ORDIN nr. 16 din 21 martie 2014

pentru aprobarea Directivei principale privind domeniul INFOSEC - INFOSEC 2

EMITENT: OFICIUL REGISTRULUI NAŢIONAL AL INFORMAŢIILOR SECRETE DE STAT
PUBLICAT ÎN: MONITORUL OFICIAL nr. 262 din 10 aprilie 2014
Data intrarii in vigoare : 10 aprilie 2014

În temeiul:

- art. 1 alin. (4) lit. b) şi art. 3 alin. (6) din Ordonanţa de urgenţă a Guvernului nr. 153/2002 privind organizarea şi funcţionarea Oficiului Registrului Naţional al Informaţiilor Secrete de Stat, aprobată prin Legea nr. 101/2003, cu modificările şi completările ulterioare;
- art. 55 alin. (1) din Regulamentul privind procedurile, la nivelul Guvernului, pentru elaborarea, avizarea şi prezentarea proiectelor de documente de politici publice, a proiectelor de acte normative, precum şi a altor documente, în vederea adoptării/aprobării, aprobat prin Hotărârea Guvernului nr. 561/2009,

directorul general al Oficiului Registrului Naţional al Informaţiilor Secrete de Stat emite prezentul ordin.

ART. 1

Se aprobă Directiva principală privind domeniul INFOSEC - INFOSEC 2, prevăzută în anexa care face parte integrantă din prezentul ordin.

ART. 2

La data intrării în vigoare a prezentului ordin se abrogă Ordinul directorului general al Oficiului Registrului Naţional al Informaţiilor Secrete de Stat nr. 483/2003 pentru aprobarea Directivei principale privind domeniul INFOSEC - INFOSEC 2, publicat în Monitorul Oficial al României, Partea I, nr. 874 din 9 decembrie 2003.

ART. 3

Prezentul ordin se publică în Monitorul Oficial al României, Partea I.

ART. 4

Oficiul Registrului Naţional al Informaţiilor Secrete de Stat va duce la îndeplinire prevederile prezentului ordin.

Directorul general
al Oficiului Registrului Naţional
al Informaţiilor Secrete de Stat,
Marius Petrescu

Bucureşti, 21 martie 2014.
Nr. 16.

ANEXĂ

DIRECTIVA PRINCIPALĂ
privind domeniul INFOSEC - INFOSEC 2

CAP. I
Introducere

SECŢIUNEA 1.1
Obiectiv

ART. 1
Directiva principală privind domeniul INFOSEC - INFOSEC 2, denumită în continuare directiva, stabileşte liniile directoare în domeniul securităţii sistemelor informatice şi de comunicaţii (SIC), în vederea protecţiei informaţiilor clasificate stocate, procesate sau transmise prin intermediul acestora, din perspectiva asigurării confidenţialităţii, integrităţii, disponibilităţii şi, după caz, a autenticităţii şi nerepudierii.

SECŢIUNEA 1.2
Definiţii

ART. 2
În cuprinsul prezentei directive, următorii termeni şi sintagme au următorul înţeles:
a) în cazul în care nu se fac precizări suplimentare, prin informaţii clasificate se definesc informaţii naţionale clasificate secret de stat, informaţii NATO clasificate, informaţii UE clasificate sau informaţii clasificate care fac obiectul unor tratate, acorduri ori înţelegeri internaţionale la care România este parte;
b) INFOSEC - aplicarea de măsuri de securitate pentru protecţia informaţiilor clasificate procesate, stocate sau transmise în SIC, precum şi a resurselor şi serviciilor SIC, prin asigurarea îndeplinirii obiectivelor securităţii informaţiilor: confidenţialitate, integritate, disponibilitate, autenticitate şi nerepudiere.

SECŢIUNEA 1.3
Domeniu de aplicabilitate

ART. 3
Aplicarea prevederilor prezentei directive este obligatorie pentru SIC care stochează, procesează sau transmit informaţii clasificate.
ART. 4
Prevederile prezentei directive pot fi aplicate, dacă se consideră necesar, şi pentru protecţia informaţiilor naţionale clasificate cu nivel de clasificare SECRET DE SERVICIU, a informaţiilor NATO sau UE care nu sunt clasificate, dar care au marcaje administrative ori de limitare a diseminării.
ART. 5
Oficiul Registrului Naţional al Informaţiilor Secrete de Stat (ORNISS), autorităţile desemnate de securitate (ADS), structurile/funcţionarii de securitate şi autorităţile operaţionale ale SIC (AOSIC) sunt responsabile cu asigurarea implementării prevederilor prezentei directive.

SECȚIUNEA 1.4
Elementele unui SIC

ART. 6
(1) Un SIC cuprinde totalitatea elementelor de infrastructură, organizaționale, de personal, componente, necesare pentru colectarea, procesarea, stocarea, transmiterea, afişarea, diseminarea şi distrugerea informațiilor.
(2) Tipul de componente ale SIC influențează tipul politicilor INFOSEC care trebuie aplicate şi determină modul în care se aplică principiile securității SIC definite în prezenta directivă.

CAP. II
Activități privind securitatea pe întregul ciclu de viață al SIC

SECȚIUNEA 2.1
Obiectivele securității informațiilor clasificate

ART. 7
(1) În procesul de asigurare a securității informațiilor clasificate trebuie avute în vedere următoarele obiective:
a) confidențialitatea - asigurarea controlului asupra dezvăluirii şi accesului la informațiile clasificate şi la serviciile şi resursele aferente sistemelor;
b) integritatea - asigurarea acurateței şi completitudinii informațiilor clasificate, precum şi a serviciilor şi resurselor aferente sistemelor;
c) disponibilitatea - asigurarea faptului că persoanele autorizate au acces şi pot utiliza informațiile clasificate, resursele şi serviciile aferente sistemelor;
d) autenticitatea - asigurarea identificării şi autentificării de încredere a persoanelor, dispozitivelor şi serviciilor SIC;
e) nerepudierea - asigurarea unei capacități corespunzătoare de a dovedi faptul că o acțiune sau un eveniment a avut loc, astfel încât să nu poată fi repudiată ulterior respectiva acțiune sau eveniment.
(2) Gradul de aplicabilitate a obiectivelor prevăzute la alin. (1) este specific fiecărui SIC şi este determinat pe baza unei serii de factori, incluzând obiectivele misiunii SIC, cerințele de securitate minime impuse de politicile de securitate națională, NATO, UE şi/sau ale respectivului SIC şi, după caz, rezultatele analizei riscului la adresa securității.

SECȚIUNEA 2.2
Principiile securității SIC

ART. 8
(1) În scopul realizării obiectivelor prevăzute la art. 7 se aplică un set de principii de bază, enunțate mai jos:
a) managementul riscurilor de securitate - derularea unor procese de management al riscurilor de securitate, pe întreg ciclul de viață al SIC, în vederea monitorizării, reducerii, eliminării, evitării sau acceptării riscurilor;
b) minimalizarea - instalarea şi utilizarea numai a funcțiilor, protocoalelor şi serviciilor necesare pentru îndeplinirea misiunii operaționale;
c) privilegii minime - utilizatorilor SIC li se vor acorda numai autorizațiile şi privilegiile de care aceştia au nevoie pentru îndeplinirea sarcinilor şi atribuțiilor de serviciu;

d) nodul autoprotejat - fiecare SIC va considera alte SIC ca fiind nesigure. Din această cauză vor fi implementate măsuri de protecţie pentru controlul schimbului de informaţii cu alte SIC;

e) apărarea în adâncime - măsurile de protecţie trebuie implementate pe diferite componente, în măsura în care acest lucru este posibil, astfel încât să nu existe o singură linie de apărare în cadrul SIC;

f) actualizarea stării de securitate - configuraţia de securitate a SIC trebuie să evolueze pentru a menţine nivelul de securitate adecvat, ţinând cont de schimbările din mediul de ameninţare;

g) reziliența - SIC critice trebuie să aibă capacitatea de a se adapta rapid şi/sau de a se recupera în urma oricărui tip de întrerupere, în vederea continuării operării la un nivel acceptabil, ţinându-se cont de obiectivele SIC şi de impactul pe care întreruperea îl are asupra securităţii SIC;

h) garantarea funcţionalităţilor de securitate - funcţionarea securizată a mecanismelor şi produselor care permit sau asigură servicii de securitate pentru SIC trebuie să fie garantată de către o autoritate cu competenţe în domeniu;

i) conformitatea securităţii - aplicarea acestor principii şi implementarea ulterioară a măsurilor de protecţie trebuie verificate în etapa iniţială şi apoi periodic de către Agenţia de Acreditare de Securitate (AAS). În situaţia în care sunt identificate deficienţe, acestea trebuie rezolvate.

