ANEXĂ

METODOLOGIA DE EVALUARE ŞI CERTIFICARE A PACHETELOR, PRODUSELOR ŞI PROFILELOR DE PROTECȚIE INFOSEC - INFOSEC 14

CAPITOLUL I - INTRODUCERE

Secțiunea 1- Scop

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

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

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

b) verificarea şi 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.

Secțiunea a 2-a Definiții

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

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

b) **evaluare** – examinarea detaliată, din punct de vedere tehnic şi 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 desfăşurarea procesului de evaluare şi 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 şi/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 aceluiaşi produs, în funcție de aceeaşi țintă de securitate, de către aceeaşi entitate evaluatoare, conduce la un rezultat similar cu cel obținut ca urmare a primei evaluări a produsului;

j) **reproductibilitate** – principiu conform căruia repetarea evaluării aceluiaşi produs, în funcție de aceeaşi 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 şi aprobarea de includere în Catalogul național cu produse, profile şi pachete de protecție a unui produs INFOSEC. Solicitantul poate fi şi o altă persoană juridică diferită de producător, de exemplu, dezvoltator, utilizator, comerciant, integrator;

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

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

Art. 4. În cuprinsul prezentei metodologii prin produs criptografic se înțeleg acele produse criptografice care nu fac parte din categoria cifrului de stat.

Art. 5. În raport cu destinația de utilizare, produsele INFOSEC se împart în două categorii: cu utilizare la nivel național şi cu regim limitat de distribuție şi utilizare la nivelul Autorităților Desemnate de Securitate, denumite în continuare ADS, cu competențe în coordonarea şi controlul măsurilor de protecție a informațiilor naționale clasificate ce vor fi protejate cu acestea.

Secțiunea a 3-a - Cadru general

Art. 6. (1) Oficiul Registrului Național al Informațiilor Secrete de Stat, denumit în continuare ORNISS, este responsabil de coordonarea proceselor de certificare a tuturor produselor INFOSEC destinate utilizării la nivel național, pentru care se solicită includerea în Catalogul național de pachete, produse şi profile de protecție INFOSEC, denumit în continuare Catalog național.

(2) Pentru produsele INFOSEC, altele decât cele criptografice:

a) Evaluarea se realizează de către o entitate acreditată de către ORNISS;

b) ORNISS realizează certificarea, pe baza elementelor din Raportul Tehnic de Evaluare, denumit în continuare RTE, întocmit de entitatea care a realizat evaluarea;

(3) Pentru produsele criptografice:

a) Evaluarea şi certificarea se realizează de către două entităţi evaluatoare aparţinând Serviciului de Informaţii Externe (SIE), Serviciului Român de Informaţii (SRI) sau Ministerului Apărării Naţionale (MApN);

b) ORNISS emite certificatul, pe baza analizei documentelor transmise la ORNISS de către cele două instituţii ale căror entităţi evaluatoare au realizat evaluarea şi certificarea; din documente trebuie să reiasă conformitatea produselor cu standardele aplicabile, precum şi eventuale condiţii şi termene de valabilitate a rezultatelor testării, eventuale cerinţe/condiţii/instrucţiuni de utilizare.

(4) În situaţii excepţionale, când se apreciază că există o ameninţare semnificativă la adresa securităţii sistemelor informatice şi de comunicaţii naţionale, astfel încât există riscul major de prejudiciere în mod deosebit de grav a intereselor naţionale, ORNISS poate decide asupra necesităţii unor evaluări suplimentare a produselor INFOSEC, altele decât cele criptografice.

Art. 7. (1) Certificarea produselor INFOSEC cu regim limitat de distribuţie şi utilizare, cu excepţia produselor criptografice, se realizează în cadrul ADS, de către structura internă INFOSEC acreditată de ORNISS, cu competenţe în coordonarea şi controlul măsurilor de protecţie a informaţiilor naţionale clasificate, pe baza RTE realizat de o entitate evaluatoare acreditată de ORNISS.

(2) Aprobarea produselor criptografice cu regim limitat de distribuţie şi utilizare destinate protecţiei informaţiilor naţionale clasificate se realizează în cadrul ADS, de către structura internă INFOSEC acreditată de ORNISS, în urma evaluării şi certificării acestora de către două entităţi evaluatoare aparţinând SIE, SRI sau MApN.

