Guvernul României

ORDIN Nr. 1.323
din 9 noiembrie 2020

pentru aprobarea Normelor tehnice privind cerinţele minime de asigurare a securităţii reţelelor şi sistemelor informatice aplicabile operatorilor de servicii esenţiale

Publicat în: Monitorul Oficial Nr. 1.142 din 26 noiembrie 2020

Având în vedere dispoziţiile art. 20 lit. b) şi s) şi ale art. 25 alin. (1) şi (3) din Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, cu modificările şi completările ulterioare,

în temeiul art. 7 alin. (6) din Hotărârea Guvernului nr. 137/2020 privind organizarea, funcţionarea şi atribuţiile unor structuri din cadrul aparatului de lucru al Guvernului,

secretarul general al Guvernului emite prezentul ordin.

Art. 1 - Se aprobă Normele tehnice privind cerinţele minime de asigurare a securităţii reţelelor şi sistemelor informatice aplicabile operatorilor de servicii esenţiale, prevăzute în anexa care face parte integrantă din prezentul ordin.

Art. 2 - În vederea îndeplinirii termenului de conformare de 6 luni prevăzut la art. 10 alin. (4) din Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, cu modificările şi completările ulterioare, operatorii de servicii esenţiale aplică normele tehnice privind cerinţele minime de asigurare a securităţii reţelelor şi sistemelor informatice aplicabile operatorilor de servicii esenţiale.

Art. 3 - În aplicarea art. 32 alin. (5) din Legea nr. 362/2018, cu modificările şi completările ulterioare, se va ţine seama de Normele tehnice privind cerinţele minime de asigurare a securităţii reţelelor şi sistemelor informatice aplicabile operatorilor de servicii esenţiale, prevăzute la art. 1.

Art. 4 - Prezentul ordin se publică în Monitorul Oficial al României, Partea I.

Secretarul general al Guvernului,
Antonel Tănase

Anexă

NORME TEHNICE
privind cerinţele minime de asigurare a securităţii reţelelor şi sistemelor informatice aplicabile operatorilor de servicii esenţiale

Cap. I
Dispoziţii generale

Art. 1 - Aplicabilitate

Prezentele norme tehnice privind cerinţele minime de asigurare a securităţii reţelelor şi sistemelor informatice, denumite în continuare ***norme,*** sunt aplicabile operatorilor de servicii esenţiale şi au ca obiect asigurarea unui nivel comun de securitate a reţelelor şi sistemelor informatice.

Art. 2 - Termeni, abrevieri şi domenii de securitate

(1) În stabilirea cerinţelor minime de asigurare a securităţii reţelelor şi sistemelor informatice se utilizează următoarele domenii de securitate:

1. guvernanţă - obiectivele domeniului sunt: elaborarea şi implementarea politicilor de securitate la nivelul organizaţional; angajamentul managementului de nivel înalt al organizaţiei în asigurarea sistemului de management al securităţii informaţiei; gestionarea managementului riscurilor privind ameninţările, vulnerabilităţile şi riscurile identificate;

2. protecţie - obiectivele domeniului sunt: asigurarea securităţii reţelelor şi sistemelor informatice, securitatea fizică şi a persoanei; administrarea şi mentenanţa resurselor reţelelor şi sistemelor informatice; controlul accesului la elementele/componentele reţelelor şi sistemelor informatice;

3. apărare cibernetică - obiectivele domeniului sunt: asigurarea managementului incidentelor de securitate; detectarea şi tratarea incidentelor de securitate care afectează securitatea reţelelor şi sistemelor informatice;

4. reziliență - obiectivele domeniului sunt: managementul continuităţii serviciilor esenţiale furnizate; gestionarea situaţiilor de criză, în special a incidentelor de securitate care au un impact major asupra serviciilor esenţiale.

(2) Termenii şi abrevierile utilizate în prezentele norme tehnice sunt prevăzute în anexa nr. 1.

(3) Domeniile de securitate se împart, la rândul lor, în categorii de activităţi de securitate, iar pentru fiecare dintre acestea sunt stabilite măsuri de securitate cu una sau mai multe cerinţe de securitate, care, la rândul lor, conţin indicatori de control.

(4) În procesul de implementare a cerinţelor de securitate, OSE identifică riscurile privind neimplementarea, planifică activităţile care stau la baza implementării şi stabileşte responsabilii pentru realizarea acestora.

Cap. II
Guvernanţă [A]

Secţiunea 1
Managementul securităţii informaţiei [A1]

Art. 3 - Analizarea şi evaluarea riscurilor [A11]

(1) Cerinţe de securitate

[A111]. Analiza riscurilor de securitate. OSE efectuează şi actualizează periodic o analiză a riscurilor de securitate a reţelelor şi sistemelor informatice care asigură furnizarea serviciilor esenţiale, identificând sistemele/echipamentele informatice critice care stau la baza furnizării serviciului esenţial şi principalele riscuri.

[A112]. Gestionarea riscurilor de securitate. Pentru aplicarea procesului de analiză şi evaluare a riscurilor, OSE stabileşte o metodologie de gestionare a riscurilor furnizării serviciilor esenţiale care va reflecta procesul de evaluare a riscurilor operatorului economic, criteriile de analiză, de acceptare şi de reducere a riscurilor.

[A113]. Evaluarea riscurilor de securitate. Rezultatul evaluării riscurilor va fi documentat în registrul de risc organizaţional.

1. În procesul de evaluare a riscurilor, OSE va avea în vedere cel puţin:

- noile ameninţări în domeniul securităţii cibernetice;
- punctele slabe descoperite recent;
- pierderea eficacităţii măsurilor de securitate;
- modificările situaţiei de risc cauzate de modificările arhitecturii reţelelor şi sistemelor informatice;

- orice alte modificări ale situaţiei de risc.

(2) Indicatori de control. ARNIS; MEGRE; RERO.

Art. 4 - Realizarea planurilor de securitate. Politica de securitate [A12]

(1) Cerinţe de securitate

[A121]. Politica de securitate. Pornind de la ARNIS, OSE elaborează, menţine şi implementează o politică de securitate a reţelelor şi sistemelor informatice care asigură furnizarea serviciilor esenţiale şi un sistem de management al securităţii informaţiilor.

1. PONIS stabileşte obiectivele strategice de securitate, descrie guvernanţa securităţii şi reflectă toate politicile specifice de securitate ale SMSI (procesul de acreditare de securitate, audit de securitate, criptografie, întreţinere securitate, manipulare incidente etc.).

[A122]. Implementarea politicii de securitate. OSE întocmeşte în beneficiul managementului său, cel puţin anual, un raport privind implementarea PONIS şi a documentelor de aplicare a acesteia.

1. Raportul specifică inventarul riscurilor, nivelul securităţii reţelelor şi sistemelor informatice şi acţiunile de securitate planificate şi realizate.

(2) Indicatori de control. PONIS; SMSI; RAIPOD.

Art. 5 - Acreditarea de securitate [A13]

(1) Cerinţe de securitate

[A131]. Acreditarea reţelelor şi sistemelor informatice. În baza ARNIS şi în conformitate cu procesul de acreditare stabilit în PONIS, OSE acreditează reţelele şi sistemele informatice, inclusiv componentele de administrare.

1. Acreditarea de securitate este o decizie formală luată de managementul de nivel înalt al OSE prin care se certifică procesul de identificare a riscurilor care afectează securitatea şi modul de implementare a măsurilor necesare pentru protejare şi are valabilitate de cel mult un an. Decizia certifică, de asemenea, faptul că orice risc rezidual a fost identificat şi acceptat la nivel managerial.

