MONITORUL OFICIAL AL ROMÂNIEI

Anul 182 (XXVI) — Nr. 242

PARTEA I
LEGI, DECRETE, HOTĂRÂRI ȘI ALTE ACTE

Vineri, 4 aprilie 2014

SUMAR

ACTE ALE ORGANELOR DE SPECIALITATE ALE ADMINISTRAȚIEI PUBLICE CENTRALE

GUVERNUL ROMÂNIEI
OFICIUL REGISTRULUI NAȚIONAL AL INFORMAȚIILOR SECRETE DE STAT

ORDIN
pentru aprobarea Ghidului privind structura și conținutul Procedurilor Operaționale de Securitate (PrOpSec) pentru sisteme informatice și de comunicații — DS 2

În temeiul:

— art. 1 alin. (4) lit. b) și art. 3 alin. (6) din Ordonanța de urgență a Guvernului nr. 153/2002 privind organizarea și funcționarea Oficiului Registrului Național al Informațiilor Secrete de Stat, aprobată prin Legea nr. 101/2003, cu modificările și completările ulterioare;

— art. 55 alin. (1) din Regulamentul privind procedurile, la nivelul Guvernului, pentru elaborarea, avizarea și prezentarea proiectelor de documente de politici publice, a proiectelor de acte normative, precum și a altor documente, în vederea adoptării/aprobării, aprobat prin Hotărârea Guvernului nr. 561/2009,

directorul general al Oficiului Registrului Național al Informațiilor Secrete de Stat emite prezentul ordin.

Art. 1. — Se aprobă Ghidul privind structura și conținutul Procedurilor Operaționale de Securitate (PrOpSec) pentru sisteme informatice și de comunicații — DS 2, prevăzut în anexa care face parte integrantă din prezentul ordin.

Art. 2. — La data intrării în vigoare a prezentului ordin se abrogă Ordinul directorului general al Oficiului Registrului Național al Informațiilor Secrete de Stat nr. 489/2003 pentru aprobarea Ghidului privind structura și conținutul Procedurilor Operaționale de Securitate (PrOpSec) pentru sisteme informatice și de comunicații (SIC) — DS 2, publicat în Monitorul Oficial al României, Partea I, nr. 866 din 5 decembrie 2003.

Art. 3. — Prezentul ordin se publică în Monitorul Oficial al României, Partea I.

Art. 4. — Oficiul Registrului Național al Informațiilor Secrete de Stat va duce la îndeplinire prevederile prezentului ordin.

Directorul general al Oficiului Registrului Național al Informațiilor Secrete de Stat,
Marius Petrescu

București, 21 martie 2014.
Nr. 18.

ANEXĂ

GHID
privind structura și conținutul Procedurilor Operaționale de Securitate (PrOpSec) pentru sisteme informatice și de comunicații — DS 2

CAPITOLUL I
Introducere

Art. 1. — Ghidul privind structura și conținutul Procedurilor Operaționale de Securitate (*PrOpSec*) pentru sisteme informatice și de comunicații — DS 2, denumit în continuare *ghid*, este elaborat în concordanță cu reglementările naționale privind protecția informațiilor clasificate și se adresează Agenției de Acreditare de Securitate (*AAS*) din cadrul Oficiului Registrului Național al Informațiilor Secrete de Stat (*ORNISS*), structurilor interne INFOSEC (*SII*) acreditate în cadrul autorităților desemnate de securitate (*ADS*) și autorităților operaționale ale sistemului informatic și de comunicații (*AOSIC*) care stochează, procesează sau transmit informații clasificate.

Art. 2. — Întocmirea PrOpSec este obligatorie pentru toate sistemele informatice și de comunicații (*SIC*) supuse procesului de acreditare de securitate, conform prevederilor Directivei privind managementul INFOSEC pentru sisteme informatice și de comunicații — INFOSEC 3, aprobată prin Ordinul directorului general al Oficiului Registrului Național al Informațiilor Secrete de Stat nr. 484/2003, denumită în continuare *INFOSEC 3*.

Art. 3. — (1) PrOpSec reprezintă descrierea precisă a implementării cerințelor de securitate definite anterior în documentațiile cu cerințele de securitate (*DCS*), a procedurilor operaționale care vor trebui urmate și a responsabilităților personalului, specifice SIC.

(2) PrOpSec se dezvoltă pe măsura elaborării și actualizării DCS și se finalizează după aprobarea DCS de către AAS.

(3) AAS aprobă forma finală a PrOpSec.

Art. 4. — Prezentul ghid stabilește structura și conținutul PrOpSec pentru următoarele categorii de personal și mod de utilizare:

a) pentru utilizatorii rețelelor locale de calculatoare (*LAN*);

b) pentru utilizatorii dispozitivelor portabile de calcul și de comunicații care vehiculează informații clasificate, în cadrul misiunilor oficiale;

c) pentru utilizarea dispozitivelor de calcul și de comunicații de către vizitatori;

d) pentru AOSIC.

CAPITOLUL II
Domeniu de aplicare

Art. 5. — (1) Potrivit prevederilor INFOSEC 3, SIC care urmează să stocheze, să proceseze sau să transmită informații naționale clasificate cu nivel de clasificare SECRET și superior sau echivalent trebuie supuse unui proces de acreditare de securitate.

(2) Acreditarea de securitate trebuie obținută și pentru SIC care stochează, procesează sau transmit informații cu nivel de clasificare maxim NATO RESTRICTED sau RESTREINT UE/EU RESTRICTED.

(3) Pentru sistemele prevăzute la alin. (1) și (2), stocarea, procesarea sau transmiterea informațiilor clasificate trebuie să fie realizate în conformitate cu prevederile PrOpSec.

(4) Suplimentar, AAS poate solicita ca PrOpSec să fie întocmite și pentru SIC care stochează, procesează sau transmit informații neclasificate, dar care poartă marcaje administrative sau de limitare a diseminării și care sunt interconectate cu alte SIC ori cu rețele publice.

(5) Documentul cu cerințele de securitate specifice sistemului (*CSSS*) elaborat pentru SIC constituie baza pentru elaborarea PrOpSec.

CAPITOLUL III
Structura PrOpSec

Art. 6. — (1) PrOpSec au structura prezentată în tabelul de mai jos, în funcție de particularitățile relevante ale fiecărui SIC.

(2) Dacă se consideră necesar, fiecare capitol poate fi întocmit și utilizat ca document de sine stătător pentru grupuri specifice de utilizatori sau administratori, pentru locații distribuite în cadrul unui SIC sau pentru folosirea de către utilizatori în misiuni a echipamentelor de calcul portabile.

Capitolul 1	Administrarea și organizarea securității
Capitolul 2	Securitatea fizică
Capitolul 3	Securitatea personalului
Capitolul 4	Securitatea informațiilor
Capitolul 5	Securitatea SIC Securitatea calculatoarelor Securitatea criptografică Securitatea emisiilor Securitatea transmisiilor
Capitolul 6	Planificarea măsurilor pentru situații de urgență și pentru continuarea activității
Capitolul 7	Managementul configurației
Capitolul 8	Proceduri operaționale asociate

(3) Conținutul fiecărui capitol poate varia în funcție de caracteristicile specifice SIC.

(4) Prezentul ghid intenționează să furnizeze o listă de verificare a tuturor aspectelor care trebuie luate în considerare. Este posibil ca în unele capitole ale PrOpSec să fie făcute doar referiri la unele documente deja întocmite pentru SIC, astfel încât să nu se repete conținutul acestora în PrOpSec. În plus, extrase din PrOpSec pot fi incluse în conținutul unor proceduri standard de operare care pot fi elaborate pentru o instituție. În cazul în care problemele de aplicabilitate și de detaliu necesită luarea unei decizii de modificare sau interpretare, trebuie consultată AAS.

(5) PrOpSec se referă strict la aspecte privind securitatea SIC. Alte considerații sau proceduri trebuie formulate într-un alt document de sine stătător sau într-o anexă a PrOpSec.

(6) PrOpSec sunt formulate în așa fel încât să permită clasificarea acestui document cu nivel de clasificare redus. Dacă este necesar, se pot întocmi mai multe anexe la PrOpSec (sau un document suplimentar) care pot avea un nivel de clasificare superior, în acest caz accesul la documentul cu PrOpSec fiind limitat conform principiului „nevoii de a cunoaște”.

CAPITOLUL IV
Conținutul PrOpSec pentru utilizatorii rețelelor locale (LAN)

Art. 7. — (1) Prezentul capitol stabilește elementele componente ale PrOpSec pentru utilizatorii rețelelor locale de calculatoare (LAN).

(2) PrOpSec trebuie să fie concise și formulate astfel încât să fie ușor de înțeles de către utilizatori.

Administrarea și organizarea societății

Art. 8. — (1) Cap. 1 „Administrarea și organizarea securității” din cuprinsul PrOpSec conține o introducere de tipul celei prezentate mai jos:

„Acest capitol, precum și capitolele următoare ale acestui document constituie PrOpSec pentru stocarea, procesarea și transmiterea informațiilor *(naționale/NATO/UE)* clasificate în *(..... numele SIC.....).*

PrOpSec au fost întocmite de către AOSIC împreună cu administratorii de securitate ai SIC *(.... enumerarea funcțiilor....)* în conformitate cu cerințele conținute în reglementările naționale privind protecția informațiilor clasificate, asociate cu..... *(enumerarea normelor specifice privind securitatea: instrucțiuni locale, politici ale rețelelor din care SIC face parte sau cu care se interconectează)..... .*

PrOpSec au fost aprobate de către ORNISS. Nu este permisă nicio abatere de la conținutul PrOpSec sau modificarea conținutului acestui document până când nu este obținut acordul explicit al AAS. Înainte de implementarea oricărei modificări semnificative în PrOpSec, AOSIC trebuie să obțină aprobarea AAS. Efectuarea unor modificări minore trebuie raportată de către AOSIC la AAS, dar implementarea acesteia nu depinde de obținerea unei aprobări prealabile.”

(2) Capitolul din PrOpSec prevăzut la alin. (1) conține, de asemenea, detalii referitoare la următoarele aspecte:

a) descriere sumară a SIC pentru care sunt aplicabile PrOpSec;

b) identificarea punctelor de contact (spre exemplu, administratorii INFOSEC) pentru aspecte legate de securitatea SIC sau incidente legate de utilizarea SIC;

c) detalii cu privire la nivelul de clasificare a informațiilor permise a fi vehiculate pe SIC;

d) proceduri administrative pentru schimbarea drepturilor de acces;

e) o prevedere conform căreia orice incident care implică încălcarea securității fizice, a securității personalului, a securității informațiilor sau a securității SIC trebuie să fie raportată imediat către administratorul de securitate al SIC;

f) o prevedere cu privire la respectarea mesajului de avertizare afișat pe ecranul calculatorului la inițierea unei sesiuni de lucru pe SIC și, dacă este cazul, a informațiilor afișate de screen-saver;

g) o prevedere cu privire la necesitatea luării la cunoștință, prin semnătură, de către utilizatorii SIC a responsabilităților pe care le au în domeniul securității SIC.

Securitatea fizică

Art. 9. — Cap. 2 „Securitatea fizică” din cuprinsul PrOpSec include prevederi referitoare la procedurile de asigurare a securității fizice a echipamentelor SIC și a mediilor de stocare, inclusiv în afara orelor de program. Totodată, include prevederi referitoare la operarea SIC în locații în care se pot afla și persoane care nu dețin certificat/autorizație de acces la informații clasificate.

Securitatea personalului

Art. 10. — Cap. 3 „Securitatea personalului” din cuprinsul PrOpSec include prevederi referitoare la certificările de securitate minime necesare utilizatorilor SIC. Totodată, trebuie precizată obligativitatea ca utilizatorii să participe la programele

de pregătire și conștientizare în domeniul securității informațiilor, organizate de instituție/companie.

