

ROMÂNIA  
MINISTERUL AFACERILOR INTERNE  
INSPECTORATUL GENERAL AL POLIȚIEI ROMÂNE  
COMISIA CENTRALĂ DE CONCURS / COMISIA DE CONCURS

- Sesiunea martie 2018 -



TEST SCRIS

LA SPECIALITATEA:

STRUCTURA DE SECURITATE – C.S.T.I.C.

Pentru fiecare întrebare a testului scris sunt prevăzute 3 variante de răspuns, notate cu litera a, b și c. Dintre aceste trei variante **una și numai una singură** reprezintă răspunsul corect.

Marcați cu semnul “X” pe *Foaia de răspuns* în căsuța din dreptul numărului întrebării și a literei corespunzătoare pe care o considerați că indică răspunsul corect. Nu faceți nicio însemnare în celelalte două spații libere din dreptul întrebării.

*Exemplu:*

Nr. întreb.	a	b	c
1	X		
2			X

Dacă la corectare se constată că sunt înscrise mai multe semne de “X” în dreptul unei întrebări, răspunsul la întrebarea respectivă nu este luat în considerare (este anulat).

De asemenea, pe *Foaia de răspuns* nu sunt admise hașurări, ștersături, adăugiri, completări, mențiuni făcute pe marginea foii de răspuns având ca scop indicarea răspunsului corect sau orice alte însemnări care pot produce confuzie în apreciere. La verificarea corectitudinii răspunsurilor, existența acestor situații atrage anularea răspunsului respectiv, indiferent dacă printre însemnările făcute este marcat și răspunsul corect.

1. Autorizația de acces la informații clasificate secrete de serviciu este emisă de:
  - a. Conducătorul unității;
  - b. Autoritatea Desemnată de Securitate;
  - c. Oficiul Registrului Național pentru Informații Secrete de Stat.
2. Potrivit Legii nr.360/2002 privind Statutul Polițistului, cu modificările și completările ulterioare, constituie recompense ce pot fi acordate polițiștilor următoarele:
  - a. Amânarea aplicării unei sancțiuni disciplinare;
  - b. Premii în bani sau obiecte, atunci când s-a evidențiat prin obținerea de rezultate exemplare în activitate;
  - c. Acordarea de permisii până la cinci zile lucrătoare.
3. Care dintre următoarele variante reprezintă un drept al polițistului:
  - a. ajutoare și alte drepturi bănești, ale căror cuantumuri se stabilesc de șeful direct la propunerea șefului nemijlocit;
  - b. locuință de intervenție, de serviciu, socială sau de protocol, după caz, în condițiile legii;
  - c. indemnizații de instalare, de mutare, de delegare sau de detașare, precum și decontarea cheltuielilor de cazare, în condițiile stabilite prin lege.

4. Constituie sancțiune disciplinară ce poate fi aplicată polițiștilor:
- Reținerea din salariul lunar în quantum de 30% din acesta;
  - Amânarea promovării în grade profesionale sau funcții superioare pe o perioadă de 1-5 ani;
  - Destituirea din poliție.
5. Poate constitui abatere disciplinară:
- Întârzierea repetată sau nejustificată a soluționării lucrărilor;
  - Absența motivată în mod repetat de la serviciu;
  - Neîndeplinirea baremelor privind evaluările sportive anuale.
6. Încetarea raporturilor de serviciu ale polițistului are loc conform prevederilor legale:
- Prin demisie;
  - Prin dispoziția șefului nemijlocit;
  - La acordarea calificativului nesatisfăcător, de trei ori.
7. Care este nivelul maxim de clasificare al informațiilor care pot fi gestionate într-o zonă de securitate clasa I:
- strict secret;
  - strict secret de importanță deosebită;
  - secret.
8. Care este nivelul minim de autorizare necesar persoanelor care accesează o zonă de securitate clasa I:
- strict secret;
  - strict secret de importanță deosebită;
  - secret.
9. În funcție de importanța valorilor protejate în raport cu eventualul prejudiciu pe care divulgarea neautorizată îl poate cauza siguranței naționale și apărării țării, informațiile sunt încadrate pe următoarele niveluri:
- Secret de serviciu, secret, strict secret și strict secret de importanță deosebită;
  - Secret și strict secret;
  - Secret, strict secret și strict secret de importanță deosebită.
10. În modelul de referință OSI, nivelul Transport are următorul rol principal:
- Se ocupă numai de transferul bițiilor dintr-un loc în altul;
  - Permite utilizatorilor de pe mașini diferite să stabilească între ei conexiuni;
  - Acceptă date de la nivelul sesiune, le descompune dacă este cazul în unități mai mici, transferă aceste unități nivelului rețea și se asigură că toate fragmentele sosesc corect la celălalt capăt.
11. Care este diferența principală între *Ping* și *Tracert*:
- Ping* timite o succesiune de pachete ping, iar *Tracert* trimite un singur pachet ping;
  - Ping* timite un singur pachet ping, iar *Tracert* trimite o succesiune de pachete ping pentru a descoperi topologia rețelei;
  - Tracert* poate fi rulat doar de administratori.

