Republica Moldova

GUVERNUL

HOTĂRÂRE Nr. HG483/2026
din 26.08.2026

cu privire la aprobarea cadrului metodologic privind evaluarea riscurilor la adresa infrastructurilor critice naționale, planurile de securitate ale gestionarilor infrastructurilor critice naționale și ofițerul de legătură pentru securitatea infrastructurii critice naționale

Publicat : 22.09.2026 în MONITORUL OFICIAL Nr. 466-469 art. 525 Data intrării în vigoare

În temeiul art. 7 alin. (2) lit. b) din Legea nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale (Monitorul Oficial al Republicii Moldova, 2025, nr.445-447, art. 608), Guvernul HOTĂRĂȘTE:

1. Se aprobă cadrul metodologic privind evaluarea riscurilor la adresa infrastructurilor critice naționale, planurile de securitate ale gestionarilor infrastructurilor critice naționale și ofițerul de legătură pentru securitatea infrastructurii critice naționale, după cum urmează:

1.1. Normele metodologice privind evaluarea riscurilor la adresa infrastructurilor critice naționale, conform anexei nr. 1;

1.2. Normele metodologice privind elaborarea, avizarea și aprobarea Planului de securitate al gestionarului infrastructurii critice naționale, conform anexei nr. 2;

1.3. Structura-cadru a Planului de securitate al gestionarului infrastructurii critice naționale, conform anexei nr. 3;

1.4. Normele metodologice privind echivalarea documentelor existente cu Planul de securitate al gestionarului infrastructurii critice naționale, conform anexei nr. 4;

1.5. Normele metodologice privind revizuirea și actualizarea Planului de securitate al gestionarului infrastructurii critice naționale, conform anexei nr. 5;

1.6. Normele metodologice privind desemnarea, statutul funcțional și atribuțiile ofițerului de legătură pentru securitatea infrastructurii critice naționale, conform anexei nr. 6.

2. Ministerul Afacerilor Interne, prin intermediul Centrului Național de Coordonare a Protecției Infrastructurilor Critice, asigură coordonarea metodologică, monitorizarea și suportul de specialitate pentru aplicarea prezentei hotărâri.

3. În sensul prezentei hotărâri, autoritățile publice responsabile sunt autoritățile desemnate prin Hotărârea Guvernului nr. 185/2026 cu privire la desemnarea autorităților publice responsabile de sectoarele și subsectoarele infrastructurii critice naționale.

4. Autoritățile publice responsabile aplică prevederile prezentei hotărâri în sectoarele și subsectoarele aflate în responsabilitatea lor, avizează planurile de securitate ale gestionarilor infrastructurilor critice naționale și monitorizează conformarea acestora cu cerințele legale și metodologice.

5. Gestionarii infrastructurilor critice naționale asigură elaborarea, aprobarea, transmiterea spre avizare, implementarea, testarea, revizuirea și actualizarea planurilor de securitate, în condițiile Legii nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale și ale cadrului metodologic aprobat prin prezenta hotărâre.

6. Documentele existente ale gestionarilor infrastructurilor critice naționale, care reglementează măsuri de securitate, continuitate, protecție fizică, securitate cibernetică, răspuns la incidente, protecție civilă sau alte măsuri relevante, pot fi recunoscute ca echivalente ale Planului de securitate al gestionarului infrastructurii critice naționale, integral sau parțial, în condițiile stabilite de prezenta hotărâre.

7. Autoritățile publice responsabile elaborează instrucțiuni sectoriale, ghiduri, modele de documente sau proceduri interne necesare pentru aplicarea prezentei hotărâri în sectoarele și subsectoarele aflate în responsabilitatea lor, cu respectarea cadrului metodologic aprobat prin prezenta hotărâre și cu informarea Centrului Național de Coordonare a Protecției Infrastructurilor Critice.

