ANUNȚ

PRIMĂRIA SECTORULUI 3 cu sediul în Bld. Basarabia nr.256, organizează în data de 17.11.2026 concurs de recrutare pentru ocuparea unor funcții publice de execuție vacante în baza art.XXII alin.(4) din Legea nr.141/2025 și art.VII alin.(7) din O.U.G. nr.121/2023 pentru modificarea și completarea Codului administrativ

➢ **Serviciul Dezvoltare Infrastructură IT**

1. Expert clasa I gradul profesional superior – 4 posturi - id posturi: 620982, 620983, 620984, 620985

- ***pregătire de specialitate: studii universitare de licență absolvite cu diplomă de licență sau echivalentă;***
- ***vechime minimă în specialitatea studiilor necesare exercitării funcției publice – minimum 7 ani;***
- **postul va fi ocupat pe perioadă nedeterminată, cu o durată normală a timpului de muncă de 8 ore/zi, 40 ore/săptămână;**

Candidații trebuie să îndeplinească condițiile prevăzute în art.465 din O.U.G. nr.57/2019 privind Codul Administrativ, cu modificările și completările ulterioare:

Poate ocupa o funcție publică persoana care îndeplinește următoarele condiții:

a) are cetățenia română și domiciliul în România;
b) cunoaște limba română, scris și vorbit;
c) are vârsta de minimum 18 ani împliniți;
d) are capacitate deplină de exercițiu;
e) este apt din punct de vedere medical și psihologic să exercite o funcție publică. Atestarea stării de sănătate se face pe bază de examen medical de specialitate, de către medicul de familie, respectiv pe bază de evaluare psihologică organizată prin intermediul unităților specializate acreditate în condițiile legii;
f) îndeplinește condițiile de studii și vechime în specialitate prevăzute de lege pentru ocuparea funcției publice;
g) îndeplinește condițiile specifice, conform fișei postului, pentru ocuparea funcției publice;
h) nu a fost condamnată pentru săvârșirea unei infracțiuni contra umanității, contra statului sau contra autorității, infracțiuni de corupție sau de serviciu, infracțiuni care împiedică înfăptuirea justiției, infracțiuni de fals ori a unei infracțiuni săvârșite cu intenție care ar face-o incompatibilă cu exercitarea funcției publice, cu excepția situației în care a intervenit reabilitarea, amnistia post-condamnatorie sau dezincriminarea faptei;
i) nu le-a fost interzis dreptul de a ocupa o funcție publică sau de a exercita profesia ori activitatea în executarea căreia a săvârșit fapta, prin hotărâre judecătorească definitivă, în condițiile legii;
j) nu a fost destituită dintr-o funcție publică sau nu i-a încetat contractul individual de muncă pentru motive disciplinare în ultimii 3 ani;
k) nu a fost lucrător al Securității sau colaborator al acesteia, în condițiile prevăzute de legislația specifică.

Datele dumneavoastră personale sunt prelucrate de Primăria Sectorului 3 în conformitate cu Regulamentul Uniunii Europene 2016/679 în scopul îndeplinirii atribuțiilor legale. Datele pot fi dezvăluite unor terți în baza unui temei legal justificat. Vă puteți exercita drepturile prevăzute în Regulamentul UE 2016/679, printr-o cerere scrisă, semnată și datată transmisă pe adresa Primăriei Sector 3.

În vederea participării la concurs, în termen de 20 de zile de la data publicării anunţului pe pagina de internet a autorităţii sau instituţiei publice organizatoare, candidaţii depun dosarul de concurs, care conţine în mod obligatoriu conform **art.94 din Anexa nr.X a O.U.G. nr.57/2019**, pentru aprobarea normelor privind organizarea şi dezvoltarea carierei funcţionarilor publici:

a) formularul de înscriere prevăzut în art.137 lit. b);
b) copia actului de identitate;
c) copia actului doveditor emis de autorităţile competente, în cazul în care a intervenit schimbarea numelui consemnat în certificatul de naştere;
d) copia carnetului de muncă şi a adeverinţei eliberate de angajator pentru perioada lucrată, care să ateste vechimea în muncă şi în specialitatea studiilor solicitate pentru ocuparea postului/funcţiei sau pentru exercitarea profesiei;
e) copii ale diplomelor de studii, certificatelor şi altor documente care atestă efectuarea unor specializări şi perfecţionări;
f) copia adeverinţei care atestă starea de sănătate corespunzătoare, eliberată cu cel mult 6 luni anterior derulării concursului de către medicul de familie al candidatului şi a avizului psihologic eliberat pe baza unei evaluări psihologice organizate prin intermediul unităţilor specializate acreditate în condiţiile legii, valabil potrivit prevederilor legale;
g) cazierul judiciar;

