DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

FIȘA DE POST
Direcția Generală Operațiuni Tehnice
Direcția Intervenție Rapidă la Incidente

Expert investigații digitale și analiză malware
#700
județul BIHOR

1 Identificarea postului

1.1 Numele si prenumele titularului

- NUME + PRENUME

1.2 Denumirea postului

- **Expert investigații digitale și analiză malware**
- *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

- **Asistent**

1.4 Poziția în COR (Clasificarea Ocupațiilor din Romania)

- **Cod COR: Expert în investigații digitale 252905**
- *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 Operațiuni Tehnice - Direcția Intervenție Rapidă la Incidente
- Sediul/locația DNSC județeană / telemuncă
- **Județul BIHOR**
- **Poziția #700 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 securitate cibernetică** - Direcția Intervenție Rapidă la Incidente
    - **Coordonator superior securitate cibernetică** - Direcția Intervenție Rapidă la Incidente
    - **Manager securitate cibernetică** - Direcția Intervenție Rapidă la Incidente
    - **Manager superior securitate cibernetică** - Direcția Intervenție Rapidă la Incidente
    - **Manager superior securitate cibernetică** - Direcția Generală Operațiuni Tehnice; Conducere - Direcția Generală Operațiuni Tehnice, care coordonează Direcția Intervenție Rapidă la Incidente
    - **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 Cibernetici
        - Direcția Management al Riscurilor Cibernetice
        - Direcția Comunicare, Media și Marketing
        - Serviciul Protecție Reputație și Marcă în Spațiul Cibernetic
    - Direcția Generală Parteneriate Instituționale (toate compartimentele)
    - Direcția Generală 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 Intervenție Rapidă la Incidente** din Direcția Generală Operațiuni Tehnice 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 la nivel național și/sau internațional.
- **Reprezintă DNSC și interesele DNSC** în raport cu părțile interne și externe implicate în activitățile specifice de investigații digitale și/sau analiză malware pe care le efectuează, conform sarcinilor de serviciu primite din partea superiorilor ierarhici.
- **Reprezintă DNSC și interesele DNSC** conform mandatului primit din partea superiorilor ierarhici, în raport cu experți individuali și organizații profesionale sau non-guvernamentale implicate în activități profesionale privind investigații digitale, analiză malware, de conștientizare și educație.

1.7.4 Control

- Nu are.

2 Descrierea postului

2.1 Scopul principal al postului

- Efectuează investigarea incidentelor de securitate cibernetică raportate/semnalate către Directorat. Inițiază și efectuează acțiuni concrete pentru a diminua cât mai mult posibil consecințele și impactul incidentelor de securitate cibernetică confirmate asigurând rezolvarea promptă și eliminarea cauzelor care au dus la acestea.
- În contextul investigării incidentelor de securitate cibernetică raportate/semnalate către Directorat:
    - Efectuează analiza artefactelor și a probelor digitale inclusiv a dispozitivelor electronice, inclusiv a computerelor, a dispozitivelor mobile și a altor suporturi digitale de stocare a datelorprin diferite metode (e.g. Runtime and Dynamic analysis, Reverse Engineering, Comparative Analysis, Media, Surface Analysis).
    - Analizează eșantioanele de malware pentru a identifica comportamentul caracteristic al artefactelor sau al sistemelor compromise, sau modul în care acestea stabilesc conectivitatea cu ținta sau centrele de comandă și control sau evită detectarea.
    - Efectuează analize și corelații în vederea descoperirii de vulnerabilități, sau pentru investigarea incidentelor cibernetice raportate/semnalate către Directorat.
- Îndeplinește rolul de expert al DNSC pe probleme tehnice legate de analiza artefactelor și a probelor digitale în contextul efectuării de investigații digitale și/sau analiză malware.