8. În cazul în care, pentru același sector sau subsector al infrastructurii critice naționale, sunt desemnate două sau mai multe autorități publice responsabile, obligațiile prevăzute la pct. 4 și 7 se exercită de fiecare autoritate în limitele competențelor sale legale și pentru domeniul aflat în responsabilitatea sa. Pentru aspectele comune, interdependente sau care vizează întregul sector ori subsector, autoritățile publice responsabile asigură coordonarea acțiunilor, schimbul de informații și, după caz, elaborarea în comun a instrucțiunilor sectoriale, a ghidurilor, a modelelor de documente sau a procedurilor necesare pentru aplicarea prezentei hotărâri, cu informarea Centrului Național de Coordonare a Protecției Infrastructurilor Critice.

9. Ministerele, autoritățile administrative din subordinea ministerelor, alte autorități administrative centrale și instituțiile publice responsabile vor aduce actele normative departamentale, procedurile interne și documentele aplicabile în concordanță cu prevederile prezentei hotărâri, în termen de 12 luni de la data intrării în vigoare a acesteia, fără a afecta obligația gestionarilor infrastructurilor critice naționale de a elabora și a transmite spre avizare Planul de securitate în termenul prevăzut de cadrul metodologic aprobat prin prezenta hotărâre.

10. Controlul asupra executării prezentei hotărâri se pune în sarcina Ministerului Afacerilor Interne.

11. Prezenta hotărâre intră în vigoare la data publicării în Monitorul Oficial al Republicii Moldova.

PRIM-MINISTRU Vasile TOFAN

Contrasemnează:

Ministrul afacerilor interne Daniella Misail-Nichitin

Nr. 483. Chişinău, 26 august 2026.

Anexa nr. 1

la Hotărârea Guvernului nr. 483/2026

NORME

metodologice privind evaluarea riscurilor la adresa infrastructurilor critice naționale

I. DISPOZIȚII GENERALE

1. Prezentele Norme reglementează modul de organizare, de realizare, de documentare și de actualizare a procesului de evaluare a riscurilor la adresa infrastructurilor critice naționale.

2. Evaluarea riscurilor la adresa infrastructurilor critice naționale reprezintă procesul structurat prin care sunt identificate, analizate, evaluate, prioritizate, monitorizate și raportate riscurile care pot afecta infrastructura critică națională, funcțiile critice, activele critice, procesele esențiale sau continuitatea serviciului esențial furnizat prin intermediul acesteia.

3. Evaluarea riscurilor are drept scop fundamentarea măsurilor de securitate, protecție, prevenire, continuitate, răspuns și recuperare care urmează a fi incluse în Planul de securitate al gestionarului infrastructurii critice naționale (denumit în continuare *Plan de securitate*).

4. Prezentele Norme se aplică gestionarilor infrastructurilor critice naționale desemnate potrivit legii (denumiți în continuare *gestionari*), indiferent de forma de proprietate, de forma juridică de organizare sau de sectorul de activitate.

5. Prezentele Norme se aplică, în limitele competențelor legale, autorităților publice responsabile, autorităților competente și altor entități implicate în procesul de evaluare, avizare, monitorizare sau valorificare a rezultatelor evaluării riscurilor.

6. Evaluarea riscurilor se realizează pentru fiecare infrastructură critică națională

desemnată, ținând cont de specificul sectorului și al subsectorului, de serviciul esențial furnizat, de componentele critice, de amplasare, de mediul operațional, de dependențe, de interdependențe și de nivelul de expunere la amenințări și pericole.

7. Evaluarea riscurilor constituie baza obligatorie pentru elaborarea, actualizarea și revizuirea Planului de securitate.

8. Prezentele Norme se aplică fără a aduce atingere obligațiilor specifice prevăzute de legislația specială aplicabilă sectorului sau subsectorului respectiv, precum și de legislația în domeniul securității cibernetice, al protecției informațiilor, al situațiilor de criză, al protecției civile, al apărării împotriva incendiilor, al securității și sănătății în muncă, al prevenirii și controlului riscurilor de mediu sau de alte reglementări speciale aplicabile.

