OMAI 810/23.09.2005 – pentru aprobarea Normelor de aplicare a standardelor nationale de protectie a informatiilor clasificate in sistemele informatice si de comunicatii – INFOSEC – in institutiile MAI

Art.2 (1) In acceptiunea prezentelor norme, prin protectia surselor generatoare de informatii se intelege protectia informatiilor in Sistemele Informatice si de Comunicatii INFOSEC.

(2) Prin Sistem Informatic side Comunicatii, denumit in continuare SIC, se intelege atat Sistem de Prelucrare a Datelor – SPAD izolat sau conectat la alte SPAD, cat si Reteaua de Transmisii de Date – RTD, in functie de situatie.

Art.3 (1) Politica INFOSEC se aplica tuturor SIC din MAI indifferent daca informatiile stocate, procesate, transmise sunt clasificate sau neclasificate.

(2) Pentru SIC care stocheaza, proceseaza sau transmit informatii NATO sau UE clasificate, politica INFOSEC se aplica in conformitate cu nivelul de clasificare a informatiilor echivalente in legislatia nationala, daca nu s-a dispus astfel prin acorduri/conventii, protocoale la care Romania este parte.

Art.4 Protectia informatiilor in SIC este parte integranta a securitatii generale, iar pentru realizarea acesteia este necesara aplicarea la conditiile specifice atat a unor masurei cucaracter general – organizarea securitatii, masuri de protectie fizica, de protectie a personalului, de protectie a documentelor, de protectie juridical, procedurale si de securitate industriala – cat si a unor masuri specifice SIC. Particularizarea masurilor de securitate este impusa de modul specific in care informatiile sunt accesate si vehiculate pe timpul procesarii.

Art.5 Prevederile prezentelor norme se aplica la nivelul fiecarei structuri si institutii din MAI si reprezinta baza legala pentru asigurarea confidentialitatii, integritatii, autenticitatii si disponibilitatii informatiilor stocate, procesate sau transmise in SIC.

Art.7 Toate SIC se acrediteaza inainte de intrarea in functiune.

Anexa 1 – Glosar

Termenii specifici, folositi in acest document, cu aplicabilitate in domeniul INFOSEC, se definesc dupa cum urmeaza:

Acreditare – procesul de acordare a autorizarii si aprobarii date unui SIC de a prelucra informatii clasificate, in spatial/mediul operational propriu.

Active X – exte un instrument de lucru utilizat in programarea controalelor necesare unei aplicatii in vederea interactiunii cu alte aplicatii. Este mult utilizat in crearea si prezentarea paginilor Web pe internet.

Amenintare – pericol potential de compromitere accidentala sau deliberate a securitatii unui SIC prin pierderea confidentialitatii, a integritatii sau disponibilitatii informatiilor.

Autentificare – masura de securitate destinata pentru a stabili veridicitatea unei transmisii, mesaj sau a unei surse; mijloace de verificare daca o persoana sau antitate este autorizata sa primeasca o anumita categorie de informatii.

Autorizatie de acces la informatii clasificate- document eliberat cu avizul structurii abilitate,prin care se confirma ca, in exercitarea atributiilor profesionale de un anumit nivel de secretizare, potrivit principiului necesitatii de a cunoaste.

Browser Web – produs software pentru a vizualiza si interactiona cu un document Web.

Certificare – in urma procesului de evaluare, se emite un document de constatare, la care se ataseaza unul de analiza, in care sunt prezentate modul in care a decurs evaluarea si rezultatele acesteia. In documentul de constatare se mentioneaza masura incare SIC verificat satisface cerintele de securitate sau gradul in care produsul de securitate destinbat protectiei acestora, raspunde exigentelor in materie de securitate.

Certificat de securitate – document eliberat persoanei cu atributii nemijlocite in domeniul protectiei informatiilor clasificate, care atesta verificarea si acreditareade a detine, de a avea acces si de a lucra cu informatiile clasificate.

Cookie – informatie stocata intr-un calculator de catre un site Web pentru a identifica un utilizator in vederea viitorelor conectari.

Compromitere – situatia in care se pierde confidentialitatea, integritatea sau disponibilitatea informatiilor clasificate sau integritatea si disponibilitatea serviciilor si resurselor SIC din cauza unei brese de securitate sau a unei actiuni subversive (spionaj, act terrorist, sabotaj sau furt). Aceasta include pierderea sau dezvaluirea informatiilor unorpersoane neautorizate, modificarea neautorizata, distrugerea intr-un mod neautorizat si acestora sau invalidarea accesului autorizat (denial of service).

Confidentialitate – proprietatea informatiei de a nu fi disponibila sau dezvaluita persoanelor sau entitatilor neautorizate.

Controlul accesului – procesul de limitare a accesului utilizatorilor la resursele unui system, programe, procese autorizate sau alte sisteme dintr-o retea.

Disponibilitate – proprietatea informatiei de a fi accesibila si folosita la cererea persoanelor sau entitatilor autorizate.

Document clasificat – orice support material care contine informatii clasificate, in original sau copie, precum:

- hartie – documente olografe, dactilografiate sau tiparite, schite, harti, planes, fotografii, desene, indigou, listing
- benzi magnetice, casete audio-video, microfilme
- medii de stocare a informatiilor in sistemele informatice – dischete, compact-discuri, hard-discuri, memorii PROM si EPROM, riboane
- dispozitive de procesare portabile – agende electronice, laptop-uri la care hard-discul este folosit pentru stocarea informatiilor.

Evaluare- consta in examinarea detaliata – din punct de vedere ethnic si functional – a aspectelor de securitate ale SIC sau a produselor informatice de securitate, de catre o autoritate abilitata in acest sens.

Prin procesul de evaluare se verifica prezenta functiilor de securitate cerute, absenta efectelor secundare compromitatoare care ar putea decurge din implementarea facilitatilor de securitate si se estimeaza functionalitatea globala a sistemului de securitate.

Prin evaluare se apreciaza in ce masura cerintele de securitate specifice prentru un SIC sunt satisfacute. De asemenea, prin evaluarea performantelor de securitate ale produsului informatic de securitate se stabileste nivelul "de incredere" al SIC sau al produsului informatic de securitate implementat.

Evaluare riscuri –procesul care se desfasoara periodic pentru identificarea riscurilor de securitate, de determinare a consecintelor posibile si de stabilire a zonelor in care trebuie sa se aplice contramasuri corespunzatoare.

