DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

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

Coordonator superior securitate cibernetică
#206

1 Identificarea postului

1.1 Numele si prenumele titularului

- NUME + PRENUME

1.2 Denumirea postului

- **Coordonator superior 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

- **II**

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 #206 în statul de funcții al DNSC**

1.6 Nivelul postului

- Conducere

1.7 Sfera relațională internă și externă

1.7.1 Ierarhice

- Se subordonează pe următoarea linie ierarhică următoarelor funcții de conducere:
  - **Manager securitate cibernetică** - Direcția Verificare și Control
  - **Manager superior securitate cibernetică** - Direcția Reglementare și Control; Conducere - Direcția Generală Reglementare și Control, care coordonează Direcția Verificare și Control
  - **Adjunctul Directorului DNSC** care coordonează Direcția Generală Reglementare și Control
  - **Directorul DNSC**
- Are în subordine:
  - Expert securitate cibernetică
  - Expert legal politici, standardizare de securitate cibernetică
  - Expert politici, strategii și cooperare securitate cibernetică
  - Asistent securitate cibernetică
  - Expert evaluator securitate rețele și sisteme informatice
  - Expert securitate rețele și sisteme informatice

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 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 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** în raport cu instituțiile din SNAOPSN, precum și din COSC, conform mandatului primit din partea superiorilor ierarhici.
- **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 control asupra îndeplinirii sarcinilor de către personalul din subordine, inclusiv contractorii și consultanții implicați, după caz.

2 Descrierea postului

2.1 Scopul principal al postului

- Coordonează **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 b) și art. 19.
- Efectuează un management activ și gestionarea resurselor, în vederea atingerii obiectivelor instituționale ale DNSC și ale **Direcției Verificare și Control.**
- Răspunde de aplicarea de 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

- **Participă și contribuie activ la efortul Direcției în vederea** pregătirii, verificării, validării și transmiterii pe baza anuală, către conducerea DNSC, a programului consolidat pentru dezvoltarea capabilităților **Direcției Verificare și Control** a DNSC, incluzând necesarului de resurse tehnice și non-tehnice, bugetul aferent împreună cu recomandări pertinente.
- **Contribuie la elaborarea strategiei instituționale de verificare și control** a entităților reglementate de DNSC și măsurilor concrete pentru dezvoltarea, revizuirea și implementarea politicilor, procedurilor și liniilor directoare de control al conformității securității cibernetice.
- **Propune modele și criterii obiective și execută sarcini specifice** pentru definirea priorităților și a foii de drum pentru activitățile **Direcției Verificare și Control.**
- Este implicat în **conducerea activităților Direcției** pe care o coordonează din punct de vedere metodologic, organizațional și operațional, inclusiv pentru personalul din subordine, contractorii, consultanții și alți colaboratori implicați.
- Acordă asistență de specialitate la dezvoltarea și implementarea politicilor, proiectelor de acte normative, procedurilor și liniilor directoare de reglementare ale DNSC.
- **Este responsabil pentru organizarea, planificarea și executarea programelor, proiectelor și activităților derulate de Direcția Verificare și Control** în parametrii stabiliți: timp, buget/cost, nivel de calitate, cerințe și obiective specifice.
- **Este responsabil pentru organizarea, planificarea și executarea activităților derulate de Direcția Verificare și Control** cu privire la verificarea și controlul laboratoarelor civile de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor care sunt utilizate în cadrul rețelelor și sistemelor informatice, în temeiul art. 19 al OUG 104/2021.
- **Întocmește, din proprie inițiativă sau la cerere, statistici și situații** privind entitățile reglementate de către DNSC.
- Menține un inventar și o înțelegere detaliată a procedurilor, metodelor, tehnicilor și instrumentelor de colectare a datelor și informațiilor aflate la dispoziția Direcției Verificare și Control, utilizându-le pentru a răspunde cerințelor și obiectivelor specifice ale DNSC.
- Acumulează experiența demonstrabilă necesară pentru a oferi formare și mentorat către grupuri și experți individuali din cadrul DNSC și al partenerilor instituționali, din România sau internațional.
- Avizează rapoartele rezultate din activitățile de verificare, evaluare și control destinate prezentării către conducerii DNSC, și este responsabil pentru formularea de propuneri de măsuri adecvate, conform legislației și reglementărilor în vigoare.
- Coordonează dezvoltarea și derularea de programe de instruire, ateliere sau prezentări pentru a educa entitățile reglementate cu privire la cerințele de conformitate cu securitatea cibernetică, cele mai bune practici și tendințele emergente.
- Coordonează activitățile personalului din subordine pe linia relaționării cu entitățile reglementate, partenerii din industrie, organizațiile guvernamentale și organizațiile internaționale și răepunde pentru îndeplinirea obiectivelor stabilite în acest sens.
- Este la curent cu evoluțiile în domeniul securității cibernetice, inclusiv actualizările legilor, reglementărilor, standardelor și bunelor practici, precum și amenințărilor și tehnologiilor digitale.
- Colaborează cu echipele interne, cum ar fi experții juridici și de reglementare, pentru a oferi îndrumări precise și în timp util cu privire la legile, reglementările și standardele de securitate cibernetică.
- Realizează dezvoltarea și implementarea de noi mecanisme pentru îmbunătățirea eficienței și a calității activităților Direcției Verificare și Control și personalului acesteia.
- **Organizează și efectuează direct și nemijlocit**, cel puțin trimestrial, sesiuni de pregătire profesională cu personalul din subordine, pentru a asigura menținerea și îmbunătățirea cunoștințelor profesionale ale acestora.