9. Aplicarea prezentelor Norme se realizează în baza următoarelor principii:

9.1. principiul legalității;

9.2. principiul abordării integrate;

9.3. principiul prevenirii;

9.4. principiul abordării bazate pe risc;

9.5. principiul proporționalității;

9.6. principiul continuității serviciilor esențiale;

9.7. principiul cooperării instituționale;

9.8. principiul trasabilității;

9.9. principiul confidențialității și protecției informațiilor;

9.10. principiul revizuirii periodice și al îmbunătățirii continue.

10. Noțiunile utilizate în prezentele Norme au semnificația prevăzută de Legea nr.223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale, precum și de actele normative în domeniile managementului riscurilor, securității naționale, securității cibernetice, situațiilor de criză și protecției informațiilor.

II. ORGANIZAREA PROCESULUI DE EVALUARE

A RISCURILOR

11. Evaluarea riscurilor se realizează de către gestionar, în cooperare cu autoritatea publică responsabilă din sectorul sau subsectorul de competență. Centrul Național de Coordonare a Protecției Infrastructurilor Critice (denumit în continuare *CNCPIC*) acordă, după caz, suport metodologic autorităților publice responsabile și gestionarilor pentru aplicarea prezentelor Norme.

12. Autoritatea publică responsabilă poate stabili cerințe suplimentare privind evaluarea riscurilor, cu respectarea cadrului metodologic aprobat prin prezenta hotărâre și cu informarea CNCPIC.

13. Procesul de evaluare a riscurilor se inițiază:

13.1. după desemnarea infrastructurii drept infrastructură critică națională;

13.2. la elaborarea Planului de securitate;

13.3. la actualizarea evaluării riscurilor;

13.4. după producerea unui incident major sau a unei perturbări semnificative;

13.5. în cazul modificării amenințărilor, vulnerabilităților, dependențelor sau interdependențelor relevante;

13.6. în cazul modificării configurației tehnice, funcționale, juridice sau organizaționale a infrastructurii critice naționale;

13.7. la solicitarea autorității publice responsabile sau a CNCPIC, în condițiile legii.

14. Gestionarul desemnează persoanele sau structurile responsabile de realizarea evaluării riscurilor.

15. În procesul de evaluare a riscurilor pot fi implicați, după caz, reprezentanți ai structurilor responsabile de securitatea fizică, de securitatea cibernetică, de continuitatea activității, de protecția civilă, de situațiile de urgență, de mentenanță, de exploatarea tehnică, de logistică, de resurse umane, de asigurare a cadrului juridic, comunicare și management operațional.

16. Pentru evaluarea riscurilor care necesită expertiză specializată, gestionarul sau autoritatea publică responsabilă poate solicita suportul unor experți ori al unor structuri competente, cu respectarea regimului de protecție a informațiilor sensibile sau clasificate.

III. OBIECTUL EVALUĂRII RISCURILOR

17. Obiectul evaluării riscurilor îl constituie infrastructura critică națională desemnată, în integralitatea sa funcțională, precum și serviciul esențial furnizat prin intermediul acesteia.

18. Evaluarea riscurilor vizează, după caz:

18.1. infrastructura, instalațiile, echipamentele, rețelele, sistemele și subsistemele aferente;

18.2. activele materiale și imateriale cu rol esențial;

18.3. funcțiile critice și procesele operaționale indispensabile;

18.4. personalul-cheie și competențele indispensabile;

18.5. sistemele informaționale, comunicațiile și alte componente digitale sau tehnologice;

18.6. furnizorii, prestatorii, lanțurile de aprovizionare și alte dependențe externe;

18.7. interdependențele cu alte infrastructuri critice, servicii esențiale ori sisteme publice sau private;

18.8. amplasamentele, nodurile, conexiunile și celelalte elemente fără de care serviciul esențial nu poate fi menținut sau reluat în termen acceptabil.