(2) În vederea implementării principiilor enunţate la alin. (1), normele INFOSEC subsecvente prezentei directive stabilesc cerinţe detaliate şi specifice.

SECŢIUNEA 2.3
Managementul riscului de securitate

ART. 9

(1) Pentru SIC care procesează, stochează sau transmit informaţii clasificate, procesul de evaluare a riscului de securitate trebuie să facă parte din procesul de dezvoltare a sistemelor în sine.

(2) Procesul de evaluare a riscurilor de securitate se desfăşoară prin colaborarea reprezentanţilor utilizatorilor, structurii responsabile cu planificarea, AOSIC şi AAS, folosind o metodologie de evaluare a riscurilor unanim acceptată.

(3) Activitatea de evaluare implică evaluarea măsurilor existente, a modificărilor sau a noilor opţiuni, incluzând ansambluri echilibrate de măsuri de securitate, tehnice şi nontehnice.

(4) Scopul evaluării este de a selecta o soluţie care să satisfacă cerinţele beneficiarului, cerinţele de cost şi cerinţele de risc rezidual de securitate, asigurându-se totodată aplicarea standardelor minime de protecţie a informaţiilor clasificate, în conformitate cu cerinţele politicii naţionale, NATO, UE şi/sau specifice SIC, după caz.

ART. 10

(1) Managementul riscului de securitate reprezintă o abordare sistematică pentru determinarea măsurilor necesare pentru asigurarea protecţiei informaţiilor şi a SIC, pe baza evaluării valorii bunurilor supuse riscului, a ameninţărilor, vulnerabilităţilor şi impactului asupra obiectivelor organizaţiei.

(2) Managementul riscurilor de securitate este procesul prin care se realizează un echilibru între costurile legate de aplicarea măsurilor de securitate suplimentare şi avantajele aplicării acestor contramăsuri. În unele cazuri, procesul de management al riscului de securitate poate conduce la acceptarea unor riscuri mai mari, în vederea reducerii costurilor, în condiţiile în care standardele minime sunt aplicate.

(3) Managementul riscului implică planificarea, organizarea, direcţionarea şi controlul resurselor pentru a asigura faptul că riscul rămâne în limite acceptabile.

ART. 11

Riscul rezidual de securitate reprezintă acel risc ce rămâne după implementarea într-un SIC a măsurilor de securitate, dat fiind faptul că nu pot fi contracarate toate ameninţările şi că nu pot fi eliminate sau reduse toate vulnerabilităţile. Ameninţările şi vulnerabilităţile sunt dinamice, de aceea şi riscul rezidual este supus schimbărilor. Din această cauză riscul va fi gestionat de-a lungul întregului ciclu de viaţă al SIC, fapt care implică alocarea de resurse adecvate pentru derularea procesului de management al riscurilor.

ART. 12

Procesele de management al riscurilor de securitate vor fi derulate pentru monitorizarea, reducerea, eliminarea, evitarea sau acceptarea riscurilor asociate SIC.

SECŢIUNEA 2.4
Ameninţări şi vulnerabilităţi

ART. 13

(1) Evaluarea riscurilor se bazează pe o evaluare la zi a ameninţărilor şi se va referi la impactul ameninţărilor şi vulnerabilităţilor asupra îndeplinirii obiectivelor securităţii.

(2) Ameninţarea reprezintă, în termeni generali, posibilitatea de compromitere accidentală sau deliberată a securităţii. În ceea ce priveşte domeniul securităţii SIC, o astfel de compromitere implică afectarea unuia sau mai multora dintre obiectivele securităţii informaţiilor.

(3) Vulnerabilitatea reprezintă o slăbiciune sau o lipsă de control care ar permite ori ar facilita concretizarea unei ameninţări împotriva unei valori sau a unei ţinte specifice. Vulnerabilitatea poate consta într-o omisiune sau poate rezulta dintr-o deficienţă a măsurilor de securitate în ceea ce priveşte tăria acestora, completitudinea ori coerenţa şi poate fi de natură tehnică, procedurală sau operaţională.

ART. 14

Informaţiile clasificate pot fi vulnerabile la accesarea lor de către utilizatori neautorizaţi, la blocarea accesării lor de către utilizatori autorizaţi, precum şi la coruperea, modificarea neautorizată şi la ştergerea neautorizată a acestora. Pe lângă acestea, echipamentele SIC sunt complexe, costisitoare şi adesea dificil de reparat sau de înlocuit în mod operativ.

ART. 15

SIC care vehiculează informaţii clasificate reprezintă o ţintă atractivă pentru operaţiunile de spionaj, în special în situaţia în care se consideră că măsurile de securitate sunt ineficiente. SIC, în general, permit obţinerea unui volum semnificativ de informaţii în mod rapid şi fără a fi detectat. Este de presupus că acţiunile lansate de către serviciile secrete sau de către membri ori simpatizanţi ai organizaţiilor subversive sau ai grupărilor teroriste împotriva intereselor NATO, UE sau ale statelor membre sunt bine planificate şi executate. Blocarea serviciilor sistemului sau deteriorarea datelor vehiculate de aceste sisteme poate constitui, de asemenea, o ţintă atractivă, iar prejudiciul adus poate fi semnificativ, indiferent dacă sunt implicate informaţii clasificate sau neclasificate.

ART. 16

(1) Personalul din interior reprezintă un vector de ameninţare unic pentru orice organizaţie, dată fiind poziţia privilegiată a acestuia în raport cu accesul fizic şi logic la SIC şi la informaţiile vehiculate de acesta. În

contrast cu o persoană din exteriorul organizaţiei, o persoană din interior are o mai bună cunoaştere a situaţiei (de exemplu: cunoaşterea punctelor slabe), mai mult timp la dispoziţie, mai puţine măsuri de securitate pe care trebuie să le depăşească şi privilegii legitime de acces în zonele securizate, de acces la SIC şi la informaţiile vehiculate de acesta, în virtutea poziţiei pe care o ocupă în organizaţie. Aceşti factori, combinaţi cu posibilitatea pe care o are o persoană din interior de a comite orice tip de act maliţios, conduc implicit la creşterea impactului oricărui incident.

(2) În vederea descurajării, prevenirii şi contracarării acestui tip particular de ameninţare, este necesară implementarea unui set de măsuri de securitate specifice. În procesul de selectare a acestor măsuri, organizaţiile trebuie să ţină cont şi de următoarele aspecte:

a) măsurile de securitate trebuie să fie proiectate pentru a trata şi ameninţările din interior şi a susţine procedurile de răspuns şi de investigare;

b) trebuie să fie consolidate cooperarea şi schimbul de informaţii dintre responsabilii cu diferitele aspecte ale securităţii din cadrul organizaţiei (explicaţie: securitatea personalului, securitatea fizică, resurse umane, protecţie internă), care pot contribui în mod adecvat la gestionarea ameninţărilor din interior.

