DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

FIȘA DE POST
Direcția Generală Reglementare și Control
Direcția Verificare și Control

Expert legal politici, standardizare securitate cibernetică
#217

1 Identificarea postului

1.1 Numele si prenumele titularului

- NUME + PRENUME

1.2 Denumirea postului

- **Expert legal politici, standardizare 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

- **Debutant**

1.4 Poziția în COR (Clasificarea Ocupațiilor din Romania)

- **Cod COR: Expert în securitate cibernetică 252904**
- *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 Reglementare și Control - Direcția Verificare și Control
- Sediul DNSC / telemuncă
- **Poziția #217 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 Verificare și Control
    - **Manager securitate cibernetică** - Direcția Verificare și Control
    - **Adjunctul Directorului DNSC** care coordonează Direcția Generală Reglementare și Control
    - **Directorul DNSC**
- Are în subordine: nu are în subordine alte posturi.

1.7.2 Funcționale

- Colaborează și cooperează cu toate funcțiile de conducere sau de execuție din:
    - Direcția Generală Reglementare și Control (toate compartimentele)
    - Direcția Generală Strategie (toate compartimentele)
    - Direcția Generală Parteneriate Instituționale (toate compartimentele)
    - Direcția Generală Operațiuni Tehnice (toate compartimentele)
    - Direcția Generală Expertiză și Proiecte (toate compartimentele)
    - Direcția Generală Internă
        - Conducere Direcția Generală Internă

- Direcția Juridică
- Direcția Protecția Datelor Personale, Etică și Securitate Internă

- Colaborează și cooperează cu membrii cabinetului Directorului DNSC.
- Colaborează și cooperează cu Adjuncții Directorului DNSC și cu membrii cabinetelor acestora, cu excepția Adjunctului care coordonează Direcția Generală Reglementare și Control, căruia i se subordonează ierarhic.
- 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 Verificare și Control din Direcția Generală Reglementare și Control (DGRC) 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, sau în raport cu experți individuali și organizații profesionale sau non-guvernamentale, după caz.
- **Reprezintă DNSC și interesele DNSC,** conform mandatului primit din partea superiorilor ierarhici, în raport cu partenerii instituționali ce gestionează inițiative de reglementare în domeniul securității cibernetice, atât la nivel național cât și internațional.
- **Reprezintă DNSC și interesele DNSC,** conform mandatului primit din partea superiorilor ierarhici, în raporturi de cooperare cu alte autorități de reglementare, agenții guvernamentale și organizații internaționale pentru a face schimb de informații și pentru a coopera pentru armonizarea reglementărilor privind securitatea cibernetică.

1.7.4 Control

- Relații de verificare și control al entităților reglementate de DNSC.

2 Descrierea postului

2.1 Scopul principal al postului

- Participă în mod activ și contribuie la **desfășurarea în bune condiții a activităților efectuate de către Direcția Verificare și Control** și de către Conducerea Direcției Generale Reglementare și Control (DGRC) în baza prevederilor OUG 104/2021 art. 5 lit. b) și art.19
- Participă în mod activ și contribuie la dezvoltarea, implementarea și punerea în aplicare a politicilor, regulamentelor, normelor, procedurilor, ghidurilor și liniilor directoare de reglementare în domeniul securității cibernetice.
- Aplică măsuri de evaluare, verificare și control, conform atribuțiilor legale ale DNSC, pentru asigurarea faptului că entitățile reglementate de DNSC respectă legile, reglementările și standardele naționale și internaționale aplicabile în materie de securitate cibernetică.

2.2 Descrierea sarcinilor / atribuțiilor / activităților postului

- Monitorizează și evaluează conformitatea entităților reglementate cu legile, reglementările și standardele aplicabile în materie de securitate cibernetică, pe domeniul de competență al Directoratului, cum ar fi:
  - OUG 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică.
  - Legea 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative.
  - Legea 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice.