19. Obiectul evaluării se delimitează în mod expres în raport cu:

19.1. perimetrul fizic și funcțional al infrastructurii critice naționale;

19.2. serviciul sau serviciile esențiale furnizate;

19.3. parametrii minimi de funcționare acceptabili;

19.4. condițiile de continuitate, de funcționare degradată și de recuperare;

19.5. orizontul de analiză și ipotezele de lucru.

IV. ETAPELE EVALUĂRII RISCURILOR

20. Evaluarea riscurilor la nivelul gestionarului se realizează cel puțin prin următoarele etape:

20.1. delimitarea obiectului evaluării;

20.2. identificarea serviciului esențial, a funcțiilor critice, a activelor critice și a proceselor esențiale;

20.3. identificarea amenințărilor, a pericolelor, a hazardelor, a surselor și a declanșatorilor de risc;

20.4. identificarea vulnerabilităților;

20.5. identificarea dependențelor și a interdependențelor;

20.6. elaborarea scenariilor de risc;

20.7. estimarea impactului;

20.8. estimarea probabilității;

20.9. determinarea scorului și a nivelului de risc;

20.10. prioritizarea riscurilor;

20.11. identificarea măsurilor existente și evaluarea eficacității acestora, precum și identificarea și prioritizarea măsurilor suplimentare de tratare a riscurilor;

20.12. documentarea rezultatelor.

21. Etapele prevăzute la pct. 20 se aplică în mod proporțional cu natura infrastructurii critice naționale, complexitatea acesteia, sectorul de apartenență și nivelul riscurilor evaluate.

22. În etapa de identificare a funcțiilor critice, a activelor critice și a proceselor esențiale, gestionarul stabilește elementele indispensabile pentru asigurarea furnizării sau a reluării serviciului esențial prin intermediul infrastructurii critice naționale.

23. Pentru fiecare funcție critică se identifică cel puțin:

23.1. activele critice asociate;

23.2. procesele esențiale și fluxurile operaționale;

23.3. personalul-cheie și competențele indispensabile;

23.4. resursele logistice, energetice, informaționale și tehnologice necesare;

23.5. dependențele interne și externe.

24. Gestionarul identifică toate categoriile relevante de amenințări, pericole, hazarde, incidente și surse de risc care pot afecta infrastructura critică națională sau serviciul esențial furnizat.

25. Identificarea amenințărilor, a pericolelor și a surselor de risc se realizează pe baza:

25.1. istoricului incidentelor și al perturbărilor;

25.2. analizelor interne și sectoriale;

25.3. informațiilor furnizate de către autoritățile competente și autoritățile publice responsabile;

25.4. rapoartelor tehnice, statistice și științifice relevante;

25.5. lecțiilor învățate din exerciții, audituri, controale și evenimente anterioare;

25.6. analizelor privind evoluțiile mediului de risc și vulnerabilitățile emergente;

25.7. evaluării naționale a riscurilor, a evaluărilor strategice și a altor documente relevante elaborate în cadrul sistemului național de management al crizelor.

26. Gestionarul identifică vulnerabilitățile de natură fizică, tehnică, tehnologică, organizațională, umană, informațională și cibernetică, precum și orice altă slăbiciune care poate facilita materializarea unui risc sau amplificarea consecințelor acestuia.

27. Se identifică distinct:

27.1. vulnerabilitățile structurale și de amplasament;

27.2. vulnerabilitățile operaționale și procedurale;

27.3. vulnerabilitățile determinate de personal, de competențe sau de acces necorespunzător;

27.4. vulnerabilitățile aferente sistemelor informaționale și tehnologice;

27.5. vulnerabilitățile generate de dependențele externe, de furnizori sau de lanțul de aprovizionare;

27.6. vulnerabilitățile rezultate din interdependența cu alte infrastructuri critice sau servicii esențiale.