SECŢIUNEA 2.5
Moduri de operare de securitate

ART. 17

SIC care stochează, procesează sau transmit informaţii naţionale clasificate SECRET şi cu nivel de clasificare superior funcţionează într-unul dintre următoarele moduri de operare de securitate sau, în cazul în care este necesar, în mai multe dintre următoarele moduri de operare de securitate, de-a lungul unor perioade diferite de timp:

a) modul de operare de securitate dedicat - modul de operare în care TOATE persoanele care au acces la SIC deţin certificat de securitate sau autorizaţie de acces pentru cel mai înalt nivel de clasificare a informaţiilor stocate, procesate sau transmise în SIC şi au o necesitate de a cunoaşte comună pentru TOATE informaţiile stocate, procesate sau transmise în sistem;

b) modul de operare de securitate nivel înalt - modul de operare în care TOATE persoanele care au acces la SIC deţin certificat de securitate sau autorizaţie de acces pentru cel mai înalt nivel de clasificare a informaţiilor stocate, procesate sau transmise prin SIC, dar NU TOATE persoanele cu acces la SIC au o necesitate comună de a cunoaşte TOATE informaţiile stocate, procesate sau transmise în SIC;

c) modul de operare de securitate multinivel - modul de operare în care NU TOATE persoanele care au acces la sistem deţin certificat de securitate sau autorizaţie de acces pentru cel mai înalt nivel de clasificare a informaţiilor stocate, procesate sau transmise în SIC şi NU TOATE persoanele cu acces la sistem au o necesitate comună de a cunoaşte TOATE informaţiile stocate, procesate sau transmise în sistem.

ART. 18

SIC care stochează, procesează sau transmit informaţii clasificate NATO CONFIDENTIAL sau cu nivel de clasificare superior, informaţii din Categoria specială ori informaţii clasificate CONFIDENTIEL UE/EU CONFIDENTIAL sau cu nivel de clasificare superior funcţionează într-unul dintre următoarele moduri de operare de securitate sau, în cazul în care este necesar, în mai multe dintre următoarele moduri de operare de securitate, de-a lungul unor perioade diferite de timp:

a) modul de operare de securitate dedicat - modul de operare în care TOATE persoanele care au acces la SIC deţin certificat de securitate sau autorizaţie de acces pentru cel mai înalt nivel de clasificare a informaţiilor stocate, procesate sau transmise în SIC şi au o necesitate de a cunoaşte comună pentru TOATE informaţiile stocate, procesate sau transmise în SIC;

b) modul de operare de securitate sistem înalt - modul de operare în care TOATE persoanele care au acces la SIC deţin certificat de securitate sau autorizaţie de acces pentru cel mai înalt nivel de clasificare a informaţiilor stocate, procesate sau transmise prin SIC, dar NU TOATE persoanele cu acces la SIC au o necesitate comună de a cunoaşte TOATE informaţiile stocate, procesate sau transmise în SIC; aprobarea de a accesa informaţiile poate fi acordată la nivel informal sau individual;

c) modul de operare de securitate compartimentat - modul de operare în care TOATE persoanele care au acces la SIC deţin certificat de securitate sau autorizaţie de acces pentru cel mai înalt nivel de clasificare a informaţiilor stocate, procesate sau transmise în SIC, dar NU TOATE persoanele cu acces la sistem au autorizaţie oficială de a accesa TOATE informaţiile stocate, procesate sau transmise prin sistem. Autorizaţia oficială indică faptul că există un management oficial, centralizat al controlului accesului, iar acordarea accesului nu este la discreţia unei singure persoane;

d) modul de operare de securitate multinivel - modul de operare în care NU TOATE persoanele care au acces la sistem deţin certificat de securitate sau autorizaţie de acces pentru cel mai înalt nivel de clasificare a informaţiilor stocate, procesate sau transmise în SIC şi NU TOATE persoanele cu acces la sistem au o necesitate comună de a cunoaşte TOATE informaţiile stocate, procesate sau transmise în SIC.

ART. 19

SIC care stochează, procesează sau transmit numai informaţii cu nivel de clasificare maxim NATO RESTRICTED sau RESTREINT UE/EU RESTRICTED funcţionează într-unul dintre următoarele moduri de operare de securitate sau, în cazul în care este necesar, în mai multe dintre următoarele moduri de operare de securitate, de-a lungul unor perioade diferite de timp:

a) modul de operare de securitate dedicat - modul de operare în care TOATE persoanele care au acces la SIC au o necesitate de a cunoaşte comună pentru TOATE informaţiile stocate, procesate sau transmise în sistem;

b) modul de operare de securitate sistem înalt - modul de operare în care NU TOATE persoanele cu acces la sistem au o necesitate comună de a cunoaşte TOATE informaţiile stocate, procesate sau transmise în sistem.

NOTĂ:

Aceste interpretări ale modurilor de operare de securitate sunt incluse pentru a ilustra faptul că pentru acces la informaţii cu nivel de clasificare maxim NATO RESTRICTED sau RESTREINT UE/EU RESTRICTED nu este necesar un certificat de securitate sau o autorizaţie de acces.

ART. 20

Informaţiile din Categoria specială sunt procesate numai în modul de operare de securitate "dedicat".

SECŢIUNEA 2.6

Procesul de acreditare de securitate

ART. 21

Procesul de acreditare de securitate determină modul în care măsurile de securitate a SIC implementate sunt conforme cu cerinţele stabilite pentru protecţia informaţiilor clasificate procesate, stocate sau transmise, precum şi a sistemelor în sine.

ART. 22

Procesul de acreditare de securitate determină dacă a fost îndeplinit un nivel adecvat de protecţie, precum şi dacă acesta se menţine. Elementul central al acestui proces este identificarea unui nivel acceptabil al riscului rezidual, care trebuie să fie monitorizat pe tot ciclul de viaţă al SIC.

ART. 23

Procesul de acreditare de securitate se desfăşoară de către AAS în conformitate cu prevederile Directivei privind managementul INFOSEC pentru sisteme informatice şi de comunicaţii - INFOSEC 3, aprobată prin Ordinul directorului general al Oficiului Registrului Naţional al Informaţiilor Secrete de Stat nr. 484/2003, denumită în continuare INFOSEC 3.

ART. 24

În conformitate cu prevederile politicii de securitate a informaţiilor şi cu specificaţiile AAS, se elaborează documentaţia de securitate a SIC. Documentaţia de securitate este necesară pe întreg ciclul de viaţă al SIC, de la etapa de planificare, până la momentul dezafectării sistemului. Procesul de dezvoltare a documentaţiei de securitate este iterativ, pe întreg ciclul de viaţă al SIC.

SECŢIUNEA 2.7

Auditul securităţii

ART. 25

Activităţile de audit de securitate sunt realizate pentru a verifica faptul că SIC care vehiculează informaţii clasificate sunt conforme cu prevederile politicii de securitate aplicabile.

ART. 26

Metodele de audit de securitate includ inspecţiile de securitate, analize, interviuri şi testări. Este recomandabil ca analizele şi testele să fie susţinute de instrumente automate.

ART. 27

Activităţile de audit de securitate se realizează de către sau sub coordonarea AAS.

SECŢIUNEA 2.8

Procesul de continuare a activităţii

ART. 28

Continuarea activităţii reprezintă un proces critic prin care se identifică elemente care ameninţă îndeplinirea misiunii organizaţiei. Totodată, acest proces creează un cadru de consolidare a rezilienţei, cu capacitatea de răspuns eficient care să minimizeze întreruperea activităţii la nivelul organizaţiei şi afectarea obiectivelor acesteia, în cazul unui incident.

ART. 29

În contextul procesului de continuare a activităţii, măsurile de securitate necesare pentru sprijinirea rezilienţei unui SIC, inclusiv planurile şi procedurile, sunt identificate prin intermediul unui proces de evaluare a riscului şi al analizei de impact şi se concretizează în planul pentru continuarea activităţii, întocmit la nivelul organizaţiei. În timp ce procesul de evaluare a riscului conduce la identificarea funcţiilor şi bunurilor critice, precum şi a riscurilor care pot determina întreruperea misiunii organizaţiei, analiza de impact identifică distrugerile sau pierderile potenţiale în cazul unui incident, forma pe care o pot lua distrugerile şi modul în care pot evolua acestea în timp.

