ORDIN nr. 18 din 21 martie 2014

pentru aprobarea Ghidului privind structura şi conținutul Procedurilor Operaționale de Securitate (PrOpSec) pentru sisteme informatice şi de comunicații - DS 2

EMITENT: OFICIUL REGISTRULUI NAȚIONAL AL INFORMAȚIILOR SECRETE DE STAT
PUBLICAT ÎN: MONITORUL OFICIAL nr. 242 din 4 aprilie 2014
Data intrarii in vigoare : 4 aprilie 2014

În temeiul:

- art. 1 alin. (4) lit. b) şi art. 3 alin. (6) din Ordonanța de urgență a Guvernului nr. 153/2002 privind organizarea şi funcționarea Oficiului Registrului Național al Informațiilor Secrete de Stat, aprobată prin Legea nr. 101/2003, cu modificările şi completările ulterioare;
- art. 55 alin. (1) din Regulamentul privind procedurile, la nivelul Guvernului, pentru elaborarea, avizarea şi prezentarea proiectelor de documente de politici publice, a proiectelor de acte normative, precum şi 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 şi conținutul Procedurilor Operaționale de Securitate (PrOpSec) pentru sisteme informatice şi 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 şi conținutul Procedurilor Operaționale de Securitate (PrOpSec) pentru sisteme informatice şi 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 şi conținutul Procedurilor Operaționale de Securitate (PrOpSec) pentru sisteme informatice şi de comunicații - DS 2

CAP. I
Introducere

ART. 1
Ghidul privind structura şi conținutul Procedurilor Operaționale de Securitate (PrOpSec) pentru sisteme informatice şi de comunicații - DS 2, denumit în continuare ghid, este elaborat în concordanță cu reglementările naționale privind protecția informațiilor clasificate şi 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) şi autorităților operaționale ale sistemului informatic şi de comunicații (AOSIC) care stochează, procesează sau transmit informații clasificate.

ART. 2
Întocmirea PrOpSec este obligatorie pentru toate sistemele informatice şi de comunicații (SIC) supuse procesului de acreditare de securitate, conform prevederilor Directivei privind managementul INFOSEC pentru sisteme informatice şi 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 şi a responsabilităților personalului, specifice SIC.

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

(3) AAS aprobă forma finală a PrOpSec.

ART. 4
Prezentul ghid stabileşte structura şi conținutul PrOpSec pentru următoarele categorii de personal şi mod de utilizare:

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

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

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

d) pentru AOSIC.

CAP. 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 şi superior sau echivalent trebuie supuse unui proces de acreditare de securitate.

(2) Acreditarea de securitate trebuie obținută şi 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) şi (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 şi pentru SIC care stochează, procesează sau transmit informații neclasificate, dar care poartă marcaje administrative sau de limitare a diseminării şi 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.

CAP. 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 şi 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 şi 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 şi 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 şi 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 aşa 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 cunoaşte".

CAP. IV

Conținutul PrOpSec pentru utilizatorii rețelelor locale (LAN)

ART. 7

(1) Prezentul capitol stabileşte elementele componente ale PrOpSec pentru utilizatorii rețelelor locale de calculatoare (LAN).

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

Administrarea şi organizarea societății

ART. 8

(1) Cap. 1 "Administrarea şi organizarea securității" din cuprinsul PrOpSec conține o introducere de tipul celei prezentate mai jos:

"Acest capitol, precum şi capitolele următoare ale acestui document constituie PrOpSec pentru stocarea, procesarea şi 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 afişat pe ecranul calculatorului la inițierea unei sesiuni de lucru pe SIC şi, dacă este cazul, a informațiilor afişate de screen-saver;

g) o prevedere cu privire la necesitatea luării la cunoştință, 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 şi a mediilor de stocare, inclusiv în afara orelor de program. Totodată, include prevederi referitoare la operarea SIC în locații în care se pot afla şi 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 şi conştientizare 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 şi de comunicații portabile (de exemplu: laptop, agende electronice, tablete).

