R O M Â N I A

Nesecret
Ex. unic

_____
(se va menţiona denumirea completă a instituţiei)

Nr. _____ din ___.___._____

A P R O B,
[CONDUCĂTORUL INSTITUȚIEI]

[NUME ŞI PRENUME]

DOCUMENTAȚIE DE SECURITATE
A
SIC [DENUMIRE SISTEM]

Versiunea __

AVIZAT,
ŞEF STRUCTURĂ DE SECURITATE/
FUNCŢIONAR DE SECURITATE

[NUME ŞI PRENUME]

Întocmit,
ŞEF CSTIC SIC *[DENUMIRE SISTEM]*/
FUNCŢIONAR DE SECURITATE TIC[1]

[NUME ŞI PRENUME]

[1] Documentaţia este întocmită de şeful CSTIC doar în situaţia în care există CSTIC constituit la nivelul instituţiei, altfel sarcina privind întocmirea documentaţiei de securitate îi revine şefului structurii de securitate/funcţionarului de securitate.

Istoricul versiunilor

Nr. crt.	Numărul Versiunii	Modificat de	Motivul modificării	Data elaborării
1.				
2.				
3.				
4.				
5.				

Notă. Pentru gestionarea unitară a versiunilor documentaţiei de securitate, acestea vor fi numerotate astfel:

versiuni intermediare: 0.1, 0.2, ….
versiune finală 1.0; (prima acreditare)
versiuni intermediare: 1.1, 1.2,….
versiune finală 2.0; (prima reacreditare)
versiuni intermediare: 2.1, 2.2,….
.....etc...

CUPRINS

1. INTRODUCERE

1. Acest document constituie Documentația de Securitate a Sistemului Informatic şi de Comunicaţii dedicat procesării şi stocării informaţiilor clasificate în cadrul _____ *se va menţiona denumirea completă a instituției*, independent faţă de celelalte sisteme informatice existente şi va fi numit în continuare ***SIC [DENUMIRE SISTEM]*** *(se va menţiona numele alocat sistemului informatic, urmând ca acesta să fie menţionat în mod unitar la nivelul întregii documentaţii)*.

1.1 Descrierea *SIC [DENUMIRE SISTEM]*

-acest subcapitol va cuprinde o descriere sumară a sistemului şi o subliniere a capacităţilor funcţionale, detalii despre modul de operare de securitate al SIC şi clasa de secretizare a informaţiilor vehiculate în SIC, în conformitate cu art. 19, alin.(2) din Ghidul privind structura şi conţinutul Procedurilor Operaţionale de Securitate (PrOpSec) pentru sisteme informatice şi de comunicaţii - DS 2. Aspecte care sunt necesare a fi cuprinse în acest subcapitol se regăsesc şi în Anexa 2 - "Structura şi conţinutul documentului cu Cerinţele de Securitate Specifice Sistemului (CSSS)" la Ghidul pentru elaborarea Documentaţiei cu Cerinţele de Securitate (DCS) pentru Sistemele Informatice şi de Comunicaţii (SIC) – DS 1.

2. Obiectivul *SIC [DENUMIRE SISTEM]* este de a procesa şi stoca informaţii clasificate "**secret de serviciu**" în cadrul _____ *se va menţiona denumirea completă a instituției*, de către personal autorizat, în baza atribuţiilor statuate prin reglementări interne.

3. *SIC [DENUMIRE SISTEM]* este compus din totalitatea resurselor tehnice, umane şi procedurale care contribuie la realizarea activităţilor de procesare, stocare şi transfer a datelor și informațiilor din activitatea curentă a _____ *se va menţiona denumirea completă a instituției*.

4. *SIC [DENUMIRE SISTEM]* este amplasat în camera numărul __, etajul __ din sediul ___ aflat la adresa _____ conform schiţei prezentate în *Anexa 1 - Schema de dispunere a SIC [DENUMIRE SISTEM]*;

5. Intrarea/ieşirea informaţiilor în/din *SIC [DENUMIRE SISTEM]* se realizează în scopul _____ ;

-se vor completa succint tipurile de operaţii referitoare la fluxurile de intrare/ieşire a datelor în/din SIC - ex: elaborării şi transmiterii documentelor solicitate către beneficiari, actualizării/consultării bazelor de date, actualizării componentelor firmware şi software, salvării fişierelor de audit/backup pe medii de stocare externe dedicate, etc.

6. Pe echipamentele din cadrul *SIC [DENUMIRE SISTEM]* se stochează informaţii care fac parte din domeniul de competenţă al _____ *se va menţiona denumirea completă a instituției*

7. În *SIC [DENUMIRE SISTEM]* pot fi vehiculate informaţii neclasificate sau informaţii clasificate "secret de serviciu", accesul la acesta realizându-se în conformitate cu *Hotărârea Guvernului României privind protecţia informaţiilor secrete de serviciu nr. 781 din 25.07.2002*;

8. Modul de operare de securitate pentru *SIC [DENUMIRE SISTEM]* va fi _____ *se va completa modul de operare ales (dedicat / de nivel înalt)*, conform *art. 264 din Standardele naţionale de protecţie a informaţiilor clasificate în România, aprobate prin HG 585/2002.* În acest mod de operare de securitate, _____ *se va completa cu descrierea modului de operare ales, conform art. 265/266 din Standardele naţionale, după caz.*

1.2 Autorităţile implicate în securitatea *SIC [DENUMIRE SISTEM]*

-în funcţie de volumul de activitate, de nivelul de încadrare a instituţiei cu resurse umane specializate şi dacă cerinţele de securitate permit, la numirea în funcţiile de administrare a securităţii se vor avea în vedere următoarele:

-structura de securitate/funcţionarul de securitate poate îndeplini şi funcţia de administrator de securitate al SIC şi cea de administrator de securitate al obiectivului - conform art. 271, alin.2 din Standardele naţionale de protecţie a informaţiilor clasificate în România aprobate prin HG 585/2002;

-atribuţiile CSTIC/funcţionarul de securitate TIC pot fi îndeplinite de administratorul de sistem. Se va avea în vedere ca atribuirea sarcinilor şi răspunderilor personalului să se facă în aşa fel încât să NU existe o persoană care să aibă cunoştinţă sau acces la toate programele şi cheile de securitate, parole, mijloace de identificare personală conform precizărilor de la art. 275 din Standardele naţionale de protecţie a informaţiilor clasificate în România, aprobate prin HG 585/2002, respectiv prevederile cuprinse în art. 276 şi art. 277. De asemenea se va avea în vedere faptul că funcţiile de administrator de securitate al SIC şi cea de administrator de sistem al SIC sunt obligatoriu a fi definite pentru administrarea securităţii SIC - în conformitate cu art. 18, respectiv art. 20 din Directiva privind structurile cu responsabilităţi în domeniul INFOSEC - INFOSEC 1;

-celelalte funcţii de administrare se definesc în situaţia în care configuraţia sistemului şi volumul datelor vehiculate de acesta reclamă acest lucru (ex: dacă sistemul gestionează baze de date va fi definită funcţia de administrator de baze de date; dacă în cadrul sistemului sunt utilizate produse sau echipamente de criptare a datelor se defineşte funcţia de administrator cripto etc.,);

-administratorul de sistem poate prelua atribuţiile administratorilor de aplicaţii, de medii de stocare, antivirus, cripto, etc.

9. Autorităţile principale implicate în securitatea *SIC [DENUMIRE SISTEM]* sunt:

- Structura de Securitate sau funcţionarul de securitate din cadrul _____ *se va menţiona denumirea completă a instituţiei*;
- Componenta de Securitate pentru Tehnologia Informaţiei şi Comunicaţiilor (CSTIC) sau funcţionarul de securitate TIC;
- Administratorul de securitate al SIC;
- Administratorul de securitate al obiectivului SIC;
- Administratorul de sistem al SIC;
- Administratorul antivirus;
- Administratorul mediilor de stocare;
- ..... *se vor completa toate funcţiile de administrare definite la nivelul SIC [DENUMIRE SISTEM]*
- Înlocuitorii administratorilor desemnaţi ai *SIC [DENUMIRE SISTEM].*

1.2.1 Structura de securitate/funcţionarul de securitate

- constituirea structurii de securitate este reglementată de art. 29 din Standardele naţionale de protecţie a informaţiilor clasificate în România, aprobate prin HG 585/2002.

10. Reprezintă punctul de contact între _____ *se va menţiona denumirea completă a instituţiei* şi autorităţile implicate în activitatea de protecţie a informaţiilor clasificate. Principalele responsabilităţi în domeniul INFOSEC ale structurii de securitate / funcţionarului de securitate sunt:

-atribuţiile generale sunt prevăzute în art. 31 din Standardele naţionale de protecţie a informaţiilor clasificate în România, aprobate prin HG 585/2002.

- elaborează normele interne privind protecţia informaţiilor naţionale clasificate, care trebuie să cuprindă şi prevederi referitoare la domeniul INFOSEC;

- coordonează activitatea internă de protecţie a informaţiilor naţionale clasificate în toate componentele acesteia, care includ şi domeniul INFOSEC;
- nominalizează componenţa CSTIC a *SIC [DENUMIRE SISTEM]*;
- execută monitorizarea internă privind aplicarea normelor de protecţie a informaţiilor naţionale clasificate vehiculate în *SIC [DENUMIRE SISTEM]* şi a modului de respectare a acestora;
- asigură relaţionarea cu structurile abilitate să coordoneze activitatea în domeniul INFOSEC şi controlează măsurile referitoare la protecţia informaţiilor naţionale clasificate vehiculate în *SIC [DENUMIRE SISTEM]*;
- asigură consultanţă pentru conducerea instituţiei din care face parte în legătură cu securitatea informaţiilor clasificate;
- organizează activităţi de pregătire specifică a persoanelor care au acces la informaţii clasificate, care să includă şi tematică specifică domeniului INFOSEC;

1.2.2 Componenta de Securitate pentru Tehnologia Informaţiei şi Comunicaţiilor - CSTIC

-instituirea CSTIC este obligatorie la nivelul fiecărui SIC în care se procesează/stochează informaţii clasificate iar atribuţiile acesteia sunt prevăzute în art. 244 din Standardele naţionale de protecţie a informaţiilor clasificate în România aprobate prin HG 585 din 13.06.2002, la alin.(2) din acelaşi articol precizându-se: "în funcţie de volumul de activitate şi dacă cerinţele de securitate permit, atribuţiile CSTIC pot fi îndeplinite numai de către funcţionarul de securitate TIC sau pot fi preluate, în totalitate, de către structura/funcţionarul de securitate din unitate".

11. Conform deciziei nr _____ din _____ *se va completa numărul şi data documentului de aprobare a constituirii CSTIC* a fost constituită CSTIC a *SIC [DENUMIRE SISTEM]* în următoarea componenţă:

-Şef CSTIC / Funcţionar de securitate TIC *se va alege după caz* : _____ *nume şi prenume*;
-Administrator de securitate al *SIC [DENUMIRE SISTEM] :* _____ *nume şi prenume*;
-Înlocuitor al administratorului de securitate al *SIC [DENUMIRE SISTEM] :* _____ *nume şi prenume*;
-Administrator de securitate al obiectivului *SIC [DENUMIRE SISTEM] :* _____ *nume şi prenume*;
-Înlocuitor al administratorului de securitate al obiectivului *SIC [DENUMIRE SISTEM] :* _____ *nume şi prenume*;
-Administrator de sistem al *SIC [DENUMIRE SISTEM] :* _____ *nume şi prenume*;
-Înlocuitor al administratorului de sistem al *SIC [DENUMIRE SISTEM] :* _____ *nume şi prenume*;
-Administrator de _____al *SIC* [*DENUMIRE SISTEM*] : _____ *nume şi prenume*.

-în continuare se vor nominaliza, dacă este cazul, toate celelalte funcţii de administrare din componenţa CSTIC inclusiv înlocuitorii acestora. În cazul în care se adoptă decizia prin care ***funcţionarul de securitate TIC*** *preia responsabilităţile* ***administratorului de sistem****, funcţia de* ***administrator de securitate al SIC*** *se poate desemna către* ***o altă persoană din cadrul CSTIC****. În funcţie de responsabilităţile nominalizate prin decizia de aprobare a constituirii CSTIC, se vor actualiza în consecinţă atribuţiile prevăzute în fişele posturilor aferente persoanelor astfel desemnate.*

În cadrul *SIC [DENUMIRE SISTEM]* funcţiile de administrator de securitate al SIC şi de administrator de sistem al SIC sunt deţinute de persoane diferite, iar funcţiile de administrator de _____, de administrator de _____ şi de administrator _____ sunt deţinute de aceeaşi persoană, atribuţiile specifice fiind detaliate în fişa postului. *(pentru a elimina posibilitatea de apariţie a unui conflict în cazul în care funcţiile de administrator de securitate al SIC şi înlocuitor al administratorului de sistem al SIC sunt deţinute de aceeaşi persoană, se recomandă ca şi funcţiile de înlocuitor al administratorului de securitate al SIC şi înlocuitor al administratorului de sistem al SIC să fie deţinute de persoane diferite)*

12. Înlocuitorii administratorilor definiţi în cadrul *SIC [DENUMIRE SISTEM]* pot prelua atribuţiile titularilor în orice moment.

13. Principalele responsabilităţi ale CSTIC / Funcţionarului de Securitate TIC a *SIC [DENUMIRE SISTEM]* sunt :

- elaborează şi actualizează documentaţia de acreditare de securitate a *SIC [DENUMIRE SISTEM]*;
- coordonează/implementează măsurile de securitate în cadrul *SIC [DENUMIRE SISTEM]*;
- asigură menţinerea nivelului de securitate la nivelul *SIC [DENUMIRE SISTEM]*;
- coordonează procesul de modificare a configuraţiei *SIC [DENUMIRE SISTEM];*
- coordonează procesul de schimbare a modului de operare de securitate ale *SIC [DENUMIRE SISTEM]*.
- comunică în cel mai scurt timp Structurii de Securitate/ Funcţionarului de Securitate evenimentele tehnice cu impact asupra securităţii şi funcţionalităţii *SIC [DENUMIRE SISTEM]* sau incidentele de securitate de la nivelul sistemului;
- participă la investigarea incidentelor de securitate constatate la nivelul *SIC [DENUMIRE SISTEM]*;
- asigură reluarea, periodic la un interval _____ *se va menţiona concret intervalul la care va fi reluat procesul de analiză de risc (ex: trimestrial/semestrial, etc)* şi ori de câte ori este necesar, a procesului de analiză de risc, activitatea finalizându-se cu un document, ce va fi avizat de şeful structurii de securitate/funcţionarul de securitate şi propus spre aprobare la nivelul conducerii instituţiei, în care se vor prezenta concluziile rezultate şi recomandări privind securitatea *SIC [DENUMIRE SISTEM]*.