SECȚIUNEA 2.9
Managementul încrederii

ART. 30

(1) Încrederea în securitatea SIC este un aspect complex care vizează SIC, componentele sale, lanțul de achiziție prin care sunt procurate acestea, precum şi alte elemente care pot avea impact asupra securității SIC.

(2) Managementul încrederii reprezintă un element esențial, dat fiind faptul că acesta permite determinarea măsurii în care SIC, componentele sale şi lanțul de achiziție sunt sigure.

(3) Elementele care contribuie la crearea încrederii pot fi de natură oficială, implicând tehnici de asigurare, cum sunt certificarea produselor sau a proceselor derulate la nivelul furnizorului, sau mai puțin riguroase, cum ar fi informațiile cu privire la producător (de exemplu: reputația).

(4) Funcțiile de securitate ale SIC care vehiculează informații clasificate trebuie să fie confirmate de către autorități competente, prin tehnici oficiale de asigurare.

(5) Tehnicile oficiale de asigurare în cazul produselor includ:

a) evaluarea, ca tehnică de examinare detaliată a aspectelor de securitate ale unui produs de către entitățile naționale sau internaționale abilitate. Evaluarea confirmă prezența funcționalităților de securitate necesare, absența efectelor secundare ale acestor funcționalități şi face o analiză a incoruptibilității acestor funcționalități. Evaluarea stabileşte măsura în care sunt satisfăcute cerințele de securitate pentru un produs şi stabileşte conformitatea funcțiilor de securitate ale unui produs;

b) certificarea, ca proces de emitere de către o autoritate națională sau internațională abilitată a unui document oficial, ca rezultat al unei evaluări încheiate cu succes.

(6) Tehnicile oficiale de asigurare în cazul SIC includ:

a) evaluarea, ca tehnică de examinare detaliată a aspectelor de securitate ale unui SIC de către entitățile naționale sau internaționale abilitate. Evaluarea stabileşte dacă SIC satisface cerințele de securitate predefinite;

b) acreditarea de securitate, ca proces care, susținut de rezultatele unei evaluări, determină dacă în SIC a fost implementat şi este menținut un nivel adecvat de protecție.

ART. 31

(1) Cerințele de securitate pentru SIC sunt identificate în etapa de planificare a SIC de către AOSIC, în colaborare cu AAS.

(2) Procesul de identificare a cerințelor de securitate pentru SIC ia în considerare cerințele stabilite în reglementările naționale, NATO, UE şi/sau specifice SIC, după caz, privind protecția informațiilor clasificate, analiza arhitecturii de securitate şi rezultatele procesului de analiză a riscului.

(3) În cazul în care sunt necesare evaluarea şi certificarea produselor, se utilizează Metodologia asociată criteriilor comune de evaluare a securității IT, ori de câte ori aceasta este aplicabilă.

(4) Metodologia prevăzută la alin. (3) nu se aplică produselor criptografice şi TEMPEST, pentru care se stabilesc criterii şi metodologii de evaluare specifice.

ART. 32

(1) Componentele hardware, firmware şi software pentru care se aplică specificații de proiectare detaliate sunt proiectate şi manufacturate în state membre NATO sau UE, după caz, în funcție de tipul informațiilor ce urmează să fie vehiculate prin SIC.

(2) În cazul în care componentele prevăzute la alin. (1) sunt proiectate şi/sau manufacturate într-un stat non-NATO sau non-UE, trebuie consultat ORNISS.

ART. 33

Pentru achiziţia produselor de securitate INFOSEC trebuie consultat Catalogul naţional cu pachete, produse şi profile de protecţie INFOSEC, aprobat prin Ordinul directorului general al Oficiului Registrului Naţional al Informaţiilor Secrete de Stat nr. 25/2012, cu modificările şi completările ulterioare.

ART. 34

Managementul încrederii în lanţul de achiziţii prin intermediul căruia SIC şi componentele acestuia sunt procurate implică şi faptul că informaţiile clasificate diseminate către industrie, generate în baza unui contract cu industria şi a contractelor clasificate, trebuie să fie protejate în conformitate cu prevederile reglementărilor naţionale în domeniul protecţiei informaţiilor clasificate.

SECŢIUNEA 2.10
Interconectarea SIC

ART. 35

(1) În vederea atingerii obiectivelor asumate, organizaţiile au nevoie să îşi interconecteze propriile SIC cu SIC ale altor organizaţii, cu diferite comunităţi de interes, diferite nivele de clasificare şi diferite standarde de securitate.

(2) În scopul respectării principiului SIC autoprotejat, sunt necesare analizarea riscului potenţial reprezentat de interconectare, fie aceasta în mod direct sau în cascadă, şi implementarea de măsuri de securitate specifice pentru protejarea interconectării.

(3) Pentru toate interconectările SIC care vehiculează informaţii clasificate este necesar ca AAS să aprobe:

a) metoda de interconectare şi serviciile oferite;

b) metodologia de management al riscului şi rezultatele analizei riscului;

c) arhitectura de securitate şi măsurile de securitate pentru asigurarea respectării obiectivelor securităţii;

d) documentaţia de securitate, inclusiv planul de testare a securităţii şi rezultatele aplicării acestui plan.

ART. 36

INFOSEC 3 stabileşte cerinţele de acreditare de securitate, iar directivele tehnice şi de implementare stabilesc măsurile care trebuie implementate.

ART. 37

(1) Cerinţele privind măsurile de protecţie ce trebuie implementate în SIC care vehiculează informaţii clasificate şi sunt conectate la internet sau la reţele similare din domeniul public trebuie să ţină seama de riscurile de securitate excepţionale pe care aceste tipuri de reţele publice le ridică, din cauza accesibilităţii necontrolate, pe scară largă, a susceptibilităţii create de protocoalele orientate pe lipsa conectării şi a vulnerabilităţii SIC finale faţă de exploatare.

(2) Interconectarea directă sau în cascadă la internet sau la alte reţele similare din domeniul public a SIC care vehiculează informaţii clasificate de nivel maxim STRICT SECRET sau echivalent trebuie să fie:

a) strict controlată;

b) în conformitate cu cerinţele stabilite de AAS;

c) evaluată şi certificată din punctul de vedere al mecanismelor de securitate;

d) supusă unei analize periodice oficiale a vulnerabilităţilor.

(3) Conectarea directă sau tip cascadă a SIC care vehiculează informaţii clasificate STRICT SECRET DE IMPORTANŢĂ DEOSEBITĂ sau echivalent ori informaţii din Categoria specială la internet sau la reţele similare din domeniul public este interzisă.

SECȚIUNEA 2.11
Conectarea SIC care vehiculează informații clasificate la internet sau la alte rețele din domeniul public

ART. 38
(1) SIC care vehiculează informații clasificate pot utiliza internetul sau rețele similare din domeniul public ca infrastructură de comunicații, în condițiile în care se asigură protecția criptografică adecvată. În acest caz, obiectivele securității trebuie analizate cu multă grijă.
(2) Singurele tipuri de informații care pot fi transmise în clar (necriptate) sunt următoarele:
a) informațiile provenind din surse deschise, informațiile cu caracter public sau informațiile naționale, NATO ori UE pentru care există aprobarea de diseminare publică;
b) informațiile NATO și UE neclasificate, care nu poartă marcaje administrative sau marcaje privind controlul diseminării, care să indice gradul de sensibilitate a informațiilor.
(3) Numai informațiile provenind din surse deschise și informațiile cu caracter public sau informațiile pentru care există aprobarea de diseminare publică pot fi postate pe site-uri web sau pagini web publice și se vor supune cerințelor de asigurare a integrității impuse de emitentul informației.
ART. 39
(1) Pentru toate conexiunile SIC la internet sau la rețele similare din domeniul public, AAS aprobă următoarele:
a) metoda de conectare și serviciile furnizate;
b) evaluarea riscului de securitate și metodologia de management al riscului utilizată, precum și rezultatele analizei riscului de securitate;
c) procedurile și mecanismele de asigurare a faptului că informațiile clasificate sau informațiile care poartă un marcaj administrativ sau de diseminare limitată nu sunt transmise pe canale de comunicații neprotejate;
d) mecanismele și/sau procedurile implementate pentru asigurarea confidențialității, integrității și/sau disponibilității informațiilor, precum și a serviciilor/resurselor sistemelor;
e) mecanismele și/sau procedurile aplicate pentru îndeplinirea cerințelor privind evidența;
f) documentația de securitate, inclusiv planul de testare și rezultatele testărilor de securitate.
(2) AAS este responsabilă pentru verificarea implementării inițiale a măsurilor de securitate și a verificărilor periodice.

