

Directorul responsabil cu securitatea informațiilor

FF09 Infrastructură, operațiuni și securitate IT · ISCO-08 1330 · CBS 0533 Manageri în domeniul TIC · vechime lead · Cunoscut și ca: CISO, Șef al departamentului de securitate a informațiilor

Deține responsabilitatea finală pentru securitatea informațiilor, stabilește politica și apetitul la risc și răspunde în fața consiliului de administrație și a autorităților de supraveghere pentru starea de securitate.

Directorul de securitate informatică coordonează funcția de securitate a unei organizații, alocă resurse și decide ce riscuri sunt acceptabile. Spre deosebire de ofițerul de securitate, acest rol dispune de mandat și buget, iar spre deosebire de directorul IT, responsabilitatea sa principală este controlul riscurilor, mai degrabă decât disponibilitatea sistemului. În procesul de selecție se acordă o importanță deosebită cunoștințelor tehnice și celor privind standardele, în timp ce, în practică, rolul eșuează din cauza lipsei de prezență executivă: un CISO trebuie să fie capabil să impună o investiție și să comunice cu directorii și supervizorii în timpul unei crize, fără a ascunde realitatea.

Cifre cheie pentru acest profil

26 competențe · 4 competențe de evaluat · 3 competențe esențiale · centrul de greutate: Tehnologia digitală, datele și inteligența artificială 47%, Conducere și organizare 20%, Abilități cognitive și rezolvarea problemelor 10%

1 Competențe de măsurat

Acestea sunt constructele de comportament și de aptitudine din acest profil. Fiecare arată ce chestionar hrmforce îl măsoară.

Competențe de măsurat	Nivel-țintă	Instrument hrnforce	Metodă de măsurare	Ancoră comportamentală la nivelul-țintă
Precizie și atenție la detalii Competență (cadrul 50): Precizie	 N5	Big Fifty, 360 Feedback	Chestionar de personalitate	Stabilește standardele privind exhaustivitatea și corectitudinea, verifică eșantioanele și atrage atenția echipelor asupra neglijențelor structurale.
integritate și fiabilitate Competență (cadrul 50): Integritate	 N5	Big Fifty (Scala de integritate), 360 Feedback, Interviu structurat	Chestionar de personalitate	Stabilește standardele de integritate ale organizației, le aplică și în relația cu părțile influente și explică public deciziile rezultate.
Disciplina și respectarea angajamentelor Competență (cadrul 50): Domeniu	 N5	Big Fifty, 15PF, 360 Feedback	Chestionar de personalitate	Stabilește standardul pentru respectarea consecventă a acordurilor de lucru și se adresează oricărei persoane, de la orice nivel, care nu respectă acest standard.
Toleranța la stres Competență (cadrul 50): Rezistența la stres	 N5	Big Fifty, 15PF, Mental Resilience (4C)	Chestionar de personalitate	Asigură funcționarea organizației în situații de criză, ia decizii în condiții de incertitudine ridicată și stabilește standardul pentru acțiuni calme sub presiune.

2 Profil complet al competențelor

Fiecare competență din acest profil, ordonată în funcție de pondere. Indicatorul comportamental de sub fiecare competență corespunde nivelului țintă.

T	Competență	Nivel-țintă	Pondere	Eliminatoriu	Metodă de măsurare	Instrument hrmforce
V	Analiza problemelor Identifică câteva cauze fundamentale ale problemelor organizaționale persistente și stabilește metoda de analiză pe care o vor utiliza celelalte echipe.	■■■■■ N5	5	da	Centru de evaluare	Competency Check, Ability Scan
V	Gândire strategică Elaborează scenarii pentru întreaga organizație, evaluează în mod explicit incertitudinile și stabilește agenda strategică împreună cu consiliul de administrație.	■■■■■ N5	5	nu	Centru de evaluare	Ability Scan, Competency Check
K	Guvernanță și conformitate Elaborează cadrul de guvernanță al organizației, definește mandatele și mecanismele de supraveghere și răspunde în fața autorităților de supraveghere externe cu privire la respectarea normelor.	■■■■■ N5	5	nu	Test de cunoștințe	Test de cunoștințe (specific clientului)