- Legea 354/2022 privind protecția sistemelor informatice ale autorităților și instituțiilor publice în contextul invaziei declanșate de Federația Rusă împotriva Ucrainei.
- Directiva (UE) 2022/2555 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (Directiva NIS 2).
- Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011.
- DNSC Ordinul nr. 1323/2020 pentru aprobarea Normelor tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale.

- Participă la derularea activităților de control, evaluări, inspecții sau audituri regulate și ad-hoc de conformitate, după cum este necesar, pentru a evalua eficacitatea controalelor, politicilor și procedurilor de securitate cibernetică ale entităților reglementate de către DNSC.
- Identifică problemele de neconformitate și domeniile de îmbunătățire și oferă recomandări entităților reglementate cu privire la modul de a atinge și menține conformitatea.
- Colaborează cu echipele interne, cum ar fi experții tehnici și de reglementare, pentru a oferi îndrumări precise și în timp util cu privire la legile, reglementările și standardele de securitate cibernetică.
- **Întocmește, din proprie inițiativă sau la cerere, statistici și situații** privind entitățile reglementate de către DNSC.
- Participă la întocmirea și menținerea de rapoarte detaliate, înregistrări și documentație privind activitățile, constatările și recomandările de control al conformității. Prezintă rapoartele rezultate din activitățile de verificare, evaluare și control superiorilor ierarhici și conducerii DNSC, cu propuneri de măsuri adecvate, conform legislației și reglementărilor în vigoare.
- Realizează verificări și evaluări, din perspectivă juridică, privind situația implementării de către entitățile care fac obiectul legislației din domeniul securității cibernetice a măsurilor impuse prin legislație și reglementările ulterioare, pe care le prezintă în scris conducerii instituției, însoțite de propuneri adecvate, în conformitate cu atribuțiile DNSC.
- Acordă sprijin juridic entităților reglementate în dezvoltarea și implementarea planurilor de remediere pentru a aborda problemele de neconformitate identificate și domeniile de îmbunătățire.
- Comunică și stabilește legătura cu entitățile reglementate, partenerii din industrie, organizațiile guvernamentale și organizațiile internaționale pentru a promova o cultură a conformității securității cibernetice și a împărtăși cele mai bune practici.
- Este la curent cu evoluțiile în domeniul securității cibernetice, inclusiv actualizările legilor, reglementărilor, standardelor și bunelor practici, precum și amenințărilor și tehnologiilor emergente.
- Furnizează contribuții scrise pentru demersurile de dezvoltare și punere în aplicare a acțiunilor de control, cum ar fi sancțiuni sau măsuri corective, în cazuri de nerespectare.
- Asigură asistență juridică în gestionarea litigiilor sau plângerilor care implică DNSC, din perspectiva de autoritate de control și verificare.
- Contribuie la derularea unor programe de formare sau ateliere de lucru privind legile, reglementările și conformitatea privind securitatea cibernetică pentru echipele interne și entitățile reglementate.
- Acordă asistență de specialitate la dezvoltarea și implementarea politicilor, proiectelor de acte normative, procedurilor și liniilor directoare de reglementare ale Directoratului.
- Participă în grupurile de lucru pe tema reglementărilor în domeniul securității cibernetice, la nivel național și internațional.
- Participă activ în programe, proiecte, activități și inițiative ale Directoratului și ale altor instituții cu competențe în domeniu, în vederea îndeplinirii obiectivelor Strategiei Naționale de Securitate Cibernetică, precum și a realizării altor sarcini legale ale Directoratului.

