ROMÂNIA

MINISTERUL AFACERILOR INTERNE
INSTITUŢIA PREFECTULUI – JUDEŢUL DOLJ

AVIZAT,
PREFECT,
DAN DIACONU

Afișat azi: 16.09.2024

ANUNŢ CONCURS
Nr. 10464 / 16.09.2024.

Instituția Prefectului-județul Dolj, organizează concurs de recrutare pentru ocuparea pe perioadă nedeterminată a funcției publice vacante de

consilier, clasa I, grad profesional superior
în cadrul Compartimentului Structura de Securitate.

Durata timpului de muncă: durată normală a timpului de muncă, **8h/zi, respectiv 40 ore/săptămână.**

Concursul se organizează în conformitate cu prevederile **art. VII alin.(4) din O.U.G. nr. 115/2023** privind unele măsuri fiscal-bugetare în domeniul cheltuielilor publice, pentru consolidare fiscală, combaterea evaziunii fiscale, pentru modificarea şi completarea unor acte normative, precum şi pentru prorogarea unor termene, cu modificările şi completările ulterioare, şi **art. VII alin. (7)/XI din O.U.G. 121/2023** pentru modificarea şi completarea Ordonanţei de urgenţă a Guvernului nr. 57/2019 privind Codul administrativ, precum şi pentru modificarea art. III din Ordonanţa de urgenţă a Guvernului nr. 191/2022 pentru modificarea şi completarea Ordonanţei de urgenţă a Guvernului nr. 57/2019 privind Codul administrativ, cu modificările şi completările ulterioare.

Concursul va avea loc la sediul Instituției Prefectului -județul Dolj din strada Amaradia nr. 93-95, Municipiul Craiova, județul Dolj, după cum urmează:

1.verificarea eligibilității candidaților - se realizează în termen de maximum 5 zile lucrătoare de la data expirării termenului de depunere a dosarelor de concurs
2. proba scrisă – 18 octombrie 2024, ora 12,00
3. proba de interviu – se susţine într-un termen de maximum 8 zile lucrătoare de la data afişării rezultatului probei scrise. Data, ora şi locul susţinerii probei interviului se afişează odată cu rezultatele la proba scrisă.

Condiții de ocupare a unei funcții publice
Candidații trebuie să îndeplinească condițiile prevăzute de art. 465 alin. (1) din Ordonanța de urgență a Guvernului nr. 57/2019 Codul administrativ, cu modificările şi completările ulterioare:

a) are cetăţenia română şi domiciliul în România;

b) cunoaşte limba română, scris şi vorbit;

c) are vârsta de minimum 18 ani împliniţi;

d) are capacitate deplină de exerciţiu;

e) este apt din punct de vedere medical şi psihologic să exercite o funcţie 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 unităţilor specializate acreditate în condiţiile legii;

f) îndeplineşte condiţiile de studii şi vechime în specialitate prevăzute de lege pentru ocuparea funcţiei publice;

g) dovedeşte prin certificat sau, după caz, prin alt tip de document absolvirea unei perfecţionări sau specializări stabilite expres de lege pentru ocuparea unor funcţii publice;

g^1) are cunoştinţe teoretice în domeniul tehnologiei informaţiei, nivel utilizator începător;

g^2) îndeplineşte condiţia de ocupare a postului referitoare la obţinerea unui aviz sau a unei autorizaţii, în condiţiile legii, în situaţia în care pentru funcţia publică respectivă este prevăzută ca obligatorie această condiţie de ocupare a postului, justificată de îndeplinirea unor atribuţii care necesită un astfel de aviz sau autorizaţie;

h) nu a fost condamnată pentru săvârşirea unei infracţiuni contra umanităţii, contra statului sau contra autorităţii, infracţiuni de corupţie sau de serviciu, infracţiuni care împiedică înfăptuirea justiţiei, infracţiuni de fals ori a unei infracţiuni săvârşite cu intenţie care ar face-o incompatibilă cu exercitarea funcţiei publice, cu excepţia situaţiei în care a intervenit reabilitarea, amnistia post-condamnatorie sau dezincriminarea faptei;

i) nu le-a fost interzis dreptul de a ocupa o funcţie publică sau de a exercita profesia ori activitatea în executarea căreia a săvârşit fapta, prin hotărâre judecătorească definitivă, în condiţiile legii;

j) nu a fost destituită dintr-o funcţie publică sau nu i-a încetat contractul individual de muncă pentru motive disciplinare în ultimii 3 ani;

k) nu a fost lucrător al Securităţii sau colaborator al acesteia, în condiţiile prevăzute de legislaţia specifică;

l) i s-a aplicat una dintre modalităţile de ocupare a funcţiilor publice prevăzute la art. 466 alin. (2).

