DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

A N U N Ț

Având în vedere:

- Ordonanța de urgență a Guvernului nr. 104 din 22.09.2021 privind înființarea Directoratului Național de Securitate Cibernetică, aprobată prin Legea nr. 11 din 07.01.2022
- Legea nr. 366 din 19.12.2022 pentru modificarea Ordonanței de urgență a Guvernului nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, precum și pentru completarea anexei nr. VIII la Legea-cadru nr. 153/2017 privind salarizarea personalului plătit din fonduri publice
- Ordonanța de urgență nr. 57/2019 privind Codul Administrativ, cu modificările și completările ulterioare
- Prevederile Legii-cadru nr. 153/2017 privind salarizarea personalului plătit din fonduri publice, cu modificările și completările ulterioare
- Prevederile Legii nr. 53/2003 – Codul muncii, republicată cu modificările și completările ulterioare.
- Prevederile Hotărârii de Guvern nr. 1336/2022 pentru aprobarea Regulamentului-cadru privind organizarea și dezvoltarea carierei personalului contractual din sectorul bugetar plătit din fonduri publice

Directoratul Național de Securitate Cibernetică (DNSC sau Directoratul) organizează la sediul său, din București, Strada Italiană nr. 22, Sector 2, un concurs pentru **angajarea unui număr de 12 persoane**, pe perioadă nedeterminată, după cum urmează:

- **Direcția Generală Reglementare și Control**
  - **Coordonator superior securitate cibernetică** – grad Superior, studii superioare, poziție de conducere – **1 post**
  - **Expert securitate cibernetică** – grad Superior, studii superioare, poziție de execuție **- 3 posturi**
  - **Expert securitate cibernetică** – grad Asistent, studii superioare, poziție de execuție **- 1 post**
  - **Expert securitate cibernetică** – grad Debutant, studii superioare, poziție de execuție **- 1 post**
  - **Expert legal politici, standardizare securitate cibernetică** – grad Superior, studii superioare, poziție de execuție **- 2 posturi**
  - **Expert legal politici, standardizare securitate cibernetică** – grad Debutant, studii superioare, poziție de execuție **- 1 post**
  - **Expert dezvoltare, implementare și administrare infrastructuri securitate cibernetică -** grad Superior, studii superioare, poziție de execuție **- 1 post**
  - **Asistent analiză surse deschise, riscuri și amenințări securitate cibernetică** – grad Debutant, studii medii, poziție de execuție – **2 posturi**

Calendarul concursului

Concursul se va desfășura după următorul calendar:

- 18.05.2023, ora 17:00 – Termenul limită pentru depunerea dosarelor de concurs
- 22.05.2023, ora 17:00 - Verificarea și selecția dosarelor depuse de candidați

- 22.05.2023, ora 17:00 – Publicare rezultate selecție dosare
- 23.05.2023, ora 17:00 – Termen limită pentru depunerea contestațiilor privind selecția dosarelor
- 24.05.2023, ora 17:00 – Publicare rezultate contestații privind selecția dosarelor
- 13.06.2023, ora 10:00 – Proba scrisă
- 14.06.2023, ora 17:00 – Publicare rezultate privind proba scrisă
- 15.06.2023, ora 17:00 – Termen limită pentru depunerea contestațiilor privind proba scrisă
- 16.06.2023, ora 17:00 – Publicare rezultate contestații privind proba scrisă
- 22-23.06.2023, ora 09:00 – Proba interviu
    - *Notă: ziua și ora realizării interviului pentru fiecare candidat în parte va depinde de numărul de candidați admiși la interviu și va fi comunicată pe site și afișată la sediul instituției*
- 23.06.2023, ora 17:00 – Publicare rezultate privind proba interviu
- 26.06.2023, ora 17:00 – Termen limită pentru depunerea contestațiilor privind proba interviu
- 27.06.2023, ora 17:00 – Publicare rezultate contestații privind proba interviu
- 27.06.2023, ora 17:00 - Publicarea rezultatelor finale

Proba scrisă și proba interviu se vor desfășura la sediul instituției prin prezența fizică a candidatului în fața comisiei de concurs.

