



# MONITORUL OFICIAL

## AL

# ROMÂNIEI

Anul 188 (XXXII) — Nr. 1142

PARTEA I  
LEGI, DECRETE, HOTĂRĂRI ȘI ALTE ACTE

Joi, 26 noiembrie 2020

### SUMAR

<u>Nr.</u>		<u>Pagina</u>
LEGI ȘI DECRETE		
272.	— Lege pentru modificarea și completarea Legii nr. 212/2015 privind modalitatea de gestionare a vehiculelor și a vehiculelor scoase din uz .....	2
908.	— Decret privind promulgarea Legii pentru modificarea și completarea Legii nr. 212/2015 privind modalitatea de gestionare a vehiculelor și a vehiculelor scoase din uz .....	2
DECIZII ALE CURȚII CONSTITUȚIONALE		
Decizia nr. 298 din 9 iunie 2020 referitoare la excepția de neconstituționalitate a dispozițiilor art. 318 alin. (15) lit. a) din Codul de procedură penală .....		3–5
ACTE ALE ORGANELOR DE SPECIALITATE ALE ADMINISTRAȚIEI PUBLICE CENTRALE		
1.323.	— Ordin al secretarului general al Guvernului pentru aprobarea Normelor tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale .....	6–16

## PARLAMENTUL ROMÂNIEI

CAMERA DEPUTAȚILOR

SENATUL

## L E G E

**pentru modificarea și completarea Legii nr. 212/2015 privind modalitatea de gestionare a vehiculelor și a vehiculelor scoase din uz**

Parlamentul României adoptă prezenta lege.

**Art. I.** — Legea nr. 212/2015 privind modalitatea de gestionare a vehiculelor și a vehiculelor scoase din uz, publicată în Monitorul Oficial al României, Partea I, nr. 554 din 27 iulie 2015, cu modificările și completările ulterioare, se modifică și se completează după cum urmează:

**1. La articolul 13, alineatul (3) se modifică și va avea următorul cuprins:**

„(3) Operatorii economici autorizați să desfășoare activități de colectare și tratare a vehiculelor scoase din uz sunt obligați să le stocheze, chiar și temporar, și să trateze vehiculele scoase din uz potrivit prevederilor art. 4 din Legea nr. 211/2011 privind regimul deșeurilor, republicată, cu modificările și completările ulterioare, și conform cerințelor prevăzute în anexa nr. 2, cu respectarea reglementărilor cu privire la sănătatea umană și mediu.”

**2. La articolul 17, alineatele (5) și (6) se modifică și vor avea următorul cuprins:**

„(5) Agenția Națională pentru Protecția Mediului transmite Comisiei Europene, pentru fiecare an calendaristic, un raport privind punerea în aplicare a art. 15, conform formatului pentru raportarea datelor stabilit de Comisia Europeană.

(6) Agenția Națională pentru Protecția Mediului transmite Comisiei Europene, pe cale electronică, raportul prevăzut la

alin. (5), în termen de 18 luni de la sfârșitul anului de raportare pentru care sunt colectate datele. Raportul indică modul în care au fost obținute datele și verificarea calității acestora.”

**3. La articolul 17, după alineatul (6) se introduce un nou alineat, alineatul (7), cu următorul cuprins:**

„(7) Prima perioadă de raportare începe în primul an calendaristic complet după adoptarea de către Comisia Europeană a actului de punere în aplicare ce stabilește formatul de raportare și cuprinde datele pentru perioada de raportare respectivă.”

**Art. II.** — Prezenta lege intră în vigoare la 3 zile de la data publicării în Monitorul Oficial al României, Partea I.

★

Prezenta lege transpune prevederile art. I din Directiva (UE) 2018/849 a Parlamentului European și a Consiliului din 30 mai 2018 de modificare a Directivei 2000/53/CE privind vehiculele scoase din uz, a Directivei 2006/66/CE privind bateriile și acumulatorii și deșeurile de baterii și acumulatori și a Directivei 2012/19/UE privind deșeurile de echipamente electrice și electronice, publicată în Jurnalul Oficial al Uniunii Europene, seria L, nr. 150 din 14 iunie 2018.

*Această lege a fost adoptată de Parlamentul României, cu respectarea prevederilor art. 75 și ale art. 76 alin. (2) din Constituția României, republicată.*

p. PREȘEDINTELE CAMEREI DEPUTAȚILOR,

**FLORIN IORDACHE**

p. PREȘEDINTELE SENATULUI,

**ROBERT-MARIUS CAZANCIUC**

București, 25 noiembrie 2020.

Nr. 272.

## PREȘEDINTELE ROMÂNIEI

## D E C R E T

**privind promulgarea Legii pentru modificarea și completarea Legii nr. 212/2015 privind modalitatea de gestionare a vehiculelor și a vehiculelor scoase din uz**

În temeiul prevederilor art. 77 alin. (1) și ale art. 100 alin. (1) din Constituția României, republicată,

**Președintele României d e c r e t e a z ă:**

Articol unic. — Se promulgă Legea pentru modificarea și completarea Legii nr. 212/2015 privind modalitatea de gestionare a vehiculelor și a vehiculelor scoase din uz și se dispune publicarea acestei legi în Monitorul Oficial al României, Partea I.

PREȘEDINTELE ROMÂNIEI  
**KLAUS-WERNER IOHANNIS**

București, 24 noiembrie 2020.

Nr. 908.

# DECIZII ALE CURȚII CONSTITUȚIONALE

## CURTEA CONSTITUȚIONALĂ

### DECIZIA Nr. 298

din 9 iunie 2020

#### referitoare la excepția de neconstituționalitate a dispozițiilor art. 318 alin. (15) lit. a) din Codul de procedură penală

Valer Dorneanu	— președinte
Cristian Deliorga	— judecător
Marian Enache	— judecător
Daniel Marius Morar	— judecător
Mona-Maria Pivniceru	— judecător
Gheorghe Stan	— judecător
Livia Doina Stanciu	— judecător
Elena-Simina Tănăsescu	— judecător
Varga Attila	— judecător
Cristina Teodora Pop	— magistrat-asistent

Cu participarea reprezentantului Ministerului Public, procuror Dana-Cristina Bunea.

1. Pe rol se află soluționarea excepției de neconstituționalitate a dispozițiilor art. 318 alin. (15) lit. a) din Codul de procedură penală, excepție ridicată de Ion Olteanu în Dosarul nr. 12.206/225/2017 al Judecătoriei Drobeta-Turnu Severin și care formează obiectul Dosarului Curții Constituționale nr. 148D/2018.

2. La apelul nominal lipsesc părțile. Procedura de citare este legal îndeplinită.

3. Cauza fiind în stare de judecată, președintele Curții acordă cuvântul reprezentantului Ministerului Public, care pune concluzii de respingere a excepției de neconstituționalitate, în principal, ca inadmisibilă, deoarece se solicită modificarea prevederilor legale criticate, și, în subsidiar, ca neîntemeiată, fiind invocată jurisprudența Curții Constituționale, respectiv Decizia nr. 48 din 22 ianuarie 2019 și Decizia nr. 744 din 21 noiembrie 2019.

CURTEA,

având în vedere actele și lucrările dosarului, constată următoarele:

4. Prin Încheierea din 23 ianuarie 2018, pronunțată în Dosarul nr. 12.206/225/2017, **Judecătoria Drobeta-Turnu Severin a sesizat Curtea Constituțională cu excepția de neconstituționalitate a prevederilor art. 318 alin. (15) lit. a) din Codul de procedură penală**, excepție ridicată de Ion Olteanu într-o cauză având ca obiect confirmarea unei soluții de renunțare la urmărirea penală.

5. În motivarea excepției de neconstituționalitate se susține că dispozițiile art. 318 alin. (15) lit. a) din Codul de procedură penală, spre deosebire de prevederile art. 341 alin. (7) pct. 2 din Codul de procedură penală, nu permit judecătorului de cameră preliminară ca odată cu respingerea cererii de confirmare a ordonanței procurorului de renunțare la urmărirea penală să dispună începerea judecării cu privire la faptele și persoanele pentru care a fost pusă în mișcare acțiunea penală, atunci când probele administrate au fost suficiente. Se susține că, pentru acest motiv, dispozițiile art. 318 alin. (15) lit. a) din Codul de procedură penală încalcă principiul egalității în

drepturi. Se arată, de asemenea, că textul criticat este neconstituțional, întrucât, în ipoteza respingerii cererii de confirmare a soluției de renunțare la urmărirea penală, nu îl obligă pe judecător să indice procurorului ce probatoriu trebuie să administreze, oferindu-i acestuia posibilitatea unor interpretări și soluții diferite, fapt care încalcă principiul calității legii, ce decurge din prevederile art. 1 alin. (5) din Constituție, conform căruia normele juridice trebuie să fie clare, precise și previzibile.

