MONITORUL OFICIAL AL ROMÂNIEI

Anul 178 (XXII) — Nr. 92

PARTEA I
LEGI, DECRETE, HOTĂRÂRI ŞI ALTE ACTE

Miercuri, 10 februarie 2010

SUMAR

ACTE ALE ORGANELOR DE SPECIALITATE ALE ADMINISTRAȚIEI PUBLICE CENTRALE

GUVERNUL ROMÂNIEI
OFICIUL REGISTRULUI NAȚIONAL AL INFORMAȚIILOR SECRETE DE STAT

ORDIN
pentru aprobarea Directivei INFOSEC privind Catalogul național cu pachete, produse și profile de protecție INFOSEC—INFOSEC 5

În temeiul art. 1 alin. (4) lit. b) și al 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, și al 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 Directiva INFOSEC privind Catalogul național cu pachete, produse și profile de protecție INFOSEC—INFOSEC 5, prevăzută în anexa care face parte integrantă din prezentul ordin.

Art. 2. — Pe data intrării în vigoare a prezentului ordin se abrogă Ordinul directorului general al Oficiului Registrului Național al Informațiilor Secrete de Stat nr. 11/2006 pentru aprobarea Directivei INFOSEC privind Catalogul național cu produse, profile și pachete de protecție INFOSEC—INFOSEC 5, publicat în Monitorul Oficial al României, Partea I, nr. 135 din 13 februarie 2006.

Art. 3. — 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, 2 februarie 2010.
Nr. 7.

ANEXĂ

DIRECTIVA INFOSEC
privind Catalogul național cu pachete, produse și profile de protecție INFOSEC—INFOSEC 5

CAPITOLUL I
Scop

Art. 1. — Directiva INFOSEC privind Catalogul național cu pachete, produse și profile de protecție INFOSEC — INFOSEC 5 este elaborată de către Oficiul Registrului Național al Informațiilor Secrete de Stat, denumit în continuare *ORNISS,* ca parte a politicii naționale de protecție a informațiilor clasificate.

Art. 2. — Directiva stabilește procesul și procedurile de realizare, actualizare și păstrare a Catalogului național cu pachete, produse și profile de protecție INFOSEC, denumit în continuare *Catalog național.*

Art. 3. — Scopul Catalogului național este de a furniza persoanelor juridice de drept public sau privat care au în administrare sisteme informatice și de comunicații, denumite în continuare *SIC,* care vehiculează informații clasificate și altor entități care au responsabilități în domeniul protecției informațiilor clasificate o listă de pachete, produse și profile de protecție INFOSEC certificate, care pot fi achiziționate în scopul îndeplinirii cerințelor operaționale de securitate.

CAPITOLUL II
Definiții

Art. 4. — În sensul prezentei directive, următorii termeni se definesc după cum urmează:

a) *nivel de evaluare a asigurării (EAL)* — un pachet de componente de asigurare din partea a 3-a a Criteriilor comune, care reprezintă un punct pe scara de asigurare predefinită a Criteriilor comune;

b) *pachet* — un set reutilizabil de componente fie funcționale, fie de asigurare (de exemplu, un EAL), combinate pentru a satisface un set de obiective de securitate identificate;

c) *pachetele, produsele și profilele de protecție INFOSEC cu regim limitat de distribuție și utilizare* — acele pachete, produse și profile de protecție INFOSEC dezvoltate în serie limitată destinată strict utilizării în cadrul uneia sau mai multor autorități desemnate de securitate, denumite în continuare *ADS*;

d) *produs* — un pachet de software, firmware și/sau hardware IT care furnizează o funcționalitate destinată utilizării sau incorporării într-o multitudine de sisteme;

e) *profil de protecție (PP)* — un set de cerințe de securitate independent de implementare pentru o categorie de ținte de evaluare care satisface cerințe specifice ale consumatorilor;

f) *țintă de evaluare (TOE)* — un produs sau sistem IT și documentația aferentă de utilizator și administrator care constituie subiectul unei evaluări;

g) *țintă de securitate (ST)* — un set de cerințe și specificații de securitate utilizate ca bază pentru evaluarea unei ținte de evaluare identificate;

h) *utilizator* — orice entitate (utilizator uman sau entitate IT externă) din afara TOE care interacționează cu TOE.

CAPITOLUL III

Domeniul de aplicabilitate

Art. 5. — Prezenta directivă este obligatorie pentru persoanele juridice care prezintă pachete, produse și profile de protecție INFOSEC pentru a fi incluse în Catalogul național.

Art. 6. — (1) În raport cu destinația de utilizare, pachetele, produsele și profilele de protecție INFOSEC se împart în două categorii: cu utilizare la nivel național și cu regim limitat de distribuție și utilizare.

(2) Pachetele, produsele și profilele de protecție INFOSEC cu utilizare la nivel național se introduc în Catalogul național.

(3) Pachetele, produsele și profilele de protecție INFOSEC cu regim limitat de distribuție și utilizare se introduc în registrele de evidență a pachetelor, produselor și profilelor de protecție INFOSEC, constituite și păstrate la nivelul ADS cu competențe în coordonarea și controlul măsurilor de protecție a informațiilor clasificate ce vor fi protejate cu acestea.

(4) ADS transmit la ORNISS lista produselor cu regim limitat de distribuție și utilizare care pot fi puse la dispoziția altor ADS, precizând numele, destinația, modelul, versiunea și nivelul de clasificare pentru care au fost certificate, precum și eventualele condiții de utilizare.

CAPITOLUL IV

Responsabilități

Art. 7. — (1) În calitate de autoritate națională de securitate, ORNISS are responsabilitatea de a asigura implementarea prezentei directive.

(2) ORNISS este responsabil de coordonarea procesului de certificare a tuturor pachetelor, produselor, profilelor de protecție INFOSEC destinate protecției informațiilor naționale clasificate, care, după certificare, se includ în Catalogul național.

(3) ORNISS este responsabil de elaborarea, actualizarea și publicarea Catalogului național.

Art. 8. — Persoanele juridice care au pachete, produse sau profile de protecție INFOSEC certificate și care solicită ORNISS introducerea acestora în Catalogul național trebuie să pună la dispoziție toate informațiile necesare desfășurării acestui proces, referitoare la:

a) obiectivele de securitate;

b) cerințele funcționale;

c) categoriile de ținte de evaluare.

Art. 9. — Dacă până la expirarea perioadei de valabilitate a certificării elementelor incluse în Catalogul național nu se ia o decizie cu privire la recertificarea acestora, pachetul, produsul, profilul de protecție INFOSEC respectiv este scos de pe listă.

Art. 10. — (1) ADS care au certificat pachete, produse și profile de protecție INFOSEC cu regim limitat de distribuție au obligația de a actualiza registrele de evidență a acestora ori de câte ori este necesar.

(2) Pachetele, produsele și profilele de protecție INFOSEC sunt incluse în registrul de evidență numai după certificarea lor.

(3) Certificarea pachetelor, produselor și profilelor de protecție INFOSEC cu regim limitat de distribuție și utilizare se realizează în cadrul ADS, de către structura internă INFOSEC acreditată de ORNISS, ce are competențe privind coordonarea și controlul măsurilor de protecție a informațiilor clasificate, pe baza raportului de evaluare realizat de entitatea evaluatoare acreditată de ORNISS.

(4) În cazul în care în cadrul ADS nu există structura INFOSEC prevăzută la alin. (3), certificarea se realizează de către ORNISS.

CAPITOLUL V

Conținutul Catalogului național

Art. 11. — Catalogul național conține următoarele categorii de liste:

a) produse și mecanisme criptografice;

b) dispozitive de încărcare a cheilor criptografice;

c) produse pentru securitatea emisiilor;

d) produse pentru securitatea tehnologiei informației (IT);

e) instrumente de securitate;

f) pachete și profile de protecție.

Art. 12. — În cadrul listelor prevăzute la art. 11 pot fi incluse în Catalogul național următoarele tipuri de pachete, produse, profile de protecție INFOSEC:

a) dezvoltate pe plan național, evaluate de entități naționale acreditate de ORNISS și certificate de ORNISS;

b) certificate într-un stat membru NATO sau UE ori de către structuri specializate din cadrul NATO sau UE, particularizate și certificate pe plan național;

c) certificate într-un stat membru NATO sau UE;

d) certificate de structurile specializate din cadrul NATO sau UE;

e) certificate conform Criteriilor comune de evaluare de securitate a tehnologiei informației;

f) certificate în alte state decât cele membre ale NATO sau UE.

Art. 13. — Includerea în Catalogul național a pachetelor, produselor și profilelor de protecție INFOSEC utilizate la nivel național se poate face ca urmare a:

a) certificării naționale de către ORNISS a produselor dezvoltate integral în România;

b) certificării de către ORNISS a modului de implementare a acestora în scopul particularizării naționale a pachetelor, produselor și profilelor de protecție INFOSEC certificate într-un stat membru NATO sau UE ori de către structuri specializate din cadrul NATO sau UE;

c) recunoașterii naționale de către ORNISS a certificării produselor NATO și/sau UE;

d) recunoașterii naționale de către ORNISS a certificării conforme Criteriilor comune de evaluare de securitate a tehnologiei informației;

e) recunoașterii reciproce de către ORNISS a certificărilor naționale, prin înțelegeri, acorduri, aranjamente bilaterale, încheiate la nivel guvernamental sau departamental.

Art. 14. — Certificarea sau recunoașterea certificării produselor destinate protecției informațiilor naționale clasificate care se includ în Catalogul național se realizează în conformitate cu normele aprobate prin ordin al directorului general al ORNISS.

SECȚIUNEA 1

Produse și mecanisme criptografice

Art. 15. — Produsele și mecanismele criptografice din Catalogul național se utilizează în funcție de tipul, clasa și nivelul informațiilor clasificate, respectiv naționale, NATO, UE ori ale statelor sau organizațiilor internaționale cu care România a încheiat tratate, înțelegeri sau acorduri care prevăd protecția informațiilor clasificate, conform certificării acestora și mențiunilor din Catalogul național.