Facilitati de securitate specifice unui SIC – prin facilitate de securitate specifice unui SIC se intelege: functii si caracteristici hardware/firmware/software; proceduri/moduri de operare; proceduri si mijloace de evidenta; controlul accesului; definirea zonei de operare a SIC; definirea zonbei de operare a posturilor de lucru/a terminalelor la distanta; restrictii impuse prin politica de managemtn; structuri desemnate pentru protectia fizica si de personal; mijloace de control ale comunicatiilor.

Toate acestea sunt necesare asigurarii unui nivel acceptabil de protectie pentru informatiile clasificate, care urmeaza a fi stocate, procesate sau transmise intr-un SIC.

Firewall – element de protectie compus din echipamente si/sau programe care asigura atat la intrare cat si la iesire, o bariera de securitate intre o retea considerate "de incredere" (interna) si orice alta retea care nu este de incredere (externa). Aceste elemente sunt realizate din doua tipuri de produse, cele pentru filtrarea pachetelor si aplicatii gateway.

Firmware – un software instalat intr-un dispozitiv hardware si care permite citirea si executarea acelui software, darn u permite modificarea acestuia, de exemplu stergerea datelor de catre utilizator.

Fisiere jurnal – prezentarea independenta a monitorizarii si examinarii inregistrarilor si a activitatilor pentru a evalua calitatea sistemului de control, pentru a asigura conformitatea cu politicile stabilite si procedurile operationale si recomanda schimbarile necesare in control, politica sau proceduri.

Gateway - - interfata care asigura compatibilitatea intre retele care folosesc viteze sau coduri de transmisie, protocoale sau masuri de securitate diferite.

Informatie – orice notiune care poate fi comunicata in orice forma.

Informatie in format electronic – reprezinta texte, date, imagini, sunete, inregistrate pe suporturi magnetice, optice, electrice sau trannise sub forma de curenti, tensiuni sau camp electromagnetic, in atmosfera sau in retele de comunicatii.

Informatie cu destinatie speciala – marcarea informatiilor cu destinatie speciala se aplica, in mod obisnuit, informatiilor clasificate care necesita o distributie limitata si o manipulare speciala, in plus fata de caracterul atribuit, prin clasificarea de securitate.

Integritate – proprietatea informatiei de a nu fi modificata sau distrusa in mod neautorizat.

Internet – conceptual este o retea a retelelor. Aceasta include un numar mare de retele locale care apartin unor institutii comerciale, academice sau guvernamentale interconectate prin intermediul protocolului TCP/IP. Nucleul central care guverneaza aceasta retea mondiala se numeste Consiliul Activitatilor Internet (Internet Activities Board – IAB).

Intranet – este o retea private a unei organizatii bazata pe protocoale de comunicatie Internet, destinata partajarii resurselor si informatiilor intre utilizatorii acesteia.

Java – limbaj de programare complet orientat pe obiecte, independent de platforma.

Managementul riscurilor de securitate – procesul continuu de identificare, control si minimalizare a efectelor evenimentelor care ar putea afecta resursele SIC. Managemtnul riscurilor de securitate este un process care urmareste evolutiile rapide ale tehnologiei si mutatiile factorilor de risc.

Masuri Tempest – un complex de activitati si masuri de testare si de realizare a securitatii impotriva scurgerii informatiilor, prin intermediul emisiilor electromagnetice parasite. Echipamentele Tempest incorporeaza tehnologii de fabricatie si elemente care elimina sau atenueaza radiatiile compromitatoare.

Mecanismul de control al accesului – elementele hardware si software, procedurile de operare, procedurile de administrare si/sau combinatia acestora in scopul detectarii si/sau prevenirii accessului neautorizat al persoanelor sau entitatilor la resursele SIC.

Ne-repudiere – presupune urmatoarele aspecte:

- verificarea originii care permite receptorului sa poata dovedi furnizarea datelor, inpiedicandu-se astfel orice incercare a unui emitator de a nu mai recunoaste transmiterea datelor sau continutul mesajelor;
- verificarea livrarii, care permite emitatorului sa fie convins sis a poata proba receptia mesajelor trimise de el, impiedicandu-se astfel orice incercare a unui receptor de a nu mai recunoaste primirea datelor sau continutul mesajelor.

Parola – un cuvant protejat sau un sir de caractere care identifica sau autentifica un utilizator, o resursa specifica sau un tip de acces.

Politica Infosec - ansamblul prevederilor legale, reglementarilor, masurilor, procedurilor si structurilor destinate protectiei informatiilor clasificate care sunt stocate, procesate sau transmise prin intermediul Sistemelor Informatice si de Comunicatii – SIC, sau al altor sisteme electronice, impotriva amenintarilor si a oricaror actiuni care pot adduce atingere confidentialitatii, integritatioi, disponibilitatii, autenticitatii si nerepudierii informatiilor clasificate, precum si functionarii SIC, indifferent daca acestea apar accidental sau intentionat.

Principiul necesitatii de a cunoaste (need-to-know) – principiul conform caruia accesul la informatii clasificate se acorda in mod individual numai persoanelor care, pentru indeplinirea indatoririlor de serviciu, trebuie sa lucreze cu astfel de informatii sau sa aiba acces la acestea.

Privilegii "root" – privilegii care apartin radacinii sistemului de fisiere.

Proceduri "back-up" – copii create pentru refacerea fisierelor de date si a bibiliotecilor de programe, precum si pentru repornirea sau inlocuiorea echipamentelor unui SIC in urma aparitiei unei functionaru defectuoase sau a unui calamitati.

Produs informatic de securitate – element de securitate care se incorporeaza intr-un SIC si care serveste la sporirea sau asigurarea confidentialitatii, integritatii sau disponibilitatii informatiilor.

Protectia fizica – ansamblul activitatilor de paza, securitate si aparare, prin masuri si dispozitive de control fizic si prin mijloace tehnice a informatiilor clasificate.

Protectia personalului – ansamblul activitatilor privind selectionarea, verificarea, avizarea si autorizarea accesului la informatiile secrete de stat, revalidarea, controlul si instruirea personalului, retragerea certificatului de securitate/autorizatiei de acces la informatii clasificate.

Protocolul punct-la-punct – un protocol de transport la nivel de retea care lucreaza pe conexiuni de retea punct-la-punct, cum ar fi liniile seriale sau de modemuri.

Proxy server – un serfver care intermediaza comunicatiile intre o statie de utilizator si o retea, asigurandu-se servicii de retea, controlul administrative si elemente de securitate.