(3) În cazul în care în cadrul ADS nu există o structură internă INFOSEC acreditată de ORNISS, certificarea se realizează de către ORNISS

(4) La nivelul SIE, SRI şi MApN utilizarea produselor criptografice destinate protecţiei informaţiilor naţionale clasificate şi constituirea registrelor de evidenţă a pachetelor, produselor şi profilelor de protecţie INFOSEC se stabilesc prin norme proprii.

CAPITOLUL II - DESCRIEREA METODOLOGIEI DE EVALUARE

1. Demararea procesului de evaluare

Art. 8. În vederea demarării procesului de evaluare a unui produs INFOSEC destinat utilizării la nivel naţional, persoanele juridice trebuie să adreseze ORNISS o solicitare scrisă.

Art. 9. Solicitarea de demarare a procesului de evaluare trebuie să fie însoţită de documentaţie care să precizeze cel puţin următoarele aspecte:

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

b) ținta de securitate;

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

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

e) copii după certificate anterioare, dacă este cazul.

Art. 10. ORNISS, prin Agenția de Securitate pentru Informatică şi Comunicații (ASIC) din cadrul său, analizează solicitarea primită.

Art. 11. 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. 12. Dacă cererea conține toate datele menționate, se vor întreprinde următoarele demersuri, după caz:

a) În cazul produselor INFOSEC, cu excepția celor criptografice:

i) ORNISS notifică solicitantul în vederea identificării entității evaluatoare disponibile pentru efectuarea evaluării;

ii) Solicitantul identifică entitatea evaluatoare şi notifică ORNISS cu privire la selectarea acesteia;

iii) ORNISS transmite către entitatea evaluatoare o adresă de solicitare a activității de evaluare.

b) În cazul produselor criptografice, ORNISS notifică SIE, SRI şi MApN, care vor stabili de comun acord asupra celor două entități care vor efectua evaluarea şi vor informa ORNISS cu privire la selectarea acestor entități .

c) Notificările transmise de ORNISS către entitățile evaluatoare includ toate datele prevăzute la art. 9.

Art. 13. După analiza documentației prevăzute la art.9, în caz de neacceptare a procesului de evaluare entitatea evaluatoare notifică ORNISS, care va informa solicitantul cu privire la această decizie.

Art. 14. (1) În cazul în care entitatea/entitățile evaluatoare acceptă să demareze procesul de evaluare, solicitantul pune la dispoziția acesteia/acestora cel puțin următoarele elemente:

a) produsul de evaluat, incluzând:

i) componentele hardware, software şi 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 şi 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 şi documentaţie aferentă, incluzând rezultatele testelor anterioare.

(2) În funcţie de tipul informaţiilor care trebuie puse la dispoziţia entităţii/entităţilor evaluatoare, între solicitant şi entitatea/entităţile evaluatoare se pot încheia acorduri de confidenţialitate, în baza cărora aceste informaţii sunt transmise.

Art. 15. Procesul de evaluare se consideră demarat după încheierea unui document de acceptare, de exemplu contract, acord etc., între solicitant şi entitatea/entităţile evaluatoare.

Art. 16. Evaluatorul întocmeşte lista cu elementele necesare evaluării şi stabileşte datele la care acestea trebuie să îi fie puse la dispoziţie.

Art. 17. În cazul în care solicitantul evaluării nu este acelaşi cu producătorul produsului supus evaluării, în vederea asigurării protecţiei unor informaţii specifice, acestea pot fi puse la dispoziţia evaluatorului, direct de producător.

Art. 18. Este important ca obiectivele evaluării să fie clar definite de solicitant, înţelese de evaluator şi transmise către toate părţile 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 şi obiectivele evaluării, precum şi responsabilităţile pe care le au în acest proces.

Etapa a 2-a - Desfăşurarea procesului de evaluare

1. Elemente generale

Art. 19. Evaluarea produselor INFOSEC se realizează de către entităţi evaluatoare acreditate, potrivit reglementărilor în vigoare.

Art. 20. (1) Procesul de evaluare a produselor INFOSEC se desfăşoară pe baza a trei elemente:

a) criterii;

b) metodologie;

c) modul de derulare a proceselor de evaluare şi certificare de securitate;

(2) Criteriile reprezintă normele şi principiile faţă de care poate fi măsurată securitatea unui produs INFOSEC, în vederea evaluării, dezvoltării şi achiziţiei, iar metodologia stabileşte modul în care trebuie realizată evaluarea, în baza criteriilor.