Documentul prevăzut la alin.(2) lit.g) poate fi înlocuit cu o declaraţie pe propria răspundere. În acest caz, candidatul declarat admis la selecţia dosarelor şi care nu a solicitat expres la înscrierea la concurs preluarea informaţiilor direct de la autoritatea sau instituţia publică competentă are obligaţia de a completa dosarul de concurs cu originalul documentului pe tot parcursul desfăşurării concursului, dar nu mai târziu de data şi ora organizării interviului, sub sancţiunea neemiterii actului administrativ de numire. În situaţia în care candidatul solicită expres la înscrierea la concurs preluarea informaţiilor direct de la autoritatea sau instituţia publică competentă, extrasul de pe cazierul judiciar se solicită potrivit legii şi procedurii aprobate la nivel instituţional.

h) declaraţia pe propria răspundere, prin completarea rubricii corespunzătoare din formularul de înscriere, sau adeverinţa care să ateste lipsa calităţii de lucrător al Securităţii sau colaborator al acesteia, în condiţiile prevăzute de legislaţia specifică.
i) declaraţia pe propria răspundere, prin completarea rubricii corespunzătoare din formularul de înscriere, privind faptul că, în ultimii 3 ani, persoana nu a fost destituită sau nu i-a încetat contractul individual de muncă pentru motive disciplinare.

Modelul orientativ al adeverinţei eliberate de angajator pentru perioada lucrată care atestă vechimea în muncă şi în specialitatea studiilor este prevăzut la art.137 lit.e) din Anexa 10 la O.U.G. nr.57/2019, cu modificările și completările ulterioare.

Copiile de pe actele menţionate se prezintă în formă legalizată sau însoţite de documentele originale, care se certifică pentru conformitate cu originalul de către secretarul comisiei de concurs

I. *CONDIŢIILE DE DESFĂŞURARE ALE CONCURSULUI :*

1. publicarea anunțului se va face în data de 16.10.2026
2. perioada în care se pot depune dosarele de înscriere – 16.10.2026 – 04.11.2026 (de luni până joi în intervalul orar 8^{30}-16^{00} şi vineri 8^{30}-13^{30}).;

3. instituţia publică la care se depun dosarele de înscriere – Primăria Sector 3, Serviciul Resurse Umane, email: resurseumane@primarie3.ro;
4. perioada de verificare eligibilitate candidaţi - în termen de 5 zile lucrătoare de la expirarea termenului de depunere a dosarelor;
5. perioada de depunere contestaţii la verificarea eligibilităţii candidaţilor - în termen de o zi lucrătoare de la data afişării rezultatului eligibilităţii candidaţilor;
6. perioada de soluţionare contestaţii la verificarea eligibilităţii candidaţilor în termen de o zi lucrătoare de la expirarea termenului de depunere a contestaţiilor;
7. data organizării concursului:
   - proba scrisă 17.11.2026 - ora 13^{00} .
   - interviul - nu mai târziu de 8 zile lucrătoare de la susţinerea probei scrise.
8. locul de desfăşurare al concursului - Primăria Sectorului 3, Bld.Basarabia nr.256, Sector 3.

Alte menţiuni referitoare la organizarea concursului se pot obţine la numărul de telefon: 0759.990.950 Serviciul Resurse Umane (secretar de comisie – Enache Narcisa, expert la Serviciul Resurse Umane şi pe site-ul instituţiei www.primarie3.ro la secţiunea Informaţii Utile/Concursuri.