Art. 16. — Pentru protecția criptografică a informațiilor naționale clasificate procesate, stocate sau transmise în format electronic se utilizează numai produse și mecanisme criptografice certificate și incluse în Catalogul național sau în registrele de evidență a produselor cu regim limitat de distribuție,

în urma evaluării acestora de către entități evaluatoare naționale acreditate de ORNISS.

Art. 17. — (1) ORNISS emite un document de aprobare pentru includerea produselor și mecanismelor criptografice în lista produselor și a mecanismelor criptografice din cuprinsul Catalogului național.

(2) Documentul de aprobare specifică:

a) tipul, clasa și nivelul de secretizare a informațiilor clasificate pentru care sunt destinate produsele;

b) cerințele de utilizare.

SECȚIUNEA a 2-a

Dispozitive de încărcare a cheilor criptografice

Art. 18. — (1) Lista dispozitivelor de încărcare a cheilor criptografice conține dispozitive care sunt aprobate pentru stocarea, procesarea sau transmiterea materialului cu chei criptografice național, NATO, UE ori care fac obiectul tratatelor, înțelegerilor și acordurilor bilaterale sau multilaterale la care România este parte.

(2) Dispozitivele sunt grupate în două categorii, astfel:

a) dispozitive care gestionează cheile în formă clară;

b) dispozitive care aplică un mecanism criptografic ce permite stocarea, procesarea și transmiterea cheii în formă criptată.

Art. 19. — Sunt eligibile spre a fi incluse în Catalogul național numai dispozitivele de încărcare a cheilor criptografice care sunt dezvoltate la nivel național ori într-un stat membru NATO sau UE și care sunt evaluate și aprobate în conformitate cu politica națională, respectiv NATO sau UE, de protecție a informațiilor clasificate.

SECȚIUNEA a 3-a

Produse pentru securitatea emisiilor

Art. 20. — (1) În cadrul Catalogului național, lista produselor pentru securitatea emisiilor cuprinde:

a) lista producătorilor naționali, precum și modelele de produse dezvoltate la nivel național, produse evaluate de o entitate națională acreditată de ORNISS și certificate de ORNISS ca fiind corespunzătoare categoriilor de produse TEMPEST, prevăzute de standardele TEMPEST în vigoare;

b) lista producătorilor externi, precum și modelele de produse recomandate de NATO;

c) lista producătorilor externi, precum și a modelelor de produse certificate din punctul de vedere al protecției TEMPEST fie de ORNISS, fie de o entitate acreditată la nivel național în țara de origine a echipamentelor, cu condiția ca între ORNISS și țara de origine să existe o înțelegere în acest sens.

(2) Schimbarea de componente între diferite serii de producție poate schimba profilul de protecție, ceea ce implică reevaluarea produsului.

SECȚIUNEA a 4-a

Produse de securitate IT

Art. 21. — Scopul listei cu produse de securitate IT din cadrul Catalogului național este să furnizeze autorităților operaționale ale sistemelor informatice și de comunicații (AOSIC), structurilor de planificare și implementare a sistemelor informatice și de comunicații, personalului implicat în proiect și utilizatorilor sistemelor informatice și de comunicații care vehiculează informații clasificate secret de stat un set de produse certificate și de informații de bază referitoare la acestea, set care poate fi folosit drept ghid în vederea îndeplinirii cerințelor naționale de securitate privind protecția informațiilor clasificate.

Art. 22. — (1) Produsele din lista prevăzută la art. 21 sunt evaluate și certificate în baza Criteriilor comune pentru evaluarea securității produselor IT (ISO 15408).

(2) Fiecărui produs i se atribuie un pachet de componente de asigurare, de exemplu, un nivel de încredere (EAL sau echivalent).

(3) În cazul în care un produs a fost evaluat sau propus spre evaluare în baza unui set de criterii naționale, trebuie să fie furnizate detalii privind corespondențele dintre criteriile naționale și Criteriile comune.

Art. 23. — (1) Produsele din listă pot fi împărțite în următoarele categorii, fără a se limita la acestea:

a) dispozitive și sisteme de control al accesului;

b) dispozitive și sisteme de protecție a perimetrului;

c) baze de date;

d) dispozitive și sisteme de detecție a intruziunilor;

e) semnătură digitală;

f) protecția datelor;

g) circuite integrate, dispozitive și sisteme Smart Card;

h) sisteme de management al cheilor;

i) rețele, sisteme și dispozitive de rețea;

j) sisteme de operare;

k) alte dispozitive și sisteme.

(2) Produsele cu modul criptografic încorporat pot fi incluse în listă în mai multe categorii sau sub o altă categorie decât criptografia (de exemplu, un sistem de operare nu va fi numit produs criptografic, deși face uz de criptografie).

Art. 24. — Informațiile necesare includerii în listă a produselor pentru securitate IT conțin cel puțin următoarele elemente, după caz:

a) denumirea și producătorul;

b) informații descriptive privind produsul, care vor include: funcționalitatea produsului și pachetul componentelor de siguranță (de exemplu, un nivel de încredere);

c) raport de certificare;

d) acord de recunoaștere reciprocă;

e) versiunile Criteriilor comune și Metodologiei comune de evaluare utilizate.

SECȚIUNEA a 5-a

Instrumente de securitate

Art. 25. — Lista instrumentelor de securitate din cadrul Catalogului național se adresează autorităților operaționale ale sistemelor informatice și de comunicații (AOSIC), structurilor de planificare și implementare a sistemelor informatice și de comunicații și personalului implicat în proiectarea sistemelor informatice și de comunicații. Aceasta este o listă a instrumentelor de securitate conforme cu prevederile Directivei INFOSEC tehnice și de implementare privind cerințele instrumentelor de securitate, selectarea, aprobarea și implementarea acestora – INFOSEC 9, aprobată prin Ordinul directorului general al Oficiului Registrului Național al Informațiilor Secrete de Stat nr. 390/2004, publicat în Monitorul Oficial al României, Partea I, nr. 1.081 din 19 noiembrie 2004.

Art. 26. — Lista include următoarele tipuri de instrumente:

a) instrumente pentru identificarea vulnerabilităților sistemelor;

b) instrumente pentru îmbunătățirea securității sistemului;

c) instrumente pentru detectarea intruziunilor;

d) instrumente pentru raportarea stării sistemului;

e) instrumente pentru monitorizarea traficului din rețea;

f) instrumente pentru administrarea sistemului.

Art. 27. — Descrierea fiecărui instrument trebuie să includă următoarele informații:

a) denumirea și producătorul;

b) caracteristicile funcționale;

c) beneficiile care vor fi obținute în urma utilizării instrumentului;

d) vulnerabilitățile, dacă este cazul, care apar prin utilizarea instrumentului;

e) constrângeri privind utilizarea instrumentului;

f) resurse/experiența/suportul/pregătirea necesare operării.

Art. 28. — Lista instrumentelor de securitate nu include detaliile cu privire la vulnerabilități. Lista face referire doar la raportul de evaluare a instrumentului. Informațiile privind vulnerabilitățile sunt puse la dispoziție numai acelor autorități ale sistemelor informatice și de comunicații și de securitate care au o „nevoie de a cunoaște" corespunzătoare.

SECȚIUNEA a 6-a

Pachete și profile de protecție

Art. 29. — Solicitantul trebuie să furnizeze cel puțin următoarele informații:

a) denumirea pachetului/profilului de protecție și a producătorului;

b) o declarație din care să reiasă dacă pachetul sau profilul de protecție este propus ca o nouă poziție în listă ori ca înlocuire a unei poziții din listă;

c) mențiuni speciale, în situația în care pachetul sau profilul de protecție conțin informații clasificate, care intră sub incidența drepturilor de autor/proprietate intelectuală sau care nu pot fi făcute publice.

Art. 30. — Informațiile necesare includerii în listă a pachetelor/profilelor de protecție vor trata cel puțin aspectele privitoare la:

a) denumirea pachetului/profilului de protecție;

b) autor;

c) autoritatea de certificare;

d) entitatea care a efectuat evaluarea;

e) nivelul de încredere;

f) data certificării;

g) versiunile Criteriilor comune și ale Metodologiei comune de evaluare utilizate.

CAPITOLUL VI

Gestionarea Catalogului național

Art. 31. — Catalogul național este actualizat periodic, pe măsura certificării de noi produse naționale și în conformitate cu modificările survenite în listele cu produse recomandate de NATO sau UE.

Art. 32. — Catalogul național este distribuit de ORNISS persoanelor juridice de drept public sau privat îndreptățite.

Art. 33. — ORNISS va conlucra în mod continuu cu producătorii naționali de produse INFOSEC pentru a asigura informațiile necesare pentru fiecare pachet, produs ori profil de protecție care urmează să fie adăugat în catalog sau pentru orice produs care trebuie să fie îndepărtat din catalog.

GUVERNUL ROMÂNIEI

OFICIUL REGISTRULUI NAȚIONAL AL INFORMAȚIILOR SECRETE DE STAT

O R D I N

privind aprobarea Metodologiei de evaluare și certificare a pachetelor, produselor și profilelor de protecție INFOSEC—INFOSEC 14

În temeiul art. 1 alin. (4) lit. b) și al 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, și al 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 următorul ordin:

Art. 1. — Se aprobă Metodologia de evaluare și certificare a pachetelor, produselor și profilelor de protecție INFOSEC—INFOSEC 14, prevăzută în anexa care face parte integrantă din prezentul ordin.

Art. 2. — Pe data intrării în vigoare a prezentului ordin se abrogă Ordinul directorului general al Oficiului Registrului Național al Informațiilor Secrete de Stat nr. 181/2006 pentru aprobarea Metodologiei de evaluare și certificare a produselor, profilelor și pachetelor de protecție INFOSEC—INFOSEC 14, publicat în Monitorul Oficial al României, Partea I, nr. 444 din 23 mai 2006, cu modificările ulterioare.