28. Pentru riscurile identificate, gestionarul elaborează scenarii de risc plauzibile, relevante și documentate, care descriu modul în care riscul se poate materializa și consecințele potențiale asupra infrastructurii critice naționale și a serviciului esențial.

29. Scenariile de risc includ, după caz:

29.1. sursa sau declanșatorul de risc;

29.2. vulnerabilitățile exploatate ori afectate;

29.3. succesiunea probabilă a evenimentelor;

29.4. efectele directe și indirecte;

29.5. durata probabilă a perturbării;

29.6. impactul asupra funcțiilor critice, a activelor critice și a serviciului esențial;

29.7. efectele de propagare și de interdependență.

V. CATEGORIILE DE RISCURI ANALIZATE

30. Evaluarea riscurilor la nivelul infrastructurilor critice naționale se realizează prin luarea în considerare a tuturor categoriilor relevante de riscuri care pot afecta direct sau indirect infrastructura critică națională, funcțiile critice, activele critice, procesele esențiale ori continuitatea serviciului esențial furnizat.

31. Evaluarea include, după caz, următoarele categorii de riscuri:

31.1. riscuri naturale, inclusiv cutremure, inundații, furtuni, temperaturi extreme, secetă, incendii de vegetație, alunecări de teren, fenomene meteorologice severe, epidemii, pandemii sau alte fenomene naturale și biologice cu efect perturbator;

31.2. riscuri tehnologice și industriale, inclusiv avarii, explozii, incendii, defecțiuni majore, indisponibilități tehnice, accidente de proces, erori de proiectare sau de mentenanță;

31.3. riscuri antropice intenționate, inclusiv sabotaj, terorism, vandalism grav, intruziuni, furt, distrugere ori compromitere deliberată;

31.4. riscuri hibride, inclusiv acțiuni coordonate sau combinate care vizează perturbarea infrastructurii critice naționale prin mijloace fizice, informaționale, economice, sociale, cibernetice sau psihologice;

31.5. riscuri cibernetice, inclusiv atacuri informatice, compromiterea sistemelor de control, indisponibilizarea rețelelor și afectarea integrității, confidențialității ori disponibilității datelor și serviciilor;

31.6. riscuri organizaționale și de personal, inclusiv erori umane, deficit de personal critic, lipsa competențelor, acces neautorizat, conflicte interne, corupție, neconformitate procedurală sau reorganizări;

31.7. riscuri legate de lanțul de aprovizionare și de dependențele externe, inclusiv întreruperi de furnizare, indisponibilitatea materiilor prime, a energiei, a comunicațiilor, a suportului tehnic ori a altor resurse critice;

31.8. riscuri reputaționale sau informaționale, în măsura în care acestea pot afecta continuitatea serviciului esențial, încrederea publică, cooperarea operațională sau capacitatea de răspuns;

31.9. alte riscuri relevante pentru sectorul și specificul infrastructurii critice naționale evaluate.

32. În cazul riscurilor hibride și al riscurilor cu impact sistemic, evaluarea include analiza efectelor potențiale asupra continuității funcțiilor vitale ale statului, asupra funcționării altor sectoare și a infrastructurilor critice naționale, precum și asupra rezilienței naționale.

33. În procesul de evaluare a riscurilor, gestionarul distinge între:

33.1. amenințări, constând în riscuri asociate unor acțiuni deliberate, ostile sau intenționate;

33.2. pericole ori hazarde, constând în evenimente, procese sau fenomene independente de intenția ostilă a unui actor.

34. Distincția prevăzută la pct. 33 se utilizează pentru alegerea metodelor de apreciere a probabilității și pentru descrierea corespunzătoare a scenariilor de risc.

VI. ESTIMAREA IMPACTULUI

35. Impactul fiecărui risc se estimează în raport cu consecințele posibile asupra:

35.1. vieții, sănătății și siguranței persoanelor;

35.2. continuității serviciului esențial și funcționării infrastructurii critice naționale;

35.3. economiei și activităților financiare;

35.4. mediului;

35.5. ordinii și securității publice;

35.6. securității naționale și capacității de guvernare;

35.7. reputației instituționale și obligațiilor relevante;

35.8. efectelor intersectoriale ori în cascadă.