SECȚIUNEA 2.12
Securitatea aplicațiilor

ART. 40
(1) Aspectele de securitate trebuie înglobate în ciclul de viață (proiectare, dezvoltare, implementare și întreținere) al componentelor software special dezvoltate pentru vehicularea de informații clasificate, avându-se în vedere obiectivele de securitate definite pentru SIC.
(2) Aplicațiile sunt supuse testărilor de securitate, managementului securității (de exemplu: versiuni de bază) și controlului modificărilor (de exemplu: patch-uri).

SECȚIUNEA 2.13
Securitatea criptografică

ART. 41
Implementarea securității criptografice în SIC care vehiculează informații clasificate se realizează în conformitate cu prevederile reglementărilor naționale, NATO, UE sau specifice SIC, după caz, specifice domeniului.

SECȚIUNEA 2.14
Securitatea emisiilor

ART. 42
Cerințele relevante din punctul de vedere al securității emisiilor sunt cuprinse în directivele și ghidurile INFOSEC emise de către ORNISS.

SECȚIUNEA 2.15
Logurile de securitate

ART. 43
(1) SIC care vehiculează informații clasificate sunt protejate de măsuri de securitate pentru detecția activităților malițioase și a defecțiunilor, prin colectarea, analiza și stocarea informațiilor referitoare la evenimente relevante din punctul de vedere al securității.
(2) Măsurile prevăzute la alin. (1) sunt necesare pentru a asigura informații suficiente, inclusiv trasabilitatea evenimentelor, în vederea investigării unei compromiteri accidentale sau deliberate a obiectivelor securității informațiilor, precum și a unei tentative de compromitere a acestora, proporțional cu prejudiciul care poate fi produs.
(3) Cerințele de colectare a informațiilor referitoare la evenimente relevante din punctul de vedere al securității sunt definite având în vedere că logurile de securitate au un rol esențial pentru sprijinirea activității de audit al securității efectuate de AAS.
(4) Perioada de analiză și de păstrare a logurilor de securitate se aprobă de către AAS, pe baza analizei riscului și având în vedere următoarele aspecte:
a) obiectivele de securitate ale SIC;
b) mediul de amenințare;
c) tipul logurilor și al datelor colectate;
d) frecvența analizei logurilor;
e) utilizarea de instrumente automate pentru verificarea logurilor;
f) cerințele privind investigarea, auditul și alte cerințe legale.

SECȚIUNEA 2.16
Configurația de securitate de bază

ART. 44
(1) Pentru SIC care vehiculează informații clasificate și componentele hardware și software critice sunt definite configurații de securitate de bază, care trebuie aplicate și păstrate la zi, prin procesele de management al configurației și de cel de control al modificărilor pe întregul ciclu de viață al SIC.
(2) Configurațiile de bază ale securității includ setările de securitate necesare pentru consolidarea configurației componentelor critice, înainte de instalare, și cerințele pentru actualizările de securitate ale componentelor aflate în operare.

SECȚIUNEA 2.17
Apărarea împotriva software-ului malițios

ART. 45
(1) Evoluția complexității software-ului malițios și capacitatea sa de a executa atacuri direcționate impun acordarea unei atenții sporite.
(2) În SIC care vehiculează informații clasificate sunt utilizate soluții de detecție care să blocheze instalarea, să prevină executarea, să trimită în carantină software-ul malițios și să alerteze personalul responsabil cu activitățile asociate răspunsului la incidente.

SECȚIUNEA 2.18
Controlul accesului

ART. 46
(1) Controlul accesului reprezintă o primă linie de apărare, dat fiind că acesta permite identificarea, autentificarea, autorizarea și evidența oricărei entități (de exemplu: persoană, dispozitiv, serviciu) care solicită acces la SIC și la elementele acestuia.
(2) În SIC care vehiculează informații clasificate, controlul accesului se implementează pentru a preveni operațiuni neautorizate asupra SIC și a elementelor acestuia (de exemplu: date, dispozitive, servicii).
ART. 47
(1) În selectarea unui model de control al accesului și a măsurilor de securitate asociate acestuia, AOSIC trebuie să țină cont de următorii factori:
a) modalitatea și măsura în care o organizație implementează managementul informațiilor pot avea impact asupra proiectării măsurilor de control al accesului;
b) măsurile tehnice sunt proiectate în contextul mediului de securitate general al SIC, pentru a funcționa în mod coerent și coordonat cu măsurile de control al accesului fizic și administrativ;
c) măsurile tehnice trebuie să permită acces securizat și granular la informații pe baza modului de operare de securitate pentru care a fost proiectat SIC și a cerințelor validate privind schimbul de informații între comunități de interese din cadrul SIC sau cu alte SIC.
(2) Limitele tradiționale ale rețelelor sunt elemente majore pentru proiectarea securității infrastructurii unui SIC.
(3) AOSIC trebuie să ia în considerare faptul că aceste limite nu pot fi considerate un punct de referință exhaustiv atunci când se are în vedere protecția informațiilor clasificate vehiculate în SIC cu cerințe complexe de schimb de informații și control al accesului.
(4) În situația prevăzută la alin. (3), AOSIC adoptă strategii de apărare în adâncime, care includ politici și măsuri de securitate specifice, pentru protecția obiectelor informaționale, pe baza identității și a altor atribute relevante ale entității care solicită accesul la aceste obiecte, precum și pe baza proprietăților acelor obiecte, denumite în mod comun metadate.
(5) În contextul controlului accesului, managementul identității și al accesului joacă un rol important, cuprinzând persoane, procese și produse necesare pentru managementul identităților digitale (de exemplu: persoane, dispozitive, servicii, date) pe întreg ciclul de viață al acestora și accesul la resursele SIC.
ART. 48
Pentru SIC aparținând NATO, accesul la resursele SIC se gestionează prin capacități de management al identificării și autentificării, care să asigure:

a) managementul identităţilor digitale, precum şi al atributelor, privilegiilor şi credenţialelor acestora;
b) furnizarea de servicii de autentificare, incluzând identificarea puternică, în funcţie de rezultatele analizei riscului;
c) prevenirea furtului şi reutilizării credenţialelor;
d) furnizarea de autorizări granulare, pe baza politicilor de acces;
e) auditul utilizatorilor şi activităţilor din sistem.

ART. 49

(1) Cerinţele minime privind identificarea şi autentificarea pe SIC care vehiculează informaţi clasificate sunt stabilite prin reglementările în domeniu emise de către ORNISS şi, după caz, se vor avea în vedere rezultatele procesului de management al riscului de securitate.
(2) Cerinţele privind identificarea şi autentificarea trebuie să definească proprietăţile mecanismelor de securitate.

SECŢIUNEA 2.19
Răspunsul la incidente

ART. 50

(1) Un incident de securitate în SIC reprezintă orice anomalie detectată care a compromis sau are potenţialul de a compromite sistemele de comunicaţii, sistemele informatice ori alte sisteme electronice sau informaţiile stocate, procesate ori transmise prin intermediul acestor sisteme.
(2) Pentru gestionarea incidentelor de securitate se desemnează personal specializat din punct de vedere tehnic.

ART. 51

Incidentele care vizează securitatea SIC se raportează la ORNISS.