Art. 3. — 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, 2 februarie 2010.
Nr. 8.

ANEXĂ

M E T O D O L O G I A
de evaluare și certificare a pachetelor, produselor și profilelor de protecție INFOSEC—INFOSEC 14

1. **Introducere**

1.1. **Scop**

Art. 1. — Prezenta metodologie stabilește activitățile aferente proceselor de evaluare și certificare a pachetelor, produselor și profilelor de protecție INFOSEC, denumite în continuare *produse INFOSEC,* destinate protecției informațiilor naționale clasificate, vehiculate în sistemele informatice și de comunicații naționale, civile și militare.

Art. 2. — Procesele de evaluare și certificare a produselor INFOSEC au următoarele obiective:

a) crearea posibilității de utilizare a unor produse INFOSEC în sisteme informatice și de comunicații care vehiculează informații clasificate;

b) verificarea și confirmarea nivelului de încredere ce poate fi acordat funcțiilor de securitate ale unui produs INFOSEC;

c) stabilirea unei baze de comparație între diferite produse INFOSEC;

d) perfecționarea procedurilor naționale de evaluare a produselor INFOSEC.

1.2. **Definiții**

Art. 3. — În sensul prezentei metodologii, următorii termeni și sintagme se definesc după cum urmează:

a) *certificare* — emiterea unui document oficial, bazat pe o analiză independentă a unei evaluări și a rezultatelor acestei evaluări, conform căruia produsul evaluat satisface parametrii de securitate predefiniți. Prin certificare se analizează rezultatele evaluării și se stabilește dacă criteriile și metodele de evaluare au fost aplicate în mod corect. Procesul de certificare verifică uniformitatea și corectitudinea procedurilor de evaluare, precum și consecvența și compatibilitatea rezultatelor evaluării;

b) *evaluare* —— examinarea detaliată, din punct de vedere tehnic și funcțional, a aspectelor de securitate ale produselor INFOSEC. Prin procesul de evaluare se verifică cel puțin:

(i) prezența facilităților/funcțiilor de securitate cerute;
(ii) absența efectelor secundare compromițătoare care ar putea decurge din implementarea facilităților de securitate;
(iii) funcționalitatea globală a produsului INFOSEC;
(iv) nivelul de încredere al produsului INFOSEC;

c) *imparțialitate* — principiu conform căruia nu există factori care pot influența desfășurarea procesului de evaluare și rezultatele acestui proces;

d) *nivel de evaluare a asigurării (EAL)* — un pachet de componente de asigurare din partea a 3-a a Criteriilor comune, care reprezintă un punct pe scara de asigurare predefinită a Criteriilor comune;

e) *obiectivitate* — principiu conform căruia rezultatele unor teste de evaluare trebuie să se bazeze pe fapte concrete, nu pe opiniile subiective ale evaluatorului. Obiectivitatea poate fi consolidată, prin supunerea produsului la cel puțin două evaluări realizate de entități independente (reproductibilitate);

f) *pachet* — un set reutilizabil de componente fie funcționale, fie de asigurare (de exemplu, un EAL), combinate pentru a satisface un set de obiective de securitate identificate;

g) *produs* — un pachet de software, firmware și/sau hardware IT, care furnizează o funcționalitate destinată utilizării sau incorporării într-o multitudine de sisteme;

h) *profil de protecție* — un set de cerințe de securitate independent de implementare pentru o categorie de TOE care satisface cerințe specifice ale consumatorilor;

i) *repetabilitate* — principiu conform căruia repetarea evaluării aceluiași produs, în funcție de aceeași țintă de securitate, de către aceeași entitate evaluatoare, conduce la un rezultat similar cu cel obținut ca urmare a primei evaluări a produsului;

j) *reproductibilitate* — principiu conform căruia repetarea evaluării aceluiași produs, în funcție de aceeași țintă de securitate, de către o altă entitate evaluatoare, conduce la un rezultat similar cu cel obținut ca urmare a primei evaluări a produsului;

k) *solicitant* — persoană juridică de drept public sau privat care solicită evaluarea, certificarea și aprobarea de includere în Catalogul național cu produse, profile și pachete de protecție a unui produs INFOSEC. Solicitantul poate fi și o altă persoană juridică diferită de producător (de exemplu, dezvoltator, utilizator, comerciant, integrator);

l) *țintă de evaluare (TOE)* — un produs sau sistem IT și documentația aferentă de utilizator și administrator care constituie subiectul unei evaluări;

m) *țintă de securitate (ST)* — un set de cerințe și specificații de securitate utilizate ca bază pentru evaluarea unei TOE identificate.

Art. 4. — Procesul de evaluare a produselor INFOSEC se desfășoară prin parcurgerea următoarelor etape, așa cum sunt prezentate în figura nr. 1:

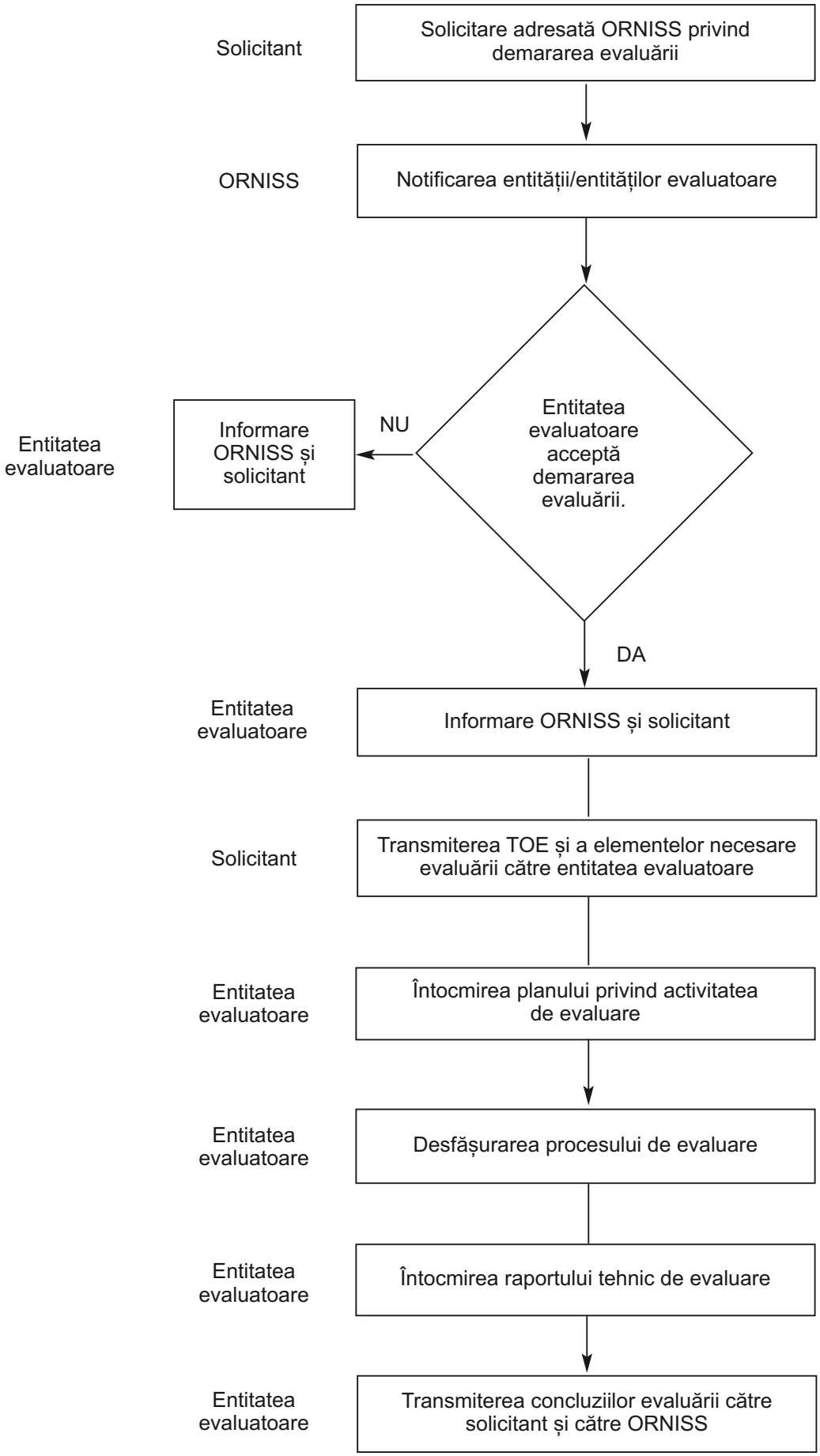

Figura nr. 1 — Schema procesului de evaluare a securității produselor INFOSEC utilizate în sistemele informatice și de comunicații care vehiculează informații naționale clasificate

2. **Descrierea metodologiei de evaluare**

2.1. **Etapa 1: Demararea procesului de evaluare**

Art. 5. — În vederea demarării procesului de evaluare a unui produs INFOSEC, persoanele juridice trebuie să adreseze Oficiului Registrului Național al Informațiilor Secrete de Stat, denumit în continuare *ORNISS,* o solicitare scrisă în acest sens.

Art. 6. — Solicitarea de demarare a procesului de evaluare trebuie să fie însoțită de documentație care să precizeze cel puțin următoarele aspecte:

a) descrierea generală a produsului pentru care se solicită evaluarea;

b) ținta de securitate;

c) clasa și, după caz, nivelul de secretizare pentru care se dorește a fi utilizat produsul;

d) manualul de administrare și utilizare (hârtie/electronic);

e) numele entității/entităților evaluatoare acreditate de ORNISS, selectată(e) de solicitant pentru realizarea evaluării;

f) copii de pe certificate anterioare, dacă este cazul.

