

GUVERNUL ROMÂNIEI
Oficiul Registrului Național al Informațiilor Secrete de Stat

**METODOLOGIA DE EVALUARE ȘI CERTIFICARE A
PACHETELOR, PRODUSELOR ȘI PROFILELOR DE PROTECȚIE
INFOSEC**

- INFOSEC 14 -

Versiunea 2.0

- 2010 -

Pagină lăsată intenționat albă

METODOLOGIA DE EVALUARE ȘI CERTIFICARE A PACHETELOR, PRODUSELOR ȘI PROFILELOR DE PROTECȚIE INFOSEC

CUPRINS

1. INTRODUCERE	5
1.1 Scop	5
1.2 Definiții	5
2. DESCRIEREA METODOLOGIEI DE EVALUARE.....	8
2.1 Etapa 1: Demararea procesului de evaluare.....	8
2.2 Etapa 2: Desfășurarea procesului de evaluare	10
2.2.1 Elemente generale	10
2.2.2 Obiectivele evaluării	10
2.2.3 Întocmirea Planului de Activități privind Evaluarea	11
2.2.4 Desfășurarea evaluării.....	11
2.3 Etapa 3: Finalizarea procesului de evaluare	12
2.3.1 Întocmirea Raportului Tehnic de Evaluare.....	12
3. DESCRIEREA METODOLOGIEI DE CERTIFICARE	13
3.1 Demararea procesului de certificare	13
3.2 Întocmirea Raportului de Certificare.....	15
3.3 Luarea deciziei privind certificarea produsului	16

Anexa nr. 1 – Cerințe de evaluare și certificare a sistemelor criptografice destinate protecției informațiilor naționale clasificate, altele decât cele din categoria cifrului de stat

Anexa nr. 2 – Exemple de activități aferente procesului de evaluare

Anexa nr. 3 – Model de Raport Tehnic de Evaluare

Anexa nr. 4 – Elemente ale Raportului privind Certificarea

Anexa nr. 5 – Bibliografie

Pagină lăsată intenționat albă

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 (SIC) 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 pre-definiți. 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 produselor INFOSEC, din punct de vedere al securității.

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. Procesele de evaluare și certificare a produselor INFOSEC se desfășoară prin parcurgerea următoarelor etape, așa cum sunt prezentate în Figura nr. 1.