II. BIBLIOGRAFIE/TEMATICĂ

Serviciul Dezvoltare Infrastructură IT

1. Constituţia României, republicată - în integralitate;
2. O.U.G. nr.57/2019 privind Codul administrativ, cu modificările şi completările ulterioare cu tematica Partea I, titlul I şi titlul II ale părţii a II- a, titlul I al părţii a IV- a, titlul I şi II ale părţii a VI- a;
3. Legea nr. 202/2002 privind egalitatea de şanse şi de tratament între femei şi bărbaţi, republicată, cu modificările şi completările ulterioare r3 - în integralitate;
4. O.G.nr.137/2000 privind prevenirea şi sancţionarea tuturor formelor de discriminare, republicată, cu modificările şi completările ulterioare r2 - în integralitate;
5. OUG nr.155/privind instituirea unui cadru pentru securitatea cibernetică a reţelelor şi sistemelor informatice din spaţiul cibernetic naţional civil, actul de transpunere a Directivei NIS2, publicată în Monitorul Oficial nr. 1332 din 31 decembrie 2024 şi aprobată ulterior cu modificări prin Legea nr. 124/2025 (MO nr. 638 din 7 iulie 2025, în vigoare de la 10 iulie 2025) - în integralitate.
6. Regulamentul nr. 1689/2024 de stabilire a unor norme armonizate privind inteligenţa artificială şi de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 şi (UE) 2019/2144 şi a Directivelor 2014/90/UE, (UE) 2016/797 şi (UE) 2020/1828 (Regulamentul privind inteligenţa artificială):
   - Capitolul I – Dispozitii Generale
   - Capitolul II – Practici interzise în domeniul IA
   - Capitolul III – Sisteme de IA cu grad ridicat de risc
   - Capitolul IV – Modele de IA de uz general
7. Reţele de calculatoare - Andrew S. Tanenbaum, ediţia a IV-a - în integralitate.
8. Bazele informaticii – Mihai Istrate, Carmen Hmelnitchi, Bucureşti 2010 - în integralitate.

Atribuțiile prevăzute în fișa de post pentru funcția publică de execuție vacantă de Expert clasa I gradul profesional superior – id post 620982 – 1 post

Serviciul Dezvoltare Infrastructură IT-

1. Analizează, coordonează și verifică activitățile de montare, demontare și relocare a echipamentelor de supraveghere video — camere, suporturi, cabluri și accesorii — în conformitate cu cerințele tehnice și standardele aplicabile.
2. Coordonează și verifică instalarea și configurarea echipamentelor din infrastructura video, inclusiv camere, NVR/DVR, alimentatoare și switch-uri, precum și realizarea setărilor necesare punerii acestora în funcțiune.
3. Analizează și stabilește soluțiile tehnice privind conectarea, cablarea, alimentarea și integrarea echipamentelor de supraveghere video în infrastructura de comunicații existentă.
4. Coordonează și verifică lucrările de joncționare a fibrei optice, inclusiv pregătirea cablurilor, realizarea sudurilor, protejarea îmbinărilor și efectuarea măsurătorilor privind continuitatea și calitatea semnalului.
5. Analizează cerințele tehnice și planifică etapele necesare instalării, extinderii, modernizării sau relocării sistemelor tehnice de securitate.
6. Stabilește și verifică soluțiile tehnice privind realizarea tubulaturii și a traseelor destinate sistemelor tehnice de securitate, în vederea asigurării unei infrastructuri de cablare corespunzătoare.
7. Coordonează și verifică realizarea cablajului aferent sistemelor tehnice de securitate, urmărind respectarea normelor tehnice, a documentațiilor și a cerințelor de calitate.
8. Coordonează, verifică și, după caz, participă la instalarea și configurarea sistemelor tehnice de detecție, antiefracție și control al accesului, conform specificațiilor tehnice aplicabile.
9. Coordonează și verifică instalarea și configurarea sistemelor de detecție, semnalizare și alarmare la incendiu, cu respectarea cerințelor tehnice și a reglementărilor în vigoare.
10. Coordonează și verifică instalarea sistemelor de televiziune cu circuit închis (TVCI) și a sistemelor tehnice de monitorizare, asigurând integrarea corespunzătoare a acestora în infrastructura existentă.
11. Coordonează și verifică operațiunile de testare și punere în funcțiune a sistemelor de detecție, antiefracție și control al accesului, de detecție, semnalizare și alarmare la incendiu, TVCI și de monitorizare.
12. Evaluează funcționarea echipamentelor și sistemelor instalate, analizează disfuncționalitățile identificate și stabilește sau implementează soluțiile tehnice necesare remedierii acestora.
13. Planifică, coordonează și verifică activitățile de mentenanță preventivă și corectivă pentru sistemele de detecție, antiefracție și control al accesului, sistemele de detecție, semnalizare și alarmare la incendiu, sistemele TVCI și de monitorizare, precum și pentru infrastructura de comunicații aferentă.
14. Coordonează și verifică activitățile de manipulare, transport și depozitare a echipamentelor IT și de securitate, urmărind respectarea normelor tehnice, de securitate și de protecție a bunurilor.
15. Analizează și aplică procedurile interne referitoare la instalarea, configurarea, administrarea și exploatarea echipamentelor și sistemelor tehnice și formulează propuneri pentru actualizarea și îmbunătățirea acestora.
16. Coordonează și verifică activitățile de inventariere și evidență a echipamentelor IT și de securitate, urmărind corectitudinea, completitudinea și actualizarea datelor înregistrate.
17. Soluționează în mod autonom, în limita competențelor, situațiile tehnice complexe și colaborează cu structurile de specialitate pentru identificarea și implementarea soluțiilor adecvate.
18. Gestionează și verifică evidența comunicărilor și a corespondenței repartizate prin intermediul programului Infocet, asigurând soluționarea și înregistrarea acestora în termenele stabilite.
19. Urmărește respectarea normelor de securitate și sănătate în muncă, precum și a cerințelor privind protecția echipamentelor, a infrastructurii informatice și a datelor prelucrate.
20. Informează periodic superiorul ierarhic cu privire la stadiul activităților, rezultatele obținute, riscurile identificate și problemele apărute și formulează propuneri de soluționare a acestora.