2.2 Descrierea sarcinilor / atribuțiilor / activităților postului

- Efectuează activitățile specifice de investigații digitale și/sau analiză malware independent sau în echipă cu colegi din **Direcția Intervenție Rapidă la Incidente,** din alte compartimente funcționale ale DNSC sau cu personal extern aparținând partenerilor instituționali ai Directoratului.
- Efectuează investigații digitale și analiză de aplicații specifice și de fișiere malițioase (malware) pe platforme de tip Windows, Unix, Linux, OSx, iOS, Android, HarmonyOS, etc.
- Efectuează investigații digitale și analiză analiza statică şi dinamica/comportamentală a fișierelor malițioase (malware) cu scopul de a înțelege mecanismele lor de funcționare, de a identifica amenințările cibernetice asociate acestora şi de a crea rapoarte și analize tehnice.
- Analizează atât preliminar cât și în detaliu artefactele digitale corespunzând incidentului de securitate cibernetică pe care îl investighează. Reconstituie, pe baza analizei artefactelor digitale (cum ar fi analiza traficului de rețea, analiza log-urilor, analiza codului malițios folosit, etc.) desfășurarea atacului cibernetic în cadrul incidentului de securitate.
- Identifică vulnerabilitățile ce au fost utilizate de atacatori, legate de incidentele de securitate cibernetică pe care le investighează.
- Participă în mod activ la activitățile de restabilire a confidențialității, integrității și disponibilității datelor și/sau infrastructurilor impactate datorită incidentului.
- Colectează și documentează date și informații suplimentare, atât din surse deschise, sau prin cooperare cu alte compartimente funcționale ale DNSC ori cu partenerii instituționali cu care **Direcția Intervenție Rapidă la Incidente** este în contact.
- Utilizează instrumente software și hardware pentru a extrage, păstra, analiza și prezenta dovezi digitale pentru investigații sau teste suplimentare.
- Pregătește și documentează indicatori de compromis (IOC - indicators of compromise IOC) și indicatori de atac (indicators of attack IOA) în formate general utilizate, spre exemplu: STIX, TAXII, YARA, etc.
- Întocmește, la cerere sau din proprie inițiativă, în limbile Română sau Engleză rapoarte privind incidentele de securitate cibernetică, investigațiile digitale și/sau analiza aplicațiilor specifice și fișiere malițioase (malware).
- Întocmește, la cerere sau din proprie inițiativă, statistici și rapoarte de analiză privind incidentele de securitate cibernetică analizate/remediate, investigațiile digitale și/sau analizele malware efectuate.
- Pregătește, la cerere sau din proprie inițiativă, anunțuri sau comunicări în vederea publicării și diseminării de informații relevante privind categoriile de incidente de securitate cibernetică analizate/remediate, investigațiile digitale și/sau analizele malware efectuate.
- Răspunde de confidențialitatea datelor și informațiilor transmise către DNSC sau procesate și analizate ca parte a activităților efectuate la nivelul **Direcției Intervenție Rapidă la Incidente**, 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 Operațiuni Tehnice (DGOT).
- Folosește în activitatea curentă proceduri (inclusiv incident response playbooks), metode, standarde, tehnici și instrumente privind incidentele de securitate cibernetică notificate către DNSC sau procesate și analizate la nivelul **Direcției Intervenție Rapidă la Incidente**.