Securitatea informațiilor

Art. 11. — (1) În cadrul cap. 4 „Securitatea informațiilor” din cuprinsul PrOpSec se precizează faptul că securitatea informațiilor vizează toate formele de documente, de exemplu documente în format hârtie, medii de stocare asociate calculatoarelor (de exemplu: CD, dispozitiv de memorie USB), dispozitive de calcul și de comunicații portabile (de exemplu: laptop, agende electronice, tablete).

(2) Atunci când este cazul, capitolul menționat la alin. (1) conține și detalii referitoare la:

a) tipul documentelor — medii de stocare fixe/detașabile, documente în format hârtie;

b) marcajele de securitate, marcajele administrative și de limitare a diseminării care trebuie aplicate pe documentele utilizate;

c) procedurile aplicabile pentru clasificarea și marcarea corespunzătoare a documentelor;

d) procedurile de transfer a informațiilor;

e) responsabilitățile și procedurile privind înregistrarea și controlul documentelor, precum și procedurile de verificare a înregistrărilor, inclusiv frecvența acestora;

f) procedurile referitoare la utilizarea, stocarea și controlul mediilor de stocare, precum și evidența acestora;

g) responsabilitățile și procedurile privind reclasificarea/declasificarea/distrugerea și scoaterea din uz a documentelor.

Securitatea SIC

Art. 12. — Cap. 5 „Securitatea SIC” din cuprinsul PrOpSec oferă detalii cu privire la metodele de utilizare și control al facilităților de protecție asigurate de componentele software, în special în ceea ce privește:

a) conceptul de identificare (user-id) — procedurile pentru stabilirea conturilor de utilizatori, grupurile de utilizatori, alocarea identificatorilor de utilizator, procedurile pentru ștergerea conturilor de utilizator la părăsirea funcției/postului sau atunci când este detectată o compromitere a acestor date;

b) conceptul de autentificare — modalități de autentificare (de exemplu: parole, token, mecanisme biometrice), proceduri de control și de schimbare, autoritatea emitentă, păstrarea evidenței pentru controlul acestor mijloace și persoana responsabilă, frecvența de schimbare și proceduri de utilizare a mecanismelor de autentificare;

c) mecanisme de control al accesului — proceduri pentru implementarea controlului accesului discreționar/obligatoriu la informații/servicii/dispozitive; procedurile pentru stabilirea drepturilor și permisiunilor utilizatorilor pentru utilizarea serviciilor și resurselor SIC; detalii cu privire la autoritățile responsabile și la păstrarea evidențelor de control.

Securitatea calculatoarelor

Protecția împotriva software-ului malițios

Art. 13. — (1) Secțiunea „Protecția împotriva software-ului malițios” din cap. 5 „Securitatea SIC” conține un sumar al tuturor mecanismelor și procedurilor de protecție împotriva software-ului malițios, relevante pentru SIC.

(2) Sumarul menționat la alin. (1) include următoarele:

a) procedurile pentru verificarea mediilor de stocare ale calculatoarelor (care conțin informații și software) primite din surse externe, incluzând procedurile de tratare a mediilor infectate;

b) procedurile pentru verificarea mesajelor de poștă electronică și a atașamentelor primite din surse externe, pentru detectarea eventualelor componente de software malițios;

c) procedurile pe care trebuie să le urmeze utilizatorii pentru a detecta evenimentele provocate de software malițios;

d) procedurile pe care trebuie să le urmeze utilizatorii pentru a importa și instala software pe LAN.

Planificarea măsurilor pentru situații de urgență și pentru continuarea activității

Art. 14. — Cap. 6 „Planificarea măsurilor pentru situații de urgență și pentru continuarea activității” din cuprinsul PrOpSec descrie acțiunile care trebuie întreprinse de către utilizatori în eventualitatea unei situații de urgență sau a detectării unui incident.

Art. 15. — Fiecare utilizator trebuie să semneze o declarație potrivit căreia este pe deplin conștient de responsabilitățile ce îi revin în ceea ce privește protecția echipamentelor și a informațiilor asociate.

CAPITOLUL V

Conținutul PrOpSec pentru utilizatorii dispozitivelor portabile de calcul și de comunicații în cadrul misiunilor oficiale

Art. 16. — (1) Dispozitivele portabile de calcul și comunicații includ laptopuri, agende electronice și palmtop cu capacitate de stocare, procesare și/sau transmitere (de exemplu: PDA, BlackBerry, tablete) și telefoane celulare/telefoane mobile GSM cu funcționalitate de PDA.

(2) PrOpSec trebuie să conțină instrucțiuni pe care utilizatorii trebuie să le aplice când utilizează dispozitive portabile de calcul și comunicații cum sunt cele menționate la alin. (1) în misiuni oficiale în afara organizației.

(3) PrOpSec trebuie să includă prevederi de tipul:

„Dispozitivele portabile de calcul și comunicații pot fi scoase în afara *(.... denumirea organizației....)* pentru a fi utilizate în cadrul unei misiuni oficiale numai cu aprobarea AAS.

Echipamentele, precum și mediile de stocare și documentația asociate vor fi protejate pe întreaga perioadă în conformitate cu standardele de securitate aplicabile celui mai înalt nivel de clasificare a informațiilor stocate sau procesate.

Dispozitivul portabil de calcul și comunicații trebuie gestionat ca document cu nivel de clasificare similar celui pentru care a fost acreditat dispozitivul.

Informațiile clasificate trebuie să fie stocate pe medii de stocare detașabile, etichetate corespunzător (de exemplu, dispozitive de memorie USB), care trebuie stocate în locații adecvate.

Hard diskul dispozitivului portabil de calcul este criptat utilizând un mecanism de criptare adecvat, a cărui utilizare a fost aprobată de AAS. În această situație dispozitivul portabil de calcul poate fi lăsat fără supraveghere (de exemplu: într-o cameră de hotel), dar trebuie luate măsurile aplicabile obiectelor de valoare.

Dispozitivul portabil de calcul trebuie purtat într-o servietă care se poate încuia, ale cărei dimensiuni permit păstrarea acesteia în permanență asupra posesorului.

Atunci când transportul se realizează cu linii aeriene comerciale, personalul de securitate al aeroportului poate inspecta echipamentul, cu condiția ca această operațiune să nu conducă la deteriorarea componentelor electronice sau la accesul la informațiile clasificate. Trebuie luate măsuri pentru a se evita furtul dispozitivului.

La sediul la care se desfășoară misiunea trebuie respectate regulile de securitate locale, care pot include inspecția tehnică de securitate a dispozitivului portabil de calcul, operațiune realizată de personal specializat. Regulile de securitate locale trebuie respectate și în ceea ce privește schimbul de informații.

Toate mediile de stocare introduse în dispozitivul portabil de calcul trebuie verificate pentru a se identifica eventualul software malițios.

Pierderea dispozitivelor portabile de calcul și comunicații, precum și a mediilor de stocare asociate acestora trebuie raportată imediat... *(se precizează autoritatea responsabilă din cadrul organizației)....*

Echipamente proprietate privată

Este interzisă utilizarea dispozitivelor portabile de calcul pentru stocarea, procesarea sau transmiterea informațiilor clasificate.

Luarea la cunoștință a responsabilităților

La plecarea în misiune, personalul trebuie să ia o copie a PrOpSec. Personalul trebuie să semneze o declarație potrivit căreia este pe deplin conștient de responsabilitățile ce îi revin în ceea ce privește protecția echipamentelor și a informațiilor asociate.

Puncte de contact

Îndrumări suplimentare pot fi obținute de la administratorul de sistem și cel de securitate... *(se precizează datele de contact)....”*

(4) În situația în care un dispozitiv portabil de calcul sau comunicații conținând mecanisme de securitate (de exemplu, mecanisme criptografice) este utilizat pentru o misiune oficială, condițiile privind transportul, protecția și utilizarea trebuie stabilite în PrOpSec.

CAPITOLUL VI

Conținutul PrOpSec pentru utilizarea dispozitivelor portabile de calcul și de comunicații de către vizitatori

Art. 17. — (1) PrOpSec trebuie să conțină instrucțiunile care trebuie cunoscute de către vizitatori, în cazul utilizării de dispozitive portabile de calcul și comunicații în cadrul organizației.

(2) Instrucțiunile detaliate trebuie înmânate vizitatorilor la sosirea în organizație.

(3) PrOpSec trebuie să includă prevederi de tipul:

„Dispozitivele portabile de calcul pot fi utilizate numai în cazul în care sunt acreditate de către AAS pentru stocare, procesare sau transmitere de informații clasificate în cadrul unor misiuni oficiale determinate.

Echipamentele și mediile de stocare asociate trebuie să fie protejate în permanență în conformitate cu standardele de securitate aplicabile celui mai înalt nivel de clasificare a informațiilor pentru care echipamentele au fost acreditate.

Mediile de stocare asociate dispozitivelor portabile de calcul ale vizitatorilor trebuie să fie utilizate pentru acele dispozitive. În cazul în care există necesitatea schimbului de informații, trebuie stabilite și aprobate de către AOSIC proceduri specifice acestei activități.

Conectarea dispozitivelor portabile de calcul la sistemele informatice și de comunicații ale ... *(denumirea organizației)...* este interzisă.

Dispozitivele portabile de calcul pot fi utilizate în camerele în care se desfășoară ședințe numai cu aprobarea președintelui de ședință.

Dispozitivele GSM (telefoane mobile/celulare) pot fi utilizate numai în locuri special indicate. În afara acestor locații dispozitivele GSM trebuie închise. Toate capacitățile de comunicații (de exemplu, Bluetooth) trebuie să fie dezactivate.

Atunci când dispozitivul GSM este dotat cu cameră video sau capacități de înregistrare audio utilizarea acestora este interzisă în zone de securitate clasa I și clasa a II-a.

Luarea la cunoștință a responsabilităților

Persoanele trebuie să semneze o declarație potrivit căreia sunt pe deplin conștiente de responsabilitățile ce le revin în ceea ce privește protecția informațiilor clasificate.

Puncte de contact

Îndrumări suplimentare pot fi obținute de la administratorul de sistem și cel de securitate... *(se precizează datele de contact).... .”*

CAPITOLUL VII

Conținutul PrOpSec pentru autoritățile operaționale ale sistemelor informatice și de comunicații (AOSIC)

Art. 18. — Prezentul capitol descrie conținutul PrOpSec, incluzând, unde este cazul, informații mai detaliate.

Administrarea și organizarea securității

Art. 19. — (1) Cap. 1 „Administrarea și organizarea securității” din cuprinsul PrOpSec conține o introducere de tipul celei prezentate mai jos:

„Acest capitol, precum și capitolele următoare ale acestui document constituie Procedurile operaționale de securitate (PrOpSec) pentru stocarea, procesarea și transmiterea informațiilor (*naționale/NATO/UE*) clasificate în (*..... numele SIC .....*).

PrOpSec au fost întocmite de către AOSIC împreună cu administratorii de securitate ai SIC (*.... enumerarea funcțiilor ....*) în conformitate cu cerințele conținute în reglementările naționale privind protecția informațiilor clasificate, asociate cu ..... (*enumerarea normelor specifice privind securitatea: instrucțiuni locale, politici ale rețelelor din care SIC face parte sau cu care se interconectează*).

PrOpSec au fost aprobate de către ORNISS.

Nu este permisă nicio abatere de la conținutul PrOpSec sau modificarea conținutului acestui document până când nu este obținut acordul explicit al AAS. Înainte de implementarea oricărei modificări semnificative în PrOpSec, AOSIC trebuie să obțină aprobarea AAS. Efectuarea unor modificări minore trebuie raportată de către AOSIC la AAS, dar implementarea acestora nu depinde de obținerea unei aprobări prealabile.”