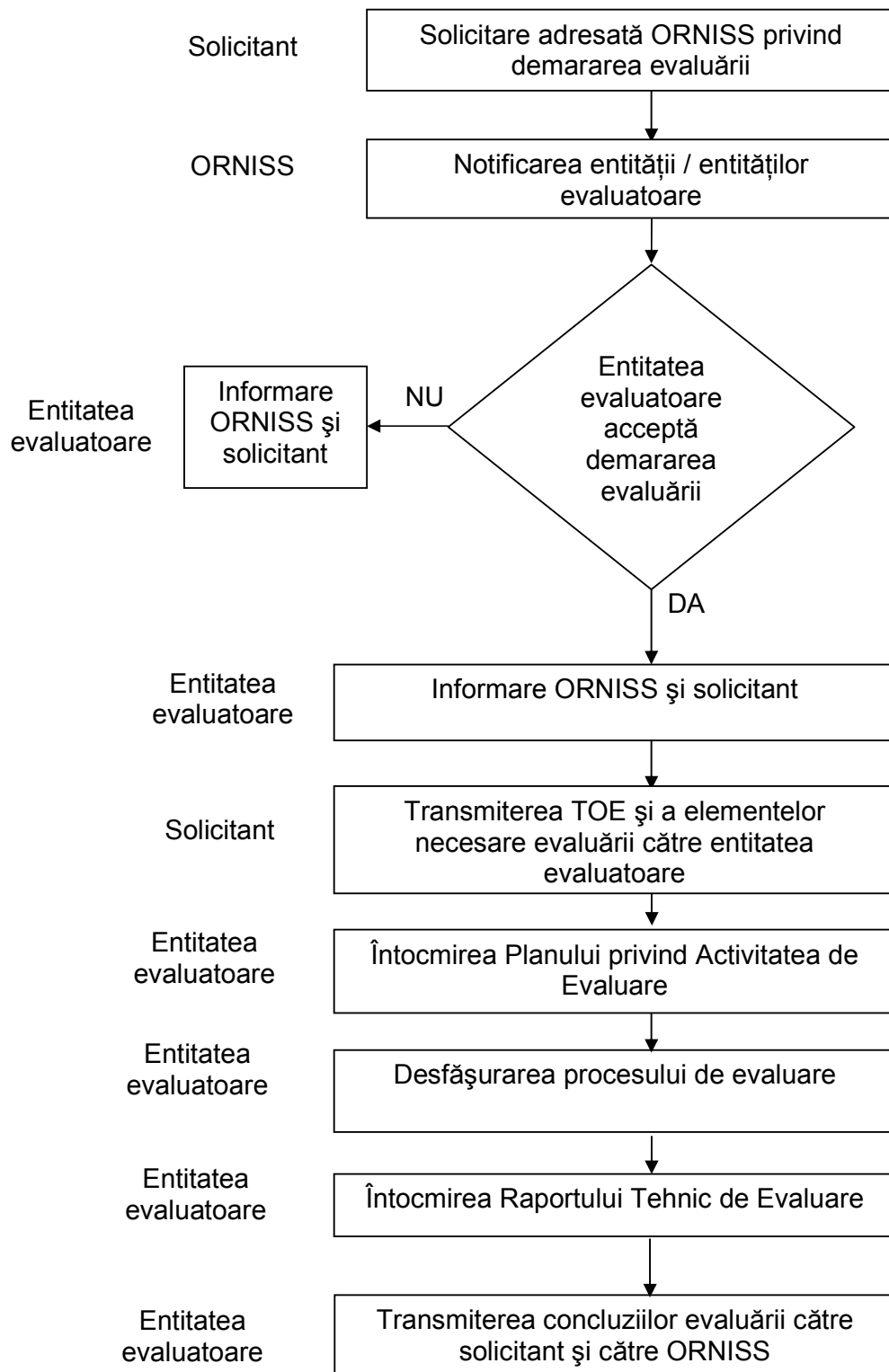


Figura nr. 1 – Schema procesului de evaluare a securității produselor INFOSEC utilizate în SIC care vehiculează informații naționale clasificate

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 (ORNISS) o solicitare scrisă.

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 după 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 precizate 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 (ASIC) 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 acestuia / acestora de către solicitant pentru

efectuarea evaluării. Notificarea transmisă de ORNISS include toate datele primite de la solicitant.

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

(2) ORNISS notifică solicitantul 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 algoritmi, 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 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 Ordinul directorului general al ORNISS nr. 167/2006, publicat în Monitorul Oficial al României, Partea I, nr. 223 din 10 martie 2006 pentru aprobarea Metodologiei de acreditare a entităților pentru evaluarea produselor INFOSEC și a sistemelor informatice și de comunicații – INFOSEC 12.

Art. 18. (1) Procesul de evaluare a produselor INFOSEC se desfășoară pe baza a trei 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, agreeate 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 exploatare.

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

Art. 23. Respectarea acestor patru 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 (PAE).

Art. 25. PAE trebuie să descrie modul în care sunt organizate activitățile legate de procesul de evaluare și inter-relaționarea 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 criteriile și metodologiile 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, aprobată prin Ordinul directorului general al ORNISS, 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. **Anexa nr. 2** prezintă o listă demonstrativă cu activități aferente procesului de evaluare.

Art. 32. Observațiile și rezultatele fiecărei activități din procesul de evaluare trebuie consemnate într-un Raport Tehnic de Evaluare (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 (rezilierii contractului / încetării acordului), entitatea evaluatoare trebuie să notifice ORNISS cu privire la acest lucru.

2.3 Etapa 3: Finalizarea procesului de evaluare

2.3.1 Întocmirea Raportului Tehnic de Evaluare

Art. 37. La finalul activităților de evaluare, evaluatorul are obligația să întocmească un Raport Tehnic de Evaluare.

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 certicator;
- 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. **Anexa nr. 3** prezintă un model de RTE, detaliind conținutul fiecărui capitol și secțiune.

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 Raportului Tehnic de Evaluare întocmit.

(2) Pentru clarificarea unor aspecte specifice, ORNISS poate solicita entităților 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.