21. Efectuează activități de inspecție și control tehnic asupra infrastructurii IT, a rețelelor de comunicații și a sistemelor tehnice de securitate aflate în administrarea instituției, în limita competențelor postului.
22. Verifică respectarea cerințelor tehnice, a procedurilor interne și a standardelor aplicabile în activitățile de instalare, configurare, exploatare și mentenanță a echipamentelor și sistemelor informatice.
23. Controlează modul de funcționare și utilizare a sistemelor de supraveghere video, control al accesului, detecție, semnalizare și alarmare, precum și a infrastructurii de comunicații aferente.
24. Verifică starea tehnică a echipamentelor, existența și integritatea acestora, concordanța dintre situația constatată în teren și evidențele tehnice și patrimoniale disponibile.
25. Identifică neconformitățile, vulnerabilitățile și riscurile tehnice care pot afecta disponibilitatea, integritatea, confidențialitatea sau funcționarea sistemelor informatice și de securitate.
26. Întocmește note de constatare, rapoarte de inspecție și informări privind deficiențele identificate și formulează propuneri de remediere, prevenire și îmbunătățire.
27. Stabilește, împreună cu structurile competente și cu aprobarea superiorului ierarhic, măsurile tehnice necesare remedierii deficiențelor constatate și urmărește ducerea acestora la îndeplinire.
28. Verifică modul de remediere a neconformităților constatate și evaluează eficiența măsurilor tehnice implementate.
29. Participă la verificarea modului în care prestatorii și furnizorii respectă obligațiile tehnice asumate prin contracte, caiete de sarcini, oferte și acorduri privind nivelul serviciilor, semnalând eventualele neconformități.
30. Verifică existența, actualizarea și corectitudinea documentației tehnice aferente sistemelor și echipamentelor, inclusiv scheme, configurații, registre de intervenții, procese-verbale și evidențe de mentenanță.
31. Participă la recepția tehnică a echipamentelor, lucrărilor și serviciilor IT și verifică îndeplinirea cerințelor tehnice și funcționale stabilite prin documentația contractuală.
32. Realizează controale periodice sau tematice privind respectarea măsurilor de securitate IT și semnalează incidentele, vulnerabilitățile și situațiile care pot genera acces neautorizat, pierderi de date sau întreruperea serviciilor.
33. Acordă asistență tehnică în cadrul activităților de audit și control desfășurate de structurile interne sau de instituțiile abilitate, punând la dispoziție informațiile și documentele solicitate, în limita competențelor.
34. Monitorizează riscurile asociate infrastructurii IT și sistemelor tehnice de securitate și formulează propuneri pentru reducerea probabilității de producere și a impactului acestora.
35. Informează operativ superiorul ierarhic cu privire la deficiențele grave, incidentele de securitate sau situațiile care pot afecta continuitatea serviciilor IT și propune măsurile care se impun.
36. Participă la elaborarea și actualizarea procedurilor, instrucțiunilor și instrumentelor de control aplicabile infrastructurii IT și sistemelor tehnice de securitate.
37. Urmărește implementarea recomandărilor formulate în urma activităților de inspecție, control sau audit și raportează stadiul măsurilor stabilite.
38. Îndeplinește orice alte atribuții dispuse de superiorul ierarhic sau de Primar, cu respectarea prevederilor legale, care corespund pregătirii profesionale, competențelor funcției publice și obiectului de activitate al structurii din care face parte, în colaborare cu personalul IT responsabil
39. Aplică și respectă procedurile sistemului de management al securității informației și alte informații documentate ale SMSI aplicabile structurii organizatorice, în conformitate cu cerințele SR EN ISO/IEC 27001:2023 și documentele interne aplicabile;
40. Respectă prevederile standardului SR ISO 37001:2017-antimită;
41. Preia responsabilitățile aferente sistemului de management al securității informației din procedurile de sistem și operaționale difuzate.
42. Cunoaște, aplică și urmărește respectarea prevederilor Regulamentului intern și ale Regulamentului de organizare și funcționare, în exercitarea atribuțiilor specifice postului.