2. Decizia de acreditare de securitate are la bază mapa de acreditare de securitate care cuprinde următoarele documente/mijloace:

- analiză riscuri şi obiective de securitate;
- proceduri şi măsuri de securitate aplicate;
- rapoarte de audit de securitate;
- rapoarte de evaluare a conformităţii;
- riscuri reziduale şi motive care justifică acceptarea acestora.

[A132]. Revizuirea validării acreditării de securitate. Anual şi ori de câte ori se identifică un eveniment/proces de dezvoltare care modifică contextul descris în procesul de acreditare sau de fiecare dată când se modifică în mod semnificativ configuraţia reţelelor şi sistemelor informatice sau a aplicaţiilor, OSE va revizui validarea acreditării de securitate. OSE are obligaţia reînnoirii aprobării imediat ce nu mai este valabilă.

(2) Indicatori de control. PEANIS; DANIS; MANIS.

Art. 6 - Indicatori de securitate [A14]

(1) Cerinţe de securitate

[A141]. Indicatori de securitate. OSE stabileşte o serie de indicatori de evaluare, pe baza cărora îşi evaluează conformitatea cu PONIS.

1. Indicatorii de securitate se pot referi la: performanţele gestionării riscurilor; menţinerea resurselor în condiţii sigure; drepturile de acces ale utilizatorilor; autentificarea accesului la resurse; administrarea resurselor.

[A142]. Metode de evaluare a securităţii. OSE specifică pentru fiecare indicator metoda de evaluare folosită şi, dacă este cazul, marja de incertitudine în evaluarea sa.

1. Dacă un indicator se schimbă semnificativ în comparaţie cu evaluarea anterioară, operatorul identifică şi specifică motivele.

(2) Indicatori de control. IEC; MEIEC.

Art. 7 - Verificarea conformităţii cu privire la securitatea informaţiei. Audit de securitate [A15]

(1) Cerinţe de securitate

[A151]. Evaluarea conformităţii. În baza ARNIS, OSE stabileşte şi actualizează periodic procedura privind evaluarea conformităţii SNIS şi efectuarea auditului de securitate a reţelelor şi sistemelor informatice.

1. Activitatea se efectuează anual la nivelul OSE de către structura de securitate sau de o echipă complexă stabilită de managementul de cel mai înalt nivel. Ea se finalizează cu un raport de evaluare a conformităţii.

[A152]. Auditul de securitate. OSE va efectua audit de securitate, cel puţin o dată la 2 ani, şi are ca rezultat un raport de audit de securitate a reţelelor şi sistemelor informatice.

1. Auditul se efectuează numai de auditori de securitate informatică pentru auditarea reţelelor şi sistemelor informatice, atestaţi de ANSRSI şi cu atestat valabil la data finalizării RASNIS.

2. RASNIS va cuprinde auditarea cerinţelor minime specificate la [A16].

(2) Indicatori de control. PRECAS; RAEC; RASNIS.

Art. 8 - Testarea şi evaluarea securităţii reţelelor şi sistemelor informatice [A16]

(1) Cerinţe de securitate

[A161]. Testare şi evaluare securitate. Procesul de testare şi evaluare va implica verificarea sistemelor operaţionale pe baza unei planificări atente astfel încât riscul întreruperii furnizării serviciului esenţial să fie minim şi se finalizează cu un raport de testare şi evaluare a securităţii reţelelor şi sistemelor informatice.

1. Testarea şi evaluarea reţelelor şi sistemelor informatice presupun identificarea şi prevenirea vulnerabilităţilor software şi hardware, respectiv:

- testarea securităţii aplicaţiilor;
- testarea securităţii infrastructurii reţelelor şi sistemelor informatice.

2. Testarea şi evaluarea securităţii reţelelor şi sistemelor informatice vor fi efectuate numai de personal specializat, atestat de către ANSRSI.

3. Rezultatele analizelor tehnice cu privire la compromiterea securităţii efectuate pe parcursul auditărilor pot fi prezentate numai persoanelor care au nevoie de aceste informaţii pentru a-şi îndeplini atribuţiile ce le revin.

(2) Indicatori de control. RATES; ATECNIS.

Art. 9 - Asigurarea securităţii personalului [A17]

(1) Cerinţe de securitate

[A171]. Asigurarea securităţii personalului. OSE elaborează un program de asigurare a securităţii personalului prin care identifică obiective şi stabileşte cerinţe de securitate pentru fiecare etapă a relaţiei avute de către angajaţi.

1. PGASP se materializează prin: fişa postului (FP); contract individual de muncă (CIM); contract colectiv de muncă (CCM).

[A172]. Verificarea înţelegerii responsabilităţilor. OSE se asigură că angajaţii înţeleg responsabilităţile şi sunt potriviţi pentru rolurile stabilite, iar contractanţii şi furnizorii îşi asumă şi angajează întreaga responsabilitate.

1. Materializat prin: instructaje de securitate pentru angajaţi (ISA); verificări privind cunoştinţele de securitate ale angajaţilor (VCSA).

2. În contractele de servicii sau furnizare servicii externe, OSE se asigură că au fost prevăzute clauze privind asigurarea securităţii personalului.

(2) Indicatori de control. PGASP; FP; CIM; CCM; ISA; VCSA; COSE.

Art. 10 - Conştientizarea şi instruirea utilizatorilor [A18]

(1) Cerinţe de securitate

[A181]. Instrumente de conştientizare. OSE pune la dispoziţia angajaţilor instrumente necesare pentru conştientizarea şi educarea acestora cu privire la tipurile de ameninţări de securitate informatică şi măsurile de protecţie corespunzătoare.

[A182]. Instruirea şi prezentarea securităţii. OSE instituie un program de prezentare a securităţii pentru tot personalul, precum şi un program de instruire în domeniul securităţii pentru angajaţii care utilizează reţelele şi sisteme informatice.

(2) Indicatori de control. INCEA; PRASA; PRISA.

Art. 11 - Gestionarea activelor [A19]

(1) Cerinţe de securitate

[A191]. Inventarierea şi gestionarea activelor. OSE stabileşte un cadru adecvat pentru identificarea, clasificarea şi implementarea unui inventar al proceselor IT, sistemelor şi elementelor componente ale reţelelor şi sistemelor informatice. În baza gestionării activelor, OSE lansează actualizări şi patch-uri şi, după caz, stabileşte ce elemente din componenţa reţelelor şi sistemelor informatice sunt afectate de noi probleme de securitate.

1. Pentru identificarea ameninţărilor, vulnerabilităţilor şi riscurilor sunt identificate activele, sistemele şi procesele organizaţiei, care se materializează printr-o listă.

2. OSE elaborează o procedură pentru etichetarea şi clasificarea datelor şi informaţiilor pentru a reflecta sensibilitatea acestora şi, în consecinţă, se asigură că aceasta este respectată, iar datele/informaţiile sunt gestionate corespunzător.

(2) Indicatori de control. LASPO; PRECDI.

Secţiunea a 2-a
Managementul ecosistemului [A2]

Art. 12 - Cartografierea ecosistemului [A21]

(1) Cerinţe de securitate

[A211]. Descrierea ecosistemului. OSE stabileşte o cartografiere a ecosistemului, inclusiv a părţilor interesate interne şi externe, incluzând, dar fără a se limita la furnizori, în special a celor cu acces la sau gestionarea activelor critice ale operatorului.

1. Cartografierea ecosistemului este materializată printr-o situaţie cartografică a ecosistemului.

2. Scopul cartografierii este identificarea şi evaluarea riscurilor potenţiale reprezentate de relaţiile cu părţile interesate ale ecosistemului şi identificată printr-o listă a riscurilor potenţiale identificate şi evaluarea efectului acestora asupra furnizării serviciilor esenţiale.