- Participă și contribuie la pregătirea sesiunilor de pregătire profesională **organizate trimestrial la nivelul Direcției Intervenție Rapidă la Incidente,** pentru a asigura menținerea și îmbunătățirea cunoștințelor profesionale proprii.
- Asigură o comunicare adecvată, prin metode de comunicare scrisă, discuții și feedback la nivelul **Direcției Intervenție Rapidă la Incidente** precum și între această direcție și alte compartimente 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, și facilitează cooperarea și lucrul în echipă la nivelul **Direcției Intervenție Rapidă la Incidente** 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 Intervenție Rapidă la Incidente**, 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 incidente gestionate într-o anumită perioadă de timp (lunar, trimestrial, anual) pe nivele de prioritate și pe sectoare / sub-sectoare și ca distribuție geografică (e.g. pe județ).
    - Procentul (%) de incidente gestionate într-o anumită perioadă de timp (lunar, trimestrial, anual) pe nivele de prioritate, din totalul incidentelor gestionate la nivelul **Direcției Intervenție Rapidă la Incidente**.
    - Nivelul mediu de satisfacție din partea raportorilor de incidente în urma feedback-ului primit (**CSAT - Customer Satisfaction Score**) pentru incidentele de securitate cibernetică pentru a căror investigare este responsabil(ă).
    - Numărul de investigații digitale efectuate într-o anumită perioadă de timp (lunar, trimestrial, anual) și procentul (%) acestora din totalul investigațiilor digitale efectuate la nivelul **Direcției Intervenție Rapidă la Incidente**.
    - Numărul de analize malware efectuate într-o anumită perioadă de timp (lunar, trimestrial, anual) și procentul (%) acestora din totalul analizelor malware efectuate la nivelul **Direcției Intervenție Rapidă la Incidente**.
- Desfășoară activități circumscrise postului, la solicitarea punctuală a conducerii Direcției Generale Operațiuni Tehnice și în alte județe.
- Efectuează coordonarea și îndrumarea activității voluntarilor (elevi, studenți, absolvenți, etc.) ce sunt îi sunt asignați în cadrul programului sau activităților de voluntariat derulate la nivelul **Direcției Intervenție Rapidă la Incidente**.
- 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 Intervenție Rapidă la Incidente**:

- Coordonator superior securitate cibernetică - Direcția Intervenție Rapidă la Incidente
- Coordonator securitate cibernetică - Direcția Intervenție Rapidă la Incidente
- Expert investigații digitale și analiză malware - Direcția Intervenție Rapidă la Incidente
- Asistent investigații digitale și analiză malware - Direcția Intervenție Rapidă la Incidente
- Expert securitate rețele și sisteme informatice - Direcția Intervenție Rapidă la Incidente
- Expert investigații digitale - Direcția Intervenție Rapidă la Incidente

iar preluarea de atribuții se face prin desemnare de către **Managerul superior securitate cibernetică, din Direcția Intervenție Rapidă la Incidente.**

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 unul/una din domeniile/ramurile/specializările:
  - Matematică, matematică-informatică, statistică
  - Informatică (toate specializările)
  - Știința sistemelor și a calculatoarelor (toate specializările)
  - Fizică
  - Automatică, automatică și informatică industrială
  - Științe inginerești
  - Inginerie electrică, electronică, telecomunicații
  - Ingineria sistemelor, calculatoare și tehnologia informației
  - Ingineria și securitatea sistemelor informatice militare
  - Cibernetică, cibernetică și previziune economică, cibernetică economică, cibernetică și statistică economică, statistică și informatică economică, cibernetică și informatică economică;
  - Calculatoare, tehnică de calcul, tehnologia informatică
  - Ingineria sistemelor și a calculatoarelor (toate specializările)
  - Rețele și software de telecomunicații
  - Tehnologii și sisteme de telecomunicații
  - Științe sociale
  - Științe economice

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 Security Incident Response Team (CSIRT)
  - Computer Emergency Response Team (CERT)
  - Computer Incident Response Center (CIRC)
  - Cyber Security Incident Response Center (CSIRC)
  - Security Operations Center (SOC)

- IT / Information Security Helpdesk
- IT Audit, IT Security Audit, Audit, Internal Audit
- Digital Forensics and Investigation (DFIR)
- Echipe de analiză și / sau investigare a incidentelor sau infracțiunilor digitale
- Echipe sau laboratoare de analiză și / sau testare a tehnologiilor digitale

- 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. 22, 23, 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 investigații digitale 252905**.
- 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.
- 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).
- Cunoștințe **la un nivel general** privind arhitectura rețelelor și sistemelor informatice; sisteme de operare; recuperarea datelor și restabilirea funcționalității infrastructurilor cibernetice în urma unor incidente de securitate cibernetică; standarde, strategii și politici de securitate cibernetică; evaluarea nivelului de securitate a rețelelor și sistemelor informatice; implementarea/gestionarea riscurilor în rețelele și sistemele informatice; stabilirea unui plan de asigurare a securității infrastructurii cibernetice.
- **Demonstrarea abilității practice** de a înțelege și a reconstitui, pe baza analizei unor artefacte digitale (cum ar fi analiza traficului de rețea, analiza log-urilor, analiza codului malițios folosit, etc.) desfășurarea unui atac în cadrul unui incident de securitate.
- 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 abilitați (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**:
    - **Managementul conflictelor - Conflict Management (C009) -** are aptitudini privind gestionarea și soluționarea conflictelor, reclamațiilor, confruntărilor sau dezacordurilor

