Acest document, în forma finală semnată de ambele părți este confidențial iar conținutul său este proprietatea DNSC. Faptul că sunteți în posesia unui exemplar, nu vă conferă dreptul de a dezvălui, copia, distribui sau disemina documentul integral sau părți ale acestuia. Dezvăluirea, copierea sau distribuirea prin orice mijloace a documentului, în forma finală semnată de ambele părți, integral sau parțial, fără acordul scris prealabil al DNSC sunt strict interzise și atrag răspunderea juridică.

DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

FIȘA DE POST
Direcția Generală Reglementare și Control
Direcția Atestare și Autorizare

Expert legal politici, standardizare securitate cibernetică
#247

Acest document, în forma finală semnată de ambele părți este confidențial iar conținutul său este proprietatea DNSC. Faptul că sunteți în posesia unui exemplar, nu vă conferă dreptul de a dezvălui, copia, distribui sau disemina documentul integral sau părți ale acestuia. Dezvăluirea, copierea sau distribuirea prin orice mijloace a documentului, în forma finală semnată de ambele părți, integral sau parțial, fără acordul scris prealabil al DNSC sunt strict interzise și atrag răspunderea juridică.

1 Identificarea postului

1.1 Numele si prenumele titularului

- NUME + PRENUME

1.2 Denumirea postului

- **Expert 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 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 Atestare și Autorizare**
- Sediul DNSC / telemuncă
- **Poziția #247 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 Atestare și Autorizare
    - **Manager securitate cibernetică** - Direcția Atestare și Autorizare
    - **Manager superior securitate cibernetică** - Conducere - Direcția Generală Reglementare 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)

Acest document, în forma finală semnată de ambele părți este confidențial iar conținutul său este proprietatea DNSC. Faptul că sunteți în posesia unui exemplar, nu vă conferă dreptul de a dezvălui, copia, distribui sau disemina documentul integral sau părți ale acestuia. Dezvăluirea, copierea sau distribuirea prin orice mijloace a documentului, în forma finală semnată de ambele părți, integral sau parțial, fără acordul scris prealabil al DNSC sunt strict interzise și atrag răspunderea juridică.

- 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 Atestare și Autorizare 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

- Nu are.

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 Atestare și Autorizare** și de către Conducerea Direcției Generale Reglementare și Control (DGRC) în baza prevederilor OUG 104/2021 art. 5 lit. b) și i).
- Elaborează şi actualizează normele metodologice, tehnice, precum şi regulamentele privind cerinţele referitoare la înfiinţarea, autorizarea şi funcţionarea echipelor CSIRT, desemnarea echipelor CSIRT sectoriale, cele referitoare la atestarea auditorilor calificaţi cu competenţe în domeniul securităţii serviciilor esenţiale şi a serviciilor digitale, precum şi normele referitoare la autorizarea formatorilor şi furnizorilor de servicii de formare și autorizarea laboratoarelor civile de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor utilizate în cadrul rețelelor și sistemelor informatice. Efectuează activități specifice de implementare și aplicare a acestor norme.
- Evaluează dacă auditorii, furnizorii de servicii de formare profesională, echipele CSIRT (Computer Security Incident Response Team) sau SOC (Security Operations Center) îndeplinesc criteriile de desfășurare a activităților în domeniul securității cibernetice pentru entitățile ce fac obiectul legislației din domeniul securității cibernetice.

2.2 Descrierea sarcinilor / atribuțiilor / activităților postului

- **Propune modele și criterii obiective pentru definirea priorităților și a foii de drum pentru activitățile Direcției Atestare și Autorizare.**

Acest document, în forma finală semnată de ambele părți este confidențial iar conținutul său este proprietatea DNSC. Faptul că sunteți în posesia unui exemplar, nu vă conferă dreptul de a dezvălui, copia, distribui sau dismina documentul integral sau părți ale acestuia. Dezvăluirea, copierea sau distribuirea prin orice mijloace a documentului, în forma finală semnată de ambele părți, integral sau parțial, fără acordul scris prealabil al DNSC sunt strict interzise și atrag răspunderea juridică.