1.2.3 Administratorul de securitate al *SIC [DENUMIRE SISTEM]*

14. Este responsabil de asigurarea implementării şi menţinerii măsurilor de securitate referitoare la domeniul INFOSEC aplicabile *SIC [DENUMIRE SISTEM]*.

15. Răspunde de modul de aplicare şi respectare a măsurilor de securitate corespunzătoare implementate pentru asigurarea confidenţialităţii, integrităţii şi disponibilităţii informaţiilor procesate şi stocate în *SIC [DENUMIRE SISTEM]* şi are ca principale responsabilităţi:

- supervizarea elaborării, implementării şi menţinerii măsurilor de securitate din cadrul *SIC [DENUMIRE SISTEM]*;
- asigurarea managementului identităţii şi autorizării utilizatorilor *SIC [DENUMIRE SISTEM]*;
- asigurarea de consultanţă pentru membri CSTIC şi utilizatorii *SIC [DENUMIRE SISTEM]* privind securitatea sistemului*;*
- participarea la investigarea incidentelor de securitate constatate la nivelul *SIC [DENUMIRE SISTEM]*;
- analizarea şi propunerea spre aprobare a cererilor de vizitare a obiectivului *SIC [DENUMIRE SISTEM]*;

- asigurarea respectării măsurilor şi procedurilor de securitate pentru activitatea de întreţinere a *SIC [DENUMIRE SISTEM]* şi actualizarea evidenţelor referitoare la această activitate;
- avizarea modificărilor configuraţiei *SIC [DENUMIRE SISTEM]*;
- asigurarea respectării măsurilor şi procedurilor de securitate în ceea ce priveşte controlul mediilor de stocare din cadrul *SIC [DENUMIRE SISTEM]*;
- gestionarea relaţiei cu contractorii pentru a se asigura că activităţile de întreţinere ale *SIC [DENUMIRE SISTEM]* se efectuează fără a fi afectată securitatea acestuia.

1.2.4 Administratorul de securitate al obiectivului *SIC [DENUMIRE SISTEM]*

-în conformitate cu prevederile art. 271 din HG 585/2002 "responsabilităţile unui administrator de securitate al obiectivului SIC pot fi îndeplinite de către structura/funcţionarul de securitate a instituţiei, ca parte a îndatoririlor sale profesionale".

16. Este responsabil de asigurarea implementării şi menţinerii măsurilor de securitate fizică aplicabile locaţiei *SIC [DENUMIRE SISTEM]* respectiv în cadrul Mediului Global de Securitate - MSG şi Mediul de Securitate Locală - MSL şi are ca principale responsabilităţi:

- supervizarea elaborării, implementării şi menţinerii măsurilor de securitate fizică specifică *SIC [DENUMIRE SISTEM]*;
- participarea la elaborarea şi actualizarea documentaţiei de acreditare a *SIC [DENUMIRE SISTEM]* în părţile ce îl privesc;
- notificarea imediată a structurii de securitate/administratorului de securitate al *SIC [DENUMIRE SISTEM]* cu privire la orice eveniment sau incident de securitate fizică survenit sau care este posibil a avea loc;
- participarea la investigarea incidentelor de securitate constatate la nivelul *SIC [DENUMIRE SISTEM]*;
- asigură desfăşurarea în condiţii de securitate a vizitelor în obiectivul *SIC [DENUMIRE SISTEM]*;
- supervizarea respectării procedurilor privind portul ecusoanelor şi însoţirea vizitatorilor în obiectivul *SIC [DENUMIRE SISTEM]*.

1.2.5 Administratorul de sistem al *SIC [DENUMIRE SISTEM]*

17. Administratorul de sistem al *SIC [DENUMIRE SISTEM]* răspunde de managementul procesului operativ de funcţionare al sistemului şi are ca principale responsabilităţi:

- asigură managementul configuraţiei;
- asigură managementul conturilor de acces în *SIC [DENUMIRE SISTEM]* în baza cererilor de acordare a drepturilor de acces la resursele SIC avizate de administratorul de securitate şi de şeful structurii de securitate/ funcţionarul de securitate şi aprobate de conducătorul instituţiei - *Anexa 2 - Cerere de acordare a drepturilor de acces la resursele SIC [DENUMIRE SISTEM];*
- utilizarea echipamentelor *SIC [DENUMIRE SISTEM]* în condiţii optime;
- gestionarea şi repartizarea resurselor hardware şi software;

- întreţinerea şi repararea echipamentelor *SIC [DENUMIRE SISTEM]*;
- actualizarea evidenţelor privind funcţionarea *SIC [DENUMIRE SISTEM]*;
- instalarea, configurarea şi actualizarea sistemele de operare în conformitate cu politicile de securitate aprobate;
- asigură notificarea imediată a administratorului de securitate cu privire la orice eveniment informatic sau incident de securitate survenit sau care este posibil a avea loc;
- coordonează activitatea de salvare, evaluare şi analiză a înregistrărilor de audit şi a jurnalelor produselor antivirus.

1.2.6 Administratorul antivirus al *SIC [DENUMIRE SISTEM]*

dacă este cazul se nominalizează separat sau se transferă atribuţiile la secţiunea administratorului de sistem

18. Administratorul antivirus răspunde de implementarea şi respectarea măsurilor de protecţie antivirus în cadrul *SIC [DENUMIRE SISTEM]* şi are ca principale responsabilităţi:

- instalarea, configurarea şi actualizarea produselor antivirus pe echipamentele din compunerea *SIC [DENUMIRE SISTEM]*;
- efectuarea controlului antivirus al mediilor de stocare utilizate;
- notificarea imediată a administratorului de securitate cu privire la orice eveniment informatic sau incident de securitate survenit sau care este posibil a avea loc.
- participarea la activitatea de evaluare şi analiză a jurnalelor produselor antivirus.

1.2.7 Administratorul mediilor de stocare al *SIC [DENUMIRE SISTEM]*

dacă este cazul se nominalizează separat sau se transferă atribuţiile la secţiunea administratorului de sistem

19. Administratorul mediilor de stocare are în responsabilitate gestionarea acestora pe întreg ciclul de viaţă al *SIC [DENUMIRE SISTEM]* şi are ca principale responsabilităţi:

- solicitarea, preluarea, înserierea, evidenţa, distribuirea şi distrugerea mediilor de stocare în conformitate cu procedurile aprobate;
- inventarierea periodică a mediilor de stocare utilizate în *SIC [DENUMIRE SISTEM],* verificarea modului de marcare şi a conţinutului acestora, în vederea asigurării faptului că pe acestea se gestionează informaţii clasificate în conformitate cu clasa de secretizare, în concordanţă cu cele specificate în *Anexa 3 - Registrul de evidenţă a mediilor de stocare ale SIC [DENUMIRE SISTEM];*
- asigurarea notificării imediate a administratorului de securitate cu privire la orice eveniment informatic sau incident de securitate survenit sau care este posibil a avea loc.

1.2.8 Administratorul de aplicaţii al *SIC [DENUMIRE SISTEM]*

dacă este cazul se nominalizează separat sau se transferă atribuţiile la secţiunea administratorului de sistem

20. Administratorul de aplicaţii răspunde de managementul aplicaţiilor în *SIC [DENUMIRE SISTEM]* şi are ca principale responsabilităţi:

- instalarea, dezinstalarea, configurarea şi actualizarea aplicaţiilor instalate în *SIC [DENUMIRE SISTEM]*;

- asigură notificarea imediată a administratorului de securitate cu privire la orice eveniment informatic sau incident de securitate survenit sau care este posibil a avea loc.

1.2.9 Administratorul de baze de date al *SIC [DENUMIRE SISTEM]*

dacă este cazul se nominalizează separat sau se transferă atribuţiile la secţiunea administratorului de sistem

21. Administratorul de baze de date răspunde de gestionarea şi securitatea bazelor de date ale *SIC [DENUMIRE SISTEM]* şi are ca principale responsabilităţi:

- implementează măsurile de securitate pentru bazele de date aflate în responsabilitate;
- asigură integritatea datelor din bazele de date şi a corelărilor dintre ele;
- asigură managementul accesului la bazele de date;
- efectuează copiile de siguranţă ale bazelor de date şi răspunde de refacerea datelor conform procedurilor aprobate;
- actualizează versiunile bazelor de date din sfera de responsabilitate;
- asigură notificarea imediată a administratorului de securitate cu privire la orice eveniment informatic sau incident de securitate survenit sau care este posibil a avea loc.

1.2.10 Utilizatorii *SIC [DENUMIRE SISTEM]*

22. În cadrul *SIC [DENUMIRE SISTEM]* toţi utilizatorii sunt obligaţi:

- să cunoască regulile de securitate şi normele de aplicare ale acestora, conţinute în documentaţia de acreditare de securitate, referitoare la exploatarea autorizată a *SIC [DENUMIRE SISTEM]* în condiţii de securitate;
- să informeze imediat administratorii de securitate ai *SIC [DENUMIRE SISTEM]* cu privire la orice incident de securitate survenit sau care este posibil a avea loc, ameninţările probabile la adresa *SIC [DENUMIRE SISTEM]* şi orice suspiciune de vulnerabilitate;
- să asigure controlul şi păstrarea corespunzătoare a mediilor de stocare;
- să exploateze *SIC [DENUMIRE SISTEM]* numai pentru îndeplinirea activităţilor autorizate, în concordanţă cu principiul necesităţii de a cunoaşte;
- să nu instaleze nici un alt tip de software şi să nu distrugă fizic echipamentele *SIC [DENUMIRE SISTEM]*;
- să nu ocolească, forţeze sau să testeze mecanismele de securitate ale *SIC [DENUMIRE SISTEM]*;
- să nu mute echipamentele *SIC [DENUMIRE SISTEM]* din locaţiile stabilite.

2. RAPORTUL PRIVIND ANALIZA DE RISC A *SIC [DENUMIRE SISTEM]* - RAR

-în scopul asigurării unui management eficient al riscului de securitate pentru SIC [DENUMIRE SISTEM] se vor avea în vedere prevederile Metodologiei privind managementul riscului de securitate pentru Sistemele Informatice şi de Comunicaţii (SIC) care stochează, procesează sau transmit informaţii clasificate - DS 3, în anexa 2 la documentul menţionat fiind prezentat şi un model de raport;
-detalii referitoare la managementul riscului de securitate se regăsesc în secţiunea 2.3 din Directiva principală privind domeniul INFOSEC - INFOSEC 2.

23. Scopul efectuării analizei de risc este de a identifica eventuale vulnerabilităţi şi ameninţări specifice *SIC [DENUMIRE SISTEM]* care pot fi exploatate, afectând integritatea, confidenţialitatea sau disponibilitatea datelor procesate şi transferate, urmate de formularea de cerinţe de securitate şi de elaborarea ulterioară a procedurilor operaţionale de securitate.

2.1 Modul de abordare a analizei riscului

24. Analiza de risc se efectuează de către Componenta de Securitate pentru Tehnologia Informaţiei şi Comunicaţiilor (CSTIC) / funcţionarul de securitate TIC a *SIC [DENUMIRE SISTEM].*

25. La efectuarea analizei de risc se au în vedere ameninţările şi vulnerabilităţile asociate unui *SIC [DENUMIRE SISTEM]* şi vizează următoarele domenii:

- securitatea fizică;
- securitatea personalului;
- securitatea documentelor;
- INFOSEC, incluzând securitatea hardware, securitatea software, protecţia antivirus, managementul şi auditul securităţii;
- planificarea măsurilor pentru situaţii de urgenţă şi pentru continuarea activităţii.

26. Analiza de risc a *SIC [DENUMIRE SISTEM]* se bazează pe documentaţia sistemului, specificul activităţii instituției care gestionează *SIC [DENUMIRE SISTEM]*, definirea fluxurilor informaţionale şi rolurilor în sistem, standarde, norme, recomandări şi ghiduri în domeniul securităţii.

27. Evaluarea riscurilor de securitate şi procesul de management al riscurilor au urmat o abordare structurată şi au inclus următoarele etape:

- identificarea scopului şi obiectivului evaluării riscurilor de securitate;
- determinarea bunurilor fizice şi informaţionale care contribuie la realizarea rolului *SIC [DENUMIRE SISTEM]*;
- determinarea valorii bunurilor fizice din componenţa *SIC [DENUMIRE SISTEM]*;
- determinarea valorii bunurilor informaţionale în contextul stabilirii impactului determinat de divulgarea, modificarea, indisponibilitatea şi / sau distrugerea informaţiilor clasificate procesate/stocate la nivelul *SIC [DENUMIRE SISTEM]*;
- identificarea ameninţărilor şi vulnerabilităţilor mediului de risc, precum şi nivelul acestora;
- identificarea contramăsurilor existente;
- determinarea contramăsurilor necesare şi compararea cu măsurile existente;

- revizuirea riscurilor de securitate şi a contramăsurilor recomandate, cu menţiunea că politica de securitate a _____ *se va menţiona denumirea completă a instituţiei*, impune aplicarea unui standard minim de protecţie pentru informaţiile clasificate;
- realizarea unui *Raport privind analiza de risc*, inclusiv o detaliere a contramăsurilor care sunt implementate şi o prezentare a riscurilor reziduale.

28. *SIC [DENUMIRE SISTEM]* va fi dezvoltat şi modificat în mod continuu, componentele hardware şi software vor fi schimbate şi actualizate cu noi versiuni iar dinamica proceselor existente la nivelul instituţiei pot genera inclusiv schimbări de personal. Toate aceste schimbări pot conduce la apariţia unor noi riscuri, iar riscurile reduse anterior pot genera noi provocări în domeniul asigurării securităţii. Din această cauză, CSTIC are în mod continuu misiunea de a efectua pe de o parte evaluarea şi estimarea riscurilor la adresa rolului *SIC [DENUMIRE SISTEM],* iar pe de altă parte identificarea şi implementarea tuturor măsurilor ce se impun pentru reducerea acestora.