Condiții de participare la concurs

a) Condiții generale (conform art.15 din Regulamentul-cadru aprobat prin HG nr. 1.336/2022, cu modificările și completările ulterioare) şi anume:

- Are cetăţenia română, cetăţenie a altor state membre ale Uniunii Europene sau a statelor aparţinând Spaţiului Economic European (SSE) sau a Confederaţiei Elveţiene şi domiciliul în România.
- Cunoaşte limba română, scris şi vorbit.
- Are capacitate de muncă în conformitate cu prevederile Legii 53/2003 – Codul muncii, republicată, cu modificările și completările ulterioare.
- Are o stare de sănătate corespunzătoare postului pentru care candidează, atestată pe baza adeverinţei medicale eliberate de medicul de familie sau de unităţile sanitare abilitate.
- Îndeplineşte condiţiile de studii şi, după caz, de vechime în specialitate sau alte condiţii specifice potrivit cerinţelor postului scos la concurs.
- Nu a fost condamnată definitiv pentru săvârşirea unei infracţiuni contra umanităţii, contra statului ori contra autorităţii, de serviciu sau în legătură cu serviciul, care împiedică înfăptuirea justiţiei, de fals ori a unor fapte de corupţie sau a unei infracţiuni săvârşite cu intenţie, care ar face-o incompatibilă cu exercitarea funcţiei, cu excepţia situaţiei în care a intervenit reabilitarea.
- Nu execută o pedeapsă complementară prin care i-a fost interzisă exercitarea dreptului de a ocupa funcția, de a exercita profesia sau meseria ori de a desfășura activitatea de care s-a folosit pentru săvârșirea infracțiunii sau față de aceasta nu s-a luat măsura de siguranță a interzicerii ocupării unei funcții sau exercitării unei profesii.

b) Condiții specifice:

- Studii de specialitate (pozițiile #169, #186, #206, #210, #243, #244): studii universitare de licență absolvite cu diplomă, respectiv studii superioare de lungă durată absolvite cu diplomă de licenţă sau echivalentă.

- Studii de specialitate (pozițiile #170, #177, #256): Studii universitare de licență absolvite cu diplomă, respectiv studii superioare de lungă durată, absolvite cu diplomă de licență sau echivalentă, **în domeniul științe juridice**.
- Studii de specialitate (poziția #331): Studii universitare de licență absolvite cu diplomă, respectiv studii superioare de lungă durată, absolvite cu diplomă de licență sau echivalentă în unul/una din domeniile/ramurile/specializările:
    - Matematică, matematică-informatică, statistică
    - Informatică (toate specializările)
    - Știința sistemelor și a calculatoarelor (toate specializările)
    - Fizică
    - Automatică, automatică și informatică industrială
    - Științe inginerești
    - Inginerie electrică, electronică, telecomunicații
    - Ingineria sistemelor, calculatoare și tehnologia informației
    - Ingineria și securitatea sistemelor informatice militare
    - Cibernetică, cibernetică și previziune economică, cibernetică economică, cibernetică și statistică economică, statistică și informatică economică, cibernetică și informatică economică;
    - Calculatoare, tehnică de calcul, tehnologia informatică
    - Ingineria sistemelor și a calculatoarelor (toate specializările)
    - Rețele și software de telecomunicații
    - Tehnologii și sisteme de telecomunicații
- **Studii de specialitate** (pozițiile #338, #339): studii medii absolvite cu diplomă de bacalaureat.
- **Certificări sau cursuri de specializare** – conform fișelor de post publicate.
- **Condiții de vechime:**
    - **#169 Expert securitate cibernetică**
        - **Experiență anterioară dovedită de minim cinci (5) ani** în domeniul reglementare, securitate cibernetică, asigurarea conformității, managementul riscului, audit, sau un domeniu conex, experiență **acumulată în ultimii zece (10) ani**.
        - **Experiență anterioară dovedită de minim doi (2) ani** pentru lucrul în echipe de **minimum trei (3) persoane**.
        - **Reprezintă un avantaj:**
            - **experiența anterioară** de lucru în analiza de impact a reglementarilor (Regulatory **Impact** Assessment - RIA).
            - **experiența anterioară** de lucru într-o instituție guvernamentală sau de reglementare.
            - **experiența anterioară** în reprezentarea sau participarea ca expert în grupuri de lucru, organisme și organizații naționale, regionale, europene, pe domeniul reglementărilor, standardizării sau al securității cibernetice.
    - **#170 Expert legal politici, standardizare securitate cibernetică**
        - **Experiență anterioară dovedită de minim un (1)** an în domeniul juridic, reglementare, securitate cibernetică, asigurarea conformității, managementul riscului, audit, protecția datelor sau un domeniu conex.
        - **Reprezintă un avantaj:**

