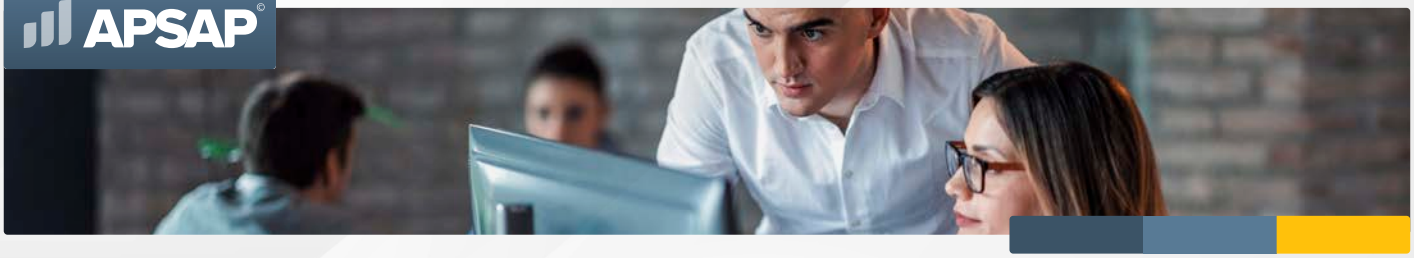
CENTRUL DE FORMARE APSAP

OFERTĂ



MEMBRU ECHIPĂ CSIRT
Cyber Security Incident Response Team

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)

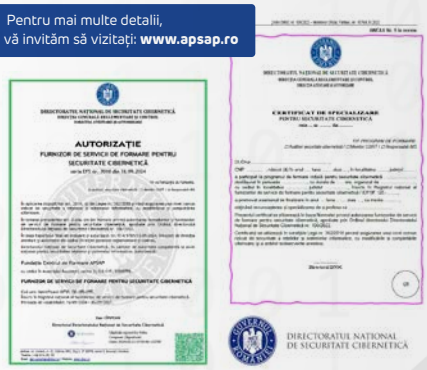
Cerință obligatorie pentru a primi Certificatul de Specializare emis de DNSC: Studii superioare, dovedite prin Diplomă de Licență

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.).

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

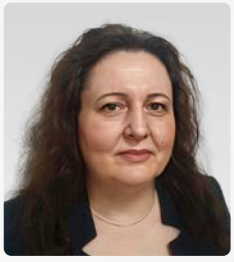


LECTORI

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

Cu o experiență de peste 20 de ani în administrarea sistemelor informatice civile și militare și a infrastructurilor de rețea, domnul Opran este un practician cu expertiză solidă în domeniul securității cibernetice.



Crina NEGOESCU

Formator și Auditor atestat DNSC, Responsabil NIS2 și DPO, cu peste 20 ani de expertiză IT&C

Activitatea sa acoperă proiectarea sistemelor, administrarea securității, acreditarea infrastructurilor critice și a sistemelor interoperabile cu nivel ridicat de securitate, cu responsabilități în controlul și auditul acestora.

Doamna Negoescu deține o expertiză solidă în managementul riscurilor, elaborarea politicilor de securitate, continuitatea activității, răspunsul la incidente, analiza jurnalelor de audit, protecția datelor și guvernanța IT, în conformitate cu standardele ISO/IEC 27001, NIST, COBIT și Common Criteria.

TEL: 0788 124 567 | **FAX:** 021/ 569 61 26

APSAP E-LEARNING

ZOOM

CENTRUL DE FORMARE APSAP

MEMBRU ECHIPĂ CSIRT
(AUTORIZAT D.N.S.C.)

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.

CENTRUL DE FORMARE APSAP

MEMBRU ECHIPĂ CSIRT
(AUTORIZAT D.N.S.C.)

TEMATICĂ

TEMATICĂ ABORDATĂ

● **Modul 1**
Cadrul legislativ și instituțional

Rolul DNSC, atribuțiile autorităților, cooperarea interinstituțională, obligațiile entităților esențiale și importante, mecanisme de control și regim sancționator, conform OUG nr. 104/2021, Legea nr. 58/2023 și OUG nr. 155/2024.

● **Modul 2**
Alerte și avertizări de securitate cibernetică

Identificare, clasificare, prioritizare și modul de acțiune. Fluxuri de notificare și utilizarea mecanismelor naționale (PNRISC), în conformitate cu obligațiile de raportare.

● **Modul 3**
Managementul vulnerabilităților

Identificare, analiză, evaluare și răspuns la vulnerabilități, corelat cu cerințele de gestionare a riscurilor de securitate cibernetică.

● **Modul 4 —**
Coordonarea răspunsului la vulnerabilități

Procese, roluri și responsabilități în cadrul entităților esențiale și importante. Colaborare instituțională și comunicare în timpul crizelor.