Regula celor doi (two men rule) – reprezinta obligativitatea lucrului in comun a cel putin doua personae pe timpul desfasurarii unei activitati specifice.

Rhost – serviciul TCP/IP care utilizeaza pentru rularea comenzilor pe calculatoare de la distanta.

Risc de securitate – posibilitatea exploatarii unei vulnerabilitati a unui SIC.

Securitatea SIC – aplicarea procedurilor si masurilor de securitate in SIC cu scopul de a preveni sau impiedica extragerea, modificarea sau distrugerea informatiilor clasificate stocate, procesate, trannsmise prin intermediul acestora – prin interceptare, alterare, distrugere, accesare neautorizata cu mijloace electronice, precum si invalidarea de servicii sau functii, prin mijloace specifice. Asigurarea securitatii SIC presupune aplicarea unui ansamblu de masuri organizatorice, Compusec, Comsec, fizice, la nivel de personal si de securitate a documentelor.

Securitatea calculatoarelor – Compusec – consta in aplicarea – la nivel de calculator – a masurilor de securitate hardware, software si firmware, pentru a preveni divulgarea, utilizarea, modificarea sau stergerea neautorizata a informatiilor sau invalidarea neautorizata a unor functii.

Securitatea comunicatiilor – Comsec – reprezinta aplicarea masurilor pentru protejarea mesajelor vehiculate prin sistemul de comunicatii, care pot fi interceptate, studiate, analizate si care, prin reconstituire pot conduce la cunoasterea informatiilor clasificate. Comsec reprezinta un set complex de masuri si proceduri, incluzand: securitatea criptografica; securitatea transmisiilor – Transec ; securitatea radiatiilor electromagnetice compromitatoare – Tempest.

Securitatea transmisiilor – Transec – componenta de securitate a comunicatiilor care contine toate masurile mai putin cele de protectie fizica, destinate pentru protejarea transmisiilor impotriva interceptarii si exploatarii neautorizate prin mijloace, altele decatcele de criptanaliza criptografica.

Shell – comanda MS-DOS pentru lucru cu alte subsisteme Windows NT.

SNMP – protocolul simplu de management de retea.

Script – lista de comenzi intr-un limbaj de programare de nivel inalt.

Streaming- o tehnica de transfer de date din internet care permite utilizatorului sa redea fisiere audio si video fara durate de timp limitate. Sursa de informatii imparte informatia in pachete mici transmitandu-le prin retea catre utilizator, care poate accesa continutul in timp ce este receptionat.

Sistem informatic si de comunicatii – SIC – ansamblu de elemente interdependente in care sunt incluse echipamente de calcul produse software de baza si applicative, metode, procedee si, daca este cazul, personal, organizate astfel incat sa asigure indeplinirea functiilor de stocare, procesare sau transmitere a informatiilor in format electronic. Este alcatuit din cel putin o statie de lucru – PC, sau poate fi organizat in retele locale de dimensiuni mici sau in retele complexe (Lan, Wan etc.) incluzand sistemele de comunicatii aferente.

Sisteme de comunicatii – SC – reprezinta ansamblu de elemente interdependente in care se inclus echipamente, programe si dispozitive de comunicatie, metode si proceduri pentru transmisie si receptie de date si controlul retelei, precum si, daca este cazul, personalul aferent.

SIC independente – sisteme care nu sunt interconactate la alte sisteme sau retele. Majoritatea sistemelor independente sunt calkculatoare cu utilizator unic sau sisteme cu mai multi utilizatori, cum ar fi calculatoarele folosite la procesarea de texte, care nu au conexiunile externe.

Sistem de operare – reprezinta o colectie integrate de rutine de serviciu pentru supravegherea secventializarii si prelucrarii unor programe de catre un calculator. Sistemul de operare controleaza alocarea resurselor catre utilizatori si programele lor si joaca un rol central in asigurarea operarii in siguranta a unui calculator. Sistemele de operare poit executa operatii de depanare-devirusare, input-output, contabilizare/evidenta alocare resurse, compilare, asignare a zonelor de memmorie si alte functii de operare specifice, sinonime cu programul de monitorizare, executie, control si de supraveghere.

Software nociv – un cod ascuns in sistem cu scopul de a provoca disfunctii acestora, de a sustrage informatii si de a distruge fisiere.

Telnet – serviciul de conectare la distanta cu alte calculatoare inlinie de comanda.

Trusted Computing Base (TCB)- totalitatea mecanismelor de protectie in cadrul sistemului informatic – hardware, firmware si software – care se pot aplica pentru impunerea unei politici de securitate. TCB consta in una sau mai multe componente de securitate care impreuna pot impune o politica de securitate unitara.

URL (Uniform Rescource Locator) – reprezinta adresa de internet/intranet unde poate fi localizata o anumita resursa.

Vulnerabilitate – o slăbiciune sau lipsa de control de natura tehnica, procedurala sau operationala, care ar putea fi speculate in scopuri ilicite.

Virus de calculator – un tip de software nociv care are capacitatea de a se multiplica si de a infecta programe si fisiere. Este doar un exemplu din multiplele forme de software nociv care poate actiona rapid si distructiv, provocand prejudicii foarte mari. Alte forme de software nociv include: bombele logice, calul Troian, viermii de retea.

Zona SIC – reprezinta o zona de lucru incare se gasesc si opereaza unul sau mai multe calculatoare, unitati periferice locale si de stocare, mijloace de control si echipamente specifice de interconactare si de comunicatii.

Zona terminal/Statie de lucru la distanta- reprezinta o zona, separate de zona SIC, in care se gasesc si functioneaza: echipamente periferice locale sau terminale associate echipamentului de calcul central; statii de lucru la distanta: echipamente de comunicatii.

Spad (Sistem de Prelucrare Automata a Datelor) – se intelege un ansamblu de elemente interdependente – in care se include: echipamentele de calcul, produsele software de baza si applicative, metodele, procedeele si daca este cazul personalul – organizate astfel incat sa asigure indeplinirea functiilor de stocare si prelucrare automata a informatiilor in forma electronica.

RTD (retea de Transmisii de Date) – este un ansamblu de elemente interdependente in care se include: dispozitive si echipamentye de comunicatie, tehnica de calcul hardware si software, metode si proceduri pentru transmisie/receptie date, precum si pentru controlul retelei. Daca este cazul, este inclus si personalul afferent. Toate acestea sunt organizate astfel incat sa asigure indeplinirea functiilor de teletransmisie a informatiilor in forma electrinica intre doua sau mai multe SPAD (SIC), sau sa permita interconectarea cu alte RTD-uri. RTD poate utilize serviciile unui singur system de comunicatii sau ale mai multor sisteme de comunicatii: mai multe RTD pot utilize serviciile unuia si acelasi system de comunicatii.