ART. 52

(1) În cazul în care survin incidente de securitate în SIC NATO care vehiculează informaţii clasificate, ORNISS raportează incidentele către Oficiul de Securitate al NATO (NOS) şi către NATO Computer Incident Response Capability (NCIRC).
(2) În cazul în care survin incidente de securitate în SIC UE care vehiculează informaţii clasificate, ORNISS raportează incidentele către Secretariatul General al Consiliului UE.
(3) În următoarele situaţii, raportarea către NOS/NCIRC, respectiv către Secretariatul General al Consiliului UE trebuie făcută cu maximă prioritate:
a) breşa de securitate vizează informaţii COSMIC TOP SECRET, NATO SECRET, informaţii din Categoria specială, TRES SECRET UE/EU TOP SECRET sau informaţii SECRET UE/EU SECRET;
b) dezvăluirea neautorizată de informaţii clasificate către mass media (de exemplu: presă, bloguri, websites) sau către alte entităţi (de exemplu: grupări politice, teroriste sau criminale);
c) culegere de date neautorizată;
d) suspiciunea de activităţi de spionaj;
e) activitate maliţioasă internă (de exemplu: ameninţări provenite din interior);
f) incidente care implică accesul privilegiat la SIC;
g) incidente care implică elemente criptografice;
h) incidente care au un impact semnificativ asupra organizaţiei.
(4) Toate celelalte tipuri de incidente de securitate care afectează SIC NATO sau SIC UE se raportează de către ORNISS la NOS, respectiv Secretariatul General al Consiliului UE, în scop de analiză şi realizarea de statistici.
(5) Identificarea, colectarea, achiziţia şi păstrarea probelor digitale sunt realizate de către personal instruit în domeniul investigaţiilor digitale, într-o

manieră sistematică şi imparţială, în vederea conservării integrităţii, autenticităţii şi calităţii de probe valabile, în conformitate cu prevederile legale.

SECŢIUNEA 2.20
Infrastructura de management al securităţii

ART. 53
În SIC care vehiculează informaţii clasificate sunt implementate mecanisme şi proceduri de management al securităţii care să asigure descurajarea, prevenirea, detectarea, rezistenţa şi recuperarea în urma unui incident care afectează securitatea informaţiilor şi a SIC.

SECŢIUNEA 2.21
Instruirea şi conştientizarea în domeniul securităţii SIC

ART. 54
(1) Un factor major în realizarea unui nivel de securitate adecvat pentru un SIC este implementarea unui program activ de instruire şi conştientizare a tuturor utilizatorilor SIC.
(2) Programele de instruire şi educaţie de securitate trebuie să îi facă pe utilizatori conştienţi cu privire la vulnerabilităţile şi ameninţările generale aplicabile sistemului pe care îl utilizează, pentru a înţelege motivul pentru care trebuie să menţină măsurile de protecţie şi responsabilităţile pe care le au în acest sens. Trebuie acordată o atenţie specială ameninţărilor emergente şi celor specifice (de exemplu: atacuri cu ţintă bine definită, ingineria socială, ameninţări din interior), dat fiind că acestea exploatează comportamentul uman.
(3) Instruirea şi educaţia de securitate trebuie să vizeze managementul superior, structurile de planificare, de implementare şi operaţionale, responsabilii cu securitatea şi utilizatorii, pentru a asigura faptul că responsabilităţile de securitate sunt corect înţelese. În acest context trebuie identificate standarde minime de instruire de securitate.

CAP. III
Activităţi legate de securitatea SIC pe întregul ciclu de viaţă al sistemului

ART. 55
(1) Prezentul capitol prezintă activităţile minime din domeniul securităţii SIC ce trebuie întreprinse de-a lungul întregului ciclu de viaţă al sistemului, precum şi autorităţile şi personalul responsabile de derularea acestor activităţi.
(2) Activităţile prevăzute la alin. (1) se bazează pe cerinţele stabilite în detaliu în directivele INFOSEC subsecvente prezentei directive.
(3) Sunt identificate următoarele etape ale ciclului de viaţă al unui SIC, care pot fi adaptate în conformitate cu cerinţele operaţionale:
a) planificarea;
b) dezvoltarea şi achiziţia;
c) implementarea şi acreditarea de securitate;
d) exploatarea operaţională;
e) modificarea;
f) scoaterea din uz şi disponibilizarea echipamentului.
(4) Activităţile minime legate de securitatea SIC prezentate în continuare în secţiunile 3.1-3.6 scot în evidenţă modul în care vor fi utilizate directivele şi ghidurile INFOSEC subsecvente prezentei directive.

SECȚIUNEA 3.1
Planificarea SIC

ART. 56
În etapa de planificare a SIC se desfăşoară următoarele activităţi legate de securitatea SIC, de care sunt responsabile următoarele autorităţi:

Activitatea	Autoritatea/Personalul/ responsabilă/responsabil
1. Informarea AAS despre planificarea unui SIC	Structura de planificare şi implementare a SIC
2. Stabilirea unei autorităţi operaţionale a SIC (AOSIC) care răspunde de securitatea sistemului (sau atribuirea acestei responsabilităţi unei structuri funcţionale deja existente). Identificarea sarcinilor legate de securitatea SIC	Structura de planificare şi implementare a SIC, în colaborare cu AAS
3. Stabilirea bazei pentru acreditarea de securitate, prin dezvoltarea unei strategii de acreditare de securitate	Structura de planificare şi implementare a SIC, în colaborare strânsă cu AAS
4. Aprobarea strategiei de acreditare de securitate	AAS
5. Identificarea cerinţelor privind evaluarea riscurilor de securitate şi a metodologiilor utilizate pentru evaluarea şi managementul riscurilor	AAS, în colaborare cu structura de planificare şi implementare sau cu managerul de proiect
6. Efectuarea unei evaluări iniţiale a riscurilor, în conformitate cu cerinţele stabilite de AAS	Structura de planificare şi implementare a SIC sau managerul de proiect (pentru aspectele tehnice şi de implementare INFOSEC) şi AOSIC, în colaborare cu AAS
7. Dezvoltarea unei arhitecturi de securitate iniţiale, pe baza obiectivelor SIC şi a rezultatelor analizei iniţiale a riscurilor de securitate	Structura de planificare şi implementare a SIC şi AOSIC, cu consultarea AAS
8. Aprobarea rezultatelor evaluării iniţiale a riscurilor de securitate	AAS
9. Identificarea cerinţelor iniţiale pentru produsele care necesită evaluare şi certificare (de exemplu: produse criptografice) şi identificarea cerinţelor aplicabile lanţului de achiziţie a acestora	Structura de planificare şi implementare a SIC sau managerul de proiect şi AOSIC, în colaborare cu AAS

10. Identificarea cerinţelor pentru configuraţia de securitate de bază, pentru managementul configuraţiei şi controlul modificărilor	Structura de planificare şi implementare a SIC sau managerul de proiect, furnizorul de servicii SIC, în colaborare cu AAS
11. Identificarea cerinţelor iniţiale de instruire şi conştientizare	Structura de planificare şi implementare a SIC sau managerul de proiect, în colaborare cu AAS
12. Identificarea cerinţelor iniţiale privind continuarea activităţii	Structura de planificare şi implementare a SIC şi AOSIC, în colaborare cu AAS
13. Identificarea cerinţelor iniţiale privind păstrarea logurilor	Structura de planificare şi implementare a SIC şi AOSIC, în colaborare cu AAS
14. Elaborarea documentaţiei cu cerinţele de securitate iniţiale sau, unde este cazul, elaborarea anexei de securitate la pachetele de capacităţi. Folosirea, unde este cazul, a profilelor de protecţie	AOSIC, structura de planificare şi implementare a SIC sau managerul de proiect, în colaborare cu AAS şi Agenţia de Securitate pentru Informatică şi Comunicaţii (ASIC)
15. Aprobarea documentaţiei cu cerinţele de securitate iniţiale sau, unde este cazul, aprobarea anexei de securitate la pachetele de capacităţi	AAS