într-o manieră constructivă pentru a minimiza impactul personal negativ; colaborează cu alte persoane pentru a încuraja cooperarea și colaborarea 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**:
  - **Criminalistică digitală - Computer Forensics (C005)** - are aptitudini privind instrumente și tehnici utilizate în recuperarea datelor și conservarea probelor electronice, inclusiv
    - Cunoașterea proceselor de confiscare și păstrare a probelor digitale
    - Cunoașterea implicațiilor investigative ale hardware-ului, sistemelor de operare și tehnologiilor de rețea.
    - Cunoașterea tipurilor și modalităților de colectare a datelor persistente.
    - Cunoașterea fișierelor de sistem (de exemplu, fișiere jurnal, registri, fișiere de configurare) pentru cele mai răspândite sisteme de operare.
    - Cunoașterea tipurilor de date și probe digitale și a modului de recunoaștere a acestora.
    - Cunoașterea instrumentelor și tehnicilor de colectare a datelor.
    - Cunoașterea tacticilor, tehnicilor și procedurilor anti-criminalistică.
    - Cunoștințe de configurare și folosire stații de lucru și a aplicațiilor software de analiză, investigații și criminalistică digitala (de exemplu, VMWare, Wireshark, EnCase, Sleuthkit, FTK, etc.).
    - Cunoașterea conceptelor și practicilor de identificare, extragere, prelucrare și analiză a datelor.
    - Competența de a păstra integritatea probelor în conformitate cu procedurile standard de operare sau cu standardele.
    - Abilitate în colectarea, prelucrarea, ambalarea, transportul și stocarea datelor probelor digitale pentru a evita modificarea, pierderea, deteriorarea fizică sau distrugerea acestora.
    - Abilități în efectuarea analizelor pentru mai multe medii ale sistemului de operare (de exemplu, sisteme de operare a dispozitivelor mobile).
    - Abilitatea de a analiza cod software anormal (pentru a detecta dacă este malițios sau benign/legitim).
    - Abilitate în analiza datelor volatile.
    - Abilitatea de a cripta și decripta colecții de date digitale.
    - Abilitatea de a efectua analize în și pentru medii Windows și Unix / Linux.
  - **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.
  - **Analiza datelor - Data Analysis (C012)** - are aptitudini privind colectarea, sintetizarea și/sau analizarea datelor și informațiilor calitative și cantitative dintr-o varietate de surse pentru a ajunge la o decizie, a face o recomandare și/sau a compila rapoarte, informări, rezumate executive și altele.

- **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.
- **Rezolvarea de probleme - Problem Solving (C040)** - are aptitudini privind determinarea exactității și relevanței informațiilor și utilizarea unei judecăți profesionale solide pentru a evalua alternative; luarea unor decizii bine informate, obiective, care să ia în considerare faptele, obiectivele, constrângerile și riscurile, percepând în același timp impactul și implicațiile deciziilor proprii.
- **Analiza amenințărilor - Threat Analysis (C055)** - are aptitudini privind procesul în care cunoașterea vulnerabilităților interne și externe relevante pentru o anumită organizație este corelată cu atacurile cibernetice din lumea reală.
- **Evaluarea vulnerabilităților - Vulnerabilities Assessment (C057)** - are aptitudini privind principiile, metodele și instrumentele de evaluare a vulnerabilităților (e.g. în infrastructuri, rețele și sisteme informatice) precum și elaborarea sau recomandarea unor contramăsuri adecvate, inclusiv:
  - Cunoștințe generale privind amenințările și vulnerabilitățile cibernetice.
  - Cunoașterea metodelor cele mai uzuale de hacking.
  - Cunoașterea metodelor de analiză la nivel de pachet de date utilizând instrumente adecvate (de exemplu, Wireshark, tcpdump).
  - Cunoașterea riscurilor de securitate a aplicațiilor (de exemplu, lista Open Web Application Security Project OWASP Top 10).

