

GUVERNUL ROMÂNIEI

Oficiul Registrului Național al Informațiilor Secrete de Stat

D I R E C T I V A

**INFOSEC PRIVIND CATALOGUL NAȚIONAL CU PACHETE, PRODUSE ȘI
PROFILE DE PROTECȚIE INFOSEC**

- INFOSEC 5 -

Versiunea 2.0

2010

Pagină lăsată intenționat albă

DIRECTIVA INFOSEC PRIVIND CATALOGUL NAȚIONAL CU PACHETE, PRODUSE ȘI PROFILE DE PROTECȚIE INFOSEC

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 (ORNIS), 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 cu pachete, produse și profile de protecție INFOSEC, definit prin prezenta directivă, este de a furniza persoanelor juridice de drept public sau privat care au în administrare Sisteme Informatice și de Comunicații 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;

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 INFOSEC 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 Autorităților Desemnate de

Securitate (ADS) cu competențe în coordonarea și controlul măsurilor de protecție a informațiilor clasificate ce vor fi protejate cu acestea.

(4) ADS - urile 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 - urile 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. În cazul în care în cadrul ADS nu există o astfel de structură INFOSEC, certificarea se realizează de către ORNISS.

CAPITOLUL V - CONȚINUTUL CATALOGULUI CU PRODUSE INFOSEC

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 prezentate la art. 11 pot fi incluse în Catalogul național următoarele tipuri de pachete, produse, profile de protecție INFOSEC:

- a) dezvoltate pe plan național, evaluate și certificate de entități naționale acreditate 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 și 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 Directorul 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 catalog.

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 sau 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 sau 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 către NATO;
- c) lista producătorilor externi, precum și a modelelor de produse certificate din punct 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 (dar nu numai):

- a) Dispozitive si sisteme de control al accesului;
- b) Dispozitive si sisteme de protecție a perimetrului;
- c) Baze de date;

- d) Dispozitive si 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 pe 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 pe listă a produselor pentru securitatea 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 SIC și personalului implicat în proiectarea SIC. Aceasta este o listă a instrumentelor de securitate conforme cu prevederile Directivei INFOSEC tehnică și de implementare privind cerințele instrumentelor de securitate, selectarea, aprobarea și implementarea acestora – INFOSEC 9, aprobată prin Ordinul Directorului General al ORNISS nr. 390 din 2004, publicat în Monitorul Oficial al României, Partea I nr. 1081 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 referință doar la raportul de evaluare a instrumentului. Informațiile privind vulnerabilitățile sunt puse la dispoziție numai acelor autorități ale SIC și de securitate care au o "nevoie de a cunoaște" corespunzătoare.

Secțiunea a 6-a - Pachete și profile de protecție

Art. 29 – (1) 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 sau 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 pe listă a pachetelor / profilelor de protecție vor trata cel puțin aspectele privitoare la:

- a) denumirea pachetului / profilului de protecție;

- b) autorul;
- 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 către 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 sau profil de protecție care urmează să fie adăugat în catalog sau pentru orice produs care trebuie să fie îndepărtat din catalog.