Art. 21. Evaluarea securităţii pe care o pot asigura produsele INFOSEC se realizează în conformitate cu standarde naţionale sau standarde internaţionale recunoscute pe plan naţional, agreate de statele membre ale NATO sau UE.

2. Obiectivele evaluării

Art. 22. Obiectivul principal al procesului de evaluare de securitate constă în verificarea faptului că funcţiile de securitate ale produsului sunt conforme cu ţinta de securitate.

Art. 23. Procesul de evaluare de securitate asigură un anumit nivel de încredere în faptul că produsul nu prezintă vulnerabilităţi care pot fi exploatate.

Art. 24. În contextul evaluării şi certificării produselor INFOSEC, trebuie acordată o atenție deosebită principiilor repetabilității, reproductibilității, imparțialității şi obiectivității.

Art. 25. Respectarea acestor patru principii trebuie să fie verificată de ORNISS, în cursul procesului de certificare.

3. Întocmirea Planului de Activități privind Evaluarea

Art. 26. Pentru a descrie structura unui proces de evaluare, precum şi conexiunile dintre diferitele activități aferente procesului, evaluatorul trebuie să întocmească un Plan de Activități privind Evaluarea, denumit în continuare PAE.

Art. 27. PAE trebuie să descrie modul în care sunt organizate activitățile legate de procesul de evaluare şi inter-relaționarea acestor activități.

Art. 28. PAE trebuie întocmit astfel încât să fie aplicabil atât pentru evaluarea unei game de produse, cât şi pentru diferite niveluri ale evaluării.

Art. 29. Acest document oferă o prezentare generală asupra modului în care trebuie realizată evaluarea, în conformitate cu criterii şi metodologii de evaluare specifice.

4. Desfăşurarea evaluării

Art. 30. Activitatea entității evaluatoare trebuie să fie conformă cu cerințele standardelor de calitate şi cu criteriile stabilite în Metodologia de acreditare a entităților pentru evaluarea produselor de securitate IT şi a sistemelor informatice şi de comunicații – INFOSEC 12.

Art. 31. 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. 32. Prezenta metodologie stabileşte cadrul general al activităților legate de procesul de evaluare şi certificare, iar la implementarea sa trebuie ținut cont de faptul că pentru fiecare produs specific pot fi necesare diferite activități şi niveluri de evaluare.

Art. 33. Anexa nr. 1 prezintă o listă exemplificativă cu activități aferente procesului de evaluare.

Art. 34. Observațiile şi rezultatele fiecărei activități din procesul de evaluare trebuie consemnate într-un RTE.

Art. 35. Pe toată durata procesului de evaluare oricare dintre părțile implicate poate solicita organizarea unor şedințe de lucru sau informații suplimentare, pentru clarificarea aspectelor de natură tehnică.

Art. 36. 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 şi, în cazul unor testări care presupun acces la informații clasificate secret de stat, notificarea prealabilă a ORNISS.

Art. 37. În cazul în care ORNISS consideră necesar, poate participa la testele efectuate la sediul solicitantului sau dezvoltatorului.

Art. 38. În cazul în care evaluarea este întreruptă din diferite cauze, de exemplu rezilierea contractului/încetarea acordului, entitatea evaluatoare trebuie să notifice ORNISS cu privire la acest lucru.

Etapa a 3-a - Finalizarea procesului de evaluare

Întocmirea RTE

Art. 39. La finalul activităților de evaluare, evaluatorul are obligația să întocmească un RTE.

Art. 40. RTE are următoarea structură:

a) descrierea activităților desfăşurate în procesul de evaluare;

b) prezentarea rezultatelor obținute şi a concluziilor rezultate din activitățile desfăşurate.

Art. 41. Entitatea evaluatoare transmite către solicitantul evaluării elemente din RTE, cu respectarea principiului necesității de a cunoaşte.

Art. 42. În cazul în care dezvoltatorul produsului nu este totodată şi solicitantul evaluării, există posibilitatea transmiterii anumitor părți din RTE către dezvoltator, dar numai cu acordul solicitantului evaluării.

Art. 43. Anexa nr. 2 prezintă un model de RTE, detaliind conținutul fiecărui capitol şi secțiune.