SECŢIUNEA 3.2
Dezvoltarea şi achiziţia SIC

ART. 57

În etapa de dezvoltare şi achiziţie a SIC se desfăşoară următoarele activităţi referitoare la securitatea SIC, de care sunt responsabile următoarele autorităţi:

Activitatea	Autoritatea/Personalul/ responsabilă/responsabil
1. Detalierea evaluării riscurilor de securitate, în conformitate cu cerinţele impuse de AAS	Structura de planificare şi implementare a SIC sau managerul de proiect, împreună cu AAS
2. Verificarea arhitecturii securităţii SIC, pentru a se asigura, unde este posibil, interoperabilitatea măsurilor de securitate şi integrarea noului SIC în infrastructura deja existentă	Structura de planificare şi implementare a SIC sau managerul de proiect
3. Aprobarea rezultatelor reevaluării riscurilor de securitate	AAS

4. Aprobarea arhitecturii de securitate	AAS
5. Elaborarea unei specificaţii detaliate cu privire la măsurile de securitate fizică, a personalului şi a informaţiilor	AOSIC, în colaborare cu structura de planificare şi implementare a SIC, administratorul de securitate al obiectivului şi AAS
6. Elaborarea unei specificaţii detaliate a măsurilor de securitate a SIC (referitoare la securitatea calculatoarelor, a transmisiei, măsuri criptografice şi radiaţii electromagnetice compromiţătoare), în conformitate cu cerinţele impuse de AAS, referitoare la funcţionalitatea securităţii şi, unde este cazul, a interconectării SIC	AOSIC, în colaborare cu structura de planificare şi implementare a SIC, administratorul de securitate al obiectivului şi AAS
7. Detalierea cerinţelor privind produsele care necesită evaluare şi certificare şi a celor privind lanţul de achiziţie a acestora	Structura de planificare şi implementare a SIC sau managerul de proiect, în colaborare cu AAS
8. Detalierea cerinţelor privind managementul configuraţiei de securitate de bază şi controlul modificărilor	Structura de planificare şi implementare a SIC sau managerul de proiect, în colaborare cu AAS
9. Detalierea cerinţelor privind instruirea şi conştientizarea	Structura de planificare şi implementare a SIC sau managerul de proiect, în colaborare cu AAS
10. Detalierea cerinţelor privind continuarea activităţii	Structura de planificare şi implementare a SIC sau managerul de proiect, în colaborare cu AAS
11. Detalierea cerinţelor privind păstrarea logurilor	Structura de planificare a SIC sau managerul de proiect, în colaborare cu AAS
12. Aprobarea cerinţelor privind managementul configuraţiei de securitate de bază şi controlul modificărilor	Structura de planificare şi implementare a SIC sau managerul de proiect, în colaborare cu AAS
13. Aprobarea cerinţelor privind instruirea şi conştientizarea	AOSIC, în colaborare cu AAS
14. Aprobarea cerinţelor privind continuarea activităţii	AOSIC, în colaborare cu AAS
15. Aprobarea cerinţelor privind păstrarea logurilor	AAS, în colaborare cu AOSIC

16. Aprobarea cerinţelor de securitate pentru produsele care necesită evaluare şi certificare şi pentru lanţul de achiziţie	AAS
17. Consultarea listelor cu produse de securitate a SIC în scopul identificării produselor care satisfac cerinţele impuse SIC	Structura de planificare şi implementare a SIC, în colaborare cu AOSIC şi AAS
18. Dezvoltarea cerinţelor operaţionale pentru produse şi mecanisme criptografice, unde este cazul	Structura de planificare şi implementare a SIC, în colaborare cu AOSIC şi AAS
19. Elaborarea caracteristicilor tehnice ale mecanismelor şi produselor criptografice pentru SIC care au şi finanţare NATO/UE, unde este cazul	NATO Consultation, Command and Control Board (C3B) sau Secretariatul General al Consiliului UE, după caz
20. Informarea ASIC cu privire la nevoia de mecanisme şi produse criptografice, unde este cazul	Structura de planificare şi implementare a SIC sau managerul de proiect
21. Stabilirea unui program pentru evaluarea şi selectarea mecanismelor şi produselor criptografice, unde este cazul	ASIC, în colaborare cu structura de planificare şi implementare a SIC sau cu managerul de proiect şi AOSIC
22. Efectuarea evaluării, selecţiei şi aprobării mecanismelor şi produselor criptografice, unde este cazul	Entităţi evaluatoare de produse criptografice, în colaborare cu ASIC
23. Stabilirea cerinţelor pentru testarea şi evaluarea securităţii SIC sau, unde este cazul, a interconectării SIC	AAS, în colaborare cu structura de planificare şi implementare a SIC sau cu managerul de proiect şi AOSIC
24. Asigurarea faptului că bugetul estimat cuprinde toate nevoile financiare pentru evaluare şi certificare în scopul stabilirii unei finanţări corespunzătoare	Structura de planificare şi implementare a SIC sau managerul de proiect, în colaborare cu AAS
25. Continuarea dezvoltării documentaţiei cu cerinţele de securitate	Structura de planificare şi implementare a SIC sau managerul de proiect, în colaborare cu AAS
26. Aprobarea documentaţiei cu cerinţele de securitate	AAS
27. Asigurarea faptului că Service Level Agreement (SLA) stabilit între AOSIC şi furnizorul de servicii pentru SIC cuprinde cel puţin cerinţele privind implementarea şi menţinerea	Structura de planificare şi implementare a SIC sau managerul de proiect, în colaborare cu AAS

măsurilor de securitate, precum şi cele privind monitorizarea şi controlul modificărilor	

SECŢIUNEA 3.3
Implementarea şi acreditarea de securitate a SIC

ART. 58

În etapa de implementare şi acreditare de securitate a unui SIC se desfăşoară următoarele activităţi referitoare la securitatea SIC, de care sunt responsabile următoarele autorităţi:

Activitatea	Autoritatea/Personalul/ responsabilă/responsabil
1. Detalierea cerinţelor privind testarea şi evaluarea securităţii SIC sau, unde este cazul, a interconectării SIC	AAS, în colaborare cu structura de planificare şi implementare a SIC şi AOSIC
2. Elaborarea planului de testare şi verificare a securităţii SIC	Structura de planificare şi implementare a SIC, în colaborare cu AOSIC şi AAS
3. Derularea, unde este cazul, a activităţilor necesare pentru evaluarea şi certificarea produselor, în conformitate cu metodologiile de evaluare aprobate	ASIC, în cooperare cu entităţile evaluatoare şi AOSIC
4. Efectuarea testării securităţii în conformitate cu planul convenit pentru testarea şi verificarea securităţii	Furnizorul de servicii pentru SIC, în colaborare cu structura de planificare şi implementare a SIC şi AAS
5. Analizarea rezultatelor testării securităţii	AAS
6. Identificarea măsurilor de securitate suplimentare care trebuie implementate în SIC, în cazul în care rezultatul testării şi verificării nu este satisfăcător	Structura de planificare şi implementare a SIC, împreună cu furnizorul de servicii şi AAS
7. Analizarea şi convenirea asupra riscului rezidual care poate fi acceptat	AOSIC
8. Analizarea şi convenirea asupra continuării procesului de management al riscurilor	AAS, împreună cu AOSIC
9. Completarea documentaţiei cu cerinţele de securitate	Structura de planificare şi implementare a SIC sau managerul de

	proiect, în colaborare cu AAS
10. Aprobarea SLA stabilit între AOSIC şi furnizorul de servicii pentru SIC	AOSIC şi furnizorul de servicii
11. Formularea Procedurilor Operaţionale de Securitate (PrOpSec) pentru SIC	Furnizorul de servicii SIC, în colaborare cu personalul care are responsabilităţi în domeniul securităţii SIC
12. Aprobarea documentaţiei cu cerinţele de securitate şi a PrOpSec	AAS
13. Realizarea instruirii şi conştientizării iniţiale	AOSIC, structura de planificare şi implementare a SIC şi furnizorul de servicii SIC, după caz
14. Acreditarea SIC sau, unde este cazul, a interconectării SIC şi emiterea documentului oficial privind acreditarea, care include perioada de valabilitate a acesteia	AAS
15. Stabilirea condiţiilor pentru reacreditarea SIC	AAS

