DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

FIȘA DE POST
Direcția Generală Strategie
Direcția Studii, Cercetare și Analiză Aprofundată

Expert analiză surse deschise, riscuri și amenințări securitate cibernetică
#30

1 Identificarea postului

1.1 Numele si prenumele titularului

- NUME + PRENUME

1.2 Denumirea postului

- **Expert analiză surse deschise, riscuri și amenințări securitate cibernetică**
- *Notă: În cazul în care denumirea postului din Directoratul Național de Securitate Cibernetică (DNSC) nu se regăsește în COR, se va trece denumirea din COR cea mai apropiată din punct de vedere al sarcinilor și responsabilităților.*

1.3 Gradul profesional / treapta profesională

- **Principal**

1.4 Poziția în COR (Clasificarea Ocupațiilor din Romania)

- **Cod COR: Expert Surse Deschise 252902**
- *Notă: În cazul în care poziția postului din DNSC nu se regăsește în COR, se va trece codul din COR pentru denumirea cea mai apropiata din punct de vedere al sarcinilor și responsabilităților.*

1.5 Compartimentul funcțional și locația

- Direcția Generală Strategie - Direcția Studii, Cercetare și Analiză Aprofundată
- Sediul DNSC / telemuncă
- **Poziția #30 în statul de funcții al DNSC**

1.6 Nivelul postului

- Execuție

1.7 Sfera relațională internă și externă

1.7.1 Ierarhice

- Se subordonează pe următoarea linie ierarhică următoarelor funcții de conducere:
    - **Coordonator superior securitate cibernetică** - Direcția Studii, Cercetare și Analiză Aprofundată
    - **Manager superior securitate cibernetică** - Direcția Studii, Cercetare și Analiză Aprofundată
    - **Manager superior securitate cibernetică** - Conducere - Direcția Generală Strategie
    - **Adjunctul Directorului DNSC** care coordonează Direcția Generală Strategie (DGS)
    - **Directorul DNSC**
- Are în subordine: nu are în subordine alte posturi.

1.7.2 Funcționale

- Colaborează și cooperează cu funcțiile de conducere sau de execuție din următoarele compartimente funcționale ale DNSC pe subiecte și activități de studii, cercetare și analiză aprofundată în domeniul securității cibernetice:
    - Direcția Generală Strategie - toate compartimentele
    - Direcția Generală Reglementare și Control
        - Conducere Direcția Generală Reglementare și Control
        - Direcția Reglementare

        - Direcția Evaluare și Certificare Securitate Cibernetică Tehnologii, Produse și Servicii
    - Direcția Generală Parteneriate Instituționale
        - Conducere Direcția Generală Parteneriate Instituționale
        - Direcția Cooperare și Parteneriate Instituționale
        - Direcția Programe de Educație, Prevenire, Conștientizare și Instruire
    - Direcția Generală Operațiuni Tehnice
        - Conducere Direcția Generală Operațiuni Tehnice
        - Direcția OSINT (Open Source Intelligence)
        - Direcția Investigații și Atribuire
    - Direcția Generală Expertiză și Proiecte
        - Conducere Direcția Generală Expertiză și Proiecte
        - Direcția Inovare, Cercetare-Dezvoltare Servicii și Proprietate Intelectuală
- Colaborează și cooperează cu analiști, cercetători și experți în securitate cibernetică ai Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), ai Comisiei Europene, ai NATO, ai universităților și instituțiilor de cercetare, ai altor organisme și organizații naționale și internaționale pe subiecte și activități de studii, cercetare și analiză aprofundată în domeniul securității cibernetice.
- Colaborează și cooperează cu Directorul DNSC și cu membrii cabinetului acestuia.
- Colaborează și cooperează cu Adjuncții Directorului DNSC și cu membrii cabinetelor acestora.
- Colaborează și cooperează cu managerii de proiect și cu membrii echipelor de proiect în care participă, inclusiv cu beneficiarii, partenerii instituționali, contractorii, subcontractorii și consultanții implicați în aceste proiecte.

1.7.3 Reprezentare

- **Reprezintă Direcția Studii, Cercetare și Analiză Aprofundată, din Direcția Generală Strategie a DNSC,** conform mandatului primit din partea superiorilor ierarhici, atunci când participă la conferințe, seminarii, grupuri de lucru, prezentări sau alte evenimente ori activități profesionale în afara instituției.
- **Reprezintă DNSC și interesele DNSC** în raport cu părțile externe implicate, cu experți individuali și organizații profesionale sau non-guvernamentale în programe, proiecte și activități specifice comune privind colectarea și analiza datelor și informațiilor din surse deschise (OSINT), în vederea elaborării de rapoarte, studii, analize, whitepapers sau puncte de vedere (în limba romana și/sau engleză) pe subiecte din domeniul securității cibernetice.