(2) Condiţia de ocupare a funcţiei publice prevăzută la alin. (1) lit. g^2) se îndeplineşte în termenele şi condiţiile prevăzute de legislaţia specifică.

Condiţii pentru ocuparea postului:

1.<u>studii de specialitate</u>: studii superioare de lungă durată absolvite cu diplomă de licenţă sau echivalentă în următoarele domenii:

- Domeniul fundamental:Ştiinţe inginereşti, Ramura de ştiinţă: **Ingineria sistemelor, calculatoare şi tehnologia informaţiei,**
- Domeniul fundamental: Matematică şi ştiinţe ale naturii, Ramura de ştiinţă: **Informatică**;

2. <u>Vechime minimă în specialitatea studiilor</u>: 7 ani

Condiţii specifice:

Pentru candidatul declarat „ADMIS" la concurs şi numit în funcţia publică, se solicită obligatoriu aviz pentru obţinerea certificatului de securitate pentru acces la informaţii clasificate- **nivelul 'strict secret"**, conform legii.

Dosarele de înscriere la concurs se pot depune în termen de 20 de zile de la data publicării prezentului anuntului pe site -ul , www.dj.prefectura.mai.gov.ro, în perioada **16.09.2024- 07.10.2024.**

Dosarul trebuie să conțină în mod obligatoriu:

a) formularul de înscriere prevăzut în anexa nr.1
b) copia cărţii 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/sau a adeverinţei eliberate de angajator pentru perioada lucrată, care să ateste vechimea în muncă şi în specialitatea studiilor necesare pentru ocuparea postului deţinut, potrivit prevederilor din prezentul cod, după caz;
e) copii ale diplomelor de studii sau echivalente, certificatelor şi altor documente care atestă efectuarea unor specializări şi perfecţionări sau deţinerea unor competenţe specifice, după caz;
f) copia adeverinţei care atestă starea de sănătate corespunzătoare, eliberată cu cel mult 6 luni anterior demarării etapei de selecţie 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;
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.

Cazierul judiciar poate fi înlocuit cu o declaraţie pe propria răspundere prin completarea rubricii corespunzătoare din formularul de înscriere. În acest caz, candidatul declarat admis la proba de verificare a eligibilităţii şi care nu a solicitat expres la înscrierea la concurs preluarea informaţiilor direct de la autoritatea sau instituţia publică competentă are obligaţia să completeze dosarul de concurs pe tot parcursul desfăşurării etapei de selecţie, dar nu mai târziu de data şi ora organizării interviului, sub sancţiunea neemiterii actului administrativ de numire în funcţia publică. În situaţia în care, la înscrierea la concurs, candidatul solicită expres 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.

Modelul orientativ al adeverinţei menţionate la lit. d) este prevăzut în Anexa nr.2. Adeverinţele care au un alt format decât cel prevăzut în Anexa nr.2 trebuie să cuprindă elemente similare acestuia, din care să rezulte cel puţin următoarele informaţii: funcţia/funcţiile ocupată/ocupate, nivelul studiilor solicitate pentru ocuparea acesteia/acestora, temeiul legal al desfăşurării activităţii, vechimea în muncă acumulată, precum şi vechimea în specialitatea studiilor.

Modalitatea de transmitere a dosarului

Dosarul de concurs se poate depune personal de către candidat la sediul Instituției Prefectului – județul Dolj din strada Amaradia, nr. 93-95, la Compartimentul Resurse umane, de luni până joi între orele 9,00 -16,30, şi vineri între orele 9,00 -14,00.

De asemenea, dosarul se poate transmite prin intermediul unui serviciu de curierat sau se poate transmite în format electronic, la adresa de e-mail: office@prefecturadolj.ro

Dosarele de concurs transmise de candidaţi la adresa de e-mail indicată mai sus după terminarea programului de lucru al instituţiei, dar în perioada de depunere a dosarelor de concurs, li se atribuie număr de înregistrare în ziua lucrătoare următoare, iar dosarul de concurs este considerat ca fiind depus în termen.