Art. 7. — (1) În cazul produselor criptografice destinate protecției informațiilor naționale clasificate, altele decât cele din categoria cifrului de stat, se aplică cerințele de evaluare și certificare prevăzute în anexa nr. 1.

(2) În cazul celorlalte produse INFOSEC, altele decât cele criptografice, ORNISS decide cu privire la certificare în baza analizei rezultatelor prezentate de o singură entitate evaluatoare acreditată de ORNISS.

(3) În situații excepționale, când se apreciază că există o amenințare semnificativă la adresa securității sistemelor informatice și de comunicații naționale, astfel încât există riscul major de prejudiciere în mod deosebit de grav a intereselor naționale, ORNISS poate decide asupra necesității unor evaluări suplimentare a produselor INFOSEC, altele decât cele criptografice prevăzute la alin. (1).

Art. 8. — Agenția de Securitate pentru Informatică și Comunicații din cadrul ORNISS analizează solicitarea primită.

Art. 9. — În cazul în care se constată că datele cuprinse în cererea de certificare sau în documentația anexată nu sunt complete, ORNISS informează solicitantul, în vederea furnizării informațiilor adiționale necesare.

Art. 10. — Dacă cererea conține toate datele menționate, ORNISS notifică entitatea/entitățile evaluatoare cu privire la selectarea acesteia/acestora de către solicitant pentru efectuarea evaluării. Notificarea transmisă de ORNISS include toate datele primite de la solicitant.

Art. 11. — (1) După analiza documentației prevăzute la art. 6, entitatea/entitățile evaluatoare notifică ORNISS cu privire la acceptarea sau neacceptarea realizării procesului de evaluare.

(2) ORNISS notifică solicitantului cu privire la decizia comunicată de entitatea/entitățile evaluatoare.

Art. 12. — (1) În cazul în care entitatea evaluatoare acceptă să demareze procesul de evaluare, solicitantul pune la dispoziția entității evaluatoare cel puțin următoarele elemente:

a) produsul de evaluat, incluzând:

(i) componentele hardware, software și firmware;

(ii) eventual alte componente necesare realizării infrastructurii de testare;

b) documentație tehnică, care, în funcție de tipul produsului, trebuie să includă cel puțin:

(i) documentație tehnică, proceduri operaționale de securitate;

(ii) descrierea arhitecturii fizice și logice;

(iii) specificații algoritm, cod sursă, mod de lucru, vectori de test, în cazul produselor criptografice;

(iv) descrierea parametrilor critici de securitate;

c) teste proprii, platforme de testare și documentație aferentă incluzând rezultatele testelor anterioare;

d) în cazul în care există certificări anterioare, se vor furniza și rapoartele tehnice de evaluare.

(2) În funcție de tipul informațiilor care trebuie puse la dispoziția entității evaluatoare, între solicitant și entitatea evaluatoare se poate încheia un acord de confidențialitate, în baza căruia aceste informații sunt transmise.

Art. 13. — Procesul de evaluare se consideră demarat după încheierea unui document de acceptare (contract, acord etc.) între solicitant și entitatea evaluatoare.

Art. 14. — Evaluatorul întocmește lista cu elementele necesare evaluării și stabilește datele la care acestea trebuie să îi fie puse la dispoziție.

Art. 15. — În cazul în care solicitantul evaluării nu este același cu producătorul produsului supus evaluării, în vederea asigurării protecției unor informații specifice, acestea pot fi puse la dispoziția evaluatorului direct de către producător.

Art. 16. — Este important ca obiectivele evaluării să fie clar definite de solicitant, înțelese de evaluator și transmise către toate părțile implicate în procesul de evaluare a produsului. Persoana responsabilă cu coordonarea procesului de evaluare trebuie să verifice că toate persoanele implicate în acest proces cunosc scopul și obiectivele evaluării, precum și responsabilitățile pe care le au în acest proces.

2.2. **Etapa 2: Desfășurarea procesului de evaluare**

2.2.1. ***Elemente generale***

Art. 17. — Evaluarea produselor INFOSEC se realizează de către entități evaluatoare acreditate de ORNISS, în conformitate cu prevederile Metodologiei de acreditare a entităților pentru evaluarea produselor de securitate IT și a sistemelor informatice și de comunicații — INFOSEC 12, aprobate prin Ordinul directorului general al Oficiului Registrului Național al Informațiilor Secrete de Stat nr. 167/2006.

Art. 18. — (1) Procesul de evaluare a produselor INFOSEC se desfășoară pe baza a 3 elemente:

a) criterii;

b) metodologie;

c) modul de derulare a proceselor de evaluare și certificare de securitate.

(2) Criteriile reprezintă normele și principiile față de care poate fi măsurată securitatea unui produs INFOSEC, în vederea evaluării, dezvoltării și achiziției, iar metodologia stabilește modul în care trebuie realizată evaluarea, în baza criteriilor.

Art. 19. — Evaluarea securității pe care o pot asigura produsele INFOSEC se realizează în conformitate cu standarde naționale sau standarde internaționale recunoscute pe plan național, agreate de statele membre ale NATO sau UE.

2.2.2. ***Obiectivele evaluării***

Art. 20. — Obiectivul principal al procesului de evaluare de securitate constă în verificarea faptului că funcțiile de securitate ale produsului sunt conforme cu ținta de securitate.

Art. 21. — Procesul de evaluare de securitate asigură un anumit nivel de încredere în faptul că produsul nu prezintă vulnerabilități care pot fi exploatate.

Art. 22. — În contextul evaluării și certificării produselor INFOSEC, trebuie acordată o atenție deosebită principiilor repetabilității, reproductibilității, imparțialității și obiectivității.

Art. 23. — Respectarea acestor 4 principii trebuie să fie verificată de ORNISS în cursul procesului de certificare.

2.2.3. ***Întocmirea planului de activități privind evaluarea***

Art. 24. — Pentru a descrie structura unui proces de evaluare, precum și conexiunile dintre diferitele activități aferente procesului, evaluatorul trebuie să întocmească un plan de activități privind evaluarea, denumit în continuare *PAE.*

Art. 25. — PAE trebuie să descrie modul în care sunt organizate activitățile legate de procesul de evaluare și interrelaționarea acestor activități.

Art. 26. — PAE trebuie întocmit astfel încât să fie aplicabil atât pentru evaluarea unei game de produse, cât și pentru diferite niveluri ale evaluării.

Art. 27. — Acest document oferă o prezentare generală asupra modului în care trebuie realizată evaluarea, în conformitate cu criterii și metodologii de evaluare specifice.

2.2.4. ***Desfășurarea evaluării***

Art. 28. — Activitatea entității evaluatoare trebuie să fie conformă cu cerințele standardelor de calitate și cu criteriile stabilite în Metodologia de acreditare a entităților pentru evaluarea produselor de securitate IT și a sistemelor informatice și de comunicații — INFOSEC 12, aprobate prin Ordinul directorului general al Oficiului Registrului Național al Informațiilor Secrete de Stat nr. 167/2006.

Art. 29. — Procesul de evaluare trebuie să includă cel puțin următoarele activități:

a) verificarea faptului că elementele necesare evaluării sunt conforme cu cerințele criteriilor de evaluare;

b) verificarea faptului că cerințele de securitate specificate în ținta de securitate sunt implementate în mod adecvat;

c) verificarea faptului că produsul operațional nu prezintă vulnerabilități exploatabile.

Art. 30. — Prezenta metodologie stabilește cadrul general al activităților legate de procesul de evaluare și certificare, iar la implementarea sa trebuie ținut cont de faptul că pentru fiecare produs specific pot fi necesare diferite activități și niveluri de evaluare.

Art. 31. — Lista demonstrativă cu activități aferente procesului de evaluare este prevăzută în anexa nr. 2.

Art. 32. — Observațiile și rezultatele fiecărei activități din procesul de evaluare trebuie consemnate într-un raport tehnic de evaluare, denumit în continuare *RTE.*

Art. 33. — Pe toată durata procesului de evaluare oricare dintre părțile implicate poate solicita organizarea unor ședințe de lucru sau informații suplimentare pentru clarificarea aspectelor de natură tehnică.

Art. 34. — În situația în care unele activități aferente procesului de evaluare impun efectuarea unor teste la sediul solicitantului sau dezvoltatorului, producătorului sau utilizatorului produsului, acestea trebuie să se realizeze în baza unor înțelegeri scrise între părțile implicate și, în cazul unor testări clasificate secret de stat, notificarea prealabilă a ORNISS.

Art. 35. — În cazul în care ORNISS consideră necesar, poate participa la testele efectuate la sediul solicitantului sau dezvoltatorului.

Art. 36. — În cazul în care evaluarea este întreruptă din diferite cauze (rezilierea contractului/încetarea acordului), entitatea evaluatoare trebuie să notifice ORNISS cu privire la acest lucru.

2.3. **Etapa 3: Finalizarea procesului de evaluare**

2.3.1. ***Întocmirea RTE***

Art. 37. — La finalul activităților de evaluare, evaluatorul are obligația să întocmească un RTE.

Art. 38. — RTE are următoarea structură:

a) descrierea activităților desfășurate în procesul de evaluare;

b) prezentarea rezultatelor obținute și a concluziilor rezultate din activitățile desfășurate.

Art. 39. — RTE se adresează, în principal:

a) ORNISS, în calitate de certificator;

b) solicitantului evaluării;

c) entității de evaluare, în vederea pregătirii altor activități de evaluare.

Art. 40. — În cazul în care dezvoltatorul produsului nu este totodată și solicitantul evaluării, există posibilitatea transmiterii anumitor părți din RTE către dezvoltator, dar numai cu acordul solicitantului evaluării.

Art. 41. — Modelul RTE, cu detalierea conținutului fiecărui capitol sau fiecărei secțiuni, este prevăzut în anexa nr. 3.