- 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.
- Evaluează, din perspectivă juridică, dacă auditorii, furnizorii de servicii de formare profesională,echipele CSIRT sau SOC și laboratoarele civile de testare, evaluare și certificare a securității cibernetice îndeplinesc criteriile pentru desfășurarea activităților de securitate cibernetică pentru entitățile ce fac obiectul legislației sin domeniul securității cibernetice, evaluându-le calificările, expertiza, experiența și performanța, precum și alte date solicitate de legislație sau reglementările subsecvente.
- Dezvoltă, implementează și menține procesul de autorizare pentru furnizorii de servicii de securitate cibernetică și certificare, asigurându-se că îndeplinesc standardele necesare pentru lucrul cu entitățile ce fac obiectul legislației din domeniul securității cibernetice.
- Desfășoară și răspunde pentru legalitatea activităților efectuate la nivelul **Direcția Atestare și Autorizare pentru pregătirea și fundamentarea deciziilor prin care Directoratul:**
    - Autorizează, revocă sau reînnoiește **autorizarea echipelor CSIRT/CERT/SOC** ce deservesc operatori de servicii esențiale ori furnizori de servicii digitale.
    - Autorizează, revocă sau reînnoiește **autorizarea formatorilor și furnizorilor de servicii de formare** pentru echipele de intervenție, respectiv pentru auditorii de securitate.
    - Autorizează, revocă sau reînnoiește **atestatul auditorilor de securitate informatică** care pot efectua audit în cadrul rețelelor și sistemelor informatice ce susțin servicii esențiale ori furnizează servicii digitale.
    - Autorizează, revocă sau reînnoiește **autorizarea** laborat**oarelor civile de testare, evaluare și certificare a securității cibernetice** a produselor și serviciilor utilizate în cadrul rețelelor și sistemelor informatice
- Prin desemnare, răspunde de întreținerea și actualizarea registrului auditorilor la nivelul DNSC, conform prevederilor legale și efectuează activități specifice:
    - Aplică prevederile regulamentelor pentru atestarea și verificarea auditorilor de securitate informatică pentru rețelele și sistemele informatice aparținând operatorilor de servicii esențiale sau furnizorilor de servicii digitale.
    - Verifică condițiile de valabilitate pentru atestatele acordate audtorilor.
    - Efectuează activități în vederea acordării, prelungirii, suspendării sau retragerii de către Directorat a atestării pentru auditorii de securitate informatică pentru rețelele și sistemele informatice aparținând operatorilor de servicii esențiale sau furnizorilor de servicii digitale, în conformitate cu prevederile legale.
    - Verifică în urma sesizărilor sau din oficiu, îndeplinirea de către auditorii atestați a obligațiilor legale ce le revin.
- Elaborează propuneri concrete pentru tematicile pentru specializarea auditorilor în vederea atestării acestora.
- Elaborează propuneri concrete pentru autorizarea, verificarea, suspendarea sau retragerea autorizării formatorilor din domeniul auditului de securitate informatică pentru rețelele și sistemele informatice ale operatorilor de servicii esențiale și furnizorilor de servicii digitale.
- Efectuează verificări sau evaluări regulate ale furnizorilor de servicii autorizați, pentru a asigura conformitatea continuă cu criteriile și pentru a identifica orice domenii de îmbunătățire sau neconformitate.
- Oferă îndrumări și sprijin auditorilor, furnizorilor de servicii de formare profesională și echipelor CSIRT/CERT/ SOC în înțelegerea și îndeplinirea criteriilor de desfășurare a activităților de securitate cibernetică pentru entitățile ce fac obiectul legislației din domeniul securității cibernetice.

Acest document, în forma finală semnată de ambele părți este confidențial iar conținutul său este proprietatea DNSC. Faptul că sunteți în posesia unui exemplar, nu vă conferă dreptul de a dezvălui, copia, distribui sau disemina documentul integral sau părți ale acestuia. Dezvăluirea, copierea sau distribuirea prin orice mijloace a documentului, în forma finală semnată de ambele părți, integral sau parțial, fără acordul scris prealabil al DNSC sunt strict interzise și atrag răspunderea juridică.