Atribuțiile prevăzute în fișa de post pentru funcția publică de execuție vacantă de Expert clasa I gradul profesional superior – id post 620983 – 1 post

Serviciul Dezvoltare Infrastructură IT-

1. Analizează neregularitățile identificate sau sesizate în activitatea structurii, stabilește cauzele acestora și formulează propuneri fundamentate privind măsurile de remediere și prevenire, în limita competențelor.
2. Coordonează, din punct de vedere tehnic, implementarea și menținerea măsurilor de securitate IT destinate prevenirii, identificării și eliminării accesului neautorizat, atacurilor informatice și programelor malițioase la nivelul echipamentelor active de rețea, serverelor și stațiilor de lucru.
3. Analizează necesitățile structurilor instituției și acordă asistență de specialitate pentru elaborarea referatelor de necesitate privind achiziționarea bunurilor, serviciilor și echipamentelor din domeniul comunicațiilor și tehnologiei informației.
4. Proiectează, dezvoltă și optimizează rapoarte necesare fundamentării deciziilor, eficientizării activității și utilizării corespunzătoare a resurselor instituției.
5. Elaborează rapoarte, analize și reprezentări grafice complexe, inclusiv cu funcționalități de tip drill-down, privind informațiile financiare, performanța operațională, utilizarea resurselor și datele structurate sau nestructurate colectate la nivelul Sectorului 3.
6. Administrează și monitorizează funcționarea rețelei de calculatoare din locația în care își desfășoară activitatea, efectuează operațiuni de mentenanță și gestionează evidența echipamentelor IT aflate în folosință.
7. Organizează și realizează instruirea utilizatorilor privind folosirea corectă și în condiții de securitate a programelor și aplicațiilor informatice, monitorizând modul de utilizare și acordând asistență tehnică de specialitate.
8. Proiectează, dezvoltă, adaptează și documentează programe sau module software în limbajele de programare stabilite, cu respectarea specificațiilor tehnice și funcționale.
9. Asigură suportul tehnic de specialitate pentru proiectarea, dezvoltarea, implementarea și integrarea programelor pentru calculator în sistemul informatic al instituției, conform specificațiilor aprobate.
10. Planifică și execută activități de testare funcțională și tehnică a programelor informatice, analizează rezultatele obținute și propune măsuri pentru remedierea neconformităților identificate.
11. Realizează activități complexe de analiză, proiectare, dezvoltare, testare, implementare și modificare a sistemelor informatice, utilizând cunoștințe avansate privind tehnologiile software și hardware.
12. Analizează și adaptează soluțiile hardware, software, sistemele de operare și aplicațiile existente sau proiectate la necesitățile reale și estimate ale utilizatorilor, în vederea optimizării performanței și a timpilor de răspuns.
13. Realizează analize tehnice și funcționale în vederea definirii specificațiilor necesare dezvoltării sau achiziționării sistemelor informatice capabile să răspundă cerințelor utilizatorilor și obiectivelor instituției.
14. Acordă expertiză de specialitate și asistență practică în administrarea sistemelor de baze de date și în utilizarea datelor informatice, pe întregul ciclu de viață al sistemelor, cu respectarea cerințelor de calitate, integritate, disponibilitate și securitate.
15. Evaluează compatibilitatea și interoperabilitatea soluțiilor hardware și software și formulează propuneri privind dezvoltarea, integrarea, modernizarea sau optimizarea infrastructurii și sistemelor informatice.
16. Elaborează documentații tehnice, instrucțiuni de lucru, specificații funcționale și rapoarte de analiză aferente sistemelor informatice administrate sau dezvoltate.
17. Efectuează deplasări în interes de serviciu pentru realizarea activităților tehnice, verificărilor, intervențiilor și evaluărilor stabilite la nivelul departamentului sau dispuse de superiorul ierarhic.
18. Colaborează cu personalul Serviciului Dezvoltare Infrastructură IT și cu celelalte structuri ale instituției pentru soluționarea cerințelor tehnice, implementarea proiectelor și asigurarea continuității serviciilor informatice.