- experiența anterioară de lucrul în echipe de minimum trei (3) persoane.
- experiența anterioară de lucru în analiza de impact a reglementarilor (Regulatory Impact Assessment - RIA).
- experiența anterioară de lucru în utilizarea platformei online „Fit for Future" a Comisiei Europene.
- experiența anterioară de lucru într-o instituție guvernamentală sau de reglementare de preferință la nivel național sau internațional.
- experiența anterioară în reprezentarea sau participarea ca expert în grupuri de lucru, organisme și organizații naționale, regionale, europene, pe domeniul reglementărilor, standardizării sau al securității cibernetice.
- cunoașterea prevederilor din Better Regulation Guidelines și Better Regulation Toolbox ale Uniunii Europene.

- **#177 Expert legal politici, standardizare securitate cibernetică**
  - **Experiență anterioară dovedită de minim cinci (5) ani** în domeniul juridic, reglementare, securitate cibernetică, asigurarea conformității, managementul riscului, audit, control, protecția datelor sau un domeniu conex, experiență **acumulată în ultimii zece (10) ani**.
  - **Experiență** anterioară **dovedită de minim doi (2) ani** pentru lucrul în echipe de **minimum trei (3) persoane**.
  - **Reprezintă un avantaj:**
    - experiența anterioară de lucrul în echipe de minimum trei (3) persoane.
    - experiența anterioară de lucru în analiza de impact a reglementarilor (Regulatory Impact Assessment - RIA).
    - experiența anterioară de lucru în utilizarea platformei online „Fit for Future" a Comisiei Europene.
    - experiența anterioară de lucru într-o instituție guvernamentală sau de reglementare de preferință la nivel național sau internațional.
    - experiența anterioară în reprezentarea sau participarea ca expert în grupuri de lucru, organisme și organizații naționale, regionale, europene, pe domeniul reglementărilor, standardizării sau al securității cibernetice.
    - cunoașterea prevederilor din Better Regulation Guidelines și Better Regulation Toolbox ale Uniunii Europene.
- **#186 Expert securitate cibernetică**
  - **Experiență anterioară dovedită de minim un (1) an în domeniul juridic,** reglementare, securitate cibernetică, asigurarea conformității, managementul riscului, audit, protecția datelor sau un domeniu conex.
  - **Reprezintă un avantaj:**
    - experiența anterioară de lucrul în echipe de minimum trei (3) persoane.
    - experiența anterioară de lucru într-o institu?ie guvernamentală sau de reglementare de preferință la nivel național sau internațional.
- **#206 Coordonator superior securitate cibernetică**
  - Experiență **anterioară dovedită de minim cinci (5) ani acumulată în ultimii zece (10) ani** în unul din domeniile următoare:
    - Reglementare
    - Control intern

- Securitate cibernetică, securitatea informației
- Testare infrastructuri, rețele și sisteme informatice
- Audit (IT Audit, IT Security Audit, Internal Audit, Privacy Audit, Third Party Assurance Audit)
- Crearea, conducerea, operaționalizarea de echipe sau executarea de activități în:
  - ✓ Computer Security Incident Response Team (CSIRT)
  - ✓ Computer Emergency Response Team (CERT)
  - ✓ Computer Incident Response Center (CIRC)
  - ✓ Cyber Security Incident Response Center (CSIRC)
  - ✓ Security Operations Center (SOC)
  - ✓ IT / Information Security Helpdesk
  - ✓ Crisis Management Center
  - ✓ Echipe de Digital Forensics and Investigation (DFIR)
  - ✓ Echipe sau laboratoare de analiză și / sau testare a tehnologiilor digitale

- Experiență anterioară dovedită de minim doi (2) ani pentru lucrul în echipe de minimum trei (3) persoane.
- Experiență anterioară dovedită în executarea a minimum 10 (zece) activități de audit, control, verificare, evaluare acumulată în ultimii cinci (5) ani.