Art. 42. — (1) În vederea certificării produsului INFOSEC, entitatea evaluatoare transmite la ORNISS un document de sinteză a RTE, care să cuprindă cel puțin următoarele elemente:

a) denumirea și descrierea caracteristicilor funcționale și de securitate ale produsului evaluat;

b) configurația și condițiile în care a fost testat produsul;

c) standardele și metodologiile în conformitate cu care s-a realizat testarea și evaluarea produsului;

d) testele realizate și rezultatele acestora;

e) concluziile finale ale procesului de evaluare;

f) condiții și termene de valabilitate a rezultatelor testării, eventuale cerințe/condiții/instrucțiuni de utilizare a produsului, astfel încât să se asigure păstrarea caracteristicilor de securitate și funcționale;

g) numărul RTE întocmit.

(2) Pentru clarificarea unor aspecte specifice, ORNISS poate solicita entității evaluatoare să îi pună la dispoziție o copie a RTE.

3. **Descrierea metodologiei de certificare**

3.1. **Demararea procesului de certificare**

Art. 43. — Principalul obiectiv al certificării este acela de a furniza o confirmare independentă a faptului că procesul de evaluare a fost realizat în mod corect, în conformitate cu criteriile, procedurile și metodologiile recunoscute și rezultatele evaluării sunt conforme cu elementele constatate. Totodată, certificarea are rolul de a crea un climat de încredere și de a confirma faptul că entitățile evaluatoare operează în conformitate cu aceleași standarde și că rezultatele obținute de oricare dintre entitățile evaluatoare sunt demne de încredere în egală măsură.

Art. 44. — Încrederea trebuie să aibă la bază respectarea principiilor imparțialității, obiectivității, repetabilității și reproductibilității.

Art. 45. — O descriere schematică a procesului de certificare este prezentată în figura nr. 2.

Art. 46. — (1) Demararea procesului de certificare se realizează printr-o solicitare adresată ORNISS de către solicitant.

(2) Solicitarea trebuie să fie însoțită de raportul sau, după caz, rapoartele tehnic(e) de evaluare a produsului, emis(e) de entitatea/entitățile evaluatoare selectate.

(3) În cazul în care documentația nu este completă, ORNISS notifică solicitantului, specificând elementele care trebuie completate.

Art. 47. — În cadrul etapei de certificare de securitate, ORNISS, prin Agenția de Securitate pentru Informatică și Comunicații, realizează o analiză independentă a rezultatelor obținute în urma etapei de evaluare, precum și a modalității în care s-a desfășurat această activitate.

Art. 48. — Procesul de certificare trebuie să analizeze următoarele aspecte:

a) criteriile, metodologiile și procedurile de lucru utilizate în procesul de evaluare;

b) resursele folosite în cadrul evaluării de securitate (echipamente, documentație, timp etc.);

c) personalul care a realizat evaluarea de securitate (calificare, obiectivitate, imparțialitate etc.);

d) rezultatele testelor de evaluare;

e) RTE.

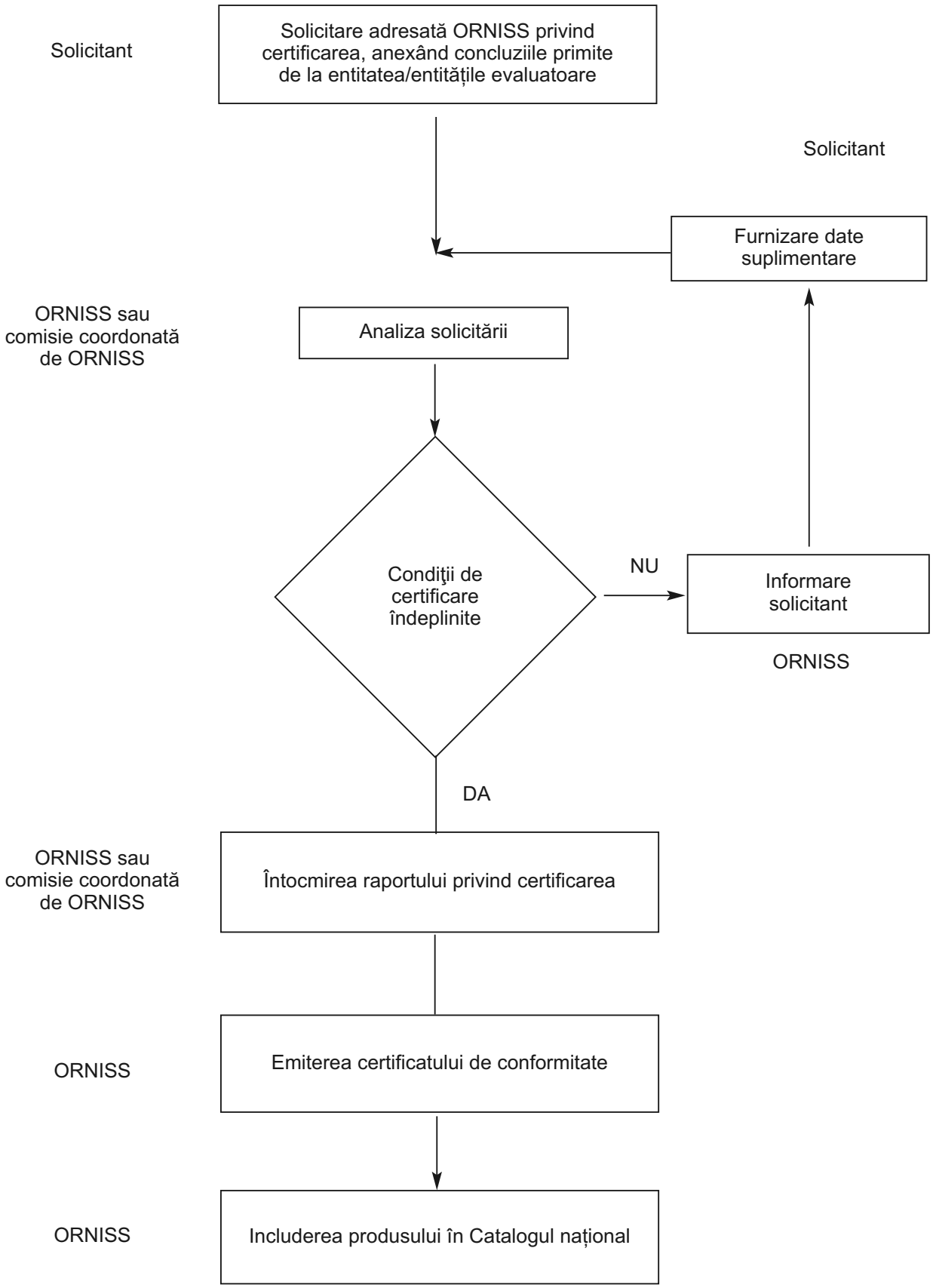

Figura nr. 2 — Schema procesului de certificare a produselor INFOSEC utilizate în sistemele informatice și de comunicații care vehiculează informații naționale clasificate

3.2. **Întocmirea raportului privind certificarea**

Art. 49. — Rezultatele activității de certificare trebuie să facă obiectul unui raport privind certificarea.

Art. 50. — Raportul privind certificarea trebuie să identifice în mod clar produsul și să conțină recomandări cu privire la decizia privind certificarea produsului evaluat.

Art. 51. — Dacă în urma analizei documentației puse la dispoziție în vederea certificării se constată că atât rezultatele obținute în urma activității de evaluare, cât și modalitatea în care aceasta s-a realizat sunt conforme standardelor și normelor în vigoare, precum și faptul că produsul îndeplinește cerințele de securitate conform țintei de securitate, raportul privind certificarea include propuneri privind certificarea produsului.

Art. 52. — În cazul în care în urma analizei se constată deficiențe în procesul de evaluare a produsului, atunci ORNISS notifică entității evaluatoare, în vederea remedierii acestor deficiențe.

Art. 53. — Pentru desfășurarea corespunzătoare a etapei de certificare, Agenția de Securitate pentru Informatică și Comunicații poate solicita entității evaluatoare alte documente cu relevanță pentru această activitate.

Art. 54. — Raportul privind certificarea va fi elaborat în termen de maximum 30 de zile de la primirea documentului de sinteză emis de entitatea/entitățile evaluatoare pe baza RTE sau, după caz, a ultimului document solicitat de Agenția de Securitate pentru Informatică și Comunicații entității evaluatoare.

Art. 55. — Un set minim de elemente care trebuie să fie cuprinse în raportul privind certificarea este prevăzut în anexa nr. 4.

3.3. **Luarea deciziei privind certificarea produsului**

Art. 56. — După parcurgerea activităților necesare luării unei decizii privind certificarea unui produs, se desprind două variante posibile:

a) certificarea produsului și emiterea Certificatului de conformitate și aprobarea includerii în Catalogul național de pachete, produse și profile de protecție INFOSEC;

b) refuzul certificării — decizie datorată identificării unor deficiențe grave referitoare la atingerea de către produs a parametrilor de securitate predefiniți.

Art. 57. — Certificatul de conformitate emis de ORNISS confirmă faptul că produsul îndeplinește standardele de securitate în baza cărora a fost evaluat, pentru ținta de securitate propusă.

Art. 58. — Produsele certificate vor fi incluse în Catalogul național de pachete, produse și profile de protecție INFOSEC, cu ocazia următoarei actualizări a acestuia, în conformitate cu prevederile Directivei INFOSEC privind Catalogul național de pachete, produse și profile de protecție INFOSEC — INFOSEC 5, aprobată prin Ordinul directorului general al Oficiului Registrului Național al Informațiilor Secrete de Stat nr. 7/2010.

Art. 59. — Anexa nr. 5 cuprinde o bibliografie a unor acte normative și documente cu relevanță în domeniu.

Art. 60. — Anexele nr. 1—5 fac parte integrantă din prezenta metodologie.