● **Modul 5 — Analiza incidentelor de securitate cibernetică**

Metode, tehnici și instrumente utilizate în investigare și răspuns. Identificarea cauzei principale și a vectorilor de atac.

● **Modul 6**
Măsuri de securitate și cerințe minime

Implementarea și evaluarea controalelor de securitate pentru rețele și sisteme informatice, conform cerințelor legale actuale.

● **Modul 7**
Detectarea intruziunilor

Tehnologii, soluții și bune practici pentru monitorizare, detecție și prevenție a activităților malițioase.

● **Modul 8**
Gestionarea artefactelor

Colectare, analiză, corelare și utilizare a artefactelor digitale (inclusiv indicatori de compromitere) în procesul de răspuns la incidente.

● **Modul 9**
Continuitatea operațională și recuperarea

Asigurarea reziliență organizaționale, planuri de continuitate și recuperare în urma incidentelor cibernetice.

● **Modul 10**
Platforme de schimb de informații (MISP)

Utilizare operațională și colaborare cu CSIRT național și alte entități relevante la nivel european.

● **Modul 11**
Evaluarea impactului incidentelor

Determinarea nivelului de perturbare a serviciilor și analiza consecințelor asupra entităților. Evaluarea dinamică a riscurilor conform Ordinului DNSC nr. 2/2025.

● **Modul 12**
Analiza riscurilor de securitate cibernetică

Evaluare dinamică a riscurilor la nivelul entităților esențiale și importante, conform metodologiilor actuale și standardelor internaționale.

● **Modul 13**
Procesul de notificare a incidentelor

Identificare, documentare, raportare și fluxuri de comunicare conform cerințelor legale (alertă timpurie în 24h, notificare completă în 72h).

CENTRUL DE FORMARE APSAP

MEMBRU ECHIPĂ CSIRT
(AUTORIZAT D.N.S.C.)

COMPETENȚE

COMPETENȚE OBȚINUTE:

▸ 1. Gestionarea alertelor și avertizărilor

Capacitatea de a recepționa, clasifica și gestiona alerte și avertizări de securitate cibernetică, conform procedurilor operaționale CSIRT și cerințelor de notificare.

▸ 2. Managementul vulnerabilităților

Abilitatea de a identifica, analiza și prioritiza vulnerabilități de securitate, precum și de a propune și urmări implementarea măsurilor de remediere.

▸ 3. Coordonarea răspunsului la incidente

Competența de a participa la coordonarea răspunsului la incidente și vulnerabilități, în colaborare cu echipe tehnice, management și autorități competente.

▸ 4. Analiza tehnică a incidentelor

Capacitatea de a efectua analiza tehnică a incidentelor de securitate cibernetică, inclusiv identificarea cauzei principale și a vectorilor de atac.

▸ 5. Implementarea măsurilor de securitate

Abilitatea de a implementa și evalua măsuri și controale de securitate pentru rețele și sisteme informatice, conform cerințelor legale aplicabile.

▸ 6. Detecția intruziunilor

Competența de a utiliza soluții de detectare a intruziunilor și instrumente de monitorizare pentru identificarea și investigarea activităților malițioase.

▸ 7. Gestionarea artefactelor digitale

Capacitatea de a colecta, analiza și gestiona artefacte digitale (inclusiv indicatori de compromitere) în procesul de răspuns la incidente.

▸ 8. Continuitate operațională și recuperare

Abilitatea de a contribui la asigurarea continuității operaționale și la recuperarea sistemelor și datelor în urma incidentelor cibernetice.

▸ 9. Threat Intelligence și colaborare

Competența de a utiliza platforme de tip threat intelligence (ex. MISP) și de a realiza schimb de informații operaționale cu structuri naționale și internaționale.

▸ 10. Evaluarea impactului și analiza riscurilor

Capacitatea de a evalua impactul incidentelor și de a realiza analiza riscurilor de securitate cibernetică la nivelul entității (esențiale sau importante), în conformitate cu cerințele legislative și standardele aplicabile.

▸ 11. Notificarea și raportarea incidentelor

Abilitatea de a întocmi documentația de notificare a incidentelor și de a aplica fluxurile oficiale de raportare către autoritățile competente (DNSC).

▸ 12. Înțelegerea cadrului legislativ

Înțelegerea responsabilităților organizaționale în domeniul securității cibernetice, inclusiv obligațiile privind managementul riscurilor, raportarea incidentelor și conformitatea cu OUG nr. 155/2024.

CENTRUL DE FORMARE APSAP

MEMBRU ECHIPĂ CSIRT
(AUTORIZAT D.N.S.C.)

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**

Actele necesare:

- **Diplomă de Licență**
  sau **Adeverință înlocuitoare valabilă** (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.

APSAP E-LEARNING

zoom