(2) Capitolul menționat la alin. (1) conține, de asemenea, detalii referitoare la următoarele aspecte:

a) descrierea SIC — o descriere sumară a sistemului, inclusiv a interconectărilor externe și o subliniere a capacităților funcționale;

b) responsabilitățile privind securitatea personalului cu atribuții în acest sens, potrivit Directivei privind structurile cu responsabilități în domeniul INFOSEC — INFOSEC 1, aprobată prin Ordinul directorului general al Oficiului Registrului Național al Informațiilor Secrete de Stat nr. 86/2013, denumită în continuare *INFOSEC 1* (de exemplu, AOSIC, administratorii de securitate ai SIC, administratorul CRIPTO, administratorul COMSEC, inclusiv personalul având responsabilități în asigurarea securității fizice, a personalului, a informațiilor și, unde este cazul, a securității industriale);

c) detalii despre modul de operare de securitate al SIC și nivelul de clasificare a informațiilor vehiculate în SIC;

d) proceduri administrative pentru actualizarea sau efectuarea de modificări în Lista cu utilizatorii autorizați ai SIC și drepturile de acces ale acestora;

e) prevederi pentru raportarea imediată a oricărui incident major care implică încălcarea securității fizice, a personalului, a informațiilor sau a SIC către administratorii de securitate ai SIC, incident care apoi trebuie raportat de către AOSIC la AAS folosindu-se formularul din INFOSEC 3;

f) prevederi care să garanteze că întregul personal al SIC a luat la cunoștință, a înțeles și și-a însușit conținutul PrOpSec, în părțile care îl privesc. Într-un mediu de rețea, pentru creșterea gradului de conștientizare a personalului privind securitatea, PrOpSec sau extrase semnificative din acest document pot fi stocate pe un server central, în așa fel încât și utilizatorii să poată avea acces ușor la procedurile care îi interesează, cu precizarea ca PrOpSec să poată fi accesate doar de utilizatorii autorizați ai SIC, conform drepturilor de acces ale acestora.

(3) Capitolul prevăzut la alin. (1) conține, de asemenea, detalii, acolo unde este cazul, referitoare la următoarele aspecte:

a) procedurile privind asistența de securitate a utilizatorilor din locațiile distribuite sau aflate la distanță ale SIC;

b) extrase din cerințele de securitate a comunicațiilor, pentru a include, de exemplu, procedurile operaționale criptografice pentru produsele și mecanismele criptografice în uz;

c) proceduri pentru controlul personalului tehnic sau al altor categorii de personal suport care necesită accesul în zona SIC sau în zonele terminalelor/stațiilor de lucru aflate la distanță;

d) proceduri pentru controlul mediilor de stocare, a componentelor software și hardware autorizate, care sunt proprietate privată;

e) proceduri pentru controlul echipamentelor și componentelor software autorizate ale contractorilor.

Securitatea fizică

Art. 20. — (1) Cap. 2 „Securitate fizică" din cuprinsul PrOpSec cuprinde măsurile de securitate fizică necesare pentru a asigura prevenirea accesului neautorizat la informații clasificate, efectuării de operațiuni neautorizate, blocării resurselor și serviciilor SIC și pentru protejarea echipamentelor.

(2) Capitolul prevăzut la alin. (1) conțin detalii, acolo unde este cazul, despre următoarele:

a) definirea zonelor unde se află componentele sistemului — încăperea/sala calculatoarelor, centrul de management al SIC, camera în care sunt instalate echipamentele criptografice, locul în care se păstrează mediile de stocare, încăperea terminalelor/stațiilor de lucru, locațiile prevăzute pentru continuarea activității în caz de dezastru, inclusiv localizarea, tipul și elementele de identificare ale întregului echipament conectat. Este necesară descrierea planului de cablare, identificându-se cablurile RED/BLACK și specificându-se distanțele de separare între aceste cabluri. Pentru terminalele/stațiile de lucru la distanță pot fi elaborate PrOpSec separate, sumare, care trebuie să specifice procedurile minime de securitate necesare pentru permiterea conectării acestora la SIC gazdă;

b) detalii cu privire la securitatea fizică a zonelor în care sunt instalate calculatoarele/echipamentele de comunicații, care să includă detalii cu privire la cheile și/sau combinațiile încuietorilor — identitatea acestora, unde se păstrează, modul de evidență și cine are permisiunea să le primească, să le predea și/sau să le folosească;

c) proceduri pentru garantarea securității fizice a zonei în care sunt instalate componentele sistemului, inclusiv echipamentele de comunicații, în afara orelor de program, incluzând, de exemplu, setările senzorilor pentru detecția intruziunilor;

d) controlul accesului personalului și echipamentelor:

(i) procedurile și modul de evidență pentru controlul vizitatorilor, inclusiv măsurile aplicate pentru prevenirea vizualizării neautorizate a informațiilor de pe dispozitivele de ieșire și afișare;

(ii) permisele — tipul de permise în uz și cerințele privind portul sau afișarea acestor permise, detalii referitoare la cine este responsabil pentru autorizarea și/sau emiterea permiselor, detalii privind păstrarea evidenței acestora;

(iii) procedurile în vigoare pentru controlul introducerii, depozitării, exploatării și scoaterii diferitelor echipamente;

e) detalii cu privire la alarmele de sesizare a intruziunilor și a problemelor apărute în mediul operațional — unde sunt dispuși senzorii, regimul lor de testare, frecvența efectuării testelor, procedurile de setare a sistemului de alarmare și procedurile privind reacția la diferite alarme.

Securitatea personalului

Art. 21. — (1) Cap. 3 „Securitatea personalului" din cuprinsul PrOpSec pentru AOSIC conține detalii, unde este cazul, despre toate aspectele securității personalului, referitoare la:

a) certificate de securitate/autorizații de acces pentru utilizatori și alte categorii de personal:

(i) cerințele privind certificarea de securitate a utilizatorilor, administratorilor de securitate, administratorilor de sistem, administratorilor CRIPTO;

(ii) personalul care are dreptul să fie prezent în camerele în care sunt instalate echipamentele SIC pe durata procesării și în afara orelor de program, inclusiv cerințele privind certificarea de securitate a acestei categorii de personal;

(iii) aplicarea regulii celor două persoane în zonele în care sunt instalate echipamente ale SIC;

(iv) pentru locațiile terminalelor/stațiilor de lucru aflate la distanță sau pentru orice altă componentă a SIC — se vor preciza categoriile de personal care are dreptul să fie prezent în camerele în care sunt instalate echipamentele SIC pe durata procesării și în afara orelor de program, inclusiv cerințele privind certificarea de securitate a acestei categorii de personal și aplicarea regulii de lucru cu două persoane;

b) personalul-cheie:

(i) detalii specifice cu privire la anumite categorii de personal — proiectanții/analiștii/programatorii de sistem, personalul operațional, consultanții comerciali, inginerii de sistem și alte categorii de personal tehnic sau de întreținere, incluzând, ca anexă la PrOpSec, o listă a funcțiilor care intră în această categorie;

(ii) detalii cu privire la personalul auxiliar, precum personalul de curățenie și muncitorii care au acces în zonele în care sunt instalate componentele SIC;

(iii) detalii cu privire la persoanele care au acces în fiecare cameră, zonă, clădire etc.;

c) educația și conștientizarea de securitate

(i) cerințele de educație/conștientizare/pregătire de securitate pentru toate categoriile de personal care au acces la SIC, incluzând fiecare dintre aspectele securității: securitatea fizică, securitatea personalului, securitatea informațiilor și securitatea SIC;

(ii) necesitatea de asumare oficială a instrucțiunilor de securitate.

(2) Măsurile și dispozițiile prevăzute la alin. (1) sunt necesare avându-se în vedere următoarele aspecte:

a) orice persoană capabilă să intre în zonele în care sunt instalate componentele SIC poate fi în situația de a interacționa sau de a avaria echipamentul și poate avea acces la informațiile clasificate afișate pe ecran sau la cele listate;

b) amenințările la adresa securității SIC pot veni din partea oricărei persoane care are pregătirea profesională, cunoștințe corespunzătoare despre SIC și posibilitatea de acces la SIC;

c) personalul care are dreptul legitim de intrare în zonele în care sunt instalate componentele SIC poate avea posibilitatea să acceseze neautorizat informații sau să permită extragerea acestora de către persoane neautorizate;

d) poate exista o anumită categorie de personal-cheie (de exemplu, programatori, analiști și ingineri de sistem, personal de întreținere, consultanți comerciali) care, prin cunoștințele lor despre caracteristicile de securitate ale SIC, pot să le compromită sau să le ocolească.

Securitatea informațiilor

Art. 22. — (1) Cap. 4 „Securitatea informațiilor” din cuprinsul PrOpSec destinate AOSIC conține detalii, acolo unde este cazul, despre următoarele:

a) toate tipurile de documente în uz — medii de stocare fixe sau detașabile ale calculatoarelor, documente în format hârtie;

b) marcajele de securitate, marcaje administrative suplimentare, marcajele de limitare a diseminării care trebuie aplicate diferitelor tipuri de documente aflate în uz;

c) proceduri corespunzătoare pentru marcarea nivelului de clasificare sau de sensibilitate a documentelor;

d) proceduri privind stocarea diferitelor tipuri de documente aflate în uz;

e) responsabilități și proceduri pentru înregistrarea și controlul documentelor și evidența controalelor, inclusiv frecvența acestora;

f) procedurile pentru păstrarea, evidența și controlul mediilor de stocare pentru calculatoare.

Pentru bibliotecile de medii de stocare, trebuie precizate următoarele:

(i) clasificarea, cerințele de etichetare, localizarea în bibliotecă;

(ii) înregistrări ale tuturor operațiunilor, inclusiv pentru documentele păstrate în alte locuri (de exemplu, mediile pentru back-up), registre de evidență pentru documentele clasificate (sau un sistem automat de evidență), formulare pentru transfer și primire și înregistrări ale istoricului clasificării documentelor;

(iii) metodele și formularele de solicitare a mediilor de stocare;

(iv) îndatoririle persoanei responsabile cu biblioteca de medii de stocare;

(v) păstrarea documentelor de control;

g) procedurile pentru primirea, schimbul și diseminarea documentelor, inclusiv rolurile persoanelor responsabile cu importul/exportul de documente și proceduri de verificare a tuturor mediilor de stocare ale calculatoarelor (purtătoare de informații sau de software) pentru a identifica eventuala prezență a virușilor de calculator sau a altor programe nocive;

h) responsabilități și proceduri pentru declasificarea/reclasificarea/distrugerea/disponibilizarea documentelor, care să reglementeze folosirea incineratoarelor, echipamentelor de demagnetizare, echipamentelor de dezintegrare, tocare etc., inclusiv unde și cum trebuie să se efectueze distrugerea, cât de frecvent și de către cine se execută operațiunea.

(2) În SIC, volumul și compactarea informațiilor stocate sau procesate, accesibilitatea lor, ușurința și viteza de copiere a informațiilor, uneori și de la stații aflate la distanță, subliniază nevoia luării unor măsuri stringente de securitate a informațiilor.

(3) Securitatea informațiilor acoperă toate formele de documente care conțin informații clasificate, de exemplu, documente în format hârtie (cum sunt documente tipărite, grafice, scheme, figuri, hărți, desene, listinguri cu loguri de audit ale sistemului), medii de stocare pentru calculatoare (CD, carduri de memorii flash, dispozitive de stocare USB, benzi magnetice, casete, discuri magnetice detașabile, dischete floppy, cartușe de date, discuri magnetice fixe, PROMs și EPROMs), microfilme și microfișe, benzi de imprimantă etc. Se adresează, totodată, dispozitivelor de calcul portabile (de exemplu laptop, notebook electronic, palmtop, PDA), atunci când harddiskul sau memoria sunt utilizate pentru stocarea informațiilor.