3. Pentru elaborarea LIRIE, OSE va avea în vedere 4 parametri majori:

- maturitatea. Care sunt capacităţile tehnice ale părţilor interesate cu privire la securitatea cibernetică?
- încrederea. Pot presupune că intenţiile părţilor interesate faţă de mine sunt fiabile?
- nivelul de acces. Care sunt drepturile de acces ale părţilor interesate la reţelele şi sistemele informatice?
- dependenţa. În ce măsură relaţia cu părţile interesate este critică pentru activitatea mea?

(2) Indicatori de control. SICAE; LIRIE.

Art. 13 - Relaţiile ecosistemului [A22]

(1) Cerinţe de securitate

[A221]. Stabilirea relaţiilor ecosistemului. OSE elaborează şi implementează o procedură de stabilire a relaţiilor ecosistemului, care include interconexiunile (relaţiile externe) între reţelele şi sisteme informatice şi terţi. În general, cerinţele de securitate trebuie luate în considerare pentru componentele reţelelor şi sistemelor informatice operate de terţi.

[A222]. Acorduri la nivel de serviciu. OSE se asigură, prin acorduri la nivel de serviciu şi/sau mecanisme de audit, că furnizorii săi stabilesc, de asemenea, măsuri de securitate adecvate. În acest sens elaborează şi păstrează o listă cu acorduri la nivel de serviciu şi/sau mecanisme de audit.

(2) Indicatori de control. PROSRE; LASMA.

Cap. III
Protecţie [B]

Secţiunea 1
Managementul arhitecturii [B1]

Art. 14 - Managementul configuraţiei reţelelor şi sistemelor informatice [B11]

(1) Cerinţe de securitate

[B111]. Arhitectura NIS. OSE elaborează şi actualizează permanent o schemă a arhitecturii reţelelor şi sistemelor informatice.

[B112]. Instalarea echipamentelor şi serviciilor. OSE instalează numai servicii şi funcţionalităţi sau conectează echipamente care sunt esenţiale pentru funcţionarea şi securitatea reţelelor şi sistemelor informatice. Evidenţa serviciilor, funcţionalităţilor şi echipamentelor este evidenţiată în ARNIS.

1. Dacă componentele suplimentare sunt inevitabile (de exemplu, din motive economice), acestea trebuie evaluate în funcţie de analiza riscurilor. Va fi materializat în MANIS.

2. ARNIS va fi actualizată permanent în funcţie de componentele suplimentare implementate la nivelul securităţii reţelelor şi sistemelor informatice.

3. Elementele componente ale reţelelor şi sistemelor informatice trebuie utilizate numai atunci când este nevoie şi cu măsuri de securitate adecvate.

(2) Indicatori de control. SANIS; MANIS; ARNIS.

Art. 15 - Managementul suporţilor de memorie externă [B12]

(1) Cerinţe de securitate

[B121]. Suporţi de memorie externă. OSE va adopta o procedură privind utilizarea suporţilor de memorie externă. Aceasta va cuprinde modul de utilizare, principii şi măsuri de securitate atât pentru dispozitive mobile, cât şi pentru suporturi de memorie externă.

1. Suporturile de scris amovibile conectate la reţelele şi sistemele informatice sunt utilizate exclusiv pentru operaţiuni legate de furnizarea serviciului esenţial şi/sau funcţionarea reţelelor şi sistemelor informatice, inclusiv pentru întreţinerea, administrarea şi asigurarea securităţii reţelelor şi sistemelor informatice.

2. La NIS vor fi conectate numai suporturi amovibile înregistrate, în registre de evidenţă a suporţilor de memorie externă, fiind monitorizat accesul în reţelele şi sistemele informatice.

(2) Indicatori de control. PRUSME; RESME.

Art. 16 - Segregarea şi segmentarea reţelelor şi sistemelor informatice [B13]

(1) Cerinţe de securitate

[B131]. Segregarea şi segmentarea. În vederea limitării propagării incidentelor de securitate cibernetică, OSE aplică o procedură privind segregarea şi segmentarea NIS.

1. OSE separă fizic sau logic reţelele şi sistemele informatice de alte sisteme informatice proprii sau de la terţi. În cazul în care reţelele şi sistemele informatice sunt compuse din subsisteme, OSE le separă din punct de vedere fizic sau logic.

2. OSE stabileşte şi pune în aplicare măsuri de securitate adecvate pentru interconectări ale reţelelor şi sistemelor informatice.

(2) Indicatori de control. PROSES; SANIS.

Art. 17 - Filtrarea traficului [B14]

(1) Cerinţe de securitate

[B141]. Filtrarea fluxurilor. OSE defineşte, implementează şi actualizează permanent procedura privind filtrarea traficului, prin care stabileşte reguli de filtrare a traficului (pe baza adresei de reţea, după numărul portului, pe bază de protocoale de comunicaţii etc.) pentru restrângea fluxurilor de trafic.

1. OSE interzice fluxurile de trafic care nu sunt necesare pentru funcţionarea reţelelor şi sistemelor informatice şi care ar putea facilita un atac cibernetic.

2. OSE filtrează fluxurile de intrare, cele existente şi fluxurile între subsistemele reţelelor şi sistemelor informatice la nivelul interconectării lor, limitând astfel fluxurile numai la cele strict necesare funcţionării şi asigurării securităţii reţelelor şi sistemelor informatice.

(2) Indicatori de control. PROFIT; ARNIS.

Art. 18 - Asigurarea protecţiei produselor şi serviciilor aferente reţelelor şi sistemelor informatice [B15]

(1) Cerinţe de securitate

[B151]. Asigurarea protecţiei criptografice. Pentru a asigura confidenţialitatea, integritatea şi autenticitatea datelor procesate, stocate sau tranzitate prin reţelele şi sistemele informatice, OSE va stabili, implementa şi menţine o procedură pentru asigurarea protecţiei criptografice pentru informaţii şi resurse.

1. Măsurile criptografice se aplică în toate etapele ciclului de viaţă a informaţiei şi au ca obiect de aplicare aplicaţiile, sistemele informatice, echipamentele de reţea şi canalele de comunicare.

[B152]. Managementul cheilor de criptare. OSE va avea în vedere utilizarea, protejarea şi gestionarea cheilor criptografice de-a lungul întregului ciclu de viaţă a acestora.

(2) Indicatori de control. PRAPC; MACC.

Art. 19 - Protecţia împotriva malware [B16]

(1) Cerinţe de securitate

[B161]. Protecţie malware. OSE va stabili măsuri de protecţie malware şi va implementa mijloace de control pentru detecţia, prevenirea şi recuperarea informaţiei în scopul protecţiei împotriva atacurilor malware.

1. În acest sens va elabora şi implementa o procedură pentru asigurarea protecţiei malware, în conformitate cu PONIS.

2. Echipamentele hardware, sistemele de operare, aplicaţiile software şi subsistemele reţelelor şi sistemelor informatice trebuie configurate şi protejate corespunzător atât împotriva atacurilor fizice, cât şi logice.

(2) Indicatori de control. PRAPMA.

Secţiunea a 2-a
Managementul administrării [B2]

Art. 20 - Administrarea conturilor [B21]

(1) Cerinţe de securitate

[B211]. Conturi de administrare. OSE stabileşte conturi de administrare destinate numai persoanelor responsabile de efectuarea operaţiunilor de administrare (instalare, configurare, întreţinere, supraveghere etc.) a resurselor reţelelor şi sistemelor informatice. Lista conturilor de administrare va fi actualizată permanent.

