



DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

FIȘA DE POST

Direcția Generală Operațiuni Tehnice

Direcția Infrastructură Tehnică

Expert dezvoltare, implementare și administrare infrastructuri securitate cibernetică

#880

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	6
3.1	Studii de specialitate	6
3.2	Experiență profesională, competențe și aptitudini necesare	6
3.3	Instrumente și tehnologii de lucru	8
3.4	Certificări sau cursuri de specializare	8
3.5	Metodologii cunoscute	9
3.6	Cunoștințe de limba română și de limbi străine.....	9
3.7	Cerințe privind cetățenia.....	9
3.8	Autorizații speciale pentru exercitarea atribuțiilor	9
4	Indicatori de performanță.....	9

1 Identificarea postului

1.1 Numele si prenumele titularului

- NUME + PRENUME

1.2 Denumirea postului

- Expert dezvoltare, implementare și administrare infrastructuri 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

- Superior

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 Operațiuni Tehnice - Direcția Infrastructură Tehnică
- Sediul DNSC / telemuncă
- Poziția #880 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 Infrastructură Tehnică
 - **Manager securitate cibernetică** - Direcția Infrastructură Tehnică
 - **Manager superior securitate cibernetică** - Direcția Infrastructură Tehnică
 - **Manager superior securitate cibernetică** - Direcția Generală Operațiuni Tehnice; Conducere - Direcția Generală Operațiuni Tehnice, care coordonează Direcția Infrastructură Tehnică
 - **Adjunctul Directorului DNSC** care coordonează Direcția Generală Operațiuni Tehnice
 - **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 Operațiuni Tehnice (toate compartimentele)
 - Direcția Generală Strategie
 - Conducere Direcția Generală Strategie
 - Direcția Studii, Cercetare și Analiză Aprofundată

- Direcția Prognoză, Raportare și Indicatori Cibernetic
- Direcția Management al Riscurilor Cibernetic
- Direcția Comunicare, Media și Marketing
- Serviciul Protecție Reputație și Marcă în Spațiul Cibernetic
- Direcția Generală Parteneriate Instituționale (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 DNSC și interesele DNSC** în raport cu părțile interne și externe implicate în activitățile specifice de preluare, analiză primară și răspuns la incidente de securitate cibernetică, în contextul funcției de CSIRT/CERT Sectorial a DNSC.
- **Reprezintă DNSC și interesele DNSC** în raport cu experți individuali și organizații profesionale sau non-guvernamentale implicate în activități profesionale, de conștientizare și educație privind echipe de tipul:
 - Security Operations Center (SOC)
 - IT / Information Security Helpdesk
 - Network Administrators

1.7.4 Control

- Nu are.

2 Descrierea postului

2.1 Scopul principal al postului

- Efectuează activități specifice de proiectare, instalare, administrare a infrastructurii IT&C, de rețea și administrarea serverelor de date de la nivelul Directoratului.

2.2 Descrierea sarcinilor / atribuțiilor / activităților postului

- Răspunde de confidențialitatea datelor privind incidentele tehnice procesate și analizate la nivelul **Direcției Infrastructură Tehnică**, în conformitate cu prevederile legale, regulamentele interne ale DNSC și cu instrucțiunile primite.
- Asigură mentenanța echipamentelor active din cadrul infrastructurii de comunicații și tehnologia informației în vederea asigurării conectivității și atingerea parametrilor normali de funcționare.
- Realizează proiectii de dezvoltare a rețelelor de comunicații de date și suportul pentru implementarea tuturor soluțiilor tehnice de la nivelul Directoratului.
- Asigură mentenanța serverelor ce deservește aplicațiile instalate și configurate la nivelul infrastructurii de date.
- Asigură intervențiile pentru remedierea disfuncționalităților sistemelor de comunicații și date, salvează și restaurează configurațiile acestora.