T	Competență	Nivel-țintă	Pondere	Eliminatoriu	Metodă de măsurare	Instrument hrmforce
V	Gestionarea riscurilor Elaborează cadrul de risc al organizației, stabilește apetitul la risc împreună cu echipa executivă și prezintă rapoarte în acest sens organismului de supraveghere.	■■■■■ N5	5	nu	Test de cunoștințe	Test de cunoștințe (specific clientului), Competency Check
V	Gestionarea accesului și a identității Stabilește politica de acces a organizației și asigură controlul permisiunilor în cadrul auditurilor.	■■■■■ N5	5	da	Testul cu probe de lucru	Test de cunoștințe (specific clientului), Testul cu probe de lucru
V	Analiza amenințărilor și a riscurilor Efectuează în mod independent o analiză a riscurilor asupra unei aplicații, ierarhizează riscurile și oferă recomandări privind măsurile de intervenție, precizând costurile și efectele acestora.	■■■■■ N4	5	da	Testul cu probe de lucru	Test de cunoștințe (specific clientului), Testul cu probe de lucru
G	Precizie și atenție la detalii Stabilește standardele privind exhaustivitatea și corectitudinea, verifică eșantioanele și atrage atenția echipelor asupra neglijențelor structurale.	■■■■■ N5	4	nu	Chestionar de personalitate	Big Fifty, 360 Feedback
G	integritate și fiabilitate Stabilește standardele de integritate ale organizației, le aplică și în relația cu părțile influente și explică public deciziile rezultate.	■■■■■ N5	4	nu	Chestionar de personalitate	Big Fifty (Scala de integritate), 360 Feedback, Interviu structurat

T	Competență	Nivel-țintă	Pondere	Eliminatoriu	Metodă de măsurare	Instrument hrmforce
V	Răspunderea față de superiori și părțile interesate Prezintă rezultatele organizaționale și incidentele către consiliul de supraveghere, mass-media sau mediul politic și face legătura între acestea și ajustările vizibile ale politicilor.	■■■■■ N5	4	nu	Centru de evaluare	Competency Check, 360 Feedback
G	Disciplina și respectarea angajamentelor Stabilește standardul pentru respectarea consecventă a acordurilor de lucru și se adresează oricărei persoane, de la orice nivel, care nu respectă acest standard.	■■■■■ N5	4	nu	Chestionar de personalitate	Big Fifty, 15PF, 360 Feedback
G	Toleranța la stres Asigură funcționarea organizației în situații de criză, ia decizii în condiții de incertitudine ridicată și stabilește standardul pentru acțiuni calme sub presiune.	■■■■■ N5	4	nu	Chestionar de personalitate	Big Fifty, 15PF, Mental Resilience (4C)
V	Securitatea informațiilor în cadrul procesului de lucru Stabilește politica de securitate a informațiilor și monitorizează la nivelul întregii organizații dacă procesele respectă cerințele stabilite.	■■■■■ N5	4	nu	Test de cunoștințe	Test de cunoștințe (specific clientului)

T	Competență	Nivel-țintă	Pondere	Eliminatoriu	Metodă de măsurare	Instrument hrmforce
V	Utilizarea platformelor cloud Stabilește strategia organizației privind cloudul și decide ce sarcini de lucru sunt alocate și unde.	■■■■■ N5	4	nu	Test de cunoștințe	Test de cunoștințe (specific clientului)
K	Conștientizarea privind securitatea informațiilor Elaborează programul de sensibilizare al organizației, măsoară efectul acestuia și ajustează abordarea pe baza rezultatelor obținute.	■■■■■ N5	4	nu	Test de cunoștințe	Test de cunoștințe (specific clientului)
V	Elaborarea politicilor Stabilește orientarea strategică pentru un anumit domeniu, asigură legătura între părțile implicate în lanț și asigură evaluarea sistematică a rezultatelor.	■■■■■ N5	4	nu	Portofoliu sau dovezi	Portofoliu, Competency Check
V	Răspunsul la incidentele de securitate Limitează în mod independent daunele în timpul unui incident, păstrează probele și oferă o cronologie trasabilă a evenimentelor.	■■■■■ N4	4	nu	Simulare	Test de cunoștințe (specific clientului), Testul cu probe de lucru
V	Învățarea din greșeli și incidente Analizează propriile erori și cele ale echipei, discută deschis cauza acestora în cadrul ședinței de lucru și ajustează acordurile.	■■■■■ N4	3	nu	Situational Judgement Test	360 Feedback, Competency Check