- **#210 Expert securitate cibernetică**
  - **Experiență anterioară dovedită de minim doi (2) ani acumulată în ultimii cinci (5) ani** în unul din domeniile următoare:
    - Reglementare
    - Control intern
    - Securitate cibernetică, securitatea informației
    - Testare infrastructuri, rețele și sisteme informatice
    - Audit (IT Audit, IT Security Audit, Internal Audit, Privacy Audit, Third Party Assurance Audit)
  - Derularea de de activități în:
    - Computer Security Incident Response Team (CSIRT)
    - Computer Emergency Response Team (CERT)
    - Computer Incident Response Center (CIRC)
    - Cyber Security Incident Response Center (CSIRC)
    - Security Operations Center (SOC)
    - IT / Information Security Helpdesk
    - Crisis Management Center
    - Echipe de Digital Forensics and Investigation (DFIR)
    - Echipe sau laboratoare de analiză și / sau testare a tehnologiilor digitale
  - **Experiență anterioară dovedită de minim doi (2) ani** pentru lucrul în echipe de **minimum trei (3) persoane**.

- **Experiență anterioară dovedită în executarea a minimum 5 (cinci) activitati de audit, control, verificare, evaluare acumulată în ultimii cinci (5) ani.**

- **#243 Expert securitate cibernetică** și **#244 Expert securitate cibernetică**
  - **Experiență anterioară dovedită de minim cinci (5) ani acumulată în ultimii zece (10) ani** în unul din domeniile următoare:
    - Reglementare
    - Securitate cibernetică, securitatea informației
    - Asigurarea conformității
    - Managementul riscului IT, de conformitate sau operațional
    - Audit (IT Audit, IT Security Audit, Internal Audit, Privacy Audit, Third Party Assurance Audit)
    - Crearea, conducerea, operaționalizarea de echipe sau executarea de activități în:
      - ✓ Computer Security Incident Response Team (CSIRT)
      - ✓ Computer Emergency Response Team (CERT)
      - ✓ Computer Incident Response Center (CIRC)
      - ✓ Cyber Security Incident Response Center (CSIRC)
      - ✓ Security Operations Center (SOC)
      - ✓ IT / Information Security Helpdesk
      - ✓ Crisis Management Center
      - ✓ Echipe de Digital Forensics and Investigation (DFIR)
      - ✓ Echipe sau laboratoare de analiză și / sau testare a tehnologiilor digitale
  - **Experiență anterioară dovedită de minim doi (2) ani** pentru lucrul în echipe de **minimum trei (3) persoane.**
  - **Are experiența anterioară dovedită și cunoștințe profesionale** specifice pe care le poate demonstra privind **cel puțin trei (3)** din următoarele standarde, metodologii sau cadre tehnice (frameworks) din lista de mai jos, recomandate de ENISA:
    - ISO/IEC 27001 "Information technology - Security techniques – Information security management systems requirements specification"
    - ISO/IEC 27002 "Information technology - Code of practice for information security management"
    - ISO/IEC 27005 "Information security risk management"
    - NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems
    - NIST Special Publication 800-53A - Guide for Assessing the Security Controls in Federal Information Systems and Organizations
    - NIST Special Publication 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations
    - CRAMM risk management methodology
    - OCTAVE, suite of tools, techniques and methods
    - IRAM2, end-to-end approach for performing business-focused information risk assessments

- BSI 100-3, methodology for performing risk analyses
- MAGERIT, methodology for Risk Analysis and Management
- MEHARI, information risk analysis assessment and risk management method
- MONARC, risk management methodology
- ISACA COBIT 5 (Control Objectives for Information and Related Technology)
- ISA-62443-1-3: System Security Compliance Metrics
- ISAE 3402 - International Standard on Assurance Engagements (ISAE) 3402 – "Assurance Reports on Controls at a Service Organization"
- ISAE 3000 - International Framework for Assurance Engagements, "Assurance Engagements Other than Audits or Reviews of Historical Financial Information"
- SOC 1, 2 & 3