Art. 44. (1) În vederea certificării produselor INFOSEC, altele decât cele criptografice, entitatea evaluatoare transmite la ORNISS un document de sinteză a RTE, care să cuprindă cel puțin următoarele elemente:

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

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

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

d) testele realizate şi rezultatele acestora;

e) concluziile finale ale procesului de evaluare;

f) condiții şi termene de valabilitate a rezultatelor testării, eventuale cerințe/condiții/instrucțiuni de utilizare a produsului, astfel încât să se asigure păstrarea caracteristicilor de securitate şi 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) În cazul produselor criptografice, cele două entități care au realizat evaluarea şi certificarea transmit la ORNISS documente din care să reiasă conformitatea produselor cu standardele aplicabile,

precum şi eventuale condiţii şi termene de valabilitate a rezultatelor testării, eventuale cerinţe/condiţii/ instrucţiuni de utilizare, astfel încât să se asigure păstrarea caracteristicilor de securitate şi funcţionale.

CAPITOLUL III - DESCRIEREA METODOLOGIEI DE CERTIFICARE

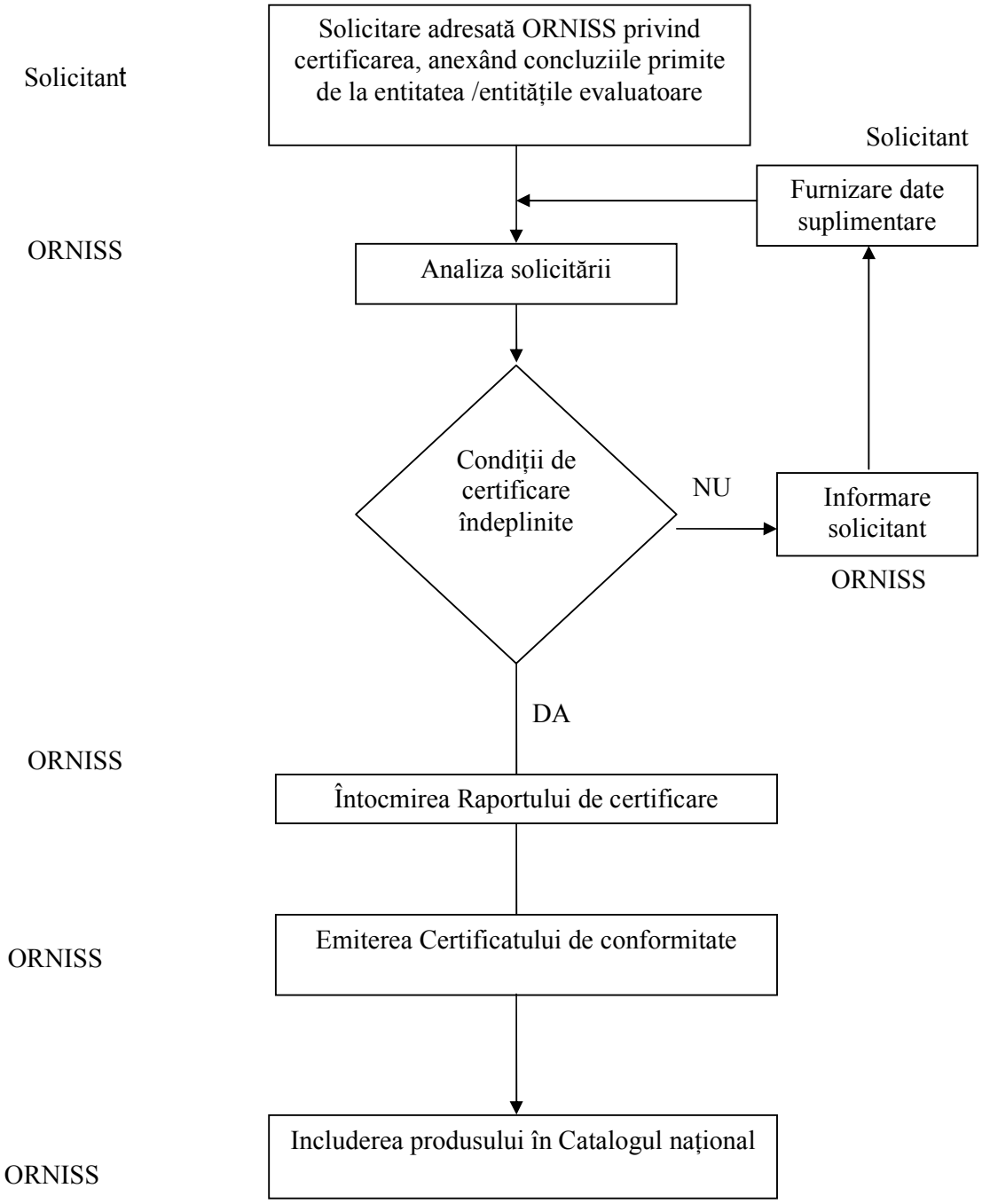
Secţiunea 1 - Demararea procesului de certificare