1.7.4 Control

- Nu are.

2 Descrierea postului

2.1 Scopul principal al postului

- **Efectuează activități specifice de identificare, corelare, analiză, monitorizare de date și informații din surse deschise** în vederea atingerii obiectivelor instituționale ale DNSC și ale Direcției de Studii, Cercetare și Analiză Aprofundată.
- **Răspunde de efectuarea de activități de studiu, cercetare și analiză** privind domenii și subdomenii ale securității cibernetice, cum ar fi:
    - Îmbunătățirea securității și rezilienței cibernetice, și a lanțului de aprovizionare digital la incidentele și amenințările cibernetice, inclusiv la provocările noi și emergente, prin bune practici și mecanisme privind:

- Punerea în aplicare a reglementarilor naționale și UE în domeniul securității cibernetice;
- Sprijinirea standardizării, certificării și auditului în materie de securitate cibernetică;
- Sprijinirea implementării treptate a schemelor criptografice rezistente cuantic;
- Sprijinirea securității cibernetice prin conceptul „security by design” în software, hardware și sisteme;
- Modele detaliate de management al riscului pentru sistemele critice și lanțurile de aprovizionare digitale;
- Tehnici și instrumente de scanare și scanare pentru testarea securității dispozitivelor;
- Tehnici și instrumente de creștere a securității cibernetice asupra mediului IT&C tradițional și al tehnologiei operaționale (OT);
- Sprijinirea securității cibernetice a noilor tehnologii: AI, 5G, IoT, Edge, Cloud, etc.

o Îmbunătățirea securității și rezilienței cibernetice prin studierea, cercetarea și analiza aprofundată a aspectelor privind:

- Implementarea strategiilor naționale de securitate cibernetică;
- Sprijinirea dezvoltării și implementării exercițiilor de securitate cibernetică (tabletop, operaționale, tehnice);
- Metode și tehnici de dezvoltare, precum și de furnizare (atât online, cât și fizică) de cursuri de formare în domeniul securității cibernetice care să vizeze diferite categorii de public, de la tehnic (comunitățile CSIRT/CERT/SOC) la tactici pentru membrii autorităților naționale competente și ai instituțiilor publice sau operatorilor economici;
- Dezvoltarea și organizarea de exerciții și competiții (e.g. Capture The Flag, Hackatons, etc.), inclusiv scenarii de apărare împotriva atacurilor cibernetice;
- Bunele practici în vederea îmbunătățirii capacităților de prevenire, alertă timpurie, detectare, analiză și răspuns la amenințările și incidentele cibernetice;
- Bunele practici în vederea îmbunătățirii schimburilor de date și informații în domeniul securității cibernetice.

o Evoluții, tendințe, corelări ale datelor, informațiilor, bunelor practici, tehnicilor, tacticilor, protocoalelor, mecanismelor și controalelor tehnice și non-tehnice privind:

- Adversary - Adversari cibernetici
- Appsec Security - Securitatea Aplicațiilor
- Cloud Security - Securitatea Cloudului
- Crypto and Blockchain Security - Securitatea criptomonelelor și a tehnologiilor blockchain
- Cyber Attack - Atacurile cibernetice
- Cyber Vulnerabilities Exploitation - Exploatarea vulnerabilităților cibernetice
- Insider Threat - Amenințările interne (din interior)
- Mobile Technologies Security - Securitatea tehnologiilor mobile
- Threat Intelligence - Informații despre amenințări

2.2 Descrierea sarcinilor / atribuțiilor / activităților postului

- Răspunde de identificarea, colectarea și organizarea informațiilor despre riscurile, vulnerabilitățile, amenințările și cibernetice și alți factori care afectează securitatea cibernetică și efectuează analize aprofundate privind acestea.