- Participă activ în programe, proiecte, activități și inițiative ale DNSC 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.
- Reprezintă DNSC 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, pe componenta de verificare și control.
- Răspunde pentru corectitudinea de fond și de formă a tuturor lucrărilor întocmite și/sau semnate.
- Răspunde de confidențialitatea datelor și informațiilor DNSC, în conformitate cu prevederile legale, regulamentele interne ale DNSC și cu instrucțiunile primite.
- Este implicat în conducerea ședințelor lunare ale Direcției, asigurând pregătirea adecvată a acestora.
- Coordonează, organizează și realizează activitățile de evaluare, verificare și control ale Direcției privind 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.
- Identifică problemele de neconformitate și domeniile de îmbunătățire și oferă recomandări entităților reglementate cu privire la modul de a atinge și menține conformitatea.
- Pregătește, menține și avizează 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.
- Acordă sprijin entităților reglementate în dezvoltarea și implementarea planurilor de remediere pentru a aborda problemele de neconformitate identificate și domeniile de îmbunătățire.
- Participă la consultări cu instituțiile statului, cu actori din mediul privat și din cel universitar, precum și cu parteneri internaționali cu privire la subiectul reglementărilor în domeniul securității cibernetice.
- Răspunde de întocmirea de **proceduri standard și/sau metodologii aplicate de de verificare și control** pe care le transmite către superiorii ierarhici și către colegii din Direcție, **pentru a fi utilizate în activitățile de verificare și control ale DNSC.**
- 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 **Direcției Verificare și Control**.
- Realizează dezvoltarea și implementarea de noi mecanisme pentru îmbunătățirea eficienței și a calității activităților **Direcției Verificare și Control** și personalului acesteia.