29. Pentru obţinerea informaţiilor necesare s-a utilizat chestionarul din *Anexa 4 - Chestionar utilizat în analiza şi evaluarea SIC [DENUMIRE SISTEM]*.

-documentul a fost creat în vederea obţinerii informaţiilor despre sistem, un exemplu de chestionar fiind prezentat şi în anexa 1 la Metodologia privind managementul riscului de securitate pentru Sistemele Informatice şi de Comunicaţii care stochează, procesează sau transmit informaţii clasificate - DS 3;

30. Matricea de risc a fost alcătuită în conformitate cu *Metodologia privind managementul riscului de securitate pentru Sistemele Informatice şi de Comunicaţii care stochează, procesează sau transmit informaţii clasificate - DS 3*, procedându-se la identificarea vulnerabilităţilor iar ulterior la identificarea ameninţărilor. Determinarea nivelului de risc pentru fiecare eveniment nedorit care poate avea impact asupra *SIC [DENUMIRE SISTEM]* se face cu ajutorul matricei nivelului de risc prezentată în *Anexa 5 - Descrierea matricei de risc a SIC [DENUMIRE SISTEM].*

2.2 Descrierea sistemului

-descrierea sistemului, pe toate componentele, se va realiza în cadrul anexelor la prezentul document incluzând prezentarea hardware-ului (staţii de lucru, servere, routere, switch-uri incluzând descrierea legăturii de comunicaţii, etc.), a software-ului (sisteme de operare, aplicaţii, etc.), a datelor şi a utilizatorilor. Deasemenea, se va prezenta diagrama de conexiuni a SIC şi fluxul datelor de intrare şi de ieşire din sistem, pentru a contura scopul procesului de analiză a riscului;

31. Din punct de vedere hardware şi software, *SIC [DENUMIRE SISTEM]* este alcătuit din componentele prezentate în *Anexa 6 - Lista componentelor aparţinând SIC [DENUMIRE SISTEM]* şi în *Anexa 7 - Lista suporţilor de memorie dedicaţi SIC [DENUMIRE SISTEM]*. *(în cazul în care apar modificări la nivelul componenţei SIC [DENUMIRE SISTEM], anexele vor fi refăcute în consecinţă)*

32. Personalul care prin natura activităţii sale are acces la *SIC [DENUMIRE SISTEM]*, este asociat uneia din funcţiile prezentate la *Capitolul 1.2 - Autorităţile implicate în securitatea SIC [DENUMIRE SISTEM]*. Acesta este autorizat corespunzător clasei de secretizare a informaţiilor procesate. Lista de acces la resursele *SIC [DENUMIRE SISTEM]* pentru administratorii/utilizatorii definiţi este prezentată în *Anexa 8 - Lista personalului autorizat cu acces la SIC [DENUMIRE SISTEM].*

33. Informaţiile vehiculate în cadrul sistemului sunt: _____

-se vor menţiona, conform situaţiei existente la nivelul instituţiei, tipurile de date/informaţii vehiculate în cadrul SIC, de ex.: informaţii clasificate, generate sau recepţionate în format electronic şi informaţii pentru actualizarea software-ului de bază/antivirus.

34. Utilizarea mediilor de stocare în cadrul *SIC [DENUMIRE SISTEM]* se va efectua conform Procedurilor Operaţionale de Securitate stabilite în cadrul acestui document.

2.3 Ameninţări la adresa sistemului

-în cadrul secţiunii 2.4 din Directiva principală privind domeniul INFOSEC - INFOSEC 2, sunt definite ameninţările şi vulnerabilităţile la adresa unui SIC;
-prezentări generale ale ameninţărilor şi ale vulnerabilităţilor unui SIC se regăsesc în cadrul Ghidului INFOSEC privind analiza naturii şi proporţiilor ameninţărilor şi vulnerabilităţilor la adresa Sistemelor Informatice şi de Comunicaţii - DS 4;

35. Ameninţarea este reprezentată de posibilitatea de compromitere accidentală sau deliberată a securităţii *SIC [DENUMIRE SISTEM]*, prin pierderea confidenţialităţii, a integrităţii şi/sau a disponibilităţii informaţiilor procesate şi transferate.

36. Materializarea unor ameninţări la adresa sistemului se constituie în atacuri ce pot avea ca efect:

- pierderea confidenţialităţii: divulgarea neautorizată a informaţiilor prin accesul neautorizat la resursele informaţionale;
- pierderea integrităţii: modificarea neautorizată a informaţiilor (integritatea informaţiilor) şi pierderea posibilităţii exploatării corecte şi compatibile a resurselor informaţionale (integritatea sistemului);
- pierderea disponibilităţii: împiedicarea accesului autorizat, întârzierea efectuării operaţiilor de importanţă pentru rolul sistemului.

37. Analiza de risc a identificat ameninţările specifice sistemului, prezentate în *Anexa 9 - Lista ameninţărilor specifice SIC [DENUMIRE SISTEM], şi obiectivele securităţii care pot fi afectate.*

-o listă cu exemple de ameninţări şi efectele lor asupra obiectivelor securităţii (confidenţialitatea, integritatea şi disponibilitatea informaţiilor) este prezentată în tabelul 3-1 din Metodologia privind managementul riscului de securitate pentru Sistemele Informatice şi de Comunicaţii care stochează, procesează sau transmit informaţii clasificate - DS 3;

2.4 Vulnerabilităţi ale sistemului

38. Vulnerabilitatea reprezintă o breşă sau o slăbiciune în proiectarea şi implementarea securităţii sistemului sau în măsurile de securitate aplicate, care ar putea fi exploatată, accidental sau intenţionat, de către o ameninţare la adresa *SIC [DENUMIRE SISTEM].*

39. Lista vulnerabilităţilor asociate ameninţărilor la adresa securităţii *SIC [DENUMIRE SISTEM]* este prezentată în *Anexa 10 - Lista vulnerabilităţilor asociate ameninţărilor la adresa securităţii SIC [DENUMIRE SISTEM].*

-o listă cu exemple de vulnerabilităţi respectiv exemple de ameninţări care pot exploata aceste vulnerabilităţi, alături de tipurile de bunuri ale SIC care pot fi afectate, este prezentată în tabelul 3-3 din DS-3 - Metodologia privind managementul riscului de securitate pentru Sistemele Informatice şi de Comunicaţii care stochează, procesează sau transmit informaţii clasificate;

2.5 Rezultatele analizei riscului

40. Măsurile de securitate implementate, planificate şi recomandate, raportate la categoria de evenimente nedorite rezultate în urma analizei de risc, sunt prezentate în *Anexa 11 - Măsuri de securitate implementate în SIC [DENUMIRE SISTEM].*

-în cadrul capitolului 3.3.4 din Metodologia privind managementul riscului de securitate pentru Sistemele Informatice şi de Comunicaţii care stochează, procesează sau transmit informaţii clasificate - DS 3, sunt prezentate categoriile de măsuri de securitate care urmează a fi implementate de către persoana juridică, în scopul reducerii probabilităţii ca o ameninţare să exploateze o vulnerabilitate a sistemului.

41. Constatările rezultate în urma analizei de risc, sunt prezentate în *Anexa 12 - Centralizatorul ameninţărilor, vulnerabilităţilor asociate, măsurilor de securitate şi riscurilor reziduale din cadrul SIC [DENUMIRE SISTEM].*

-pentru completarea anexei, este necesară determinarea: probabilităţii de producere a unui eveniment nedorit, impactul producerii evenimentului nedorit, riscurile şi nivelurile asociate. Detalii despre aceste elemente se regăsesc în capitolele 3.3.5, 3.3.6, 3.3.7 din Metodologia privind managementul riscului de securitate pentru Sistemele Informatice şi de Comunicaţii care stochează, procesează sau transmit informaţii clasificate - DS 3;

2.6 Riscurile reziduale

42. Riscul rezidual reprezintă riscul acceptat, rămas neacoperit după implementarea în sistem a măsurilor de securitate recomandate. După implementarea măsurilor de securitate recomandate, din ***Centralizatorul ameninţărilor, vulnerabilităţilor asociate, măsurilor de securitate şi riscurilor reziduale din cadrul SIC [DENUMIRE SISTEM]***, riscul rezidual s-a redus la nivelul mic *(se va calcula în baza matricei de risc. În cazul în care riscul calculat depăşeşte acest nivel se va analiza completarea/implementarea unor măsuri suplimentare de securitate astfel încât să rezulte un risc rezidual mic.)* pentru toate ameninţările care pot exploata vulnerabilităţile sistemului.

43. Evaluarea / estimarea nivelului de risc, rezultat în urma analizei de risc privind *SIC [DENUMIRE SISTEM]*, este un proces continuu, care se reia periodic la un interval _____ *(se va menţiona concret intervalul la care va fi reluat procesul de analiză de risc (ex: trimestrial/semestrial, etc) -se va avea în vedere faptul că intervalul a fost stabilit şi la Capitolul 1.2.2 - Componenta de Securitate pentru Tehnologia Informaţiei şi Comunicaţiilor - CSTIC)* și ori de câte ori este necesar *se vor avea în vedere inclusiv cazurile care implică modificări la adresa SIC [DENUMIRE SISTEM] care nu determină noi ameninţări şi vulnerabilităţi)*.

3. CERINȚE DE SECURITATE SPECIFICE SISTEMULUI ALE *SIC [DENUMIRE SISTEM]* - CSSS

-prezentate detaliat în Anexa 2 - Structura şi conţinutul documentului cu Cerinţele de Securitate Specifice Sistemului (CSSS) la Ghidul pentru elaborarea Documentaţiei cu Cerinţele de Securitate (DCS) pentru Sistemele Informatice şi de Comunicaţii DS 1;

44. În contextul prezentului document, securitatea cuprinde politica generală de securitate, cerinţe şi proceduri care guvernează securitatea în toate formele.

45. CSSS identifică şi descrie mediile, cerinţele şi măsurile de securitate privind protecţia informaţiilor vehiculate prin *SIC [DENUMIRE SISTEM]*.

46. CSSS defineşte ceea ce presupune securitatea *SIC [DENUMIRE SISTEM]* şi precizează cum se obţin, administrează şi monitorizează toate aspectele relevante privind securitatea sistemului.

3.1 Sumarul cerinţelor de securitate

47. Pentru a putea contracara ameninţările şi vulnerabilităţile la adresa sistemului, cerinţele de securitate care se impun trebuie să acopere următoarele aspecte de securitate:

- accesul şi controlul accesului;
- identitatea şi autentificarea;
- evidenţa;
- auditul;
- scoaterea din uz şi reutilizarea obiectelor sistemului;
- integritatea şi disponibilitatea;

3.2 Definirea mediilor de securitate

-în anexa 1 la Ghidul pentru elaborarea Documentaţiei cu Cerinţele de Securitate (DCS) pentru Sistemele Informatice şi de Comunicaţii - DS 1, sunt definite mediile de securitate;

48. Noţiunile de Mediu de Securitate Globală (MSG), Mediu de Securitate Locală (MSL) şi Mediu de Securitate Electronică (MSE) sunt utilizate pentru demarcarea clară a responsabilităţilor privind securitatea unui SIC;

49. **Mediul de Securitate Globală (MSG)** se referă la domeniul de securitate al obiectivului şi este reprezentat de sediul _____ *se va menţiona denumirea completă a instituţiei* aflat la adresa _____ *se va completa adresa instituţiei*.

50. **Mediul de Securitate Locală (MSL)** se referă la domeniul de securitate în care este instalat sistemul şi este reprezentat de camera numărul __, etajul __ din sediul __ *se va menţiona denumirea completă a a instituţiei* Locaţia unde este amplasat sistemul este organizată şi delimitată ca *se va specifica zona administrativă sau după caz de securitate, conform organizării proprii la nivelul instituţiei* în cadrul Programului de Prevenire a Scurgerii de Informaţii Clasificate (*PPSIC*), înregistrat la nr. _____ din data de _____ *în cazul în care la momentul elaborării prezentei documentaţii, PPSIC nu este încă aprobat/avizat, numărul şi data înregistrării acestuia se vor menţiona olograf după aprobarea acestuia* şi este marcată corespunzător.

51. **Mediul de Securitate Electronică (MSE)** se referă la domeniul de securitate în care sunt luate măsuri de protecţie a componentelor sistemului şi a informaţiilor atunci când sunt procesate şi transferate în formă electronică, şi este reprezentat de *SIC [DENUMIRE SISTEM]*.

3.3 Definirea măsurilor de securitate

3.3.1 Accesul, controlul accesului, identificarea şi autentificarea

52. Accesul este un tip specific de interacţiune între un subiect (utilizator) şi un obiect (date) care are ca rezultat fluxul de informaţii de la unul la celălalt. **Controlul accesului** constituie exercitarea controlului asupra acestei interacţiuni. **Identificarea** şi **autentificarea** reprezintă procesul de stabilire a validităţii unei identităţi revendicate.

53. **Cerinţa politicii de securitate** este ca **accesul** la informaţiile clasificate trebuie să fie limitat la persoanele care deţin autorizaţie de acces conform clasei de secretizare a informaţiilor vehiculate, potrivit principiului nevoii de a cunoaşte. **Personalul autorizat** la *SIC [DENUMIRE SISTEM]* şi la informaţiile sale clasificate trebuie să fie identificat în mod corespunzător.

54. **Riscul asociat** este ca persoanele fără autorizaţie de acces corespunzătoare clasei de secretizare a informaţiilor vehiculate sau care nu respectă principiul necesităţii de a cunoaşte, pot intenţionat sau accidental să obţină **accesul** neautorizat la informaţiile clasificate protejate ale *SIC [DENUMIRE SISTEM]*. Totodată un alt risc asociat este ca personalul autorizat / neautorizat să poată lua **identitatea** unei persoane autorizate pentru a obţine acces la informaţii pentru care nu are necesitatea de a cunoaşte sau autorizaţie de acces.