(4) Un document este definit ca fiind orice informație înregistrată, indiferent de forma sau caracteristicile sale fizice, incluzând, spre exemplu, materiale scrise sau listate, cartele și benzi pentru procesarea datelor, hărți, planșe, fotografii, picturi, desene, gravuri, schițe, notițe de lucru, indigo sau riboane, sau alte tipuri de reproduceri, precum și sunete, voci, înregistrări magnetice, electronice, optice sau video în orice format, precum și echipamentele IT portabile cu medii de stocare fixe și medii de stocare detașabile.

Securitatea SIC

Art. 23. — Mecanismele de securitate hardware, firmware și software pot contribui individual și în combinație la securitatea SIC, prin furnizarea de facilități pentru următoarele:

a) identificarea serviciilor, dispozitivelor, mediilor și utilizatorilor care reprezintă elemente individuale ale sistemelor de control al securității;

b) controlul software al accesului prin care este restricționat accesul utilizatorilor la elementele hardware, firmware și software și la informațiile la care le este permis accesul, precum și la informațiile pentru care este interzis accesul neautorizat;

c) detectarea activităților neautorizate (de exemplu, încercările de acces neautorizat), susținută de mecanisme de reacție și raportare;

d) verificări care să garanteze funcționarea corectă a celor menționate la lit. a), b) și c).

Securitatea calculatoarelor

Securitatea hardware

Art. 24. — (1) Securitatea hardware se referă la caracteristicile de securitate asigurate de către componentele fizice ale SIC.

(2) Secțiunea „Securitatea hardware” oferă detalii despre sau, acolo unde este cazul, face referiri la următoarele aspecte ale securității hardware:

a) proceduri și documentație de securitate referitoare la pornirea echipamentelor SIC;

b) proceduri și documentație de securitate referitoare la oprirea echipamentelor SIC;

c) instrucțiuni și proceduri referitoare la conectarea/deconectarea echipamentelor relevante pentru securitate;

d) proceduri privind efectuarea de verificări periodice pentru punerea în evidență a eventualelor încercări de desfacere a echipamentelor și pentru asigurarea faptului că modulele hardware sunt păstrate încuiate, în mod normal, în carcasa echipamentului;

e) configurația calculatorului utilizată pentru procesarea în diferite condiții; de exemplu, trebuie precizat ce terminale/stații de lucru trebuie să fie deconectate și/sau ce periferice trebuie dezactivate într-o situație specifică de exploatare;

f) procedurile de securizare a configurației calculatorului pregătit pentru întreținere și reparare, incluzând următoarele:

(i) nivelul de autorizare necesar pentru modificarea configurației echipamentului, introducerea de hardware și software nou sau schimbarea oricărei componente hardware, inclusiv placa de bază care poate stoca, procesa sau transmite informații clasificate;

(ii) orice restricții impuse referitoare la momentele în care se pot realiza sau nu întreținerile periodice;

(iii) detalii referitoare la orice rutine de diagnosticare care se instalează fie în mod periodic, fie conform unui program de întreținere sau unor modificări hardware. În situațiile excepționale în care AAS a considerat că tehnicile de diagnoză și mentenanță de la distanță sunt necesare și pot fi acceptate, trebuie specificate procedurile de securitate aplicabile;

(iv) specificații referitoare la programele de întreținere periodică, inclusiv instrucțiuni pentru identificarea rapoartelor de diagnosticare care pot conține informații clasificate;

(v) proceduri referitoare la identificarea, păstrarea și controlul pieselor de schimb și accesoriilor relevante din punctul de vedere al securității;

g) procedurile care trebuie urmate în caz de defecțiune hardware, cu descrierea acțiunilor care trebuie întreprinse și a persoanelor care trebuie să întreprindă aceste acțiuni, în vederea securizării calculatorului la deconectare, și ce date trebuie păstrate referitoare la astfel de incidente hardware;

h) procedurile pentru reconectarea terminalelor/stațiilor de lucru de la distanță care au fost deconectate din motive de securitate;

i) în cazul în care se asigură și protecția TEMPEST pentru SIC, acest lucru trebuie precizat în această secțiune și corelat cu prevederile din secțiunea „Securitatea emisiei".

Securitatea software

Art. 25. — (1) Securitatea software se referă la caracteristicile de securitate asigurate de următoarele componente:

a) firmware — instrucțiuni software, de obicei scrise de furnizorii de hardware, care simulează hardware-ul și pot fi înlocuite prin implementarea hardware efectivă;

b) sistemul de operare;

c) programe utilitare — asigură facilități comune și frecvent utilizate, cum ar fi funcții automatizate de birou, sisteme de gestiune a bazelor de date, compilatoare de programe, sortare și concatenare de fișiere, programe de verificare, scanare, control, audit etc.;

d) programe de aplicație — care satisfac cerințele utilizatorilor.

(2) Secțiunea „Securitatea software" furnizează detalii, acolo unde este cazul, despre metoda de utilizare și control al caracteristicilor de protecție furnizate prin software, specificând în particular următoarele:

a) metoda de identificare (identificatorul utilizatorului) — proceduri de stabilire a conturilor utilizatorilor, a grupurilor de utilizatori și de alocare a identificatorilor utilizatorilor, proceduri de ștergere a conturilor utilizatorilor în cazul plecării personalului de la post sau atunci când a fost detectată o compromitere a contului respectiv;

b) metoda de autentificare — include protecția informațiilor de autentificare (de exemplu, parole, token sau metode biometrice), procedurile de control și schimbare, autoritatea emitentă, păstrarea înregistrărilor de control și de către cine, frecvența schimbării și procedurile utilizate pentru mecanismul de autentificare;

c) mecanismele de control al accesului — proceduri de implementare a controlului accesului discreționar și/sau obligatoriu la informații/servicii/dispozitive, proceduri pentru stabilirea drepturilor și permisiuni utilizatorilor de accesare și utilizare a informațiilor, serviciilor și resurselor SIC, detalii despre autoritățile responsabile și păstrarea evidențelor privind controlul;

d) evidența versiunii sistemului de operare, programelor utilitare și pachetelor software, inclusiv cele care vor fi folosite în situații deosebite;

e) controlul asupra facilităților de copiere sau de modificare a sistemului de operare, cu detalii despre autoritatea și documentația necesară;

f) detalii despre măsurile de precauție ce trebuie luate înainte și după procesare sau în timpul pregătirii diferitelor tipuri de activități clasificate, incluzând rutine de ștergere a memoriei principale, reguli de declasificare sau de suprascriere a versiunilor anterioare și proceduri care să asigure că bufferele sunt curățate și că toate datele din fișierele jurnalelor de audit au fost listate și suprascrise.

(3) Secțiunea software furnizează, de asemenea, unde este cazul, detalii privind software-ul de sistem și de aplicații, după cum urmează:

a) responsabilități pentru generare și utilizare;

b) procedurile de primire și introducere în sistem, autorizări și formularele necesare;

c) clasificarea;

d) controlul copierii;

e) utilizarea limbajelor de programare/compilatoarelor/macro-urilor;

f) proceduri de audit și validare a componentelor software — ce, de către cine, cu ce frecvență și ce înregistrări se păstrează;

g) copiile de siguranță ale sistemului — ce conțin și unde se păstrează, în ce formă, ce verificări se fac, cu ce frecvență și cine este autorizat să activeze/să folosească aceste copii;

h) proceduri care trebuie urmate în caz de erori și ce înregistrări trebuie păstrate;

i) controlul copiilor în format hârtie.

Protecția antivirus a calculatoarelor

Art. 26. — (1) Secțiunea „Protecția antivirus a calculatoarelor" conține un sumar al tuturor procedurilor și mecanismelor de protecție împotriva software-ului malițios, atât manuale, cât și automate, și responsabilitățile individuale relevante pentru SIC.

(2) Secțiunea menționată la alin. (1) include următoarele:

a) proceduri de verificare a sistemelor de operare instalate, a pachetelor software și a programelor utilitare, privind prezența virușilor sau a altui software malițios, incluzând proceduri pentru ștergerea acestora în cazul detectării lor;

b) proceduri pentru verificarea mediilor de stocare (conținând informații și software) primite din surse externe, incluzând proceduri pentru dezinfectarea lor;

c) proceduri pentru verificarea mesajelor electronice și a atașamentelor primite din surse externe pentru a identifica eventuala prezență a software-ului malițios;

d) proceduri care trebuie urmate de către utilizatori în cazul detectării unor evenimente cauzate de software malițios;

e) proceduri pentru raportarea incidentelor cauzate de viruși atât către expeditorul mediului de stocare infectat, cât și la AAS, folosindu-se formularul din Directiva privind managementul INFOSEC pentru sisteme informatice și de comunicații — INFOSEC 3, aprobată prin Ordinul directorului general al Oficiului Registrului Național al Informațiilor Secrete de Stat nr. 484/2003.

Managementul și auditul automat al securității

Art. 27. — (1) Secțiunea „Managementul și auditul automat al securității" conține un sumar al tuturor măsurilor și procedurilor automate de management al securității, al procedurilor de audit, atât cele manuale, cât și cele asigurate de sistem, alocarea responsabilităților relevante pentru SIC.

(2) Secțiunea menționată la alin. (1) include următoarele:

a) procedurile pentru rularea instrumentelor/programelor automate de management al securității și detalii despre facilitățile de audit;

b) detalii despre evenimentele relevante pentru securitate care trebuie luate în evidență (logged) (de exemplu, tipul evenimentului și informația asociată fiecărui tip de eveniment);

c) detalii despre modul cum sunt folosite jurnalele (log-urile) de securitate, atât pentru investigarea erorilor, cât și pentru anumite fișiere sau categorii de personal, bazate pe urmărirea evenimentelor sau activităților, a tendințelor anormale, incluzând detalii despre evenimentele care trebuie supravegheate;

d) desfășurarea inspecțiilor/analizelor periodice ale înregistrărilor de audit, în scopul descoperirii prompte a accesului neautorizat sau a încercărilor de acces și pentru luarea măsurilor corespunzătoare de remediere;

e) responsabilitățile persoanelor care trebuie să ruleze și să valideze integritatea instrumentelor/programelor de management automat al securității și să desfășoare investigări și analize în cazul descoperirii de anomalii;

f) proceduri de reacție la evenimente specifice, de exemplu, activarea alarmelor în timp real;

g) detalii privind perioada de păstrare a fișierelor de audit;

h) proceduri care trebuie urmate în cazul apariției de anomalii ale auditului.

Securitatea criptografică

Art. 28. — Secțiunea „Securitatea criptografică" furnizează detalii cu privire la următoarele aspecte ale securității criptografice, acolo unde este cazul:

a) stabilirea persoanei responsabile cu implementarea și controlul procedurilor privind securitatea criptografică și cerințele de certificare de securitate pentru această persoană;

b) stabilirea administratorului COMSEC, conform INFOSEC 1 și instrucțiunilor privind managementul, utilizarea și protecția materialului criptografic în România;

c) detalii despre administratorul CRIPTO al SIC (de exemplu, funcție, responsabilități) pentru acele SIC care folosesc echipament criptografic ca o componentă a sistemului;

d) proceduri specifice de utilizare a echipamentului criptografic, în special managementul materialelor criptografice. Secțiunea trebuie să facă referire la instrucțiunile privind managementul, utilizarea și protecția materialului criptografic în România, pentru detalii în ceea ce privește măsurile de protecție a materialului criptografic și responsabilitățile utilizatorilor acestui material.