T	Competență	Nivel-țintă	Pondere	Eliminatoriu	Metodă de măsurare	Instrument hrmforce
V	Actualitatea profesională și literatura de specialitate Urmărește sursele și liniile directe din punct de vedere structural, evaluează calitatea acestora și își adaptează propria metodă de lucru la noile cunoștințe.	■■■■■ N4	3	nu	Portofoliu sau dovezi	Portofoliu, Test de cunoștințe (specific clientului)
V	Redactarea documentației tehnice Redactează documentația completă pentru un sistem sau un proces, o testează cu un cititor care nu este familiarizat cu aceasta și gestionează versiunile.	■■■■■ N4	3	nu	Testul cu probe de lucru	Testul cu probe de lucru, Portofoliu
V	Automatizarea proceselor Describe un proces pas cu pas, automatizează etapele repetabile și integrează verificări privind erorile și excepțiile.	■■■■■ N4	3	nu	Testul cu probe de lucru	Testul cu probe de lucru, Portofoliu
V	Managementul funcțional și al aplicațiilor Gestionează în mod independent o aplicație, stabilește prioritățile cererilor de modificare împreună cu utilizatorii și testează noile versiuni înainte ca acestea să fie lansate.	■■■■■ N4	3	nu	Testul cu probe de lucru	Test de cunoștințe (specific clientului), Testul cu probe de lucru

T	Competență	Nivel-țintă	Pondere	Eliminatoriu	Metodă de măsurare	Instrument hrmforce
V	Gestionarea incidentelor și rezolvarea problemelor Stabilește o linie de investigare pentru o defecțiune necunoscută, restabilește serviciul și înregistrează cauza și soluția pentru a le putea reutiliza.	 N3	3	nu	Testul cu probe de lucru	Testul cu probe de lucru, Test de cunoștințe (specific clientului)
V	Clasificarea și păstrarea datelor Stabilește clasificarea și perioada de păstrare a unui flux de informații și verifică dacă curățarea se efectuează conform planului.	 N4	2	nu	Test de cunoștințe	Test de cunoștințe (specific clientului), Testul cu probe de lucru
K	Cunoștințe de bază privind rețelele Deducă, pe baza simptomelor, în ce strat de rețea se află o problemă și susține această deducție cu propriile măsurători.	 N3	2	nu	Test de cunoștințe	Test de cunoștințe (specific clientului)
V	Furnizori IT și gestionarea contractelor Organizează întâlniri cu furnizorii privind performanța și costurile, consemnează acordurile și intervine atunci când acestea nu sunt respectate.	 N3	1	nu	Interviu structurat	Interviu structurat, Portofoliu

T	Competență	Nivel-țintă	Pondere	Eliminatoriu	Metodă de măsurare	Instrument hrmforce
V	Administrarea și monitorizarea sistemelor Efectuează sarcini de întreținere programate și actualizări conform manualului de operațiuni și raportează abaterile observate în semnalele de monitorizare.		1	nu	Testul cu probe de lucru	Test de cunoștințe (specific clientului), Testul cu probe de lucru

3 Niveluri în funcție de vechime

Același profil cu ajustarea vechimii în cadrul familiei de posturi aplicată. Nivelurile țintă sunt limitate la 1-5.

Competență	lead
Analiza problemelor	N5
Gândire strategică	N5
Guvernanță și conformitate	N5
Gestionarea riscurilor	N5
Gestionarea accesului și a identității	N5
Analiza amenințărilor și a riscurilor	N4
Precizie și atenție la detalii	N5
integritate și fiabilitate	N5
Răspunderea față de superiori și părțile interesate	N5
Disciplina și respectarea angajamentelor	N5
Toleranța la stres	N5
Securitatea informațiilor în cadrul procesului de lucru	N5
Utilizarea platformelor cloud	N5
Conștientizarea privind securitatea informațiilor	N5
Elaborarea politicilor	N5
Răspunsul la incidentele de securitate	N4
Învățarea din greșeli și incidente	N4
Actualitatea profesională și literatura de specialitate	N4
Redactarea documentației tehnice	N4
Automatizarea proceselor	N4
Managementul funcțional și al aplicațiilor	N4
Gestionarea incidentelor și rezolvarea problemelor	N3
Clasificarea și păstrarea datelor	N4