55. **Măsuri de securitate aplicabile în MSG/MSL/MSE privind accesul, controlul accesului, identificarea şi autentificarea**

-în acest paragraf vor fi specificate măsurile de securitate efectiv implementate, la nivelul fiecărui mediu de securitate (ex: deţinerea autorizaţiilor de acces corespunzător clasei de secretizare a informaţiilor vehiculate pentru întreg personalul, utilizarea procedurilor privind controlul accesului vizitatorilor respectiv personalului care nu aparţine instituţiei şi are acces temporar în locaţia sistemului, utilizarea procedurilor privind drepturile de acces în sistem, acordarea şi revocarea privilegiilor, identificarea personalului prin intermediul ecusoanelor, cardurilor de identificare şi permiselor de acces, utilizarea procedurilor privind managementul parolelor şi a dispozitivelor de identificare personală, setarea unui nivel de complexitate adecvat şi schimbarea tuturor parolelor implicite înainte ca echipamentele să fie puse în funcţiune). Aspecte detaliate privind identificarea şi autentificarea în SIC sunt prezentate în Ghidul INFOSEC tehnic şi de implementare privind Identificarea şi Autentificarea în sistemele informatice şi de comunicaţii care vehiculează informaţii clasificate - DS 11 respectiv în Ghidul general de securitate a Sistemelor Informatice şi de Comunicaţii - DS 5;

3.3.2 Evidenţa şi Auditul

56. **Evidenţa** reprezintă înregistrarea procesării şi transferului informaţiilor.

57. **Auditul** reprezintă activitatea de monitorizare a evenimentelor referitoare la securitatea sistemului, pentru detectarea şi avertizarea asupra oricărei activităţi care ar putea ameninţa securitatea acestuia.

58. **Cerinţa politicii de securitate** este ca evidenţa informaţiilor procesate sau transferate să fie individuală şi orice încălcare sau tentativă de încălcare a securităţii sistemului trebuie să fie înregistrată. **Înregistrările** privind evenimentele de securitate

trebuie analizate periodic pentru a detecta şi avertiza în legătură cu activităţile care pot ameninţa securitatea sistemului.

59. **Riscul asociat** este evaluat pe de o parte din perspectiva faptului că personal autorizat/neautorizat poate avea acces la informaţii (*log-uri, fişiere de audit, jurnale de evenimente*, *etc.*) care depăşesc dimensiunea principiului necesităţii de a cunoaşte iar pe de altă parte din perspectiva acţiunilor care pot încălca securitatea, intenţionat sau accidental şi pot să nu fie detectate. Acest aspect poate avea ca efect faptul că măsurile pentru prevenirea sau împiedicarea producerii încălcărilor ulterioare sunt ineficiente.

60. **Măsuri de securitate** aplicabile în **MSG/MSL/MSE** privind evidenţa şi auditul.

-în acest paragraf vor fi specificate măsurile de securitate efectiv implementate, la nivelul fiecărui mediu de securitate (ex: modalitatea de asigurare a evidenţei datelor de audit, instituirea formelor de evidenţă a documentelor şi a mediilor de stocare intrate / ieşite în / din MSL / MSE inclusiv din perspectiva valorificării datelor preluate din aplicaţia de control al porturilor de intrare-ieşire (descrise în Anexa 6 - Lista componentelor aparţinând SIC - secţiunea Descriere Software), modul de implementare a politicii de efectuare a auditului din perspectiva evenimentelor de auditat cum ar fi crearea şi modificarea de obiecte, accesul utilizatorilor, modificarea privilegiilor etc.) raportat la completitudinea datelor colectate (data şi ora, utilizatorul, natura evenimentului, finalizare), modul de analizare şi valorificare a înregistrărilor de audit, asigurarea disponibilităţii şi protecţiei mecanismelor de audit împotriva accesului neautorizat. Aspecte detaliate privind evidenţa şi auditul la nivelul SIC sunt prezentate în Ghidul pentru elaborarea Documentaţiei cu Cerinţele de Securitate (DCS) pentru Sistemele Informatice şi de Comunicaţii - DS 1;

3.3.3 Scoaterea din uz şi disponibilizarea componentelor sistemului

61. La scoaterea din uz a echipamentelor şi/sau disponibilizarea unor componente ale sistemului se va analiza oportunitatea păstrării/distrugerii mediilor de stocare aparţinând echipamentului disponibilizat.

62. Reutilizarea mediilor de stocare rezultate în urma disponibilizării unor echipamente pe care au fost gestionate informaţii clasificate se realizează în conformitate cu *Ghidul INFOSEC privind reutilizarea, reclasificarea şi declasificarea mediilor de stocare ale calculatoarelor - DS 14* respectiv cu *Ghidul INFOSEC privind estimarea nivelurilor de încredere pentru medii specifice în care operează Sisteme Informatice şi de Comunicaţii - DS 13.*

63. Cerinţele politicii de securitate impun ca la reutilizarea mediilor de stocare rezultate în urma disponibilizării unor echipamente pe care au fost gestionate informaţii clasificate să fie utilizate produse software de suprascriere în conformitate cu *Directiva privind catalogul naţional cu pachete, produse şi profile de protecţie INFOSEC - INFOSEC 5*[2].

64. **Riscul asociat** este ca medii de stocare care au aparţinut echipamentului *SIC [DENUMIRE SISTEM]* să fie refolosite în alte sisteme în mod necorespunzător.

65. **Măsura de securitate** este ca ştergerea datelor şi informaţiilor să se realizeze conform procedurilor, de către administratorul de sistem/administratorul mediilor de stocare[3], prin utilizarea unor produse software în conformitate cu *Directiva privind catalogul naţional cu pachete, produse şi profile de protecţie INFOSEC - INFOSEC 5*.

66. Scoaterea din uz şi disponibilizarea/reutilizarea componentelor sistemului se realizează cu avizul administratorului de securitate al *SIC [DENUMIRE SISTEM].*

[2] se actualizează permanent prin Ordin al Directorului General al ORNISS.
[3] sau administratorul de sistem care îndeplineşte şi atribuţiile administratorului mediilor de stocare.

67. Mediile de stocare propuse pentru distrugere vor fi prezentate în mod detaliat în cadrul unui proces-verbal de distrugere, prezentat ca model în *Anexa 13 - Proces verbal distrugere suporţi de memorie,* ce va fi semnat de două persoane asistente autorizate să aibă acces la informaţii clasificate secrete de serviciu, avizat de structura de securitate/funcţionarul de securitate şi aprobat de conducătorul unităţii în conformitate cu prevederile *art. 79* din *Standardele Naţionale de protecţie a informaţiilor clasificate în România,* aprobate prin *HG 585/2002*.

3.3.4 Controlul integrităţii şi al disponibilităţii

68. Controlul Integrităţii este necesar pentru a nu exista nicio pierdere de integritate, consistenţă şi înţeles a informaţiei, autenticitate şi corectitudine a operaţiilor efectuate.

69. Controlul Disponibilităţii este necesar pentru asigurarea posibilităţii de consultare a informaţiei ori de câte ori este necesar, în conformitate cu principiul necesităţii de a cunoaşte, precum şi împiedicarea accesului neautorizat la serviciile şi resursele sistemului.

-această secţiune trebuie să acopere toate funcţiile necesare pentru a demonstra că informaţiile nu au fost modificate în mod neautorizat, cele privind asigurarea că resursele sunt accesibile şi pot fi utilizate la cerere de către o entitate autorizată şi cele privind detectarea/remedierea erorilor în vederea limitării impactului asupra operării SIC [DENUMIRE SISTEM] (ex: se vor invoca utilizarea procedurilor privind accesul şi controlul accesului, identificarea şi autentificarea utilizatorilor, utilizarea procedurilor privind controlul configuraţiei hardware şi software, utilizarea procedurilor privind evidenţa şi auditul operaţiilor efectuate, utilizarea procedurilor privind efectuarea copiilor de siguranţă, etc.).
Aspecte detaliate privind controlul integrităţii şi disponibilităţii la nivelul SIC sunt prezentate în Ghidul pentru elaborarea Documentaţiei cu Cerinţele de Securitate pentru Sistemele Informatice şi de Comunicaţii - DS 1;

3.4 Administrarea securităţii

-în acest paragraf va fi specificat modul în care se asigură administrarea securităţii SIC, aspecte detaliate în acest sens fiind prezentate în Ghidul pentru elaborarea Documentaţiei cu Cerinţele de Securitate (DCS) pentru Sistemele Informatice şi de Comunicaţii - DS 1;

70. Structurile cu responsabilităţi privind managementul securităţii *SIC [DENUMIRE SISTEM]* sunt prezentate în *Capitolul 1.2 - Autorităţile implicate în securitatea SIC [DENUMIRE SISTEM].*

71. Modul de realizare a analizei de risc aferentă *SIC [DENUMIRE SISTEM]* se regăseşte în *Capitolul 2 - Raportul privind analiza de risc a SIC [DENUMIRE SISTEM] - RAR.*

72. Procedurile Operaţionale de Securitate descriu modul de implementare al cerinţelor de securitate specifice *SIC [DENUMIRE SISTEM]*, metodele care trebuie urmată şi atribuţiile personalului responsabil cu aplicarea lor a căror detaliere se regăseşte în *Capitolul 4 - Proceduri Operaţionale de Securitate ale SIC [DENUMIRE SISTEM] - PrOpSec.*

73. Managementul configuraţiei constă în identificarea, păstrarea evidenţei şi auditul tuturor schimbărilor aduse *SIC [DENUMIRE SISTEM]* şi documentaţiei acestuia, pe toată durata ciclului său de viaţă.

3.4.1 Întreţinerea tehnică a sistemului

-această secţiune trebuie să prezinte informaţii privind instrucţiunile referitoare la folosirea furnizorului autorizat în mod corespunzător sau a personalului propriu al SIC, pentru întreţinerea hardware şi software, precum şi instrucţiunile referitoare la scoaterea echipamentelor şi a mediilor de stocare din locaţiile SIC în vederea reparării, aspecte detaliate în Ghidul pentru elaborarea Documentaţiei cu Cerinţele de Securitate (DCS) pentru Sistemele Informatice şi de Comunicaţii - DS 1;

74. Întreţinerea şi repararea echipamentelor *SIC [DENUMIRE SISTEM]* va fi asigurată conform procedurilor, pe toată perioada de utilizare a sistemului. Toate activităţile de întreţinere şi reparare se vor executa sub coordonarea şi supravegherea administratorului de securitate şi vor fi consemnate în *Anexa 14 - Registrul de intervenţii hardware şi software.*

3.4.2 Documentaţia sistemului

75. Documentaţia *SIC [DENUMIRE SISTEM]* va fi luată în evidenţă, păstrată şi mânuită conform prevederilor legale în vigoare.

76. Documentaţia şi eventualele completări ulterioare aprobate vor fi aduse la cunoştinţa utilizatorilor, în părţile ce-i privesc, în cadrul activităţilor de instruire şi pregătire a personalului autorizat al *SIC [DENUMIRE SISTEM]*.

3.4.3 Instruirea şi pregătirea personalului autorizat al *SIC [DENUMIRE SISTEM]*

77. În corelare cu responsabilităţile şi atribuţiile specifice, trebuie asigurată o instruire de securitate eficientă a întregului personal autorizat al sistemului. Instruirea se realizează periodic *(se va trece perioada/intervalul de realizare)* sau ori de câte ori este necesar *(ex: pt noi utilizatori, la schimbarea unor proceduri de lucru, etc.)*, fiind prelucrate teme specifice domeniului INFOSEC cât şi extrase/pasaje de interes din documentaţia de acreditare. La sfârşitul şedinţelor de pregătire utilizatorii vor semna fişele de instruire, un model pentru acestea regăsindu-se în *Anexa 15 - Fişa de instruire individuală a personalului autorizat al SIC [DENUMIRE SISTEM]*.

3.4.4 Acreditarea şi reacreditarea

78. În vederea acreditării *SIC [DENUMIRE SISTEM]* trebuiesc parcurse următoarele etape:

- derularea unui proces de management al riscului de securitate - etapa de analiză a riscului şi etapa de reducere a riscului;
- verificarea mediilor de securitate, precum şi a modului de implementare, însuşire şi respectare a măsurilor implementate la nivelul sistemului, în concordanţă cu cerinţele de securitate specifice, prin mecanisme de evaluare, testare şi certificare de securitate.
- analiza, evaluarea, avizarea şi propunerea spre aprobare a documentaţiei de securitate;

79. **Reacreditarea** reprezintă procesul de reluare a activităţii de acreditare de securitate şi devine obligatorie în oricare din situaţiile de mai jos:

- expirarea intervalului pentru care a fost obţinută acreditarea/reacreditarea;
- schimbarea ameninţărilor şi vulnerabilităţilor la adresa *SIC [DENUMIRE SISTEM]* care să conducă la necesitatea implementării unor noi măsuri de securitate;

- schimbarea MSG sau MSL a *SIC [DENUMIRE SISTEM]*;
- încălcarea normelor de securitate, compromiterea securităţii *SIC [DENUMIRE SISTEM]* sau un eveniment nedorit datorat unor breşe în proiectarea securităţii;
- schimbarea semnificativă a măsurilor de securitate fizică implementate sau a conţinutului documentaţiei de securitate;
- schimbarea semnificativă a configuraţiei *SIC [DENUMIRE SISTEM] (ex: schimbări semnificative la nivelul configuraţiei hardware ale SIC, adăugarea/modificarea unor echipamente ce oferă noi funcţii care nu au fost avute în vedere în etapa analizei de risc (înlocuirea unei imprimante cu un echipament multifuncţional ce are activate funcţii de copiere/multiplicare/scanare documente). În cazul în care modificările sunt minore respectiv nu sunt de natură să identifice noi ameninţări şi vulnerabilităţi asupra sistemului, se va proceda la detalierea acestora în cadrul unei noi analize de risc, nefiind necesară reacreditarea SIC (înlocuirea unei imprimante cu un echipament multifuncţional ce are dezactivate funcţiile de copiere/multiplicare/scanare documente).*
- modificarea componenţei *SIC [DENUMIRE SISTEM] în cazul în care SIC [DENUMIRE SISTEM] este reprezentat de o reţea de calculatoare*.