Securitatea emisiilor

Art. 29. — Secțiunea „Securitatea emisiilor" furnizează detalii cu privire la următoarele aspecte ale securității emisiei, acolo unde este cazul:

a) stabilirea persoanei responsabile cu implementarea și controlul procedurilor de securitate a emisiei;

b) proceduri de analizare a cerințelor TEMPEST, pentru locațiile SIC, cu acordul ORNISS;

c) proceduri pentru stabilirea locului în care echipamentele de calcul portabile și calculatoare/stațiile de lucru de sine stătătoare pot opera în interiorul locațiilor SIC;

d) informații despre metodele corespunzătoare de instalare ale echipamentului;

(i) trimiteri către informațiile furnizate de către producător;

(ii) specificații în conformitate cu Directiva privind selectarea și instalarea echipamentelor și sistemelor care vehiculează informații clasificate, în format electronic — INFOSEC 6, versiunea 2, aprobată prin Ordinul directorului general al Oficiului Registrului Național al Informațiilor Secrete de Stat nr. 358/2008;

e) detalii cu privire la cerințele de evaluare și certificare a echipamentelor și evaluare a locațiilor în care sunt instalate echipamentele SIC.

Securitatea transmisiilor

Art. 30. — Secțiunea „Securitatea transmisiilor" furnizează detalii despre următoarele aspecte ale securității transmisiei, acolo unde este cazul:

a) stabilirea persoanei responsabile cu implementarea și controlul procedurilor de securitate a transmisiei;

b) proceduri asociate cu protecția adecvată a comunicațiilor în sistemele autorizate, deduse din analiza secțiunilor necriptate ale acestor comunicații;

c) proceduri de reducere a conținutului informațional prin secțiunile neprotejate ale sistemelor de comunicații;

d) proceduri operaționale pentru sistemele care asigură securitatea fluxului informațional.

Planificarea măsurilor pentru situații de urgență și pentru continuarea activității

Art. 31. — (1) Cap. 6 „Planificarea măsurilor pentru situații de urgență și pentru continuarea activității" din cuprinsul PrOpSec pentru AOSIC furnizează detalii despre procedurile obișnuite relevante pentru securitate, referitoare la efectuarea salvărilor de siguranță (back-up), incluzând următoarele aspecte, acolo unde este cazul:

a) detalii despre metodele de salvare de siguranță a informațiilor relevante din punctul de vedere al securității și a informațiilor utilizatorilor;

b) frecvența realizării salvărilor de siguranță;

c) cerințe privind transmiterea și păstrarea copiilor de back-up;

d) testarea copiilor de back-up;

e) proceduri privind accesul la copiile de back-up și utilizarea acestora.

(2) Capitolul menționat la alin. (1) furnizează, de asemenea, detalii despre procedurile de securitate sau face referiri la acestea, incluzând proceduri de distrugere a informațiilor în caz de urgență și proceduri de recuperare a informațiilor în caz de dezastru, care trebuie urmate în situații excepționale, de exemplu:

a) defecțiuni hardware, erori software sau descoperirea introducerii de viruși sau de software malițios;

b) indisponibilitatea liniilor de telecomunicație;

c) variații ale tensiunii de alimentare sau căderea acesteia;

d) aspecte privind mediul operațional al SIC (de exemplu: fum, foc, explozii, inundații, scurgeri de lichide, probleme ale structurii de rezistență a clădirii, cutremure, furtuni și alte calamități naturale);

e) acțiuni subversive, sabotaj, terorism, mișcări sociale sau amenințări cu bombe.

(3) Capitolul precizat la alin. (1) include, unde este cazul, proceduri cu privire la distrugerea echipamentelor criptografice și a materialului cu chei criptografice, în situații de urgență.

(4) Capitolul prevăzut la alin. (1) furnizează, de asemenea, un sumar al modului de exersare a procedurilor de urgență și frecvența cu care se fac aceste exerciții sau face referiri la documente interne care conțin aceste prevederi.

Managementul configurației

Art. 32. — (1) Managementul configurației SIC constă în identificarea, controlul, păstrarea evidenței, diseminarea și auditul tuturor modificărilor efectuate în timpul etapelor de proiectare, dezvoltare, exploatare, întreținere și îmbunătățire a ciclului de viață al SIC.

(2) Cap. 7 „Managementul configurației" din cuprinsul PrOpSec pentru AOSIC furnizează detalii despre următoarele caracteristici ale planului de management al configurației, acolo unde acestea sunt legate de aspecte ale securității hardware, firmware și software:

a) responsabilitățile personalului pentru controlul și organizarea actualizării configurației;

b) documentația care descrie configurația de bază autorizată pentru SIC;

c) măsurile de securitate aplicate pentru a garanta faptul că arhitectura/configurația de bază autorizată pentru SIC nu poate face obiectul unor modificări neautorizate, de exemplu, prin introducerea unui software neautorizat;

d) controale care se efectuează la modificarea documentației de proiectare și de implementare;

e) controale care se efectuează la generarea unei noi versiuni a sistemului, incluzând pachetele utilitare și cele software;

f) măsuri aplicabile în cazul actualizării sistemului de operare (service packs, hot fixes, security patches), incluzând pachetele utilitare și de software;

g) măsurile (tehnice, fizice și procedurale) care se efectuează pentru protecția față de modificarea sau distrugerea neautorizată a copiei principale sau a copiilor tuturor celorlalte materiale utilizate pentru generarea sistemului, incluzând pachetele software și utilitarele;

h) controale care se efectuează pentru configurarea dispozitivelor de comunicații (de exemplu, routere) și a dispozitivelor de protecție a limitelor sistemului (de exemplu, firewall);

i) procedurile pentru solicitarea modificării configurației hardware, firmware și software a SIC;

j) procedurile pentru solicitarea de modificări specifice ale configurației hardware sau a mediului operațional al sistemului, acolo unde există nevoia punerii de acord cu standardul TEMPEST și pentru auditul implementării modificărilor specifice;

k) procedurile postimplementare necesare pentru actualizarea documentației privind modificarea configurației.

(3) Capitolul menționat la alin. (1) include, de asemenea, detalii cu privire la procedurile de implementare a actualizărilor aplicațiilor antivirus, a sistemului de operare prin service packs/hotfixes/security patches.

CAPITOLUL VIII

Proceduri operaționale asociate

Art. 33. — Capitolul 8 „Proceduri operaționale asociate" precizează, dacă este cazul, alte documente cu proceduri operaționale de securitate asociate care au fost elaborate pentru a stabili responsabilități pentru anumite grupuri de utilizatori.

MINISTERUL AFACERILOR INTERNE

O R D I N

pentru modificarea și completarea Ordinului viceprim-ministrului, ministrul afacerilor interne, nr. 38/2014 privind coordonarea activității și delegarea unor competențe în cadrul Ministerului Afacerilor Interne

În temeiul art. 7 alin. (5) din Ordonanța de urgență a Guvernului nr. 30/2007 privind organizarea și funcționarea Ministerului Afacerilor Interne, aprobată cu modificări prin Legea nr. 15/2008, cu modificările și completările ulterioare,

viceprim-ministrul, ministrul afacerilor interne, emite următorul ordin:

Art. I. — Ordinul viceprim-ministrului, ministrul afacerilor interne, nr. 38/2014 privind coordonarea activității și delegarea unor competențe în cadrul Ministerului Afacerilor Interne, publicat în Monitorul Oficial al României, Partea I, nr. 199 din 21 martie 2014, se modifică și se completează după cum urmează:

1. **La articolul 2, litera f) se abrogă.**

2. **La articolul 5 alineatul (1), după litera d) se introduce o nouă literă, litera e), cu următorul cuprins:**

„e) Direcția generală pentru monitorizarea, controlul operațional și inspecția activității serviciilor de ambulanță și UPU/CPU."

3. **La articolul 6 alineatul (1), după litera l) se introduce o nouă literă, litera m), cu următorul cuprins:**

„m) Oficiul Responsabilului cu Protecția Datelor Personale."

Art. II. — Prezentul ordin se publică în Monitorul Oficial al României, Partea I.

Viceprim-ministru, ministrul afacerilor interne,

Gabriel Oprea

București, 2 aprilie 2014.

Nr. 48.

R E P U B L I C Ă R I

L E G E A Nr. 129/1992
privind protecția desenelor și modelelor*)

CAPITOLUL I
Dispoziții generale

Art. 1. — (1) Drepturile asupra desenelor și modelelor sunt dobândite și protejate în România prin înregistrare la Oficiul de Stat pentru Invenții și Mărci, denumit în continuare *O.S.I.M.,* în condițiile prezentei legi.

(2) Prezenta lege se aplică desenelor și modelelor ce fac obiectul unei înregistrări sau solicitări de înregistrare în România ori care își produc efectele în România, ca urmare a unei protecții comunitare sau internaționale.

(3) Străinii cu domiciliul sau sediul în afara teritoriului României beneficiază de prevederile prezentei legi în condițiile convențiilor internaționale privind desenele și modelele, la care România este parte.

Art. 2. — În înțelesul prezentei legi, termenii sau expresiile de mai jos se definesc după cum urmează:

a) *Aranjamentul de la Haga* — Aranjamentul privind depozitul internațional de desene și modele industriale, adoptat la Haga la 6 noiembrie 1925, cu modificările și completările ulterioare, la care România a aderat prin Legea nr. 44/1992;

b) *autor* — persoana fizică sau un grup de persoane fizice constituit pe baza unei înțelegeri, care a creat desenul sau modelul;

c) *certificat de înregistrare* — titlul de protecție acordat de O.S.I.M. pentru desenele și modelele înregistrate;

d) *desen sau model* — aspectul exterior al unui produs sau al unei părți a acestuia, redat în două sau trei dimensiuni, rezultat din combinația dintre principalele caracteristici, îndeosebi linii, contururi, culori, formă, textură și/sau materiale ale produsului în sine și/sau ornamentația acestuia;

e) *desen sau model comunitar* — desenul sau modelul protejat în condițiile Regulamentului nr. 6/2002/CE, publicat în Jurnalul Oficial al Comunităților Europene L nr. 3 din 5 ianuarie 2002, de către Oficiul pentru Armonizare în Piața Internă, cu efect pe întregul teritoriu al Comunităților Europene;

f) *detalii nesemnificative* — acele elemente grafice sau de formă, care nu determină caracterul individual al desenului sau modelului;

g) *înregistrare* — modul de dobândire a drepturilor asupra desenelor și modelelor în temeiul prezentei legi sau al convențiilor internaționale la care România este parte;

h) *mandatar autorizat* — persoana care exercită profesiunea de consilier în proprietate industrială în condițiile legii și care poate reprezenta o parte interesată în procedurile în fața O.S.I.M.;

i) *produs* — orice articol obținut printr-un proces industrial sau artizanal, conținând printre altele și elemente concepute spre a fi asamblate într-un produs complex, ambalaje, forme de prezentare, aranjamente, simboluri grafice, caractere tipografice; programele de calculator nu sunt considerate produs;

j) *produs complex* — un produs compus din elemente multiple ce pot fi înlocuite de o manieră care să permită dezasamblarea și reasamblarea produsului;

k) *solicitant* — persoana fizică sau juridică ce solicită la O.S.I.M. înregistrarea, respectiv eliberarea unui certificat de înregistrare a unui desen sau model;

l) *titular* — persoana fizică sau juridică căreia îi aparțin drepturile conferite prin înregistrarea desenului sau modelului și pentru care se eliberează certificatul de înregistrare.

Art. 3. — (1) Dreptul la eliberarea certificatului de înregistrare aparține autorului desenului sau modelului ori succesorului său în drepturi, pentru desenele și modelele create în mod independent.

(2) În cazul în care mai multe persoane au creat în mod independent un desen sau model, dreptul la eliberarea certificatului de înregistrare aparține persoanei care a depus prima cererea de înregistrare.

(3) În cazul în care desenul sau modelul a fost creat ca urmare a unor contracte cu misiune creativă sau de către salariați, în cadrul atribuțiilor de serviciu, dreptul aparține persoanei care l-a comandat.

Art. 4. — Până la proba contrară, solicitantul este prezumat a avea dreptul la eliberarea certificatului de înregistrare a desenului sau modelului.

