



DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

FIȘA DE POST

Direcția Generală Reglementare și Control

Direcția Monitorizare Reglementări Interne și Internaționale

Expert legal, politici, standardizare securitate cibernetică

#255

1	Identificarea postului	2
1.1	Numele si prenumele titularului.....	2
1.2	Denumirea postului.....	2
1.3	Gradul profesional / treapta profesională	2
1.4	Poziția în COR (Clasificarea Ocupațiilor din Romania)	2
1.5	Compartimentul funcțional și locația.....	2
1.6	Nivelul postului	2
1.7	Sfera relațională internă și externă.....	2
1.7.1	Ierarhice	2
1.7.2	Funcționale	2
1.7.3	Reprezentare	3
1.7.4	Control	3
2	Descrierea postului	3
2.1	Scopul principal al postului	3
2.2	Descrierea sarcinilor / atribuțiilor / activităților postului	3
2.3	Delegarea de atribuții și competență.....	6
3	Condiții specifice de ocupare a postului	7
3.1	Studii de specialitate	7
3.2	Experiență profesională, competențe și aptitudini necesare	7
3.3	Instrumente și tehnologii de lucru	9
3.4	Certificări sau cursuri de specializare	9
3.5	Metodologii cunoscute	9
3.6	Cunoștințe de limba română și de limbi străine.....	10
3.7	Cerințe privind cetățenia.....	10
3.8	Autorizații speciale pentru exercitarea atribuțiilor	10
4	Indicatori de performanță.....	11

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

- 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 apropiată din punct de vedere al sarcinilor și responsabilităților.*

1.5 Compartimentul funcțional și locația

- Direcția Generală Reglementare și Control - Direcția Monitorizare Reglementări Interne și Internaționale
- Sediul DNSC / telemuncă
- Poziția #255 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 Monitorizare Reglementări Interne și Internaționale
 - **Manager securitate cibernetică** - Direcția Monitorizare Reglementări Interne și Internaționale
 - **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 Expertiză și Proiecte (toate compartimentele)

- 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 Monitorizare Reglementări Interne și Internaționale 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 Monitorizare Reglementări Interne și Internaționale** și de către Conducerea Direcției Generale Reglementare și Control (DGRC) în baza prevederilor OUG 104/2021 art. 5 b) și art.10 alin. (10).
- Răspunde de cunoașterea la zi și efectuează monitorizarea și analiza continuă a legislației și reglementărilor naționale și internaționale referitoare la securitatea cibernetică, sau a celor din domenii conexe, în scopul identificării oricăror modificări care au un impact asupra activității, rolului și/sau responsabilităților Directoratului.
- Efectuează analiza de impact a propunerilor și inițiativelor de acte normative în domeniul securității cibernetice și pregătește și emite puncte de vedere, rapoarte și recomandări către Conducerea Directoratului, Conducerea compartimentelor funcționale ale Directoratului sau către parteneri instituționali, ori public, după caz.

2.2 Descrierea sarcinilor / atribuțiilor / activităților postului

- Participă în mod activ și contribuie la elaborarea, validarea și implementarea strategiei de reglementare a DNSC, împreună cu personalul de conducere și execuție din **Direcția Monitorizare Reglementări Interne și Internaționale**.
- Propune modele și criterii obiective pentru definirea priorităților și a foii de drum pentru activitățile Direcției Monitorizare Reglementări Interne și Internaționale.