- Întocmește rapoarte, studii, analize, whitepapers, cărți, cursuri, ghiduri articole, conținut pentru bloguri, manuale sau puncte de vedere pe subiecte din domeniul securității cibernetice, pe care le supune verificării, avizării și aprobării din partea următoarei ierarhii:
    - **Coordonator superior securitate cibernetică** - Direcția Studii, Cercetare și Analiză Aprofundată
    - **Manager superior securitate cibernetică** - Direcția Studii, Cercetare și Analiză Aprofundată
    - **Manager superior securitate cibernetică** - Conducere - Direcția Generală Strategie
    - **Adjunctul Directorului DNSC** care coordonează Direcția Generală Strategie (DGS)
    - **Directorul DNSC**
- Efectuează o serie de activități specifice **de identificare, corelare, analiză, monitorizare de date și informații din surse deschise** în vederea efectuării următoarelor, în linie cu bunele practici la nivel internațional (e.g. National Institute of Standards and Technologies - NIST)
    - T0562: Ajustează operațiunile de colectare sau planul de colectare (a datelor necesare) pentru a aborda problemele/provocările identificate și pentru a sincroniza efortul de colectare a datelor cu cerințele operaționale generale.
    - T0604: Compară activele și resursele alocate și disponibile cu cererea de colectare a datelor, exprimată prin cerințe.
    - T0626: Întocmește planuri și matrici de colectare a datelor utilizând îndrumări și proceduri stabilite.
    - T0651: Dezvoltarea unei metode de comparare a rapoartelor de colectare a datelor cu cerințele restante pentru identificarea lacunelor în materie de informații necesare.
    - T0681: Stabilirea unor căi alternative de prelucrare, exploatare și diseminare a datelor și informațiilor necesare pentru a aborda problemele sau problemele identificate.
    - T0725: Identificarea și atenuarea riscurilor la adresa capacității de gestionare a colectării de date necesare pentru a sprijini planul, operațiunile și activitățile.
    - T0734: Emiterea de solicitări de informații.
    - T0773: Prioritizează cerințele de colectare pentru platformele de colectare pe baza capacităților platformei.
    - T0779: Furnizează consiliere/asistență pentru factorii de decizie cu privire la realocarea activelor și resurselor de colectare de date ca răspuns la situații operaționale dinamice..
- **Lucrează împreună cu Direcția Comunicare, Media și Marketing pentru a efectua publicarea, după verificare, avizare și aprobare**, a materialelor întocmite (rapoarte, studii, analize, whitepapers, cărți, cursuri, ghiduri articole, conținut pentru bloguri, manuale sau puncte de vedere) destinate publicării, pe site-ul web al instituției, pe conturile de social media sau pe alte canale de comunicare disponibile.
- **Lucrează împreună cu Direcția Cooperare și Parteneriate Instituționale și cu Direcția Programe de Educație, Prevenire, Conștientizare și Instruire (din Direcția Generală Parteneriate Instituționale - DGPI)** pentru transmiterea materialelor întocmite (rapoarte, studii, analize, whitepapers, cărți, cursuri, ghiduri articole, conținut pentru bloguri, manuale sau puncte de vedere) către parteneri instituționali sau alți actori relevanți.
- **Participă activ, în baza mandatului primit din partea superiorilor ierarhici, în grupuri de lucru** pentru elaborarea de studii, pentru realizarea de activități de cercetare și / sau de analiză aprofundată pe subiecte din domeniul securității cibernetice.
- Răspunde de gestionarea instrumentelor disponibile pentru stocarea/structurarea informațiilor colectate în vederea întocmirii de rapoarte, studii, analize, whitepapers sau puncte de vedere.
- **Furnizează recomandări și contribuie activ** la întocmirea strategiei privind domeniul de studii, cercetare și analiză aprofundată al DNSC.

- Se asigură că orice analiză, set de date sau informație pe care o pregătește și o prezintă intern, public sau către terți este corectă, adecvată și în conformitate cu cadrul normativ în vigoare.
- **Identifică activ voluntari (elevi, studenți, absolvenți, etc.) în vederea colaborării cu DNSC** și propune superiorilor ierarhici modalități de implicare a acestora în activitățile Directoratului.
- Efectuează coordonarea și îndrumarea activității voluntarilor (elevi, studenți, absolvenți, etc.) ce sunt îi sunt asignați în cadrul programului sau activităților de voluntariat derulate la nivelul **Direcției Studii, Cercetare și Analiză Aprofundată**.
- Îndeplinește, în conformitate cu art.81-82 din HG 1336/2022, **rolul de îndrumător** pentru unul sau mai mulți salariați debutanți.
- **Participă, după caz, ca membru sau președinte** al comisiei, în comisiile de concurs sau examen pentru posturile scoase la concurs de către DNSC.
- **Participă, după caz, ca membru sau președinte** al comisiei, în comisiile de inventariere înființate la nivelul DNSC.
- **Participă, după caz, ca membru** al comisiei, în comisiile de evaluare, de contestații și/sau de recepție a achizițiilor publice organizate de DNSC. Participă, după caz, la pregătirea caietelor de sarcini și în comisiile de evaluare/negociere a contractelor de achiziție publică specifice nevoilor și activității **Direcției Studii, Cercetare și Analiză Aprofundată.**
- **Răspunde de confidențialitatea datelor și informațiilor DNSC la care are acces,** inclusiv a celor transmise către DNSC de către terți, în conformitate cu prevederile legale, regulamentele interne ale DNSC și cu instrucțiunile primite.
- Participă, după caz, în echipele de implementare a proiectelor finanțate prin programe, instrumente, mecanisme, fonduri naționale, europene sau internaționale, precum și a celor finanțate prin Planul Național de Redresare și Reziliență (PNRR) al României ocupând în cadrul proiectelor o funcție / rol corespunzător experienței, aptitudinilor și cunoștințelor tehnice și non-tehnice. Participarea în proiect a titularului postului se face prin numire astfel:
    - Prin decizie a **Directorului DNSC;** sau
    - Prin decizie a **Adjunctului Directorului DNSC** care coordonează **Direcția Generală Strategie (DGS)**, în acest caz cu avizul și aprobarea:
        - **Directorului DNSC,** și a
        - **Adjunctului Directorului DNSC** care coordonează Direcția Generală Expertiză și Proiecte
- **Propune, alege, adaptează, evaluează și folosește** în activitatea curentă proceduri, metode, standarde, tehnici și instrumente privind activitățile pentru care este responsabil(ă) sau în care este implicat(ă).
- **Furnizează la cerere sau din proprie inițiativă**, expertiză tehnică, asistență și recomandări privind către Conducerea DNSC și către funcțiile de conducere sau de execuție din compartimentele funcționale ale DNSC, după caz.
- Participă la sesiunile de pregătire profesională **organizate trimestrial la nivelul Direcției Studii, Cercetare și Analiză Aprofundată**, pentru a asigura menținerea și îmbunătățirea cunoștințelor profesionale proprii.
- **Participă activ la ședințele interne organizate lunar la nivelul Direcției.**
- Asigură o comunicare adecvată, prin metode de comunicare scrisă, discuții și feedback la nivelul **Direcției** precum și între această direcție și alte compartimente funcționale din cadrul DNSC și/sau partenerii instituționali.
- Răspunde pentru corectitudinea de fond și de formă a tuturor lucrărilor întocmite și/sau semnate.
- Pregătește datele și informațiile necesare și întocmește raportarea trimestrială, pentru **indicatorii de performanță (KPIs - Key Performance Indicators)** ai activităților proprii.