- În colaborare cu Serviciul Secretariat, întocmește, completează și actualizează permanent lista de contacte instituționale a DNSC (instituții, persoane de contact, adresa poștală, numere de telefon, adrese de email) care fac obiectul direct sau incidental al activității reglementare a DNSC.
- Participă la forumuri din industrie, conferințe, workshop-uri, seminarii și grupuri de lucru pentru a fi la curent cu cele mai recente evoluții în politica de securitate cibernetică și pentru a contribui la formularea celor mai bune practici.
- Elaborează contribuții pentru răspunsuri și/sau puncte de vedere asupra actelor normative, a proiectelor de acte normative sau a adreselor privind acestea, care intră în sfera de competență a Directoratului, în calitate de autoritate de reglementare în domeniul securității cibernetice.
- Furnizează la cerere, expertiză și suport juridic, asistență, sprijin direct și/sau recomandări către funcțiile de conducere sau de execuție din compartimentele funcționale ale DNSC, în vederea îndeplinirii unor activități sau proiecte specifice.
- Identifică voluntari (elevi, studenți, absolvenți, etc.) în vederea colaborării cu DNSC și propune superiorilor ierarhici modalități de implicare a acestora în activitățile Directoratului.
- Participă, după caz, în pregătirea caietelor de sarcini și în comisiile de evaluare/negociere a contractelor de achiziție publică specifice nevoilor și activității **Direcției Verificare și Control.**
- Păstrează confidențialitatea datelor și informațiilor DNSC de care are cunoștință și care nu sunt de interes public, 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 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 Reglementare și Control (DGRC).**
- Propune, alege, adaptează, evaluează și folosește în activitatea curentă proceduri, metode, standarde, tehnici și instrumente privind activitățile de reglementare pentru care este responsabil(ă) sau în care este implicat(ă).
- Participă la sesiunile de pregătire profesională **organizate trimestrial la nivelul Direcției Verificare și Control**, pentru a asigura menținerea și îmbunătățirea cunoștințelor profesionale proprii.
- Participă activ la **ședințele interne organizate lunar** la nivelul **Direcției Verificare și Control.**
- 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.
- Susține cooperarea și lucrul în echipă la nivelul Direcției prin comunicare verbală și scrisă cu personalul acesteia și efectuează diseminarea permanentă a tuturor informațiilor relevante, conform propriilor atribuții, pentru buna desfășurare a activităților la nivelul Direcției.
- Identifică permanent și transmite atât către personalul de execuție de la nivelul Direcției cât și către superiorii ierarhici date și informații privind bunele practici, standarde, și legislația aplicabilă activităților Direcției.
- Răspunde pentru corectitudinea de fond și de formă a tuturor lucrărilor întocmite și/sau semnate.
- Face propuneri concrete de îmbunătățire a mijloacelor și metodelor de lucru la nivelul DGRC, pentru a maximiza utilizarea eficientă a timpului de lucru și a resurselor avute la dispoziție, în scopul 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.
- Pregătește datele și informațiile necesare și întocmește raportarea periodică, pentru indicatorii de performanță (KPIs - Key Performance Indicators) ai activităților proprii.
- 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.
- 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 din atribuțiile sale menționate în secțiunea anterioară vor fi preluate prin delegare de către una sau mai multe din următoarele funcții din **Direcția Verificare și Control**:
    - Coordonator superior securitate cibernetică - Direcția Verificare și Control
    - Expert legal politici, standardizare de securitate cibernetică - Direcția Verificare și Control
    - Asistent legal politici, standardizare de securitate cibernetică - Direcția Verificare și Control

  iar preluarea de atribuții se face prin desemnare de către **Managerul securitate cibernetică, din Direcția Verificare și Control.**

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, **în domeniul științe juridice**.

3.2 Experiență profesională, competențe și aptitudini necesare

- **NU SE SOLICITĂ EXPERIENȚĂ ANTERIOARĂ.**
- **Este de dorit experiența anterioară** în domeniul juridic, reglementare, securitate cibernetică, asigurarea conformității, managementul riscului, audit, protecția datelor sau un domeniu conex.
- **Este de dorit experiența anterioară** de lucrul în echipe de **minimum trei (3) persoane**.
- **Este de dorit experiența anterioară** de lucru în analiza de impact a reglementarilor (Regulatory Impact Assessment - RIA).
- **Este de dorit experiența anterioară de lucru în utilizarea platformei online „Fit for Future" a Comisiei Europene.**
- **Este de dorit experiența anterioară** de lucru într-o instituție guvernamentală sau de reglementare de preferință la nivel național sau internațional.
- **Este de dorit 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.
- Cunoașterea prevederilor din:

- OUG 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică.
- Ordonanţa nr. 2/2001 - privind regimul juridic al contravenţiilor, cu modificările și completările ulterioare.
- Legea 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative;
- Legea 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice.
- Legea 354/2022 privind protecția sistemelor informatice ale autorităților și instituțiilor publice în contextul invaziei declanșate de Federația Rusă împotriva Ucrainei.
- 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.
- Directiva (UE) 2022/2555 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (Directiva NIS 2);
- 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).