36. Impactul se apreciază prin utilizarea unei scări unitare cu cinci trepte, de la 1 la 5, după cum urmează:

36.1. nivelul 1 – impact foarte scăzut: consecințe gestionabile prin resursele curente ale gestionarului, fără afectarea semnificativă a valorilor protejate, fără întreruperi relevante ale serviciului esențial și fără efecte în cascadă;

36.2. nivelul 2 – impact scăzut: perturbări limitate, controlabile, cu afectare redusă și temporară a unei componente, a unei comunități restrânse ori a unui segment limitat al serviciului esențial, fără consecințe grave asupra funcționării generale;

36.3. nivelul 3 – impact moderat: consecințe serioase asupra unei regiuni, a unui operator, a unui sector esențial ori a continuității normale a serviciului, cu afectarea funcționalității curente și cu necesitatea adoptării unor măsuri operative și manageriale suplimentare;

36.4. nivelul 4 – impact înalt: perturbări majore, cu afectarea gravă a funcțiilor critice, cu posibilitatea producerii unor pierderi semnificative de vieți omenești, a unor pagube economice considerabile, a afectării simultane a mai multor valori protejate sau a propagării semnificative în alte sisteme ori sectoare;

36.5. nivelul 5 – impact critic: consecințe catastrofale, pierderi masive de vieți omenești, indisponibilizarea extinsă a serviciilor esențiale, compromiterea funcțiilor vitale ori imposibilitatea menținerii serviciului esențial la un nivel minim acceptabil.

37. În cazul în care scenariul de risc afectează simultan mai multe domenii de impact, scorul final de impact se stabilește:

37.1. ca valoare maximă a impactului identificat, atunci când una dintre consecințe este dominantă; sau

37.2. ca valoare agregată justificată, atunci când afectarea este distribuită semnificativ asupra mai multor domenii.

38. Alegerea metodei de stabilire a scorului final de impact se consemnează expres în fișa de evaluare a riscului.

VII. ESTIMAREA PROBABILITĂȚII

39. Probabilitatea fiecărui risc se estimează în funcție de natura riscului, de frecvența sau plauzibilitatea materializării acestuia și de datele disponibile.

40. Probabilitatea se apreciază prin utilizarea unei scări unitare cu cinci trepte, de la 1 la 5, după cum urmează:

40.1. nivelul 1 – probabilitate foarte scăzută: scenariul este puțin plauzibil; nu există precedente relevante ori acestea sunt excepționale; condițiile necesare pentru materializare apar rar;

40.2. nivelul 2 – probabilitate scăzută: scenariul este posibil, dar puțin probabil; există puține indicii sau precedente limitate; condițiile necesare pentru materializare se întrunesc rar;

40.3. nivelul 3 – probabilitate moderată: scenariul este plauzibil și se poate produce în anumite condiții; există vulnerabilități sau precedente relevante; condițiile necesare pentru materializare se pot întruni periodic;

40.4. nivelul 4 – probabilitate înaltă: scenariul este foarte plauzibil; există indicii, tendințe ori vulnerabilități semnificative; materializarea se poate produce frecvent sau în condiții ușor de întrunit;

40.5. nivelul 5 – probabilitate foarte înaltă: scenariul este iminent, repetitiv ori aproape cert în lipsa unor măsuri suplimentare; există indicii clare, precedente multiple sau vulnerabilități critice persistente.

41. Pentru riscurile de tip pericol sau hazard, probabilitatea se fundamentează, în principal, pe date statistice, frecvențe observate, modele de prognoză, tendințe validate și istoricul incidentelor.

42. Pentru riscurile de tip amenințare, probabilitatea se apreciază în baza informațiilor disponibile privind intenția, capabilitatea, expunerea, vulnerabilitatea, contextul operațional și contextul de securitate.