Competență	lead
Cunoștințe de bază privind rețelele	N3
Furnizori IT și gestionarea contractelor	N3
Administrarea și monitorizarea sistemelor	N2

4 Scala de competență

Nivel	Etichetă	Autonomie	Complexitate	Domeniul de aplicare	Nivelul de cunoștințe
N1	Ghidat	lucrează sub supraveghere și respectă instrucțiunile	rutină, câte o variabilă pe rând	sarcină proprie	înțelegere de bază a terminologiei
N2	Aplicare	lucrează în mod independent în cadrul unor limite stabilite	situații familiare, cu variații limitate	propria funcție	cunoștințe practice, aplică o abordare standard
N3	Competență avansată	își stabilește propria abordare și solicită în mod proactiv opinii	mai multe variabile, o anumită ambiguitate	propria echipă sau propriul proces	cunoștințe aprofundate, evaluează alternativele
N4	Nivel avansat	coordonează activitatea altora și decide asupra abordării	complex, cu interese contradictorii	mai multe echipe sau un departament	cunoștințe aprofundate, oferă sfaturi altora
N5	Conducere	stabilește standardul și politica	strategic, în condiții de incertitudine ridicată	organizație, lanț valoric sau profesie	autoritate, contribuie la dezvoltarea profesiei

5 Repere comportamentale pentru fiecare competență

Punctele de referință se află la N1, N3 și N5. N2 și N4 nu sunt ancorate în mod deliberat: evaluatorii interpolatează între ele, urmând convenția O*NET.

Competență	N1	N3	N5
Analiza problemelor Descompune o problemă în părți, separă cauzele de efecte și precizează ce informații sunt necesare pentru a avansa.	Precizează exact ce anume nu funcționează corect și ce date lipsesc, și aduce aceste informații la cunoștința superiorului.	Analizează o plângere recurentă în funcție de cauzele posibile, le verifică pe baza datelor proprii și identifică cauza cea mai probabilă.	Identifică câteva cauze fundamentale ale problemelor organizaționale persistente și stabilește metoda de analiză pe care o vor utiliza celelalte echipe.

Competență	N1	N3	N5
Gândire strategică Analizarea evoluțiilor din mediul de afaceri, de pe piață și din domeniul tehnologic și deducerea din acestea a opțiunilor și alternativelor strategice pe termen lung pentru o organizație sau o unitate.	Colectează date despre piață și concurenți la cerere și sintetizează principalele evoluții pentru manager.	Prezintă cifre, semnale din partea clienților și tendințe una lângă alta și identifică două sau trei opțiuni strategice, precum și consecințele acestora.	Elaborează scenarii pentru întreaga organizație, evaluează în mod explicit incertitudinile și stabilește agenda strategică împreună cu consiliul de administrație.
Guvernanță și conformitate Cunoașterea legilor, a codurilor de conduită și a regulilor interne aplicabile propriului domeniu, precum și a modului în care sunt organizate supravegherea, mandatul și responsabilitatea în cadrul organizației.	Identifică principalele reguli care se aplică propriului post și consultă procedura aplicabilă atunci când are îndoieli.	Verifică dacă metodele de lucru respectă legislația și regulile interne și semnalează abaterile, împreună cu justificările corespunzătoare, către responsabilul de serviciu.	Elaborează cadrul de guvernanță al organizației, definește mandatele și mecanismele de supraveghere și răspunde în fața autorităților de supraveghere externe cu privire la respectarea normelor.
Gestionarea riscurilor Identificarea riscurilor la locul de muncă, în cadrul proiectelor sau al politicilor, evaluarea probabilității și a impactului acestora, alegerea măsurilor de control și testarea periodică a eficacității acestor măsuri.	Raportează situațiile nesigure sau riscante din propria activitate prin canalul de raportare convenit.	Elaborează o listă de riscuri cu probabilitatea, impactul și măsurile corespunzătoare fiecărui risc și o revizuieste periodic împreună cu persoanele implicate.	Elaborează cadrul de risc al organizației, stabilește apetitul la risc împreună cu echipa executivă și prezintă rapoarte în acest sens organismului de supraveghere.
Gestionarea accesului și a identității Acordă permisiuni în funcție de rol și de necesitate, verifică periodic cine are acces la ce și retrace drepturile în cazul schimbărilor sau al plecării angajaților.	Procesează cererile de acces în conformitate cu schema de roluri stabilită și înregistrează fiecare modificare.	Proiectează rolurile și permisiunile pentru o aplicație, efectuează revizuirea periodică și corectează accesul excesiv.	Stabilește politica de acces a organizației și asigură controlul permisiunilor în cadrul auditurilor.