- Are capacitatea de înțelege și a aplica prevederile legilor, reglementărilor, standardelor, principiilor și bunelor practici naționale și internaționale de securitate cibernetică și de protecția datelor.
- Conștientizarea peisajului actual al securității cibernetice, inclusiv actorii amenințărilor, vectorii de atac, controalele de securitate, managementul riscurilor și răspunsul la incident.
- Cunoașterea rolurilor și responsabilităților diferitelor părți interesate din ecosistemul de securitate cibernetică, cum ar fi agențiile guvernamentale, industria și societatea civilă.
- Înțelegerea la un nivel general a tehnologiilor digitale cele mai uzuale și a impactului lor potențial din punct de vedere al securității cibernetice asupra societății, economiei, organizațiilor sau utilizatorilor.
- Abilități excelente de comunicare scrisă și verbală pentru a transmite informații complexe de reglementare în mod eficient către diverse părți interesate, inclusiv către publicul non-tehnic.
- Abilitatea de a identifica, analiza și rezolva probleme juridice complexe legate de conformitatea cu reglementările și standardele de securitate cibernetică.
- Abordare proactivă pentru identificarea oportunităților de îmbunătățire și luarea de măsuri pentru a îmbunătăți politicile, procedurile și liniile directoare de reglementare.
- Capacitatea de a oferi îndrumări și direcții echipelor interne și entităților reglementate în probleme de conformitate și de a promova o cultură a respectării reglementărilor.
- **Cunoștințe, competențe și abilitați (KSAs - knowledge, skills, and abilities) adecvate efectuării de activități de reglementare în domeniul securității cibernetice**, conform modului în care au fost 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 **tehnice**:

- **Rezolvarea de probleme - Problem Solving (C040)** - are aptitudini privind determinarea exactității și relevanței informațiilor și utilizarea unei judecăți profesionale solide pentru a evalua alternative; luarea unor decizii bine informate, obiective, care să ia în considerare faptele, obiectivele, constrângerile și riscurile, percepând în același timp impactul și implicațiile deciziilor proprii.
- **Managementul cunoștințelor - Knowledge Management (C029)** - are aptitudini privind valoarea informațiilor și cunoștințelor colectate/acumulate și metodele de partajare a acestora în cadrul unei organizații.
- **Cunoașterea/conștientizarea evoluțiilor tehnologice - Technology Awareness (C053)** - are aptitudini privind cunoașterea evoluțiilor tehnologice și utilizarea eficientă a tehnologiei pentru a obține rezultate.

- Cunoștințe, competențe și abilități **operaționale**:
  - **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.

- Experiență în analiza de date și informații și în pregătirea 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 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.
- Aptitudini de luare a deciziilor, inițiativă și autonomie în acțiune.

3.3 Instrumente și tehnologii de lucru

- Are experiență anterioară și poate să utilizeze **la un nivel general** aplicații de tip Office din lista de mai jos 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.
- Poate să utilizeze **la un nivel general** platforma online „Fit for Future” a Comisiei Europene.