VIII. DETERMINAREA SCORULUI ȘI A NIVELULUI DE RISC

43. Scorul de risc se calculează prin înmulțirea scorului de impact cu scorul de probabilitate, potrivit următoarei formule:

Scorul de risc = Impact × Probabilitate.

44. Scorul de risc poate avea valori cuprinse între 1 și 25.

45. În scopul clasificării și al prioritizării, nivelurile de risc se stabilesc după cum urmează:

45.1. 1-4 – risc scăzut;

45.2. 5-10 – risc moderat;

45.3. 11-15 – risc înalt;

45.4. 16-25 – risc critic.

46. Matricea de risc are format 5 × 5 și se utilizează pentru poziționarea, compararea și ierarhizarea riscurilor.

Impact\ probabilitate	**1**	**2**	**3**	**4**	**5**
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

47. Matricea de risc servește pentru:

47.1. clasificarea riscurilor;

47.2. compararea riscurilor între ele;

47.3. stabilirea priorităților de intervenție;

47.4. fundamentarea măsurilor prevăzute în Planul de securitate;

47.5. justificarea alocării resurselor.

IX. PRIORITIZAREA ȘI TRATAREA RISCURILOR

48. După determinarea nivelului de risc, gestionarul prioritizează riscurile în funcție de gravitate, de efectele asupra serviciului esențial, de vulnerabilitățile asociate și de capacitatea existentă de prevenire, protecție, răspuns, continuitate și recuperare.

49. Riscurile încadrate ca înalte sau critice se tratează cu prioritate.

50. Pentru fiecare risc prioritar se stabilesc:

50.1. măsurile de securitate existente;

50.2. măsurile suplimentare necesare;

50.3. ordinea de implementare;

50.4. responsabilii;

50.5. resursele necesare;

50.6. termenul de implementare;

50.7. indicatorii de realizare;

50.8. modalitatea de verificare.

51. Măsurile de tratare a riscurilor pot include:

51.1. evitarea riscului;

51.2. reducerea probabilității;

51.3. reducerea impactului;

51.4. transferul sau partajarea riscului, după caz;

51.5. acceptarea justificată a riscului rezidual;

51.6. pregătirea pentru răspuns și recuperare.

52. Măsurile de tratare a riscurilor pot fi:

52.1. măsuri organizatorice;

52.2. măsuri tehnice;

52.3. măsuri procedurale;

52.4. măsuri de securitate fizică;

52.5. măsuri de securitate cibernetică;

52.6. măsuri de continuitate;

52.7. măsuri de intervenție și răspuns;

52.8. măsuri de instruire și exerciții;

52.9. măsuri de comunicare și avertizare;

52.10. măsuri de redundanță și recuperare.

53. Riscul rezidual se documentează, se justifică și se monitorizează de către gestionar.

54. Măsurile de tratare a riscurilor se includ în Planul de securitate sau în documentele asociate acestuia.

X. DOCUMENTAREA EVALUĂRII RISCURILOR

55. Rezultatele evaluării riscurilor se consemnează în fișe de evaluare a riscurilor, întocmite pentru fiecare risc relevant sau grup omogen de riscuri.

56. Fișa de evaluare a riscului conține cel puțin:

56.1. denumirea riscului;

56.2. descrierea scenariului de risc;

56.3. activele, funcțiile și procesele afectate;

56.4. vulnerabilitățile și dependențele relevante;

56.5. impactul și probabilitatea estimate;

56.6. scorul și nivelul de risc;

56.7. măsurile existente;

56.8. măsurile suplimentare propuse;

56.9. sursele de date și gradul de încredere al acestora;

56.10. data evaluării și persoanele responsabile.

57. Gestionarul păstrează datele, referințele, calculele, scenariile și celelalte documente justificative care au fundamentat evaluarea riscurilor.