80. Procesul de acreditare/reacreditare se finalizează după aprobarea documentaţiei de securitate prin emiterea certificatului de *re/*acreditare de securitate în care sunt evidenţiate **denumirea SIC, clasa de secretizare a informaţiilor gestionate la nivelul sistemului, modul de operare de securitate şi perioada de valabilitate**. Un model de certificat de acreditare este prezentat în *Anexa 16 - Certificat de Acreditare de Securitate pentru SIC [DENUMIRE SISTEM]*.

4. PROCEDURI OPERAŢIONALE DE SECURITATE ALE *SIC [DENUMIRE SISTEM] - ProOpSec*

*-în acest capitol vor fi prezentate în detaliu **propriile** proceduri de lucru **utilizate**[4] în mediile de securitate aferente SIC. În cazul în care, conform situaţiei existente la nivelul instituţiei nu există unele **tipuri de activităţi**, pentru acestea nu se vor prezenta proceduri de lucru (ex: accesul delegaţiilor străine atunci când nu este cazul, scanarea atunci când activitatea nu se realizează, etc.). Detalii sunt prezentate în Ghidul privind structura şi conţinutul Procedurilor Operaţionale de Securitate (PrOpSec) pentru Sisteme Informatice şi de Comunicaţii - DS 2.*

4.1 Administrarea şi organizarea securităţii *SIC [DENUMIRE SISTEM]*

81. Procedurile Operaţionale de Securitate descriu modul de implementare al cerinţelor de securitate specifice *SIC [DENUMIRE SISTEM]*, metodele care trebuie urmată şi atribuţiile personalului responsabil cu aplicarea lor.

82. Nu sunt permise abateri de la conţinutul Procedurilor Operaţionale de Securitate sau modificări neautorizate a conţinutului acestora, după ce ele au fost aprobate.

83. Prevederile Procedurilor Operaţionale de Securitate sau modificările conţinutului acestora vor fi aduse la cunoştinţa întreg personalului autorizat al *SIC [DENUMIRE SISTEM]*, în părţile care-i privesc, iar aceştia vor semna un angajament prin care se obligă să respecte întocmai procedurile de securitate - *Anexa 17 - Model de angajament al personalului autorizat al SIC [DENUMIRE SISTEM].*

4.1.1 Proceduri administrative ale *SIC [DENUMIRE SISTEM]*

84. Întregul personal al *SIC* [DENUMIRE SISTEM] deţine autorizaţie de acces la informaţii clasificate "***secret de serviciu***", emisă de conducătorul unităţii deţinătoare. *conform modelului prezentat în anexa nr. 2 la HG nr. 781/2002*.

85. Administratorul de securitate al *SIC [DENUMIRE SISTEM]* răspunde de menţinerea măsurilor de securitate în cadrul sistemului şi acordă utilizatorilor dreptul de acces la acesta. Fiecare utilizator care se conectează la sistem deţine un mecanism de autentificare pe baza căruia îi este permis accesul şi îi sunt acordate drepturi şi privilegii de a accesa/utiliza resursele sistemului.

86. Administratorul de securitate avizează cererea de acordare a drepturilor de acces la resursele *SIC [DENUMIRE SISTEM],* prezentată în *Anexa 2 - Cerere de acordare a drepturilor de acces la resursele SIC [DENUMIRE SISTEM],* numai după ce s-a asigurat că solicitantul deţine autorizaţie de acces la informaţii clasificate din clasa secretelor de serviciu.

87. În cazul în care unui utilizator al *SIC [DENUMIRE SISTEM]* îi sunt atribuite alte sarcini de serviciu ce implică modificarea unor drepturi de acces la resursele *SIC [DENUMIRE SISTEM],* acesta are obligaţia de a solicita aprobarea unei noi cereri de acordare a drepturilor de acces la resursele *SIC [DENUMIRE SISTEM]*, administratorul de sistem al SIC urmând să actualizeze privilegiile de acces aferente contului acestui utilizator.

88. În cazul în care un utilizator al *SIC [DENUMIRE SISTEM]* părăseşte instituţia (temporar sau definitiv), administratorul de sistem blochează contul acestui utilizator, în funcţie de situaţie.

[4] în funcţie de modul de lucru, operaţiile efectuate la nivelul SIC, organizarea proprie a instituţiei, etc.

4.1.2 Raportarea incidentelor de securitate

89. Întregul personal al *SIC [DENUMIRE SISTEM]* este responsabil pentru asigurarea securităţii sistemului. O componentă a acestei responsabilităţi este raportarea în cel mai scurt timp a ***oricărei acţiuni sau inacţiuni contrare reglementărilor de securitate, a cărei consecinţă a determinat sau este de natură să determine compromiterea informaţiilor vehiculate în SIC***. În urma constatării producerii unui incident de securitate, personalul *SIC [DENUMIRE SISTEM]* este obligat să ia măsuri pentru minimizarea efectelor şi să informeze de îndată despre incident administratorul de securitate al SIC.

90. Concluziile privind cercetarea administrativă a cauzelor producerii incidentului de securitate respectiv măsuri de prevenire / reducere a riscurilor de repetare a incidentului de securitate constatat, se vor prezenta conducerii instituţiei într-un document al cărui model este prezentat în *Anexa 18 - Raport privind cercetarea unui incident de securitate INSOSEC în cadrul SIC [DENUMIRE SISTEM]*. Instituţia în cadrul căreia s-a produs incidentul are obligaţia de a notifica imediat autorităţile cu atribuţii în domeniul protecţiei informaţiilor clasificate în conformitate *cu art. 88 şi art. 90 din Standardele naţionale de protecţie a informaţiilor clasificate în România aprobate prin HG 585 din 2002 respectiv art. 1 lit. c) din HG 781 din 2002*.

91. Incidentele de securitate *INFOSEC* se pot referi la:

- orice activitate sau eveniment care compromite integritatea sistemului;
- orice activitate sau eveniment care blochează utilizarea resurselor şi serviciilor sistemului;
- orice activitate sau eveniment care compromite informaţiile vehiculate în sistem;
- fraudarea, exploatarea greşită sau abuzul în exploatarea sistemului;
- deteriorarea sau pierderea de software sau informaţii care aparţin sistemului;
- deteriorarea echipamentelor din componenţa sistemului;
- conectarea la sistem a unor medii de stocare care nu sunt dedicate sistemului sau care nu au fost înregistrate în formele de evidenţă specifice;
- descoperirea unor vulnerabilităţi hardware sau software care pot conduce la producerea unuia dintre evenimentele enumerate mai sus.

4.1.3 Luarea la cunoştinţă a PrOpSec

92. Toţi utilizatorii *SIC [DENUMIRE SISTEM]* sunt obligaţi să-şi însuşească prevederile Procedurilor Operaţionale de Securitate, în părţile ce-i privesc, ca etapă a procesului de instruire/pregătire de securitate a personalului cu acces la sistem.

4.2 Securitatea fizică

4.2.1 Mediile de securitate ale *SIC [DENUMIRE SISTEM]*

93. Măsurile de securitate fizică sunt necesare pentru contracararea posibilelor ameninţări din interiorul sau exteriorul locaţiei *SIC [DENUMIRE SISTEM]*. Se au în vedere procedurile de securitate definite în cadrul sistemului, folosite pentru prevenirea accesului neautorizat la resursele şi serviciile protejate ale *SIC [DENUMIRE SISTEM]*. În cadrul sistemului sunt definite trei medii de securitate care delimitează zonele în care sunt

implementate mecanisme specifice de control al securităţii detaliate la *Capitolul 2.2 - Descrierea Sistemului.*

4.2.1.1 Securitatea fizică în Mediul de Securitate Globală (MSG)

94. Securitatea clădirii/perimetrului în care este amplasat *SIC [DENUMIRE SISTEM]* este asigurată conform ***Planului de Paza şi Protecţie nr.*** _____ ***din*** _____ *se vor completa numărul şi data aprobării documentului procedural elaborat conform Legii 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor* .

-în continuare se va prezenta detaliat controlul accesului personalului în obiectivul în care este amplasat SIC [DENUMIRE SISTEM] (ex: Personalul de pază permite accesul în obiectiv numai persoanelor autorizate. Toate persoanele care intră în locaţia SIC [DENUMIRE SISTEM] trebuie să prezinte permisul de acces personalului de pază de la intrarea în obiectiv. Persoanele cu drept de acces privilegiat sunt notificate într-o listă separată de acces în obiectiv, care este actualizată în permanenţă de către structura de securitate. Persoanele din afara instituţiei (de exemplu, vizitatorii) sunt însoţite în permanenţă în interiorul locaţiei SIC [DENUMIRE SISTEM], etc.)

95. Administratorul de securitate al obiectivului răspunde de securitatea în MSG a *SIC [DENUMIRE SISTEM]*.

4.2.1.2 Securitatea fizică în Mediul de Securitate Locală (MSL)

96. Sistemul de control acces în MSL permite accesul numai personalului autorizat şi este un sistem de control pe bază de _____*(se va completa modalitatea de control acces la nivelul MSL)*. Camerele în care se află *SIC [DENUMIRE SISTEM]*, se închid cu _____ *(se va completa în funcţie de specificul instituţiei, ex: cheie, card de acces, amprentă,etc.) şi sunt dotate cu senzori de _____ (se va completa în funcţie de specificul instituţiei ex: mişcare, fum, etc.)*.

97. Controalele/măsurile de securitate implementate în MSL al *SIC [DENUMIRE SISTEM]* includ următoarele:

- securitatea fizică a echipamentelor (staţia de lucru, cablajul);
- securitatea fizică a mediilor de stocare;
- controlul configuraţiei hardware şi software.

4.2.1.3 Securitatea fizică în Mediul de Securitate Electronică (MSE)

98. MSE al *SIC [DENUMIRE SISTEM]* este reprezentat de sistemul informatic însuşi şi este în responsabilitatea administratorului de securitate. Măsurile de securitate care sunt implementate la nivelul MSE sunt descrise în detaliu în *Capitolul 4.5 - INFOSEC* al acestui document.

99. Accesul la *SIC [DENUMIRE SISTEM]* este permis numai personalului autorizat, iar monitoarele staţiilor de lucru sunt poziţionate în aşa fel încât să prevină vizualizarea informaţiilor afişate de către personalul neautorizat.

4.2.1.4 Delimitarea şi marcarea perimetrului

100. Zona în care este amplasat *SIC [DENUMIRE SISTEM]*, unde sunt vehiculate informaţii clasificate _____*(se va completa clasa/nivelul maxim al informaţiilor gestionate în cadrul MSL)* este delimitată în *Programul de Prevenire a Scurgerii de Informaţii Clasificate* ca zonă _____*(se va completa după caz, zonă de securitate clasa I/II sau zonă administrativă)*. La intrarea în această zonă este afişat un mesaj de atenţionare de forma: „ZONĂ _____” *se va completa după caz, zonă de securitate clasa I/II sau zonă administrativă.*

4.2.2 Cheile şi combinaţiile încuietorilor

-în continuare se va descrie procedura specifică fiecărei instituții. (ex: - Cheile de la uşile încăperilor SIC [DENUMIRE SISTEM] sunt mânuite numai de către acele persoane care au fost stabilite şi autorizate în scris de către şeful instituţiei. Personalul de serviciu răspunde de modul de păstrare al cheilor în cutiile special destinate în condiţii de securitate şi de modul de primire-predare a acestor chei, fiind obligat să verifice dacă la terminarea programului au fost predate toate cheile de la încăperile SIC [DENUMIRE SISTEM] şi au fost sigilate toate încăperile, operaţii ce vor fi evidenţiate într-un registru, al cărui model este prezentat în Anexa 22 - Registrul de predare-primire chei şi de evidenţă a cardurilor de acces. *În afara orelor de program cheile stau la personalul de serviciu, în cutii metalice sigilate. Acestea se predau şi se primesc pe semnătură în registrul special destinat. În cazul sesizării unor situaţii de nesigilare a spaţiilor de lucru, personalul de serviciu informează personalul în cauză sau şeful de structură, după caz, consemnează situaţia în procesul-verbal de predare-primire a serviciului şi aduce la cunoştinţa şefului instituției aceste aspecte. Administratorul de securitate al obiectivului SIC (sau persoana care îndeplineşte atribuţiile administratorului de obiectiv) este obligat să verifice periodic dacă predarea-primirea cheilor s-a efectuat conform regulilor stabilite. Cheile de rezervă se păstrează în cutii metalice sigilate, la personalul de serviciu în locuri special destinate şi pot fi folosite în situaţii de urgenţă în conformitate cu procedurile aprobate pentru aceste situaţii. (se va detalia procedura care se urmează în cazul în care este necesar utilizarea cheii de rezervă). În cazul pierderii sau dispariţiei unei chei, chiar şi pentru o scurtă perioadă de timp, încuietoarea pentru care era folosită acea cheie va fi înlocuită imediat. Structura de securitate a obiectivului va fi informată imediat despre eveniment, indiferent dacă acesta s-a petrecut în timpul orelor de program sau în afara lor. La predarea-primirea schimbului de către personalul de serviciu se efectuează o verificare a securităţii întregii locaţii a SIC [DENUMIRE SISTEM]. Aceasta cuprinde verificarea încuierii şi sigilării încăperilor în care se află echipamente SIC [DENUMIRE SISTEM], verificarea situaţiei înapoierii cheilor preluate de personalul SIC [DENUMIRE SISTEM] la începerea programului. Aspectele rezultate se consemnează în procesul verbal de predare-primire a serviciului.)etc..).*

4.2.3 Controlul accesului în locaţia *SIC [DENUMIRE SISTEM]*

-în continuare se va descrie procedura de realizare al pazei şi securităţii locaţiei SIC [DENUMIRE SISTEM] specifică fiecărei instituții.

101. Intrarea personalului în zona *SIC [DENUMIRE SISTEM]* se face numai în scopuri operaţionale (exploatare şi întreţinere), iar regulile de acces sunt impuse de administratorul de securitate al *SIC [DENUMIRE SISTEM]*.

102. În zona *SIC [DENUMIRE SISTEM]* este permis accesul **personalului autorizat** care exploatează şi/sau efectuează operaţii de întreţinere a *SIC [DENUMIRE SISTEM]* precum şi a altor persoane care au calitatea de **vizitatori**, accesul acestora fiind reglementat prin proceduri stabilite în acest sens. Toate persoanele care au acces în zona *SIC [DENUMIRE SISTEM]* sunt notificate în *Anexa 23 - Lista personalului cu acces în locaţia SIC [DENUMIRE SISTEM]*. Persoanele care nu sunt notificate în lista de acces sunt luate în evidenţă într-un registru al cărui model este prezentat în *Anexa 19 - Registrul de evidenţă a persoanelor care au primit aprobare de acces în zona SIC [DENUMIRE SISTEM]*.