6. **Judecătoria Drobeta-Turnu Severin** opinează că excepția de neconstituționalitate este neîntemeiată. Se arată că cele două instituții de drept procesual penal prevăzute la art. 318 și art. 341 din Codul de procedură penală sunt diferite, astfel încât soluțiile ce pot fi dispuse de către judecătorul de cameră preliminară sunt și ele diferite, fără ca prin aceasta să fie încălcate prevederile constituționale invocate de autorul excepției. În consecință, se arată că art. 318 alin. (15) lit. a) din Codul de procedură penală nu încalcă standardele de calitate a legii și nici principiul egalității în drepturi.

7. Potrivit prevederilor art. 30 alin. (1) din Legea nr. 47/1992, încheierea de sesizare a fost comunicată președinților celor două Camere ale Parlamentului, Guvernului și Avocatului Poporului, pentru a-și exprima punctele de vedere asupra excepției de neconstituționalitate.

8. **Avocatul Poporului** arată că prevederile art. 318 alin. (15) lit. a) din Codul de procedură penală sunt constituționale. Se susține că textul criticat nu încalcă dispozițiile art. 16 alin. (1) din Constituție, fiind invocată, în acest sens, jurisprudența Curții Constituționale referitoare la principiul egalității în fața legii, respectiv Decizia Plenului Curții Constituționale nr. 1 din 8 februarie 1994, precum și Deciziile nr. 107 din 13 iunie 2000 și nr. 781 din 17 noiembrie 2015. Se susține că procedura prin care judecătorul de cameră preliminară admite sau respinge o cerere de confirmare a soluției de renunțare la urmărirea penală asigură toate garanțiile procesuale specifice drepturilor fundamentale invocate în prezenta cauză. În subsidiar, se arată că aspectele criticate de autorul excepției de neconstituționalitate vizează interpretarea și aplicarea legii, competențe care aparțin exclusiv instanțelor de judecată.

9. **Președinții celor două Camere ale Parlamentului și Guvernul** nu au comunicat punctele lor de vedere asupra excepției de neconstituționalitate.

CURTEA,

examinând încheierea de sesizare, punctul de vedere al Avocatului Poporului, raportul întocmit de judecătorul-raportor, concluziile procurorului, dispozițiile legale criticate, raportate la prevederile Constituției, precum și Legea nr. 47/1992, reține următoarele:

10. Curtea Constituțională a fost legal sesizată și este competentă, potrivit dispozițiilor art. 146 lit. d) din Constituție,

precum și ale art. 1 alin. (2), ale art. 2, 3, 10 și 29 din Legea nr. 47/1992, să soluționeze excepția de neconstituționalitate.

11. **Obiectul excepției de neconstituționalitate** îl constituie dispozițiile art. 318 alin. (15) lit. a) din Codul de procedură penală, care au următorul cuprins: „*Judecătorul de cameră preliminară verifică legalitatea și temeinicia soluției de renunțare la urmărirea penală pe baza lucrărilor și a materialului din dosarul de urmărire penală și a înscrisurilor noi prezentate și, prin încheiere, admite sau respinge cererea de confirmare formulată de procuror. În cazul în care respinge cererea de confirmare, judecătorul de cameră preliminară:*

a) *desființează soluția de renunțare la urmărire penală și trimite cauza la procuror pentru a începe sau a completa urmărirea penală ori, după caz, pentru a pune în mișcare acțiunea penală și a completa urmărirea penală; [...]*”

12. Se susține că textele criticate contravin prevederilor constituționale ale art. 1 alin. (5) cu privire la calitatea legii și ale art. 16 alin. (1) referitor la egalitatea în drepturi.

13. Examinând excepția de neconstituționalitate, Curtea reține că în ipoteza în care este sesizat cu o cerere de confirmare a unei soluții de renunțare la urmărirea penală, judecătorul de cameră preliminară este investit în vederea verificării legalității și temeiniciei soluției de renunțare la urmărirea penală, pe baza lucrărilor și a materialului din dosarul de urmărire penală și a înscrisurilor noi prezentate. Ca urmare a verificărilor anterior menționate, acesta poate pronunța una dintre următoarele două soluții: desființarea soluției de renunțare la urmărire penală și trimiterea cauzei la procuror pentru a începe sau a completa urmărirea penală ori, după caz, pentru a pune în mișcare acțiunea penală și a completa urmărirea penală; desființarea soluției de renunțare la urmărirea penală și dispunerea soluției de clasare.

14. Așa fiind, în ipoteza invocată de autorul excepției de neconstituționalitate, aceea a desființării de către judecătorul de cameră preliminară a soluției de renunțare la urmărirea penală, atunci când a fost pusă în mișcare acțiunea penală, iar probele administrate sunt suficiente pentru trimiterea în judecată, judecătorul de cameră preliminară investit cu soluționarea cererii formulate conform art. 318 din Codul de procedură penală nu poate proceda la verificarea legalității administrării probelor și a efectuării actelor de către organele de urmărire penală, conform art. 342 din Codul de procedură penală. Aceasta, întrucât procedura prevăzută la art. 318 alin. (15) din Codul de procedură penală nu îi oferă acestuia competența funcțională de a reține cauza spre a o soluționa conform procedurii camerei preliminare. Așa fiind, în ipoteza analizată, pentru investirea instanței în vederea desfășurării verificărilor specifice etapei camerei preliminare, judecătorul de cameră preliminară sesizat cu cererea de încuviințare a renunțării la urmărirea penală va proceda conform art. 318 alin. (15) lit. a) din Codul de procedură penală, desființând soluția de renunțare la urmărire penală și trimițând cauza la procuror pentru completarea urmăririi penale. Acesta din urmă, dacă apreciază, la rândul său, că probele administrate sunt suficiente pentru trimiterea în judecată a inculpatului, va proceda la emiterea rechizitoriului și la sesizarea instanței competente în vederea începerii procedurii camerei preliminare.

15. Această soluție legislativă este în acord, pe de o parte, cu natura și caracteristicile etapei urmăririi penale, iar, pe de altă parte, cu cele ale etapei camerei preliminare.

16. Astfel, potrivit art. 56 alin. (1) din Codul de procedură penală, procurorul este organul judiciar competent să conducă și să controleze nemijlocit activitatea de urmărire penală a

poliției judiciare și a organelor de cercetare penală speciale, prevăzute de lege, și, de asemenea, să supravegheze ca actele de urmărire penală să fie efectuate cu respectarea dispozițiilor legale. De asemenea, din interpretarea dispozițiilor art. 285—341 din Codul de procedură penală, Curtea reține că întreaga activitate de urmărire penală se desfășoară sub supravegherea procurorului și se încheie, conform art. 327 din Codul de procedură penală, fie cu emiterea actului de sesizare a instanței, respectiv a rechizitoriului, fie cu emiterea ordonanței prin care se clasează cauza sau se renunță la urmărire penală. Așa fiind, în vederea sesizării instanței cu rechizitoriul, procurorul este cel care apreciază cu privire la existența faptei, la săvârșirea sa de către inculpat și la capacitatea acestuia de a răspunde penal, astfel cum aceste aspecte rezultă din materialul de urmărire penală. Prin urmare, doar în urma emiterii rechizitoriului conform considerentelor anterior arătate, se poate trece la judecarea cauzei în etapa camerei preliminare, conform art. 342 și următoarele din Codul de procedură penală.

17. Pe de altă parte, procedura prevăzută la art. 318 alin. (15) din Codul de procedură penală are ca scop unic verificarea legalității și a temeiniciei soluției de renunțare la urmărirea penală, neconfundându-se și neputând fi extinsă la cea specifică etapei camerei preliminare. Aceasta din urmă presupune, conform art. 342 și următoarele din Codul de procedură penală, repartizarea aleatorie a dosarului, stabilirea unui termen pentru soluționarea cererilor și a excepțiilor formulate sau ridicate din oficiu, în camera de consiliu, cu citarea părților și în prezența procurorului, precum și pronunțarea unei soluții dintre cele prevăzute la art. 346 din Codul de procedură penală. În urma acestei proceduri, poate fi pronunțată însă oricare dintre soluțiile prevăzute la art. 346 din Codul de procedură penală, respectiv începerea judecății, ipoteză invocată de autorul excepției, și restituirea cauzei la parchet, pentru unul dintre motivele prevăzute la art. 346 alin. (3) din Codul de procedură penală. Așa fiind, continuarea procedurii prevăzute la art. 318 alin. (15) din Codul de procedură penală cu procedura camerei preliminare, prevăzută la art. 342 și următoarele din Codul de procedură penală, poate avea ca efect restituirea cauzei la procuror pentru alte motive decât cele prevăzute la art. 318 alin. (15) lit. a) din Codul de procedură penală, aspect ce ar deturna procedura de verificare a legalității și temeiniciei soluției de renunțare la urmărirea penală de la scopul propus de legiuitor. Pentru acest motiv, instituția renunțării la urmărire penală, în ipoteza prevăzută la art. 318 alin. (15) lit. a) din Codul de procedură penală, nu și-ar mai atinge finalitatea.