- 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 răspunsuri sau 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 DNSC, în calitate de autoritate de control și verificare.
- Furnizează la cerere, expertiză și suport tehnic, 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.
- Efectuează coordonarea și îndrumarea activității voluntarilor (elevi, studenți, absolvenți, etc.) care îi sunt asignați, în cadrul programului sau activităților de voluntariat derulate la nivelul **Direcției Verificare și Control.**
- Organizează și coordonează procurarea de bunuri și servicii necesare în cadrul Direcției și face propuneri concrete pentru necesarul de instrumente de lucru, aplicații și programe software, infrastructură, resurse umane și bugete, pe care le transmite către Conducerea DNSC.
- Face parte, după caz, din comisiile de concurs sau examen pentru posturile scoase la concurs de către DNSC, sau din comisiile de evaluare a achizițiilor publice organizate de DNSC, atât ca membru/membră, cât și ca președinte al comisiei.
- Răspunde de confidențialitatea datelor și informațiilor DNSC, 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).**
- 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.
- Colaborează și cooperează cu compartimentele funcționale ale DNSC, cu partenerii instituționali, inclusiv cu contractorii și consultanții implicați, pentru **identificarea, analiza și evaluarea de noi tehnologii, aplicații și programe software ce pot fi necesare activităților Direcției Verificare și Control**, și face propuneri concrete către superiorii ierarhici privind implementarea acestora la nivelul Direcției, al DGRC sau al DNSC.
- Facilitează cooperarea și lucrul în echipă la nivelul Direcției prin comunicare verbală și scrisă cu personalul acesteia și efectuează diseminarea permanentă a tuturor informațiilor relevante precum și urmărirea folosirii de către personalul Direcției a informațiilor furnizate.
- 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.
- Propune, alege, adaptează, evaluează și folosește în activitatea curentă proceduri, metode, standarde, tehnici și instrumente **privind activitățile de verificare și control** pentru care este responsabil(ă) sau în care este implicat(ă).

- 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.
- Răspunde pentru corectitudinea de fond și de formă a tuturor lucrărilor întocmite și/sau semnate.
- **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 securitate cibernetică - Direcția Verificare și Control
    - Expert 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.

3.2 Experiență profesională, competențe și aptitudini necesare

- **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**.
- Cunoașterea prevederilor din:
  - 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.
  - 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.
  - 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) 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).
  - DNSC Ordinul nr. 599/2019 privind aprobarea Normelor metodologice de identificare a operatorilor de servicii esențiale și furnizorilor de servicii digitale.
  - 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.
  - DNSC Decizia nr. 88/2020 privind aprobarea Listei standardelor și specificațiilor europene și internaționale.
- Cunoașterea **la un nivel general** a principiilor și conceptelor de bază privind securitatea informației / securitatea cibernetică: confidențialitate, disponibilitate, autentificare, integritate, control al accesului, non-repudiere, privacy (protecția datelor personale).
- 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 tehnologiilor emergente și a impactului lor potențial asupra securității cibernetice, protecției datelor și confidențialității.
- 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.

- Capacitate de a colabora eficient cu colegii, partenerii externi și părțile interesate într-un cadru de echipă.
- 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.
- Dorința de a învăța și de a se dezvolta continuu profesional în domeniul reglementării securității cibernetice.
- Capacitatea de a rămâne eficient și de a menține calmul sub presiune, într-un mediu de reglementare dinamic și cu ritm rapid.
- **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.
        - **Analiza amenințărilor - Threat Analysis (C055)** - are aptitudini privind procesul în care cunoașterea vulnerabilităților interne și externe relevante pentru o anumită organizație este corelată cu atacurile cibernetice din lumea reală.
        - **Evaluarea vulnerabilităților - Vulnerabilities Assessment (C057)** - are aptitudini privind principiile, metodele și instrumentele de evaluare a vulnerabilităților (e.g. în infrastructuri, rețele și sisteme informatice) precum și elaborarea sau recomandarea unor contramăsuri adecvate.
        - **Protejarea rețelelor - Computer Network Defense (C007)** - are aptitudini privind măsuri defensive pentru a detecta incidente, a răspunde și a proteja informațiile, sistemele informatice și rețelele împotriva amenințărilor cibernetice.
        - **Managementul incidentelor - Incident Management (C021)** - are aptitudini privind tactici, tehnologii, principii și procese pentru a analiza, prioritiza și gestiona incidentele cibernetice.
        - **Sisteme informatice / securitatea retelelor - Information Systems/Network Security (C024)** - are aptitudini privind metode, instrumente și proceduri, inclusiv elaborarea de planuri de securitate a informațiilor pentru a preveni vulnerabilitățile sistemelor informatice și pentru a menține sau a restabili securitatea sistemelor informatice și a serviciilor de rețea.
        - **Analiza de informații - Intelligence Analysis (C027)** - are aptitudini privind procesul prin care informațiile colectate despre un adversar sunt folosite pentru a răspunde la întrebări tactice despre operațiunile curente sau pentru a prezice comportamentul viitor al adversarilor cibernetici.