- Monitorizează și analizează legislația, reglementările și standardele naționale și internaționale de securitate cibernetică pentru a identifica tendințele emergente, impactul potențial și cerințele de conformitate.
- Menține un inventar și o înțelegere cuprinzătoare și actualizată a peisajului legal și de reglementare actual legat de securitatea cibernetică (inclusiv cea specifică sectoarelor din aria de responsabilitate a DNSC, respectiv din domeniile conexe, cum ar fi protecția datelor cu caracter personal, protecția infrastructurilor critice, standardizarea și certificarea, gestionarea documentelor clasificate).
- Dezvoltă și menține o evidență actualizată a legilor, reglementărilor și standardelor relevante pentru a facilita accesul la informații și pentru a sprijini eforturile de conformare.
- Pregătește rapoarte, buletine, note, briefing-uri și prezentări pentru a comunica palierelor de conducere din DNSC actualizările legislative și de reglementare relevante pentru domeniul securității cibernetice, precum și propuneri în consecință.
- Colaborează cu structurile din cadrul DNSC și cu părțile interesate externe pentru a evalua impactul potențial al noilor legi, reglementări și standarde asupra organizației și entităților reglementate.
- Furnizează îndrumări și sprijin altor structuri din cadrul DNSC și entităților reglementate cu privire la conformitatea cu legile, reglementările și standardele de securitate cibernetică.
- Acordă asistență de specialitate la dezvoltarea și implementarea politicilor, proiectelor de acte normative, procedurilor și liniilor directe de reglementare privind securitatea cibernetică ale DNSC.
- 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.
- **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.
- Monitorizează activ site-urile de web ale partenerilor instituționali din Statele Membre ale UE, Instituții UE și internațional și întocmește lunar rapoarte și/sau note de informare privind inițiativele, activitățile și publicațiile de reglementare, certificare și standardizare privind securitatea cibernetică ale acestora.
- **Dezvoltă, furnizează și participă activ** la programe de formare sau ateliere de lucru privind legile, reglementările și conformitatea privind securitatea cibernetică pentru echipele interne, parteneri instituționali și pentru entitățile reglementate.
- Răspunde de publicarea pe site-ul web al DNSC a unei secțiuni privind inițiativele legislative și/sau de reglementare ori acte normative **relevante la nivel național sau internațional** și cooperează cu **Direcția Comunicare, Media și Marketing** și respectiv cu **Direcția Infrastructură Tehnică** în vederea modernizării și actualizării formei și conținutului site-ului web / paginii.
- Face propuneri concrete privind activități de comunicare și schimb de cunoștințe între DNSC și partenerii instituționali ai DNSC pe domeniul de reglementare al securității cibernetice, inclusiv pentru monitorizarea reglementărilor în pregătire sau deja implementate.
- 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.
- **Stabilește și menține canale de comunicare și schimb de informații** (person-to-person, team-to-team, machine-to-machine) precum și relații de cooperare, colaborare și de consultare periodică cu experți în domeniul de reglementare din cadrul partenerilor instituționali ai DNSC.
- Efectuează analize și oferă recomandări cu privire la:
 - Claritatea limbajului sau a conceptelor introduse de actele normative de la nivel național, european și internațional și modul în care acestea se aplică industriei și mediului de securitate cibernetică aferent.

- Capacitatea de a crea mecanismele de aplicare a reglementărilor relevante în materie de securitate cibernetică.
- Coerența politicilor și reglementărilor naționale în domeniul securității cibernetică cu strategia națională și alte norme legale și reglementări naționale și internaționale.
- **Participă activ** la forumuri din industrie, conferințe, workshop-uri, seminarii și grupuri de lucru pe tema reglementărilor în domeniul securității cibernetică 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, la nivel național și internațional.
- **Asigură în mod activ, pregătește și sprijină efectiv participarea Directoratului** la lucrările comisiilor de specialitate ale Parlamentului României, sau la grupuri de lucru guvernamentale, în vederea susținerii punctelor de vedere ale DNSC asupra proiectelor de acte normative aflate pe agenda de lucru a comisiilor.
- **Elaborează în mod activ 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 reglementare pe domeniul civil al securității cibernetică.
- **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 coordonarea și îndrumarea activității voluntarilor (elevi, studenți, absolvenți, etc.) care îi sunt asigurați, în cadrul programului sau activităților de voluntariat derulate la nivelul **Direcției Monitorizare Reglementări Interne și Internaționale**.
- 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 Monitorizare Reglementări Interne și Internaționale**.
- **Păstrează și răspunde de confidențialitatea datelor și informațiilor** transmise către DNSC sau procesate și analizate ca parte a activităților efectuate la nivelul Direcției, de care are cunoștință, 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 Monitorizare Reglementări Interne și Internaționale**, pentru a asigura menținerea și îmbunătățirea cunoștințelor profesionale proprii.
- **Participă activ la ședințele interne organizate lunar la nivelul Direcției Monitorizare Reglementări Interne și Internaționale.**
- Asigură o comunicare adecvată, prin metode de comunicare scrisă, discuții și feedback la nivelul Direcției precum și între această direcție și alte compartimente funcționale din cadrul DNSC și/sau partenerii instituționali.
- Răspunde pentru corectitudinea de fond și de formă a tuturor lucrărilor întocmite și/sau semnate.
- Pregătește datele și informațiile necesare și întocmește raportarea 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 Monitorizare Reglementări Interne și Internaționale**:
 - Coordonator superior securitate cibernetică
 - Expert legal politici, standardizare de securitate cibernetică
 - Asistent legal politici, standardizare de securitate cibernetică

iar preluarea de atribuții se face prin desemnare de către **Managerul securitate cibernetică, din Direcția Monitorizare Reglementări Interne și Internaționale.**