12. Pentru a schimba conexiunile de rețea trebuie:
- Să se utilizeze comanda *Advanced Settings* din fereastra Network and Dial-Up Connections;
  - Să se modifice manual regiștrii;
  - Să se eliminate și să se reinstaleze protocoalele afectate.
13. Dacă se dorește verificarea conectivității de rețea între două calculatoare se folosește:
- Comanda *Ping*;
  - Ipcfg*;
  - Ipcfg/all*.
14. Scopul principal al DHCP este:
- automatizarea înregistrării numelor DNS;
  - livrarea automată a informațiilor de adresă IP clienților;
  - să permită mutarea traficului WINS.
15. Ce se verifică mai întâi atunci când se depanează o problemă în rețea?
- Configurația DNS;
  - Configurația TCP/IP;
  - Conecțivitatea fizică.
16. Informațiile se declasifică dacă:
- Acest lucru este solicitat expres de către organele de urmărire penală;
  - Dezvăluirea lor nu mai aduce atingere datelor cu caracter personal;
  - Dezvăluirea informațiilor nu mai poate prejudicia siguranța națională, apărarea țării, ordinea publică, ori interesele persoanelor de drept public sau privat deținătoare.
17. Declasificarea sau trecerea la un alt nivel de secretizare a informațiilor secrete de stat se realizează:
- De către deținător la solicitarea oricărei persoane fizice sau juridice;
  - De către împuterniciții și funcționarii superiori abilitați prin lege să atribuie niveluri de secretizare, cu avizul prealabil al instituțiilor care coordonează activitatea și controlul măsurilor privitoare la protecția informațiilor clasificate, potrivit competențelor materiale;
  - Prin decizie a instituțiilor care coordonează activitatea și controlul măsurilor privitoare la protecția informațiilor clasificate, potrivit competențelor materiale.
18. La stabilirea măsurilor de protecție a informațiilor clasificate vor fi avute în vedere și:
- Volumul și suportul informațiilor;
  - Forma de organizare din punct de vedere structural al unității deținătoare de informații clasificate;
  - Posibilitățile logistice ale unității.
19. Care dintre următoarele nu este o metodă de autentificare IPSec:
- autentificare NTLM;
  - prin certificate;
  - Kerberos.
20. Se dorește să se verifice ce IPSec este activ pe un calculator. Ce trebuie să se utilizeze pentru aceasta?
- Instrumentul *ipsecmon*;
  - Instrumentul *ipconfig*;
  - Caseta de dialog IP Security Properties.