SECŢIUNEA 3.4
Exploatarea operaţională a SIC

ART. 59

În etapa de exploatare operaţională a unui SIC se desfăşoară următoarele activităţi referitoare la securitatea SIC, de care sunt responsabile următoarele autorităţi:

Activitatea	Autoritatea/Personalul/ responsabilă/responsabil
1. Autorizarea SIC în vederea operării	AOSIC
2. Stocarea, procesarea sau transmiterea informaţiilor clasificate în mediul operaţional, în conformitate cu PrOpSec aprobate, inclusiv administrarea SIC şi a securităţii acestuia, şi în acord cu prevederile SLA	Furnizorul de servicii SIC, în colaborare cu personalul care are responsabilităţi în domeniul securităţii SIC
3. Menţinerea configuraţiilor de securitate de bază prin managementul configuraţiei şi controlul modificărilor	Furnizorul de servicii SIC, în colaborare cu AAS

4. Continuarea procesului de management al riscurilor de securitate, în conformitate cu cerinţele AAS. Aceasta include raportarea către conducerea organizaţiei care utilizează sistemul şi AAS a schimbărilor apărute privind riscurile datorate evoluţiei ameninţărilor şi vulnerabilităţilor, precum şi schimbărilor în starea sistemului (de exemplu: configurare, conformitate cu configuraţiile de securitate de bază, măsuri de securitate fizică şi de personal)	AOSIC, în colaborare cu furnizorul de servicii SIC şi AAS
5. Detectarea şi răspunsul la incidentele INFOSEC, în conformitate cu cerinţele politicilor naţionale, NATO, UE şi PrOpSec	AOSIC şi furnizorul de servicii SIC, în colaborare cu AAS
6. Asigurarea periodică a instruirii şi conştientizării	AOSIC sau furnizorul de servicii SIC, după caz
7. Realizarea, în acord cu cerinţele AAS, a evaluărilor periodice ale vulnerabilităţilor şi maximizarea utilizării instrumentelor automate pentru evaluarea permanentă a conformităţii SIC cu configurările de securitate de bază	Furnizorul de servicii SIC sau o echipă de evaluare a vulnerabilităţilor constituită separat, în colaborare cu AAS şi AOSIC
8. Efectuarea de inspecţii/verificări periodice ale securităţii SIC sau, unde este cazul, a interconectării SIC	AAS, în colaborare cu AOSIC şi furnizorul de servicii SIC

SECŢIUNEA 3.5
Modificarea SIC

ART. 60

Pentru modificarea unui SIC se desfăşoară o serie de activităţi referitoare la securitatea SIC, de care sunt responsabile următoarele autorităţi:

Activitatea	Autoritatea/Personalul/ responsabilă/responsabil
1. Derularea, dacă este cazul, a proceselor de recertificare a produselor INFOSEC	Autorităţi naţionale, NATO, UE responsabile pentru activităţi de evaluare, certificare, aprobare produse INFOSEC, în colaborare cu structura de planificare şi implementare a SIC, furnizorul de servicii SIC şi AAS
2. Reluarea procesului de evaluare a	Structura de planificare şi

riscului de securitate, în conformitate cu cerinţele AAS	implementare a SIC, împreună cu AOSIC, furnizorul de servicii SIC şi AAS
3. Reanalizarea arhitecturii de securitate şi verificarea conformităţii acesteia cu arhitectura de securitate de referinţă, în vederea asigurării, dacă este posibil, a interoperabilităţii de securitate şi integrării noului SIC în infrastructuri existente	Structura de planificare şi implementare a SIC
4. Aprobarea rezultatelor reevaluării riscurilor	AAS, în coordonare cu AOSIC
5. Aprobarea arhitecturii de securitate	AAS
6. Identificarea măsurilor suplimentare de securitate necesare a fi implementate	Structura de planificare şi implementare a SIC, împreună cu furnizorul de servicii SIC şi AAS
7. Identificarea schimbărilor necesare privind instruirea şi conştientizarea	Structura de planificare şi implementare a SIC/AOSIC/furnizorul de servicii SIC, după caz
8. Identificarea schimbărilor necesare privind cerinţele care se aplică pentru continuarea activităţilor	AOSIC, în coordonare cu AAS
9. Identificarea schimbărilor necesare privind cerinţele aplicabile păstrării logurilor de securitate	Structura de planificare şi implementare a SIC, împreună cu AOSIC, furnizorul de servicii SIC şi AAS
10. Stabilirea cerinţelor pentru testarea şi evaluarea securităţii SIC sau, unde este cazul, a interconectării SIC	AAS, în colaborare cu structura de planificare şi implementare a SIC şi furnizorul de servicii SIC
11. Elaborarea unui plan pentru testarea şi evaluarea securităţii	Structura de planificare şi implementare a SIC, în colaborare cu furnizorul de servicii SIC şi AAS
12. Efectuarea testării securităţii în conformitate cu planul de testare şi evaluare convenit	Furnizorul de servicii SIC, în colaborare cu structura de planificare şi implementare şi AAS
13. Analizarea rezultatelor testării securităţii	ASIC şi AAS
14. Identificarea, ca rezultat al testării, a măsurilor de securitate suplimentare necesar a fi implementate	Structura de planificare şi implementare a SIC, în colaborare cu furnizorul de servicii SIC şi AAS
15. Analizarea şi convenirea asupra riscului rezidual care poate fi	

acceptat	AAS, împreună cu AOSIC
16. Analizarea şi convenirea asupra continuării procesului de management al riscurilor	AAS, împreună cu AOSIC
17. Actualizarea documentaţiei cu cerinţele de securitate Utilizarea, unde este cazul, a profilelor de protecţie	AOSIC, în colaborare cu AAS
18. Actualizarea PrOpSec	AOSIC, în colaborare cu personalul care are responsabilităţi în domeniul securităţii SIC şi AAS
19. Reaprobarea documentaţiei cu cerinţele de securitate şi a PrOpSec	AAS
20. Reacreditarea SIC sau, unde este cazul, a interconectării SIC Eliberarea unui nou certificat de acreditare de securitate a SIC	AAS
21. Revizuirea şi stabilirea noilor condiţii pentru reacreditarea de securitate	AAS

SECŢIUNEA 3.6
Scoaterea din uz a SIC şi disponibilizarea echipamentelor

ART. 61
În etapa de scoatere din uz a unui SIC şi disponibilizare a echipamentelor acestuia, se desfăşoară următoarele activităţi referitoare la securitatea SIC, de care sunt responsabile următoarele autorităţi:

Activitatea	Autoritatea/Personalul/ responsabilă/responsabil
1. Identificarea componentelor care necesită arhivare şi/sau declasificare şi/sau disponibilizare şi/sau distrugere, precum şi cerinţele corespunzătoare	AOSIC şi/sau furnizorul de servicii SIC
2. Efectuarea arhivării corespunzătoare sau declasificarea şi distrugerea mediilor de stocare fixe şi detaşabile asociate calculatoarelor şi actualizarea evidenţelor referitoare la acestea	AOSIC şi/sau furnizorul de servicii SIC
3. Executarea procedurilor corespunzătoare disponibilizării şi/sau	AOSIC şi/sau furnizorul de servicii SIC

distrugerii echipamentelor având scopuri speciale, inclusiv a produselor şi sistemelor criptografice şi a materialelor asociate acestora	
4. Arhivarea sau distrugerea documentaţiei asociate SIC, aflată în format hârtie	AOSIC şi/sau furnizorul de servicii SIC