Art. 5. — (1) Drepturile asupra unui desen sau model dobândite conform prezentei legi nu prejudiciază drepturile asupra desenelor sau modelelor neînregistrate, mărcilor și altor semne distinctive, brevetelor de invenție și modelelor de utilitate, caracterelor tipografice, topografiilor de produse semiconductoare.

(2) Protecția desenului sau modelului înregistrat în conformitate cu prezenta lege nu exclude și nu prejudiciază protecția prin drept de autor a acestuia.

CAPITOLUL II
Condiții pentru protecția desenelor și modelelor

Art. 6. — (1) Obiectul cererii poate fi înregistrat în măsura în care constituie un desen sau model, în sensul art. 2, este nou și are un caracter individual.

(2) Un desen sau model este considerat nou dacă niciun desen ori model identic nu a fost făcut public înaintea datei de depunere a cererii de înregistrare sau, dacă a fost revendicată prioritatea, înaintea datei de prioritate.

(3) Se consideră că desenele sau modelele sunt identice dacă trăsăturile lor caracteristice diferă numai în ceea ce privește detaliile nesemnificative.

(4) Se consideră că un desen sau model are caracter individual dacă impresia globală pe care o produce asupra utilizatorului avizat este diferită de cea produsă asupra unui asemenea utilizator de orice desen ori model făcut public înaintea datei de depunere a cererii de înregistrare sau, dacă a fost revendicată prioritatea, înaintea datei de prioritate.

(5) La evaluarea caracterului individual trebuie să se ia în considerare gradul de libertate a autorului în elaborarea desenului sau modelului.

(6) Dacă un desen sau model aplicat la un produs ori încorporat într-un produs constituie o parte componentă a unui

---

*) Republicată în temeiul art. 248 din Legea nr. 187/2012 pentru punerea în aplicare a Legii nr. 286/2009 privind Codul penal, publicată în Monitorul Oficial al României, Partea I, nr. 757 din 12 noiembrie 2012, cu modificările ulterioare.

Legea nr. 129/1992 a mai fost republicată în Monitorul Oficial al României, Partea I, nr. 876 din 20 decembrie 2007 și ulterior a mai fost modificată prin Legea nr. 76/2012 pentru punerea în aplicare a Legii nr. 134/2010 privind Codul de procedură civilă, publicată în Monitorul Oficial al României, Partea I, nr. 365 din 30 mai 2012, cu modificările ulterioare.

produs complex, acesta va fi considerat nou și având caracter individual numai dacă sunt îndeplinite cumulativ următoarele condiții:

a) partea componentă, odată încorporată în produsul complex, rămâne vizibilă pe durata utilizării normale a acestuia; *utilizare normală* înseamnă utilizarea de către beneficiar, fără a include întreținerea sau reparațiile;

b) caracteristicile vizibile ale părții componente îndeplinesc ele însele condițiile privind noutatea și caracterul individual.

Art. 7. — (1) În sensul aplicării art. 6, se consideră că un desen sau model a fost făcut public dacă a fost publicat ori dezvăluit în alt mod, expus, utilizat în comerț, cu excepția situațiilor în care aceste evenimente nu ar fi putut, în mod rezonabil și în cadrul activității obișnuite, să devină cunoscute cercurilor specializate din sectorul în cauză care acționează în cadrul Uniunii Europene înainte de data de depunere a cererii de înregistrare sau, dacă a fost invocată o prioritate, înaintea datei de prioritate. Cu toate acestea, nu se va considera că desenul sau modelul a fost făcut public pentru simplul motiv că a fost dezvăluit unei terțe persoane în condiții explicite sau implicite de confidențialitate.

(2) În aplicarea art. 6 alin. (2) și (4), divulgarea nu este luată în considerare dacă desenul sau modelul pentru care se solicită protecție a fost făcut public:

a) de către autor sau succesorul său în drepturi ori de către un terț pe baza informațiilor furnizate sau actelor îndeplinite de autor sau succesor;

b) în perioada de 12 luni precedând data de depozit a cererii de înregistrare sau, dacă o prioritate este revendicată, la data de prioritate.

(3) Dispozițiile alin. (2) sunt aplicabile și în situația în care desenul sau modelul a fost făcut public, ca urmare a unui abuz în legătură cu autorul sau succesorul său.

Art. 8. — (1) Desenul sau modelul care este determinat exclusiv de o funcție tehnică nu poate fi înregistrat.

(2) Nu poate fi înregistrat un desen sau model care trebuie reprodus în forma și la dimensiunile exacte, pentru a permite ca produsul în care acesta este încorporat sau căruia îi este aplicat să fie conectat mecanic ori amplasat, în jurul sau pe un alt produs, astfel încât fiecare produs să își poată îndeplini funcția proprie.

(3) Poate fi înregistrat un desen sau model care permite asamblări sau conexiuni multiple între produsele interschimbabile în cadrul unui sistem modular.

Art. 9. — Sunt excluse de la protecție desenele sau modelele contrare ordinii publice sau bunelor moravuri.

CAPITOLUL III

Înregistrarea și eliberarea titlului de protecție

Art. 10. — (1) Cererea de înregistrare a unui desen sau model trebuie să cuprindă:

a) solicitarea de înregistrare a desenului sau modelului;

b) datele de identificare a solicitantului;

c) numărul de desene sau modele pentru care se solicită protecția;

d) indicarea produselor în care este încorporat desenul sau modelul, dacă este cazul;

e) descrierea elementelor noi, caracteristice desenului sau modelului pentru care se solicită protecția, așa cum apar în reprezentările grafice depuse;

f) numele autorilor sau o declarație pe răspunderea solicitantului că autorii au renunțat la dreptul de a fi menționați în cerere și/sau în publicațiile desenului sau modelului;

g) reprezentările grafice ale desenului sau modelului, în 3 exemplare.

(2) Cererea de înregistrare mai poate conține, după caz, și alte elemente care nu condiționează data depozitului reglementar:

a) datele de identificare a mandatarului autorizat, în cazul în care acesta a fost desemnat în cererea de înregistrare;

b) actele de prioritate, în cazul în care se invocă una dintre prioritățile prevăzute la art. 16 și 17;

c) solicitarea amânării publicării;

d) procura de reprezentare în fața O.S.I.M.;

e) declarația indicând informațiile care, după cunoștința solicitantului, permit să se dovedească îndeplinirea condițiilor de acordare a protecției desenului sau modelului pentru care se solicită înregistrarea.

Art. 11. — (1) Reprezentările grafice trebuie să redea complet desenul sau modelul care face obiectul cererii de înregistrare, astfel încât caracteristicile sale estetice să fie evidențiate. În caz contrar, cererea de înregistrare se respinge. Reprezentările grafice trebuie să fie de o calitate suficientă, pentru ca toate detaliile desenului sau modelului să fie evidențiate și publicarea să fie posibilă.

(2) În cazul unui desen, reprezentările grafice pot fi însoțite de 3 specimene.

(3) Nu se admit la înregistrare desene sau modele reprezentate grafic în mod schematic sau de principiu.

Art. 12. — (1) Cererea de înregistrare și descrierea, prezentate conform art. 10 și redactate în limba română, însoțite de reprezentările grafice ale desenului sau modelului ori, după caz, de specimene, se depun la O.S.I.M. și constituie depozitul reglementar.

(2) O.S.I.M. înregistrează cererea dacă sunt depuse minimum următoarele: o cerere care să conțină solicitarea de înregistrare a desenului sau modelului, datele de identificare a solicitantului și reprezentările grafice sau specimenele, într-un exemplar.

(3) Dacă în termen de două luni de la data depunerii cererii de înregistrare conform alin. (2) nu sunt depuse completările necesare pentru constituirea depozitului reglementar conform alin. (1), cererea de înregistrare se respinge.

(4) Data depozitului reglementar este data la care au fost depuse documentele prevăzute la alin. (2) sau data care rezultă din tratatele ori convențiile privind desenele sau modelele la care România este parte.

(5) Cererea de înregistrare având dată de depozit se înscrie în Registrul cererilor depuse.

(6) Registrul cererilor depuse poate să fie realizat atât pe format hârtie, cât și în format electronic.

Art. 13. — (1) În procedurile în fața O.S.I.M. solicitantul înregistrării sau succesorul său în drepturi poate fi reprezentat de un consilier în proprietate industrială autorizat.

(2) Pentru persoanele care nu au domiciliul sau sediul pe teritoriul României, reprezentarea conform alin. (1) este obligatorie, cu excepția depunerii cererii.

Art. 14. — (1) Un depozit multiplu poate cuprinde mai multe desene sau modele ale aceleiași categorii de produse, în conformitate cu clasificarea internațională a desenelor și modelelor.

(2) Desenele și modelele care fac obiectul unui depozit multiplu trebuie să satisfacă o regulă de unitate de concepție, de unitate de producție sau de unitate de utilizare ori trebuie să aparțină aceluiași ansamblu sau aceleiași compoziții de articole.

Art. 15. — Depozitul reglementar asigură solicitantului un drept de prioritate, cu începere de la data constituirii acestuia, față de orice alt depozit ulterior privind același desen sau model.

Art. 16. — (1) Persoanele fizice sau persoanele juridice ale statelor părți la convențiile la care România este parte beneficiază de un drept de prioritate de 6 luni, cu începere de la data primului depozit, dacă solicită protecția în acest termen, pentru același desen sau model.

(2) Se recunoaște un drept de prioritate de 6 luni, întemeiat pe un depozit de model de utilitate.

Art. 17. — Dacă solicitantul a prezentat anumite produse și servicii în cadrul unei expoziții internaționale oficiale sau oficial recunoscute, în sensul Convenției privind expozițiile internaționale, semnată la Paris la data de 22 noiembrie 1928, ratificată de România prin Legea nr. 246/1930, cu modificările și completările ulterioare, organizată pe teritoriul României sau într-un stat membru al Convenției de la Paris pentru protecția proprietății industriale, în forma revizuită la Stockholm la 14 iulie 1967, și dacă o cerere de înregistrare a desenului sau modelului sub care au fost prezentate aceste produse a fost depusă la O.S.I.M. într-un termen de 6 luni de la data prezentării în expoziție, solicitantul va beneficia de un drept de prioritate de la data introducerii produsului în expoziție; această perioadă nu prelungește termenul de prioritate prevăzut la art. 16.

Art. 18. — Prioritățile prevăzute la art. 16 și 17 sunt recunoscute dacă sunt invocate odată cu depunerea cererii și dacă în termen de 3 luni de la data depunerii cererii se confirmă prin acte de prioritate.

Art. 19. — (1) Cererile de înregistrare depuse la O.S.I.M. vor fi supuse unei examinări preliminare din care să rezulte:

a) îndeplinirea condițiilor de formă ale cererii, prevăzute la art. 10 alin. (1);

b) îndeplinirea condițiilor prescrise pentru reprezentările grafice, prevăzute la art. 11;

c) îndeplinirea condițiilor prescrise pentru celelalte documente sau acte anexate la cerere, prevăzute la art. 10 alin. (2);

d) achitarea taxelor în termenul și cuantumul prevăzute de lege.

(2) În cazul în care neregularitățile nu sunt remediate în termenul acordat de O.S.I.M., cererea se va respinge sau, după caz, nu se va recunoaște prioritatea.

(3) Dacă se constată neregularități, acestea se notifică solicitantului, acordându-i-se un termen necesar pentru remedieri.

(4) Cererile care nu îndeplinesc condițiile de depozit multiplu se vor diviza de către solicitant, la cererea O.S.I.M.

(5) Solicitantul are obligația să divizeze cererea în termenul acordat de O.S.I.M., constituind câte un depozit reglementar pentru fiecare grup de desene sau modele care îndeplinesc condițiile prevăzute la art. 14.