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 doi (2) ani** pentru lucrul în echipe de **minimum trei (3) persoane**.
- **Este de dorit experiența anterioară de lucru în analiza de impact a reglementărilor (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 cibernetică.**
- **Cunoașterea prevederilor din Better Regulation Guidelines și Better Regulation Toolbox ale Uniunii Europene.**
- Cunoașterea prevederilor din:
 - Ordonanța de urgență a Guvernului nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, aprobată prin Legea nr. 11 din 07.01.2022.
 - Legea 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative.
 - Legea nr. 362 din 28 decembrie 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 Guvernului nr. 1321/2021 privind aprobarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027, precum și a Planului de acțiune pentru implementarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027.
 - 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 cibernetică pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică).
- **Înțelegerea cuprinzătoare a legilor, reglementărilor, standardelor și bunelor practici naționale și internaționale de securitate cibernetică.**
- **Familiarizarea cu legile, reglementările și principiile privind protecția datelor și confidențialitatea.**
- **Conștientizarea peisajului actual al securității cibernetică, 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 cibernetică, 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.
- 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 abilități (KSAs - knowledge, skills, and abilities) adecvate efectuării de activități de reglementare în domeniul securității cibernetică, 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 cibernetică 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.
 - **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.
- **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.
- **Managementul relațiilor - Client/Stakeholder Relationship Management (C003)** - are aptitudini privind conceptele, practicile și tehnicile utilizate pentru a identifica, a se angaja cu, a influența și monitoriza relațiile cu persoane și grupuri conectate la un efort de lucru, inclusiv cei implicați activ, cei care exercită influență asupra procesului și a rezultatelor sale și cei care au un interes legitim în rezultat (pozitiv sau negativ).

- **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.
- 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:**
 - 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

3.5 Metodologii cunoscute

- 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 C1 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 C1 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 muncă 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

- **Număr de rapoarte, buletine, note, briefing-uri și prezentări pe care le-a pregătit** pentru a comunica propunerile de actualizări legislative și de reglementare relevante într-o anumită perioadă de timp (lunar, trimestrial, anual) și procentul (%) documentelor de acest tip care conțin propuneri concrete.
 - **Numărul și procentul situațiilor în care a inițiat consultări 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, urmare a realizării de rapoarte, buletine, note, briefing-uri și prezentări cu scopul de comunicare a actualizărilor legislative. Măsura în care din demersurile subsecvente acestor activități de cooperare rezultă date și informații care sunt ulterior transpuse în acte de reglementare.
 - **Numărul de răspunsuri sau contribuții pentru răspunsuri sau puncte de vedere** asupra actelor normative, a proiectelor de acte normative sau a adreselor privind acestea.
 - **Numărul de participări la comisiile de specialitate ale Parlamentului României sau la grupuri de lucru guvernamentale** în vederea susținerii punctelor de vedere ale DNSC asupra proiectelor de acte normative și procentul (%) în care proiectele respective sunt respinse sau aprobate în forul legislativ.
 - **Numărul de proiecte de acte normative inițiate de către DNSC** pentru reglementarea domeniului securității cibernetice la elaborarea cărora a contribuit activ și direct într-o anumită perioadă de timp (lunar, trimestrial, anual).
 - **Coordonarea și îndrumarea activității pentru minimum un (1) voluntar anual**, asignat Direcției, 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 sau fizic în domenii relevante pentru activitatea Direcției Monitorizare Reglementări Interne și Internaționale:**
 - 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 Monitorizare Reglementări Interne și Internaționale**, 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.

Nume + Prenume

Data _____

Nume + Prenume

Data _____

Nume + Prenume

Data _____

Nume + Prenume

Data _____