Art. 45. 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 şi metodologiile recunoscute şi rezultatele evaluării sunt conforme cu elementele constatate. Totodată, certificarea are rolul de a crea un climat de încredere şi de a confirma faptul că entităţile evaluatoare operează în conformitate cu aceleaşi standarde şi că rezultatele obţinute de oricare dintre entităţile evaluatoare sunt demne de încredere în egală măsură.

Art. 46. Încrederea trebuie să aibă la bază respectarea principiilor imparţialităţii, obiectivităţii, repetabilităţii şi reproductibilităţii.

Art. 47. O descriere schematică a procesului de certificare este prezentată în schema de mai jos.

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



Art. 48. (1) Demararea procesului de certificare se realizează printr-o solicitare adresată ORNISS de către solicitant.

(2) Solicitarea trebuie să fie însoțită de concluziile formulate de entitatea/entitățile evaluatoare în urma procesului de testare-evaluare a produsului.

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

Art. 49. În cadrul etapei de certificare de securitate, ORNISS, prin ASIC realizează o analiză independentă a rezultatelor obținute în urma etapei de evaluare, precum şi a modalității în care s-a desfăşurat această activitate.

Art. 50. Procesul de certificare trebuie să analizeze următoarele aspecte:

a) criteriile, metodologiile şi procedurile de lucru utilizate în procesul de evaluare;
b) resursele folosite în cadrul evaluării de securitate, de exemplu echipamente, documentație, timp etc.;
c) personalul care a realizat evaluarea de securitate, ca de exemplu calificare, obiectivitate, imparțialitate etc.;
d) rezultatele testelor de evaluare;
e) RTE sau elemente din acesta, după caz.

Secțiunea a 2-a - Întocmirea Raportului de certificare

Art. 51. Rezultatele activității de certificare trebuie să facă obiectul unui Raport de certificare.

Art. 52. Raportul de certificare trebuie să identifice în mod clar produsul şi să conțină recomandări cu privire la decizia privind certificarea produsului evaluat.

Art. 53. Dacă în urma analizei documentației pusă la dispoziție în vederea certificării se constată că, atât rezultatele obținute în urma activității de evaluare, cât şi modalitatea în care aceasta s-a realizat sunt conforme standardelor şi normelor în vigoare, precum şi faptul că produsul îndeplineşte cerințele de securitate conform țintei de securitate, Raportul de certificare include propuneri privind certificarea produsului.

Art. 54. 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. 55. Pentru desfăşurarea corespunzătoare a etapei de certificare, ORNISS, prin ASIC, poate solicita entității evaluatoare alte documente cu relevanță pentru această activitate.

Art. 56. Raportul de Certificare 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. 57. Anexa nr. 3 prezintă un set minim de elemente ale Raportului de certificare.

Secțiunea a 3-a - Luarea deciziei privind certificarea produsului

Art. 58. După parcurgerea activităților necesare luării unei decizii privind certificarea unui produs, se desprind două variante posibile:

a) certificarea produsului şi emiterea Certificatului de conformitate şi aprobarea includerii în Catalogul național;

b) refuzul certificării – decizie datorată identificării unor deficiențe grave referitoare la atingerea de către produs a parametrilor de securitate pre-definiți.

Art. 59. Certificatul de conformitate emis de Directorul General al ORNISS confirmă faptul că produsul îndeplineşte standardele de securitate în baza cărora a fost evaluat, pentru ținta de securitate propusă.

Art. 60. Produsele certificate vor fi incluse în Catalogul național, cu ocazia următoarei actualizări a acestuia, în conformitate cu prevederile Directivei INFOSEC privind Catalogul național cu pachete, produse şi profile de protecție INFOSEC – INFOSEC 5.

Art. 61. Anexa nr. 4 cuprinde o bibliografie a unor acte normative şi documente cu relevanță în domeniu.

Art. 62. Anexele nr. 1- 4 fac parte integrantă din prezenta metodologie.