Documentele care constituie dosarul de concurs se depun în copie, cu obligaţia candidatului de a prezenta secretarului comisiei de concurs originalele acestor documente, pentru certificare pentru conformitate cu originalul, până cel târziu la data desfăşurării probei interviului, sub sancţiunea neemiterii actului administrativ de numire în funcţia publică în cazul promovării concursului.

Bibliografie /tematică

1. Constituția României, republicată
   cu tematica:Constituția României, republicată
2. Ordonanța Guvernului nr. 137/2000 privind prevenirea și sancționarea tuturor formelor de discriminare, republicată, cu modificările și completările ulterioare ,
   cu tematica: Ordonanța Guvernului nr. 137/2000 privind prevenirea și sancționarea tuturor formelor de discriminare, republicată, cu modificările și completările ulterioare
3. Legea nr. 202/2002 privind egalitatea de șanse și de tratament între femei și bărbați, republicată, cu modificările și completările ulterioare
   cu tematica: Legea nr. 202/2002 privind egalitatea de șanse și de tratament între femei și bărbați, republicată, cu modificările și completările ulterioare
4. Partea I, titlul I şi titlul II ale părții a II-a, titlul I al părții a IV-a, titlul I şi II ale părţii a VI-a din Ordonanța de urgență a Guvernului nr. 57/2019, cu modificările și completările ulterioare
   cu tematica: Partea I, titlul I şi titlul II ale părții a II-a, titlul I al părții a IV-a, titlul I şi II ale părţii a VI-a din Ordonanța de urgență a Guvernului nr. 57/2019, cu modificările și completările ulterioare
5. Legea nr. 182/2002 privind protecția informațiilor clasificate, cu modificările si completările ulterioare,
   cu tematica: Cap. I. Secțiunea 2- definiții- Cap. II. Informații secrete de stat Cap. III Informații secrete de serviciu Cap. V Obligații, răspunderi și sancțiuni
6. H.G. nr. 585/2002 pentru aprobarea Standardelor naționale de protecție a informațiilor clasificate în România, cu modificările si completările ulterioare
   cu tematica: Cap. 2- Clasificarea și declasificarea informațiilor, măsuri minime de protecție specifice claselor și nivelurilor de secretizare; Cap. 3- Reguli generale privind evidența, întocmirea, păstrarea, procesarea, multiplicarea, manipularea, transportul, transmiterea și distrugerea informațiilor clasificate;
7. Ordinul directorului general al ORNISS nr. 16/2014 pentru aprobarea Directivei principale privind domeniul INFOSEC– INFOSEC 2 (www.orniss.ro);
   cu tematica: Cap. II- Activităţi privind securitatea pe întregul ciclu de viaţă al SIC;

Atribuțiile prevăzute în fișa postului:

1. în calitate de şef C.S.T.I.C. îndeplineşte următoarele atribuţii:

a) solicită acreditarea/reacreditarea SIC de la A.A.I.A.S. (Autoritatea Administraţiei şi Internelor de Acreditare de Securitate) pentru următoarele activităţi:

- planifică dezvoltarea sau achiziţia unui SIC care stochează, procesează sau transmit informaţii clasificate- propune schimbarea configuraţiei de sistem existente
- propune conectarea cu un alt SIC
- propune schimbări ale modului de operare protejată al SIC- propune modificarea sau înlocuirea software-ului pentru optimizarea securităţii SIC
- iniţiază proceduri de modificare a clasei sau nivelului de secretizare a SIC care au fost deja acreditate- planifică sau propune desfăşurarea oricărei alte activităţi în scopul îmbunătăţirii securităţii SIC care au fost deja create

b) solicită asistenţă de specialitate din partea A.A.I.A.S. (Autoritatea Administraţiei şi Internelor de Acreditare de Securitate) şi A.A.I.S.I.C. (Autoritatea Administraţiei şi Internelor de Securitate pentru Informatică şi Comunicaţii) pentru stabilirea cerinţelor de securitate şi procedurilor de aplicare necesare şi respectării de către furnizorii de echipamente, pe durata întregului proces de dezvoltare, instalare şi testare SIC

c) răspunde de alegerea, implementarea, justificarea şi controlul facilităţilor de securitate, de natură tehnică, care reprezintă parte componentă a SIC

d) asigură exploatarea în condiţii de securitate a SIC

e) realizează legătura între contractant, A.A.I.S.I.C. şi A.A.I.A.S.