19. Administrează procesul operativ de funcționare a SIC SSPS3, monitorizează disponibilitatea și performanța componentelor acestuia și propune măsuri pentru asigurarea continuității operaționale.
20. Asigură managementul configurației SIC SSPS3, menține evidența configurațiilor aprobate și controlează implementarea modificărilor tehnice autorizate.
21. Administrează conturile și drepturile de acces la resursele SIC SSPS3, în baza cererilor avizate de administratorul de securitate și de șeful structurii de securitate sau funcționarul de securitate și aprobate de conducătorul instituției.
22. Monitorizează utilizarea echipamentelor SIC SSPS3 și asigură exploatarea acestora în condiții optime, cu respectarea cerințelor tehnice și a politicilor de securitate aplicabile.
23. Gestionează și repartizează resursele hardware și software ale SIC SSPS3, în raport cu necesitățile operaționale, drepturile aprobate și cerințele de securitate.
24. Planifică, realizează și monitorizează activitățile de întreținere, diagnosticare și reparare a echipamentelor SIC SSPS3, urmărind remedierea defecțiunilor și restabilirea serviciilor.
25. Actualizează și verifică evidențele tehnice și operaționale referitoare la funcționarea, configurarea, mentenanța și incidentele aferente SIC SSPS3.
26. Instalează, configurează, actualizează și monitorizează sistemele de operare și componentele software ale SIC SSPS3, în conformitate cu configurațiile și politicile de securitate aprobate.
27. Identifică și notifică imediat administratorul de securitate cu privire la incidentele, vulnerabilitățile sau evenimentele informatice produse ori susceptibile să afecteze securitatea și funcționarea SIC SSPS3.
28. Coordonează, din punct de vedere tehnic, activitățile de colectare, salvare, protejare, evaluare și analiză a înregistrărilor de audit, jurnalelor de sistem și jurnalelor generate de soluțiile antivirus.
29. Analizează jurnalele și evenimentele înregistrate de sistemele informatice, identifică abaterile sau comportamentele neobișnuite și formulează propuneri privind măsurile tehnice necesare.
30. Elaborează, revizuiește, documentează și propune actualizarea politicilor și procedurilor aplicabile Sistemului de management al securității informației, în conformitate cu cerințele SR EN ISO/IEC 27001:2023 și cu reglementările aplicabile.
31. Monitorizează respectarea politicilor, procedurilor și instrucțiunilor specifice Sistemului de management al securității informației și semnalează neconformitățile identificate.
32. Evaluează performanța Sistemului de management al securității informației și elaborează rapoarte pentru conducerea instituției privind rezultatele obținute, riscurile identificate și oportunitățile de îmbunătățire.
33. Participă la stabilirea acțiunilor corective și preventive aferente neconformităților identificate și monitorizează implementarea și eficacitatea acestora.
34. Asigură comunicarea și difuzarea controlată a politicii privind securitatea informației și a procedurilor aferente SMSI către structurile și persoanele responsabile.
35. Formulează propuneri privind îmbunătățirea continuă a Sistemului de management al securității informației, reducerea riscurilor și creșterea nivelului de protecție a resurselor informaționale ale instituției.
36. Efectuează verificări privind funcționarea, utilizarea și administrarea infrastructurii, echipamentelor, aplicațiilor și serviciilor TIC.
37. Verifică respectarea procedurilor, instrucțiunilor, politicilor și măsurilor interne aplicabile activităților din domeniul TIC.
38. Identifică și analizează riscurile asociate activităților și sistemelor informatice din domeniul repartizat.
39. Identifică și consemnează neconformitățile, vulnerabilitățile și deficiențele constatate în urma verificărilor efectuate.
40. Întocmește note de constatare, rapoarte de verificare, informări și propuneri de măsuri pentru remedierea deficiențelor identificate.
41. Verifică implementarea măsurilor dispuse în urma activităților de control și informează șeful serviciului cu privire la stadiul și rezultatele acestora.
42. Participă la evaluarea incidentelor informatice, analizează cauzele acestora și propune măsuri pentru limitarea efectelor și prevenirea reapariției lor.