▪ **Reprezintă un avantaj:**

- **experiența anterioară** în reprezentarea sau participarea ca expert în grupuri de lucru, organisme și organizații naționale, regionale, europene, pe domeniul reglementărilor, standardizării, auditării sau al securității cibernetice.
- **experiența anterioară** de lucru într-o instituție guvernamentală sau de reglementare.
- **experiența anterioară dovedită ca membru, presedinte sau vicepresedinte în următoarele formate profesionale la nivel național, european sau internațional (sau echivalent):**
  - ✓ Ad-Hoc Working Group (AHWG) gestionate sub egida European Union Agency for Cybersecurity (ENISA), cum ar fi:
    - ❖ Security Operation Centres (SOCs) Ad-Hoc Working Group
    - ❖ 5G Cybersecurity Certification Ad-Hoc Working Group
    - ❖ Cloud Services Ad-Hoc Working Group
    - ❖ Enterprise Security Ad-Hoc Working Group
    - ❖ Awareness Raising Ad-Hoc Working Group
    - ❖ Artificial Intelligence Cybersecurity Ad-Hoc Working Group
    - ❖ National Cyber Security Strategy (NCSS) Ad-Hoc Working Group
    - ❖ Cyber Threat Landscapes Ad-Hoc Working Group
  - ✓ Grupuri de lucru ale Information Systems Audit and Control Association (ISACA)
  - ✓ Grupuri de lucru ale Information Systems Security Association (ISSA)
  - ✓ Grupuri de lucru ale Cloud Security Alliance (CSA)
  - ✓ Grupuri de lucru ale National Institute of Standards and Technology (NIST)
  - ✓ Grupuri de lucru ale autorităților naționale competente în domeniul securității cibernetice din statele membre ale Uniunii Europene.

o **#256 Expert legal politici, standardizare securitate cibernetică**

▪ **Experiență anterioară dovedită de minim cinci (5) ani** în domeniul juridic, reglementare, securitate cibernetică, asigurarea conformității, managementul riscului, audit, control, protecția datelor sau un domeniu conex, experiență **acumulată în ultimii zece (10) ani**.

- **Experiență anterioară dovedită de minim doi (2) ani** pentru lucrul în echipe de **minimum trei (3) persoane**.
- **Reprezintă un avantaj:**
  - **experiența anterioară** de lucru în analiza de impact a reglementarilor (Regulatory Impact Assessment - RIA).
  - **experiența anterioară de lucru în utilizarea platformei online „Fit for Future" a Comisiei Europene.**
  - **experiența anterioară** de lucru într-o instituție guvernamentală sau de reglementare de preferință la nivel național sau internațional.
  - **experiența anterioară** în reprezentarea sau participarea ca expert în grupuri de lucru, organisme și organizații naționale, regionale, europene, pe domeniul reglementărilor, standardizării sau al securității cibernetice.