f) participă la selecţionarea, organizarea şi realizarea pregătirii personalului cu atribuţii în domeniul INFOSEC

g) organizează şi desfăşoară convocări de instruire cu personalul din subordine şi utilizatorii din SIC

h) stabileşte responsabilităţile personalului din subordine

i) verifică periodic sau în timp real, implementarea măsurilor de protecţie în SIC, din cadrul unităţii/structurii, pentru a se asigura că securitatea acestuia este în concordanţă cu cerinţele de securitate aprobate de A.A.I.A.S.

j) ţine evidenţa echipamentelor SIC, proprietate privată, autorizate să funcţioneze în incinta unităţii, în condiţiile capitolului XI din OMAI nr. 810/2005

k) cercetează incidentele de securitate şi raportează rezultatele, ierarhic, A.A.I.A.S. şi A.A.I.S.I.C., concomitent cu aplicarea unor măsuri de reducere a consecinţelor

2. în calitate de administrator de securitate al SIC îndeplineşte următoarele atribuţii principale:

a) elaborează şi actualizează Procedurile Operaţionale de Securitate;

b) monitorizează permanent toate aspectele de securitate specifice SIC;

c) participă la elaborarea şi actualizarea documentelor „Cerinţele de Securitate Specifice", „Cerinţele de Securitate Comune", „Cerinţele de Securitate Specifice pentru Protecţia Informaţiilor în Format Electronic într-un SIC" pentru sistemele de care răspunde;

d) actualizează şi ţine evidenţa tuturor utilizatorilor autorizaţi;

e) aplică măsurile adecvate de control al accesului la SIC respectiv;

f) verifică elementele de identificare a utilizatorilor,

g) asigură evidenţa evenimentelor legate de securitatea sistemului şi a sesiunilor de lucru;

h) evaluează implicaţiile, în planul securităţii, privind modificările software, hardware, firmware şi procedurale propuse pentru SIC;

i) verifică dacă modificările de configuraţie a SIC afectează securitatea şi dispune măsurile în consecinţă;

j) verifică dacă personalul cu acces autorizat la SIC cunoaşte responsabilităţile care revin în domeniul protecţiei informaţiilor;

k) verifică modul de executare a întreţinerii şi actualizării software-ului pentru a nu se periclita securitatea sistemului;

l) asigură un control riguros al mediilor de stocare a informaţiilor şi documentaţiei sistemului, verificând concordanţa între clasa sau nivelul de secretizare a informaţiilor stocate şi marcajul de secretizare al mediilor de stocare;

m) ia măsuri tehnice şi organizatorice pentru protecţia mediilor de stocare a informaţiilor faţă de câmpurile electromagnetice şi accesul neautorizat la informaţiile clasificate;

n) execută controale privind modul de utilizare a mediilor de stocare a informaţiilor;

o) asigură păstrarea şi consultarea documentaţiei şi a datelor de evidenţă şi control, referitoare la securitate, în conformitate cu PrOpSec;

p) stabileşte proceduri de verificare pentru utilizarea în SIC numai a software-ului autorizat;

q) asigură, împreună cu administratorul de sistem/reţea, aplicarea celor mai eficiente proceduri de creare a copiilor de rezervă şi de recuperare software;

r) asigură instruirea şi pregătirea corespunzătoare a administratorilor de securitate în zona terminalelor izolate;

s) raportează şefului CSTIC orice breşe de securitate, vulnerabilităţi şi încălcări ale măsurilor de securitate.

3. În calitate de administrator COMSEC îndeplineşte următoarele atribuţii principale:

a) verifică şi răspunde de instalarea echipamentelor SIC folosite în transmiterea informaţiilor clasificate în conformitate cu cerinţele COMSEC;

b) verifică şi răspunde de aplicarea în mod corespunzător a măsurilor de securitate a emisiilor EMSEC şi a transmisiilor-TRANSEC;

c) ţine evidenţa echipamentelor şi sistemelor folosite la transmiterea informaţiilor clasificate.