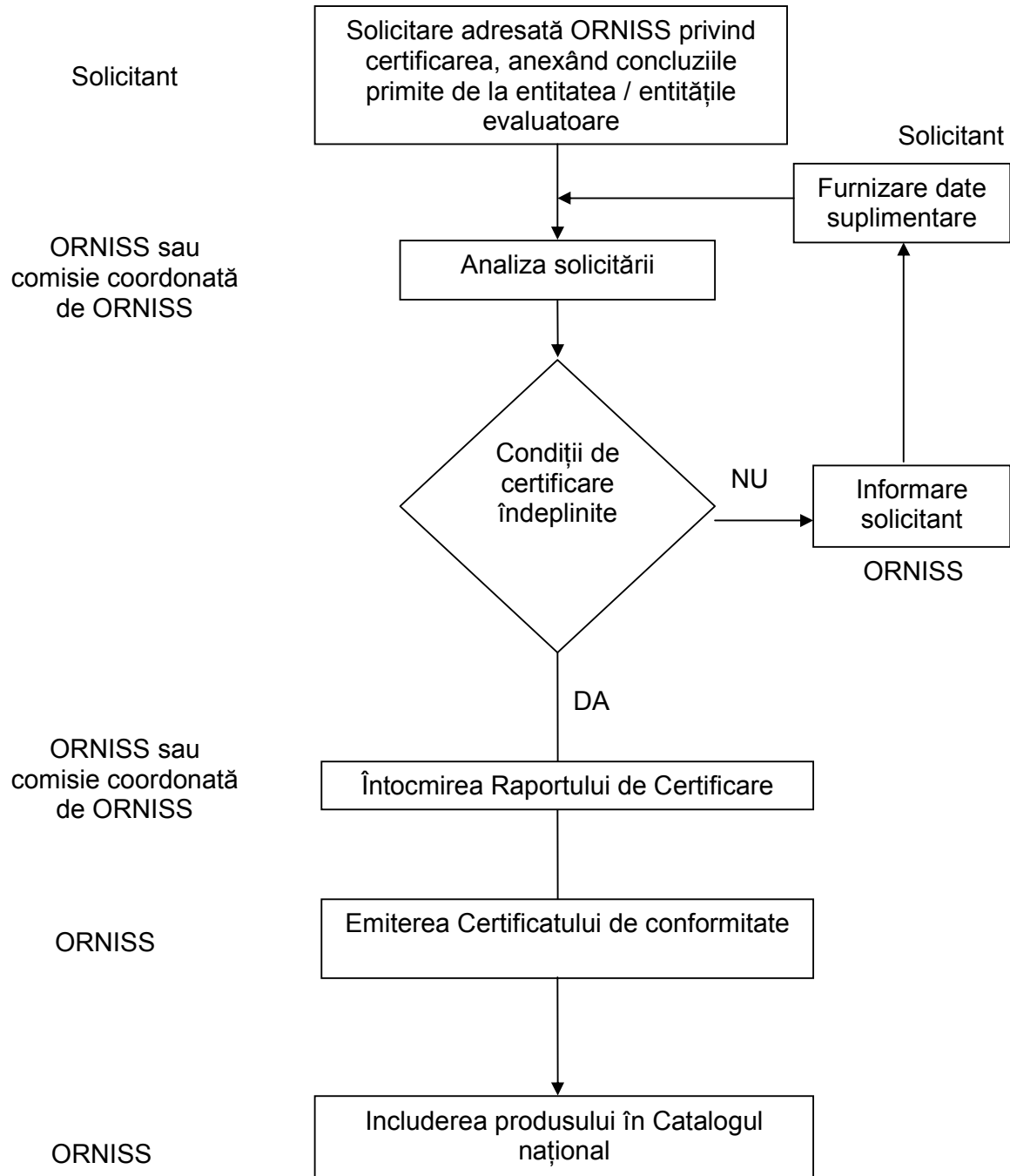


Figura 2 - Schema procesului de certificare a produselor INFOSEC utilizate în SIC care vehiculează informații naționale clasificate

Art. 45. O descriere schematică a procesului de certificare este prezentată în **Figura 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 solicitantul, 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) Raportul tehnic de evaluare.

3.2 Întocmirea Raportului de Certificare

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 pusă 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 de Certificare 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 entitatea evaluatoare, în vederea remedierii acestor deficiențe.

Art. 53. Pentru desfășurarea corespunzătoare a etapei de certificare, ASIC 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 ASIC entității evaluatoare.

Art. 55. Anexa nr. 4 prezintă un set minim de elemente care trebuie să fie cuprinse în Raportul privind Certificarea.

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 pre-definiți.

Art. 57. Certificatul de conformitate emis de Directorul General al 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 v. 2.

Art. 59. Anexele nr. 1-5 fac parte integrantă din prezenta metodologie.