ANEXA Nr. 1
la metodologie

C E R I N Ț E
de evaluare și certificare a sistemelor criptografice destinate protecției informațiilor naționale clasificate, altele decât cele din categoria cifrului de stat

Pentru protecția informațiilor naționale clasificate sunt utilizate sisteme criptografice evaluate și certificate, după cum urmează:

A. **Sisteme criptografice dezvoltate pe plan național**

a) Pentru protecția informațiilor clasificate SECRET DE SERVICIU, sistemele criptografice trebuie să fie:

(i) evaluate de o entitate evaluatoare acreditată de Oficiul Registrului Național al Informațiilor Secrete de Stat, denumit în continuare *ORNISS*; și

(ii) certificate de o comisie coordonată de ORNISS.

b) Pentru protecția informațiilor clasificate SECRET, sistemele criptografice trebuie să fie:

(i) evaluate de o entitate evaluatoare acreditată de ORNISS; și

(ii) certificate de ORNISS.

c) Pentru protecția informațiilor clasificate STRICT SECRET, sistemele criptografice trebuie să fie:

(i) evaluate de două entități evaluatoare acreditate de ORNISS; și

(ii) certificate de ORNISS;

(iii) în cazul în care nu există două entități evaluatoare acreditate care să aibă capacitatea de a realiza evaluarea, sistemele trebuie să fie:

1. evaluate de o entitate evaluatoare acreditată de ORNISS; și

2. certificate de o comisie coordonată de ORNISS și formată din reprezentanți ai tuturor entităților evaluatoare acreditate de ORNISS pentru a desfășura activități de evaluare criptografică.

d) Pentru protecția informațiilor clasificate STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ, sistemele criptografice trebuie să fie:

(i) evaluate de două entități evaluatoare acreditate de ORNISS; și

(ii) certificate de o comisie coordonată de ORNISS și formată din reprezentanți ai entităților evaluatoare implicate.

B. **Sisteme criptografice realizate de producători externi**

a) Pentru protecția informațiilor clasificate SECRET DE SERVICIU pot fi utilizate sistemele aflate în una dintre următoarele situații:

(i) certificate pentru cel puțin nivelul echivalent de clasificare de către una dintre următoarele:

1. structuri specializate ale NATO;

2. structuri specializate ale UE;

3. un stat membru NATO sau UE;

4. state cu care România a încheiat înțelegeri, acorduri, aranjamente bilaterale, la nivel guvernamental sau departamental;

(ii) evaluate de o entitate evaluatoare acreditată de ORNISS și certificate de o comisie coordonată de ORNISS.

b) Pentru protecția informațiilor clasificate SECRET pot fi utilizate sistemele aflate în una dintre următoarele situații:

(i) certificate pentru un nivel superior de clasificare de către una dintre următoarele:

1. structuri specializate ale NATO;

2. structuri specializate ale UE;

(ii) certificate pentru un nivel superior de clasificare de către structuri specializate din state membre NATO sau UE, evaluate de două entități evaluatoare acreditate de ORNISS și certificate de ORNISS;

(iii) certificate pentru un nivel superior de clasificare de către autorități competente din state cu care România a încheiat aranjamente de securitate privind recunoașterea reciprocă a certificatelor de conformitate pentru produse de securitate IT,

evaluate de două entități evaluatoare acreditate de ORNISS și certificate de ORNISS.

c) Pentru protecția informațiilor clasificate STRICT SECRET pot fi utilizate sisteme care îndeplinesc cumulativ următoarele cerințe:

(i) sunt modele certificate pentru un nivel echivalent de clasificare de către structuri ale NATO, UE, autorități competente din state membre NATO sau UE, state cu care România a încheiat aranjamente de securitate privind recunoașterea reciprocă a certificatelor de conformitate pentru produse de securitate IT;

(ii) particularizate prin implementarea de algoritmi criptografici naționali certificați;

(iii) evaluate de două entități evaluatoare acreditate de ORNISS;

(iv) certificate de ORNISS.

d) Pentru protecția informațiilor clasificate STRICT SECRET DE IMPORTANȚĂ DEOSEBITĂ nu este permisă utilizarea de sisteme criptografice realizate de producători externi.

Prin excepție de la prevederile lit. A și B, sistemele criptografice utilizate de autoritățile desemnate de securitate (*ADS*) pentru destinații specifice se evaluează de către o entitate evaluatoare acreditată de ORNISS și sunt certificate de către structura INFOSEC acreditată de ORNISS în cadrul ADS. În cazul în care nu există o structură INFOSEC acreditată, certificarea produselor se realizează de către ORNISS.

ANEXA Nr. 2
la metodologie

LISTA DEMONSTRATIVĂ
cu activități aferente procesului de evaluare

1. Prezentăm în continuare o listă exemplificativă cu activități aferente procesului de evaluare:

a) verificarea analizei de conformitate;

b) verificarea analizei caracterului unitar;

c) examinarea eficienței mecanismelor de asigurare a securității;

d) examinarea vulnerabilităților constructive;

e) examinarea ușurinței de utilizare;

f) examinarea vulnerabilităților operaționale;

g) verificarea cerințelor;

h) verificarea proiectului de arhitectură a produsului;

i) verificarea proiectului detaliat;

j) verificarea implementării mecanismelor de asigurare a securității;

k) verificarea mediului de dezvoltare;

l) verificarea documentației de operare;

m) verificarea mediului operațional;

n) realizarea de teste de penetrare;

o) întocmirea raportului de evaluare.

2. Pentru claritate, precizăm că termenul „verificare” implică analiza elementelor de evaluare, în timp ce termenul „examinarea” furnizează date de intrare pentru realizarea testelor de penetrare. Deși testele de penetrare sunt în mod explicit corelate cu activitățile anterioare, acestea au fost specificate ca activitate distinctă din două motive:

a) pentru a sublinia faptul că analizele anterioare trebuie consolidate și apoi trebuie concepute testele, pe baza acestor analize;

b) pentru a indica faptul că, în general, diferitele teste de penetrare sunt realizate împreună.

3. Prin activitatea de verificare a analizei de conformitate evaluatorul verifică analiza efectuată de dezvoltatorul produsului. Verificarea poate pune în evidență unele vulnerabilități rezultate, din cauza faptului că anumite funcții de securitate nu asigură atingerea unuia dintre obiectivele securității, în condițiile unei amenințări identificate în ținta de securitate.

4. Activitatea de verificare a analizei caracterului unitar constă în examinarea analizei efectuate de dezvoltatorul produsului și stabilește dacă setul de funcții de securitate implementate, luate ca ansamblu, asigură în mod adecvat îndeplinirea obiectivelor securității.

5. Prin examinarea eficienței mecanismelor de asigurare a securității evaluatorul identifică eventualele mecanisme care nu ating eficiența minimă cerută prin ținta de securitate.

6. În procesul de examinare a vulnerabilităților rezultate din procesul de construcție a produsului, evaluatorul trebuie să identifice eventuale astfel de vulnerabilități ale acestuia. Erorile identificate în procesul de evaluare a corectitudinii procesului de dezvoltare a produsului reprezintă o sursă de vulnerabilități constructive. Această activitate presupune examinarea erorilor, precum și a diferitelor funcționalități introduse în fiecare etapă a dezvoltării produsului.

7. Examinarea ușurinței de utilizare presupune identificarea modurilor de operare nesigure ale produsului. Prin urmare, această activitate este strâns legată de cerințele operaționale.

8. Activitatea de evaluare a vulnerabilităților operaționale presupune ca evaluatorul să examineze modul de operare a produsului, pentru a identifica eventuale vulnerabilități apărute în cursul acestui proces.

9. Vulnerabilitățile operaționale tratează aspecte la limita dintre măsurile de securitate IT și cele non-IT, cum ar fi proceduri operaționale privind securitatea fizică, modalități nonelectronice de management al cheilor, distribuția ecusoanelor de securitate etc. Măsurile de securitate non-IT trebuie să facă obiectul preocupărilor entității evaluatoare în următoarele situații:

a) apar ca parte a documentației de operare;

b) ținta de securitate este formulată pe baza unei politici de securitate a sistemului;

c) apar ca parte a documentației produsului.

10. În procesul de analiză a vulnerabilităților operaționale ale produsului, evaluatorii trebuie să analizeze dacă măsurile de securitate non-IT implementate contracarează vulnerabilitățile constructive identificate.

11. Activitatea de verificare a cerințelor presupune ca evaluatorul să determine dacă ținta de securitate definește în mod corect funcțiile care asigură implementarea securității. Ținta de securitate trebuie să identifice clar aceste funcții, nivelul de evaluare solicitat, precum și măsurile de securitate implementate și care trebuie avute în vedere în procesul de evaluare a produsului.

12. Prima etapă în procesul de dezvoltare a produsului, de la faza de cerințe la cea de proiect de arhitectură, prezintă o importanță deosebită, avându-se în vedere faptul că asigură corespondența dintre funcțiile abstracte și componentele logice și fizice ale produsului. În acest context, una dintre principalele activități din procesul de evaluare este verificarea proiectului de arhitectură, în urma căreia evaluatorul decide dacă există o separare bine definită între funcționalitățile care asigură securitatea și celelalte funcționalități ale produsului. În acest caz, activitatea de evaluare poate fi focalizată asupra elementelor care contribuie la asigurarea securității, iar ținta de securitate poate fi urmărită cu ușurință, pe măsură ce proiectul este analizat mai în detaliu.

13. Activitatea de verificare a proiectului detaliat presupune analiza modului în care este respectată politica privind separarea componentelor care asigură securitatea de celelalte componente, precum și verificarea faptului că toate componentele care asigură implementarea securității sunt corect implementate.

14. Verificarea implementării presupune analiza modului în care sunt implementate mecanismele de asigurare a securității, într-un mod mai detaliat decât în cursul activității de verificare a proiectului. Analiza se bazează pe concluziile activității de verificare a proiectului detaliat, după care devine posibilă testarea funcțională.