Competență	N1	N3	N5
Analiza amenințărilor și a riscurilor Identifică amenințările, punctele slabe și consecințele pentru un sistem sau un proces, evaluează probabilitatea în raport cu impactul și propune măsuri adecvate.	Realizează un inventar al riscurilor folosind o listă dată de amenințări și transmite rezultatul specialistului.	Efectuează în mod independent o analiză a riscurilor asupra unei aplicații, ierarhizează riscurile și oferă recomandări privind măsurile de intervenție, precizând costurile și efectele acestora.	Stabilește apetitul la risc al organizației și metoda de analiză și prezintă consiliului de administrație imaginea de ansamblu a riscurilor de securitate.
Precizie și atenție la detalii Lucrează cu atenție, își verifică propria muncă pentru a depista eventualele erori și respectă angajamentele privind exhaustivitatea și corectitudinea datelor.	Verifică propria muncă cu ajutorul unei liste de verificare și corectează erorile găsite înainte ca lucrarea să fie predată.	Include momente de verificare în propriul proces, ține evidența erorilor și previne repetarea acestora prin ajustarea metodei.	Stabilește standardele privind exhaustivitatea și corectitudinea, verifică eșantioanele și atrage atenția echipelor asupra neglijențelor structurale.
Integritate și fiabilitate Acționarea în conformitate cu standardele și acordurile aplicabile, chiar și fără supraveghere, precum și transparența cu privire la propriile interese, greșeli și cazuri îndoielnice.	Respectă acordurile și regulile de conduită stabilite și raportează propriile greșeli managerului.	Raportează din proprie inițiativă un posibil conflict de interese și solicită o analiză înainte de luarea unei decizii.	Stabilește standardele de integritate ale organizației, le aplică și în relația cu părțile influente și explică public deciziile rezultate.
Răspunderea față de superiori și părțile interesate Prezentarea rezultatelor, a deciziilor și a incidentelor în fața unui consiliu de supraveghere, a unui comitet de întreprindere, a clienților sau a unei autorități de inspecție, cu prezentarea faptelor, a contextului și a consecințelor vizibile asupra politicii.	Furnizează date concrete pentru un raport de responsabilitate și verifică acuratețea și exhaustivitatea acestora.	Prezintă rezultatele echipei către sponsor și comitetul de întreprindere, indicând totodată ce nu a funcționat și care sunt pașii următori.	Prezintă rezultatele organizaționale și incidentele către consiliul de supraveghere, mass-media sau mediul politic și face legătura între acestea și ajustările vizibile ale politicilor.

Competență	N1	N3	N5
Disciplina și respectarea angajamentelor Respectă acordurile, procedurile și angajamentele chiar și fără supraveghere și raportează în timp util atunci când un angajament se dovedește a fi imposibil de îndeplinit.	Sosește la ora stabilită cu munca convenită și raportează orice întârziere superiorului.	Își asumă doar ceea ce este fezabil, își monitorizează propriile angajamente și informează persoanele implicate imediat ce un termen limită este pus sub presiune.	Stabilește standardul pentru respectarea consecventă a acordurilor de lucru și se adresează oricărei persoane, de la orice nivel, care nu respectă acest standard.
Toleranța la stres Continuă să furnizeze rezultate de aceeași calitate chiar și sub presiunea timpului, în fața opoziției sau a unor situații neprevăzute și menține un ton profesional în relațiile cu ceilalți.	Continuă să lucreze la sarcina curentă pe măsură ce presiunea crește și îl întreabă pe superior care dintre sarcini poate aștepta.	Lucrează în mod structurat chiar și în perioadele de vârf, menține claritate în acordurile cu clienții și semnalează din timp care rezultate sunt expuse riscului.	Asigură funcționarea organizației în situații de criză, ia decizii în condiții de incertitudine ridicată și stabilește standardul pentru acțiuni calme sub presiune.
Securitatea informațiilor în cadrul procesului de lucru Aplică măsuri de securitate în activitatea zilnică, cum ar fi partajarea, clasificarea și stocarea în condiții de siguranță a informațiilor, și semnalează practicile de lucru riscante.	Respectă regulile de securitate privind partajarea și stocarea informațiilor și raportează imediat orice incident suspect.	Evaluează riscurile de securitate la stabilirea unor noi acorduri de lucru, adaptează măsurile și abordează colegii cu privire la comportamentele nesigure.	Stabilește politica de securitate a informațiilor și monitorizează la nivelul întregii organizații dacă procesele respectă cerințele stabilite.
Utilizarea platformelor cloud Configurează și gestionează serviciile într-un mediu cloud, stabilește permisiunile și costurile și alege dintre tipurile de servicii disponibile în funcție de cerințe.	Utilizează serviciile cloud existente conform instrucțiunilor și raportează administratorului comportamentele neobișnuite sau costurile neașteptate.	Configurează în mod independent serviciile cloud pentru o aplicație, gestionează permisiunile și copiile de rezervă și monitorizează costurile și utilizarea.	Stabilește strategia organizației privind cloudul și decide ce sarcini de lucru sunt alocate și unde.