Lista cu acronimele utilizate

AAS – Autoritatea deAcreditare de Securitate
AAIAS- Autoritatea Administratiei si Internelor de Acreditare de Securitate
AAISIC – Autoritatea Administratiei si Internelor de Securitate pentru Informatica si Comunicatii
AAIPC – Autoritatea Administratiei si Internelor de Protectie Criptografica
CSTIC – Componenta de Securitate pentru Tehnologia Informatiei si Comunicatiilor
CAS- Comitetul de Acreditare de Securitate
CSC – Cerintele de Securitate Comune
CSS – Cerintele de Securitate Specifice
CSSI – Cenrintele de Securitate Specifice pentru Protectia Informatiilor in format electronic intr-un SIC
COMPUSEC – Securitatea Calculatoarelor
COMSEC – Securitatea Comunicatiilor
DCS – Documentatia cu Cerintele de Securitate
EMSEC – Securitatea Emisiilor
MSG – Mediul de Securitate Globala
MSE- Mediul de Securitate Electronica
ORNISS – Oficiul Registrului National al Informatiilor Secrete de Stat
PrOpSec – Procedurile Operationale de Securitate
SIC – Sistem Informatic si de Comunicatii
TRANSEC – Securitatea Transmisiilor.

Art.13 (1) In structurile si institutiile MAI, in care functioneaza SIC, ce stocheaza, proceseaza sau transmit informatii in format electronic, se infiinteaza Componenta deSecuritate pentru Tehnologia Informatiei si Comunicatiilor, denumita in continuare CSTIC.

(2) CSTIC functioneaza incadrul structurii de securitate.

(3) Pentru institutiile MAI in care functioneaza mai multe SIC interconectate, responsabilitatea interconexiunii este a sefilor CSTIC implicate.

Art.14 CSTIC isi exercita atributiile in subdomeniile:

a. securitatea calculatoarelor, denumit in continuare COMPUSEC

b. securitatea comunicatiilor, denumit in continuare COMSEC.

Art.15 Daca volumul de activitate este redus si daca cerintele de securitate permit, atributiile CSTIC pot fi indeplinite de catre seful CSTIC.

Art.16 (1) Pentru COMPUSEC in vederea indeplinirii atributiilor functionale, se numeste urmatorul personal astfel:

a. pentru securitate SIC : administrator de securitate al SIC, administrator de securitate in zona terminalelor isolate
b. pentru administrarea SIC: administrator de system/retea, administrator WEB, administrator de baze de date

(2) Pentru COMSEC in vederea indeplinirii atributiilor functionale, se numeste urmatorul personal astfel:

a. pentru securitetea transmisiilor: administrator TRANSEC
b. pentru securitatea emisiilor: administrator EMSEC
c. pentru securitatea echipamentelor criptografice: administrator cripto sau custodele cripto.

Sectiunea 2 – Responsabilitati de securitate

Art.23 Seful structurii de securitate in domeniul Infosec, indeplineste urmatoarele atributii principale:

a. este responsabil pentru implementarea si asigurarea masurilor de securitate, conform normelor in vigoare;
b. pune la dispozitia sefului CSTIC lista cu ceritificatele de securitate/autorizatiile de acces la informatii clasificate detinute de personalul MAI
c. monitorizeaza echipamentele care intra/ies din zonele de securitate.

Art.24 CSTIC relationeaza cu AAIA, AAISIC, AAIPC in situatiile in care o structura/institutie din cadrul MAI:

a. planifica dezvoltarea sau achizitia unui SIC care stocheaza, proceseaza sau transmit informatii clasificate
b. propune schimbari configuratiei de system existente
c. propune conectarea cu un alt SIC
d. propune schimbari ale modului de operare protejata al SIC
e. propune modificarea sau inlocuirea software pentru optimizarea securitatii SIC
f. initiaza proceduri de modificare a clasei sau nivelului de secretizare ale SIC care au fost deja acreditate
g. planifica sau propune desfasurarea oricarei alte activitati in scopul imbunatatirii securitatii SIC care au fost deja acreditate.

Art.25 CSTIC isi exercita atributiile pe intregul ciclu de viata al SIC incepand cu proiectarea, continuand cu elaborarea specificatiilor, testarea instalarii, acreditarea, testarea periodica in vederea reacreditarii, exploatarea operationala, modificarea si incheind cu scoaterea din uz a acestora.

Art.26 Seful CSTIC se subordoneaza sefului structurii de securitate si indeplineste urmatoarele atributii principale:

a. solicita acreditarea/reacreditarea SIC de la AAIAS pentru toate activitatile prevazute la art.24
b. solicita asistenta de specialitate din partea AAIAS si AAISIC pentru stabilirea cerintelor de securitate si procedurilor de aplicare necesare si respectarii de catre furnizori de echipamente, pe durata intregului process de dezvoltare, instalare si testare SIC
c. raspunde de alegerea, implementarea, justificarea si controlul facilitatilor de securitate, de natura tehnica, care reprezinta parte componenta a SIC
d. asigura exploatarea in conditii de securitate a SIC
e. realizeaza legatura intre contractant, AAISIC si AAIAS
f. participa la selectionarea, organizarea si realizarea pregatirii personalului cu atributii in domeniul INFOSEC
g. organizeaza si desfasoara convocari de instruire cu personalul din subordine si utilizatorii din SIC
h. stabileste responsabilitatile personalului din subordine
i. verifica periodic sau in timp real, implementarea masurilor de protectie in SIC, din cadrul unitatii/structurii, pentru a se asigura ca securitatea acestuia este in concordanta cu cerintele de securitate aprobate de AAIAS

j. tine evidenta echipamentelor SIC, proprietate private, autorizate sa functioneze in incinta unitatii. inconditiile capitolului XI
k. cerceteaza incidentele de securitate si raporteaza rezultatele ierarhic, AAIAS si AAISIC, concomitant cu aplicarea unor masuri de reducere a consecintelor

Art.27 Administratorul COMPUSEC se subordoneaza sefului CSTIC si raspunde de asigurarea dezvoltarii, implementarii si mentinerii masurilor de securitate SIC

Art.28 In functie de dimensiunea si complexitatea SIC, atributiile administratorului COMPUSEC pot fi indeplinite de catre administratorul de securitate.