- Participă la recepții calitative/cantitative a serviciilor, mijloacelor tehnice și materialelor din domeniul comunicațiilor de date.
- Asigură funcționarea continuă a sistemelor informatice aflate în administrare și monitorizează funcționarea serverelor, mașinilor virtuale și aplicațiilor software aflate în administrare.
- Monitorizează sistemele de electroalimentare și climatizare ale camerelor tehnice aflate în administrare care găzduiesc echipamente IT&C.
- Asigură reviziile tehnice și reparațiile echipamentelor de prelucrare a datelor în scopul menținerii la nivelurile maxime a parametrilor tehnico-funcționali.
- Desfășoară activități de instalare, administrare, exploatare și întreținere a serverelor, bazelor de date și aplicațiilor informatice aflate în producție și urmărește asigurarea continuă a parametrilor tehnici și funcționali definiți în specificațiile tehnice.
- Asigură optimizarea procedurilor manuale în scopul sporirii gradului de automatizare a acestora, îmbunătățirii calității datelor și reducerii timpului de răspuns al sistemului.
- Administrează aplicațiile software utilizate în cadrul soluțiilor de virtualizare și de stocare necesare, utilizate la implementarea serverelor de date.
- Administrează și întreține site-urile și portal-urile web ale instituției.
- Administrează și întreține server-ul de mail al instituției precum și conturile de poștă electronică.
- Asigură intervenții și remediază problemele de natură hardware și software la tehnica de calcul repartizată personalului Directoratului.
- Efectuează instalări, reinstalări, configurări, conectări și optimizări software.
- Desfășoară activități de testare funcțională a unor aplicații și produse informatice.
- Execută lucrări de cablare a unor rețele structurate noi și de extindere a celor existente.
- Dezvoltă site-uri web și utilizează aplicații de tip CMS (Content Management System).
- Monitorizează și optimizează performanța website-urilor dezvoltate.
- Testează periodic securitatea site-urilor web aflate în administrare în vederea identificării unor eventuale vulnerabilități.
- Asigură managementul flotei de abonați ficși și mobili utilizați de personalul Directoratului și administrează echipamentele de interconectare voce-date.
- Implementează măsurile de securitate aplicabile configurației hardware și software pentru sistemele informatice pe care se gestionează informații clasificate, activitate realizată sub coordonarea administratorului de securitate.
- Implementează modificările și îmbunătățirile configurației sistemelor pe care se gestionează informații clasificate, astfel încât obiectivele securității acestora să nu fie afectate.
- Asigură gestionarea conturilor de acces create pe sistemele informatice și de comunicații pe care se gestionează informații clasificate, din perspectiva creării/blocării/dezactivării acestora.
- Comunică către structura de securitate orice incident/suspiciune de incident/prejudicii/vulnerabilități/anomalii în ceea ce privește funcționarea sistemelor informatice și de comunicații pe care se gestionează informații clasificate.
- Asigură gestionarea și repartizarea capacităților hardware/software precum și utilizarea echipamentelor informatice și de comunicații pe care se gestionează informații clasificate în condiții optime.
- Asigură întreținerea și repararea sistemelor informatice și de comunicații pe care se gestionează informații clasificate.
- Asigură, din punct de vedere tehnic, fundamentarea și implementarea programelor de investiții și întreținere pentru echipamentele de comunicații și tehnologia informației.
- 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 Operațiuni Tehnice (DGOT).
- Folosește în activitatea curentă proceduri, metode, standarde, tehnici și instrumente privind incidentele de securitate cibernetică respectiv administrarea sistemelor informatice existente la nivelul **Direcției Infrastructură Tehnică**.
- Participă la sesiunile de pregătire profesională **organizate trimestrial la nivelul Direcției Infrastructură Tehnică**, pentru a asigura menținerea și îmbunătățirea cunoștințelor profesionale proprii.
- Asigură o comunicare adecvată, prin metode de comunicare scrisă, discuții și feedback la nivelul **Direcției Infrastructură Tehnică** precum și între această direcție și alte compartimente funcționale din cadrul DNSC, constituenți și/sau partenerii instituționali.
- Răspunde pentru corectitudinea de fond și de formă a tuturor lucrărilor întocmite și/sau semnate.
- Lucrează atât individual cât și în echipă; facilitează cooperarea și lucrul în echipă la nivelul **Direcției Infrastructură Tehnică** prin comunicare verbală și scrisă cu personalul direcției, diseminarea permanentă a tuturor informațiilor relevante către personalul direcției.
- Face propuneri concrete de îmbunătățire a mijloacelor și metodelor de lucru la nivelul **Direcției Infrastructură Tehnică**, pentru a maximiza utilizarea eficientă a timpului de lucru și a resurselor avute la dispoziție, în scopul atingerii obiectivelor instituționale.
- **Asigură identificarea și rezolvarea cu celeritate** a problemelor apărute în derularea activităților curente în care este implicat(ă) și informează la timp superiorii ierarhici despre problemele apărute pe care nu le poate rezolva la nivelul său.
- Pregătește datele și informațiile necesare și întocmește raportarea periodică, pentru următorii **indicatori de performanță (KPIs - Key Performance Indicators)** ai activităților proprii:
 - Numărul total și numărul mediu de intervenții tehnice gestionate într-o anumită perioadă de timp (lunar, trimestrial, anual) pe nivele de prioritate.
 - Procentul (%) de incidente tehnice gestionate într-o anumită perioadă de timp (lunar, trimestrial, anual) pe nivele de prioritate, din totalul incidentelor tehnice gestionate la nivelul **Direcției Infrastructură Tehnică**.
 - Durata medie de timp necesară pentru a răspunde sau rezolva un incident tehnic (**MTTR - Mean Time to Resolution**) pentru rezolvarea căruia este responsabil(ă), pe baza datelor și informațiilor aferente tichetelor procesate la nivelul **Direcției Infrastructură Tehnică**.
 - Rata cu care incidentele sunt rezolvate în timpul primei apariții.
- Efectuează coordonarea și îndrumarea activității voluntarilor (elevi, studenți, absolvenți, etc.) ce sunt îi sunt asigurați în cadrul programului sau activităților de voluntariat derulate la nivelul **Direcției Infrastructură Tehnică**.
- 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 Infrastructură Tehnică**:
 - Expert dezvoltare, implementare și administrare infrastructuri securitate ciberneticăiar preluarea de atribuții se face prin desemnare de către **Managerul superior securitate cibernetică, din Direcția Infrastructură Tehnică**.