Competență	N1	N3	N5
Conștientizarea privind securitatea informațiilor Cunoaște cele mai frecvente amenințări, precum phishingul, ransomware-ul și înșelăciunea, le recunoaște semnele și știe ce acțiuni se așteaptă să întreprindă în astfel de situații.	Recunoaște un mesaj evident de phishing, nu dă clic pe acesta și raportează mesajul prin canalul desemnat.	Le explică colegilor modul în care funcționează amenințările, evaluează în mod independent cazurile îndoielnice și își adaptează propriul comportament la noile amenințări.	Elaborează programul de sensibilizare al organizației, măsoară efectul acestuia și ajustează abordarea pe baza rezultatelor obținute.
Elaborarea politicilor Elaborează politici prin analiza problemelor, explorarea opțiunilor, consultarea părților interesate și concretizarea acestora în obiective, instrumente și evaluare.	Colectează date și documente pentru analiza unei politici sub îndrumare și sintetizează pe scurt concluziile.	Elaborează în mod independent o propunere de politică, cu opțiuni și efecte preconizate, și organizează consultarea părților implicate.	Stabilește orientarea strategică pentru un anumit domeniu, asigură legătura între părțile implicate în lanț și asigură evaluarea sistematică a rezultatelor.
Răspunsul la incidentele de securitate Intervine în cazul unui incident de securitate, urmând procedurile din manualul de intervenții, prin izolarea acestuia, păstrarea probelor, restabilirea funcționalității și informarea la timp a părților implicate.	Raportează imediat un incident suspect, nu atinge nimic și urmează instrucțiunile coordonatorului.	Limitează în mod independent daunele în timpul unui incident, păstrează probele și oferă o cronologie trasabilă a evenimentelor.	Conduce echipa de intervenție la nivel de organizație, ia decizii privind comunicarea externă și îmbunătățește manualul de proceduri după fiecare exercițiu.
Învățarea din greșeli și incidente În urma unei erori sau a unui incident, investighează ce s-a întâmplat, identifică cauza fără a atribui vina și modifică metoda de lucru în acel aspect.	Raportează imediat o eroare proprie superiorului și repetă sarcina urmând instrucțiunile corectate.	Analizează propriile erori și cele ale echipei, discută deschis cauza acestora în cadrul ședinței de lucru și ajustează acordurile.	Se asigură că incidentele sunt raportate în condiții de siguranță la nivelul întregii organizații, că cauzele sunt analizate în mod structurat și că lecțiile învățate sunt integrate în politici și standarde.