21. Nivelul de secretizare se marchează pe prima pagină a documentelor conținând informații clasificate:
- Sub legendă, titlu sau scara de reprezentare;
  - În partea de jos și de sus, la mijlocul paginii;
  - În partea dreaptă sus și jos.
22. Atribuirea aceluiași număr de înregistrare unor documente cu conținut diferit:
- Este posibilă cu aprobarea conducătorului unității și consemnarea în registrul special constituit;
  - Este interzisă;
  - Este permisă doar cu aprobarea conducătorului unității și avizul autorității desemnate de securitate.
23. Multiplicarea documentelor clasificate poate fi realizată de către:
- persoane autorizate, cu aprobarea conducătorului unității;
  - persoane autorizate, doar conform cererii de multiplicare aprobată de structura/funcționarul de securitate;
  - persoane autorizate, numai în încăperi special destinate, cu aprobarea conducătorului unității și cu avizul structurii/funcționarului de securitate, ambele înscrise pe cererea de multiplicare sau pe adresa de însoțire în care se menționează necesitatea multiplicării.
24. Anexele unui document clasificat se clasifică:
- În funcție de conținutul propriu;
  - În strictă concordanță cu documentul de bază;
  - În funcție de necesitatea de diseminare.
25. Care este perioada maximă de valabilitate a certificatului/ autorizației de acces la informații clasificate:
- 2 ani;
  - 3 ani;
  - 4 ani.
26. În fiecare unitate care administrează SPAD și RTD - SIC în care se stochează, se procesează sau se transmit informații clasificate, se va institui o componentă de securitate pentru tehnologia informației și a comunicațiilor - CSTIC, în subordinea:
- Structurii/funcționarului de securitate;
  - Şefului unității;
  - ORNISS.
27. Care sunt modurile de operare ale SPAD și RTD - SIC care stochează, procesează sau transmit informații clasificate:
- nivel scăzut;
  - nivel înalt;
  - nivel mediu.
28. Mediile de stocare care conțin informații clasificate strict secrete de importanță deosebită, după ieșirea din uz, trebuie să fie:
- declasificate;
  - refolosite pentru gestionarea informațiilor clasificate secret de serviciu, doar în urma suprascrieri;
  - distruse.

29. Înainte de a fi utilizate pentru stocarea, procesarea sau transmiterea informațiilor clasificate, toate SPAD și RTD – SIC trebuie să fie:
- Acreditate de către Agenția de Acreditare de Securitate;
  - Formatate de către formațiunea de comunicații și informatică;
  - Suprascrise de către Structura de Securitate.
30. Care este persoana competentă să aprobe introducerea mediilor de stocare amovibile, a software-ului și a hardware-ului aflate în proprietate privată, în zonele în care se stochează, se procesează sau să transmită informații clasificate?
- Şeful Structurii de Securitate/Funcționarul de securitate;
  - Conducătorul unității;
  - Administratorul de securitate.
31. Administratorul de securitate al rețelei pentru un SIC de mari dimensiuni sau în cazul interconectării mai multor SPAD, este desemnat de:
- Formațiunea de comunicații și informatică;
  - Componența de Securitate pentru Tehnologia Informației și Comunicațiilor;
  - Unitatea specializată din cadrul Direcției Generale de Protecție Internă.
32. Zona de securitate clasa a II-a necesită:
- perimetru clar determinat și protejat, în care toate intrările și ieșirile sunt supravegheate;
  - controlul sistemului de intrare, care să permită numai accesul persoanelor verificate corespunzător și autorizate în mod special;
  - indicarea existenței registrului de evidență a informațiilor secrete de serviciu existente în zonă.
33. Măsurile de protecție a personalului au drept scop:
- să prevină accesul persoanelor neautorizate la informații publice;
  - să garanteze că informațiile secrete de stat sunt distribuite deținătorilor de certificate de securitate/autorizații de acces, cu respectarea principiului necesității de a cunoaște;
  - să permită identificarea procedurilor care pot pune în pericol securitatea informațiilor clasificate.
34. Modul de operare în care toate persoanele cu drept de acces la SIC au certificat de securitate/autorizație de acces la informații clasificate pentru cel mai înalt nivel de secretizare a informațiilor stocate, procesate sau transmise în SIC, dar accesul la informații se face diferențiat, conform principiului „necesitatea de a cunoaște”, este modul:
- nivel dedicat;
  - de nivel scăzut;
  - de nivel înalt.
35. Pentru securitate care dintre următoarele sisteme de fișiere sunt recomandate pentru toate partiiile unui controlor de domeniu:
- FAT;
  - FAT32;
  - NTFS.