- Menține înregistrări exacte și actualizate ale furnizorilor de servicii de securitate cibernetică autorizați, inclusiv detaliile privind autorizarea, informațiile de contact și starea de conformitate a acestora.
- Prin desemnare, ține evidența și publică pe website-ul DNSC listele actualizate ale auditorilor atestați, formatorilor, echipelor CSIRT/CERT/SOC și laboratoarelor de testare, evaluare și certificare autorizate.
- Colaborează cu echipele interne, cum ar fi experții tehnici, pentru a oferi îndrumări precise și în timp util cu privire la reglementările de securitate cibernetică și aplicabilitatea acestora la diverși furnizori de servicii.
- Elaborează propuneri concrete pentru autorizarea, verificarea, suspendarea sau retragerea autorizării echipelor CSIRT/CERT/ SOC și laboratoarelor civile de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor utilizate în cadrul rețelelor și sistemelor informatice.
- Pregătește și furnizează programe de formare, ateliere de lucru sau prezentări pentru a educa furnizorii de servicii de securitate cibernetică cu privire la criteriile de certificare și procesul de certificare.
- Este permanent la curent cu evoluțiile din mediul securității cibernetice, inclusiv actualizările legilor, reglementărilor, standardelor și bunelor practici, precum și amenințărilor și tehnologiilor emergente.
- Contribuie la dezvoltarea, revizuirea și implementarea regulamentelor, politicilor, procedurilor și liniilor directoare legate de evaluarea și autorizarea furnizorilor de servicii de securitate cibernetică și certificare de securitate cibernetică.
- Asigură legătura cu entitățile care beneficiază de servicii din domeniul securității cibernetice oferite de furnizori autorizați sau acreditați de DNSC, pentru a se asigura că interacționează cu furnizorii de servicii autorizați sau acreditați și pentru a oferi îndrumări privind selectarea furnizorilor potriviți în funcție de nevoile lor specifice.
- Organizează din proprie inițiativă, sau la cerere, consultări cu auditorii, furnizorii de servicii de formare profesională, echipele CSIRT/CERT/SOC, laboratoarele civile de testare, evaluare și certificare a securității cibernetice, cu privire la subiectul reglementărilor în domeniul securității cibernetice.
- Prin desemnare, ține evidența și verifică îndeplinirea condițiilor de eligibilitate de către membrii Comitetului de Reglementare al DNSC, în baza OUG nr.104/2021 art.10.
- Prin desemnare, asigură funcția de Secretariat al Comitetului de Reglementare al DNSC, în baza OUG nr.104/2021 art.10.
- Asigură participarea DNSC în grupurile de lucru pe tema reglementărilor în domeniul securității cibernetice, la nivel național și internațional, pe subiectele legate de atestarea și autorizarea auditorilor, furnizorilor de servicii de formare, și echipelor CSIRT/CERT/SOC.
- Prin desemnare, **gestionează informațiile postate pe site-ul web al DNSC privind activitățile de atestare și autorizare** ale Directoratului, precum și cele de pe pagina proprie de intranet/wiki a **Direcției Atestare și Autorizare**, pentru creșterea transparenței și vizibilității activității acesteia; și cooperează cu **Direcția Comunicare, Media și Marketing** și respectiv **Direcția Infrastructură Tehnică** în vederea modernizării și actualizării formei si conținutului site-ului web / paginii.
- 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 Atestare și Autorizare**.
- Realizează dezvoltarea și implementarea de noi mecanisme pentru îmbunătățirea eficienței și a calității activităților **Direcției Atestare și Autorizare** și personalului acesteia.
- Identifică nevoile, planifică și organizează derularea activității de pregătire continuă a personalului propriu, cu obiectivul general de a dezvolta, menține și diversifica resursele și expertiza existentă la nivelul Direcției.
- Ține evidența și gestionează documentele și actele normative interne distribuite la nivelul Direcției.

Acest document, în forma finală semnată de ambele părți este confidențial iar conținutul său este proprietatea DNSC. Faptul că sunteți în posesia unui exemplar, nu vă conferă dreptul de a dezvălui, copia, distribui sau disemina documentul integral sau părți ale acestuia. Dezvăluirea, copierea sau distribuirea prin orice mijloace a documentului, în forma finală semnată de ambele părți, integral sau parțial, fără acordul scris prealabil al DNSC sunt strict interzise și atrag răspunderea juridică.