103. În vederea realizării pazei şi securităţii clădirii şi a perimetrului, obiectivul în care se află *SIC [DENUMIRE SISTEM]* beneficiază de _____

-în continuare se vor prezenta detalii privind modul de asigurare a pazei şi securităţii perimetrului de amplasare al SIC [DENUMIRE SISTEM]. (ex: la nivelul obiectivului sunt operaţionalizate 5 posturi de pază şi control-acces. Pentru supravegherea perimetrului exterior al obiectivului este instalat un sistem TV cu circuit închis cu posibilitatea de a reţine datele înregistrate pentru un interval de 3 luni.

Terminalul sistemului (monitorul) este dispus în camera de executare a serviciului de permanenţă, situată la intrarea în clădire În cazul în care este operaţionalizat un sistem de alarmare atunci se va detalia modul de amplasare şi posibilitatea de accesare şi valorificare a acestuia. ex: Monitorizarea sistemului de detecţie a intruziunilor este efectuata de către _____, în camera __, etajul __. Modul de activare, dezactivare, răspuns sau de acţiune la avertizările date de sistemul de detecţie este inclus în atribuţiile _____, şi este prevăzut în documentul cu nr. _____. Lunar/Trimestrial... Administratorul de securitate al obiectivului SIC [DENUMIRE SISTEM] verifică periodic___ buna funcţionare a sistemelor de protecţie fizică , supraveghere video şi alarmare.)

4.2.4 Proceduri de control pentru personalul tehnic şi de întreţinere din afara instituţiei

104. Personalului tehnic, de întreţinere, de curăţenie sau alte categorii de personal vor fi însoţite şi supravegheate permanent de către personal autorizat al *SIC [DENUMIRE SISTEM]*. Toate echipamentele electronice, mediile de stocare şi alte echipamente necesare îndeplinirii activităţii acestor categorii de personal sunt verificate şi aprobate de către administratorul de securitate, înainte de a fi utilizate în locaţia *SIC [DENUMIRE SISTEM]*. Accesul acestor categorii de persoane în locaţiile *SIC [DENUMIRE SISTEM]* se face cu aprobarea şefului instituţiei şi avizul administratorului de securitate.

4.2.5 Proceduri referitoare la vizitatori

105. Pentru reducerea riscului de compromitere a informaţiilor clasificate, aprobarea accesului vizitatorilor în locaţia *SIC [DENUMIRE SISTEM]* trebuie analizată cu atenţie.

106. Vizitatorii sunt însoţiţi de personal autorizat pe întreaga durată a vizitei. Responsabilităţile personalului de însoţire sunt următoarele :

- întâmpină vizitatorii la intrarea în locaţia *SIC [DENUMIRE SISTEM]* şi îi însoţeşte şi supraveghează direct pe toată perioada vizitei;
- anunţă personalul din zona respectivă că urmează să fie primit un vizitator şi nominalizează încăperile în care este autorizat să aibă acces;
- se asigură că monitoarele staţiilor de lucru ale SIC *[DENUMIRE SISTEM]* sunt poziţionate în aşa fel încât conţinutul afişat de acestea să nu poată fi vizualizat de vizitatori;
- la terminarea vizitei însoţeşte vizitatorii la ieşirea din locaţia *SIC [DENUMIRE SISTEM]*.

107. Utilizatorii sistemului răspund de protejarea documentelor clasificate pe durata prezenţei vizitatorilor în zona *SIC [DENUMIRE SISTEM]*.

108. Şeful obiectivului furnizează administratorului de securitate toate informaţiile şi dispoziţiile necesare privind accesul privilegiat în locaţia sistemului, traseul şi cerinţele de însoţire pentru oficialităţi, reprezentanţi ai diferitelor instituţii ale statului, etc.

109. Dacă este necesar delegaţiile oficiale străine pot fi autorizate să viziteze locaţia *SIC [DENUMIRE SISTEM]*. Procedurile pentru autorizarea vizitelor delegaţiilor oficiale străine sunt stabilite de către CSTIC şi sunt supuse aprobării şefului instituţiei de către şeful structurii de securitate/funcţionarul de securitate. Procedurile de autorizare şi desfăşurare a unor astfel de activităţi au la bază respectarea strictă a principiului necesităţii de a cunoaşte. Şeful instituţiei precizează administratorilor de securitate traseul, zonele în care au acces vizitatorii, cerinţele privind însoţirea acestora şi ce

informaţii de interes general referitoare la activitatea din cadrul *SIC [DENUMIRE SISTEM]* pot fi aduse la cunoştinţa delegaţiilor.

4.2.6 Permise şi ecusoane

110. Intrarea personalului în locaţia *SIC [DENUMIRE SISTEM]* se face pe baza *(se va completa modalitatea de acces. ex: permis de acces, legitimaţiie de serviciu, card acces, etc.)* ce va fi purtat la vedere pe toată durata cât se află în locaţia *SIC [DENUMIRE SISTEM]*.

4.2.7 Controlul accesului echipamentelor în locaţia SIC

111. Administratorul de sistem al *SIC [DENUMIRE SISTEM]* întocmeşte, actualizează şi păstrează lista echipamentelor aprobate pentru a fi folosite în locaţia sistemului şi ţine evidenţa clară pe tipuri, serii, nivel de clasificare al informaţiilor pentru care sunt autorizate a fi folosite, loc de dispunere şi personalul care utilizează aceste echipamente.

112. Dacă pentru efectuarea unor lucrări de întreţinere sau pentru remedierea unor defecţiuni este necesară scoaterea unui echipament, ce conţine un mediu de stocare, din locaţia *SIC [DENUMIRE SISTEM],* atunci mediul de stocare va fi extras din echipament şi gestionat în conformitate cu normele în vigoare.

113. Lucrările de întreţinere şi depanare la echipamentele care aparţin *SIC [DENUMIRE SISTEM]* se efectuează numai de către personal propriu sau firme autorizate, respectând cerinţele de securitate, sub coordonarea administratorului de securitate. Toate operaţiile de întreţinere sunt evidenţiate într-un registru de intervenţii hardware şi software, conform modelului din *Anexa 14 - Registrul de intervenţii hardware şi software.*

4.3 Securitatea de personal

-în acest capitol vor fi prezentate detalii referitoare la certificările de securitate minime necesare utilizatorilor SIC [DENUMIRE SISTEM]. Totodată, trebuie precizată obligativitatea ca utilizatorii să respecte prevederile documentaţiei de securitate şi să participe la programele de pregătire şi conştientizare în domeniul securităţii informaţiilor, organizate de instituţie/companie.

4.3.1 Utilizatorii autorizaţi ai *SIC [DENUMIRE SISTEM]*

114. Toţi utilizatorii *SIC [DENUMIRE SISTEM]* sunt autorizaţi conform procedurilor în vigoare referitoare la securitatea de personal. Fiecare utilizator al *SIC [DENUMIRE SISTEM]* primeşte dreptul de a accesa numai acele informaţii clasificate care îi sunt necesare pentru îndeplinirea sarcinilor de serviciu conform principiului necesităţii de a cunoaşte. În *Anexa 8 - Lista personalului autorizat cu acces la SIC [DENUMIRE SISTEM]* este evidenţiat personalul precum şi seriile autorizaţiilor de acces ale acestora.

4.3.2 Personalul *SIC [DENUMIRE SISTEM]*

115. Administratorului de sistem al *SIC [DENUMIRE SISTEM]* atribuie drepturile de acces la sistem conform sarcinilor de serviciu, domeniului de activitate şi funcţiei îndeplinite, în baza:

- autorizaţiei de acces;
- cererii de acordare a drepturilor de acces la resursele *SIC [DENUMIRE SISTEM]* aprobate de conducătorul unităţii;

116. Funcţiile autorizate să utilizeze resursele *SIC [DENUMIRE SISTEM]* sunt stabilite de conducătorul instituţiei şi sunt prezentate în *Capitolul 1.2 - Autorităţile implicate în securitatea SIC [DENUMIRE SISTEM]*.

4.3.3 Pregătirea de securitate, educarea şi conştientizarea personalului *SIC [DENUMIRE SISTEM]*

117. Programul de pregătire de securitate, educare şi conştientizare este obligatoriu pentru întregul personal al *SIC [DENUMIRE SISTEM]* şi are scopul de a asigura îndeplinirea corespunzătoare a responsabilităţilor ce le revin tuturor utilizatorilor *SIC [DENUMIRE SISTEM]* privind securitatea sistemului. În cadrul programului vor fi incluse teme de instruire a utilizatorilor *SIC [DENUMIRE SISTEM]* referitoare la componenta *INFOSEC*.

-se vor specifica teme de interes funcţie de nivelul de pregătire, experienţă şi necesităţi de pregătire constatate. (ex: Managementul securităţii, Rolul şi responsabilităţile utilizatorilor, Raportarea incidentelor de securitate, Facilităţile tehnice de securitate, Permisiuni şi privilegii de acces, Capabilităţi de securitate ale sistemului, Protecţie antivirus,etc.).

118. Pregătirea de securitate, educarea şi conştientizarea personalului se efectuează periodic, în baza planificării stabilite de către structura de securitate.

4.3.4 Accesul în locaţiile *SIC [DENUMIRE SISTEM]* a persoanelor care nu au autorizaţie de acces

-se va descrie procedura specifică fiecărei instituții, în funcţie de categoria de zonă în care este amplasat SIC [DENUMIRE SISTEM] - în conformitate cu art. 98, art. 100 din HG 585/2002. (ex: în cazul în care SIC este amplasat într-o zonă administrativă sau zona de securitate clasa a II-a : Accesul personalului de curăţenie, muncitorilor, contractorilor şi altor categorii de personal care nu deţin autorizaţie de acces, dar care trebuie să aibă acces în locaţia SIC [DENUMIRE SISTEM], este permis numai cu aprobarea şefului obiectivului şi cu înştiinţarea administratorului de securitate al SIC [DENUMIRE SISTEM]. Aceştia sunt însoţiţi şi supravegheaţi pe întreaga durată de desfăşurare a activităţii în locaţia sistemului. etc.)

4.4 Securitatea informaţiilor

-conform art. 11 din Ghidul privind structura şi conţinutul Procedurilor Operaţionale de Securitate (PrOpSec) pentru sisteme informatice şi de comunicaţii - DS 2, în această secţiune se precizează faptul că securitatea informaţiilor vizează toate formele de documente, de exemplu documente în format hârtie, medii de stocare asociate calculatoarelor (de exemplu: CD, dispozitiv de memorie USB), dispozitive de calcul şi de comunicaţii portabile (de exemplu: laptop, agende electronice, tablete). Atunci când este cazul, capitolul va conţine şi detalii referitoare la:

- *a) tipul documentelor - medii de stocare fixe/detaşabile, documente în format hârtie;*
- *b) marcajele de securitate, marcajele administrative şi de limitare a diseminării care trebuie aplicate pe documentele utilizate;*
- *c) procedurile aplicabile pentru clasificarea şi marcarea corespunzătoare a documentelor;*
- *d) procedurile de transfer a informaţiilor;*
- *e) responsabilităţile şi procedurile privind înregistrarea şi controlul documentelor, precum şi procedurile de verificare a înregistrărilor, inclusiv frecvenţa acestora;*
- *f) procedurile referitoare la utilizarea, stocarea şi controlul mediilor de stocare, precum şi evidenţa acestora;*
- *g) responsabilităţile şi procedurile privind reclasificarea/ declasificarea/distrugerea şi scoaterea din uz a documentelor.*

119. Procedurile adoptate pentru asigurarea securităţii documentelor în cadrul *SIC [DENUMIRE SISTEM]* răspund riscurilor asociate gestionării volumului informaţiilor procesate sau transmise identificate, la nivelul sistemului, în vederea asigurării integrităţii, confidenţialităţii şi a disponibilităţii informaţiilor stocate/procesate în cadrul SIC.

4.4.1 Controlul informaţiei în format electronic

120. Informaţia în format electronic este reprezentată de texte, date, imagini sau sunete, înregistrate pe dispozitive de stocare sau pe suporturi magnetice, optice, electrice sau transmise sub formă de curenţi, tensiuni sau câmp electromagnetic în eter sau în reţele de comunicaţii.

121. Controlul informaţiilor clasificate şi al mediilor de stocare utilizate în *SIC [DENUMIRE SISTEM]* este în responsabilitatea administratorului de securitate şi a personalului special desemnat.

122. Suporţii de memorie externă se păstrează de către _____,*(se va specifica funcţia de administrare desemnată să gestioneze suporţii de memorie externă ex: administratorul mediilor de stocare, administratorul de sistem, etc.)* în _____*(se va specifica locul în care se păstrează suporţii de memorie externă. ex: cutii metalice sigilate, fişet metalic, dulap prevăzut cu cheie)*.

4.4.2 Mediile de stocare

4.4.2.1 Evidenţa şi gestionarea mediilor de stocare

123. Evidenţa şi gestionarea mediilor de stocare utilizate în cadrul *SIC [DENUMIRE SISTEM]* se va efectua astfel: _____

-în continuare va fi prezentat modul de gestionare a mediilor de stocare (ex: administratorul mediilor de stocare / administratorul de sistem păstrează evidenţa mediilor de stocare corespunzător clasei de secretizare a informaţiilor stocate pe acestea. Personalul autorizat este obligat să semneze în registrul de evidenţă pentru primirea unui mediu de stocare clasificat. După intrarea în posesia mediului de stocare clasificat, utilizatorii răspund de mânuirea şi păstrarea acestora în condiţiile de securitate. La restituirea mediului de stocare clasificat, utilizatorii sunt obligaţi să verifice dacă administratorul mediilor de stocare/administratorul de sistem a semnat în registrul de evidenţă pentru înapoierea acestora.etc.)