- Facilitează cooperarea și lucrul în echipă la nivelul **Direcției** prin comunicare verbală și scrisă cu personalul serviciului, diseminarea permanentă a tuturor informațiilor relevante și urmărirea folosirii de către personalul direcție a informațiilor furnizate.
- Face propuneri concrete de îmbunătățire a metodelor de lucru la nivelul **Direcției Studii, Cercetare și Analiză Aprofundată**, atât direct în cadrul direcție sau la nivelele ierarhice superioare, pentru a maximiza utilizarea eficientă a timpului de lucru și a resurselor în atingerii obiectivelor instituționale.
- **Asigură identificarea și rezolvarea cu celeritate a problemelor apărute** în derularea activităților curente în care este implicat(ă) și informează la timp superiorii ierarhici despre problemele apărute pe care nu le poate rezolva la nivelul său, său propunând în mod pro-activ soluții.
- **Acționează cu bună-credință și amabilitate în exercitarea sarcinilor profesionale**, prezentând o atitudine civilizată și un comportament bazat pe respect, corectitudine, integritate morală și profesională.
- **Îndeplinește orice alte atribuții dispuse de conducerea instituției**, în limitele competențelor legale.
- **Respectă dispozițiile Regulamentului European nr. 679/2016 și a Legii nr. 190/2018** privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date.

2.3 Delegarea de atribuții și competență

- În situația și pe perioada în care titularul postului se află în imposibilitatea de a-și îndeplini atribuțiile de serviciu (spre exemplu: concediu de odihnă, concediu pentru incapacitate de muncă, delegații, concediu fără plată, suspendare, detașare etc.), o parte dintre atribuțiile sale menționate în secțiunea anterioară vor fi preluate prin delegare de către una sau mai multe din următoarele funcții din **Direcția Studii, Cercetare și Analiză Aprofundată:**
    - Expert securitate cibernetică
    - Expert analiză surse deschise, riscuri și amenințări securitate cibernetică
    - Expert legal politici, standardizare de securitate cibernetică
    - Asistent securitate cibernetică
    - Asistent politici, strategii și cooperare securitate cibernetică
    - Expert politici publice

  iar preluarea de atribuții se face prin desemnare de către **Managerul** superior **securitate cibernetică din Direcția Studii, Cercetare și Analiză Aprofundată.**

3 Condiții specifice de ocupare a postului

3.1 Studii de specialitate

- Studii universitare de licență absolvite cu diplomă, respectiv studii superioare de lungă durată, absolvite cu diplomă de licență sau echivalentă.