- Cunoștințe, competențe și abilități **operaționale**:
  - **Continuitatea activitatii - Business Continuity (C002)** - are aptitudini privind planificarea și pregătirea unei organizatii pentru a se asigura că depășește incidentele grave sau dezastrele și își reia operațiunile normale într-o perioadă rezonabil de scurtă
  - **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.
  - **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.
  - **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.

- Permis auto categoria B.

3.3 Instrumente și tehnologii de lucru

- Are experiență anterioară și poate să utilizeze **la un nivel avansat** aplicații de tip Office din lista de mai jos sau echivalent:
  - Microsoft Word, Excel, Powerpoint, Outlook, Teams, etc.

- Google Docs, Sheets, Slides, Calendar, Sites etc.
- Libre Office Writer, Calc, Impress, Draw, Math, Base etc.

- Are experiență anterioară practică cu, sau poate să utilizeze **la un nivel avansat** cel puțin doua (2) din platformele următoare de tip Malware Analysis (sau echivalent):
  - Autoruns
  - CrowdStrike Falcon Insight
  - Cuckoo Sandbox
  - Fiddler
  - FTK Imager
  - Ghidra
  - Google Takeout Convertor
  - IDA Pro
  - Limon
  - PeStudio
  - ProDiscover Forensic
  - Process Hacker
  - Process Monitor (ProcMon)
  - ProcDot
  - Radare2/Cutter
  - Redline
  - Reverse.it
  - SIFT Workstation
  - SNORT
  - Sleuth Kit (+Autopsy)
  - VirusTotal
  - Volatility
  - Wireshark
  - x64dbg
- Are experiență anterioară practică cu, sau poate să utilizeze **la un nivel general** cel puțin una din platformele următoare de tip Security Information and Event Management (SIEM) sau Incident Response (sau echivalent):
  - Request Tracker for Incident Response (RTIR)
  - Malware Information Sharing Platform (MISP)
  - ArcSight Enterprise Security Manager (ESM)
  - CrowdStrike Falcon Insight
  - Cynet 360
  - LogRhythm SIEM
  - IBM QRadar
  - IBM X-Force Incident Response and Intelligence Services (IRIS)
  - IntelMQ
  - SolarWinds Security Event Manager
  - Splunk Security Orchestration and Automation (Splunk SOAR) / Splunk Phantom
  - TheHive, etc.

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):
  - CISM (Certified Information Security Manager)
  - CISA (Certified Information Systems Auditor)
  - CISSP (Certified Information Systems Security Professional)
  - CRISC (Certified in Risk and Information Systems Control)
  - IACIS Certified Forensic Computer Examiner (CFCE)
  - CompTIA Security+
  - CompTIA Cybersecurity Analyst (CySA+)
  - EC-Council Certified Incident Handler (E|CIH)
  - EC-Council Certified SOC Analyst (CSA)

- EC-Council Computer Hacking Forensic Investigator (CHFI)
- EnCase Certified Examiner (EnCe)
- GIAC Advanced Smartphone Forensics (GASF)
- GIAC Certified Forensic Analyst (GCFA)
- GIAC Certified Forensic Examiner (GCFE)
- GIAC Certified Incident Handler (GCIH)
- GIAC Cloud Forensics Responder (GCFR)
- GIAC Cyber Threat Intelligence (GCTI)
- GIAC Network Forensic Analyst (GNFA)
- GIAC Reverse Engineering Malware (GREM)
- GIAC Response and Industrial Defense (GRID)
- GIAC Security Operations Certified (GSOC)
- ISO/IEC 27001 Lead Auditor
- ISO/IEC 27001 Lead Implementer
- MITRE ATT&CK Fundamentals
- MITRE ATT&CK Defender
- OSWP (Offensive Security Wireless Professional)