36. La câte domenii poate fi membru la un moment dat, un controlor de domeniu:
- 0;
  - 1;
  - Orice număr de domenii.
37. Care dintre următoarele pictograme de pe desktop pot fi folosite pentru utilizarea altor calculatoare din rețea?
- Internet Explorer;
  - My Network Places;
  - Briefcase.
38. Care dintre următoarele componente Active Directory joacă un rol în alocarea numelui în cadrul DNS:
- Domeniile (Domains);
  - Unitățile Organizaționale (OU);
  - Grupurile (Groups).
39. Retragerea autorizației de acces la informații secrete de serviciu se face de către conducătorul unității în cazul:
- Căsătoriei sau divorțului persoanei, după caz;
  - La solicitarea Oficiului Registrului Național pentru Informații Secrete de Stat;
  - Când deținătorul autorizației a încălcă reglementările privind protecția informațiilor secrete de serviciu.
40. Transportul corespondenței clasificate secret de stat, se realizează pe teritoriul României prin:
- Personal propriu al unităților de poliție;
  - Prin intermediul unității specializate a Serviciului Roman de Informații;
  - Prin serviciul specializat al S.N. Poșta Română.
41. Distrugerea ciornelor neînregistrate care au stat la baza întocmirii documentelor clasificate secrete de stat se realizează:
- De către personalul care le-a creat pe bază de proces – verbal avizat de șeful Structurii de Securitate/funcționarul de securitate și aprobat de conducătorul unității;
  - De către compartimentul documente clasificate și secretariat al unității pe bază de proces – verbal avizat de șeful Structurii de Securitate/funcționarul de securitate și aprobat de conducătorul unității;
  - De către persoanele care le-au creat.
42. Informațiile strict secrete de importanță deosebită vor fi distruse:
- La expirarea termenului de păstrare indicat de emitent, doar cu acordul acestuia și se consemnează într-un proces – verbal avizat de șeful Structurii de Securitate/funcționarul de securitate și aprobat de conducătorul unității;
  - De către emitent, după restituirea acestora, urmând ca activitatea să fie consemnată într-un proces – verbal avizat de șeful Structurii de Securitate/funcționarul de securitate și aprobat de conducătorul unității;
  - De către emitent, doar după propunerea de desecretizare cu avizul Autorității Desemnate de Securitate.

43. Normele interne de aplicare a măsurilor privind protectia informațiilor clasificate se aprobă:
- De conducătorul unității cu avizul Autorității Desemnate de Securitate;
  - De către Autoritatea Desemnată de Securitate la propunerea conducătorului unității deținătoare de informații clasificate;
  - De către conducătorul unității deținătoare de informații clasificate.
44. Fotografierea, filmarea, cartografierea sau executarea de lucrări de arte plastice în zonele de securitate și administrative ale unităților deținătoare de secrete de stat este permisă:
- Cu aprobarea scrisă a împoternicișilor abilități să atribuie niveluri de secretizare conform art. 19 din Legea 182/2002, potrivit competențelor materiale;
  - Cu aprobarea scrisă a șefului Structurii de Securitate/funcționarul de securitate și a conducătorului unității;
  - Cu avizul prealabil al Autorității Desemnate de Securitate și aprobarea conducătorului unității deținătoare de informații clasificate, în condițiile stipulate de art. 19 din Legea 182/2002, potrivit competențelor materiale.
45. Polițistul are dreptul, conform celor statuate prin Legea nr. 218/2002 privind organizarea și funcționarea Poliției Române, cu modificările și completările ulterioare (republicată):
- Să poarte armamentul din dotare la vedere, în interesul serviciului și propriu, pentru descurajarea unor acte de ultraj;
  - Să folosească gratuit, pe baza legitimației de serviciu, mijloacele de transport în comun în timpul serviciului pentru executarea unor misiuni;
  - Să utilizeze mijloacele de transport aerian, feroviar și rutier ale companiilor naționale pentru deplasări pe distanțe mari, cu decontarea la nivelul unității.
46. Care dintre următoarele operații nu se pot face prin intermediul utilitarului Active Directory Users and Computers:
- Redenumirea unui obiect de tip calculator;
  - Crearea unui obiect de tip utilizator;
  - Redenumirea unui obiect de tip utilizator.
47. Restricționarea afișării anumitor tipuri de obiecte din cadrul utilitarului Active Directory Users and Computers, este cunoscută sub numele:
- Filtering;
  - Restriction;
  - Excluding.
48. Care dintre următoarele nu este o categorie implicită de obiecte ale Active Directory în caseta de dialog *Find*:
- Organizational Units;
  - Users, Contacts and Groups;
  - Servers and Domain Controllers.
49. Un utilizator are probleme în a folosi un Shared Folder (un folder partajat) localizat într-o anume unitate organizațională și vrea să știe pe cine să contacteze pentru a rezolva această situație. O bună modalitate de a face acest lucru este să:
- Execute clic-dreapta pe obiectul Shared Folder și apoi să selecteze Contacts;
  - Execute clic-dreapta pe obiectul Shared Folder și apoi să selecteze Notify Operator;
  - Execute clic-dreapta pe obiectul Shared Folder și apoi să selecteze Properties. În cadrul tab-ului Managed By va găsi informația necesară.