3.2 Experiență profesională, competențe și aptitudini necesare

- **Experiență anterioară de minim doi (2) ani acumulată în ultimii cinci (5) ani** în unul din domeniile sau ocupațiile următoare (sau echivalent):
    - Securitate cibernetică, protecția datelor, informatică, telecomunicații
    - Proiectare/implementare/operare de tehnologii, soluții, infrastructuri sau servicii digitale,
    - Investigații, investigații digitale, forensics
    - Cercetare / inovare (securitate cibernetică, protecția datelor, informatică, telecomunicații, tehnologii digitale)

- Coordonare și/sau implementare de programe/proiecte/contracte de cercetare (securitate cibernetică, protecția datelor, informatică, telecomunicații, tehnologii digitale)
- Consultanță sau servicii profesionale (securitate cibernetică, protecția datelor, informatică, telecomunicații, tehnologii digitale)
- Experiență în una din ocupațiile următoare (sau echivalent):
  - Grupă de bază cod COR 1330 - Conducători in servicii de tehnologia informației si comunicațiilor
    - COR 133001 Director centru de calcul
    - COR 133002 Șef oficiu de calcul
    - COR 133003 Șef atelier informatică
    - COR 133004 Șef laborator informatică
    - COR 133005 Director divizie informatică
    - COR 133006 Director departament informatică
    - COR 133007 Manager tehnologia informațiilor și comunicații
  - Grupă de bază cod COR 2120 - Matematicieni, actuari și statisticieni
    - COR 212023 Cercetător în matematică informatică
    - COR 212024 Asistent de cercetare în matematică-informatică
  - Grupă de bază cod COR 2149 - Ingineri și asimilați neclasificați în grupele de bază anterioare
    - COR 214917 Cercetător în informatică
    - COR 214918 Asistent de cercetare în informatică
  - Grupă de bază cod COR 2432 - Specialiști in relații publice
    - COR 243201 Specialist în relații publice
    - COR 243212 Specialist relații sociale
    - COR 243213 Expert relații externe
  - Grupă de bază cod COR 2519 - Analiști programatori in domeniul software neclasificați in grupele de bază anterioare
    - COR 251203 Inginer de sistem în informatică
    - COR 251901 Consultant în informatică
  - Grupă de bază cod COR 2529 - Specialiști in baze de date si rețele neclasificați în grupele de baza anterioare
    - COR 252902 expert surse deschise
    - COR 252903 specialist în securitate cibernetică pentru sisteme automatizate de comandă-control
    - COR 252904 expert în securitate cibernetică
    - COR 252905 expert în investigații digitale
    - COR 252907 consultant de securitate cibernetică
    - COR 252909 expert în criminalistică informatică
    - COR 252910 manager de securitate sisteme informatice

- **Experiență anterioară ce poate fi dovedită prin publicarea (în calitate de autor sau co-autor)** de rapoarte, studii, analize, whitepapers, cărți, cursuri, ghiduri articole, bloguri, manuale sau puncte de vedere pe subiecte relevante din domeniul securitate cibernetică, digitalizare, telecomunicații, transformare digitală, tehnologii digitale, informatică:
    - **Minim o (1) publicație în calitate de autor sau co-autor.**
- **Este de dorit experiență anterioară ce poate fi dovedită prin participarea efectivă în calitate de expert în domeniul securitate cibernetică, digitalizare, telecomunicații, transformare digitală, tehnologii digitale, informatică, în proiecte naționale și/sau internaționale ce au avut** ca rezultat elaborarea și publicarea de rapoarte, studii, analize, whitepapers, cărți, cursuri, ghiduri articole, bloguri, manuale sau puncte de vedere pe subiecte relevante domeniului securității cibernetice.
- **Este de dorit experiență anterioară ce poate fi dovedită prin calitatea de expert(ă) în grupuri de lucru tehnice sau de cercetare** din domeniul securității cibernetice organizate de una din organizațiile și/sau instituțiile următoare: ENISA, Comisia Europeană, NATO, OSCE, ITU, ONU, ISACA, CISA, BEREC sau de către autorități naționale competente din țări ale Uniunii Europene, Marea Britanie, SUA, Canada.
- Cunoștințe practice și experiență anterioară în utilizarea de aplicații și platforme pentru datele și informațiile disponibile în domeniul securității cibernetice din surse deschise:
    - Social media
    - Bloguri, forumuri, platforme de discuții, chat, Q&A
    - Platforme de web intelligence (domain and IP research, websites analysis, web history, website capture)
    - Platforme colaborative academice sau de cercetare ce includ domeniul securității cibernetice (ResearchGate, Open Science Framework, Joinup)
    - Dark web / deep web
- Cunoașterea prevederilor legale din:
    - OUG nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică;
    - Hotărârea Guvernului nr. 1321/2021 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
    - Legea 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative.
    - Directiva (UE) 2022/2555 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (Directiva NIS 2).
- Are competențele următoare conform **European e-Competence Framework 3.0**:
    - **E.4. Relationship Management - Level 3 / Nivel 3.** Accounts for own and others actions in managing a limited number of stakeholders. Este capabil(ă) să aibă responsabilități pentru acțiunile proprii și ale altora, în gestionarea unui număr limitat de părți interesate.
- **Cunoștințe, competențe și abilitați (KSAs - knowledge, skills, and abilities) specifice efectuării de activități în cadrul unei organizații de securitate cibernetică**, așa cum acestea sunt definite de National Institute of Standards and Technologies (NIST) National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity Education **(i.e. NICE Framework):**
    - Cunoștințe, competențe și abilități **profesionale**:
        - **Gândire critică - Critical Thinking (C011)** - are aptitudini privind analiza obiectivă a faptelor pentru a forma o judecată profesională.
        - **Comunicare orală/verbală - Oral Communication (C036)** - are aptitudini privind exprimarea informațiilor sau a ideilor prin viu grai.