Competență	N1	N3	N5
Actualitatea profesională și literatura de specialitate Urmărește evoluțiile din propria profesie prin intermediul literaturii de specialitate, al ghidurilor și al rețelelor și integrează noile cunoștințe relevante în propria practică.	Citește informațiile profesionale primite și identifică care parte este relevantă pentru propria activitate.	Urmărește sursele și liniile directe din punct de vedere structural, evaluează calitatea acestora și își adaptează propria metodă de lucru la noile cunoștințe.	Evaluează situația actuală din domeniu, analizează cercetările contradictorii și stabilește liniile directe pe care organizația le va urma de acum înainte.
Redactarea documentației tehnice Redactează manuale, documentație de sprijin și înregistrări ale deciziilor pe care un cititor fără cunoștințe prealabile le poate urma pas cu pas și care rămân actuale.	Completează un șablon de documentație cu etapele unei sarcini și solicită unui coleg să verifice textul.	Redactează documentația completă pentru un sistem sau un proces, o testează cu un cititor care nu este familiarizat cu aceasta și gestionează versiunile.	Stabilește standardul de documentare al organizației și se asigură că documentația face parte din fiecare livrare.
Automatizarea proceselor Analizează un proces de lucru recurent, creează sau comandă automatizarea etapelor acestuia și verifică dacă rezultatul rămâne fiabil.	Execută un proces de automatizare existent și generează rapoarte atunci când rezultatul diferă de cel așteptat.	Describe un proces pas cu pas, automatizează etapele repetabile și integrează verificări privind erorile și excepțiile.	Stabilește agenda de automatizare a organizației și decide care procese sunt automatizate și care nu.
Managementul funcțional și al aplicațiilor Asigură funcționarea și adaptarea unei aplicații la nevoile utilizatorilor prin colectarea cerințelor, gestionarea setărilor și coordonarea modificărilor cu furnizorul.	Răspunde la întrebările utilizatorilor cu privire la o cerere, conform instrucțiunilor, și înregistrează solicitările în registrul prevăzut în acest scop.	Gestionează în mod independent o aplicație, stabilește prioritățile cererilor de modificare împreună cu utilizatorii și testează noile versiuni înainte ca acestea să fie lansate.	Stabilește modul în care este organizată gestionarea funcțională și decide asupra duratei de viață a aplicațiilor.
Gestionarea incidentelor și rezolvarea problemelor Preia sesizările privind întreruperile, identifică cauza prin măsuri specifice, restabilește serviciul și ține la curent persoanele care au semnalat problema și părțile interesate.	Înregistrează o întrerupere în întregime, parcurge pașii standard și escaladează problema imediat ce măsurile pe care le poate lua singur nu dau rezultate.	Stabilește o linie de investigare pentru o defecțiune necunoscută, restabilește serviciul și înregistrează cauza și soluția pentru a le putea reutiliza.	Elaborează procesul de gestionare a incidentelor din cadrul organizației, coordonează răspunsul la perturbări majore și raportează acest lucru conducerii și clienților.

Competență	N1	N3	N5
Clasificarea și păstrarea datelor Clasifică informațiile în funcție de gradul de confidențialitate și importanță, le asociază perioade de păstrare și asigură că ștergerea și arhivarea au loc efectiv.	Atribue o etichetă de clasificare conform schemei și trimite cazurile neclare către administrator.	Stabilește clasificarea și perioada de păstrare a unui flux de informații și verifică dacă curățarea se efectuează conform planului.	Elaborează politica de clasificare și retenție a organizației și o prezintă în cadrul auditurilor și al activităților de supraveghere.
Cunoștințe de bază privind rețelele Cunoaște la nivel general modul de funcționare a rețelelor, cum ar fi adresarea, rutarea, porturile și rezolvarea numelor, și poate identifica situațiile în care pot apărea probleme de conexiune.	Explică din ce părți este alcătuită o conexiune și efectuează o verificare specificată, cum ar fi un test de conectivitate.	Deducă, pe baza simptomelor, în ce strat de rețea se află o problemă și susține această deducție cu propriile măsurători.	Difuzează cunoștințele privind rețelele în cadrul organizației, stabilește principiile de proiectare și analizează proiectele de rețea prezentate de furnizori.
Furnizori IT și gestionarea contractelor Gestionează acordurile cu furnizorii IT privind livrarea, performanța și costurile, monitorizează respectarea acestora și ia măsuri în cazul abaterilor.	Verifică facturile și serviciile prestate în raport cu contractul și raportează abaterile către managerul de contract.	Organizează întâlniri cu furnizorii privind performanța și costurile, consemnează acordurile și intervine atunci când acestea nu sunt respectate.	Stabilește politica organizației privind furnizorii, încheie contractele principale și decide cu privire la reziliere sau schimbare.
Administrarea și monitorizarea sistemelor Asigură funcționarea sistemelor prin gestionarea setărilor, actualizărilor și permisiunilor, configurează monitorizarea și ia măsuri în urma semnalelor înainte ca utilizatorii să fie afectați.	Efectuează sarcini de întreținere programate și actualizări conform manualului de operațiuni și raportează abaterile observate în semnalele de monitorizare.	Gestionează în mod independent un mediu de sistem, stabilește praguri de monitorizare și elimină cauzele recurente ale intreruperilor.	Stabilește standardele de administrare și monitorizare ale organizației și decide asupra proiectării mediului de sistem.