3.4 Certificări sau cursuri de specializare

- **Are obligația ca în termen de maximum un (1) an de la data preluării postului, să obțină cel puțin una (1) din următoarele certificări** (sau echivalent) - costurile aferente fiind suportate de către DNSC:
  - CISM CompTIA Security+
  - CASP + - CompTIA Advanced Security Practitioner
  - CySA + - CompTIA Cybersecurity Analyst
  - CGEIT - Certified in the Governance of Enterprise IT

- CHA - Certified Hacker Analyst
- CHAT - Certified Hacker Analyst Trainer
- CISA - Certified Information Systems Auditor
- CISM - Certified Information Security Manager
- CISSP - Certified Information Systems Security Professional
- COBIT5 - COBIT 5 Certification
- CRISC - Certified in Risk and Information Systems Control
- CTA - OSSTMM Certified Trust Analyst
- ECSA - EC-Council / Certified Security Analyst
- GCIP - GIAC Critical Infrastructure Protection
- GIAC – GSEC Security Essentials Certification
- GIAC - GSNA Systems and Network Auditors
- GIAC - GCCC Critical Controls Certification
- GICSP - GIAC Global Industrial Cyber Security Professional
- GRID - GIAC Response and Industrial Defense
- OPSE - OSSTMM Professional Security Expert
- SSCP – Systems Security Certified Practitioner
- ISO 27001, ISO 27002, ISO 27005, ISO 270035, ISO 270032
- National Cyber Strategy
- Stakeholders Management
- Cyber Security Policy and Strategy
- Cyber Diplomacy
- Digital Diplomacy

3.5 Metodologii cunoscute

- **Este de dorit să cunoască cel puțin una (1)** din metodologiile sau cadrele tehnice (frameworks) din lista de mai jos:
  - Better Regulation Guidelines ale Uniunii Europene
  - Better Regulation Toolbox a Uniunii Europene

3.6 Cunoștințe de limba română și de limbi străine

- 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.

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

- **Procentul de entități reglementate evaluate / controlate pentru conformitatea cu reglementările și standardele aplicabile de securitate cibernetică** într-o anumită perioadă de timp (lunar, trimestrial, anual), din totalul entități reglementate de către Directorat.
- **Numărul de rapoarte de verificare și/sau control la a căror întocmire a contribuit.**
- **Procentul (%) de recomandări** scrise pentru care entitățile reglementate au adoptat planuri de remediere pentru a aborda problemele de neconformitate sau domeniile de îmbunătățire identificate.
- **Numărul total și numărul mediu de zile/om efectuat pentru activitățile de verificare și/sau control pe care le-a executat** într-o anumită perioadă de timp (lunar, trimestrial, anual).
- **Numărul de acțiuni de verificare și/sau control pe care le-a executat** într-o anumită perioadă de timp (lunar, trimestrial, anual) pe categorii de entități reglementate și ca distribuție geografică.
- **Procentul (%) de acțiuni de verificare și/sau control pe care le-a** executat într-o anumită perioadă de timp (lunar, trimestrial, anual), din totalul acțiunilor efectuate la nivelul **Direcției Verificare și Control**.
- **Numărul total și numărul mediu de solicitări de îndrumări sau sprijin primite de la entitățile reglementate**, care i-au fost alocate spre soluționare, precum și procentul de solicitări la care a răspuns în termen.
- **Numărul de voluntari** (elevi, studenți, absolvenți, etc.) pe care i-a identificat în vederea colaborării cu Directoratul.
- Efectuarea anual a unui **număr minimal de doua zeci și patru (24) ore de cursuri online sau fizic în domenii relevante pentru activitatea Direcției Verificare și Control:**
    - Reglementări naționale sau internaționale în domeniul securității cibernetice
    - Cooperare și parteneriat instituțional (național sau internațional)
    - Politici și strategii de securitate cibernetică
    - Standarde și certificări de securitate cibernetică
    - Metode și practici privind analiza de impact a reglementarilor (Regulatory Impact Assessment)
    - Management al activităților și sarcinilor specifice (task management)
    - Utilizarea aplicațiilor tip Office

  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**, 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 pentru care este responsabil(ă) sau în care este implicat(ă), venite din partea partenerilor instituționali, a contractorilor sau consultanților implicați.

Directoratul Național de Securitate Cibernetică

Nume + Prenume

Data _____

Nume + Prenume

Data _____

Nume + Prenume

Data _____

Angajat/Salariat

Nume + Prenume

Data _____