- **#331 Expert dezvoltare, implementare și administrare infrastructuri securitate cibernetică**
  - **Experiență anterioară de minim trei (3) ani** ca programator / dezvoltator / arhitect software, programator de sistem informatic, administrator de sistem software, proiectant sisteme informatice, consultant în informatică, cercetător în informatică, inginer de sistem în informatică ori comunicații și tehnologia informației, tester, **cu experiență acumulată în ultimii cinci (5) ani**.
  - **Experiență anterioară dovedită de minim doi (2) ani** pentru lucrul în echipe de **minimum trei (3) persoane**.
  - **Experiență anterioară** de minimum un (1) an în echipe de testare sau laboratoare de testare, sau în planificarea și executarea de teste din următoarele categorii:
    - **Functional Testing:** Unit Testing, Integration Testing, System Testing, Acceptance Testing
    - **Non-Functional Testing:** Performance Testing, Load Testing, Stress Testing, Volume Testing, Security Testing, Usability Testing, Compatibility Testing, Installation Testing, Uninstallation Testing, Recovery Testing, Documentation Testing
  - **Experiență anterioară** în instalarea și utilizarea soluții și sisteme de testare IT&C sau tehnologii digitale; în redactarea planurilor și dosarelor de testare, a scenariilor de testare, automatizarea testării și executarea testelor funcționale și nefuncționale.
- **#338 Asistent analiză surse deschis e, riscuri și amenințări securitate cibernetică** – grad Debutant, studii medii, poziție de execuție
  - Nu este obligatorie experiența profesională anterioară.
  - **Reprezintă un avantaj:**
    - experiență acumulată în investigații din surse deschise (OSINT), investigații digitale, forensics, securitate cibernetică, analize și raportări, consultanță, educație, învățământ, servicii profesionale, implementare sau gestionare infrastructuri IT&C, sau similar.
- **#339 Asistent analiză surse deschis e, riscuri și amenințări securitate cibernetică** – grad Debutant, studii medii, poziție de execuție
  - Nu este obligatorie experiența profesională anterioară.
  - **Reprezintă un avantaj:**
    - experiență acumulată în investigații din surse deschise (OSINT), investigații digitale, forensics, securitate cibernetică, analize și raportări, consultanță, educație, învățământ, servicii profesionale, implementare sau gestionare infrastructuri IT&C, sau similar.

- **Alte condiții**:
  - Cunoașterea limbii române ca limbă maternă sau limbă română de **minimum nivel C1** conform Common European Framework of Reference for Languages CEFR.
  - Cunoașterea limbii engleze de **minimum nivel B2** conform Common European Framework of Reference for Languages CEFR. Titularul postului are obligația ca în termen de maximum trei (3) luni de la data angajării să prezinte dovada îndeplinirii cerinței obligatorii de limbă engleză de minimum nivel B2 conform Common European Framework of Reference for Languages CEFR.
  - Cunoașterea unei a doua limbi străine la nivel operațional este de dorit.

Atribuții/cerințe ale postului

- **Direcția Generală Reglementare și Control - Direcția Reglementare**
  - **#169 Expert securitate cibernetică** – grad Superior, studii superioare, poziție de execuție - conform fișei de post publicate
  - **#170 Expert legal politici, standardizare securitate cibernetică** – grad Debutant, studii superioare, poziție de execuție - conform fișei de post publicate
  - **#177 Expert legal politici, standardizare securitate cibernetică** - grad Superior, studii superioare, poziție de execuție - conform fișei de post publicate
- **Direcția Generală Reglementare și Control - Direcția Evidență și Sprijin**
  - **#186 Expert securitate cibernetică** – grad Debutant, studii superioare, poziție de execuție - conform fișei de post publicate
- **Direcția Generală Reglementare și Control - Direcția Verificare și Control**
  - **#206 Coordonator superior securitate cibernetică** - grad Superior, studii superioare, poziție de conducere - conform fișei de post publicate
  - **#210 Expert securitate cibernetică** – grad Asistent, studii superioare, poziție de execuție - conform fișei de post publicate
- **Direcția Generală Reglementare și Control - Direcția Atestare și Autorizare**
  - **#243 Expert securitate cibernetică** – grad Superior, studii superioare, poziție de execuție - conform fișei de post publicate
  - **#244 Expert securitate cibernetică** – grad Superior, studii superioare, poziție de execuție - conform fișei de post publicate
- **Direcția Generală Reglementare și Control - Direcția Monitorizare, Reglementări Interne și Internaționale**
  - **#256 Expert legal politici, standardizare securitate cibernetică** - grad Superior, studii superioare, poziție de execuție - conform fișei de post publicate
- **Direcția Evaluare și Certificare Securitate Cibernetică Noi Tehnologii, Produse și Servicii**
  - **#331 Expert dezvoltare, implementare și administrare infrastructuri securitate cibernetică** - grad Superior, studii superioare, poziție de execuție - conform fișei de post publicate
  - **#338 Asistent analiză surse deschis e, riscuri și amenințări securitate cibernetică** – grad Debutant, studii medii, poziție de execuție - conform fișei de post publicate
  - **#339 Asistent analiză surse deschise, riscuri și amenințări securitate cibernetică** – grad Debutant, studii medii, poziție de execuție - conform fișei de post publicate