6 Metode de evaluare și validitate

Validitățile sunt estimările meta-analitice corectate ale lui Sackett, Zhang, Berry și Lievens (2022) din Journal of Applied Psychology, care înlocuiesc cifrele mai vechi ale lui Schmidt și Hunter (1998). Dispersia este la fel de importantă ca media: cu o deviație standard ridicată, validitatea variază puternic în funcție de context.

Metodă de măsurare	rho	SD	Ce este
Centru de evaluare	0.29	0.09	Exerciții multiple, evaluatori multipli, notare pe dimensiuni.
Test de cunoștințe	0.40	0.13	Test de cunoștințe declarative privind posturile, elaborat de obicei pentru fiecare client în parte.
Testul cu probe de lucru	0.33	0.09	Candidatul realizează o probă de lucru reprezentativă în condiții standardizate.
Chestionar de personalitate	0.40	0.15	Autoevaluarea preferințelor comportamentale. La adresa hrnforce se găsesc testele „Big Fifty” și „15PF”.
Portofoliu sau dovezi	-	-	O colecție de lucrări sau rezultate anterioare, evaluate în funcție de criterii prestabilite.
Simulare	-	-	Situație de lucru simulată, de obicei în format digital, cu notare standardizată.
Situational Judgement Test	0.12	0.11	Scenariu cu opțiuni de răspuns, notat în funcție de cunoștințe sau de tendințe comportamentale.
Interviu structurat	0.42	0.19	Interviu bazat pe comportament, cu întrebări fixe și o scală de evaluare pentru fiecare întrebare.

7 Instrumente de evaluare pentru acest post

Instrument hrnforce	Competențe	Ce măsoară
Test de cunoștințe (specific clientului)	14	Test de cunoștințe profesionale, personalizat pentru fiecare client
Testul cu probe de lucru	9	Eșantion reprezentativ de muncă în condiții standardizate
Competency Check	6	Evaluarea competențelor la nivel comportamental
360 Feedback	5	Evaluări multiple bazate pe repere comportamentale

Instrument hrmforce	Competențe	Ce măsoară
Portofoliu	5	Evaluarea activității anterioare în raport cu criterii prestabilite
Big Fifty	3	Chestionar de personalitate, 150 de itemi, 25 de factori
Ability Scan	2	Test de aptitudini: abilități de raționament verbal, numeric și abstract
Interviu structurat	2	Interviu comportamental cu structură fixă
15PF	2	Profilul de personalitate, o alternativă mai succintă la Big Fifty
Big Fifty (Scala de integritate)	1	
Mental Resilience (4C)	1	Reziliența mentală conform modelului 4C

8 Cum se utilizează acest profil

1. Conveniți asupra profilului cu managerul de recrutare înainte de evaluarea primului candidat. Modificările de ponderare efectuate ulterior fac ca rezultatul să fie de nejustificat.
2. Alegeți metoda de evaluare pentru fiecare competență din coloana „Metoda de evaluare”. Combinați cel mult trei metode pentru fiecare candidat.
3. Calibrați evaluatorii într-o sesiune de două ore, utilizând punctele de referință din capitolul 5. Punctele de referință fără instruirea evaluatorilor au un efect redus.
4. Completați calculatorul de compatibilitate și discutați lacunele în cadrul conversației privind dezvoltarea profesională. Tipurile A și G sunt criterii de selecție, nu obiective de dezvoltare trimestriale.

Sursă: hrmforce Skills Framework 2.0, versiunea 2.0.0, creată la 2026-09-08. Corelații cu ESCO v1.2.1, O*NET 31.0, Lightcast Open Skills, SFIA 9, DigComp 3.0, EntreComp, LifeComp, GreenComp, AILit, WEF Future of Jobs 2025, ISCO-08 și clasificarea ocupațională olandeză CBS BRC 2014, ediția 2025. Acest profil reprezintă un punct de plecare, nu un standard: adaptați-l la propria organizație înainte de a-l utiliza ca bază pentru selecție.