- **Comunicare scrisă - Written Communication (C060)** - are aptitudini privind formularea și comunicarea oricărui tip de mesaj care utilizează cuvântul scris.

- Cunoștințe, competențe și abilități **operaționale**:
  - **Managementul relațiilor - Client/Stakeholder Relationship Management (C003)** - are aptitudini privind conceptele, practicile și tehnicile utilizate pentru a identifica, a se angaja cu, a influența și monitoriza relațiile cu persoane și grupuri conectate la un efort de lucru, inclusiv cei implicați activ, cei care exercită influență asupra procesului și a rezultatelor sale și cei care au un interes legitim în rezultat (pozitiv sau negativ).
  - **Confidențialitatea și protecția datelor - Data Privacy and Protection (C014)** - are aptitudini privind relația dintre colectarea, stocarea și difuzarea datelor, protejând în același timp viața privată a persoanelor fizice.
  - **Juridic, Guvernanță și Jurisprudență - Legal, Government, and Jurisprudence (C030)** - are aptitudini privind legi, reglementări, politici și etică, care pot avea un impact asupra activităților organizaționale.
  - **Cunoașterea practicilor de gestionare a riscurilor lanțului de furnizori** - Knowledge of Supply Chain Risk Management Practices (K0126) (NIST SP 800-161).
  - **Cunoașterea modelelor de securitate standard din industrie** - Knowledge of industry standard security models (K0288).
  - **Cunoașterea proceselor de management al riscului (de exemplu, metode de evaluare și atenuare a riscurilor)** - Knowledge of risk management processes (e.g. methods for assessing and mitigating risk) (K0002).
  - **Cunoașterea legilor, reglementărilor, politicilor și eticii în ceea ce privește securitatea cibernetică și confidențialitatea** - Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy (K0003).
  - **Cunoașterea politicilor, cerințelor și procedurilor de securitate a lanțului de aprovizionare și de gestionare a riscurilor lanțului de aprovizionare (IT)** - Knowledge of information technology (IT) supply chain security and supply chain risk management policies, requirements, and procedures (K0169).

- Cunoștințe, competențe și abilități **tehnice**:
  - **Cunoașterea amenințărilor și vulnerabilităților cibernetice** - Knowledge of cyber threats and vulnerabilities (K0005).
  - **Cunoașterea impactului operațional specific al deficiențelor de securitate cibernetică** - Knowledge of specific operational impacts of cybersecurity lapses (K0006).
  - **Cunoașterea tehnologiilor noi și emergente din domeniul tehnologiei informației (IT) și al securității cibernetice** - Knowledge of new and emerging information technology (IT) and cybersecurity technologies (K0059).
  - **Cunoașterea metodologiilor de hacking** - Knowledge of hacking methodologies (K0310).

- Abilitatea de a procesa și analiza date și informații în scopul pregătirii de **rapoarte și rezumate de un nivel calitativ foarte ridicat**, ce includ utilizarea de tabele, imagini ilustrative sau grafice pentru sublinierea de concluzii și inter-relaționare a datelor și informațiilor analizate.
- Capacitatea de a colabora eficient cu colegii, partenerii externi și părțile interesate.
- Gândire critică și centrată pe rezolvarea problemelor profesionale din domeniul propriu.
- Abilitatea de a respecta instrucțiuni orale și scrise.
- Abilitatea de a procesa, analiza și gestiona informații contextuale și volume mari de date.
- Abilitatea de a acționa într-o manieră logică și investigativă și cu atenție sporită la detalii.
- Abilitatea de a-și exercita profesia și atribuțiile cu onestitate, bună credință și responsabilitate.

- Aptitudini excelente de prezentare, comunicare, relaționare și interpersonale.
- Aptitudini de planificare, organizare și control a activității proprii și într-un cadru de echipă.
- Aptitudini de luare a deciziilor, inițiativă și autonomie în acțiune.