1. Permisiunile administratorilor sunt individualizate şi restricţionate la perimetrul funcţional şi tehnic al fiecărui administrator.

2. Conturile de administrator sunt utilizate numai pentru conectarea la SIA.

3. Operaţiunile de administrare a reţelelor şi sistemelor informatice sunt realizate exclusiv de pe conturile de administrator.

(2) Indicatori de control. LICA.

Art. 21 - Administrarea reţelelor şi sistemelor informatice [B22]

(1) Cerinţe de securitate

[B221]. Utilizarea sistemelor de administrare. OSE stabileşte şi aplică procedura privind utilizarea sistemelor informatice de administrare utilizate pentru operaţiuni de administrare a NIS, respectând cel puţin regulile:

1. Resursele hardware şi software ale SIA sunt utilizate exclusiv pentru efectuarea operaţiunilor de administrare.

- Când motivele tehnice sau organizaţionale o justifică, SIA poate fi utilizată pentru a efectua alte operaţiuni decât cele administrative. În acest caz, trebuie să fie puse în aplicare mecanismele de protecţie a sistemului de operare şi a compartimentării mediilor de lucru, pentru a permite izolarea mediului "utilizator" faţă de "administrator".

2. Mediul de lucru "administrator" folosit pentru operaţiuni de administrare nu trebuie utilizat şi în alte scopuri, cum ar fi accesarea site-urilor web sau a serverelor de e-mail.

3. Un utilizator nu trebuie să se conecteze la SIA prin intermediul unui mediu de lucru "utilizator" pentru alte funcţii decât operaţiuni de administrare a reţelelor şi sistemelor informatice.

4. Fluxurile de date asociate cu alte operaţiuni şi fluxurile de administrare trebuie să fie separate prin mecanisme de criptare şi autentificare, în conformitate cu MS-B15.

5. SIA sunt conectate la resursele reţelelor şi sistemelor informatice printr-o legătură de reţea fizică folosită exclusiv pentru operaţiunile de administrare. Resursele reţelelor şi sistemelor informatice sunt administrate prin interfaţa lor de administrare fizică.

- Când motivele tehnice împiedică administrarea unei resurse a reţelelor şi sistemelor informatice printr-o legătură de reţea fizică sau prin interfaţa de administrare fizică, operatorul pune în aplicare măsuri de reducere a riscurilor, cum ar fi măsuri logice de securitate. În acest caz, descrie aceste măsuri şi justificările acestora în MANIS.

6. Fluxurile de administrare a reţelelor şi sistemelor informatice sunt protejate de mecanisme de criptare şi autentificare, în conformitate cu MS-B15.

- Dacă criptarea şi autentificarea acestor fluxuri nu sunt posibile din motive tehnice, operatorul pune în aplicare măsuri pentru a proteja confidenţialitatea şi integritatea acestor fluxuri şi pentru a consolida controlul şi trasabilitatea operaţiunilor de administrare. În acest caz, descrie aceste măsuri şi justificările acestora în MANIS.

7. Jurnalele care înregistrează evenimentele generate de resursele SIA nu conţin nicio parolă sau alt element secret de autentificare în text simplu sau sub forma unei amprente criptografice.

[B222]. Parole administrare. Nicio parolă, sub formă de text simplu sau hash, nu este scrisă în jurnalele de înregistrare a evenimentelor produse de resursele utilizate pentru administrare şi nu este stocată sub această formă în niciun moment.

1. Evidenţa parolelor de administrare se păstrează, în plic închis şi sigilat [PPSIA], la componenta de securitate sau administrare a reţelelor şi sistemelor informatice.

(2) Indicatori de control. PRUSIA; PONIS; JIERU; PPSIA.

Art. 22 - Managementul accesului de la distanţă [B23]

(1) Cerinţe de securitate

[B231]. Lucrul la distanţă. OSE adoptă o procedură privind lucrul la distanţă, în baza PONIS.

1. PROLD va cuprinde modurile de realizare, măsurile de securitate aferente pentru protejarea resurselor şi a informaţiilor accesate, prelucrate şi stocate din şi în locaţiile în care se lucrează la distanţă.

2. Când furnizarea serviciului esenţial necesită ca reţelele şi sistemele informatice să fie accesibile printr-o reţea publică, operatorul protejează accesul prin intermediul unor mecanisme criptografice, în conformitate cu MS-B15.

(2) Indicatori de control. PROLD; PRAPC.

Secţiunea a 3-a
Managementul identităţii şi accesului [B3]

Art. 23 - Managementul identificării şi autentificării utilizatorilor [B31]

(1) Cerinţe de securitate

[B311]. Identificarea utilizatorilor. Pentru identificare, OSE stabileşte şi ţine evidenţa conturilor unice pentru utilizatori sau pentru procesele automatizate care trebuie să acceseze resursele reţelelor şi sistemelor informatice.

1. Conturile neutilizate sau care nu mai sunt necesare trebuie să fie dezactivate.

2. Se instituie un proces permanent de revizuire şi actualizare a evidenţei conturilor pentru utilizatori şi pentru procesele automatizate.

3. Atunci când acest lucru nu este posibil din motive tehnice sau operaţionale, OSE dezvoltă un set de măsuri de trasabilitate şi reducere a riscurilor şi le descrie în MANIS.

[B312]. Autentificarea utilizatorilor. Pentru autentificare, OSE protejează accesul la resursele NIS pentru utilizatori sau procese automatizate, folosind un mecanism de autentificare. OSE defineşte regulile de gestionare a certificatelor de autentificare la reţelele şi sistemele informatice.

1. Pentru procesele critice, OSE va stabili un mecanism de autentificare în cel puţin doi paşi.

2. OSE trebuie să schimbe datele de autentificare implicite instalate de producătorul/furnizorul unei resurse înainte ca acea resursă să intre în funcţiune. Neglijarea acestui aspect prezintă un risc ridicat pentru securitatea oricărei infrastructuri din care face parte o astfel de resursă sau cu care interacţionează.

(2) Indicatori de control. ECUPA; MANIS; ARNIS; MEAUP.

Art. 24 - Managementul drepturilor de acces [B32]

(1) Cerinţe de securitate

[B321]. Acordarea drepturilor de acces. În baza regulilor stabilite în PONIS, OSE acordă drepturi de acces unui utilizator sau unui proces automat doar atunci când accesul este strict necesar pentru ca utilizatorul să îşi îndeplinească atribuţiile, iar procesul automatizat să îşi desfăşoare operaţiunile tehnice.

1. În acordarea drepturilor de acces, OSE aplică principiul necesităţii de a cunoaşte şi principiul celui mai mic privilegiu.

2. OSE defineşte drepturile de acces la multiplele funcţionalităţi ale reţelelor şi sistemelor informatice şi alocă aceste drepturi de acces strict utilizatorilor/proceselor automatizate care au o necesitate clară.

3. Cel puţin o dată pe an, OSE examinează atribuirea drepturilor de acces, identificând legăturile dintre conturi, drepturile de acces asociate şi resursele sau funcţionalităţile care sunt accesate prin drepturile de acces, şi păstrează actualizată o listă a conturilor privilegiate pe nivele de acces şi funcţionalităţi accesabile.

[B322]. Verificarea conturilor privilegiate. OSE implementează un sistem de verificare a potenţialelor modificări ale unui cont privilegiat, pentru a identifica dacă drepturile de acces la resurse şi funcţionalităţi sunt alocate pe baza principiului celui mai mic privilegiu (sunt acordate doar drepturile strict necesare) şi sunt adecvate cu utilizarea contului.