18. Având în vedere aceste considerente, Curtea reține că nereglementarea de către legiuitor a posibilității judecătorului de cameră preliminară de a proceda la soluționarea cauzei în etapa camerei preliminare, în cazul în care acesta este sesizat conform art. 318 din Codul de procedură penală, iar probele administrate în cauză sunt suficiente pentru trimiterea în judecată a inculpatului, are ca scop respectarea naturii celor două instituții de drept procesual penal, renunțarea la urmărire penală și judecata în primă instanță, precum și asigurarea atingerii scopului acestora.

19. Mai mult, această manieră de reglementare a procedurii soluționării cererilor de confirmare a renunțării la urmărire penală constituie opțiunea legiuitorului, exprimată potrivit art. 61 alin. (1) din Constituție și în marja de apreciere prevăzută de acesta.

20. În ceea ce privește discriminarea invocată de autorul excepției între inculpații cărora le sunt aplicate prevederile

art. 318 alin. (15) lit. a) din Codul de procedură penală și cei cărora li se aplică dispozițiile art. 314 din Codul de procedură penală, sub aspectul posibilității judecătorului de cameră preliminară de a proceda la verificarea legalității administrării probelor și a efectuării urmăririi penale și de a dispune începerea judecării, în ipoteza prevăzută la art. 341 alin. (7) pct. 2 din Codul de procedură penală, soluție ce nu poate fi dispusă în cazul prevăzut la art. 318 alin. (15) lit. a) din Codul de procedură penală, Curtea reține că această diferență este dată de natura instituției renunțării la urmărire penală.

21. Renunțarea la urmărire penală reprezintă o excepție de la principiul legalității procesului penal, specific dreptului continental, principiu prevăzut la art. 2 din Codul de procedură penală, instituită în favoarea principiului oportunității urmăririi penale, specific dreptului anglo-saxon, a cărei reglementare a fost motivată de supraîncărcarea organelor judiciare cu cauze penale și de necesitatea unei soluții intermediare, între soluția de clasare și cea de trimitere în judecată. Această instituție este caracterizată prin faptul că actul renunțării la urmărire penală presupune hotărârea procurorului de a renunța la realizarea activităților de investigare a infracțiunilor săvârșite și la tragerea la răspundere penală a suspectilor, în situația în care constată săvârșirea de către aceștia a unor fapte prevăzute de legea penală, dacă apreciază că nu există interes public în urmărirea penală a respectivelor fapte.

22. Așa fiind, persoanele în privința cărora procurorul dispune soluția renunțării la urmărire penală sunt într-o situație diferită de cele în privința cărora a fost dispusă o soluție de clasare, soluție împotriva căreia este formulată plângere, conform art. 340 din Codul de procedură penală. Această diferență justifică reglementarea de către legiuitor a unui regim juridic diferit sub aspectul posibilității judecătorului de cameră preliminară de a dispune soluția trimiterii în judecată în ipotezele prevăzute la art. 318 alin. (15) lit. a) și art. 341 alin. (7) pct. 2 din Codul de procedură penală.

23. Pentru aceste considerente, Curtea reține că prevederile art. 318 alin. (15) lit. a) din Codul de procedură penală nu contravin dispozițiilor art. 16 alin. (1) din Constituție referitoare la egalitatea în drepturi.

24. În subsidiar, Curtea constată că neconstituționalitatea unei dispoziții legale nu poate fi dedusă din compararea ei cu o

altă dispoziție legală, ci din raportarea celei dintâi la prevederile Legii fundamentale, motiv pentru care nu pot fi reținute criticile ce au la bază compararea prevederilor art. 318 alin. (15) lit. a) din Codul de procedură penală cu cele ale art. 341 alin. (7) pct. 2 din Codul de procedură penală.

25. Cu privire la critica potrivit căreia textul criticat este neconstituțional întrucât, în ipoteza respingerii cererii de confirmare a soluției de renunțare la urmărirea penală, nu îl obligă pe judecător să indice procurorului ce probatoriu trebuie să administreze, Curtea constată că și aceasta este neîntemeiată. În acest sens, Curtea reține că, din interpretarea prevederilor art. 318 alin. (15) din Codul de procedură penală în ansamblul instituției renunțării la urmărire penală, în ipoteza analizată, judecătorul de cameră desființează soluția de renunțare la urmărire penală și trimite cauza la procuror pentru a începe sau a completa urmărirea penală ori, după caz, pentru a pune în mișcare acțiunea penală și a completa urmărirea penală, ca urmare a constatării că există un interes public în urmărirea faptei. Cu toate acestea, începerea sau completarea urmăririi penale presupune desfășurarea acestei etape procesuale de către organele de urmărire penală, în sensul realizării unor activități de cercetare penală care să aibă ca rezultat strângerea și administrarea de probe sau de noi probe, în scopul trimiterii în judecată. Așa fiind, cunoașterea de către judecătorul de cameră preliminară, la momentul pronunțării soluției prevăzute la art. 318 alin. (15) lit. a) din Codul de procedură penală, a probelor necesare, ce urmează a fi administrate după trimiterea cauzei la procuror, este, practic, imposibilă, acestea urmând a fi rezultatul activității de cercetare penală ce urmează a fi efectuată. Mai mult, conform art. 56 alin. (1) din Codul de procedură penală, activitatea de urmărire penală a poliției judiciare și a organelor de cercetare penală speciale este condusă și controlată de către procuror, acesta supraveghind ca actele de urmărire penală să fie efectuate cu respectarea legii. Prin urmare, soluția juridică analizată, care nu îl obligă pe judecătorul de cameră preliminară ca, în ipoteza prevăzută la art. 318 alin. (15) lit. a) din Codul de procedură penală, să indice probele ce urmează a fi administrate ca urmare a trimiterii cauzei la procuror, este în acord cu natura și caracteristicile etapei urmăririi penale, textul criticat nefiind contrar dispozițiilor constituționale ale art. 1 alin. (5).

26. Pentru considerentele expuse mai sus, în temeiul art. 146 lit. d) și al art. 147 alin. (4) din Constituție, al art. 1—3, al art. 11 alin. (1) lit. A.d) și al art. 29 din Legea nr. 47/1992, cu unanimitate de voturi,

## CURTEA CONSTITUȚIONALĂ

În numele legii

DECIDE:

Respinge, ca neîntemeiată, excepția de neconstituționalitate ridicată de Ion Olteanu în Dosarul nr. 12.206/225/2017 al Judecătoriei Drobeta-Turnu Severin și constată că dispozițiile art. 318 alin. (15) lit. a) din Codul de procedură penală sunt constituționale în raport cu criticile formulate.

Definitivă și general obligatorie.

Decizia se comunică Judecătoriei Drobeta-Turnu Severin și se publică în Monitorul Oficial al României, Partea I.

Pronunțată în ședința din data de 9 iunie 2020.

PREȘEDINTELE CURȚII CONSTITUȚIONALE

prof. univ. dr. **VALER DORNEANU**

Magistrat-asistent,  
**Cristina Teodora Pop**

# ACTE ALE ORGANELOR DE SPECIALITATE ALE ADMINISTRAȚIEI PUBLICE CENTRALE

GUVERNUL ROMÂNIEI

SECRETARIATUL GENERAL AL GUVERNULUI

## ORDIN

### pentru aprobarea Normelor tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale

Având în vedere dispozițiile art. 20 lit. b) și s) și ale art. 25 alin. (1) și (3) din Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cu modificările și completările ulterioare, în temeiul art. 7 alin. (6) din Hotărârea Guvernului nr. 137/2020 privind organizarea, funcționarea și atribuțiile unor structuri din cadrul aparatului de lucru al Guvernului,

**secretarul general al Guvernului** emite prezentul ordin.

Art. 1. — Se aprobă Normele tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale, 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 rețelelor și sistemelor informatice, cu modificările și completările ulterioare, operatorii de servicii esențiale aplică normele tehnice privind

cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale.