- **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:
  - CISM (Certified Information Security Manager)
  - CISA (Certified Information Systems Auditor)
  - CISSP (Certified Information Systems Security Professional)
  - CRISC (Certified in Risk and Information Systems Control)
  - IACIS Certified Forensic Computer Examiner (CFCE)
  - CompTIA Security+
  - CompTIA Cybersecurity Analyst (CySA+)
  - EC-Council Certified Incident Handler (E|CIH)
  - EC-Council Certified SOC Analyst (CSA)
  - EC-Council Computer Hacking Forensic Investigator (CHFI)
  - EnCase Certified Examiner (EnCe)
  - GIAC Advanced Smartphone Forensics (GASF)
  - GIAC Certified Forensic Analyst (GCFA)
  - GIAC Certified Forensic Examiner (GCFE)
  - GIAC Certified Incident Handler (GCIH)
  - GIAC Cloud Forensics Responder (GCFR)
  - GIAC Cyber Threat Intelligence (GCTI)
  - GIAC Network Forensic Analyst (GNFA)
  - GIAC Reverse Engineering Malware (GREM)
  - GIAC Response and Industrial Defense (GRID)

- GIAC Security Operations Certified (GSOC)
- ISO/IEC 27001 Lead Auditor
- ISO/IEC 27001 Lead Implementer
- MITRE ATT&CK Fundamentals
- MITRE ATT&CK Defender
- OSWP (Offensive Security Wireless Professional)

3.5 Metodologii cunoscute

- Trebuie să cunoască **la un nivel general** metodologiile sau cadrele tehnice (frameworks) din lista de mai jos sau echivalent:
  - FIRST - Computer Security Incident Response Team (CSIRT) Services Roles and Competencies
  - FIRST - Computer Security Incident Response Team (CSIRT) Services Framework
  - MITRE ATT&CK
  - NIST - Computer Security Incident Handling Guide, Special Publication 800-61
  - NIST - Guide to Malware Incident Prevention and Handling, Special Publication 800-83
  - NIST - Guide to Integrating Forensic Techniques into Incident Response, Special Publication 800-86
  - NISTIR 8428 - Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT)
  - OWASP Security Knowledge 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 munca în aceleași condiții în care pot fi angajați și cetățenii români.*

3.8 Autorizații speciale pentru exercitarea atribuțiilor

- Nu este cazul.

4 Indicatori de performanță

- **Numărul total și numărul mediu de incidente gestionate într-o anumită perioadă de timp** (lunar, trimestrial, anual) pe nivele de prioritate și pe sectoare / sub-sectoare și ca distribuție geografică.
- Procentul (%) de incidente gestionate într-o anumită perioadă de timp (lunar, trimestrial, anual) pe nivele de prioritate, din totalul incidentelor gestionate la nivelul **Direcției Intervenție Rapidă la Incidente**.

- Nivelul mediu de satisfacție din partea raportorilor de incidente în urma feedback-ului primit (**CSAT - Customer Satisfaction Score**) pentru incidentele de securitate cibernetică pentru a căror investigare este responsabil(ă).
- Numărul de investigații digitale efectuate într-o anumită perioadă de timp (lunar, trimestrial, anual) și procentul (%) acestora din totalul investigațiilor digitale efectuate la nivelul **Direcției Intervenție Rapidă la Incidente**.
- Numărul de analize malware efectuate într-o anumită perioadă de timp (lunar, trimestrial, anual) și procentul (%) acestora din totalul analizelor malware efectuate la nivelul **Direcției Intervenție Rapidă la Incidente**.
- Efectuarea anuală a unui **număr minimal de șaisprezece (16) ore de cursuri online de pregătire profesională în domenii relevante pentru Direcția Intervenție Rapidă la Incidente**, 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 Intervenție Rapidă la Incidente**, 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 investigarea și privind analiza cărora este responsabil(ă) sau în rezolvarea cărora este implicat(ă) ca parte a activității derulate în **Direcția Intervenție Rapidă la Incidente**.

Directoratul Național de Securitate Cibernetică	Angajat
Nume + Prenume	**Nume + Prenume**
Data _____	Data _____
Nume + Prenume	
Data _____	
Nume + Prenume	
Data _____	