(2) Indicatori de control. PONIS; LICPA; LICA; SIVMOC.

Secţiunea a 4-a
Managementul mentenanţei [B4]

Art. 25 - Mentenanţa reţelelor şi sistemelor informatice [B41]

(1) Cerinţe de securitate

[B411]. Menţinere securitate. OSE elaborează şi implementează o procedură pentru menţinerea securităţii reţelelor şi sistemelor informatice, în conformitate cu PONIS.

1. În acest scop, procedura:

- defineşte condiţiile care permit menţinerea unui nivel minim de securitate a resurselor;
- descrie politica de instalare a oricărei noi versiuni sau măsuri corective pentru o resursă desemnată;
- obligă informarea cu privire la informaţii despre vulnerabilităţi şi măsuri corective de securitate care privesc resursele reţelelor şi sistemelor informatice (hardware şi software).

[B412]. Actualizare resurse. OSE instalează şi menţine doar versiuni ale resurselor hardware şi software care sunt acceptate de furnizorii sau producătorii lor şi sunt actualizate din punctul de vedere al securităţii.

1. OSE verifică originea şi integritatea versiunii înainte de instalarea acesteia (conform calendarului definit în PROMNIS) şi analizează impactul tehnic şi operaţional al versiunii respective asupra securităţii reţelelor şi sistemelor informatice.

2. În unele cazuri justificate, din motive tehnice sau operaţionale, OSE decide ca pentru anumite resurse să nu instaleze o versiune acceptată de furnizor sau producător. În aceste cazuri, OSE aplică procedura pentru reducerea riscurilor legate de utilizarea unei versiuni învechite, elaborată conform PONIS, şi descrie în MANIS măsurile luate, precum şi motivele care au justificat să nu instaleze versiunea acceptată.

[B413]. Protejare resurse. OSE protejează accesul la resursele reţelelor şi sistemelor informatice atunci când accesul se face din reţele terţe.

1. În acest caz, OSE protejează prin criptare şi mecanisme de autentificare accesul la reţelele şi sistemele informatice, ţine evidenţa echipamentelor utilizate pentru accesarea reţelelor şi sistemelor informatice şi, de asemenea, gestionează şi configurează aceste echipamente.

(2) Indicatori de control. PROMNIS; PRORUVI; PONIS; MANIS; PRAPC.

Art. 26 - Sisteme de control industrial. SCADA - Monitorizare, control şi achiziţii de date [B42]

(1) Cerinţe de securitate

[B421]. Sisteme de control industriale. Multe servicii esenţiale depind de sisteme de control industriale, funcţionale şi sigure. Dacă este cazul, OSE ia în considerare cerinţele de securitate specifice pentru ISC.

1. Abordarea clasică a tehnologiei informaţiei (axată pe transferul şi accesul de/la informaţii) ar putea fi înlocuită cu o abordare tehnologică operaţională (hardware şi software - utilizate pentru detectarea modificării unui proces fizic).

[B422]. Limitarea accesului. Sistemele SCADA folosesc diferite conexiuni combinate, radio, seriale sau modem în funcţie de necesităţi. Pentru amplasamente mari sunt folosite, de asemenea, conexiuni Ethernet şi IP/Sonet.

1. În aceste condiţii, OSE trebuie să identifice şi analizeze riscurile de securitate şi să implementeze măsuri de securitate pentru limitarea accesului neautorizat.

(2) Indicatori de control. CEISC; ANISMS.

Secţiunea a 5-a
Managementul securităţii fizice [B5]

Art. 27 - Asigurarea protecţiei fizice a reţelelor şi sistemelor informatice [B51]

(1) Cerinţe de securitate

[B511]. Acces la resurse. OSE previne accesul fizic neautorizat, deteriorarea şi interferenţa la informaţiile şi facilităţile de procesare a informaţiilor în reţelele şi sistemele informatice.

1. În acest sens, OSE elaborează şi aplică o procedură privind accesul şi securitatea resurselor şi informaţiilor.

(2) Indicatori de control. PRASI

Cap. IV
Apărare cibernetică [C]

Secţiunea 1
Managementul detecţiei [C1]

Art. 28 - Managementul vulnerabilităţilor şi alertelor de securitate [C11]

(1) Cerinţe de securitate

[C111]. Fluxul alertelor de securitate. OSE elaborează, actualizează şi implementează, în conformitate cu PONIS, o procedură pentru detectarea alertelor şi incidentelor de securitate care afectează reţelele şi sistemele informatice.

1. PRODAIS prevede măsuri organizatorice şi tehnice destinate detectării alertelor şi incidentelor de securitate care afectează reţelele şi sistemele informatice.

- Măsurile organizatorice includ procedurile de operare pentru dispozitivele de detectare şi descriu lanţul de procesare pentru evenimentele de securitate identificate de aceste dispozitive.

- Măsurile tehnice specifică natura şi poziţionarea dispozitivelor de detectare.

2. OSE instituie un sistem de detectare a incidentelor şi alertelor de securitate.

- Dispozitivele de detecţie analizează fluxurile de date care tranzitează reţelele şi sistemele informatice pentru a identifica evenimente care ar putea afecta reţelele şi sistemele informatice.

- Atunci când acest lucru nu este posibil din motive tehnice, operatorul descrie în MANIS motivele tehnice care au împiedicat utilizarea dispozitivelor de detecţie.

[C112]. Evaluarea şi monitorizarea vulnerabilităţilor. OSE dezvoltă un proces de identificare, clasificare, remediere şi eliminare a vulnerabilităţilor, în special în software şi firmware.

1. Pentru limitarea riscurilor de securitate şi corectarea vulnerabilităţilor, OSE va implementa un program pentru managementul vulnerabilităţilor, care poate include, fără a se limita la acestea:

- instalarea unui patch;
- modificări în PONIS;
- reconfigurarea unui software (de exemplu, Firewall);
- educarea utilizatorilor despre social engineering.

(2) Indicatori de control. PRODAIS; SIENIS; MANIS; PEIREV; PGMAVU; ARNIS.

Art. 29 - Înregistrarea evenimentelor [C12]

(1) Cerinţe de securitate

[C121]. Monitorizare evenimente. OSE pune în aplicare un sistem de înregistrare evenimente la nivelul reţelelor şi sistemelor informatice pentru evenimente legate de autentificarea utilizatorului, conturilor şi gestionării drepturilor de acces, accesului la resurse, modificărilor regulilor NIS şi funcţionării reţelelor şi sistemelor informatice.

1. SIENIS ajută la detectarea incidentelor de securitate prin colectarea datelor de înregistrare.

2. Evenimentele înregistrate de SIENIS sunt timbrate cu ajutorul surselor de timp sincronizate, centralizate şi arhivate pentru o perioadă de cel puţin şase luni.

3. Formatul de arhivare a evenimentelor permite cercetarea automată a acestor evenimente.

[C122]. Sisteme de management. În vederea apărării cibernetice a securităţii reţelelor şi sistemelor informatice, OSE dezvoltă şi implementează un SIEM (Security Information and Event Management) ca un set de instrumente care combină SEM (gestionarea evenimentelor de securitate) şi SIM (gestionarea informaţiilor de securitate).

(2) Indicatori de control. SIENIS; SIEM.

Art. 30 - Jurnalizarea şi asigurarea trasabilităţii activităţilor în cadrul reţelelor şi sistemelor informatice [C13]

(1) Cerinţe de securitate

[C131]. Jurnalizare şi trasabilitate. OSE pune în aplicare un sistem de corelaţie şi analiză de jurnal care exploatează evenimentele înregistrate de SIENIS, pentru a detecta evenimente susceptibile care afectează securitatea reţelelor şi sistemelor informatice. SCAJ ajută la detectarea incidentelor de securitate prin analizarea datelor de jurnal.