(6) În cazul în care solicitantul nu divizează cererea în termenul acordat, O.S.I.M. divizează din oficiu cererea în mai multe cereri divizate și va lua în examinare numai prima cerere, respingându-le pe celelalte.

(7) Cererile divizate nu pot fi depuse decât pentru elementele care nu depășesc conținutul cererii inițiale. Cererile divizate sunt considerate ca fiind depuse la data de depozit a cererii inițiale.

Art. 20. — (1) Cererea de înregistrare a desenului sau modelului, precum și reproducerea, fotografia sau reprezentarea grafică a acestuia se publică în Buletinul oficial de proprietate industrială al O.S.I.M., în format electronic, în termen de maximum 4 luni de la data constituirii depozitului reglementar, în alb-negru sau, la cerere, în culori.

(2) Publicarea prevăzută la alin. (1) poate fi amânată, la cererea solicitantului, pe o perioadă care nu poate depăși 30 de luni, calculată de la data depunerii cererii sau de la data priorității, când aceasta a fost invocată.

(3) Publicarea cererilor internaționale de către Organizația Mondială a Proprietății Intelectuale este considerată o publicare conform alin. (1).

Art. 21. — (1) Persoanele interesate pot face opoziții scrise la O.S.I.M. privind cererea de înregistrare a desenului sau modelului, în termen de două luni de la data publicării acestuia, pentru motivele prevăzute la art. 22 alin. (3).

(2) O.S.I.M. notifică solicitantului cererii opoziția formulată, indicând numele persoanei care a formulat-o, precum și motivele opoziției privind înregistrarea desenului sau modelului.

(3) În termen de două luni de la data notificării opoziției, solicitantul poate prezenta punctul său de vedere.

(4) Opoziția formulată cu privire la cererea de desen sau model publicată se soluționează de către o comisie din cadrul Serviciului desene și modele în termen de 3 luni de la depunere. Comisia emite un raport de admitere sau de respingere a opoziției, care va fi avut în vedere la examinarea de fond.

(5) Soluționarea opoziției poate fi suspendată în următoarele situații:

a) când se bazează pe o cerere de înregistrare a unui desen sau model, până la luarea unei hotărâri cu privire la aceasta;

b) desenul sau modelul opus face obiectul unei acțiuni în anulare, până la soluționarea definitivă a cauzei.

Art. 22. — (1) Cererile de înregistrare a desenelor sau modelelor se examinează de către Comisia de examinare a desenelor și modelelor. Comisia hotărăște, după caz, înregistrarea sau respingerea desenului sau modelului, în termen de 12 luni de la data publicării cererii, ori poate lua act de renunțarea la cerere sau de retragerea acesteia. Comisia va lua hotărârea de înregistrare a desenului sau modelului pe baza unui raport de examinare și în conformitate cu prevederile art. 2, 6 și 7.

(2) Înregistrarea desenelor sau modelelor se face în Registrul desenelor și modelelor și se publică în Buletinul oficial de proprietate industrială al O.S.I.M.

(3) Cererea de înregistrare a unui desen sau model va fi respinsă sau înregistrarea va fi anulată pentru următoarele motive:

a) nu sunt îndeplinite prevederile art. 2, 6 și 7;

b) obiectul cererii se încadrează în prevederile art. 8 și 9;

c) încorporează, fără acordul titularului, o operă protejată prin Legea nr. 8/1996 privind dreptul de autor și drepturile conexe, cu modificările și completările ulterioare, sau orice alt drept de proprietate industrială protejat;

d) constituie o utilizare improprie a oricăruia dintre obiectele menționate în lista cuprinsă în art. 6 ter din Convenția de la Paris pentru protecția proprietății industriale, în forma revizuită la Stockholm la 14 iulie 1967, la care România a aderat prin Decretul nr. 1.177/1968, sau o utilizare abuzivă a emblemelor și stemelor, altele decât cele menționate în art. 6 ter din convenție;

e) solicitantul nu a făcut dovada că este persoană îndreptățită la înregistrarea desenului sau modelului în sensul art. 3;

f) desenul sau modelul este în conflict cu un desen sau model anterior care a făcut obiectul unei divulgări publice după data de depozit a cererii de înregistrare sau după data de prioritate, dacă o prioritate este revendicată, și care este protejat de la o dată anterioară prin înregistrarea unui desen sau model comunitar ori printr-o cerere de înregistrare a unui desen sau model comunitar, sau prin înregistrarea unui desen sau model în România ori printr-o cerere de obținere a protecției în România;

g) desenul sau modelul folosește un semn distinctiv ce conferă titularului semnului dreptul de a interzice această utilizare.

(4) Când un desen sau model a fost respins la înregistrare ori când un drept asupra unui desen sau model a fost declarat nul în temeiul alin. (3), desenul sau modelul poate fi înregistrat ori dreptul asupra desenului poate fi menținut într-o formă modificată, dacă în acea formă cerințele de protecție vor fi îndeplinite, iar identitatea desenului sau modelului va fi păstrată. Înregistrarea sau menținerea într-o formă modificată poate să includă înregistrarea însoțită de o renunțare parțială din partea deținătorului dreptului asupra desenului sau modelului ori de înregistrarea în Registrul desenelor și modelelor a hotărârii judecătorești a instanței care a pronunțat nulitatea parțială a dreptului asupra desenului sau modelului.

(5) Dreptul asupra unui desen poate fi declarat nul chiar după ce a expirat sau s-a renunțat la el.

(6) În examinarea cererii, se vor lua în considerare fondul documentar de desene și modele existent la O.S.I.M., înregistrările internaționale de desene și modele la Organizația Mondială a Proprietății Intelectuale, desenele/modelele comunitare, precum și orice alte documente relevante pentru procedurile de examinare depuse de persoanele interesate. În procedurile de examinare, O.S.I.M. poate solicita orice completări necesare, iar în cazul desenelor, chiar specimene.

(7) Dispozițiile prezentei legi se aplică și cererilor internaționale depuse conform Aranjamentului de la Haga, care își extind efectele lor în România, în afară de cazul în care nu se prevede altfel.

Art. 23. — Dacă înregistrarea unui desen sau model, reînnoirea înregistrării acestuia sau înscrierea unei modificări în Registrul de desene și modele a fost afectată, în mod evident, din eroare materială, O.S.I.M. poate, în termen de 3 luni cu începere de la data înregistrării sau de la data înscrierii, să revoce înregistrarea, reînnoirea sau înscrierea modificării efectuate. Hotărârea de revocare, motivată, se comunică persoanelor interesate în termen de 30 de zile.

Art. 24. — (1) Hotărârile privind cererile de înregistrare a desenului sau modelului pot fi contestate, în scris și motivat, la O.S.I.M., în termen de 30 de zile de la comunicare.

(2) Contestația va fi examinată, în termen de cel mult 3 luni de la depunerea contestației, de către Comisia de contestații din Departamentul de apeluri al O.S.I.M.*)

Art. 25. — (1) Hotărârea Comisiei de contestații se comunică părților în termen de 30 de zile de la pronunțare și poate fi atacată cu contestație la Tribunalul București, în termen de 30 de zile de la comunicare. Hotărârea este supusă numai apelului.

(2) Hotărârile Comisiei de contestații rămase definitive se publică în Buletinul oficial de proprietate industrială al O.S.I.M., în termen de 60 de zile de la pronunțarea hotărârii.

(3) În fața Comisiei de contestații părțile se pot prezenta personal sau pot fi reprezentate prin avocat, prin consilier juridic sau printr-un consilier în proprietate industrială autorizat.

Art. 26. — Toate hotărârile luate în cadrul O.S.I.M. vor fi motivate.

Art. 27. — Eliberarea certificatelor de înregistrare de desene sau modele de către O.S.I.M. se face în temeiul hotărârilor de admitere a cererii de înregistrare a desenelor sau modelelor, în termen de 30 de zile de la data la care hotărârea de admitere a rămas definitivă și irevocabilă.

Art. 28. — (1) Procedurile privind cererile de înregistrare de desene și modele și certificatele de înregistrare sunt supuse taxelor, în cuantumul și la termenele stabilite conform legii. Taxele se plătesc în contul O.S.I.M.

(2) Taxele datorate de persoanele fizice și persoanele juridice cu domiciliul sau, după caz, cu sediul în străinătate se plătesc în valută în contul O.S.I.M.

(3) Neplata taxelor la termenele legale atrage neefectuarea procedurii respective sau respingerea cererii de înregistrare a desenului ori modelului.

Art. 29. — (1) Solicitantul sau titularul certificatului de înregistrare care, din motive de forță majoră, nu a putut să respecte un termen privind procedurile în fața O.S.I.M. este repus în termen, dacă prezintă o cerere motivată, în termen de 60 de zile de la încetarea cauzei care l-a împiedicat să acționeze, dar nu mai târziu de un an de la expirarea termenului nerespectat.

(2) Dispozițiile alin. (1) nu se aplică în următoarele situații:

a) invocarea priorității conform art. 16—18;

b) plata taxelor de înregistrare și publicare;

c) înregistrarea unei opoziții conform art. 21;

d) formularea contestațiilor conform art. 24.

(3) Cererea de repunere în termen va fi însoțită de dovada privind plata taxei legale.

CAPITOLUL IV
Drepturi și obligații

Art. 30. — Pe întreaga durată de valabilitate a înregistrării desenelor sau modelelor, titularul are un drept exclusiv de a le utiliza și de a împiedica utilizarea lor de o terță parte care nu dispune de consimțământul său. Titularul are dreptul de a interzice terților să efectueze, fără consimțământul său, următoarele acte: reproducerea, fabricarea, comercializarea ori oferirea spre vânzare, punerea pe piață, importul, exportul sau folosirea unui produs în care desenul sau modelul este încorporat ori la care acesta se aplică sau stocarea unui astfel de produs în aceste scopuri.

Art. 31. — (1) Întinderea protecției este determinată de reprezentările grafice ale desenelor sau modelelor înregistrate.

(2) Protecția acordată unui desen sau model în baza prezentei legi se extinde la orice desen sau model care nu produce o impresie vizuală globală diferită asupra unui utilizator avizat.

(3) La stabilirea sferei de protecție se ia în considerare gradul de libertate a autorului în realizarea desenului sau modelului.

Art. 32. — Drepturile conferite la art. 30 nu se exercită în privința:

a) actelor efectuate exclusiv în scop personal și necomercial, experimental, de cercetare sau învățământ, cu condiția ca aceste acte să nu prejudicieze exploatarea normală a desenelor sau modelelor și să se menționeze sursa;

b) activităților de reproducere în domeniul cercetării sau învățământului, în scopul citării ori predării, cu condiția ca aceste activități să fie compatibile cu practica comercială loială, să nu aducă atingere în mod nedrept exploatării normale a desenului sau modelului și ca sursa să fie menționată;

c) echipamentelor aflate pe vehicule de transport maritim sau aerian înregistrate într-o altă țară, atunci când acestea intră temporar pe teritoriul României, ori importului de piese de schimb și accesorii în scopul reparării acestor vehicule sau al executării de reparații pe aceste vehicule;

d) folosirii sau luării măsurilor efective și serioase de folosire a desenelor sau modelelor de către terți, în intervalul de timp dintre decăderea din drepturi a titularului și revalidarea certificatului;

e) folosirii desenului sau modelului cu bună-credință, în perioada cuprinsă între data publicării decăderii din drepturi a titularului și data publicării dreptului restabilit.

Art. 33. — Drepturile decurgând din înregistrarea desenului sau modelului nu se vor putea exercita în cazul introducerii pe piața comunitară a produselor în care sunt încorporate desene

---

*) Organizarea și funcționarea Oficiului de Stat pentru Invenții și Mărci sunt reglementate de Hotărârea Guvernului nr. 573/1998, publicată în Monitorul Oficial al României, Partea I, nr. 345 din 11 septembrie 1998, cu modificările ulterioare.

sau modele protejate ori la care acestea se aplică, introduse pe piață anterior de către titularul certificatului de înregistrare sau cu consimțământul acestuia.