124. Procedurile pentru gestionarea informaţiilor şi mediilor de stocare clasificate impun respectarea regulilor generale privind evidenţa, întocmirea, păstrarea, procesarea, multiplicarea, manipularea, transportul, transmiterea şi distrugerea informaţiilor clasificate.

125. În cadrul *SIC [DENUMIRE SISTEM]* toate mediile de stocare, inclusiv cele care conţin software original, copii de siguranţă şi alte date de interes (update-uri ale sistemului de operare, update-uri ale software-ului antivirus, etc.), sunt înregistrate, gestionate şi păstrate conform prevederilor legale în materie. În *Anexa 3 - Registrul de evidenţă a mediilor de stocare ale SIC [DENUMIRE SISTEM]* este prezentat un model al registrului de evidenţă al tuturor mediilor de stocare inclusiv cele dedicate *SIC [DENUMIRE SISTEM]* *(conform rubricaţiei registrului menţionat, se vor evidenţia pe lângă caracteristicile tehnice ale suporţilor de memorie şi detalii referitoare la distribuirea/trasabilitatea acestora)*. În *Anexa 7 - Lista suporţilor de memorie dedicaţi SIC [DENUMIRE SISTEM]* este prezentată lista mediilor de stocare înregistrate şi dedicate *(Noţiunea de mediu de stocare dedicat se referă la faptul că acesta este utilizat în cadrul SIC cu un anumit scop şi în baza unei proceduri bine definite, detaliate în documentaţia de acreditare de securitate. (ex:CD-RW dedicat actualizării produsului antivirus, memory-stick dedicat transferurilor de date în/din SIC, memory-stick dedicat salvării copiilor de siguranţă, memory-stick dedicat stocării imaginii sistemului de operare şi salvării fişierelor de audit)* *SIC [DENUMIRE SISTEM]*, inclusiv HDD-ul staţiei de lucru Lista se actualizează periodic, în funcţie de situaţia concretă a suporţilor de memorie alocaţi *SIC [DENUMIRE SISTEM]*.

4.4.2.2 Marcarea şi etichetarea mediilor de stocare

126. Mediile de stocare se înregistrează şi se marchează înainte de utilizare în mod corespunzător, un model de etichetă de marcare fiind prezentată în *Anexa 20 - Sigilii şi etichete aplicate în SIC [DENUMIRE SISTEM]*.

127. În locaţia *SIC [DENUMIRE SISTEM]* este interzisă vehicularea mediilor de stocare care nu sunt luate în evidenţă şi marcate corespunzător.

4.4.2.3 Declasificarea / distrugerea mediilor de stocare

-reutilizarea/reclasificarea şi declasificarea mediilor de stocare se realizează în conformitate cu prevederile Ghidului INFOSEC privind reutilizarea, reclasificarea şi declasificarea mediilor de stocare ale calculatoarelor - DS14.

128. În cadrul *SIC [DENUMIRE SISTEM]* mediile de stocare sunt declasificate sau distruse conform normelor în vigoare, în urma operaţiei efectuându-se şi actualizarea corespunzătoare a registrelor de evidenţă.

4.4.2.4 Transferul de date prin intermediul mediilor de stocare

129. În cadrul *SIC [DENUMIRE SISTEM]* transferul datelor în/din SIC se realizează astfel:

-se va completa conform regulilor stabilite la nivelul instituţiei. Se vor avea în vedere necesitatea verificării antivirus şi existenţa unei aprobări a conducerii instituţiei privind introducerea/extragerea datelor clasificate din cadrul SIC (ex: Transferul datelor între SIC [DENUMIRE SISTEM] şi alte SIC sau alţi suporţi de memorie externă se realizează prin intermediul mediilor de stocare externe dedicate acestui scop. Atât la introducerea cât şi la extragerea datelor în/din SIC [DENUMIRE SISTEM] se va efectua controlul antivirus iar în cazul în care nu se generează alerte în acest sens se procedează la transferarea datelor şi se consemnează această activitate în Anexa 14- Registrul de intervenţii hardware şi software. Evidenţa operaţiilor de transfer se asigură automat prin activarea mecanismelor specifice de auditare şi control acces....etc.)

4.4.3 Proceduri referitoare la echipamentele şi dispozitivele electronice proprietate privată

130. Este interzisă utilizarea echipamentelor de calcul, mediilor de stocare şi a altor dispozitive electronice, proprietate privată, care pot stoca, procesa sau transmite informaţii clasificate.

4.4.4 Proceduri privind utilizarea echipamentelor de tip imprimantă / scaner / fax / copiator

131. În cadrul *SIC [DENUMIRE SISTEM]* sunt utilizate ___ (se va specifica numărul echipamentelor din acest tip din componenţa SIC [DENUMIRE SISTEM] imprimante/scaner/fax/copiator) ale căror caracteristici, mod de conectare şi amplasare se regăsesc în *Anexa 6 - Lista componentelor aparţinând SIC [DENUMIRE SISTEM]* respectiv în *Anexa 1 - Schema de dispunere a SIC [DENUMIRE SISTEM].*

132. Au fost instituite următoarele măsuri de securitate_____

-se vor descrie efectiv măsurile implementate în cadrul SIC [DENUMIRE SISTEM]. (ex: a fost instituit un registru de listare/copiere/scanare/multiplicare, pentru fiecare echipament (raportat la funcţiile activate/operaţiile ce pot fi efectuate cu fiecare echipament). Evenimentele legate de listare/copiere/scanare sunt auditate (se va specifica efectiv modalitatea de auditare, perioada de analiză a fişierelor de audit, perioada de păstrare a acestora, persoana ce are în responsabilitate verificările operaţiilor prin compararea înregistrărilor din registrul specific şi fişierul de audit corespunzător).

4.5 INFOSEC

-în acest capitol se vor descrie procedurile de securitate referitoare la utilizarea calculatoarelor în cadrul locaţiei SIC.

133. Protecţia informaţiilor clasificate, stocate, prelucrate sau transmise prin sisteme informatice şi de comunicaţii (INFOSEC) reprezintă ansamblul structurilor de protecţie şi măsurilor întreprinse împotriva ameninţărilor şi a oricăror acţiuni care pot aduce atingere confidenţialităţii, integrităţii, disponibilităţii, autenticităţii şi nerepudierii informaţiilor clasificate şi/sau pot afecta funcţionarea sistemelor informatice, indiferent dacă acestea apar accidental sau intenţionat.

134. Componentele hardware şi software ale *SIC [DENUMIRE SISTEM]* şi mecanismele de identificare şi autentificare ale utilizatorilor asigură împreună un sistem de control combinat al securităţii.

4.5.1 Securitatea hardware

-se vor prezenta detalii cu privire la implementarea măsurilor de securitate hardware, care se referă la caracteristicile de securitate asigurate de către componentele fizice ale SIC. Se vor avea în vedere aspecte prezentate în art. 24 din Ghidul privind structura şi conţinutul Procedurilor Operaţionale de Securitate (PrOpSec) pentru sisteme informatice şi de comunicaţii - DS 2. (ex: Toţi utilizatorii sistemului sunt obligaţi să cunoască şi să respecte procedurile de pornire-oprire a echipamentelor SIC [DENUMIRE SISTEM] la care au acces conform atribuţiilor funcţionale aşa cum sunt specificate în documentaţia tehnică a acestora. Orice defecţiune apărută este adusă imediat la cunoştinţa administratorului de securitate. La terminarea programului de lucru, înainte de a pleca din încăpere utilizatorii sunt obligaţi să verifice dacă au oprit şi au deconectat de la reţeaua de alimentare staţiile de lucru pe care le exploatează. Administratorul de sistem răspunde de instalarea corectă, întreţinerea şi modificarea setărilor componentelor hardware. Acesta răspunde de sigilarea carcaselor tuturor echipamentelor de calcul din locaţia SIC şi verificarea periodica a integrităţii sigiliilor. Aplicarea sigiliilor se face conform normelor interne cu ajutorul etichetelor de securitate stabilite la nivelul instituţiei şi se consemnează în Anexa 14 - Registrul de intervenţii hardware şi software. Este interzisă îndepărtarea sau deteriorarea de către utilizatori a sigiliilor aplicate pe carcasele staţiilor de lucru pe care le exploatează. În cazul constatării lipsei sau deteriorării sigiliului, utilizatorul este obligat să informeze imediat administratorul de securitate al SIC. În Anexa 20 - Sigilii şi etichete sunt prezentate modele ale sigiliilor şi etichetelor utilizate în cadrul SIC [DENUMIRE SISTEM]. Este interzisă mutarea elementelor sistemului din încăperile în care acestea au fost instalate, fără aprobarea administratorului de securitate al SIC [DENUMIRE SISTEM]. Este interzisă introducerea sau utilizarea de tehnică de calcul, echipamente periferice sau componente hardware proprietate personală sau privată în locaţia SIC [DENUMIRE SISTEM]. Lucrările de întreţinere sau reparaţie sunt efectuate numai de către personal autorizat care posedă autorizaţie de acces. Pe durata efectuării lucrărilor, administratorul de securitate al SIC ia toate măsurile necesare pentru asigurarea securităţii informaţiilor conţinute de mediile de stocare.)

4.5.2 Securitatea software

-se vor prezenta detalii cu privire la implementarea măsurilor de securitate software care se referă la caracteristicile de securitate asigurate de componentele firmware, sistemul de operare, sisteme de gestiune a bazelor de date, programe utilitare şi programe de aplicaţie. Se vor avea în vedere aspecte ale securităţii software prezentate în art. 25 din Ghidul privind structura şi conţinutul Procedurilor Operaţionale de Securitate (PrOpSec) pentru sisteme informatice şi de comunicaţii - DS 2.

135. Aplicaţiile software folosite în cadrul *SIC [DENUMIRE SISTEM]* sunt detaliate în *Anexa 6 - Lista componentelor aparţinând SIC [DENUMIRE SISTEM]*.

136. Este interzisă introducerea, instalarea şi utilizarea altui sistem de operare sau a oricăror altor aplicaţii software în afara celor aprobate pentru utilizare în cadrul *SIC [DENUMIRE SISTEM]*. La alegerea produselor software de securitate ce vor fi instalate se vor avea în vedere *Ghidul INFOSEC privind estimarea nivelurilor de încredere pentru medii specifice în care operează Sisteme Informatice şi de Comunicaţii - DS 13* respectiv

Directiva privind catalogul naţional cu pachete, produse şi profile de protecţie INFOSEC - INFOSEC 5.

137. Instalarea/modificarea/actualizarea componentelor software utilizate în cadrul *SIC [DENUMIRE SISTEM]* poate fi făcută numai de către administratorul de sistem conform procedurilor aprobate.

138. În cazul constatării nefuncţionării sau funcţionării anormale a sistemului de operare sau a unor aplicaţii software, utilizatorii vor anunţa imediat administratorul de sistem al *SIC [DENUMIRE SISTEM]*, fără a întreprinde din proprie iniţiativă nici o altă acţiune asupra echipamentului.

4.5.3 Identificarea utilizatorilor

139. Administratorul de securitate al *SIC [DENUMIRE SISTEM]* avizează atribuirea conturilor de utilizator şi ţine evidenţa nominală, intr-un tabel centralizator, a utilizatorilor şi a conturilor aferente.

140. Accesul utilizatorilor la resursele *SIC [DENUMIRE SISTEM]* se realizează prin intermediul contului de utilizator şi al parolei, pe care sistemul de operare le verifică la conectare. Pe staţia de lucru sunt definite conturile administratorilor desemnaţi ai SIC [DENUMIRE SISTEM] / înlocuitorii acestora şi conturile utilizatorilor autorizaţi *(se vor preciza toate conturile asociate administratorilor/utilizatorilor prezentată în Anexa 8 - Lista personalului autorizat cu acces la SIC [DENUMIRE SISTEM])*. Conturile persoanelor care si-au pierdut calitatea de administrator/utilizator al *SIC [DENUMIRE SISTEM]* vor fi dezactivate.

141. Administratorul de sistem creează/modifică contul şi acordă drepturile utilizatorului în *SIC [DENUMIRE SISTEM]*, în conformitate cu cererea aprobată.

4.5.4 Autentificarea utilizatorilor

*-în acest capitol se vor prezenta măsurile referitoare la autentificare, efectiv implementate în SIC [DENUMIRE SISTEM]. Se vor detalia existenţa mai multor niveluri de acces (alocare parolă BIOS, alocare parolă Windows), stabilirea modului de accesare a BIOS-ului (cu drepturi de administrare/utilizare), definirea unei parole iniţiale la nivelul sistemului de operare pentru utilizatori şi obligativitatea acestora de a o schimba după prima conectare, condiţii pe care trebuie să le îndeplinească parola, modul de gestionare şi evidenţă a parolelor, responsabilităţi ale administratorilor/ utilizatorilor. Un capitol dedicat managementului parolelor este cuprins în cadrul Ghidului general de securitate a sistemelor informatice şi de comunicaţii - DS 5. (ex: sistemul de operare utilizat în SIC [DENUMIRE SISTEM] verifică autenticitatea parolelor de utilizator. Administratorul de sistem alocă fiecărui utilizator nou o parolă temporară. La prima sesiune de lucru utilizatorul accesează calculatorul prin folosirea parolei temporare pe care apoi o va schimba cu parola personală. Parola de acces este memorată de către utilizator, fiind interzisă notarea acesteia sub orice formă (pe hârtie, în memoria telefonului personal, în memoria agendelor electronice, în fişiere stocate pe suporţi de memorie). Este interzisă comunicarea parolei de acces unei terţe părţi, inclusiv administratorilor sistemului. Administratorul de sistem este obligat să stabilească o parola de administrare BIOS pentru staţia de lucru din cadrul SIC [DENUMIRE SISTEM] alături de înlocuitorul acestuia sunt singurele persoane care pot efectua modificări la configuraţia BIOS. Acesta va dezactiva din BIOS toate celelalte posibilităţi de iniţializare a secvenţei de boot în afara celei de pe partiţia pe care este instalat sistemul de operare. Utilizatorul stabileşte şi setează parola de BIOS de pornire a staţiei de lucru din cadrul SIC [DENUMIRE SISTEM]. În situaţia în care staţia de lucru este folosita în comun de mai mulţi utilizatori, aceştia folosesc aceeaşi parola de BIOS de pornire. Parolele de administrare de BIOS şi parolele de BIOS de pornire a staţiilor de lucru se schimbă ori de câte ori este nevoie de către administratorul de sistem, respectiv de utilizatorii staţiei. Parolele de autentificare la nivelul sistemului de operare ale utilizatorilor vor avea o lungime de **minim 9 caractere**, se schimbă la expirarea termenului de valabilitate de **180 de zile** şi ori de câte ori este nevoie de către utilizatori. Sistemul de operare avertizează automat utilizatorul la expirarea perioadei de valabilitate a parolei, solicitându-i acestuia să introducă noua parolă. Se va stabili unu istoric al parolelor de **24** şi se va **activa opţiunea de complexitate** a parolelor. Dacă utilizatorul nu va schimba parola, sistemul de operare va bloca accesul utilizatorului la calculator şi numai un administrator de sistem al SIC va putea debloca contul blocat. Administratorul de sistem blochează contul unui utilizator în următoarele situaţii:atunci când este înştiinţat oficial de către administratorul de securitate că un utilizator nu mai are dreptul*

permanent sau temporar să utilizeze resursele sistemului; atunci când este înştiinţat oficial de către administratorul de securitate ca autorizaţia de securitate a fost retrasă ca urmare a unor măsuri administrative sau a expirării perioadei de valabilitate a acesteia; atunci când este înştiinţat oficial de către administratorul de securitate că este posibil că din anumite motive un utilizator poate intenţiona să aducă prejudicii instituţiei sau altor persoane care îşi desfăşoară activitatea în cadrul instituţiei. Administratorul de sistem păstrează parola de administrare de BIOS într-un plic sigilat în dulapul metalic aprobat aflat în camera nr. __. Plicul în care se păstrează parola de administrare de BIOS şi/sau alte parole de administrare ale SIC [DENUMIRE SISTEM], este un document clasificat şi se gestionează în conformitate cu prevederile legale.