Art.29 Administratorul de securitate al SIC se subordoneaza sefului CSTIC si indeplineste urmatoarele atributii principale:

a. elaboreaza si actualizeaza Procedurile Operationale de Securitate, denumite in continuare PrOpSec
b. monitorizeaza permanent toate aspectele de securitate specifice SIC
c. participa la elaborarea si actualizarea documentelor Cerinte deSecuritate Specifice, Cerintele deSecuritate Comune si Cerintele de Securitate Specifice pentru Protectia Informatiilor in format electronic intr-un SIC pentru sistemele de care raspunde
d. actualizeaza si tine evidenta tuturor utilizatorilor autorizati
e. apolica masurile adecvate de control al accesului la SIC respective
f. verifica elementele de identificare a utilizatorilor
g. asigura evidenta evenimentelor legate de securitatea sistemului si a sesiunilor de lucru
h. evalueaza implicatiile, in planul securitatii privind modificarile software, hardware, firmware si procedurale propuse pentru SIC
i. verifica daca modificarile de configuratie a SIC afecteaza securitatea si dispune masurile in consecinta
j. verifica daca personalul cu acces autorizat la SIC cunoaste responsabilitatile care revin in domeniul protectiei informatiilor
k. verifica modul de executare a iontretinerii si actualizarii software pentru a nu se periclita securitatea sistemului
l. asigura un control riguros al mediilor de stocare a informatiilor si dopcumentatiei sistemului verificand concordanta intre clasa sau nivelul de secretizare a informatiilor stocate si marcajul de secretizare al mediilor stocate
m. ia msuri telnice si organizatorice pentru protectia mediilor de stocare a informatiilor fata de campurile electromagnetice si accesul neautorizat la informnatiile clasificate
n. executa controale privind modul de utilizare a mediilor de stocare a informatiilor
o. asigura pastrarea si consultarea documentatiei si a datelor de evidenta si control, referitoare la securitate, in conformitate cu PrOpSec
p. stabileste proceduri de verificare pentru utilizarea in SIC numai a software autorizat
q. asigura, impreunma cu administratorul system/retea, aplicarea celor mai eficiente proceduri de creare a copiilor de rezerva si de recuperare software
r. asigura instruirea si pregatiorea corespunzatoare a administratorilor de securitate in zona terminalelor isolate
s. raporteaza sefului CSTIC orice brese de securitate, vulnerabilitati si inclacari ale masurilor de securitate.

Art.30 In situatia in care un SIC are terminale sau alte echipamente aflate in cladiri diferite apartinand aceluiasi obiectiv se numeste un administrator cu securitatea in zona terminalelor isolate.

Art.31 Administratorul de securitate in zona terminalelor izolate se subordoneaza sefului CSTIC si indeplineste urmatoarele atributii principale:

a. aplica masuri de securitate specifice terminalelor izolate si celorlalte echipamente aferente aflate in zona sa de responsabilitate
b. asigura indeplinirea atributiilor de administrator de securitate, in lipsa acestuia
c. raporteaza sefului CSTIC orice brese/incidente de securitate]
d. aplica prevederile PrOpSec specifice zonei sau incaperii in care functioneaza terminalele izolate.

Art.32 (1) Administratorul de system/retea raspunde de dezvoltarea, implementarea si functionarea unui SIC

(2) Administratorul de system/retea se subordoneaza sefului CSTIC si indeplineste urmatoarele atributii principale:

a. participa la elaborarea urmatoarelor documente: Cerintele de securitate specifice, Cerintele de securitate commune si Procedurile operationale de securitate

b. asigura managementul configuratiei sistemelor sau retelelor acreditate si stabilite in Cerintele de securitate specifice sau Cerintele de securitate commune

c. elaboreaza propuneri de dezvoltare a SIC, avand in vedere si aspectele legate de evaluare si certificare

d. participa la elaborarea propunerilor de efectuare a unor modificari pentru imbunatatirea securitatii SIC

E. asigura functionarea SIC in concordanta cu Cerintele de securitate specifice si Procedurilor Operationale de Securitate

f. asigura pregatirea de specialitate a utilizatorilor echipamentelor SIC.

Art.34 Administratorul COMSEC se subordoneaza sefului CSTIC si indeplineste urmatoarele atributii principale:

a. verifica si raspunde de instalarea echipamentelor SIC folosite in transmiterea informatiilor clasificate in conformitate cu cerintele COMSEC;
b. verifica si raspunde de aplicarea in mod corespunzator a masurilor de securitate a emisiilor – EMSEC si a transmisiilor – TRANSEC
c. tine evidenta echipamentelor si sistemelor folosite la transmiterea informatiilor clasificate

Capitolul III – Amenintari si vulnerabilitati ale SIC

Art.41 Informatiile stocate, procesate sau transmise in SIC sunt vulnerabile la accesul, modificarea sau distrugerea de catre utilizatori neautorizati datorita urmatorilor factori:

a. volumul substantial de informatii stocate care sunt accesate si transferate cu viteze foarte mari
b. dificultate in realizarea controlului accesului la informatiile stocate in SIC
c. posibilitatea de a evita masurile de securitate de catre utilizatorii autorizati experimentati
d. capacitatea foarte mare a mediilor de stocare care faciliteaza sustragerea unui volum consistent de informatii
e. posibilitatea pierderii integritatii informatiilor ca urmare a defectiunilor in functionare a hardware si software
f. posibilitatea interceptarii comunicatiilor pe canale neprotejate sau a emisiilor compromitatoare.

Art.42 (1) Amenintarile specifice SIC se impart in trei categorii:

a. din interior – care au ca sursa actiunile rau intentionate, actiunile neintentionate sau erorile de operare ale utilizatorilor autorizati
b. din exterior – care au ca sursa actiunile intentionate sau neintentionate ale persoanelor fara acces ale persoanelor fara acces la SIC
c. fizice – care au ca sursa incidente sau calamitati naturale care afecteaza perimetrul in care sunt amplasate SIC.

(2) Amenintarile si vulnerabilitatile sunt specifice fiecarui SIC in parte.

Cap.IV – Protectia informatiilor in SIC – Sectiunea 1 – Reguli generale

Art. 47 Este interzisa conectarea unui SIC care proceseaza informatii nesecrete si/sau secrete de serviciu cu un SIC care proceseaza informatii secrete de stat, fara procedura de acreditare aferenta aprobata de functionarul de securitate al MAI.

