesc condițiile de studii minime, vor susține un examen online, prin care vor fi testate cunoștințele și abilitățile dobândite pe parcursul instruirii.

În urma promovării examenului, participanții vor dobândi Certificatul de Specializare emis de Directoratul Național de Securitate Cibernetică (D.N.S.C.). autenticității educației primite.



Pentru mai multe detalii, vă invităm să vizitați: www.apsap.ro



LECTORI



Cătălin OPRAN

Formator autorizat D.N.S.C., Specialist în Securitate Cibernetică Civilă și Militară,
Expert în Protecția Infrastructurilor Informatice Critice cu peste 20 de ani de experiență în domeniile: IT, NIS și INFOSEC



Sorin MUREȘAN

Formator autorizat DNSC și expert în securitate cibernetică și conformitate NIS 2,
Sorin Mureșan are peste 30 de ani de experiență în IT, telecomunicații și digitalizare publică.

A ocupat funcții tehnice și de management, coordonând proiecte de e-guvernare și modernizare a serviciilor publice în cadrul administrației centrale, cu impact inclusiv în domeniul securității cibernetice.



BENEFICII



BENEFICIILE PARTICIPĂRII LA CURS

► **Suport de curs și materiale auxiliare** - vă oferim materiale de învățare bine structurate și ușor de urmărit, care acoperă toate aspectele esențiale ale cursului. Acestea sunt concepute de lectori, adaptate și actualizate, pentru a facilita înțelegerea noțiunilor predate. Pe lângă suportul de curs principal, veți avea acces la o varietate de materiale suplimentare, inclusiv studii de caz, legislație sau modele de lucru, care vor îmbogăți experiența dumneavoastră de învățare.

► **Îndrumări din partea formatorilor** - lectorii vă vor oferi îndrumări personalizate, sfaturi și clarificări pe tot parcursul programului de curs. Această interacțiune directă, live, vă va ajuta să navigați prin complexitatea subiectului și să vă dezvoltați cunoștințele.

► **Sesiuni de întrebări și răspunsuri** - organizăm sesiuni interactive de întrebări și răspunsuri, unde puteți clarifica orice nelămuriri și puteți discuta subiectele cursului cu formatorii și colegii de curs.

► **Modul special pentru pregătirea susținerii examenului de absolvire** - pentru a vă asigura că sunteți bine pregătiți pentru examenul final, oferim un modul dedicat pregătirii acestuia. Acesta include sfaturi pentru examen, simulări de teste și strategii de studiu eficiente.

► **Dezvoltarea competențelor și cunoștințelor** - cursul vă permite îmbunătățirea și actualizarea competențelor, sporind astfel performanța și generând noi oportunități în carieră.

► **Flexibilitatea** - desfășurându-se online, cursul vă oferă flexibilitatea de a învăța în propriul ritm, din confortul propriei case și de a vă organiza studiul în jurul altor angajamente, precum munca sau familia.

► **Recunoaștere oficială și echivalare europeană** - Cursul se finalizează printr-o sesiune de evaluare, în vederea obținerii Certificatului de Specializare, acreditat de Directoratul Național pentru Securitate Cibernetică (DNSC). Evaluarea vizează atât cunoștințele teoretice, cât și competențele practice dobândite pe parcursul programului.

Pentru recunoașterea internațională, certificatele obținute în România pot fi apostilate (pentru statele semnatare ale Convenției de la Haga) sau supralegalizate (pentru statele nesemnatare).

► **Networking și colaborare** - deși este online, cursul oferă posibilități de a interacționa cu alți cursanți și cu lectorii, facilitând schimbul de idei și construirea unei rețele profesionale.

► **Costuri reduse** - cursul online este mai accesibil din punct de vedere financiar decât cel tradițional, fiind eliminate costurile asociate cu deplasarea.

► **Îmbunătățirea CV-ului** - finalizarea unui curs autorizat va adăuga valoare CV-ului dumneavoastră, demonstrând angajatorilor că sunteți dedicat învățării continue și dezvoltării profesionale.

► **Încredere sporită** - dobândirea de noi abilități și cunoștințe va crește încrederea în sine și va deschide ușa spre noi provocări și oportunități în carieră.

Obținerea unei noi calificări reprezintă un pas esențial spre revitalizarea și îmbunătățirea carierei dumneavoastră profesionale. Acest proces nu numai că vă va aduce un suflu nou de energie și motivație, dar vă va și deschide uși către noi posibilități și perspective în domeniul ales. Indiferent de obiectivul dumneavoastră - fie că aspirați să explorați noi orizonturi în carieră sau doriți să vă solidificați și să vă extindeți cunoștințele și abilitățile în cadrul rolului actual - Centrul de Formare APSAP este aici pentru a vă susține în această călătorie.