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

a) tipul documentelor - medii de stocare fixe/detaşabile, documente în format hârtie;

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

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

d) procedurile de transfer a informațiilor;

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

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

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

Securitatea SIC

ART. 12

Cap. 5 "Securitatea SIC" din cuprinsul PrOpSec oferă detalii cu privire la metodele de utilizare şi control al facilităților de protecție asigurate de componentele software, în special în ceea ce priveşte:

a) conceptul de identificare (user-id) - procedurile pentru stabilirea conturilor de utilizatori, grupurile de utilizatori, alocarea identificatorilor de utilizator, procedurile pentru ştergerea 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 şi de schimbare, autoritatea emitentă, păstrarea evidenței pentru controlul acestor mijloace şi persoana responsabilă, frecvența de schimbare şi 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 şi permisiunilor utilizatorilor pentru utilizarea serviciilor şi resurselor SIC; detalii cu privire la autoritățile responsabile şi 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 şi 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 şi software) primite din surse externe, incluzând procedurile de tratare a mediilor infectate;

b) procedurile pentru verificarea mesajelor de poştă electronică şi a ataşamentelor 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 şi instala software pe LAN.

Planificarea măsurilor pentru situații de urgență şi pentru continuarea activității

ART. 14

Cap. 6 "Planificarea măsurilor pentru situații de urgență şi 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 conştient de responsabilitățile ce îi revin în ceea ce priveşte protecția echipamentelor şi a informațiilor asociate.

CAP. V

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

ART. 16

(1) Dispozitivele portabile de calcul şi comunicații includ laptopuri, agende electronice şi palmtop cu capacitate de stocare, procesare şi/sau transmitere (de exemplu: PDA, BlackBerry, tablete) şi 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 şi 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 şi comunicații pot fi scoase în afara (.... denumirea organizației....) pentru a fi utilizate în cadrul unei misiuni oficiale numai cu aprobarea AAS.

Echipamentele, precum şi mediile de stocare şi 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 şi 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 detaşabile, 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 desfăşoară 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 şi în ceea ce priveşte 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 şi comunicații, precum şi 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 cunoştință 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 conştient de responsabilitățile ce îi revin în ceea ce priveşte protecția echipamentelor şi a informațiilor asociate.

Puncte de contact

Îndrumări suplimentare pot fi obținute de la administratorul de sistem şi 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 şi utilizarea trebuie stabilite în PrOpSec.

CAP. VI

Conținutul PrOpSec pentru utilizarea dispozitivelor portabile de calcul şi 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 şi 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 şi 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 şi aprobate de către AOSIC proceduri specifice acestei activități.

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

Dispozitivele portabile de calcul pot fi utilizate în camerele în care se desfăşoară şedințe numai cu aprobarea preşedintelui de şedință.

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 şi clasa a II-a.

Luarea la cunoştință a responsabilităților

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

Puncte de contact

Îndrumări suplimentare pot fi obținute de la administratorul de sistem şi cel de securitate... (se precizează datele de contact).... ."

CAP. VII

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

ART. 18

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

Administrarea şi organizarea securității

ART. 19

(1) Cap. 1 "Administrarea şi organizarea securității" din cuprinsul PrOpSec conține o introducere de tipul celei prezentate mai jos:

"Acest capitol, precum şi capitolele următoare ale acestui document constituie Procedurile operaționale de securitate (PrOpSec) pentru stocarea, procesarea şi 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 şi 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 şi, unde este cazul, a securității industriale);

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

d) proceduri administrative pentru actualizarea sau efectuarea de modificări în Lista cu utilizatorii autorizați ai SIC şi 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 cunoştință, a înțeles şi şi-a însuşit conținutul PrOpSec, în părțile care îl privesc. Într-un mediu de rețea, pentru creşterea gradului de conştientizare a personalului privind securitatea, PrOpSec sau extrase semnificative din acest document pot fi stocate pe un server central, în aşa fel încât şi utilizatorii să poată avea acces uşor 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 şi 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 şi hardware autorizate, care sunt proprietate privată;

e) proceduri pentru controlul echipamentelor şi 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 şi serviciilor SIC şi 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 şi elementele de identificare ale întregului echipament conectat. Este necesară descrierea planului de cablare, identificându-se cablurile RED/BLACK şi 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 şi/sau

combinațiile încuietorilor - identitatea acestora, unde se păstrează, modul de evidență şi cine are permisiunea să le primească, să le predea şi/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 şi echipamentelor:

(i) procedurile şi modul de evidență pentru controlul vizitatorilor, inclusiv măsurile aplicate pentru prevenirea vizualizării neautorizate a informațiilor de pe dispozitivele de ieşire şi afişare;

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

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

e) detalii cu privire la alarmele de sesizare a intruziunilor şi a problemelor apărute în mediul operațional - unde sunt dispuşi senzorii, regimul lor de testare, frecvența efectuării testelor, procedurile de setare a sistemului de alarmare şi 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 şi 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 şi 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 şi în afara orelor de program, inclusiv cerințele privind certificarea de securitate a acestei categorii de personal şi aplicarea regulii de lucru cu două persoane;

b) personalul-cheie:

(i) detalii specifice cu privire la anumite categorii de personal - proiectanții/analiştii/programatorii de sistem, personalul operațional, consultanții comerciali, inginerii de sistem şi 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 şi 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 şi conştientizarea de securitate

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

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

(2) Măsurile şi 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 şi poate avea acces la informațiile clasificate afişate pe ecran sau la cele listate;

b) amenințările la adresa securității SIC pot veni din partea oricărei persoane care are pregătirea profesională, cunoştințe corespunzătoare despre SIC şi 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, analişti şi ingineri de sistem, personal de întreținere, consultanți comerciali) care, prin cunoştințele 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 detaşabile 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 şi proceduri pentru înregistrarea şi controlul documentelor şi evidența controalelor, inclusiv frecvența acestora;

f) procedurile pentru păstrarea, evidența şi 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 şi primire şi înregistrări ale istoricului clasificării documentelor;

(iii) metodele şi 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 şi diseminarea documentelor, inclusiv rolurile persoanelor responsabile cu importul/exportul de documente şi proceduri de verificare a tuturor mediilor de stocare ale calculatoarelor (purtătoare de informații sau de software) pentru a identifica eventuala prezență a viruşilor de calculator sau a altor programe nocive;

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

(2) În SIC, volumul şi compactarea informațiilor stocate sau procesate, accesibilitatea lor, uşurința şi viteza de copiere a informațiilor, uneori şi 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 detaşabile, dischete floppy, cartuşe de date, discuri magnetice fixe, PROMs şi EPROMs), microfilme şi microfişe, 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 şi benzi pentru procesarea datelor, hărți, planşe, fotografii, picturi, desene, gravuri, schițe, notițe de lucru, indigo sau riboane, sau alte tipuri de reproduceri, precum şi sunete, voci, înregistrări magnetice, electronice, optice sau video în orice format, precum şi echipamentele IT portabile cu medii de stocare fixe şi medii de stocare detaşabile.

Securitatea SIC

ART. 23

Mecanismele de securitate hardware, firmware şi software pot contribui individual şi în combinație la securitatea SIC, prin furnizarea de facilități pentru următoarele:

a) identificarea serviciilor, dispozitivelor, mediilor şi 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 şi software şi la informațiile la care le este permis accesul, precum şi la informațiile pentru care este interzis accesul neautorizat;

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

d) verificări care să garanteze funcționarea corectă a celor menționate la lit. a), b) şi 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 şi documentație de securitate referitoare la pornirea echipamentelor SIC;

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

c) instrucțiuni şi 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 şi 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 şi/sau ce periferice trebuie dezactivate într-o situație specifică de exploatare;