- Acordă asistență de specialitate la dezvoltarea și implementarea politicilor, proiectelor de acte normative, procedurilor și liniilor directoare de reglementare ale 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 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 atestare și autorizare**.
- **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.
- Efectuează activități de coordonare și îndrumare a activității voluntarilor (elevi, studenți, absolvenți, etc.) care îi sunt asignați, în cadrul programului sau activităților de voluntariat derulate la nivelul **Direcției Atestare și Autorizare.**
- 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 sau președinte** al comisiei, în comisiile de evaluare/negociere a contractelor de achiziție publică specifice nevoilor și activității **Direcției Atestare și Autorizare.**
- Răspunde de confidențialitatea datelor și informațiilor transmise către DNSC sau procesate și analizate ca parte a activităților efectuate la nivelul Direcției, 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 Reglementare și Control (DGRC),** în acest caz cu avizul și aprobarea:
        - **Directorului DNSC,** și a
        - **Adjunctului Directorului DNSC** care coordonează Direcția Generală Expertiză și Proiecte (DGEP).
- 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).
- **Participă activ și contribuie la efectuarea sesiunilor de pregătire profesională organizate trimestrial la nivelul Direcției**, pentru a asigura menținerea și îmbunătățirea cunoștințelor profesionale proprii.
- **Participă activ la ședințele interne organizate lunar** la nivelul **Direcției Atestare și Autorizare.**
- 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.

Acest document, în forma finală semnată de ambele părți este confidențial iar conținutul său este proprietatea DNSC. Faptul că sunteți în posesia unui exemplar, nu vă conferă dreptul de a dezvălui, copia, distribui sau disemina documentul integral sau părți ale acestuia. Dezvăluirea, copierea sau distribuirea prin orice mijloace a documentului, în forma finală semnată de ambele părți, integral sau parțial, fără acordul scris prealabil al DNSC sunt strict interzise și atrag răspunderea juridică.

- Răspunde pentru corectitudinea de fond și de formă a tuturor lucrărilor întocmite și/sau semnate.
- Pregătește datele și informațiile necesare și întocmește raportarea periodică 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 acesteia; și efectuează diseminarea permanentă a tuturor informațiilor relevante, conform propriilor atribuții, precum și urmărirea folosirii de către personalul Direcției a informațiilor furnizate.
- **Face propuneri concrete de îmbunătățire a metodelor de lucru la nivelul Direcției**, atât direct în cadrul Direcției sau la nivelele ierarhice superioare, pentru a maximiza utilizarea eficientă a timpului de lucru și a resurselor avute la dispoziție în scopul atingerii obiectivelor instituționale.
- **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.
- **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, 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 din atribuțiile sale menționate în secțiunea anterioară vor fi preluate prin delegare de către una sau mai multe din următoarele funcții din **Direcția Atestare și Autorizare**:
    - Coordonator superior securitate cibernetică - Direcția Atestare și Autorizare
    - Expert legal politici, standardizare de securitate cibernetică - Direcția Atestare și Autorizare

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

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

- **Experiență anterioară dovedită de minim trei (3) ani** în domeniul juridic, reglementare, securitate cibernetică, asigurarea conformității, managementul riscului, audit, control, protecția datelor sau un domeniu conex, experiență **acumulată în ultimii zece (10) ani**.
- **Experiență anterioară dovedită de minim un (1) an** pentru lucrul în echipe de **minimum trei (3) persoane**.

Acest document, în forma finală semnată de ambele părți este confidențial iar conținutul său este proprietatea DNSC. Faptul că sunteți în posesia unui exemplar, nu vă conferă dreptul de a dezvălui, copia, distribui sau disemina documentul integral sau părți ale acestuia. Dezvăluirea, copierea sau distribuirea prin orice mijloace a documentului, în forma finală semnată de ambele părți, integral sau parțial, fără acordul scris prealabil al DNSC sunt strict interzise și atrag răspunderea juridică.