Art. 3. — În aplicarea art. 32 alin. (5) din Legea nr. 362/2018, cu modificările și completările ulterioare, se va ține seama de Normele tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale, prevăzute la art. 1.

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

Secretarul general al Guvernului,  
**Antonel Tănase**

București, 9 noiembrie 2020.  
Nr. 1.323.

ANEXĂ

## NORME TEHNICE

### privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale

#### CAPITOLUL I Dispoziții generale

##### ARTICOLUL 1 Aplicabilitate

Prezentele norme tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice, denumite în continuare *norme*, sunt aplicabile operatorilor de servicii esențiale și au ca obiect asigurarea unui nivel comun de securitate a rețelelor și sistemelor informatice.

##### ARTICOLUL 2

#### Termeni, abrevieri și domenii de securitate

(1) În stabilirea cerințelor minime de asigurare a securității rețelelor și sistemelor informatice se utilizează următoarele domenii de securitate:

1. guvernanta — obiectivele domeniului sunt: elaborarea și implementarea politicilor de securitate la nivelul organizațional; angajamentul managementului de nivel înalt al organizației în asigurarea sistemului de management al securității informației;

gestionarea managementului riscurilor privind amenințările, vulnerabilitățile și riscurile identificate;

2. protecție — obiectivele domeniului sunt: asigurarea securității rețelelor și sistemelor informatice, securitatea fizică și a persoanei; administrarea și mentenanța resurselor rețelelor și sistemelor informatice; controlul accesului la elementele/componentele rețelelor și sistemelor informatice;

3. apărare cibernetică — obiectivele domeniului sunt: asigurarea managementului incidentelor de securitate; detectarea și tratarea incidentelor de securitate care afectează securitatea rețelelor și sistemelor informatice;

4. reziliență — obiectivele domeniului sunt: managementul continuității serviciilor esențiale furnizate; gestionarea situațiilor de criză, în special a incidentelor de securitate care au un impact major asupra serviciilor esențiale.

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

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

(4) În procesul de implementare a cerințelor de securitate, OSE identifică riscurile privind neimplementarea, planifică activitățile care stau la baza implementării și stabilește responsabilitățile pentru realizarea acestora.

## CAPITOLUL II Guvernanță [A]

### SECȚIUNEA 1

#### Managementul securității informației [A1]

### ARTICOLUL 3

#### Analizarea și evaluarea riscurilor [A11]

##### (1) Cerințe de securitate

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

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

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

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

- noile amenințări în domeniul securității cibernetice;
- punctele slabe descoperite recent;
- pierderea eficacității măsurilor de securitate;
- modificările situației de risc cauzate de modificările arhitecturii rețelelor și sistemelor informatice;
- orice alte modificări ale situației de risc.

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

### ARTICOLUL 4

#### Realizarea planurilor de securitate. Politica de securitate [A12]

##### (1) Cerințe de securitate

[A121]. Politica de securitate. Pornind de la ARNIS, OSE elaborează, menține și implementează o politică de securitate a rețelelor și sistemelor informatice care asigură furnizarea serviciilor esențiale și un sistem de management al securității informațiilor.

1. PONIS stabilește obiectivele strategice de securitate, descrie guvernanța securității și reflectă toate politicile specifice de securitate ale SMSI (procesul de acreditare de securitate, audit de securitate, criptografie, întreținere securitate, manipulare incidente etc.).

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

1. Raportul specifică inventarul riscurilor, nivelul securității rețelelor și sistemelor informatice și acțiunile de securitate planificate și realizate.

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

### ARTICOLUL 5

#### Acreditarea de securitate [A13]

##### (1) Cerințe de securitate

[A131]. Acreditarea rețelelor și sistemelor informatice. În baza ARNIS și în conformitate cu procesul de acreditare stabilit

în PONIS, OSE acreditează rețelele și 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 și modul de implementare a măsurilor necesare pentru protecție și are valabilitate de cel mult un an. Decizia certifică, de asemenea, faptul că orice risc rezidual a fost identificat și 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 și obiective de securitate;
- proceduri și măsuri de securitate aplicate;
- rapoarte de audit de securitate;
- rapoarte de evaluare a conformității;
- riscuri reziduale și motive care justifică acceptarea acestora.

[A132]. Revizuirea validării acreditării de securitate. Anual și 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 configurația rețelelor și sistemelor informatice sau a aplicațiilor, OSE va revizui validarea acreditării de securitate. OSE are obligația reînnoirii aprobării imediat ce nu mai este valabilă.

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

### ARTICOLUL 6

#### Indicatori de securitate [A14]

##### (1) Cerințe de securitate

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

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

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

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

(2) Indicatori de control. IEC; MEIEC.

### ARTICOLUL 7

#### Verificarea conformității cu privire la securitatea informației. Audit de securitate [A15]

##### (1) Cerințe de securitate

[A151]. Evaluarea conformității. În baza ARNIS, OSE stabilește și actualizează periodic procedura privind evaluarea conformității SNIS și efectuarea auditului de securitate a rețelelor și 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 conformității.

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

1. Auditul se efectuează numai de auditori de securitate informatică pentru auditarea rețelelor și sistemelor informatice, atestați de ANSRSI și cu atestat valabil la data finalizării RASNIS.

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

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

## ARTICOLUL 8

**Testarea și evaluarea securității rețelelor și sistemelor informatice [A16]**

## (1) Cerințe de securitate

[A161]. Testare și evaluare securitate. Procesul de testare și evaluare va implica verificarea sistemelor operaționale pe baza unei planificări atente astfel încât riscul întreruperii furnizării serviciului esențial să fie minim și se finalizează cu un raport de testare și evaluare a securității rețelelor și sistemelor informatice.

1. Testarea și evaluarea rețelelor și sistemelor informatice presupun identificarea și prevenirea vulnerabilităților software și hardware, respectiv:

- testarea securității aplicațiilor;
- testarea securității infrastructurii rețelelor și sistemelor informatice.

2. Testarea și evaluarea securității rețelelor și sistemelor informatice vor fi efectuate numai de personal specializat, atestat de către ANRSRI.

3. Rezultatele analizelor tehnice cu privire la compromiterea securității efectuate pe parcursul auditărilor pot fi prezentate numai persoanelor care au nevoie de aceste informații pentru a-și îndeplini atribuțiile ce le revin.

(2) Indicatori de control. RATES; ATECNIS.

## ARTICOLUL 9

**Asigurarea securității personalului [A17]**

## (1) Cerințe de securitate

[A171]. Asigurarea securității personalului. OSE elaborează un program de asigurare a securității personalului prin care identifică obiective și stabilește cerințe de securitate pentru fiecare etapă a relației avute de către angajați.

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

[A172]. Verificarea înțelegerii responsabilităților. OSE se asigură că angajații înțeleg responsabilitățile și sunt potriviți pentru rolurile stabilite, iar contractanții și furnizorii își asumă și angajează întreaga responsabilitate.

1. Materializat prin: instructaje de securitate pentru angajați (ISA); verificări privind cunoștințele de securitate ale angajaților (VCSA).

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

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

## ARTICOLUL 10

**Conștientizarea și instruirea utilizatorilor [A18]**

## (1) Cerințe de securitate

[A181]. Instrumente de conștientizare. OSE pune la dispoziția angajaților instrumente necesare pentru conștientizarea și educarea acestora cu privire la tipurile de amenințări de securitate informatică și măsurile de protecție corespunzătoare.

[A182]. Instruirea și prezentarea securității. OSE instituie un program de prezentare a securității pentru tot personalul, precum și un program de instruire în domeniul securității pentru angajații care utilizează rețelele și sisteme informatice.

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

## ARTICOLUL 11

**Gestionarea activelor [A19]**

## (1) Cerințe de securitate

[A191]. Inventarierea și gestionarea activelor. OSE stabilește un cadru adecvat pentru identificarea, clasificarea și

implementarea unui inventar al proceselor IT, sistemelor și elementelor componente ale rețelelor și sistemelor informatice. În baza gestionării activelor, OSE lansează actualizări și patch-uri și, după caz, stabilește ce elemente din componența rețelelor și sistemelor informatice sunt afectate de noi probleme de securitate.

1. Pentru identificarea amenințărilor, vulnerabilităților și riscurilor sunt identificate activele, sistemele și procesele organizației, care se materializează printr-o listă.

2. OSE elaborează o procedură pentru etichetarea și clasificarea datelor și informațiilor pentru a reflecta sensibilitatea acestora și, în consecință, se asigură că aceasta este respectată, iar datele/informațiile sunt gestionate corespunzător.

(2) Indicatori de control. LASPO; PRECDI.