1. SCAJ este instalat şi funcţionează pe un sistem informatic dedicat exclusiv în scopul detectării evenimentelor care ar putea afecta securitatea reţelelor şi sistemelor informatice.

(2) Indicatori de control. SCAJ.

Secţiunea a 2-a

Managementul incidentelor de securitate [C2]

Art. 31 - Răspuns la incidente de securitate [C21]

(1) Cerinţe de securitate

[C211]. Fluxul incidentelor. OSE creează, actualizează şi pune în aplicare o procedură pentru gestionarea, răspunsul şi analiza incidentelor care afectează funcţionarea sau securitatea reţelelor şi sistemelor informatice, în conformitate cu PONIS.

[C212]. Monitorizarea incidentelor. OSE trebuie să implementeze un sistem de monitorizare şi management al evenimentelor şi incidentelor de securitate, bazat cel puţin pe un senzor de detectare a intruziunilor la nivel de reţea care beneficiază de o sursă perpetuă de indicatori de compromitere şi pe analiza logurilor de pe echipamentele sau staţiile de lucru critice pentru desfăşurarea activităţii, în vederea identificării abaterilor de la politicile de securitate şi a intruziunilor.

[C213]. Gestionarea incidentelor. OSE pune în aplicare un sistem informatic dedicat pentru gestionarea incidentelor, pentru a depozita, printre altele, evidenţa tehnică a analizei incidentelor.

1. OSE separă SIDGI de reţelele şi sistemele informatice afectate de incident şi păstrează registrele tehnice aferente pentru o perioadă de cel puţin o jumătate de an.

2. OSE ia în considerare, la proiectarea sistemului, nivelul de confidenţialitate al documentelor stocate.

(2) Indicatori de control. PRORAI; SMMEIS; SIDGI.

Art. 32 - Raport incidente [C22]

(1) Cerinţe de securitate

[C221]. Raportarea incidentelor. OSE creează, actualizează şi implementează o procedură pentru raportarea incidentelor de securitate.

(2) Indicatori de control. PRORIS.

Art. 33 - Comunicarea cu ANSRSI şi CSIRT Naţional [C23]

(1) Cerinţe de securitate

[C231]. Interconectare naţională. OSE se interconectează la serviciul de alertare şi cooperare al CERT-RO care îi permite să ia notă, fără întârziere, de informaţiile transmise de CERT-RO, ca CSIRT Naţional, cu privire la incidente, vulnerabilităţi, ameninţări şi informări relevante.

1. OSE elaborează şi implementează o procedură de interconectare la serviciul de alertare şi cooperare al CERT-RO.

2. OSE asigură monitorizarea permanentă a alertelor şi solicitărilor primite prin acest serviciu ori prin celelalte modalităţi de contact.

[C232]. Responsabili NIS. OSE nominalizează responsabili cu securitatea reţelelor şi sistemelor informatice însărcinaţi cu monitorizarea mijloacelor de contact (responsabili NIS) şi furnizează către CERT-RO, ANSRSI, datele de contact la zi ale acestora (numele şi prenumele, funcţiile şi departamentele din care fac parte, numere de telefon, adrese de e-mail etc.).

1. OSE elaborează şi actualizează permanent lista responsabililor NIS.

[C233]. Gestionare informaţii primite de la CERT-RO. OSE implementează o procedură pentru gestionarea informaţiilor primite şi, după caz, a măsurilor de securitate adoptate pentru protejarea reţelelor şi sistemelor informatice.

(2) Indicatori de control. PISAC; LIRNIS; PRIMSA.

Cap. V
Reziliență [D]

Secţiunea 1
Managementul continuităţii afacerii [D1]

Art. 34 - Asigurarea disponibilităţii serviciului esenţial şi a funcţionării reţelelor şi sistemelor informatice [D11]

(1) Cerinţe de securitate

[D111]. Asigurarea disponibilităţii. În conformitate cu PONIS, OSE defineşte o procedură privind managementul asigurării disponibilităţii serviciului esenţial, în caz de incident de securitate cibernetică.

(2) Indicatori de control. PRADE.

Art. 35 - Managementul recuperării datelor în caz de dezastre [D12]

(1) Cerinţe de securitate

[D121]. Recuperarea datelor. În conformitate cu PONIS, OSE defineşte o procedură privind managementul recuperării datelor în caz de dezastre, precum şi în caz de incidente severe de securitate cibernetică.

(2) Indicatori de control. PROMRE.

Secţiunea a 2-a
Managementul crizelor [D2]

Art. 36 - Organizarea gestionării crizelor [D21]

(1) Cerinţe de securitate

[D211]. Organizarea gestionării crizelor cibernetice. OSE defineşte în PONIS sau separat o procedură privind organizarea gestionării crizelor în caz de incidente de securitate cibernetică pentru asigurarea continuităţii activităţilor organizaţionale.

(2) Indicatori de control. PROCIS.

Art. 37 - Procesul de gestionare a crizelor [D22]

(1) Cerinţe de securitate

[D221]. Gestionarea crizelor cibernetice. OSE defineşte în PONIS sau separat procesele de gestionare a crizelor pe care le va implementa în caz de incidente de securitate cibernetică pentru asigurarea continuităţii activităţilor organizaţionale.

(2) Indicatori de control. PEGEC.

Cap. VI
Dispoziţii finale

Art. 38 - Obligaţii privind implementarea cerinţelor minime de securitate

(1) OSE are obligaţia de a stabili obiective, de a elabora strategii, planuri şi scheme şi de a implementa măsurile minime de securitate stabilite în aceste norme.

(2) După implementarea cerinţelor minime de asigurare a securităţii reţelelor şi sistemelor informatice şi intrarea în conformitate, OSE va informa ANSRSI, prin canalele de comunicare cunoscute (NIS@cert.ro).

Art. 39 - Aplicarea legilor speciale

(1) În cazul în care există legi speciale mai restrictive din punctul de vedere al cerinţelor minime de securitate, se aplică acestea.

(2) Aplicarea legilor speciale nu exclude obligaţia operatorului economic în identificarea ca OSE şi nici îndeplinirea celorlalte obligaţii ce îi revin conform Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, cu modificările şi completările ulterioare.

Art. 40 - Solicitările autorităţii naţionale

OSE va pune la dispoziţia ANSRSI, la solicitarea acesteia, documentele care au stat la baza implementării cerinţelor minime de securitate.

Art. 41 - Corespondenţă privind implementarea şi auditarea cerinţelor minime de securitate

Grila de corespondenţă privind implementarea şi auditarea cerinţelor minime de securitate este prevăzută în anexa nr. 2.

Art. 42 - Anexe la normele tehnice

Anexele nr. 1 şi 2 fac parte integrantă din prezentele norme tehnice.