- **Este de dorit experiența anterioară** de lucru în laboratoare de testare a produselor și serviciilor digitale sau de securitate cibernetică, sau 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 nr.104/2021 privind înființarea Directoratului Național de Securitate Cibernetică;
    - Legea nr.58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative;
    - Legea nr.362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice;
    - Hotărârea nr.1.321/2021 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).
    - 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.
    - DNSC Ordinul nr. 559/2021 privind aprobarea Regulamentului pentru atestarea și verificarea auditorilor de securitate cibernetică.
    - DNSC Decizia nr. 107/2022 privind aprobarea tematicilor pentru formarea auditorilor de securitate cibernetică, a membrilor echipelor CSIRT și a responsabililor cu securitatea rețelelor și sistemelor informatice.
    - DNSC Ordinul nr. 106/2022 pentru aprobarea Normelor privind autorizarea și verificarea furnizorilor de servicii de formare pentru securitate cibernetică.
- 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.

Acest document, în forma finală semnată de ambele părți este confidențial iar conținutul său este proprietatea DNSC. Faptul că sunteți în posesia unui exemplar, nu vă conferă dreptul de a dezvălui, copia, distribui sau disemina documentul integral sau părți ale acestuia. Dezvăluirea, copierea sau distribuirea prin orice mijloace a documentului, în forma finală semnată de ambele părți, integral sau parțial, fără acordul scris prealabil al DNSC sunt strict interzise și atrag răspunderea juridică.

- Capacitate de a analiza, folosi și interpreta informații complexe de reglementare, de a evalua impactul potențial și de a oferi îndrumări clare și concise.
- Competență în efectuarea de cercetări cuprinzătoare pe subiecte complexe de securitate cibernetică utilizând diverse surse și instrumente și să rămână la curent cu cele mai recente evoluții.
- 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 legate de conformitatea cu reglementările și standardele de securitate cibernetică.
- Capacitate de a gestiona mai multe sarcini, de a prioritiza sarcinile de lucru și de a respecta termenele limită într-un mediu cu ritm rapid.
- Capacitatea de a se adapta la schimbările din peisajul de reglementare și de a rămâne la curent cu amenințările și tehnologiile în evoluție pentru securitatea cibernetică.
- Capacitatea de a evalua în mod critic informațiile de reglementare și de a lua decizii informate pe baza datelor disponibile.
- Angajamentul față de conduita etică, profesionalismul și aderarea la cele mai bune practici de reglementare, precum și capacitatea de a naviga dilemele etice și de a lua decizii corecte în contextul reglementării securității cibernetice.
- 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.
- 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**:
        - **Managementul conflictelor - Conflict Management (C009)** - are aptitudini privind la gestionarea și soluționarea conflictelor, reclamațiilor, confruntărilor sau dezacordurilor într-o manieră constructivă pentru a minimiza impactul negativ personal; colaborează cu alte persoane pentru a încuraja cooperarea și lucrul în echipă.
        - **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.

Acest document, în forma finală semnată de ambele părți este confidențial iar conținutul său este proprietatea DNSC. Faptul că sunteți în posesia unui exemplar, nu vă conferă dreptul de a dezvălui, copia, distribui sau disemina documentul integral sau părți ale acestuia. Dezvăluirea, copierea sau distribuirea prin orice mijloace a documentului, în forma finală semnată de ambele părți, integral sau parțial, fără acordul scris prealabil al DNSC sunt strict interzise și atrag răspunderea juridică.

- **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.

- 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 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.
- 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.

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:
    - CompTIA Security+
    - CySA + - CompTIA Cybersecurity Analyst
    - 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
    - CRISC - Certified in Risk and Information Systems Control
    - COBIT5 - COBIT 5 Certification
    - 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

Acest document, în forma finală semnată de ambele părți este confidențial iar conținutul său este proprietatea DNSC. Faptul că sunteți în posesia unui exemplar, nu vă conferă dreptul de a dezvălui, copia, distribui sau disemina documentul integral sau părți ale acestuia. Dezvăluirea, copierea sau distribuirea prin orice mijloace a documentului, în forma finală semnată de ambele părți, integral sau parțial, fără acordul scris prealabil al DNSC sunt strict interzise și atrag răspunderea juridică.