- **Analiza amenințărilor - Threat Analysis (C055)** - are aptitudini privind procesul în care cunoașterea vulnerabilităților interne și externe relevante pentru o anumită organizație este corelată cu atacurile cibernetice din lumea reală.
- **Evaluarea vulnerabilităților - Vulnerabilities Assessment (C057)** - are aptitudini privind principiile, metodele și instrumentele de evaluare a vulnerabilităților (e.g. în infrastructuri, rețele și sisteme informatice) precum și elaborarea sau recomandarea unor contramăsuri adecvate.

- 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.
  - **Cunoașterea/conștientizarea situației externe - External Awareness (C019) - este de dorit -** are aptitudini privind identificarea și înțelegerea modului în care problemele interne și externe influențează activitatea unei organizații.
  - **Managementul Riscului – Risk Management (C044)** - are aptitudini privind metode și instrumente utilizate pentru identificarea, evaluarea și gestionarea riscurilor.
- Cunoștințe, competențe și abilități **de leadership**:
  - **Instruirea celorlalți - Teaching Others (C052)** – are aptitudini pentru transmiterea de cunoștințe sau oferirea de informații sau instruire (despre un subiect sau o calificare).
  - **Management de proiect - Project Management (C042)** – cunoaște și aplică principiile, metodele sau instrumentele pentru dezvoltarea, planificarea, coordonarea și gestionarea proiectelor și resurselor, inclusiv monitorizarea și inspectarea costurilor, a lucrărilor și a performanței contractorilor.

- 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.
- 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 avansat** 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.
- Are experiență anterioară și poate să utilizeze **la un nivel avansat cel puțin una (1)** din următoarele aplicații, platforme sau instrumente de lucru din lista de mai jos sau echivalent:
  - COBIT® Online

- ISACA European Cybersecurity Audit Program
- ISACA VMware Server Virtualization Audit Program
- ISACA UNIX/LINUX Operating System Security Audit Program
- ISACA Microsoft Windows File Server Audit Program
- ISACA Microsoft SQL Server Database Audit Program
- ISACA Microsoft SharePoint Audit Program
- ISACA Microsoft Exchange Server Audit Program
- ISACA Network Perimeter Security Audit Program
- ISACA Identity Management Audit Program
- ISACA Cybercrime Audit Program
- ISACA IT Business Continuity Audit Program
- ISACA Azure Audit Program | Digital | English
- ISACA Amazon Web Services (AWS) Audit Program
- ISACA Windows Active Directory Audit Program
- ISACA MySQL Server Audit Program
- ISACA Social Media Audit Program
- ISACA Outsourced IT Environments Audit Program
- AuditBoard
- Intelex
- Tipalti
- SAP Audit Management
- TeamMate+ Audit
- KNIME
- Splunk
- Qlik
- Maltego
- Nessus
- AdaptiveGRC

3.4 Certificări sau cursuri de specializare

- **Trebuie să posede, la momentul angajării, cel puțin una (1)** din următoarele certificări sau cursuri de specializare (sau echivalent):
  - CompTIA Security+
  - CASP + - CompTIA Advanced Security Practitioner
  - 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
- CySA + - CompTIA Cybersecurity Analyst
- CASP+ - CompTIA Advanced Security Practitioner
- 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
- Cursuri organizate de autorități naționale competente (din state membre UE) sau de instituții ale UE în domeniul reglementării sau certificării de securitate cibernetică.