Anexa Nr. 1
la Normele tehnice

GLOSAR
Termeni şi abrevieri

ANSRSI - autoritatea competentă la nivel naţional pentru securitatea reţelelor şi sistemelor informatice

ARNIS - analiza riscurilor de securitate a reţelelor şi sistemelor informatice, document elaborat la nivelul OSE, prin care sunt identificate elementele critice care stau la baza furnizării serviciului esenţial şi sunt identificate principalele riscuri în vederea gestionării şi diminuării acestora

ANISMS - analiza riscurilor de securitate şi implementarea măsurilor de securitate pentru limitarea accesului neautorizat

ATECNIS - analiză tehnică cu privire la compromiterea securităţii reţelelor şi sistemelor informatice

CEISC - cerinţe de securitate specifice pentru sistemele de control industrial

COSE - contractele de servicii sau furnizare servicii externe

DANIS - decizia de acreditare; decizie formală luată de managementul de nivel înalt al OSE

ECUPA - evidenţa conturilor pentru utilizatori şi pentru procesele automatizate

IEC - indicatori de evaluare, pe baza cărora OSE îşi evaluează conformitatea cu PONIS

INCEA - instrumente necesare pentru conştientizarea şi educarea angajaţilor cu privire la tipurile de ameninţări de securitate informatică şi măsurile de protecţie corespunzătoare în vederea limitării incidentelor

ISC - sisteme de control industriale

JIERUA - jurnalele de înregistrare a evenimentelor produse de resursele utilizate pentru administrare. Jurnalele sunt constituite şi ţinute sub formă electronică sau pe hârtie.

LASMA - listă cu acorduri la nivel de serviciu şi/sau mecanisme de audit a reţelelor şi sistemelor informatice

LASPO - lista activelor, sistemelor şi proceselor organizaţiei

LICA - lista conturilor de administrare

LICPA - lista conturilor privilegiate pe nivele de acces şi funcţionalităţi accesabile

LIRIE - lista riscurilor potenţiale identificate şi evaluarea acestora în furnizarea serviciilor esenţiale. Riscurile sunt reprezentate de relaţiile cu părţile interesate ale ecosistemului

LIRNIS - lista responsabililor NIS

MACC - managementul cheilor de criptare; proces prin care se asigură producerea, utilizarea şi evidenţa materialului criptografic, inclusiv cheile de criptare

MANIS - mapa de acreditare de securitate; document în baza căruia se emite DANIS

MEAUP - mecanism de autentificare pentru utilizatori şi procese automatizate la resursele reţelelor şi sistemelor informatice

MEGRE - metodologie de gestionare a riscurilor furnizării serviciilor esenţiale, document prin care este prezentat procesul de evaluare a riscurilor operatorului economic, criteriile de analiză, de acceptare şi de reducere a riscurilor

MEIEC - metoda de evaluare a indicatorilor de conformitate

NIS - reţele şi sisteme informatice

OSE - operator de servicii esenţiale

PEANIS - procesul de acreditare stabilit în PONIS prin care OSE acreditează NIS utilizate în furnizarea serviciilor esenţiale, inclusiv componentele de administrare

PEGEC - procese de gestionare a crizelor; documente prin care OSE stabileşte procesele şi modurile de implementare în caz de incidente de securitate cibernetică pentru asigurarea continuităţii activităţilor organizaţionale

PEIREV - proces de identificare, clasificare, remediere şi eliminare a vulnerabilităţilor, în special în software şi firmware, la nivelul reţelelor şi sistemelor informatice

PGMAVU - program pentru managementul vulnerabilităţilor în reţelele şi sistemele informatice

PONIS - politica de securitate a reţelelor şi sistemelor informatice care asigură furnizarea serviciilor esenţiale

PPSIA - plicul cu parole utilizate pentru sisteme informatice de administrare a reţelelor şi sistemelor informatice

PRADE - procedură privind managementul asigurării disponibilităţii serviciului esenţial, în caz de incident de securitate cibernetică

PRAPC - procedură pentru asigurarea protecţiei criptografice pentru informaţii şi resurse

PRAPMA - procedură pentru asigurarea protecţiei malware

PRASA - program de prezentare a securităţii pentru tot personalul

PRASI - procedură privind accesul şi securitatea resurselor şi informaţiilor

PGASP - program de asigurare a securităţii personalului; document prin care OSE identifică obiective şi stabileşte cerinţe de securitate pentru fiecare etapă a relaţiei avute de către angajaţi

PRECAS - procedură privind evaluarea conformităţii NIS şi efectuarea auditului de securitate a reţelelor şi sistemelor informatice

PRECDI - procedură privind etichetarea şi clasificarea datelor şi informaţiilor

PRIMSA - procedură pentru gestionarea informaţiilor primite şi, după caz, a măsurilor de securitate adoptate pentru protejarea NIS

PRISA - program de instruire în domeniul securităţii pentru angajaţii care utilizează reţelele şi sistemele informatice care stau la baza furnizării serviciilor esenţiale

PRISAC - procedură de interconectare la serviciul de alertare şi cooperare al CERT-RO

PROCIS - procedură privind organizarea gestionării crizelor în caz de incidente de securitate cibernetică pentru asigurarea continuităţii activităţilor organizaţionale

PRODAIS - procedură pentru detectarea incidentelor de securitate care afectează reţelele şi sistemele informatice

PROFIT - procedură privind filtrarea traficului

PROLD - procedură privind lucrul la distanţă

PROMNIS - procedură pentru menţinerea securităţii reţelelor şi sistemelor informatice

PROMRE - procedură privind managementul recuperării datelor în caz de dezastre, precum şi în caz de incidente severe de securitate cibernetică

PRORAI - procedură pentru gestionarea, răspunsul şi analiza incidentelor care afectează funcţionarea sau securitatea reţelelor şi sistemelor informatice

PRORIS - procedură pentru raportarea incidentelor de securitate

PRORUVI - procedură pentru reducea riscurilor legate de utilizarea unei versiuni învechite

PROSES - procedură privind segregarea şi segmentarea reţelelor şi sistemelor informatice utilizate pentru furnizarea serviciilor esenţiale

PROSRE - procedură de stabilire a relaţiilor ecosistemului; documentul include interconexiunile (relaţiile externe) între reţelele şi sistemele informatice şi terţi

PRUSIA - procedură privind utilizarea sistemelor informatice de administrare

PRUSME - procedură privind utilizarea suporţilor de memorie externă

RAEC - raport de evaluare a conformităţii

RAIPOD - raport privind implementarea politicii de securitate a reţelelor şi sistemelor informatice care asigură furnizarea serviciilor esenţiale şi a documentelor de aplicare a acesteia

RASNIS - raport de audit de securitate a reţelelor şi sistemelor informatice

RATES - raport de testare şi evaluare a securităţii reţelelor şi sistemelor informatice

RERO - registrul de risc organizaţional

RESME - registre de evidenţă a suporţilor de memorie externă

SACNIS - serviciul de alertare şi cooperare al CERT-RO

SANIS - schema arhitecturii reţelelor şi sistemelor informatice folosite la furnizarea serviciilor esenţiale

SCAJ - sistem de corelaţie şi analiză de jurnal

SIA - sisteme informatice de administrare a reţelelor şi sistemelor informatice

SICAE - situaţia cartografică a ecosistemului; document prin care se realizează stabilirea şi identificarea ecosistemului care stă la baza furnizării serviciului esenţial atât NIS, cât şi alte componente. De asemenea include, dar fără a se limita la acestea, părţi interesate, interne şi externe, şi furnizori, în special cei cu acces la NIS sau la gestionarea activelor critice ale operatorului economic.