TEMATICĂ



TEMATICĂ ABORDATĂ

● Modulul 1:

Cadrul legal și instituțional al securității cibernetice

- concepte și terminologie în domeniul securității cibernetice conform cadrului NIS2
- cadrul legislativ european și național privind securitatea cibernetică
- rolul și atribuțiile Directoratului Național de Securitate Cibernetică (DNSC)
- atribuțiile autorităților și instituțiilor cu responsabilități în domeniul securității și apărării cibernetice
- mecanismele de cooperare instituțională și schimbul de informații în domeniul securității cibernetice
- mecanismele europene de cooperare și rolul ENISA în consolidarea rezilienței cibernetice

● Modulul 2:

Clasificarea entităților și obligațiile aplicabile

- clasificarea entităților esențiale și entităților importante
- criterii de încadrare și domeniul de aplicare al cadrului normativ
- sectoare reglementate și responsabilitățile specifice entităților
- determinarea impactului perturbator semnificativ asupra serviciilor
- registrul entităților și actualizarea informațiilor relevante

● Modulul 3:

Managementul riscurilor de securitate cibernetică

- evaluarea și analiza riscurilor la nivelul entității
- măsuri tehnice și organizatorice pentru gestionarea riscurilor de securitate cibernetică
- cerințe minime de securitate privind protecția sistemelor informatice
- politici de criptografie, jurnalizare și trasabilitate
- gestionarea vulnerabilităților și monitorizarea continuă a securității
- metodologia de evaluare a nivelului de risc și criteriile de determinare a impactului serviciilor

● Modulul 4:

Securitatea lanțului de aprovizionare

- evaluarea și selecția furnizorilor de servicii TIC
- riscurile de securitate asociate lanțului de aprovizionare
- cerințe contractuale și clauze de securitate pentru furnizori
- transparența și trasabilitatea relațiilor cu terții
- gestionarea incidentelor de securitate în lanțul de aprovizionare

● Modulul 5:

Notificarea și gestionarea incidentelor de securitate cibernetică

- identificarea și clasificarea incidentelor de securitate cibernetică
- obligațiile de raportare și notificare a incidentelor către autoritatea competentă
- utilizarea mecanismelor naționale de notificare a incidentelor (PNRISC)
- termenele legale de notificare și raportare a incidentelor
- analiza incidentelor și comunicarea cu autoritățile competente și utilizatorii afectați
- cooperarea cu echipele de răspuns la incidente (CSIRT)

● Modulul 6:

Guvernanța securității cibernetice și responsabilitățile conducerii

- responsabilitățile legale ale organelor de conducere în domeniul securității cibernetice
- desemnarea și rolul Responsabilului pentru securitatea rețelor și sistemelor informatice în cadrul organizației
- integrarea securității cibernetice în managementul organizațional
- evaluarea maturității cibernetice și monitorizarea conformității
- auditul de securitate cibernetică și evaluarea internă a conformității

● Modulul 7:

Supravegherea, controlul și regimul sancționator

- mecanismele de supraveghere, verificare și control exercitate de DNSC
- desfășurarea inspecțiilor și obligațiile entităților în cadrul controalelor
- regimul sancționator aplicabil entităților esențiale și entităților importante
- măsuri corective și proceduri de conformare
- pregătirea organizațiilor pentru verificări și audituri de conformitate

● Modulul 8:

Studii de caz și exerciții practice

- studii de caz privind implementarea cerințelor cadrului normativ în organizații
- exerciții practice privind evaluarea riscurilor de securitate cibernetică
- simulări privind notificarea incidentelor și utilizarea platformei PNRISC
- scenarii privind cooperarea cu autoritatea competentă și echipele CSIRT
- bune practici în implementarea măsurilor de securitate cibernetică

Cadrul normativ de referință include, fără a se limita la:

- Directiva (UE) 2022/2555 – NIS2, care stabilește măsuri pentru asigurarea unui nivel comun ridicat de securitate cibernetică în Uniunea Europeană și consolidează cooperarea între statele membre în domeniul securității rețelelor și sistemelor informatice
- OUG nr. 155/2024 privind instituirea cadrului pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, care stabilește obligațiile entităților esențiale și importante privind gestionarea riscurilor, raportarea incidentelor și cooperarea cu autoritatea competentă
- Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, care reglementează organizarea și funcționarea sistemului național de securitate cibernetică și stabilește responsabilitățile instituțiilor și mecanismele de cooperare în domeniu
- OUG nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică (DNSC), care stabilește rolul și atribuțiile autorității competente în domeniul securității cibernetice
- Ordinul Directorului DNSC nr. 1/2025 pentru aprobarea Cerințelor privind procesul de notificare în vederea înregistrării și metoda de transmitere a informațiilor
- Ordinul Directorului DNSC nr. 2/2025 pentru aprobarea Criteriilor și pragurilor de determinare a gradului de perturbare a unui serviciu și a Metodologiei privind evaluarea nivelului de risc al entităților
- Ordinul Directorului DNSC nr. 3/2025 pentru aprobarea Normelor de aplicare a dispozițiilor privind supravegherea, verificarea și controlul respectării prevederilor Ordonanței de urgență a Guvernului nr. 155/2024

Acest cadru legislativ definește obligațiile organizațiilor privind gestionarea riscurilor de securitate cibernetică, raportarea incidentelor, cooperarea instituțională și implementarea măsurilor necesare pentru asigurarea rezilienței infrastructurilor digitale.