- **Are obligația ca în termen de maximum un (1) an de la data angajării, să obțină cel puțin una din următoarele certificări** (sau echivalent) - costurile aferente acesteia fiind suportate de către DNSC:
  - CISM CompTIA Security+
  - CASP + - CompTIA Advanced Security Practitioner
  - 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
  - CySA + - CompTIA Cybersecurity Analyst
  - CASP+ - CompTIA Advanced Security Practitioner
  - 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

3.5 Metodologii cunoscute

- Trebuie să cunoască **la un nivel avansat cel puțin una (1)** din metodologiile sau cadrele tehnice (frameworks) din lista de mai jos:
  - FIRST - Computer Security Incident Response Team (CSIRT) Services Roles and Competencies
  - FIRST - Computer Security Incident Response Team (CSIRT) Services Framework
  - ENISA - CSIRT maturity framework
  - Open CSIRT Foundation - Security Incident management Maturity Model (SIM3)
  - Information Technology Security Evaluation Criteria (ITSEC)
  - Committee of Sponsoring Organizations of the Treadway Commission (COSO)
  - Center for Internet Security's (CIS) Controls (v7.1 / 8.0)
  - Cybersecurity Maturity Model Certification (CMMC)
  - ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation (CC)
  - Common Methodology for Information Technology Security Evaluation (CEM)
  - Information Technology Infrastructure Library (ITIL)
  - Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)
  - EBIOS Risk Manager (EBIOS RM)
  - OWASP Security Knowledge Framework (SKF)
  - Information Technology Infrastructure Library (ITIL)

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 europene 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

- Deținere/obținere autorizație de acces la informații clasificate secrete de stat, **nivel STRICT SECRET.**
- *Notă: neeliberarea sau retragerea autorizației de acces determină încetarea contractului individual de muncă.*

4 Indicatori de performanță

- **Îndeplinirea cu succes** a pregătirii, verificării, validării și transmiterii pe baza anuală, către conducerea DNSC, a programului consolidat pentru dezvoltarea capabilităților **Direcției Verificare și Control** a DNSC, incluzând necesarului de resurse tehnice și non-tehnice, bugetul aferent împreună cu recomandări pertinente.
- Pregătirea și susținerea anuală a **unui (1) seminar de specialitate** la nivel național, **în format fizic, online sau hibrid**, cu focus pe activitatea și domeniile de competență ale **Direcției Verificare și Control** a DNSC precum și publicarea cu celeritate a raportului seminarului. Concluzii pozitive primite prin formularul de evaluare (feedback) completat de participanții la seminar.
- Numărul de programe de instruire, ateliere sau prezentări dezvoltate și furnizate de către **Direcția Verificare și Control** a DNSC pentru a educa entitățile reglementate cu privire la cerințele de conformitate și cele mai bune practici în materie de securitate cibernetică.
- Procentul de entități reglementate evaluate 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 acțiuni de verificare și/sau control pe care le-a coordonat și/sau executat** într-o anumită perioadă de timp (lunar, trimestrial, anual) pe categorii de entități reglementate și ca distribuție geografică.
- **Numărul de rapoarte de verificare și/sau control pe care le-a coordonat și/sau întocmit** în termenele stabilite (i.e. fără întârzieri nejustificate).
- **Numărul total și numărul mediu de zile/om pentru activitățile de verificare și/sau control pe care le-a coordonat și/sau executat** într-o anumită perioadă de timp (lunar, trimestrial, anual).
- **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 **proceduri standard de verificare și control** pe care le-a întocmit sau le-a actualizat într-o anumită perioadă de timp (lunar, trimestrial, anual).
- **Pregătirea și efectuarea** trimestrială a sesiunilor de pregătire profesională cu personalul din subordine, pentru a asigura menținerea și îmbunătățirea cunoștințelor profesionale ale acestora.
- **Pregătirea și efectuarea** adecvată a ședințelor lunare ale Direcției.
- Coordonarea și îndrumarea activității pentru **minimum un (1) voluntar anual,** asignat **Direcției Verificare și Control**, pe o perioadă de voluntariat de minimum o (1) lună.
- **Numărul de voluntari** (elevi, studenți, absolvenți, etc.) pe care i-a identificat în vederea colaborării cu Directoratul.
- Efectuarea anual a unui **număr minimal de șaisprezece (16) ore de cursuri online în domenii relevante pentru activitatea Direcției Verificare și Control,** 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.
- **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 Angajat

Nume + Prenume

Data _____

Nume + Prenume

Data _____

Nume + Prenume

Data _____

Nume + Prenume

Data _____