4. În calitate de administrator TRANSEC îndeplineşte următoarele atribuţii principale:

a) asigură implementarea procedurilor de securitate şi eficacitatea măsurilor de securitate a transmisiilor, în timpul testării SIC, precum şi pe durata desfăşurării exerciţiilor şi aplicaţiilor;

b) coordonează elaborarea programelor TRANSEC;

c) elaborează, verifică şi aprobă rapoarte TRANSEC;

d) prezintă probleme de specialitate în cadrul şedinţelor de pregătire pe tema vulnerabilităţii unui sistem de comunicaţii deschis, neprotejat şi pe alte teme TRANSEC.

5. În calitate de administrator EMSEC îndeplineşte următoarele atribuţii principale:

a) asigură măsurile tehnice de instalare a echipamentelor din SIC, în conformitate cu cerinţele de securitate stabilite;

b) supraveghează ca executarea întreţinerilor şi modificările aduse echipamentelor protejate TEMPEST să se execute de personal calificat utilizându-se numai piese de schimb şi componente avizate de şeful INFOSEC şi aprobate de funcţionarul de securitate M.A.I.;

c) solicită efectuarea controalelor periodice pe linie de TEMPEST sau când apar premise de scurgere a informaţiilor prin radiaţii electromagnetice compromiţătoare.

6. În calitate de custode cripto îndeplineşte următoarele atribuţii principale:

a) ţine evidenţa sistemelor criptografice deţinute de CSTIC din structura/unitatea din care face parte;

b) distribuie materialele criptografice numai persoanelor autorizate;

c) solicită asigurarea cu echipamente şi materiale criptografice necesare funcţionării sistemului de asigurare a protecţiei informaţiilor clasificate;

d) distruge materialele criptografice, în conformitate cu prevederile legale în vigoare;

e) raportează administratorului COMSEC şi şefului CSTIC toate aspectele de insecuritate legate de gestionarea sistemelor criptografice.

7. În calitate de ADMINISTRATOR DE SECURITATE LOCAL al componentei distante a SIC ICC are următoarele responsabilităţi:

a) elaborează Procedurile Operaţionale de Securitate de la nivelul punctului de prezenţă al SIC ICC de la nivelul Instituţiei Prefectului-Judeţul Dolj, în concordanţă cu modelul prezentat în Anexa 18 a PrOpSec ale SIC ICC;

b) cooperează cu administratorul de securitate al SIC ICC cu privire la toate aspectele conexe asigurării securităţii componentei distante a sistemului;

c) aplică măsurile cuprinse în Programul de prevenire a scurgerii de informaţii clasificate al Instituţiei Prefectului-Judeţul Dolj, referitoare la managementul securităţii componentei distante a SIC ICC;

d) elaborează şi actualizează lista utilizatorilor PP a SIC ICC;

e) informează şeful structurii de securitate din cadrul Instituţiei Prefectului-Judeţul Dolj şi pe administratorul de securitate al SIC cu privire la indiciile referitoare la încălcarea măsurilor protective instituite, sau a oricăror încercări de compromitere a confidenţialităţii, integrităţii sau disponibilităţii informaţiilor vehiculate în SIC ICC;

f) asigură corecta aplicare a măsurilor de securitate fizică şi buna funcţionare a acestora la nivelul locaţiilor proprii în care sunt dispuse resursele SIC;

g) asigură controlul periodic al integrităţii sigiliilor de securitate aferente resurselor componentei distante a SIC ICC;

h) aplică măsurile de control al accesului în locaţia componentei distante a SIC ICC, potrivit Programului de prevenire a scurgerii de informaţii clasificate al Instituţiei Prefectului-Judeţul Dolj şi Procedurilor Operaţionale de Securitate de la nivelul punctului de prezenţă al SIC ICC din cadrul Instituţiei Prefectului-Judeţul Dolj;

i) asigură instruirea şi pregătirea utilizatorilor PP a SIC ICC în domeniul protecţiei informaţiilor clasificate naţionale;

j) asigură evidenţa şi actualizarea fişelor de pregătire individuală a utilizatorilor componentei distante a SIC ICC;