## SECȚIUNEA a 2-a

**Managementul ecosistemului [A2]**

## ARTICOLUL 12

**Cartografierea ecosistemului [A21]**

## (1) Cerințe de securitate

[A211]. Descrierea ecosistemului. OSE stabilește o cartografiere a ecosistemului, inclusiv a părților interesate interne și 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 situație cartografică a ecosistemului.

2. Scopul cartografierii este identificarea și evaluarea riscurilor potențiale reprezentate de relațiile cu părțile interesate ale ecosistemului și identificată printr-o listă a riscurilor potențiale identificate și evaluarea efectului acestora asupra furnizării serviciilor esențiale.

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

- maturitatea. Care sunt capacitățile tehnice ale părților interesate cu privire la securitatea cibernetică?
- încrederea. Pot presupune că intențiile părților interesate față de mine sunt fiabile?

- nivelul de acces. Care sunt drepturile de acces ale părților interesate la rețelele și sistemele informatice?
- dependența. În ce măsură relația cu părțile interesate este critică pentru activitatea mea?

(2) Indicatori de control. SICAE; LIRIE.

## ARTICOLUL 13

**Relațiile ecosistemului [A22]**

## (1) Cerințe de securitate

[A221]. Stabilirea relațiilor ecosistemului. OSE elaborează și implementează o procedură de stabilire a relațiilor ecosistemului, care include interconexiunile (relațiile externe) între rețelele și sisteme informatice și terți. În general, cerințele de securitate trebuie luate în considerare pentru componentele rețelelor și sistemelor informatice operate de terți.

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

(2) Indicatori de control. PROSRE; LASMA.



## CAPITOLUL III

**Protecție [B]**

## SECȚIUNEA 1

**Managementul arhitecturii [B1]**

## ARTICOLUL 14

**Managementul configurației rețelelor și sistemelor informatice [B11]**

## (1) Cerințe de securitate

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

[B112]. Instalarea echipamentelor și serviciilor. OSE instalează numai servicii și funcționalități sau conectează echipamente care sunt esențiale pentru funcționarea și securitatea rețelelor și sistemelor informatice. Evidența serviciilor, funcționalităților și echipamentelor este evidențiată în ARNIS.

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

2. ARNIS va fi actualizată permanent în funcție de componentele suplimentare implementate la nivelul securității rețelelor și sistemelor informatice.

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

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

## ARTICOLUL 15

**Managementul suporturilor de memorie externă [B12]**

## (1) Cerințe de securitate

[B121]. Suporturi de memorie externă. OSE va adopta o procedură privind utilizarea suporturilor de memorie externă. Aceasta va cuprinde modul de utilizare, principiile și măsuri de securitate atât pentru dispozitive mobile, cât și pentru suporturi de memorie externă.

1. Suporturile de scris amovibile conectate la rețelele și sistemele informatice sunt utilizate exclusiv pentru operațiuni legate de furnizarea serviciului esențial și/sau funcționarea rețelelor și sistemelor informatice, inclusiv pentru întreținerea, administrarea și asigurarea securității rețelelor și sistemelor informatice.

2. La NIS vor fi conectate numai suporturi amovibile înregistrate, în registre de evidență a suporturilor de memorie externă, fiind monitorizat accesul în rețelele și sistemele informatice.

(2) Indicatori de control. PRUSME; RESME.

## ARTICOLUL 16

**Segregarea și segmentarea rețelelor și sistemelor informatice [B13]**

## (1) Cerințe de securitate

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

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

2. OSE stabilește și pune în aplicare măsuri de securitate adecvate pentru interconectări ale rețelelor și sistemelor informatice.

(2) Indicatori de control. PROSES; SANIS.

## ARTICOLUL 17

**Filtrarea traficului [B14]**

## (1) Cerințe de securitate

[B141]. Filtrarea fluxurilor. OSE definește, implementează și actualizează permanent procedura privind filtrarea traficului, prin care stabilește reguli de filtrare a traficului (pe baza adresei de rețea, după numărul portului, pe bază de protocoale de comunicații etc.) pentru restrângerea fluxurilor de trafic.

1. OSE interzice fluxurile de trafic care nu sunt necesare pentru funcționarea rețelelor și sistemelor informatice și care ar putea facilita un atac cibernetic.

2. OSE filtrează fluxurile de intrare, cele existente și fluxurile între subsistemele rețelelor și sistemelor informatice la nivelul interconectării lor, limitând astfel fluxurile numai la cele strict necesare funcționării și asigurării securității rețelelor și sistemelor informatice.

(2) Indicatori de control. PROFIT; ARNIS.

## ARTICOLUL 18

**Asigurarea protecției produselor și serviciilor aferente rețelelor și sistemelor informatice [B15]**

## (1) Cerințe de securitate

[B151]. Asigurarea protecției criptografice. Pentru a asigura confidențialitatea, integritatea și autenticitatea datelor procesate, stocate sau tranzitate prin rețelele și sistemele informatice, OSE va stabili, implementa și menține o procedură pentru asigurarea protecției criptografice pentru informații și resurse.

1. Măsurile criptografice se aplică în toate etapele ciclului de viață a informației și au ca obiect de aplicare aplicațiile, sistemele informatice, echipamentele de rețea și canalele de comunicare.

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

(2) Indicatori de control. PRAPC; MACC.

## ARTICOLUL 19

**Protecția împotriva malware [B16]**

## (1) Cerințe de securitate

[B161]. Protecție malware. OSE va stabili măsuri de protecție malware și va implementa mijloace de control pentru detecția, prevenirea și recuperarea informației în scopul protecției împotriva atacurilor malware.

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

2. Echipamentele hardware, sistemele de operare, aplicațiile software și subsistemele rețelelor și sistemelor informatice trebuie configurate și protejate corespunzător atât împotriva atacurilor fizice, cât și logice.

(2) Indicatori de control. PRAPMA.

## SECȚIUNEA a 2-a

**Managementul administrării [B2]**

## ARTICOLUL 20

**Administrarea conturilor [B21]**

## (1) Cerințe de securitate

[B211]. Conturi de administrare. OSE stabilește conturi de administrare destinate numai persoanelor responsabile de efectuarea operațiunilor de administrare (instalare, configurare, întreținere, supraveghere etc.) a resurselor rețelelor și sistemelor informatice. Lista conturilor de administrare va fi actualizată permanent.

1. Permisunile administratorilor sunt individualizate și restricționate la perimetrul funcțional și tehnic al fiecărui administrator.

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

3. Operațiunile de administrare a rețelelor și sistemelor informatice sunt realizate exclusiv de pe conturile de administrator.

(2) Indicatori de control. LICA.

#### ARTICOLUL 21

##### Administrarea rețelelor și sistemelor informatice [B22]

(1) Cerințe de securitate

[B221]. Utilizarea sistemelor de administrare. OSE stabilește și aplică procedura privind utilizarea sistemelor informatice de administrare utilizate pentru operațiuni de administrare a NIS, respectând cel puțin regulile:

1. Resursele hardware și software ale SIA sunt utilizate exclusiv pentru efectuarea operațiunilor de administrare.

— Când motivele tehnice sau organizaționale o justifică, SIA poate fi utilizată pentru a efectua alte operațiuni decât cele administrative. În acest caz, trebuie să fie puse în aplicare mecanismele de protecție a sistemului de operare și a compartimentării mediilor de lucru, pentru a permite izolarea mediului „utilizator” față de „administrator”.

2. Mediul de lucru „administrator” folosit pentru operațiuni de administrare nu trebuie utilizat și 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 funcții decât operațiuni de administrare a rețelelor și sistemelor informatice.

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

5. SIA sunt conectate la resursele rețelelor și sistemelor informatice printr-o legătură de rețea fizică folosită exclusiv pentru operațiunile de administrare. Resursele rețelelor și sistemelor informatice sunt administrate prin interfața lor de administrare fizică.

— Când motivele tehnice împiedică administrarea unei resurse a rețelelor și sistemelor informatice printr-o legătură de rețea fizică sau prin interfața 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 și justificările acestora în MANIS.

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

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

7. Jurnalul care înregistrează evenimentele generate de resursele SIA nu conțin 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 și nu este stocată sub această formă în niciun moment.

1. Evidența parolelor de administrare se păstrează, în plic închis și sigilat [PPSIA], la componenta de securitate sau administrare a rețelelor și sistemelor informatice.

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

#### ARTICOLUL 22

##### Managementul accesului de la distanță [B23]

(1) Cerințe de securitate

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

1. PROLD va cuprinde modurile de realizare, măsurile de securitate aferente pentru protejarea resurselor și a informațiilor accesate, prelucrate și stocate din și în locațiile în care se lucrează la distanță.