15. Prin activitatea de verificare a mediului de dezvoltare se analizează în special standardele conform cărora este dezvoltat produsul. În cursul acestei activități se analizează:

a) controlul configurației;

b) limbajele de programare și compilatoarele;

c) măsurile de securitate implementate de dezvoltator.

16. Activitatea de verificare a documentației de operare presupune verificarea faptului că produsul poate fi administrat și utilizat în acord cu obiectivele sale de securitate.

17. Verificarea mediului de operare presupune ca evaluatorul să analizeze dacă produsul operațional este identic cu produsul rezultat din procesul de dezvoltare și dacă acesta poate fi operat în conformitate cu obiectivele securității.

18. Testele de penetrare au rolul de a identifica eventuale vulnerabilități, care pot fi exploatate în procesul de utilizare a produsului.

19. Observațiile și rezultatele fiecărei activități din procesul de evaluare trebuie consemnate în raportul tehnic de evaluare.

ANEXA Nr. 3
la metodologie

MODEL DE RAPORT TEHNIC DE EVALUARE *(RTE)*

CAPITOLUL I
Introducere

SECȚIUNEA 1

Elemente generale

1. Prezenta secțiune conține date generale cu privire la procesul de evaluare și trebuie să prezinte cel puțin următoarele elemente:

a) denumirea, numărul de identificare și versiunea/modelul produsului INFOSEC supus evaluării;

b) date privind dezvoltatorul produsului și, dacă este cazul, date privind subcontractanții care au contribuit la dezvoltarea produsului;

c) date privind solicitantul evaluării;

d) programarea activităților aferente procesului de evaluare;

e) date cu privire la entitatea evaluatoare.

SECȚIUNEA a 2-a

Obiective

2. Prezenta secțiune trebuie să prezinte obiectivele RTE.

3. În principal, obiectivele sunt:

a) prezentarea elementelor necesare susținerii unei anumite concluzii cu privire la produsul supus evaluării;

b) susținerea procesului de reevaluare a produsului, în cazul în care solicitantul dorește acest lucru.

SECȚIUNEA a 3-a

Domeniu de aplicabilitate

4. Prezenta secțiune trebuie să sublinieze faptul că RTE se referă la întreaga activitate desfășurată în cursul procesului de evaluare.

5. În caz contrar, trebuie specificate motivele pentru care RTE nu acoperă întreaga activitate de evaluare.

SECȚIUNEA a 4-a

Structură

6. Prezenta secțiune trebuie să prezinte structura RTE.

CAPITOLUL II
Sumar

7. Prevederile prezentului capitol furnizează date cu privire la rezultatele evaluării.

8. Dispozițiile prezentului capitol trebuie să conțină informațiile generale necesare introducerii produsului INFOSEC în Catalogul național de pachete, produse și profile de protecție INFOSEC, după certificare.

9. Prin urmare, sumarul nu trebuie să conțină informații clasificate.

10. Prezentul capitol trebuie să conțină:

a) date cu privire la entitatea evaluatoare;

b) nivelul de evaluare atins efectiv;

c) numărul de identificare și versiunea/modelul produsului INFOSEC;

d) sumarul principalelor concluzii ale evaluării;

e) date cu privire la solicitantul evaluării;

f) scurtă descriere a produsului INFOSEC supus evaluării;

g) scurtă descriere a caracteristicilor de securitate ale produsului INFOSEC supus evaluării.

CAPITOLUL III
Descrierea produsului INFOSEC supus evaluării

SECȚIUNEA 1

Funcționalitatea produsului INFOSEC

11. Prezenta secțiune trebuie să conțină o prezentare succintă a rolului operațional al produsului, precum și a funcțiunilor pentru care a fost proiectat. Descrierea trebuie să conțină cel puțin următoarele elemente:

a) tipul de date care pot fi procesate utilizând produsul (nivel de clasificare etc.);

b) categoriile de utilizatori care vor utiliza produsul (corelat cu precizările de la punctul anterior).

SECȚIUNEA a 2-a

Etapele procesului de dezvoltare

12. Prezenta secțiune trebuie să prezinte etapele parcurse în realizarea produsului.

13. De asemenea, trebuie prezentate metodologiile, tehnicile, instrumentele și standardele relevante pentru realizarea produsului.

14. Totodată, prezenta secțiune trebuie să includă descrierea elementelor necesare evaluării puse la dispoziția entității evaluatoare de către solicitant. Descrierea trebuie să includă data la care au fost puse la dispoziție aceste elemente și numărul de înregistrare cu care a fost luat în evidență fiecare element.

SECȚIUNEA a 3-a

Arhitectura produsului

15. Prezenta secțiune trebuie să conțină un sumar al proiectului general al produsului. Trebuie să se precizeze gradul de separare între componentele care asigură implementarea securității și celelalte componente. Secțiunea va prezenta și modul de implementare și distribuția între componentele hardware, firmware și software a elementelor care asigură implementarea securității.

16. Toate numerele modelelor/versiunilor acestor componente trebuie specificate într-o anexă la RTE (anexa C).

SECȚIUNEA a 4-a

Descrierea componentelor hardware

17. Descrierea componentelor hardware trebuie să prezinte în detaliu toate componentele relevante pentru procesul de evaluare, la nivel de arhitectură.

SECȚIUNEA a 5-a

Descrierea componentelor firmware

18. Descrierea componentelor firmware trebuie să prezinte în detaliu toate componentele relevante pentru procesul de evaluare.

SECȚIUNEA a 6-a

Descrierea componentelor software

19. Descrierea componentelor software trebuie să prezinte în detaliu toate componentele relevante pentru procesul de evaluare. Descrierea trebuie să furnizeze legătura dintre componentele software și cele hardware și firmware.

CAPITOLUL IV
Caracteristici de securitate ale produsului INFOSEC

20. Trebuie subliniat că înțelegerea țintei de securitate este un element esențial pentru înțelegerea RTE. De aceea, este recomandabil ca acest capitol să includă descrierea completă a țintei de securitate.

21. Capitolul trebuie să abordeze cel puțin următoarele aspecte:

a) politica de securitate pentru produsul INFOSEC;

b) specificarea funcțiilor de implementare a securității;

c) specificarea mecanismelor de securitate;

d) precizarea nivelului minim estimat de eficiență a mecanismelor de securitate;

e) nivelul de evaluare solicitat.

CAPITOLUL V
Evaluarea

22. Prevederile prezentului capitol detaliază activitățile efectuate în procesul de evaluare, cu specificarea tuturor problemelor identificate, atât a celor de natură tehnică, cât și a celor de natură managerială.

23. Capitolul trebuie să conțină date care să sprijine activitatea comisiei de certificare de securitate, în analiza aspectelor de natură tehnică și managerială. Totodată, datele cuprinse în acest capitol pot să contribuie și la eficientizarea activității entității evaluatoare.

SECȚIUNEA 1

Etapele evaluării

24. Această secțiune este similară celei în care sunt prezentate etapele procesului de dezvoltare și trebuie să includă date cu privire la:

a) data la care a fost demarat procesul de evaluare;

b) data la care au fost furnizate elementele necesare evaluării, inclusiv ținta de securitate a produsului;

c) perioada în care au fost realizate testele de penetrare;

d) eventuale vizite efectuate la sediile dezvoltatorului sau ale utilizatorului final al produsului;

e) data la care s-au încheiat activitățile tehnice.

25. Secțiunea trebuie să precizeze toate metodele, tehnicile, instrumentele și standardele utilizate în procesul de evaluare.

SECȚIUNEA a 2-a

Procedura de evaluare

26. Această secțiune trebuie să conțină un sumar al PAE. Sumarul trebuie să includă:

a) activitățile desfășurate de evaluator, conform PAE;

b) totalitatea activităților desfășurate în procesul de evaluare, cu evidențierea activităților care nu au fost cuprinse în PAE, dar au fost efectuate în practică; va fi precizată motivația existenței acestor discrepanțe.

SECȚIUNEA a 3-a

Domeniul de aplicare a evaluării

27. Prezenta secțiune trebuie să precizeze componentele care au făcut obiectul evaluării, precum și ipotezele făcute cu privire la componentele care nu au fost examinate.

SECȚIUNEA a 4-a

Constrângeri și ipoteze

28. Prezenta secțiune trebuie să precizeze eventualele constrângeri asupra procesului de evaluare și ipotezele făcute în cursul acestui proces.

CAPITOLUL VI
Sumarul rezultatelor evaluării

29. Prevederile prezentului capitol trebuie să prezinte sumarul rezultatelor evaluării, pentru toate activitățile efectuate în cursul procesului.

30. Se recomandă structurarea pe secțiuni care să corespundă fiecăreia dintre activitățile desfășurate.

31. Fiecare secțiune trebuie să fie corelată cu setul de activități desfășurate.

32. Prezentăm în continuare, cu titlu de exemplu, o listă de aspecte care fac obiectul acestui capitol:

a) Eficiența constructivă

— Aspect 1 — Conformitatea funcționalității

— Aspect 2 — Interrelaționarea funcționalităților

— Aspect 3 — Eficiența mecanismelor

— Aspect 4 — Evaluarea vulnerabilităților constructive

b) Eficiența operațională

— Aspect 1 — Flexibilitatea în utilizare

— Aspect 2 — Evaluarea vulnerabilităților operaționale

c) Realizarea produsului — Procesul de dezvoltare

— Etapa 1 — Cerințe

— Etapa 2 — Proiectul arhitecturii

— Etapa 3 — Proiectul detaliat

— Etapa 4 — Implementarea

d) Realizarea produsului — Mediul de dezvoltare

— Aspect 1 — Controlul configurației

— Aspect 2 — Limbaje de programare și compilatoare

— Aspect 3 — Măsurile de securitate implementate de către dezvoltator
e) Operare — Documentația de operare
— Aspect 1 — Documentația de utilizare
— Aspect 2 — Documentația de administrare
f) Operare — Mediul operațional
— Aspect 1 — Livrarea și configurarea produsului
— Aspect 2 — Punerea în funcțiune și operarea.