3.3 Instrumente și tehnologii de lucru

- Are experiență anterioară dovedită și poate să utilizeze **la un nivel avansat** aplicații de tip Office (sau echivalent):
    - Microsoft Word, Excel, Powerpoint, Outlook, Teams, etc.
    - Google Docs, Sheets, Slides, Calendar, Sites etc.
    - Libre Office Writer, Calc, Impress, Draw, Math, Base etc.
- Are experiență cu și poate să utilizeze **la un nivel general a cel puțin una (1)** din următoarele platforme de comunicare video (sau echivalent):
    - Microsoft Teams, Zoom, Jitsi, Cisco Webex, Google Hangouts, Google Meet, GoToMeeting
    - Dialpad Meetings, TrueConf Online, Skype, FreeConference, Lifesize Go, Slack Video Calls
    - Facebook Live, YouTube Live, Twitter Live

3.4 Certificări sau cursuri de specializare

- **Este de dorit să posede, la data preluării postului, cel puțin una (1)** din următoarele certificări sau cursuri de specializare (sau echivalent):
    - Open Source Intelligence Professional - IntelTechniques
    - SEC497: Practical Open-Source Intelligence (OSINT) - SANS
    - SEC587: Advanced Open-Source Intelligence (OSINT) - SANS
    - GIAC Open Source Intelligence (GOSI)
    - CISSP (Certified Information Systems Security Professional)
    - CRISC (Certified in Risk and Information Systems Control)
    - CISM (Certified Information Security Manager)
    - CISA (Certified Information Systems Auditor)
    - IACIS Certified Forensic Computer Examiner (CFCE)
    - CompTIA Security+
    - CompTIA Cybersecurity Analyst (CySA+)
    - MITRE ATT&CK Fundamentals
    - MITRE ATT&CK Defender
    - Certified Public Relations Specialist (CPRS)
    - EU Cyber Diplomacy Toolbox, Cyber Diplomacy, Digital Diplomacy
    - Standarde și cadre de management al riscurilor, de cerificare și/sau securitate cibernetică: NIST SP 800-30, NIST SP 800-37, NIST SP 800-39, NIST SP 800-53, COBIT, RiskIT, Monarc, Ebios, ISO 27005, BSI Standard 100-1, BSI Standard 100-2, BSI Standard 200-2, EU ITSRM², The Open Group Risk Analysis (O-RA) Standard, sau echivalent.
    - Curs acreditat de Ministerul Muncii și Solidarității Sociale (MMSS), Minist erul Educației (ME), Autoritatea Națională pentru Calificări (ANC) sau de Comisia de Autorizare a Furnizorilor de Formare Profesională (CAFFPA) pentru următoarele ocupații:
        - COR 212023 Cercetător în matematică informatică
        - COR 212024 Asistent de cercetare în matematică-informatică

- COR 214917 Cercetător în informatică
- COR 214918 Asistent de cercetare în informatică
- COR 243201 Specialist în relații publice
- COR 243212 Specialist relații sociale
- COR 243213 Expert relații externe
- COR 251203 Inginer de sistem în informatică
- COR 251901 Consultant în informatică
- COR 252902 Expert surse deschise
- COR 252903 Specialist în securitate cibernetică pentru sisteme automatizate de comandă-control
- COR 252904 expert în securitate cibernetică
- COR 252905 expert în investigații digitale
- COR 252907 consultant de securitate cibernetica˘
- COR 252909 expert în criminalistică informatică
- COR 252910 manager de securitate sisteme informatice

- **Are obligația ca în termen de maximum un (1) an de la data preluării postului, să obțină/finalizeze cel puțin una (1) din următoarele certificări sau cursuri de specializare** (sau echivalent) - costurile aferente acesteia fiind suportate de către Directorat:
  - Open Source Intelligence Professional - IntelTechniques
  - SEC497: Practical Open-Source Intelligence (OSINT) - SANS
  - SEC587: Advanced Open-Source Intelligence (OSINT) - SANS
  - GIAC Open Source Intelligence (GOSI)
  - CISSP (Certified Information Systems Security Professional)
  - CRISC (Certified in Risk and Information Systems Control)
  - CISM (Certified Information Security Manager)
  - CISA (Certified Information Systems Auditor)
  - IACIS Certified Forensic Computer Examiner (CFCE)
  - CompTIA Security+
  - CompTIA Cybersecurity Analyst (CySA+)
  - MITRE ATT&CK Fundamentals
  - MITRE ATT&CK Defender
  - Certified Public Relations Specialist (CPRS)
  - EU Cyber Diplomacy Toolbox, Cyber Diplomacy, Digital Diplomacy
  - Standarde și cadre de management al riscurilor, de cerificare și/sau securitate cibernetică: NIST SP 800-30, NIST SP 800-37, NIST SP 800-39, NIST SP 800-53, COBIT, RiskIT, Monarc, Ebios, ISO 27005, BSI Standard 100-1, BSI Standard 100-2, BSI Standard 200-2, EU ITSRM², The Open Group Risk Analysis (O-RA) Standard, sau echivalent.
  - Curs acreditat de Ministerul Muncii și Solidarității Sociale (MMSS), Minist erul Educației (ME), Autoritatea Națională pentru Calificări (ANC) sau de Comisia de Autorizare a Furnizorilor de Formare Profesională (CAFFPA) pentru următoarele ocupații:
    - COR 212023 Cercetător în matematică informatică