Art.48 Toate SIC si echipamentele aferente acestora se clasifica si se marcheaza corespunzator celui mai inalt nivel de secretizare a informatiilor stocate, procesate sau transmise cu ajutorul acestora, conform prevederilor legale in vigoare.

Sectiunea 2 – Documente care reglementeaza securitatea SIC

Art.51 Functionarea unui SIC in conditii de securitate se reglementeaza in baza urmatoarelor documente:

a. Raportul de analiza a riscului de securitate
b. Documentatia cu Cerintele de Securitate
c. PrOpSec

Art.58 (1) PrOpSec reprezinta documentul in care sunt descries modul de aplicare a politicii de securitate stabilita in DCS, procedurile de operare care se aplica, precum si responsabilitatile personalului.

(2) PrOpSec se elaboreaza de catre administratorul de securitate, se avizeaza de catre AAIAS si se aproba decatre functionarul de securitate al MAI.

(3) PrOpSec se aproba de catre AAIAS inainte de a autoriza stocarea, procesarea sau transmiterea informatiilor clasificate.

(4) Modalitatea de intocmire a PrOpSec este prezentata in Ghidul privind structura si continutul PrOpSec, prevazut in anexa 5.

Sectiunea 3 – Modurile de operare protejata

Art.59 Toate SIC care stocheaza, prelucreaza sau transmit informatii in format electronic se acrediteaza sa functioneze in unul din modurile de operare protejate astfel:

a. Dedicat
b. Nivel inalt
c. Multi nivel

Sectiunea 4 – Protectia fizica

Art.66 In cadrul SIC sunt definite trei medii de securitate care delimiteaza zonele in care sunt implementate controale specifice ale securitatii:

a. Mediul de Securitate Generala – denumit in continuare MSG este reprezentat de cladirea sau cladirile in care functioneaza SIC. Notiunea de MSG cuprinde in general intreaga locatie a SIC si este in responsabilitatea functionarului de securitate fizica si administratorului de securitate CSTIC. In cazul retelelor poate exista un numar disjunct de MSG
b. Mediul de Securitate Locala, denumit in continuare MSL, este reprezentat de toate incaperile in care se afla echipamente ale SIC si este mediul de protectie fizica, a personalului, a documentelor si procedurala aflat in sfera de responbsabilitate a CSTIC administratorul de securitate
c. Mediul de Securitate Electronica denumit in continuare MSE al SIC este reprezentat de SIC insusi si este in responsabilitatea administratorului de securitate al SIC (ex. Interfetele om-masina, interfetele interne si externe, firewall-ul, security guard si gateway-ul).

Art.68 Zonele SICunde sunt sau vor fi vehiculate informatii clasificate sunt organizate in zona de securitate corespunzator nivelului de clasificare al informatiilor vehiculate in fiecare zona, astfel:

a. Zona de securitate clasa I este zona in care sunt vehiculate informatii cu nivel de clasificare STRICT SECRET si cu un nivel superior, in asa fel incat intrarea in aceasta zona reprezinta practice acces la aceste informatii. La intrarea in aceasta zona este afisat un mesaj de atentionare de forma:

ATENTIE! INTRATI IN ZONA DE SECURITATE CLASA I

b. Zona de securitate clasa II este zona in care sunt vehiculate informatii cu nivel maxim de clasificare SECRET, in asa fel incat informatiile clasificate pot fi protejate impotriva accesarii de catre personae neautorizate, prin masuri si mijloace interne specifice. La intrarea in aceasta zona este afisat un mesaj de atentionare de forma:

ATENTIE! INTRATI IN ZONA DE SECURITATE CLASA II

c. Zona administrative este zona situate in jurul sau vecinatatea zonelor de securitate clasa I si II si pentru care sunt stabilite masuri de securitate mai permissive. In aceste zone sunt vehiculate informatii cu nivel maxim declasificare SECRET DE SERVICIU, in asa fel incat aceste informatii pot fi accesate de personal pentru indeplinirea sarcinilor de serviciu. La intrarea in aceasta zona este afisat un mesaj de atentionare de forma:

ATENTIE! INTRATI IN ZONA ADMINISTRATIVA

Art.72 Accesul la statiile de lucru ale SIC este permis numai personalului autorizat care poseda certificate de securitate corespunzator nivelului de clasificare al informatiilor la care au drept de acces pentru indeplinirea sarcinilor de serviciu, iar monitoarele acestora sunt pozitionate in asa fel incat sa previna vizualitatea informatiilor afisate de catre personalul neautorizat si sunt acoperite sau deconectate atunci cand in incapere este prezent un vizitator.

Sectiunea 5 – Protectia personalului

Art.73 Utilizatorii sunt autorizati si au acces la informatii clasificate pe baza principiului necesitatea de a cunoaste" si in functie de clasa sau nivelul de secretizare a informatiilor stocate, procesate sau transmise in SIC.

Art.74 Fiecare persoana, care intra in posesia informatiilor clasificate, are obligatia de a se asigura ca acestea sunt transmise numai persoanelor autorizate/certificate corespunzator clasei sau nivelului de secretizare a informatiilor respective.

Art.84 (1) Persoanelor care au incalcat masurile de securitate stabilite in PeOpSec, li se suspenda temporar, dreptul de acces pana la clarificarea situatiei.

(2) Modalitatile de raportare a acestor cazuri si masurile care se impugn intr-o asemenea situatie se detaliaza in PrOpSec.

Art.85 Toti utilizatorii autorizati trebuie sa semneze de luare la cunostinta despre prevederile PrOpSec. Un exemplar al PrOpSec, semnat de utilizatori se pastreaza de catre seful CSTIC.

Art..87 (1) Vizitatorii, carora li s-a aorobat intrarea in zonele de securitate, sunt insotiti permanent.

(2) In fiecare incapere/incinta se stabilesc masuri pentru prevenirea contactului visual al vizitatorilor cu informatiile afisate pe monitoare sau rezultate la imprimanta.

Sectiunea 6 – Controlul si evidenta accesului

Art.89 Inainte de deschiderea unei sesiuni de lucru, este obligatory afisarea unui mesaj de avertizare prin care utilizatorul este instiintat ca a ccesat un SIC proprietatea MAI si este obligat sa respecte normele privind protectia informatiilor clasificate.

Art.90 (1) Evidenta automata a accesului la informatii secrete de stat se pastreaza si sub forma fisierelor jurnal.