SECȚIUNEA 1

Teste de penetrare

33. Rezultatele testelor de penetrare au fost analizate separat deoarece testele de penetrare sunt de cele mai multe ori realizate ca parte a unei anumite activități.

34. Prezenta secțiune trebuie să prezinte toate opțiunile de configurare folosite în timpul testelor de penetrare.

SECȚIUNEA a 2-a

Vulnerabilități exploatabile identificate

35. Prezenta secțiune trebuie să descrie vulnerabilitățile ce pot fi exploatate, care au fost identificate în timpul evaluării, precizând:
a) funcția de implementare a securității la care a fost identificată vulnerabilitatea;
b) descrierea vulnerabilității;
c) acțiunile întreprinse de evaluator în momentul identificării vulnerabilității;
d) activitatea în cursul căreia a fost identificată vulnerabilitatea;
e) persoana care a identificat vulnerabilitatea (dezvoltatorul sau evaluatorul);
f) data la care a fost identificată vulnerabilitatea;
g) dacă vulnerabilitatea a fost remediată (se menționează data) sau nu;
h) sursa generatoare a vulnerabilității (dacă este posibil).

SECȚIUNEA a 3-a

Observații legate de vulnerabilități ce nu pot fi exploatate

36. Prezenta secțiune trebuie să descrie vulnerabilitățile ce nu pot fi exploatate și au fost identificate în cadrul evaluării (subliniindu-le pe cele rămase în produsul operațional).

SECȚIUNEA a 4-a

Erori identificate

37. Prezenta secțiune trebuie să precizeze impactul pe care îl pot avea erorile identificate în cadrul procesului de evaluare.

CAPITOLUL VII
Ghid pentru reevaluare și analiză a impactului

38. Prezentul capitol este opțional. Poate fi omis dacă solicitantul evaluării a declarat că nu necesită informații privind o reevaluare sau analiză a impactului.

39. Dacă va fi inclus, acest capitol trebuie să precizeze:
a) includerea fiecărei componente a produsului INFOSEC în una dintre următoarele categorii: componente care asigură implementarea securității, componente relevante pentru securitate sau componente care nu sunt relevante pentru securitate;
b) identificarea instrumentelor de dezvoltare care sunt relevante pentru securitate;
c) modalitatea în care constrângerile sau ipotezele făcute în procesul de evaluare pot avea impact în cazul reevaluării sau refolosirii produsului;
d) orice concluzii privind tehnici de evaluare sau instrumente care pot fi utile în cazul unei reevaluări;
e) detalii de arhivare necesare reînceperii evaluării;
f) pregătire specifică necesară reevaluatorilor pentru demararea unui proces de reevaluare.

CAPITOLUL VIII
Concluzii și recomandări

40. Prezentul capitol trebuie să cuprindă concluziile și recomandările evaluării. Concluzia principală va preciza dacă produsul îndeplinește obiectivul de securitate stabilit și dacă are vulnerabilități ce pot fi exploatate.

41. Trebuie să se specifice faptul că recomandările se referă la componentele produsului care au făcut obiectul evaluării și că pot exista și alți factori de care evaluatorii nu sunt conștienți, iar acești factori pot influența procesul de certificare a produsului.

42. Recomandările pot include sugestii către alte entități, precum solicitantul evaluării sau dezvoltatorul produsului, pentru a fi înaintate comisiei de certificare de securitate.

43. Trebuie să se specifice faptul că rezultatele evaluării sunt valabile numai pentru o anumită versiune a produsului INFOSEC, configurată într-un anumit mod, iar comisia de certificare de securitate trebuie informată despre orice schimbări aduse produsului.

Anexa A — Lista elementelor necesare evaluării

44. Această anexă trebuie să identifice, cu numerele versiunii și datele la care au fost recepționate, toate elementele necesare evaluării sau se face o referire la lista elementelor.

Anexa B — Lista de acronime/Glosar de termeni

45. Această anexă trebuie să explice toate acronimele și abrevierile folosite în RTE. De asemenea, trebuie să definească termenii specifici utilizați.

Anexa C — Configurația evaluată

46. Configurațiile produsului INFOSEC examinate în cadrul evaluării (în special configurații folosite la testele de penetrare, verificare a fiabilității) trebuie identificate clar.

47. Trebuie precizate orice presupuneri făcute sau configurații care nu au fost luate în considerare.

Descrierea componentelor hardware

48. Descrierea componentelor hardware trebuie să furnizeze informații despre configurație, privind toate componentele la nivel arhitectural ce sunt relevante pentru evaluare și, în consecință, pentru implementarea securității.

Descrierea componentelor firmware

49. Descrierea componentelor firmware trebuie să furnizeze informații despre configurație, despre toate componentele care sunt relevante pentru procesul de evaluare și, în consecință, pentru implementarea securității.

Descrierea componentelor software

50. Descrierea componentelor software trebuie să furnizeze informații despre configurație privind părți ale aplicațiilor software utilizate de produsul INFOSEC care sunt relevante pentru procesul de evaluare și, în consecință, pentru implementarea securității.

Anexa D — Rapoartele activităților de evaluare

51. Această anexă nu este necesară dacă toate rapoartele de activitate sunt incluse în cap. 6 al RTE.

52. Dacă este prezentă, această anexă trebuie să cuprindă înregistrări ale tuturor activităților de evaluare (incluzând rezultatele testelor efectuate, tehnici și instrumente utilizate).

Anexa E — Probleme identificate

53. Această anexă trebuie să cuprindă rapoarte cu privire la toate problemele identificate în cursul procesului de evaluare.

54. Rapoartele pot fi emise și înainte de finalizarea evaluării și trebuie să conțină cel puțin următoarele elemente:
a) numărul și versiunea produsului supus evaluării;
b) activitatea în cursul căreia a fost identificată problema;
c) descrierea problemei identificate.

ANEXA Nr. 4
la metodologie

Elemente ale raportului privind certificarea

Un raport privind certificarea trebuie să includă cel puțin următoarele elemente:

a) Introducere:

— date generale cu privire la produsul INFOSEC supus evaluării.

b) Rezumat:

— detalii cu privire la entitatea de evaluare;

— identificarea completă a produsului INFOSEC supus evaluării, inclusiv a codului de identificare, versiunii etc.;

— sumarul concluziilor formulate de evaluator;

— date privind dezvoltatorul și, dacă este cazul, date privind subcontractanții acestuia care au contribuit la dezvoltarea produsului;

— date privind solicitantul certificării;

— nivelul de evaluare atins efectiv.

c) Prezentarea produsului:

— descrierea produsului INFOSEC, în configurația supusă evaluării;

— descrierea hardware;

— descrierea firmware;

— descrierea software;

— descrierea documentației produsului.

d) Evaluarea:

— descrierea sumară a țintei de securitate, care să cuprindă și descrierea caracteristicilor de securitate ale produsului INFOSEC;

— elemente de identificare ale RTE;

— sumarul principalelor concluzii formulate de entitatea de evaluare.

e) Certificarea:

— propuneri referitoare la luarea unei decizii cu privire la certificarea produsului INFOSEC;

— specificarea eventualelor restricții care trebuie avute în vedere în procesul de utilizare a produsului (de exemplu: limitarea nivelului de clasificare a informațiilor, utilizare în medii operaționale specifice etc.).

ANEXA Nr. 5
la metodologie

BIBLIOGRAFIE

1. Standardele naționale de protecție a informațiilor clasificate în România, aprobate prin Hotărârea Guvernului nr. 585/2002, publicată în Monitorul Oficial al României, Partea I, nr. 485 din 5 iulie 2002, cu modificările și completările ulterioare.

2. Normele privind protecția informațiilor clasificate ale Organizației Tratatului Atlanticului de Nord în România, aprobate prin Hotărârea Guvernului nr. 353/2002, publicată în Monitorul Oficial al României, Partea I, nr. 315 din 13 mai 2002, cu modificările ulterioare.

3. Metodologia de acreditare a entităților pentru evaluarea produselor de securitate IT și a sistemelor informatice și de comunicații — INFOSEC 12, aprobată prin Ordinul directorului general al Oficiului Registrului Național al Informațiilor Secrete de Stat nr. 167/2006, publicat în Monitorul Oficial al României, Partea I, nr. 223 din 10 martie 2006.

4. Guidelines for the Evaluation and Certification of ADP Systems and Networks and Computer Security (COMPUSEC) Products, AC/35-N/275.

5. Procedure CER/P/01.1 — Certification of the security provided by IT products and systems, February 9, 2004 — Secrétariat Général de la Défense Nationale, France.

6. Information Technology Security Evaluation Manual (ITSEM), version 1.0, Commission of the European Communities.

7. Scheme overview, draft 0.3, April 15, 2005 — Swedish Certification Body for IT Security.

8. Evaluation and Certification, draft 0.9, April 15, 2005 — Swedish Certification Body for IT Security.

9. Common Criteria Evaluation and Validation Scheme For Information Technology Security, Guidance to Validators of IT Security Evaluations, Version 1.0, February 2002, National Institute for Standards and Technologies, U.S.

10. Common Criteria Evaluation and Validation Scheme Policy Letter — National Information Assurance Partnership, U.S.

11. Information Technology Security Testing — Common Criteria, April 1999, Version 1.1, U.S. Department of Commerce.

12. Guidelines for Evaluation Work Program (EWP), January 14, 1998, JEIDA Japan.

EDITOR: PARLAMENTUL ROMÂNIEI — CAMERA DEPUTAȚILOR

„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. 021.411.58.33 și 021.410.47.30, fax 021.410.77.36 și 021.410.47.23
Tiparul: „Monitorul Oficial” R.A.

MONITORUL OFICIAL

5 948368 440784

Monitorul Oficial al României, Partea I, nr. 92/10.II.2010 conține 16 pagini. Prețul: 3,20 lei **ISSN** 1453—4495