2. Când furnizarea serviciului esențial necesită ca rețelele și sistemele informatice să fie accesibile printr-o rețea publică, operatorul protejează accesul prin intermediul unor mecanisme criptografice, în conformitate cu MS-B15.

(2) Indicatori de control. PROLD; PRAPC.

#### SECȚIUNEA a 3-a

##### Managementul identității și accesului [B3]

#### ARTICOLUL 23

##### Managementul identificării și autentificării utilizatorilor [B31]

(1) Cerințe de securitate

[B311]. Identificarea utilizatorilor. Pentru identificare, OSE stabilește și ține evidența conturilor unice pentru utilizatori sau pentru procesele automatizate care trebuie să acceseze resursele rețelelor și sistemelor informatice.

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

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

3. Atunci când acest lucru nu este posibil din motive tehnice sau operaționale, OSE dezvoltă un set de măsuri de trasabilitate și reducere a riscurilor și 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 definește regulile de gestionare a certificatelor de autentificare la rețelele și sistemele informatice.

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

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

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

#### ARTICOLUL 24

##### Managementul drepturilor de acces [B32]

(1) Cerințe 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 își îndeplinească atribuțiile, iar procesul automatizat să își desfășoare operațiunile tehnice.

1. În acordarea drepturilor de acces, OSE aplică principiul necesității de a cunoaște și principiul celui mai mic privilegiu.

2. OSE definește drepturile de acces la multiplele funcționalități ale rețelelor și sistemelor informatice și alocă aceste drepturi de acces strict utilizatorilor/proceselor automatizate care au o necesitate clară.

3. Cel puțin o dată pe an, OSE examinează atribuirea drepturilor de acces, identificând legăturile dintre conturi, drepturile de acces asociate și resursele sau funcționalitățile care sunt accesate prin drepturile de acces, și păstrează

actualizată o listă a conturilor privilegiate pe nivele de acces și funcționalități accesabile.

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

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

#### SECȚIUNEA a 4-a

### Managementul mentenanței [B4]

#### ARTICOLUL 25

##### Mentenanța rețelelor și sistemelor informatice [B41]

(1) Cerințe de securitate

[B411]. Menținere securitate. OSE elaborează și implementează o procedură pentru menținerea securității rețelelor și sistemelor informatice, în conformitate cu PONIS.

1. În acest scop, procedura:

— definește condițiile care permit menținerea 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 informații despre vulnerabilități și măsuri corective de securitate care privesc resursele rețelelor și sistemelor informatice (hardware și software).

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

1. OSE verifică originea și integritatea versiunii înainte de instalarea acesteia (conform calendarului definit în PROMNIS) și analizează impactul tehnic și operațional al versiunii respective asupra securității rețelelor și sistemelor informatice.

2. În unele cazuri justificate, din motive tehnice sau operaționale, 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, și descrie în MANIS măsurile luate, precum și motivele care au justificat să nu instaleze versiunea acceptată.

[B413]. Protejare resurse. OSE protejează accesul la resursele rețelelor și sistemelor informatice atunci când accesul se face din rețele terțe.

1. În acest caz, OSE protejează prin criptare și mecanisme de autentificare accesul la rețelele și sistemele informatice, ține evidența echipamentelor utilizate pentru accesarea rețelelor și sistemelor informatice și, de asemenea, gestionează și configurează aceste echipamente.

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

#### ARTICOLUL 26

##### Sisteme de control industrial.

##### SCADA — Monitorizare, control și achiziții de date [B42]

(1) Cerințe de securitate

[B421]. Sisteme de control industriale. Multe servicii esențiale depind de sisteme de control industriale, funcționale și sigure. Dacă este cazul, OSE ia în considerare cerințele de securitate specifice pentru ISC.

1. Abordarea clasică a tehnologiei informației (axată pe transferul și accesul de/la informații) ar putea fi înlocuită cu o abordare tehnologică operațională (hardware și software — utilizate pentru detectarea modificării unui proces fizic).

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

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

(2) Indicatori de control. CEISC; ANISMS.

#### SECȚIUNEA a 5-a

### Managementul securității fizice [B5]

#### ARTICOLUL 27

##### Asigurarea protecției fizice a rețelelor și sistemelor informatice [B51]

(1) Cerințe de securitate

[B511]. Acces la resurse. OSE previne accesul fizic neautorizat, deteriorarea și interferența la informațiile și facilitățile de procesare a informațiilor în rețelele și sistemele informatice.

1. În acest sens, OSE elaborează și aplică o procedură privind accesul și securitatea resurselor și informațiilor.

(2) Indicatori de control. PRASI

#### CAPITOLUL IV

### Apărare cibernetică [C]

#### SECȚIUNEA 1

### Managementul detecției [C1]

#### ARTICOLUL 28

##### Managementul vulnerabilităților și alertelor de securitate [C11]

(1) Cerințe de securitate

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

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

— Măsurile organizatorice includ procedurile de operare pentru dispozitivele de detectare și descriu lanțul de procesare pentru evenimentele de securitate identificate de aceste dispozitive.

— Măsurile tehnice specifică natura și poziționarea dispozitivelor de detectare.

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

— Dispozitivele de detecție analizează fluxurile de date care tranzitează rețelele și sistemele informatice pentru a identifica evenimente care ar putea afecta rețelele și sistemele informatice.

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

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

1. Pentru limitarea riscurilor de securitate și corectarea vulnerabilităților, OSE va implementa un program pentru managementul vulnerabilităților, 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; PGMVU; ARNIS.

#### ARTICOLUL 29

##### Înregistrarea evenimentelor [C12]

(1) Cerințe de securitate

[C121]. Monitorizare evenimente. OSE pune în aplicare un sistem de înregistrare evenimente la nivelul rețelelor și sistemelor informatice pentru evenimente legate de autentificarea utilizatorului, conturilor și gestionării drepturilor de acces, accesului la resurse, modificărilor regulilor NIS și funcționării rețelelor și 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 și arhivate pentru o perioadă de cel puțin șase luni.

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

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

(2) Indicatori de control. SIENIS; SIEM.

#### ARTICOLUL 30

##### Jurnalizarea și asigurarea trasabilității activităților în cadrul rețelelor și sistemelor informatice [C13]

(1) Cerințe de securitate

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

1. SCAJ este instalat și funcționează pe un sistem informatic dedicat exclusiv în scopul detectării evenimentelor care ar putea afecta securitatea rețelelor și sistemelor informatice.

(2) Indicatori de control. SCAJ.

#### SECȚIUNEA a 2-a

##### Managementul incidentelor de securitate [C2]

#### ARTICOLUL 31

##### Răspuns la incidente de securitate [C21]

(1) Cerințe de securitate

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

[C212]. Monitorizarea incidentelor. OSE trebuie să implementeze un sistem de monitorizare și management al evenimentelor și incidentelor de securitate, bazat cel puțin pe un senzor de detectare a intruziunilor la nivel de rețea care beneficiază de o sursă perpetuă de indicatori de compromitere și pe analiza logurilor de pe echipamentele sau stațiile de lucru critice pentru desfășurarea activității, în vederea identificării abaterilor de la politicile de securitate și a intruziunilor.

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

1. OSE separă SIDGI de rețelele și sistemele informatice afectate de incident și păstrează registrele tehnice aferente pentru o perioadă de cel puțin o jumătate de an.

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

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

#### ARTICOLUL 32

##### Raport incidente [C22]

(1) Cerințe de securitate

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

(2) Indicatori de control. PRORIS.

#### ARTICOLUL 33

##### Comunicarea cu ANSRSI și CSIRT Național [C23]

(1) Cerințe de securitate

[C231]. Interconectare națională. OSE se interconectează la serviciul de alertare și cooperare al CERT-RO care îi permite să ia notă, fără întârziere, de informațiile transmise de CERT-RO, ca CSIRT Național, cu privire la incidente, vulnerabilități, amenințări și informații relevante.

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

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

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

1. OSE elaborează și actualizează permanent lista responsabililor NIS.

[C233]. Gestionare informații primite de la CERT-RO. OSE implementează o procedură pentru gestionarea informațiilor primite și, după caz, a măsurilor de securitate adoptate pentru protejarea rețelelor și sistemelor informatice.

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

#### CAPITOLUL V

##### Reziliență [D]

#### SECȚIUNEA 1

##### Managementul continuității afacerii [D1]

#### ARTICOLUL 34

##### Asigurarea disponibilității serviciului esențial și a funcționării rețelelor și sistemelor informatice [D11]

(1) Cerințe de securitate

[D111]. Asigurarea disponibilității. În conformitate cu PONIS, OSE definește o procedură privind managementul asigurării disponibilității serviciului esențial, în caz de incident de securitate cibernetică.