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

(i) nivelul de autorizare necesar pentru modificarea configurației echipamentului, introducerea de hardware şi 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 şi mentenanță de la distanță sunt necesare şi 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 şi controlul pieselor de schimb şi accesoriilor relevante din punctul de vedere al securității;

g) procedurile care trebuie urmate în caz de defecțiune hardware, cu descrierea acțiunilor care trebuie întreprinse şi a persoanelor care trebuie să întreprindă aceste acțiuni, în vederea securizării calculatorului la deconectare, şi 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 şi protecția TEMPEST pentru SIC, acest lucru trebuie precizat în această secțiune şi 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 şi pot fi înlocuite prin implementarea hardware efectivă;

b) sistemul de operare;

c) programe utilitare - asigură facilități comune şi frecvent utilizate, cum ar fi funcții automatizate de birou, sisteme de gestiune a bazelor de date, compilatoare de programe, sortare şi concatenare de fişiere, 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 şi 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 şi de alocare a identificatorilor utilizatorilor, proceduri de ştergere 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 şi schimbare, autoritatea emitentă, păstrarea înregistrărilor de control şi de către cine, frecvența schimbării şi procedurile utilizate pentru mecanismul de autentificare;

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

d) evidența versiunii sistemului de operare, programelor utilitare şi 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 şi documentația necesară;

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

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

a) responsabilități pentru generare şi utilizare;

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

c) clasificarea;

d) controlul copierii;

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

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

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

h) proceduri care trebuie urmate în caz de erori şi 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 şi mecanismelor de protecție împotriva software-ului malițios, atât manuale, cât şi automate, şi 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 şi a programelor utilitare, privind prezența viruşilor sau a altui software malițios, incluzând proceduri pentru ştergerea acestora în cazul detectării lor;

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

c) proceduri pentru verificarea mesajelor electronice şi a ataşamentelor 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 viruşi atât către expeditorul mediului de stocare infectat, cât şi la AAS, folosindu-se formularul din Directiva privind managementul INFOSEC pentru sisteme informatice şi de comunicații - INFOSEC 3, aprobată prin Ordinul directorului general al Oficiului Registrului Național al Informațiilor Secrete de Stat nr. 484/2003.

Managementul şi auditul automat al securității

ART. 27

(1) Secțiunea "Managementul şi auditul automat al securității" conține un sumar al tuturor măsurilor şi procedurilor automate de management al securității, al procedurilor de audit, atât cele manuale, cât şi 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 şi detalii despre facilitățile de audit;

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

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

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

e) responsabilitățile persoanelor care trebuie să ruleze şi să valideze integritatea instrumentelor/programelor de management automat al securității şi să desfăşoare investigări şi 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 fişierelor 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 şi controlul procedurilor privind securitatea criptografică şi cerințele de certificare de securitate pentru această persoană;

b) stabilirea administratorului COMSEC, conform INFOSEC 1 şi instrucțiunilor privind managementul, utilizarea şi 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 şi protecția materialului criptografic în România, pentru detalii în ceea ce priveşte măsurile de protecție a materialului criptografic şi 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 şi 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 şi 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 şi instalarea echipamentelor şi 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 şi certificare a echipamentelor şi 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 şi 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 şi pentru continuarea activității

ART. 31

(1) Cap. 6 "Planificarea măsurilor pentru situații de urgență şi pentru continuarea activității" din cuprinsul PrOpSec pentru AOSIC furnizează detalii despre procedurile obişnuite 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 şi a informațiilor utilizatorilor;

b) frecvența realizării salvărilor de siguranță;

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

d) testarea copiilor de back-up;

e) proceduri privind accesul la copiile de back-up şi 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 şi 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 viruşi 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 şi alte calamități naturale);

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

(3) Capitolul precizat la alin. (1) include, unde este cazul, proceduri cu privire la distrugerea echipamentelor criptografice şi 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 şi 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 şi auditul tuturor modificărilor efectuate în timpul etapelor de proiectare, dezvoltare, exploatare, întreținere şi 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 şi software:

a) responsabilitățile personalului pentru controlul şi 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 şi de implementare;

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

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

g) măsurile (tehnice, fizice şi 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 şi utilitarele;

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

i) procedurile pentru solicitarea modificării configurației hardware, firmware şi 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 şi 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.

CAP. 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.