k) primeşte cererile de vizitare a componentei distante a SIC ICC coordonând toate activităţile aferente;

l) asigură instruirea şi pregătirea utilizatorilor terminalului distant al SIC privind securitatea informaţiilor, resurselor şi serviciilor sistemului;

m) asigură reluarea semestrială a procesului de analiză de risc la nivelul componentei distante a SIC, rezultatele urmând a fi transmise AOSIC;

n) coordonează activităţile legate de accesul în locaţia componentei distante a SIC ICC;

o) informează în cel mai scurt timp pe administratorul de securitate al SIC cu privire la orice eveniment tehnic sau incident de securitate care afectează, sau este posibil a afecta, securitatea SIC ICC;

p) asigură implementarea și menținerea măsurilor de securitate fizică în locație;

q) primește cererile de vizitare a SIC ICC PP;

r) coordonează împreună cu administratorul de securitate al obiectivului PP al Instituției Prefectului-Județul Dolj activitățile legate de vizitarea locației;

s) supraveghează realizarea oricăror modificări ale securității fizice a mediului global de securitate (MGS) pentru a se asigura că acestea nu afectează securitatea SIC;

t) asigură verificarea periodică a modului de acțiune a personalului desemnat pentru situații de urgență;

u) coordonează verificarea periodică a implementării măsurilor de securitate INFOSEC;

v) notifică, imediat, SII MAI din cadrul DGPI, în vederea comunicării către SRI, cu privire la orice eveniment informatic sau incident de securitate survenit sau care este posibil a avea loc;

w) participă la investigarea cazurilor de încălcare a securității sau a încercărilor de încălcare a securității SIC ICC

8. În calitate de CUSTODE CRIPTO al SIC ICC are următoarele responsabilităţi:

a) primeşte în custodie materialul criptografic utilizat în activitatea specifică SIC, ţine evidenţa acestuia şi îi asigură securitatea;

b) asigură utilizarea corespunzătoare a mecanismelor de protecţie criptografică implementate în SIC ICC;

c) respectă întocmai procedurile de securitate criptografică cu privire la primirea, păstrarea şi utilizarea în siguranţă, precum şi returnarea sau distrugerea materialului criptografic utilizat în SIC ICC;

d) execută recepţia, păstrarea, returnarea, ambalarea coletelor ce conţin material criptografic şi asigură securitatea acestora în perioada cât le deţine;

e) asigură relaţionarea cu personalul cu responsabilităţi în administrarea SIC, actualizează şi comunică administratorului CRIPTO lista personalului cu responsabilităţi în administrarea echipamentelor criptografice utilizate în cadrul SIC, în locaţia proprie;

f) notifică administratorul de Securitate local cu privire la incidentele de securitate sau defectele constatate la nivelul echipamentelor criptografice ale SIC ICC;

g) sprijină administratorul CRIPTO sau administratorul COMSEC, în vederea remedierii defectelor hardware semnalate sau pentru efectuarea schimbărilor, modificărilor şi actualizărilor de firmware la nivelul echipamentelor criptografice ale SIC;

h) ţine evidenţa schimbărilor, modificărilor firmware, precum şi a defectelor hardware la nivelul produselor criptografice ale SIC;

i) participă la inventarierea periodică a materialului criptografic aflat în custodie;

j) informează, imediat, administratorul de securitate al SIC despre orice circumstanţe, suspiciuni, cazuri sau acţiuni intenţionate sau din neglijenţă care pot conduce la divulgarea sau diseminarea materialului criptografic către persoane neautorizate;

k) participă la formele de pregătire în domeniul protecţiei materialului criptografic organizate de administratorul CRIPTO local.

9. Administrează, întreține și extinde sistemul de supraveghere video din instituție

Coordonate de contact pentru primirea dosarelor de concurs: dosarele de concurs se depun la sediul Instituției Prefectului Județului Dolj din Str. Amaradia, nr. 93-95 Municipiul Craiova, județul Dolj, telefon 0251416703, interior 29050, fax: 0251411210, e-mail office@prefecturadolj.ro, persoana de contact: Lupu Daniela, expert, clasa I, grad profesional superior în cadrul Compartimentului Resurse Umane.

Sef Serviciu CRUAAI,
Vana Doina Maria

Intocmit,
Lupu Daniela