(2) Perioada de pastrare a fisierelor jurnal listate se stabileste in conformitate cu prevederile actelor normative specifice si se mentioneaza atat in CSS, cat si in PrOpSec.

Art.91 Inregistrarile din fisierele jurnal trebuie sa cuprinda urmatoarele date:

a. data si ora activitatii/operatiunii
b. operatiunea executata
c. codul de identificare al utilizatorului in contul caruia apare operatiunea
d. daca operatiunea s-a finalizat corespunzator sau nu
e. tentativele de executie a unei operatii ilegale
f. intrare/iesire in/din sesiunea de lucru
g. pornirea/oprirea sistemului
h. modificarile parametrilor de securitate

Art.92 (2) Informatiile stocate in aceste fisiere sunt examinate periodic, cel putin o data pe luna, de catre administratorul de securitate care urmareste orice violare sau tentative de violare a sistemului de securitate.

(3) Semestrial se creeaza copii de rezerva ale fisierelor jurnal, care se vor pastra pe medii de stocare a informatiilor de tipul disponibil doar pentru citire – read inly – carora li se asigura protectie corespunzatoare nivelului de secretizare atribuit SIC.

Sectiunea 8 – Protectia mediilor de stocare a informatiilor

Art.102 (2) Evidenta mediilor de stocare a informatiilor clasificate se tine de catre administratorul de securitate sau de catre o persoana desemnata din cadrul compartimentului de exploatare al SIC.

Sectiunea 9 – Protectia software

Art.103 (1) In SIC din MAI se utilizeaza numai software licentiate si care este autorizat de catre AAIAS.

Art.108 (1) Versiunile software-ului utilizate current se examineaza si testeaza la intervale regulate de timp, nu mai mari de 6 luni, pentru verificarea integritatii acestora si corectitudinii in operare.

(2) Se interzice utilizarea unor versiuni noi sau modificate de software pentru prelucrarea informatiilor secrete de stat, pana nu au fost testate facilitatile de securitate de catre administratorul de securitate si aprobate de AAIAS in functie de conditiile dereacriditare stabilite in CSS.

Art. 114 (1) Utilizatorii sunt obligate sa-si creeze copii de siguranta proprii domeniului pentru care este autorizat.

(2) Administratorului de system/retea creeaza obligatoriu copii de siguranta ale bazelor dedate conform procedurilor stabilite in PrOpSec.

Sectiunea 10 – Protectia Hardware

Art.116 In SIC din MAI se utilizeaza sau conecteaza numai hardware autorizat de catre AAIAS.

Art.121 Toate echipamentele din compunerea sistemului se sigileaza de catre administratorul de securitate. Sigilarea se face dupa caz folosind etichete cu stampila structurii MAI, sigiliul administratorului aplicat pe support de ceara sau alte metode, care respecta masurile de securitate impuse.

Art.122 Porturile neautorizate ale sistemului se sigileaza sau se deconecteaza decatre administratorul de securitate.

Art.124 (1) Verificarea integritatii sigiliilor se face zilnic de catre utilizatori la inceperea programului de lucru sau la luarea in primire a serviciului.

(2) Administratorii de securitate verifica lunar integritatea sigiliilor la toate componentele SIC.

Art.125 Administratorul de securitate tine evidenta componentelor care stocheaza, chiar si temporar, informatiile clasificate si le verifica periodic intr-o maniera similara cu documentele clasificate redactate pe support de hartie.

Capitolul V – PARTICULARITATI PRIVIND PROTECTIA INFORMATIILOR IN SIC

Sectiunea 1 – Protectia informatiilor in sisteme informatice independente

Art.169 Pentru sistemele informatice, denumite in continuare SI, independente, se asigura masuri de protectie fizica in conformitate cu clasa sau nivelul desecretizare a informatiilor procesate in system.

Art.170 Masurile de protectie fizica adoptate au drept scop prevenirea:

a. accesului neautorizat la sistem si la informatiile stocate;
b. introducerii, modificarii sau scoaterii neautorizate a unor componente ale sistemului;
c. sustragerii sistemului sau unor componente din acesta.

Art.171 SI indenpendente care contin medii de stocare nedetasabile se protejeaza fizic impotriva accesului neautorizat. Masurile de protectie fizica se realizeaza prin:

a. dispunerea SI in incaperi/incinte securizate si certificate in concordanta cu clasa sau nivelul de secretizare a informatiilor stocate;
b. pastrarea componentelor sistemului, care contin informatii clasificate, intr-un container de securitate certificate in conformitate cu clasa sau nivelul de secretizare a informatiilor stocate. Pentru componentele sistemelor pastrate in afara containerelor de securitate, se iau masuri de protectie pentru prevenirea sau detectarea tentativelor de sustragere sau de violare a integritatii fizice a acestora;
c. izolarea sursei de alimentare, a monitorului, plasarea tastaturii in interiorul containerului etc., pentru impiedicarea accesului neautorizat la informatiilor protejate.

Art.172 (1) Mediile de stocare detasabile de system se scot si se pastreaza in concordanta cu clasa sau nivelul desecretizare a informatiilor stocate pe acesta.

(2) SI independent din care au fost scoase mediile de stocare clasificate si care nu mai contine nici o alta componenta clasificata separate poate fi considerat neclasificat.

Art.73 Toti utilizatorii autorizati ai unui SI independent trebuie sa aiba certificate de securitate/autorizati de acces la informatii clasificate pentru cel mai inalt nivel de sercretizare a informatiilor la care au drept de acces. Nivelul minim de certificare este stability in Cerintele deSecuritate Specifice si Proceduri Operationale de Securitate.

Serctiunea 2 – Protectia informatiilor in SIC portabile

Art.178 SIC portabile interzise, dar a caror utilizare este justificata de ratiuni operationale, pot fi supuse spre evaluare AAIAS care le autorizeaza, dupa caz.

Capitaolul VIII – ACREDITAREA SI REACRIDITAREA

Sectiunea 1 – Reguli generale

Art.231 (1) Toate SIC care proceseaza informatii se acrediteaza de AAIAS.

Sectiunea 4 – Reacreditarea

Art.248 SIC se reacrediteaza dupa cum urmeaza:

a. annual, SIC care stocheaza proceseaza sau transmit informatii strict secrete de importanta deosebita si cudestinatie speciala
b. periodic, la fiecare doi ani, SICcare stocheaza, proceseaza sau transmit informatii secrete de stat, cu exceptia celor prevazute la lit.a;
c. periodic, la fiecare trei ani SIC care stocheaza, proceseaza sau tramsit informatii secrete de serviciu
d. dupa executarea unor modificari hardware si software care afecteaza securitatea SICrespectiv:
e. la recomandarea administratorului COMSEC, ca urmare a unor modificari care ar putea avea impact asuprasecuritatoo comunicatiilor precum: modificari in configuratia zonelor de securitate

ale obiectivului respective, in amplasarea echipamentelor sau modificari de configuratie necesare pentru corectarea unor deficiente majore la nivel hardware.