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 dovedită de minimum un (1) an în echipe de tipul următor (sau echivalent), acumulată în ultimii cinci (5) ani:**
 - Computer Emergency Response Team (CERT)
 - Security Operations Center (SOC)
 - IT / Information Security Helpdesk
 - Network Administrators
- 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, Secțiunea a 3-a Managementul incidentelor Art. 27, 28, 29;
 - 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;
 - Standardul Ocupațional din Romania pentru: Codul Nomenclator / COR al calificării / ocupației: **Expert în securitate cibernetică 252904**.
- Cunoașterea **la un nivel general** a principiilor și conceptelor de bază privind securitatea informației / securitatea cibernetică: confidențialitate, disponibilitate, autentificare, integritate, control al accesului, non-repudiare, privacy (protecția datelor personale).
- Abilitatea de a procesa și analiza date și informații în scopul pregătirii de **rapoarte și rezumate de un nivel calitativ foarte ridicat**, ce includ utilizarea de tabele, imagini ilustrative sau grafice pentru sublinierea de concluzii și inter-relaționare a datelor și informațiilor analizate.
- 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.
- 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.

- **Cunoștințe, competențe și abilități (KSAs - knowledge, skills, and abilities) specifice efectuării de activități în cadrul unui CSIRT**, așa cum acestea sunt definite de National Institute of Standards and Technologies (NIST) National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity Education (i.e. NICE Framework):
 - **Cunoștințe, competențe și abilități profesionale:**
 - **Gândire critică - Critical Thinking (C011)** - are aptitudini privind analiza obiectivă a faptelor pentru a forma o judecată profesională.
 - **Comunicare orală/verbală - Oral Communication (C036)** - are aptitudini privind exprimarea informațiilor sau a ideilor prin viu grai.
 - **Comunicare scrisă - Written Communication (C060)** - are aptitudini privind formularea și comunicarea oricărui tip de mesaj care utilizează cuvântul scris.
 - **Cunoștințe, competențe și abilități 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.
 - **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 rețelelor - 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.