Documentele necesare înscrierii la concurs ce se vor regăsi în dosarele depuse de candidați

- Formular de înscriere la concurs disponibil pe site-ul DNSC.
- Curriculum vitae, model comun european;
- Copia actului de identitate sau orice alt document care atestă identitatea, potrivit legii, aflate în termen de valabilitate;
- Copia certificatului de căsătorie sau a altui document prin care s-a realizat schimbarea de nume, după caz;
- Copiile documentelor care atestă nivelul studiilor şi ale altor acte care atestă efectuarea unor specializări, precum şi copiile documentelor care atestă îndeplinirea condiţiilor specifice ale postului (originalele vor fi necesare pentru certificare);
- Copia carnetului de muncă, a adeverinței eliberate de angajator pentru perioada lucrată, care să ateste vechimea în muncă şi în specialitatea studiilor solicitate pentru ocuparea postului;
- Certificat de cazier judiciar, extrasul de pe cazierul judiciar, sau o declarație pe propria răspundere privind lipsa antecedentelor penale care să-l facă incompatibil cu funcția pentru care candidează. Prezenta declarație este valabilă până la momentul depunerii cazierului judiciar, în conformitate cu prevederile legale în vigoare;
- Adeverință medicală care să ateste starea de sănătate corespunzătoare, eliberată de către medicul de familie al candidatului sau de către unitățile sanitare abilitate cu cel mult 6 luni anterior derulării concursului. Adeverința care atestă starea de sănătate conține, în clar, numărul, data, numele emitentului şi calitatea acestuia, în formatul standard stabilit prin ordin al ministrului sănătății. Pentru candidaţii cu dizabilităţi, în situaţia solicitării de adaptare rezonabilă, adeverința care atestă starea de sănătate trebuie însoțită de copia certificatului de încadrare într-un grad de handicap, emis în condiţiile legii - original;
- Pentru persoanele cu dizabilități care se vor prezenta la concursul organizat de DNSC, se vor asigura condițiile necesare după caz, conform legislației în vigoare.

Înscrierea la concurs

Înscrierea la concurs se face prin transmiterea / depunerea documentelor necesare înscrierii la concurs:

- În format electronic la adresa de email HR@dnsc.ro până cel târziu în data de **18.05.2023, ora 17:00**;
- În format letric prin transmiterea la sediul Directoratului Național de Securitate Cibernetică (DNSC), Str. Italiană 22, Sector 2, 020976 București, România până cel târziu în data de **18.05.2023, ora 17:00**;
- În format letric prin depunerea la secretariatul comisiei de concurs, la sediul Directoratului Național de Securitate Cibernetică (DNSC), Str. Italiană 22, Sector 2, 020976 București, România **între orele 09:00-17:00 și până cel târziu în data de 18.05.2023, ora 17:00**, candidații au obligația de a se prezenta la secretarul comisiei de concurs cu documentele prevăzute anterior în original, pentru certificarea acestora, pe tot parcursul desfășurării concursului, dar nu mai târziu de data şi ora organizării probei scrise/practice, după caz, sub sancțiunea neemiterii actului administrativ de angajare.

În situația în care candidații transmit dosarele de concurs la sediul DNSC, prin Poșta Română, servicii de curierat rapid sau poștă electronică platformele informatice ale instituțiilor sau autorităților publice, candidații primesc codul unic de identificare la o adresă de e-mail comunicată de către aceștia şi au obligația de a se prezenta la secretarul comisiei de concurs cu documentele prevăzute anterior în original, pentru certificarea acestora, pe tot parcursul desfășurării concursului, dar nu mai târziu de data şi ora organizării probei scrise/practice, după caz, sub sancțiunea neemiterii actului administrativ de angajare.

Transmiterea documentelor prin poșta electronică sau prin platformele informatice ale autorităților sau instituțiilor publice se realizează în format .doc sau .pdf cu volum maxim de 20 MB, documentele fiind acceptate doar în formă lizibilă. Nerespectarea acestor prevederi conduce la respingerea candidatului.

Documentele redactate în limbi străine sunt însoțite de traducerea autorizată în limba română.