SIDGI - sistem informatic dedicat pentru gestionarea incidentelor

SIEM - managementul monitorizării, cercetării şi identificării rapide a principalelor cauze de afectare a securităţii, precum şi ale încălcării politicilor de securitate

SIENIS - sistem de înregistrare evenimente la nivelul reţelelor şi sistemelor informatice

SIVMOC - sistem de verificare a potenţialelor modificări ale unui cont privilegiat

SMMEIS - sistem de monitorizare şi management al evenimentelor şi incidentelor de securitate

SMSI - sistemul de management al securităţii informaţiei

SNIS - securitatea reţelelor şi sistemelor informatice

Anexa Nr. 2
la Normele tehnice

GRILA DE CORESPONDENŢĂ
privind implementarea şi auditarea cerinţelor minime de securitate

Domenii de securitate [D]		Categorii de activităţi de securitate [C]		Măsuri de securitate [MS]		Cerinţe de securitate [CS]		Indicatori de control [IC]	
Denumire	ID	Denumire	ID	Denumire	ID	Denumire	ID	Denumire	ID
GUVERNANŢĂ	A	Managementul securităţii informaţiei	A1	Analizarea şi evaluarea riscurilor	A11	Analiza riscurilor de securitate	A111	ARNIS	I01
						Gestionarea riscurilor de securitate	A112	MEGRE	I02
						Evaluarea riscurilor de securitate	A113	RERO	I03
				Realizarea planurilor de securitate. Politica de securitate	A12	Politica de securitate	A121	PONIS	I04
								SMSI	I05
						Implementarea politicii de securitate	A122	RAIPOD	I06

				Acreditarea de securitate	A13	Acreditarea reţelelor şi sistemelor informatice	A131	PEANIS	I07
								DANIS	I08
								MANIS	I09
						Revizuirea validării acreditării de securitate	A132	DANIS	I08
								MANIS	I09
				Indicatori de securitate	A14	Indicatori de securitate	A141	IEC	I10
						Metode de evaluare a securităţii	A142	MEIEC	I11
				Verificarea conformităţii cu privire la securitatea informaţiei. Audit de securitate	A15	Evaluarea conformităţii	A151	PRECAS	I12
								RAEC	I13
						Auditul de securitate	A152	RASNIS	I14
				Testarea şi evaluarea securităţii reţelelor şi sistemelor informatice	A16	Testare şi evaluare securitate	A161	RATES	I15
								ATECNIS	I16
				Asigurarea securităţii personalului	A17	Asigurarea securităţii personalului	A171	PRASP	I17
								FP	I18
								CIM	I19
								CCM	I20
						Verificarea înţelegerii responsabilităţilor	A172	ISA	I21
								VCSA	I22
								COSE	I23
				Conştientizarea şi instruirea utilizatorilor	A18	Instrumente de conştientizare	A181	INCEA	I24
						Instruirea şi prezentarea securităţii	A182	PRASA	I25
								PRISA	I26
				Gestionarea activelor	A19	Inventarierea şi gestionarea activelor	A191	LASPO	I27
								PRECDI	I28
		Managementul ecosistemului	A2	Cartografierea ecosistemului	A21	Descrierea ecosistemului	A211	SICAE	I29
								LIRIE	I30
				Relaţiile ecosistemului	A22	Stabilirea relaţiilor ecosistemului	A221	PROSRE	I31
						Acorduri la nivel de serviciu	A222	LASMA	I32
PROTECŢIE	B	Managementul arhitecturii	B1	Managementul configuraţiei reţelelor şi sistemelor informatice	B11	Arhitectura NIS	B111	SANIS	I33
						Instalarea echipamentelor şi serviciilor	B112	ARNIS	I01
								MANIS	I09
					B12	Suporţi de memorie externă	B121	PRUSME	I34

				Managementul suporţilor de memorie externă				RESME	I35
				Segregarea şi segmentarea reţelelor şi sistemelor informatice	B13	Segregarea şi segmentarea	B131	PROSES	I36
								SANIS	I33
				Filtrarea traficului	B14	Filtrarea fluxurilor	B141	PROFIT	I37
								ARNIS	I01
				Asigurarea protecţiei produselor şi serviciilor aferente reţelelor şi sistemelor informatice	B15	Asigurarea protecţiei criptografice	B151	PRAPC	I38
						Managementul cheilor de criptare	B152	MACC	I39
				Protecţia împotriva malware	B16	Protecţie malware	B161	PRAPMA	I40
		Managementul administrării	B2	Administrarea conturilor	B21	Conturi de administrare	B211	LICA	I41
				Administrarea reţelelor şi sistemelor informatice	B22	Utilizarea sistemelor de administrare	B221	PRUSIA	I42
								PONIS	I04
						Parole administrare	B222	JIERU	I43
								PPSIA	I44
				Managementul accesului de la distanţă	B23	Lucrul la distanţă	B231	PROLD	I45
								PRAPC	I38
		Managementul identităţii şi accesului	B3	Managementul identificării şi autentificării utilizatorilor	B31	Identificarea utilizatorilor	B311	ECUPA	I46
								ARNIS	I01
								MANIS	I09
						Autentificarea utilizatorilor	B312	MEAUP	I47
				Managementul drepturilor de acces	B32	Acordarea drepturilor de acces	B321	PONIS	I04
								LICPA	I48
								LICA	I41
						Verificarea conturilor privilegiate	B322	SIVMOC	I49
		Managementul mentenanţei	B4	Mentenanţa reţelelor şi sistemelor informatice	B41	Menţinere securitate	B411	PROMNIS	I50
						Actualizare resurse	B412	PRORUVI	I51
								PONIS	I04

								MANIS	I09
						Protejare resurse	B413	PRAPC	I38
				Sisteme control industrial. SCADA - Monitorizare, control şi achiziţii de date	B42	Sisteme de control industriale	B421	CEISC	I52
						Limitarea accesului	B422	ANISMS	I53
		Managementul securităţii fizice	B5	Asigurarea protecţiei fizice a reţelelor şi sistemelor informatice	B51	Acces la resurse	B511	PRASI	I54
APĂRARE CIBERNETICĂ	C	Managementul detecţiei	C1	Managementul vulnerabilităţilor şi alertelor de securitate	C11	Fluxul alertelor de securitate	C111	PRODIS	I55
								SIENIS	I56
								MANIS	I09
						Evaluarea şi monitorizarea vulnerabilităţilor	C112	PEIREV	I57
								PGMAVU	I58
								ARNIS	I01
				Înregistrarea evenimentelor	C12	Monitorizare evenimente	C121	SIENIS	I56
						Sisteme de management	C122	SIEM	I59
				Jurnalizarea şi asigurarea trasabilităţii activităţilor în cadrul reţelelor şi sistemelor informatice	C13	Jurnalizare şi trasabilitate	C131	SCAJ	I44
		Managementul incidentelor de securitate	C2	Răspuns la incidente de securitate	C21	Fluxul incidentelor	C211	PRORAI	I60
						Monitorizarea incidentelor	C212	SMMEIS	I61
						Gestionarea incidentelor	C213	SIDGI	I62
				Raport incidente	C22	Raportarea incidentelor	C221	PRORIS	I63
				Comunicarea cu Autoritatea competentă la nivel naţional pentru securitatea reţelelor şi sistemelor informatice (ANSRSI) şi CSIRT Naţional	C23	Interconectare naţională	C231	PISAC	I64
						Responsabili NIS	C232	LIRNIS	I65
						Gestionare informaţii primite de la CERT-RO	C233	PRIMSA	I66

REZILIENŢĂ	D	Managementul continuităţii afacerii	D1	Asigurarea disponibilităţii serviciului esenţial şi a funcţionării reţelelor şi sistemelor informatice	D11	Asigurarea disponibilităţii	D111	PRADE	I67
				Managementul recuperării datelor în caz de dezastre	D12	Recuperarea datelor	D121	PROMRE	I68
		Managementul crizelor	D2	Organizarea gestionării crizelor	D21	Organizarea gestionării crizelor cibernetice	D211	PROCIS	I69
				Procesul de gestionare a crizelor	D22	Gestionarea crizelor cibernetice	D221	PEGEC	I70