COMPETENȚE

COMPETENȚE OBȚINUTE:

► **Înțelegerea cadrului legislativ în domeniul securității cibernetice:**

interpretarea și aplicarea cerințelor Directivei NIS2 și ale legislației naționale privind securitatea cibernetică.

► **Identificarea entităților reglementate:**

clasificarea entităților esențiale și importante și analizarea obligațiilor legale care le revin.

► **Analiza riscurilor de securitate cibernetică:**

evaluarea amenințărilor, vulnerabilităților și impactului potențial asupra serviciilor furnizate.

► **Implementarea măsurilor de gestionare a riscurilor:**

aplicarea măsurilor tehnice și organizatorice necesare pentru protejarea rețelelor și sistemelor informatice.

► **Gestionarea securității lanțului de aprovizionare:**

evaluarea riscurilor asociate furnizorilor de servicii TIC și definirea cerințelor de securitate aplicabile.

► **Gestionarea incidentelor de securitate cibernetică:**

identificarea, clasificarea și analiza incidentelor de securitate cibernetică la nivel organizațional.

► **Raportarea incidentelor către autorități:**

utilizarea mecanismelor de notificare și raportare, inclusiv platforma PNRISC.

► **Gubernanța securității cibernetice:**

integrarea cerințelor de securitate cibernetică în procesele de management și responsabilitățile conducerii organizației.

► **Evaluarea conformității organizaționale:**

analizarea nivelului de conformitate cu cerințele cadrului normativ privind securitatea cibernetică.

► **Pregătirea pentru controale și verificări:**

aplicarea procedurilor necesare pentru cooperarea cu autoritățile competente și implementarea măsurilor corective.

► **Aplicarea practică a cerințelor de securitate cibernetică:**

utilizarea studiilor de caz și a exercițiilor practice pentru evaluarea riscurilor și gestionarea incidentelor.



INFO



Informații suplimentare

După finalizarea cursului și promovarea examenului, participanții vor primi **Certificatul de Specializare** emis de Directoratul Național de Securitate Cibernetică (D.N.S.C.).

Pentru mai multe detalii, vă invităm să vizitați: www.apsap.ro



DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ



Actele necesare:

- **Ultima diplomă de studii obținută** (copie)
- **Act de identitate** (copie)
- **Certificat de naștere** (copie)
- **Certificat de căsătorie**, în cazul schimbării numelui (copie)

Recunoașterea internațională a Certificatului de Absolvire

Pentru recunoașterea internațională a certificatelor obținute în România este necesară apostilarea (țări semnatare ale Convenției de la Haga) sau supralegalizarea (țări nesemnatare ale Convenției de la Haga).

Detalii privind tematicile cursurilor, organizarea și desfășurarea programelor de perfecționare se pot obține apelând numărul de telefon:

0788 124 567



Detalii tehnice

Cursul este conceput pentru a fi accesibil și interactiv, utilizând un format audio-video live, online. Pentru a vă asigura că aveți cea mai bună experiență posibilă și puteți participa activ la sesiunile cursului, este important ca fiecare participant să îndeplinească următoarele cerințe tehnice:

1. Să utilizeze un dispozitiv electronic adecvat:

fiecare participant trebuie să dețină un dispozitiv electronic, fie că este vorba de un calculator sau un telefon mobil, care să fie capabil să ruleze aplicația Zoom și să suporte streaming video. Este esențial ca dispozitivul să aibă o performanță tehnică suficientă pentru a asigura o experiență de învățare fără întreruperi.

2. Să dețină o conexiune stabilă la Internet:

o conexiune bună la Internet este crucială pentru a putea accesa cursul online fără probleme tehnice. Vă recomandăm să verificați viteza conexiunii de Internet înainte de începerea cursului și să vă asigurați că aveți o conexiune stabilă și suficient de rapidă pentru streaming video.

3. Să dețină un microfon și o cameră web funcționale:

pentru a facilita interacțiunea și comunicarea eficientă în timpul sesiunilor live, fiecare participant trebuie să aibă un microfon funcțional și o cameră web. Acestea vă vor permite să participați la discuții și să interacționați cu formatorii și cu ceilalți cursanți.

4. Să descarce aplicația Zoom (gratuit):

este esențial ca fiecare participant să descarce aplicația Zoom pe dispozitivul de pe care intenționează să acceseze cursul on-line. Zoom este o platformă user-friendly și ușor de utilizat, care permite desfășurarea cursurilor live într-un mod eficient. Vă recomandăm să instalați aplicația și să vă familiarizați cu funcțiile acesteia înainte de începerea cursului.

Respectând aceste cerințe, veți putea beneficia la maximum de experiența cursului nostru online și vă veți asigura că participarea dumneavoastră la sesiunile live va fi eficientă și plăcută.



Minister