Nedepunerea dosarului în termenul prevăzut sau depunerea unui dosar incomplet determină automat respingerea candidatului. Lipsa documentelor, neconcordanța între informațiile din dosar și documentele solicitate candidaților, depunerea acestora la alta adresă decât cea indicată în anunț sau după termenul limită precizat atrag automat excluderea/ respingerea dosarului candidatului.

Conformitatea documentelor prezentate se poate face și pe parcursul derulării procedurii de angajare, cel târziu în momentul semnării contractului de muncă, în cazul candidaților declarați admiși.

Bibliografia și tematica de concurs

- Constituția României
    - Titlul III – Autoritățile publice
- OUG 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică
    - Se va studia actul normativ în integralitate
- Hotărârea 1.321 din 30 decembrie 2021 privind aprobarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027, precum și a Planului de acțiune pentru implementarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027
    - Se va studia actul normativ în integralitate
- Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice
    - Se va studia actul normativ în integralitate
- Legea 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative
    - Se va studia actul normativ în integralitate
- Ordonanță de Urgență nr. 119 din 22 iulie 2020 pentru modificarea și completarea Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice
    - Se va studia actul normativ în integralitate
- HG nr.963/2020 pentru aprobarea Listei serviciilor esențiale
    - Se va studia actul normativ în integralitate
- HG nr. 976/2020 privind aprobarea valorilor de prag pentru stabilirea efectului perturbator semnificativ al incidentelor la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale
    - Se va studia actul normativ în integralitate
- HG nr. 1003/2020 NORME TEHNICE de stabilire a impactului incidentelor pentru categoriile de operatori de servicii esențiale și furnizori de servicii digitale
    - Se va studia actul normativ în integralitate
- Ordinul nr. 600/2019 privind aprobarea Normelor metodologice de organizare și funcționare a Registrului operatorilor de servicii esențiale
    - Se va studia actul normativ în integralitate
- Ordinul nr. 599/2019 privind aprobarea Normelor metodologice de identificare a operatorilor de servicii esențiale și furnizorilor de servicii digitale
    - Se va studia actul normativ în integralitate
- Ordinul nr. 601/2019 pentru aprobarea Metodologiei de stabilire a efectului perturbator semnificativ al incidentelor la nivelul rețelelor și sistemelor informatice ale operatorilor de servicii esențiale
    - Se va studia actul normativ în integralitate

- Ordinul nr. 1323/2020 pentru aprobarea Normelor tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale
    - Se va studia actul normativ în integralitate
- Ordinul nr. 559/2021 559 privind aprobarea Regulamentului pentru atestarea și verificarea auditorilor de securitate cibernetică
    - Se va studia actul normativ în integralitate
- Ordinul nr. 105/11.10.2022 pentru aprobarea Normelor de aplicare a dispozițiilor privind verificarea și controlul îndeplinirii obligațiilor de securitate cibernetică pentru spațiul cibernetic național civil
    - Se va studia actul normativ în integralitate
- Ordinul nr. 106/14.10.2022 pentru aprobarea Normelor privind autorizarea și verificarea furnizorilor de servicii de formare pentru securitate cibernetică
    - Se va studia actul normativ în integralitate
- Decizia 88/30.04.2020 privind aprobarea Listei standardelor și specificațiilor europene și internaționale
    - Se va studia actul normativ în integralitate
- Decizia nr. 301/22.12.2021 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, cu modificările și completările ulterioare
    - Se va studia actul normativ în integralitate
- Decizia nr. 107/03.11.2022 pentru aprobarea tematicilor pentru formarea auditorilor de securitate cibernetică, a membrilor echipelor CSIRT și a responsabililor cu securitatea rețelelor și sistemelor informatice
    - Se va studia actul normativ în integralitate
- Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2)
    - Se va studia actul normativ în integralitate
- Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică)
    - Se va studia actul normativ în integralitate

NOTĂ: *Candidații vor avea în vedere la studierea actelor normative din bibliografia stabilită în vederea susținerii concursului inclusiv republicările, modificările și completările acestora.*

Relații suplimentare pot fi obținute la telefon **0742 999 645** sau pe email la **HR@dnsc.ro.**