Acest document, în forma finală semnată de ambele părți este confidențial iar conținutul său este proprietatea DNSC. Faptul că sunteți în posesia unui exemplar, nu vă conferă dreptul de a dezvălui, copia, distribui sau disemina documentul integral sau părți ale acestuia. Dezvăluirea, copierea sau distribuirea prin orice mijloace a documentului, în forma finală semnată de ambele părți, integral sau parțial, fără acordul scris prealabil al DNSC sunt strict interzise și atrag răspunderea juridică.

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)

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

- Deținere/obținere autorizație de acces la informații clasificate secrete de stat, nivel **STRICT SECRET**.

4 Indicatori de performanță

- Numărul de evaluări de atestare/autorizare efectuate într-o perioadă de timp specificată, pentru diverselor categoriile de entități.
- Procentul (%) de auditori, furnizori de servicii de formare profesională, echipe CSIRT/CERT/SOC, laboratoare civile de testare, evaluare și certificare a securității cibernetice care obțin cu succes atestarea după ce au fost evaluați.
- Procentul (%) de evaluări de atestare/autorizare finalizate în termenele stabilite.

Acest document, în forma finală semnată de ambele părți este confidențial iar conținutul său este proprietatea DNSC. Faptul că sunteți în posesia unui exemplar, nu vă conferă dreptul de a dezvălui, copia, distribui sau disemina documentul integral sau părți ale acestuia. Dezvăluirea, copierea sau distribuirea prin orice mijloace a documentului, în forma finală semnată de ambele părți, integral sau parțial, fără acordul scris prealabil al DNSC sunt strict interzise și atrag răspunderea juridică.

- Numărul de solicitări de asistență primite de la furnizorii de servicii care solicită îndrumări cu privire la criteriile și procesele de certificare și procentul de solicitări rezolvate în timpul de răspuns stabilit.
- Numărul de programe de instruire, ateliere sau prezentări dezvoltate și oferite de specialist pentru a educa furnizorii de servicii de securitate cibernetică cu privire la criteriile și procesele de atestare/autorizare.
- Timpul mediu necesar pentru a finaliza evaluările de atestare/autorizare.
- Nivelul de implicare și impactul generat în dezvoltarea, revizuirea și implementarea politicilor, regulamentelor, procedurilor și liniilor directoare de atestare/autorizare.
- Pregătirea și susținerea anuală **a unui (1) seminar de specialitate (în format fizic, online sau hibrid)** privind activitatea **Direcției Atestare și Autorizare**, precum și publicarea cu celeritate a raportului seminarului; concluzii pozitive primite prin formularul de evaluare (feedback) completat de participanții la seminar.
- Coordonarea și îndrumarea activității pentru **minimum un (1) voluntar anual,** asignat **Direcției Atestare și Autorizare**, 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 Atestare și Autorizare, spre exemplu:**
    - Reglementări naționale sau internaționale în domeniul securității cibernetice
    - Politici și strategii de securitate cibernetică
    - Standarde și certificări de securitate cibernetică
    - Audit, IT Audit, Security Audit, Third Party Assurance
    - Activități ale entităților de tip CERT/CSIRT/SOC
    - Management al activităților și sarcinilor specifice (task management)
    - Confidențialitatea și protecția datelor
    - 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 Atestare și Autorizare**, 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	Angajat
Nume + Prenume	**Nume + Prenume**
Data _____	Data _____

Nume + Prenume

Data _____

Nume + Prenume

Data _____

Acest document, în forma finală semnată de ambele părți este confidențial iar conținutul său este proprietatea DNSC. Faptul că sunteți în posesia unui exemplar, nu vă conferă dreptul de a dezvălui, copia, distribui sau disemina documentul integral sau părți ale acestuia. Dezvăluirea, copierea sau distribuirea prin orice mijloace a documentului, în forma finală semnată de ambele părți, integral sau parțial, fără acordul scris prealabil al DNSC sunt strict interzise și atrag răspunderea juridică.