(2) Indicatori de control. PRADE.

#### ARTICOLUL 35

##### Managementul recuperării datelor în caz de dezastre [D12]

(1) Cerințe de securitate

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

(2) Indicatori de control. PROMRE.

SECȚIUNEA a 2-a  
**Managementul crizelor [D2]**

## ARTICOLUL 36

**Organizarea gestionării crizelor [D21]**

## (1) Cerințe de securitate

[D211]. Organizarea gestionării crizelor cibernetice. OSE definește în PONIS sau separat o procedură privind organizarea gestionării crizelor în caz de incidente de securitate cibernetică pentru asigurarea continuității activităților organizaționale.

## (2) Indicatori de control. PROCIS.

## ARTICOLUL 37

**Procesul de gestionare a crizelor [D22]**

## (1) Cerințe de securitate

[D221]. Gestionarea crizelor cibernetice. OSE definește în PONIS sau separat procesele de gestionare a crizelor pe care le va implementa în caz de incidente de securitate cibernetică pentru asigurarea continuității activităților organizaționale.

## (2) Indicatori de control. PEGEC.

## CAPITOLUL VI

**Dispoziții finale**

## ARTICOLUL 38

**Obligații privind implementarea cerințelor minime de securitate**

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

(2) După implementarea cerințelor minime de asigurare a securității rețelelor și sistemelor informatice și intrarea în conformitate, OSE va informa ANSRSI, prin canalele de comunicare cunoscute (NIS@cert.ro).

## ARTICOLUL 39

**Aplicarea legilor speciale**

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

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

## ARTICOLUL 40

**Solicitările autorității naționale**

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

## ARTICOLUL 41

**Corespondență privind implementarea și auditarea cerințelor minime de securitate**

Grila de corespondență privind implementarea și auditarea cerințelor minime de securitate este prevăzută în anexa nr. 2.

## ARTICOLUL 42

**Anexe la normele tehnice**

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

ANEXA Nr. 1  
la Normele tehnice

**G L O S A R****Termeni și abrevieri**

*ANSRSI* — autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice

*ARNIS* — analiza riscurilor de securitate a rețelelor și sistemelor informatice, document elaborat la nivelul OSE, prin care sunt identificate elementele critice care stau la baza furnizării serviciului esențial și sunt identificate principalele riscuri în vederea gestionării și diminuării acestora

*ANISMS* — analiza riscurilor de securitate și implementarea măsurilor de securitate pentru limitarea accesului neautorizat

*ATECNIS* — analiză tehnică cu privire la compromiterea securității rețelelor și sistemelor informatice

*CEISC* — cerințe 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* — evidența conturilor pentru utilizatori și pentru procesele automatizate

*IEC* — indicatori de evaluare, pe baza cărora OSE își evaluează conformitatea cu PONIS

*INCEA* — instrumente necesare pentru conștientizarea și educarea angajaților cu privire la tipurile de amenințări de securitate informatică și măsurile de protecție 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 și ținute sub formă electronică sau pe hârtie.

*LASMA* — listă cu acorduri la nivel de serviciu și/sau mecanisme de audit a rețelelor și sistemelor informatice

*LASPO* — lista activelor, sistemelor și proceselor organizației

*LICA* — lista conturilor de administrare

*LICPA* — lista conturilor privilegiate pe nivele de acces și funcționalități accesabile

*LIRIE* — lista riscurilor potențiale identificate și evaluarea acestora în furnizarea serviciilor esențiale. Riscurile sunt reprezentate de relațiile cu părțile interesate ale ecosistemului

*LIRNIS* — lista responsabililor NIS

*MACC* — managementul cheilor de criptare; proces prin care se asigură producerea, utilizarea și evidența 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 și procese automatizate la resursele rețelelor și sistemelor informatice

*MEGRE* — metodologie de gestionare a riscurilor furnizării serviciilor esențiale, document prin care este prezentat procesul de evaluare a riscurilor operatorului economic, criteriile de analiză, de acceptare și de reducere a riscurilor

*MEIEC* — metoda de evaluare a indicatorilor de conformitate

*NIS* — rețele și sisteme informatice

*OSE* — operator de servicii esențiale

*PEANIS* — procesul de acreditare stabilit în PONIS prin care OSE acreditează NIS utilizate în furnizarea serviciilor esențiale, inclusiv componentele de administrare

**PEGEC** — procese de gestionare a crizelor; documente prin care OSE stabilește procesele și modurile de implementare în caz de incidente de securitate cibernetică pentru asigurarea continuității activităților organizaționale

**PEIREV** — proces de identificare, clasificare, remediere și eliminare a vulnerabilităților, în special în software și firmware, la nivelul rețelelor și sistemelor informatice

**PGMAVU** — program pentru managementul vulnerabilităților în rețelele și sistemele informatice

**PONIS** — politica de securitate a rețelelor și sistemelor informatice care asigură furnizarea serviciilor esențiale

**PPSIA** — plicul cu parole utilizate pentru sisteme informatice de administrare a rețelelor și sistemelor informatice

**PRADE** — procedură privind managementul asigurării disponibilității serviciului esențial, în caz de incident de securitate cibernetică

**PRAPC** — procedură pentru asigurarea protecției criptografice pentru informații și resurse

**PRAPMA** — procedură pentru asigurarea protecției malware

**PRASA** — program de prezentare a securității pentru tot personalul

**PRASI** — procedură privind accesul și securitatea resurselor și informațiilor

**PGASP** — program de asigurare a securității personalului; document prin care OSE identifică obiective și stabilește cerințe de securitate pentru fiecare etapă a relației avute de către angajați

**PRECAS** — procedură privind evaluarea conformității NIS și efectuarea auditului de securitate a rețelelor și sistemelor informatice

**PRECDI** — procedură privind etichetarea și clasificarea datelor și informațiilor

**PRIMSA** — procedură pentru gestionarea informațiilor primite și, după caz, a măsurilor de securitate adoptate pentru protejarea NIS

**PRISA** — program de instruire în domeniul securității pentru angajații care utilizează rețelele și sistemele informatice care stau la baza furnizării serviciilor esențiale

**PRISAC** — procedură de interconectare la serviciul de alertare și cooperare al CERT-RO

**PROCIS** — procedură privind organizarea gestionării crizelor în caz de incidente de securitate cibernetică pentru asigurarea continuității activităților organizaționale

**PRODAIS** — procedură pentru detectarea incidentelor de securitate care afectează rețelele și sistemele informatice

**PROFIT** — procedură privind filtrarea traficului

**PROLD** — procedură privind lucrul la distanță

**PROMNIS** — procedură pentru menținerea securității rețelelor și sistemelor informatice

**PROMRE** — procedură privind managementul recuperării datelor în caz de dezastre, precum și în caz de incidente severe de securitate cibernetică

**PRORAI** — procedură pentru gestionarea, răspunsul și analiza incidentelor care afectează funcționarea sau securitatea rețelelor și sistemelor informatice

**PRORIS** — procedură pentru raportarea incidentelor de securitate

**PRORUVI** — procedură pentru reducerea riscurilor legate de utilizarea unei versiuni învechite

**PROSES** — procedură privind segregarea și segmentarea rețelelor și sistemelor informatice utilizate pentru furnizarea serviciilor esențiale

**PROSRE** — procedură de stabilire a relațiilor ecosistemului; documentul include interconexiunile (relațiile externe) între rețelele și sistemele informatice și terți

**PRUSIA** — procedură privind utilizarea sistemelor informatice de administrare

**PRUSME** — procedură privind utilizarea suporturilor de memorie externă

**RAEC** — raport de evaluare a conformității

**RAIPOD** — raport privind implementarea politicii de securitate a rețelelor și sistemelor informatice care asigură furnizarea serviciilor esențiale și a documentelor de aplicare a acestora

**RASNIS** — raport de audit de securitate a rețelelor și sistemelor informatice

**RATES** — raport de testare și evaluare a securității rețelelor și sistemelor informatice

**RERO** — registrul de risc organizațional

**RESME** — registre de evidență a suporturilor de memorie externă

**SACNIS** — serviciul de alertare și cooperare al CERT-RO

**SANIS** — schema arhitecturii rețelelor și sistemelor informatice folosite la furnizarea serviciilor esențiale

**SCAJ** — sistem de corelație și analiză de jurnal

**SIA** — sisteme informatice de administrare a rețelelor și sistemelor informatice

**SICAE** — situația cartografică a ecosistemului; document prin care se realizează stabilirea și identificarea ecosistemului care stă la baza furnizării serviciului esențial atât NIS, cât și alte componente. De asemenea include, dar fără a se limita la acestea, părți interesate, interne și externe, și 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 și identificării rapide a principalelor cauze de afectare a securității, precum și ale încălcării politicilor de securitate