3.3 Instrumente și tehnologii de lucru

- Are experiență anterioară dovedită 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 practică cu, sau poate să proiecteze/opereze **la un nivel avansat** cel puțin în următoarele domenii/tehnologii/produse:
 - Tehnologii de rețea
 - Virtualizare / Hyper-V
 - Microsoft AZURE
 - Administrarea de sisteme Linux
 - Storage area networks
 - Docker
 - Soluții de firewall
 - Programare PHP
 - Programare .NET

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):
 - Cisco Certified Network Professional (CCNP)
 - COBIT® 5 Foundation
 - COBIT® 5 Implementation
 - CompTIA Network+
 - Microsoft 365 Certified: Enterprise Administrator Expert
 - Linux Enterprise Professional Certification
 - ATT&CK Fundamentals
 - CompTIA Security+
 - CompTIA Cybersecurity Analyst (CySA+)
 - EC-Council Certified Incident Handler (E|CIH)
 - EC-Council Certified SOC Analyst (CSA)
 - GIAC Certified Incident Handler (GCIH)
 - Hyper-V Administration
- **Are obligația ca în termen de maximum un (1) an de la data angajării, să obțină cel puțin una (1) din următoarele certificări** (sau echivalent) - costurile aferente fiind suportate de către DNSC:
 - Cisco Certified Network Professional (CCNP)
 - COBIT® 5 Foundation
 - COBIT® 5 Implementation
 - CompTIA Network+
 - Microsoft 365 Certified: Enterprise Administrator Expert

- Linux Enterprise Professional Certification
- ATT&CK Fundamentals
- CompTIA Security+
- CompTIA Cybersecurity Analyst (CySA+)
- EC-Council Certified Incident Handler (E|CIH)
- EC-Council Certified SOC Analyst (CSA)
- GIAC Certified Incident Handler (GCIH)
- Hyper-V Administration
- ITIL 3 Foundation
- ITIL 4 Foundation

3.5 Metodologii cunoscute

- Trebuie să cunoască **la un nivel general** metodologiile sau cadrele tehnice (frameworks) din lista de mai jos (sau echivalent):
 - ITIL - Information Technology Infrastructure Library
 - COBIT® - Control Objectives for Information and related Technology
 - FIRST - Computer Security Incident Response Team (CSIRT) Services Roles and Competencies
 - FIRST - Computer Security Incident Response Team (CSIRT) Services Framework

3.6 Cunoștințe de limba română și de limbi străine

- Cerință obligatorie de limbă română ca limbă maternă sau limbă română de **minimum nivel C1** conform [Common European Framework of Reference for Languages CEFR](#)
- Cunoașterea limbii engleze de **minimum nivel B2** conform [Common European Framework of Reference for Languages CEFR](#). Titularul postului are obligația ca în termen de maximum trei (3) luni de la data angajării să prezinte dovada îndeplinirii cerinței obligatorii de limbă engleză de minimum nivel B2 conform Common European Framework of Reference for Languages CEFR.
- Cunoașterea unei a doua limbi străine europene (franceza, germana, italiana, spaniola, olandeza, maghiara, greaca, etc.) 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

- 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

- Numărul total și numărul mediu de incidente tehnice gestionate într-o anumită perioadă de timp (lunar, trimestrial, anual) pe nivele de prioritate.
- Procentul (%) de incidente tehnice gestionate într-o anumită perioadă de timp (lunar, trimestrial, anual) pe nivele de prioritate, din totalul incidentelor gestionate la nivelul **Direcției Infrastructură Tehnică**.

- **Durata medie de timp necesară pentru a răspunde sau rezolva un incident** (MTTR - Mean Time to Resolution) pentru rezolvarea căruia este responsabil(ă), pe baza datelor și informațiilor aferente tichetelor procesate la nivelul **Direcției Infrastructură Tehnică**.
- Rata cu care incidentele sunt rezolvate în timpul primei apariții.
- Efectuarea anuală a unui număr minimal de șaisprezece (16) ore de cursuri online de pregătire profesională în domenii relevante pentru Direcția Infrastructură Tehnică, 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 Infrastructură Tehnică**, 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** venite din partea constituenților implicați cu privire la incidentele de securitate cibernetică pentru procesarea cărora este responsabil(ă) sau în rezolvarea cărora este implicat(ă) ca parte a activității derulate în **Direcția Infrastructură Tehnică**.

Directoratul Național de Securitate Cibernetică

Angajat

Nume + Prenume

Nume + Prenume

Data _____

Data _____

Nume + Prenume

Data _____

Nume + Prenume

Data _____