50. Acțiunile în forță desfășurate de poliție trebuie subordonate principiilor:
- Oportunității, priorității și proporționalitate;
  - Necesității, gradualitate și proporționalitate;
  - Legalitate, oportunității și demnității.
51. Polițistul trebuie să acorde sprijin, conform competențelor legale, victimelor infracțiunilor atunci când:
- Intră în contact cu acestea pe timpul și în afara îndeplinirii atribuțiilor de serviciu;
  - Este solicitat doar pe timpul îndeplinirii atribuțiilor de serviciu;
  - Când sesizează incapacitatea acestora de a se proteja, în timpul îndeplinirii atribuțiilor de serviciu.
52. Atenționarea polițistului se dispune pentru prevenirea săvârșirii de abateri disciplinare și reprezintă:
- O primă sancțiune disciplinară;
  - O măsură cu caracter administrativ-preventiv;
  - O măsură complementară sancțiunii disciplinare.
53. Datele cu caracter personal destinate a face obiectul prelucrării trebuie să fie:
- Reale și furnizate direct de către persoanele fizice;
  - Adequate, pertinente și neexcesive prin raportare la scopul în care sunt colectate și ulterior prelucrate;
  - Păstrate în formă clasificată.
54. Polițistul care deține gradul de subcomisar de poliție poate fi avansat la împlinirea stagiului minim în grad, respectiv:
- 2 ani;
  - 3 ani;
  - 4 ani.
55. Avansarea polițiștilor la gradul profesional de chestor de poliție este efectuată de către:
- Președintele României;
  - Ministrul Afacerilor Interne;
  - Inspectorul General al Poliției Române.
56. Autoritatea de supraveghere, în sensul Legii nr.677/2001, este:
- Autoritatea Desemnată de Securitate;
  - Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal;
  - Oficiul Registrului Național pentru Informații Secrete de Stat.
57. Este interzisă utilizarea mediilor de stocare amovibile, a software-ului și a hardware-ului, aflate în proprietate privată, pentru stocarea, procesarea și transmiterea informațiilor:
- Secret de serviciu și secret;
  - Secrete de Stat;
  - Secret de serviciu și strict secret.
58. Utilizarea într-un obiectiv a echipamentelor și a software-ului contractanților, pentru stocarea, procesarea sau transmiterea informațiilor clasificate este permisă:
- Numai cu avizul conducerii unității;
  - Cu avizul personalului specializat din cadrul structurilor de comunicații și informatică;
  - Numai cu avizul CSTIC și aprobarea șefului unității.

59. Ce trebuie să existe înainte de a stabili o conexiune VPN?
- O conexiune IPSec;
  - Un set de dovezi VPN;
  - O conexiune LAN.
60. În funcție de obiectivele urmărite, controalele asupra măsurilor privitoare la protecția informațiilor clasificate pot fi:
- De fond, inopinate și impuse de situații de urgență;
  - De fond, punctuale și de securitate;
  - Tematice, de specialitate și de securitate.

NOTE:

- ✓ Timpul alocat rezolvării este de 3 ore (180 de minute);
- ✓ Răspunsurile se completează pe *Foaia de răspuns*;
- ✓ Fiecare răspuns corect este apreciat cu 0,15 puncte. Punctajul maxim care poate fi obținut este 9 puncte;
- ✓ Se acordă un punct din oficiu;
- ✓ Aprecierea testului se face prin însumarea punctajului cu punctul din oficiu, obținându-se nota.