- COR 212024 Asistent de cercetare în matematică-informatică
- COR 214917 Cercetător în informatică
- COR 214918 Asistent de cercetare în informatică
- COR 243201 Specialist în relații publice
- COR 243212 Specialist relații sociale
- COR 243213 Expert relații externe
- COR 251203 Inginer de sistem în informatică
- COR 251901 Consultant în informatică
- COR 252902 Expert surse deschise
- COR 252903 Specialist în securitate cibernetică pentru sisteme automatizate de comandă-control
- COR 252904 expert în securitate cibernetică
- COR 252905 expert în investigații digitale
- COR 252907 consultant de securitate cibernetică
- COR 252909 expert în criminalistică informatică
- COR 252910 manager de securitate sisteme informatice

3.5 Metodologii cunoscute

- Nu este cazul.

3.6 Cunoștințe de limba română și de limbi străine

- Cerință obligatorie de limbă română 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**.

3.7 Cerințe privind cetățenia

- Cetățenie română, a unui alt stat membru al Uniunii Europene ori al Spațiului Economic European, ori cetățenia Confederației Elvețiene.
- *Notă: Persoanele care au cetățenia unui alt stat membru al Uniunii Europene ori al Spațiului Economic European ori cetățenia Confederației Elvețiene pot fi încadrate în muncă pe teritoriul României în baza unui contract individual de munca în aceleași condiții în care pot fi angajați și cetățenii români.*

3.8 Autorizații speciale pentru exercitarea atribuțiilor

- Nu este cazul.

4 Indicatori de performanță

- **Numărul de inițiative, proiecte, acțiuni de studiu, cercetare și analiză** pentru care este responsabil(ă) sau în care este implicat(ă) într-o perioadă de timp (lunar, trimestrial, anual, de la începutul anului calendaristic).
- **Numărul de materiale (rapoarte, studii, analize, whitepapers, cărți, cursuri, ghiduri articole, conținut pentru bloguri, manuale sau puncte de vedere)** pe care le-a întocmit și care au fost

publicate pe site-ul web al instituției, pe conturile de social media ale DNSC sau pe alte canale de comunicare disponibile.

- Pregătirea și publicarea unui număr de **minimum patru (4) rapoarte, studii, analize**, **whitepapers sau cărți,** în domeniul securității cibernetice, pe baza unei tematici aprobate de superiorii ierarhici, anual.
- Numărul de linkuri pe site-uri web ale cercetătorilor în domeniul securității cibernetice, partenerilor instituționali ai DNSC către materiale pe care le-a pregătit și/sau publicat.
- **Numărul de voluntari (elevi, studenți, absolvenți, etc.)** pe care i-a identificat în vederea colaborării cu DNSC.
- Coordonarea și îndrumarea activității pentru **minimum doi (2) voluntari anual,** asignați **Direcției Studii, Cercetare și Analiză Aprofundată**, pe o perioadă de voluntariat de minimum o (1) lună.
- Efectuarea anual a unui **număr minimal de șaisprezece (16) ore de cursuri online sau în format fizic în domenii relevante postului**, dovedită cu certificat de participare/absolvire/diplomă sau similar. În cazul în care sunt costuri implicate de efectuarea cursurilor, acestea vor fi suportate de către DNSC, cu aprobarea superiorilor ierarhici.
- Lipsa absențelor nemotivate pentru participarea la sesiunile de pregătire profesională **organizate trimestrial la nivelul Direcției Studii, Cercetare și Analiză Aprofundată**, ce au ca obiectiv asigurarea menținerii și îmbunătățirii cunoștințelor profesionale proprii.
- **Concluzii pozitive la evaluarea independentă bi-anuală (la 6 luni)** a performanței în acest post, cu accent pe îndeplinirea sarcinilor, atribuțiilor și activităților postului.
- **Lipsa unor plângeri sau reclamații fundamentate** privind activitățile specifice de purtător de cuvânt ale DNSC pentru care este responsabil(ă) sau în care este implicat(ă), venite din partea partenerilor instituționali, a jurnaliștilor sau reprezentanților mass-media implicați.

Directoratul Național de Securitate Cibernetică	Angajat/Salariat
Nume + Prenume	**Nume + Prenume**
Data _____	Data _____
Nume + Prenume	
Data _____	
Nume + Prenume	
Data _____	