43. Asigură suportul tehnic necesar desfășurării misiunilor de audit informatic și pregătește documentele și informațiile solicitate.
44. Participă la elaborarea răspunsurilor și planurilor de măsuri formulate în urma recomandărilor entităților de audit și control.
45. Verifică evidențele privind echipamentele, licențele, aplicațiile și celelalte resurse TIC și semnalează neconcordanțele identificate.
46. Verifică din punct de vedere tehnic respectarea cerințelor și nivelurilor de servicii asumate de furnizorii și prestatorii IT.
47. Colaborează cu structurile de specialitate ale instituției și cu cele ale entităților subordonate Consiliului Local al Sectorului 3 în cadrul verificărilor repartizate.
48. Participă la testarea măsurilor privind continuitatea serviciilor IT, recuperarea datelor și restabilirea funcționării sistemelor.
49. Formulează propuneri privind actualizarea procedurilor și îmbunătățirea mecanismelor de control intern din domeniul TIC.
50. Contribuie la eficacitatea sistemului de management al securității informației;
51. Îndeplinește și alte atribuții dispuse de superiorul ierarhic sau de Primar, în condițiile legii, care corespund pregătirii profesionale, competențelor postului și domeniului de activitate al structurii.
52. Aplică și respectă procedurile sistemului de management al securității informației și alte informații documentate ale SMSI aplicabile structurii organizatorice, în conformitate cu cerințele SR EN ISO/IEC 27001:2023 și documentele interne aplicabile;
53. Respectă prevederile standardului SR ISO 37001:2017- antimită;
54. Preia responsabilitățile aferente sistemului de management al securității informației din procedurile de sistem și operaționale difuzate;
55. Cunoaște, aplică și urmărește respectarea prevederilor Regulamentului intern și ale Regulamentului de organizare și funcționare, în exercitarea atribuțiilor specifice postului.

Atribuțiile prevăzute în fișa de post pentru funcțiile publice de execuție vacante de Expert clasa I gradul profesional superior – id post 620984 și 620985 – 2 posturi

1. Participă la stabilirea strategia de informatizare și digitalizare pe termen scurt, mediu și lung a Primăriei Sectorului 3;
2. Participă, în calitate de consultant tenic, la selecțiile de oferte sau licitațiile organizate pentru achizițiile de tehnică de calcul (hardware și software);
3. Propune achiziționarea de consumabile pentru tehnica de calcul în baza evaluării solicitărilor formulate de compartimentele Primăriei;
4. Asigură managementul resurselor software (licențe), resurselor hardware și de rețea ale instituției;
5. Propune achiziționarea de consumabile pentru tehnica de calcul în baza evaluării solicitărilor formulate de compartimentele Primăriei;
6. Asigură relația cu furnizorii și implementarea contractelor de servicii;
7. Participă împreună cu furnizorii de programe software la realizarea analizei în vederea implementării programelor;
8. Susține proiectarea și dezvoltarea de noi soluții/aplicații și asigură implementarea acestora
9. Identifică și evaluează factorii de risc pentru activitățile proprii;
10. Gestionează eficient resursele materiale și tehnologice existente ;
11. Stabilește necesitățile de tehnică de calcul și programe informatice ale compartimentelor Primăriei Sector 3 și propune achizițiile necesare ;
12. Planifică procesul de îmbunătățire al activităților de implementare a sistemului informatic;
13. Colaborează cu serviciile de specialitate din PMB, cu alte Primării de sector sau municipii, precum și cu instituțiile publice subordonate Consiliului local Sector 3 pentru realizarea unei strategii comune de informatizare ;
14. Completează și actualizează registrul riscurilor la nivelul serviciului;