Art. 34. — (1) Începând cu data publicării cererii persoana fizică sau persoana juridică îndreptățită la eliberarea certificatului de înregistrare beneficiază provizoriu de aceleași drepturi conferite în conformitate cu prevederile art. 30, până la eliberarea certificatului de înregistrare, cu excepția cazurilor în care cererea de înregistrare a fost respinsă sau retrasă.

(2) Încălcarea prevederilor alin. (1) atrage pentru persoanele vinovate obligația de despăgubire potrivit dreptului comun; titlul pentru plata despăgubirilor se poate executa numai după eliberarea certificatului de înregistrare a desenului sau modelului.

Art. 35. — (1) Perioada de valabilitate a unui certificat de înregistrare a desenului sau modelului este de 10 ani de la data constituirii depozitului reglementar și poate fi reînnoită pe 3 perioade succesive de 5 ani.

(2) Pe întreaga perioadă de valabilitate a certificatului, titularul este obligat la plata taxelor de menținere în vigoare a acestuia.

(3) O.S.I.M. acordă un termen de grație de cel mult 6 luni pentru plata taxelor de menținere în vigoare, pentru care se percep majorări.

(4) Neplata acestor taxe atrage decăderea titularului din drepturi.

(5) Decăderea titularului din drepturi se publică în Buletinul oficial de proprietate industrială al O.S.I.M.

(6) În cazul decăderii din drepturi a titularului, acesta poate solicita la O.S.I.M. revalidarea certificatului de înregistrare, în termen de 6 luni de la data decăderii, pentru motive temeinice.

Art. 36. — Dreptul exclusiv de exploatare decurgând din înregistrarea desenului sau modelului încetează în următoarele situații:

a) la expirarea perioadei de valabilitate;

b) prin anularea certificatului de înregistrare;

c) prin decăderea titularului din drepturi;

d) prin renunțarea titularului certificatului de înregistrare.

Art. 37. — Titularii certificatelor de înregistrare a desenelor sau modelelor pot menționa pe produse semnul D, respectiv litera „D” majusculă, înscrisă într-un cerc, însoțită de numele titularului sau de numărul certificatului.

Art. 38. — (1) Dreptul la eliberarea certificatului de înregistrare a desenului sau modelului, drepturile care decurg din cererea de înregistrare a desenului sau modelului, precum și drepturile născute din înregistrare sunt transmisibile în tot sau în parte.

(2) Transmiterea se poate face pe cale succesorală, prin cesiune sau licență.

(3) Transmiterea se înscrie la O.S.I.M. în Registrul desenelor și modelelor și produce efecte față de terți numai de la data publicării în Buletinul oficial de proprietate industrială al O.S.I.M. a mențiunii de transmitere.

(4) Înscrierea transmiterii de drepturi asupra desenelor sau modelelor aflate în litigiu se suspendă până la data rămânerii definitive a hotărârilor judecătorești cu privire la acestea.

Art. 39. — (1) Autorul, titular al certificatului de înregistrare a desenului sau modelului, beneficiază de drepturi patrimoniale stabilite pe bază de contract cu persoanele care exploatează desenul sau modelul.

(2) În cazul încheierii unui contract de cesiune, drepturile patrimoniale ale autorului se stabilesc în acest contract.

Art. 40. — Cererile internaționale făcute în conformitate cu Aranjamentul de la Haga se depun la Organizația Mondială a Proprietății intelectuale, direct sau prin intermediul O.S.I.M.

Art. 41. — (1) Autorul are dreptul să i se menționeze numele, prenumele și calitatea în certificatul de înregistrare eliberat, precum și în orice acte sau publicații privind desenul sau modelul.

(2) Datele din certificatul de înregistrare se înscriu în carnetul de muncă.

Art. 42. — (1) Înregistrarea desenului sau modelului poate fi anulată, în tot sau în parte, la cererea unei persoane interesate, pentru motivele prevăzute la art. 22 alin. (3).

(2) Anularea poate fi cerută pe toată durata de valabilitate a certificatului de înregistrare și se judecă de către Tribunalul București.

(3) Hotărârea de anulare se înregistrează la O.S.I.M. și se publică în termen de maximum două luni de la data înregistrării acesteia.

Art. 43. — Litigiile cu privire la calitatea de autor al desenului sau modelului, calitatea de titular al certificatului de înregistrare, cele cu privire la drepturile patrimoniale născute din contractele de cesiune sau licență sunt de competența instanțelor judecătorești, potrivit dreptului comun.

CAPITOLUL V
Desenele și modelele comunitare

Art. 44. — Desenele și modelele comunitare beneficiază de protecție pe teritoriul României, în baza Regulamentului nr. 6/2002/CE privind desenele și modelele comunitare, publicat în Jurnalul Oficial al Comunităților Europene L nr. 3 din 5 ianuarie 2002.

Art. 45. — Cererile de desene și modele comunitare pot fi depuse direct la Oficiul pentru Armonizare în Piața Internă sau prin intermediul O.S.I.M.

Art. 46. — Când o cerere de desen sau model comunitar este depusă la O.S.I.M. în temeiul art. 35 din Regulamentul nr. 6/2002/CE, O.S.I.M. înscrie data primirii pe cerere, și, fără să procedeze la examinare, o transmite la Oficiul comunitar în termen de două săptămâni, cu plata unei taxe de transmitere în cuantum de 70 de lei.

Art. 47. — Litigiile având ca obiect desene sau modele comunitare, pentru care Regulamentul nr. 6/2002/CE atribuie competența tribunalelor de desene și modele comunitare în sensul art. 80 alin. (1) din regulament, sunt de competența Tribunalului București, care soluționează cauzele în primă instanță.

CAPITOLUL VI
Atribuțiile Oficiului de Stat pentru Invenții și Mărci în domeniul protecției desenelor și modelelor

Art. 48. — O.S.I.M. este organul guvernamental de specialitate, cu autoritate unică pe teritoriul României, care asigură protecția desenelor și modelelor.

Art. 49. — O.S.I.M. are următoarele atribuții în domeniul protecției desenelor și modelelor:

a) acordă protecție prin eliberarea certificatului de înregistrare a desenelor și modelelor;

b) este depozitarul Registrului cererilor depuse și al Registrului desenelor și modelelor;

c) efectuează, la cerere, cercetări documentare privind desenele și modelele publicate și servicii de mediere;

d) întreține relații cu organizațiile guvernamentale similare și cu organizațiile internaționale de specialitate la care România este membră;

e) informează Comisia Europeană cu privire la dispozițiile naționale adoptate în scopul transpunerii dispozițiilor Directivei 98/71/CE a Parlamentului European și a Consiliului din 13 octombrie 1998 privind protecția juridică a desenelor și modelelor industriale;

f) acordă, la cerere, asistență în domeniul proprietății industriale, organizează cursuri de instruire pentru specialiștii în domeniu;

g) editează și publică periodic în Buletinul oficial de proprietate industrială al O.S.I.M. date privitoare la desene și modele.

CAPITOLUL VII

Răspunderi și sancțiuni

Art. 50. — (1) Însușirea fără drept, în orice mod, a calității de autor al desenului ori modelului constituie infracțiune și se pedepsește cu închisoare de la 3 luni la 2 ani sau cu amendă.

(2) Împăcarea înlătură răspunderea penală.

Art. 51. — În cazul în care, printr-o hotărâre judecătorească, se stabilește că o altă persoană decât cea care figurează în cererea de înregistrare sau în certificatul de înregistrare este îndreptățită la eliberarea certificatului de înregistrare, O.S.I.M. eliberează certificatul de înregistrare persoanei îndreptățite și publică schimbarea titularului.

Art. 52. — (1) Săvârșirea fără drept a oricărui act prevăzut la art. 30, după data înregistrării desenului sau modelului, constituie infracțiunea de contrafacere și se pedepsește cu închisoare de la 3 luni la 2 ani ori cu amendă.

(2) Împăcarea înlătură răspunderea penală.

Art. 53. — (1) Dacă titularul unui desen ori model înregistrat sau orice altă persoană care exercită dreptul de proprietate industrială cu consimțământul titularului face dovada credibilă că dreptul de proprietate industrială asupra desenului sau modelului face obiectul unei acțiuni ilicite, actuale sau iminente și că această acțiune riscă să îi cauzeze un prejudiciu greu de reparat, poate să ceară instanței judecătorești luarea unor măsuri provizorii.

(2) Instanța judecătorească poate să dispună în special:

a) interzicerea încălcării sau încetarea ei provizorie;

b) luarea măsurilor necesare pentru a asigura conservarea probelor. Sunt aplicabile prevederile Ordonanței de urgență a Guvernului nr. 100/2005 privind asigurarea respectării drepturilor de proprietate industrială, aprobată cu modificări prin Legea nr. 280/2005, cu modificările și completările ulterioare.

(3) Dispozițiile procedurale aplicabile sunt cuprinse în dispozițiile Codului de procedură civilă privitoare la măsurile provizorii în materia drepturilor de proprietate intelectuală.

(4) Măsurile provizorii pot fi dispuse și împotriva unui intermediar ale cărui servicii sunt utilizate de către un terț pentru a încălca un drept protejat prin prezenta lege.

Art. 54. — Autoritățile vamale pot dispune, fie din oficiu, fie la cererea titularului desenului sau modelului înregistrat, suspendarea vămuirii la importul mărfurilor, în cazurile prevăzute la art. 53, până la pronunțarea hotărârii judecătorești.

Art. 55. — Certificatele de înregistrare a desenelor și modelelor în vigoare reprezintă active necorporale și pot fi înregistrate în patrimoniul titularului, persoană juridică.

Art. 56. — (1) La cererea instanței judecătorești, O.S.I.M. este obligat să înainteze actele, documentele și informațiile necesare judecării cauzei cu care a fost învestită.

(2) În toate litigiile privind desenele și modelele citarea titularilor este obligatorie.

★

Prezenta lege*) transpune dispozițiile Directivei 98/71/CE privind protecția juridică a desenelor și modelelor comunitare, publicată în Jurnalul Oficial al Comunităților Europene L nr. 289 din 28 octombrie 1998, și creează cadrul juridic necesar aplicării directe, de la data aderării României la Uniunea Europeană, a Regulamentului nr. 6/2002/CE privind desenele și modelele comunitare, publicat în Jurnalul Oficial al Comunităților Europene L nr. 3 din 5 ianuarie 2002.

*) Mențiunea privind transpunerea normelor comunitare este prevăzută în Legea nr. 280/2007 pentru modificarea și completarea Legii nr. 129/1992, publicată în Monitorul Oficial al României, Partea I, nr. 729 din 26 octombrie 2007.

EDITOR: GUVERNUL ROMÂNIEI

„Monitorul Oficial” R.A., Str. Parcului nr. 65, sectorul 1, București; C.I.F. RO427282,
IBAN: RO55RNCB0082006711100001 Banca Comercială Română — S.A. — Sucursala „Unirea” București
și IBAN: RO12TREZ7005069XXX000531 Direcția de Trezorerie și Contabilitate Publică a Municipiului București
(alocat numai persoanelor juridice bugetare)
Tel. 021.318.51.29/150, fax 021.318.51.15, e-mail: marketing@ramo.ro, internet: www.monitoruloficial.ro
Adresa pentru publicitate: Centrul pentru relații cu publicul, București, șos. Panduri nr. 1,
bloc P33, parter, sectorul 5, tel. 021.401.00.70, fax 021.401.00.71 și 021.401.00.72
Tiparul: „Monitorul Oficial” R.A.

MONITORUL OFICIAL

5 948368 804692

Monitorul Oficial al României, Partea I, nr. 242/4.IV.2014 conține 16 pagini. Prețul: 3,20 lei **ISSN** 1453—4495