4.5.5 Copiile de siguranţă

-se va prezenta procedura de efectuare a copiilor de siguranţă. Această procedură va cuprinde detalii despre: personalul autorizat să realizeze/să valorifice copiile de siguranţă, produsul software utilizat, tipul de backup efectuat (integral/incremental/diferenţial), frecvenţa cu care se efectuează, conţinutul pe scurt al tipurilor de date ce vor face obiectul efectuării copiilor de siguranţă (log-uri ale sistemului de operare, ale produsului antivirus, documente, etc.), suporţii de memorie pe care se vor stoca aceste copii, locaţia unde se vor păstra, modalitatea de restaurare a datelor la nevoie, etc.

142. Realizarea copiilor de siguranţă este evidenţiată în registrul constituit în acest sens - *Anexa 21 - Registrul de evidenţă a copiilor de siguranţă din cadrul SIC [DENUMIRE SISTEM].*

4.5.6 Erori de sistem / continuarea activităţii în situaţii de urgenţă

-se va specifica modalitatea de acţiune şi de remediere în cazul în care SIC [DENUMIRE SISTEM] devine nefuncţional, inclusiv în cazul producerii incendiilor, inundaţiilor, exploziilor precum şi în cazul calamităţilor naturale dar şi procedurile pentru reluarea sau continuarea activităţii în cadrul SIC [DENUMIRE SISTEM]. Prin planificarea acestor măsuri sunt atribuite responsabilităţi şi sarcini specifice pentru asigurarea protecţiei personalului şi a datelor, echipamentelor şi facilităţilor de o importanţă vitală pentru misiunea SIC [DENUMIRE SISTEM]. (ex: SIC [DENUMIRE SISTEM] este prevăzut cu o staţie de rezervă. Această staţie este configurată şi actualizată la zi, astfel încât în situaţia în care staţia de lucru de bază se defectează, aceasta să poată fi înlocuită până la depanare, cu staţia de rezervă. În cazul în care se constată o defecţiune şi la staţia de rezervă, atunci administratorul de sistem va proceda la configurarea în regim de urgenţă a unui alt echipament disponibil, utilizând copiile de tip imagine a sistemului de operare şi software-ului instalat, respectiv copiile de siguranţă ale datelor salvate pe suporţi de memorie dedicaţi în acest sens, conform procedurii descrise la Capitolul 4.5.5. - Copiile de siguranţă).

4.5.7 Protecţia antivirus

-se va prezenta un sumar al tuturor procedurilor şi mecanismelor de protecţie împotriva software-ului maliţios şi responsabilităţile individuale relevante pentru SIC. (ex: proceduri de verificare privind prezenţa viruşilor sau a altui software maliţios a sistemelor de operare instalate, a pachetelor software şi a programelor utilitare, proceduri pentru ştergerea acestora în cazul detectării lor, pentru verificarea mediilor de stocare primite din surse externe şi dezinfectarea acestora, pentru raportarea incidentelor cauzate de viruşi.). Detalii referitoare la protecţia antivirus sunt prezentate în cadrul Ghidului INFOSEC tehnic şi de implementare pentru protejarea sistemelor informatice şi de comunicaţii împotriva programelor informatice nocive – DS 9 iar aspecte privind modul de abordare în cadrul documentaţiei se regăsesc la art. 26 din Ghidul privind structura şi conţinutul Procedurilor Operaţionale de Securitate (PrOpSec) pentru sisteme informatice şi de comunicaţii - DS 2.

143. Soluţia de protecţie antivirus instalată pe *SIC [DENUMIRE SISTEM]* este prezentată în *Anexa 6 - Lista componentelor aparţinând SIC [DENUMIRE SISTEM]* şi are activate următoarele funcţii: _____

-se vor preciza concret funcţiile activate ale programului antivirus. (ex: programul antivirus se lansează automat la pornirea calculatorului şi rămâne rezident în memorie cu posibilitatea verificării automate a conţinutului suporţilor de memorie la introducerea acestora în dispozitivele de citire (dacă acestea nu au fost dezactivate), programul efectuează automat o scanare antivirus completă a tuturor partiţiilor hard-disk-ului calculatorului, săptămânal, la prima pornire a calculatorului, raportul cu rezultatul scanării este scris automat, prin adăugare în fişierul de audit al programului antivirus, etc.)

144. Administratorul _____*(se va specifica funcţia de administrare desemnată să asigure protecţia antivirus al SIC [DENUMIRE SISTEM])* va realiza actualizarea bazei de date cu semnături a produsului antivirus ori de câte ori este necesar, dar cel puţin _____ *(se va specifica intervalul (zilnic/săptămânal/lunar/trimestrial/etc.) la care se realizează actualizarea în funcţie de volumul şi frecvenţa activităţilor de transfer)*.

145. Actualizarea bazei de date cu semnături a produsului antivirus se realizeză astfel _____ *(se va preciza concret procedura de actualizare a bazei de date cu semnături a produsului antivirus pornind de la menţionarea echipamentelor utilizate pentru descărcarea update-urilor de pe site-urile producătorilor, suporţii de memorie utilizaţi la transferul acestora, eventualele echipamente intermediare pe care se poate realiza testarea bunei funcţionări a fişierelor de update descărcate, până la modul de instalare/configurare a acestora pe SIC [DENUMIRE SISTEM)*.

146. Este interzisă instalarea de către utilizatori a oricărui alt software de protecţie antivirus sau modificarea de către aceştia a setărilor stabilite şi activate la nivelul *SIC [DENUMIRE SISTEM]*.

147. Utilizatorii *SIC [DENUMIRE SISTEM]* sunt obligaţi să nu întrerupă executarea proceselor de scanare antivirus, iar în cazul semnalării unor alerte sau a unor suspiciuni de existenţă a unui virus sau software maliţios aceştia vor anunţa imediat administratorul de sistem *SIC [DENUMIRE SISTEM]*, fără a întreprinde din proprie iniţiativă nici o altă acţiune asupra echipamentului.

4.5.8 Managementul şi auditul securităţii

-se vor prezenta procedurile de management al securităţii, procedurile de audit, precum şi alocarea responsabilităţilor relevante pentru SIC [DENUMIRE SISTEM]. Detalii referitoare la aceste proceduri sunt cuprinse în art. 27 din Ghidul privind structura şi conţinutul Procedurilor Operaţionale de Securitate (PrOpSec) pentru sisteme informatice şi de comunicaţii - DS 2. (ex: La nivelul SIC [DENUMIRE SISTEM] sunt activate opţiunile referitoare la managementul şi auditul automat al securităţii oferite de sistemul de operare. Auditul securităţii asigură înregistrarea acţiunilor desfăşurate de utilizatori şi a proceselor care au fost executate de către aceştia pe staţia de lucru. Rapoartele de audit sunt analizate la un interval de __ sau ori de câte ori este necesar, de către administratorul de sistem. Rapoartele de audit ale sistemului de operare furnizează următoarele informaţii: tipul evenimentului,data şi ora producerii evenimentului, încercările nereuşite de deschidere a unei sesiuni de lucru şi contul de utilizator unde au fost efectuate aceste încercări, închiderea anormală a unei sesiuni de lucru,alte evenimente. Ceasul staţiei de lucru va fi setat şi verificat permanent de administratorul de sistem. Administratorul de sistem al SIC [DENUMIRE SISTEM] efectuează şi păstrează copii ale fişierelor de audit. Înregistrările de audit ale sistemului de operare nu se şterg decât după ce au fost salvate).

4.6 Managementul configuraţiei

-se vor preciza concret aspecte privind managementul configuraţiei SIC [DENUMIRE SISTEM], ce includ identificarea, controlul, păstrarea evidenţei, diseminarea şi auditul tuturor modificărilor efectuate în timpul etapelor de proiectare, dezvoltare, exploatare şi întreţinere pe întreg ciclul de viaţă al SIC [DENUMIRE SISTEM]. Detalii referitoare la managementul configuraţiei se regăsesc în art. 32 din Ghidul privind structura şi conţinutul Procedurilor Operaţionale de Securitate (PrOpSec) pentru sisteme informatice şi de comunicaţii - DS 2.

148. **Administratorul de sistem** al *SIC [DENUMIRE SISTEM]* răspunde de respectarea procedurilor de management al configuraţiei, care constau în identificarea, controlul, păstrarea evidenţei şi auditul tuturor modificărilor efectuate în configuraţiile hardware şi software ale sistemului.

149. Orice modificări sau suspiciuni privind modificarea configuraţiilor hardware sau software ale echipamentelor utilizate, trebuie aduse imediat la cunoştinţa persoanelor cu atribuţii în administrarea *SIC [DENUMIRE SISTEM]*.

150. Conducătorul unităţii care gestionează informaţii clasificate este obligat să asigure respectarea normelor interne de aplicare a măsurilor privind protecţia informaţiilor clasificate în toate componentele acesteia.*(conform art. 86 din Standardele naţionale de protecţie a informaţiilor clasificate în România aprobate prin HG 585/2002 coroborat cu art. 1 din HG 781/2002 privind protecţia informaţiilor clasificate secrete de serviciu).*

-în continuare se vor preciza concret aspecte privind activităţile întreprinse în vederea asigurării managementului configuraţiei la nivelul SIC [DENUMIRE SISTEM]. (ex: Structura de securitate/funcţionarul de securitate din cadrul instituţiei are obligativitatea realizării controalelor periodice privind menţinerea permanentă a măsurilor de securitate aprobate prin documentaţia de acreditare a SIC [DENUMIRE SISTEM] prin efectuarea următoarelor activităţi: verificarea integrităţii etichetelor autoadezive de securitate aplicate pe carcasa echipamentelor aparţinând SIC [DENUMIRE SISTEM], verificarea implementării mecanismelor de restricţionare a accesului utilizatorilor în BIOS şi la nivelul sistemului de operare, verificarea activării, funcţionării corespunzătoare şi actualizării periodice a aplicaţiei de control antivirus, verificarea periodică a modului de efectuare a transferurilor de date în/din SIC [DENUMIRE SISTEM], menţinerea măsurilor de securitate fizică la nivelul MSL, organizarea activităţii de pregătire specifică a persoanelor care au acces la informaţii clasificate, care să includă şi problematică specifică domeniului INFOSEC, etc.).

DOCUMENTE DE REFERINŢĂ

1. *Legea nr. 182 din 12.04.2002 privind protecţia informaţiilor clasificate;*
2. *Legea nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor;*
3. *Hotărârea Guvernului României nr. 585 din 13.06.2002 pentru aprobarea Standardelor naţionale de protecţie a informaţiilor clasificate în România;*
4. *Hotărârea Guvernului României nr. 781 din 25.07.2002 privind protecţia informaţiilor secret de serviciu;*
5. *Directiva privind structurile cu responsabilităţi în domeniul INFOSEC – INFOSEC 1;*
6. *Directiva principală privind domeniul INFOSEC - INFOSEC 2;*
7. *Directiva INFOSEC privind Catalogul naţional cu pachete, produse şi profile de protecţie INFOSEC – INFOSEC 5;*
8. *Ghid pentru elaborarea documentaţiei cu cerinţele de securitate (DCS) pentru sisteme informatice şi de comunicaţii (SIC) – DS 1;*
9. *Ghid privind structura şi conţinutul Procedurilor Operaţionale de Securitate (PrOpSec) pentru sisteme informatice şi de comunicaţii – DS 2;*
10. *Metodologie privind Managementul Riscului de Securitate pentru sistemele informatice şi de comunicaţii care stochează, procesează sau transmit informaţii clasificate– DS 3;*
11. *Ghid INFOSEC privind analiza naturii şi proporţiilor ameninţărilor şi vulnerabilităţilor la adresa sistemelor informatice şi de comunicaţii (SIC) – DS 4;*
12. *Ghid general de securitate a sistemelor informatice şi de comunicaţii - DS 5;*
13. *Ghid INFOSEC tehnic şi de implementare pentru protejarea sistemelor informatice şi de comunicaţii împotriva programelor informatice nocive – DS 9;*
14. *Ghid INFOSEC tehnic şi de implementare privind identificarea şi autentificarea în sistemele informatice şi de comunicaţii care vehiculează informaţii clasificate – DS 11;*
15. *Ghid INFOSEC privind estimarea nivelurilor de încredere pentru medii specifice în care operează sisteme informatice şi de comunicaţii – DS 13;*
16. *Ghid INFOSEC privind reutilizarea, reclasificarea şi declasificarea mediilor de stocare ale calculatoarelor - DS14;*