15. Testează la nivel de utilizator în mediu de test și realizează rapoarte în urma testărilor efectuate;
16. Elaborează programe sau module de program în limbajul de programare specificat de programator sau inginer de sistem;
17. Instruiește și monitorizează folosirea corectă a programelor/aplicațiilor de către utilizatori și acordă asistență atunci când situația o cere;
18. Asigură suportul tehnic pentru realizarea analizei în vederea definirii specificațiilor pentru construirea efectivă a sistemelor informatice, centralizând cerințele utilizatorilor;
19. Activități care combină aptitudinile analitice și de proiectare cu cunoștințe adecvate de tehnologie software și hardware, în vederea definirii, proiectării, realizării, testării, implementării și modificării sistemelor informatice ce conțin software ca principală component;
20. Activități de adaptare și/sau de armonizare a soluțiilor hardware, software și a sistemelor de operare, precum și a aplicațiilor existente ori proiectate la necesitățile reale sau estimate ale utilizatorilor, în vederea îndeplinirii cerințelor privind satisfacerea gradului de solicitare (timpul de răspuns);
21. Activități de asigurare a suportului tehnic pentru realizarea analizei în vederea definirii specificațiilor pentru construirea efectivă a sistemelor informatice, susceptibile să răspundă cerințelor utilizatorilor;
22. Efectuează deplasări în interes de serviciu pe teren în funcție de necesitățile departamentale trasate de către superiorul ierarhic;
23. Îndeplinește orice alte atribuții date de către superiorul ierarhic sau de către Primar, care prin natura lor sunt de competența sau se încadrează în obiectul și atribuțiile departamentale împreuna cu Serviciul Dezvoltare Infrastructură IT;
24. Activități de furnizare a expertizei de specialitate și a asistenței practice în managementul sistemelor de baze de date și în utilizarea datelor informatice pentru a răspunde cerințelor sistemului informatic în orice moment al ciclului de viață, în conformitate cu criteriile de calitate definite;
25. Activități de realizare a analizei în vederea definirii specificațiilor pentru construirea efectivă a sistemelor informatice, susceptibile să răspundă cerințelor utilizatorilor;
26. Activități care combină aptitudinile analitice și de proiectare cu cunoștințe adecvate de tehnologie software și hardware, în vederea definirii, proiectării, realizării, testării, implementării și modificării sistemelor informatice ce conțin software ca principală component;
27. Activități de adaptare și/sau de armonizare a soluțiilor hardware, software și a sistemelor de operare, precum și a aplicațiilor existente ori proiectate la necesitățile reale sau estimate ale utilizatorilor, în vederea îndeplinirii cerințelor privind satisfacerea gradului de solicitare (timpul de răspuns);
28. Activități de asigurare a suportului tehnic pentru realizarea analizei în vederea definirii specificațiilor pentru construirea efectivă a sistemelor informatice, susceptibile să răspundă cerințelor utilizatorilor;
29. Efectuează verificări privind funcționarea, utilizarea și administrarea infrastructurii, echipamentelor, aplicațiilor și serviciilor TIC.
30. Verifică respectarea procedurilor, instrucțiunilor, politicilor și măsurilor interne aplicabile activităților din domeniul TIC.
31. Identifică și analizează riscurile asociate activităților și sistemelor informatice din domeniul repartizat.
32. Identifică și consemnează neconformitățile, vulnerabilitățile și deficiențele constatate în urma verificărilor efectuate.
33. Întocmește note de constatare, rapoarte de verificare, informări și propuneri de măsuri pentru remedierea deficiențelor identificate.
34. Verifică implementarea măsurilor dispuse în urma activităților de control și informează șeful serviciului cu privire la stadiul și rezultatele acestora.
35. Participă la evaluarea incidentelor informatice, analizează cauzele acestora și propune măsuri pentru limitarea efectelor și prevenirea reapariției lor.
36. Asigură suportul tehnic necesar desfășurării misiunilor de audit informatic și pregătește documentele și informațiile solicitate.
37. Participă la elaborarea răspunsurilor și planurilor de măsuri formulate în urma recomandărilor entităților de audit și control.
38. Verifică evidențele privind echipamentele, licențele, aplicațiile și celelalte resurse TIC și semnalează neconcordanțele identificate.

E-MAIL resurseumane@primarie3.ro
Calea Dudești nr. 191, Sector 3, 031084, București

39. Verifică din punct de vedere tehnic respectarea cerințelor și nivelurilor de servicii asumate de furnizorii și prestatorii IT.
40. Colaborează cu structurile de specialitate ale instituției și cu cele ale entităților subordonate Consiliului Local al Sectorului 3 în cadrul verificărilor repartizate.
41. Participă la testarea măsurilor privind continuitatea serviciilor IT, recuperarea datelor și restabilirea funcționării sistemelor.
42. Formulează propuneri privind actualizarea procedurilor și îmbunătățirea mecanismelor de control intern din domeniul TIC.
43. Contribuie la eficacitatea sistemului de management al securității informației;
44. Aplică și respectă procedurile sistemului de management al securității informației și alte informații documentate ale SMSI aplicabile structurii organizatorice, în conformitate cu cerințele SR EN ISO/IEC27001:2023 și documentele interne aplicabile;
45. Respectă prevederile standardului SR ISO 37001:2017- antimită;
46. Preia responsabilitățile aferente sistemului de management al securității informației din procedurile de sistem și operaționale difuzate.
47. Cunoaște, aplică și urmărește respectarea prevederilor Regulamentului intern și ale Regulamentului de organizare și funcționare, în exercitarea atribuțiilor specifice postului.

PRIMAR
ROBERT SORIN NEGOIȚĂ

DISP.OZ.
NR. 2371 /2026
VICEPRIMAR
ADRIAN MARIAN COCOȘ

Director Executiv Adjunct II,

Eugenia Demeter

Șef Serviciu,
Elena Mărculescu

Întocmit,
Narcisa Enache