Capitolul X – ACTIVITATEA DE INTRETINERE SI REPARATII A SIC

Art. 259 Este interzis persoianelor neautorizate pentru efectuarea unor activitati de intretinere sau reparare si care reprezinta atributul echipelor deservice sau a producatorilor de sisteme informatice.

Art.263 Administratorul de system tine evidenta intretinerilor effectuate.

Art.265 Reparatea, casarea, retragerea din serviciu/disponibilizarea unor componente software dintr-un SIC clasificat se face obligatoriu cu aprobarea administratorilor de securitate si de system/retea.

Capitolul XI – FOLOSIREA ECHIPAMENTELOR SIC DIN EXTERIOR

Art.268 Este interzisa introducerea mediilor de stocare, a software-ului si hardware-ului, aflate in proprietate private, in zonele in aprobarea functionarului de securitate, a unitatii/structurii respective care se stocheaza, se proceseaza sau se transmit informatii clasificate.

Art.269 Este interzisa utilizarea mediilor de stocare amovibile, a software si hardware, aflate in poroprietate private, pentru stocarea, procesarea si transmiterea informatiilor clasificate.

Art.270 Utilizarea mediilor de stocare amovibile, a software si hardware, aflate in proprietate private, pentru stocarea, procesarea sau transmiterea informatiilor nesecrete este permisa numai cu avizul CSTIC si aprobarea functionarului de securitate a unitatii/structurii respective, cu respectarea politicii INFOSEC.

Art.271 Utilizarea echipamentelor si software puse la dispozitie decatre alte instituii sau autoritati publice sau privat pentru stocarea, procesarea sau transmiterea informatiilor clasificate se acrediteaza de catre AAIAS.

Art.272 (1) Echipamentele puse la dispozitie de catre alte institutii sau autoritati publice sau private se iau in evidenta unitatii.

(2) Este obligatorie acreditarea SIC prevazute la alin.1 inainte de intrarea in functiune.

Capitolul XIII – PREGATIREA SI INSTRUIREA PERSONALULUI

Art.278 (1) Pregatirea si instruirea in domeniul INFOSEC este obligatorie pentru intreg personalul care isi desfasoara activitatea in SIC.

(2) Activitateade instruire se efectueaza planificat, permanent si diferentiat, in functie de atributiile personalului, precum si de clasa sau nivelul de secretizare acordat prin certificatul de securitate/autorizatia de acces la informatii clasificate.

(3) Personalul autorizat cu acces in zona de operare a SIC este instruit cu privire la necesitatea respectarii masurilor si procedurilor de securitate, atat la inceperea activitatii cat si periodic.

Art.279 (1) Administratorul de securitate se numeste din randul personalului cu studii superioare in domeniul Tehnologiei Informatiilor si Comunicatiilor – TIC si pregatire de specialitate in securitatea informatiilor sau care a lucrat in domeniu, fiind propus de seful CSTIC si avizat de functionarul de securitate.

(2) Administratorul de securitate se va selectiona,pe cat posibil, din randul personalului care a indeplinit anterior functii de administratori de system/retea.

Art.280 Principalele etape in selectionarea si verificarea administratorului de securitate constau in:

a. identificarea personalului cu pregatire profesionala adecvata;
b. obtinerea acceptului persoanei selectionate, prin raport scris;
c. obtinerea certificatului de securitate corespunzator clasei sau nivelului de secretizare cel mai inalt pentru informatiile stocate, procesate sau transmise in SIC.

Art.281 (1) In urma desfasurarii procesului de selectionare si verificare, pe baza solicitarii scrise a functionarului de securitate a unitatii/structurii respective, administratorul de securitate este avizat din punct de vedere al cerintelor de securitate de catre AAISIC.

(2) Avizarea trebuie sa aiba loc inainte de numirea in functie.

Art.282 (1) Administratorul desecuritate, de system/retea sunt atestati din punct de vedere al pregatirii de specialitate in urma absolvirii cursului de pregatire al informatiilor clasificate in format electronic.

(2) Tematica cursului se intocmeste in colaborare cu AAISIC.

(3) Din comisia de examinare face parte, obligatoriu un reprezentant al AAISIC.

Art.,287 (1) Utilizatorii din cadrul unui SIC vor fi instruiti trimestrial priuvind cunoasterea PrOpSex, de catre seful CSTIC.

(2) In cazul producerii unor incidente de securitate, seful CSTIC prelucreaza cu intreg personal autorizat sa aiba acces la SIC, cauzele, modul derezolvare si masurile luatye in situatiile respective in colaborare cu AAISIC.

Art.288 Planul de pregatire a personaluhi este elaborate,annual, de catre seful CSTIC si este parte componenta din Planul specific de pregatire a personalului.. In continutul acestuia sunt mentionate responsabilitatile, termenele, mijloacele si metodele de instruire si de educatie de securitate.

Art.289 In cadrul temelor de pregatire specifica, se are in vedere introducerea unor lectii, informari, prelegeri, simpozioane, sedinte cu character aplicativ referitoare la:

a. cunoasterea si identificarea amenintarilor, vulnerabilitatilor si riscurilor privind securitatea SIC
b. protectia fizica a hardware si software
c. cunoasterea configuratiei sistemului
d. accesul in zonele in care functioneaza SIC
e. protectia diferentiata a informatiilor, resurselor, proceselor si mediilor de stocare
f. protectia antivirus
g. asigurarea protectiei transmisiilor de date si voce.

Art.290 Fiecare forma de pregatire la care participa utilizatorii si personalul cu atributii privind securitatea SIC se inscrie in fisa individuala de pregatire de catre seful CSTIC.

Capitaolul XIV – DISPOZITII FINALE

Art. 291 Annual si ori de cate ori este nevoie se executa, pe durata a 1-3 zile, instruirea personalului care incadreaza structurile cu responsabilitati in domeniul INFOSEC.

Art.292 Organizarea si coordonarea activitatii de pregatire se executa de catre Directia Generala de Informatii si Protectie Interna, prin AAIAS.