**SIENIS** — sistem de înregistrare evenimente la nivelul rețelelor și sistemelor informatice

**SIVMOC** — sistem de verificare a potențialelor modificări ale unui cont privilegiat

**SMMEIS** — sistem de monitorizare și management al evenimentelor și incidentelor de securitate

**SMSI** — sistemul de management al securității informației

**SNIS** — securitatea rețelelor și sistemelor informatice

*ANEXA Nr. 2  
la Normele tehnice*

### GRILA DE CORESPONDENȚĂ privind implementarea și auditarea cerințelor minime de securitate

Domenii de securitate [D]		Categorii de activități de securitate [C]		Măsurile de securitate [MS]		Cerințe de securitate [CS]		Indicatori de control [IC]	
Denumire	ID	Denumire	ID	Denumire	ID	Denumire	ID	Denumire	ID
GVERNANȚĂ	A	Managementul securității informației	A1	Analizarea și 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

Domenii de securitate [D]		Categorii de activități de securitate [C]		Măsurile de securitate [MS]		Cerințele de securitate [CS]		Indicatorii de control [IC]		
Denumire	ID	Denumire	ID	Denumire	ID	Denumire	ID	Denumire	ID	
				Acreditarea de securitate	A13	Acreditarea rețelelor și 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 securității	A142	MEIEC	I11	
				Verificarea conformității cu privire la securitatea informației. Audit de securitate	A15	Evaluarea conformității	A151	PRECAS	I12	
						Auditul de securitate	A152	RASNIS	I14	
				Testarea și evaluarea securității rețelelor și sistemelor informatice	A16	Testare și evaluare securitate	A161	RATES	I15	
								ATECNIS	I16	
				Asigurarea securității personalului	A17	Asigurarea securității personalului	A171	PRASP	I17	
								FP	I18	
								CIM	I19	
						Verificarea înțelegerii responsabilităților	A172	CCM	I20	
	ISA	I21								
	VCSA	I22								
	Conștientizarea și instruirea utilizatorilor	A18	Instrumente de conștientizare	A181	INCEA	I24				
			Instruirea și prezentarea securității	A182	PRASA	I25				
	Gestionarea activelor	A19	Inventarierea și gestionarea activelor	A191	PRISA	I26				
					LASPO	I27				
	Managementul ecosistemului	A2	Cartografierea ecosistemului	A21	PRECDI	I28				
					SICAE	I29				
			Relațiile ecosistemului	A22	LIRIE	I30				
	PROTECȚIE	B	Managementul arhitecturii	B1	Managementul configurației rețelelor și sistemelor informatice	B11	Stabilirea relațiilor ecosistemului	A221	PROSRE	I31
							Arhitectura NIS	B111	LASMA	I32
					Instalarea echipamentelor și serviciilor	B112	Acorduri la nivel de serviciu	A222	SANIS	I33
							ARNIS	I01		
					Managementul suporturilor de memorie externă	B12	Suporturi de memorie externă	B121	MANIS	I09
									PRUSME	I34
Segregarea și segmentarea rețelelor și sistemelor informatice					B13	Segregarea și segmentarea	B131	RESME	I35	
								PROSES	I36	
Filtrarea traficului					B14	Filtrarea fluxurilor	B141	SANIS	I33	
								PROFIT	I37	
Asigurarea protecției produselor și serviciilor aferente rețelelor și sistemelor informatice					B15	Asigurarea protecției criptografice	B151	ARNIS	I01	
						Managementul cheilor de criptare	B152	PRAPC	I38	
Protecția împotriva malware					B16	Protecție malware	B161	MACC	I39	
								PRAPMA	I40	
Managementul administrării					B2	Administrarea conturilor	B21	Conturi de administrare	B211	LICA
	Utilizarea sistemelor de administrare	B221	PRUSIA	I42						
	Administrarea rețelelor și sistemelor informatice	B22	PONIS	I04						
			Parole administrare	B222		JIERU	I43			
	Managementul accesului de la distanță	B23	Lucrul la distanță	B231		PPSIA	I44			
						PROLD	I45			
Managementul identității și accesului	B3	Managementul identificării și autentificării utilizatorilor	B31	PRAPC	I38					
				Identificarea utilizatorilor	B311	ECUPA	I46			
		Managementul drepturilor de acces	B32	Autentificarea utilizatorilor	B312	ARNIS	I01			
				Acordarea drepturilor de acces	B321	MANIS	I09			
				Verificarea conturilor privilegiate	B322	MEAUP	I47			
Managementul mentenanței	B4	Mentenanța rețelelor și sistemelor informatice	B41	PONIS	I04					
				LICPA	I48					
PROMNIS	I50									

Domenii de securitate [D]		Categoriile de activități de securitate [C]		Măsurile de securitate [MS]		Cerințele de securitate [CS]		Indicatorii de control [IC]			
Denumire	ID	Denumire	ID	Denumire	ID	Denumire	ID	Denumire	ID		
				Sisteme control industrial. SCADA — Monitorizare, control și achiziții de date	B42	Actualizare resurse	B412	PRORUVI	151		
								PONIS	104		
								MANIS	109		
				Protejare resurse	B413	PRAPC	138				
				Sisteme de control industriale	B421	CEISC	152				
				Limitarea accesului	B422	ANISMS	153				
		Managementul securității fizice	B5	Asigurarea protecției fizice a rețelelor și sistemelor informatice	B51	Acces la resurse	B511	PRASI	154		
		APĂRARE CIBERNETICĂ	C	Managementul detecției	C1	Managementul vulnerabilităților și alertelor de securitate	C11	Fluxul alertelor de securitate	C111	PRODIS	155
										SIENIS	156
										MANIS	109
Evaluarea și monitorizarea vulnerabilităților	C112					PEIREV	157				
						PGMAVU	158				
						ARNIS	101				
Înregistrarea evenimentelor	C12			Monitorizare evenimente	C121	SIENIS	156				
				Sisteme de management	C122	SIEM	159				
Jurnalizarea și asigurarea trasabilității activităților în cadrul rețelelor și sistemelor informatice	C13			Jurnalizare și trasabilitate	C131	SCAJ	144				
Managementul incidentelor de securitate	C2			Răspuns la incidente de securitate	C21	Fluxul incidentelor	C211	PRORAI	160		
								Monitorizarea incidentelor	C212	SMMEIS	161
								Gestionarea incidentelor	C213	SIDGI	162
				Raport incidente	C22	Raportarea incidentelor	C221	PRORIS	163		
				Comunicarea cu Autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice (ANSRSI) și CSIRT Național	C23	Interconectare națională	C231	PISAC	164		
						Responsabili NIS	C232	LIRNIS	165		
Gestionare informații primite de la CERT-RO	C233	PRIMSA	166								
REZILIENȚĂ	D	Managementul continuității afacerii	D1	Asigurarea disponibilității serviciului esențial și a funcționării rețelelor și sistemelor informatice	D11	Asigurarea disponibilității	D111	PRADE	167		
				Managementul recuperării datelor în caz de dezastre	D12	Recuperarea datelor	D121	PROMRE	168		
		Managementul crizelor	D2	Organizarea gestionării crizelor	D21	Organizarea gestionării crizelor cibernetice	D211	PROCIS	169		
				Procesul de gestionare a crizelor	D22	Gestionarea crizelor cibernetice	D221	PEGEC	170		

EDITOR: PARLAMENTUL ROMÂNIEI — CAMERA DEPUTAȚILOR



„Monitorul Oficial” R.A., Str. Parcului nr. 65, sectorul 1, București; C.I.F. RO427282,  
IBAN: RO55RNCB0082006711100001 Banca Comercială Română — S.A. — Sucursala „Unirea” București  
și IBAN: RO12TREZ7005069XXX000531 Direcția de Trezorerie și Contabilitate Publică a Municipiului București  
(alocat numai persoanelor juridice bugetare)

Tel. 021.318.51.29/150, fax 021.318.51.15, e-mail: marketing@ramo.ro, internet: www.monitoruloficial.ro

Adresa pentru publicitate: Centrul pentru relații cu publicul, București, șos. Panduri nr. 1,  
bloc P33, parter, sectorul 5, tel. 021.401.00.73, fax 021.401.00.71 și 021.401.00.72

Tiparul: „Monitorul Oficial” R.A.



5 948493 253006