58. Gestionarul întocmește un registru al riscurilor, care include riscurile identificate, scorul acestora, nivelul de risc, măsurile existente, măsurile suplimentare și stadiul implementării acestora.

59. Rezultatele evaluării riscurilor se includ în raportul de evaluare a riscurilor la adresa infrastructurii critice naționale.

60. Raportul de evaluare a riscurilor se aprobă de către conducătorul gestionarului sau de către persoana împuternicită în acest sens.

61. Raportul de evaluare a riscurilor se transmite autorității publice responsabile, împreună cu Planul de securitate sau cu documentele relevante solicitate în procesul de avizare.

XI. ACTUALIZAREA EVALUĂRII RISCURILOR

62. Evaluarea riscurilor se actualizează cel puțin o dată pe an, într-un termen care să permită valorificarea rezultatelor acesteia la elaborarea rapoartelor prevăzute la art. 6 alin. (2) și (3) din Legea nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale, precum și ori de câte ori intervin schimbări semnificative privind infrastructura critică națională, serviciul esențial, mediul de risc, dependențele, interdependențele ori vulnerabilitățile relevante.

63. Actualizarea evaluării riscurilor se realizează cel puțin în următoarele situații:

63.1. după producerea unui incident major sau a unei perturbări semnificative;

63.2. după modificări structurale, funcționale, tehnologice sau organizaționale;

63.3. după schimbări relevante ale lanțului de aprovizionare ori ale dependențelor externe;

63.4. după audituri, controale, exerciții sau teste care indică neconformități ori vulnerabilități noi;

63.5. la apariția unor amenințări noi sau la modificarea nivelului amenințărilor existente;

63.6. la modificarea interdependențelor relevante;

63.7. la modificarea nivelului de alertă sau la declararea unei stări de criză, atunci când aceasta afectează ori poate afecta infrastructura critică națională sau continuitatea serviciului esențial furnizat;

63.8. la solicitarea autorității publice responsabile sau a CNCPIC, în condițiile legii.

64. Orice modificare substanțială a evaluării riscurilor se documentează prin notă de actualizare.

65. Nota de actualizare cuprinde cel puțin:

65.1. cauza actualizării;

65.2. riscurile noi identificate;

65.3. riscurile modificate;

65.4. vulnerabilitățile noi sau modificate;

65.5. schimbările privind impactul sau probabilitatea;

65.6. măsurile suplimentare necesare;

65.7. impactul asupra Planului de securitate.

66. În cazul în care actualizarea evaluării riscurilor determină modificări substanțiale ale profilului de risc sau ale măsurilor de securitate, gestionarul inițiază revizuirea Planului de securitate potrivit normelor metodologice privind revizuirea și actualizarea acestuia.

XII. PROTECȚIA INFORMAȚIILOR

67. Informațiile utilizate sau rezultate în procesul de evaluare a riscurilor se gestionează cu respectarea regimului juridic aplicabil informațiilor atribuite la secret de stat, datelor cu caracter personal, informațiilor sensibile privind infrastructurile critice naționale și altor categorii de informații protejate de lege.

68. Accesul la informațiile privind evaluarea riscurilor se acordă potrivit principiului necesității de a cunoaște și exclusiv persoanelor cu atribuții directe în procesul de evaluare, avizare, monitorizare, control sau implementare a măsurilor de securitate.

69. Gestionarul și autoritatea publică responsabilă asigură evidența, păstrarea, transmiterea, arhivarea și, după caz, distrugerea documentelor aferente evaluării riscurilor, în condițiile legii.

70. Datele privind vulnerabilitățile, scenariile de risc, interdependențele critice, măsurile de securitate, capacitățile de răspuns și punctele sensibile ale infrastructurii critice naționale se tratează ca informații sensibile și se protejează corespunzător nivelului de risc generat de divulgarea acestora.

71. În cazul infrastructurilor critice din domeniul apărării, ordinii publice și securității statului, termenele și procedurile de transmitere, verificare și avizare a documentelor se adaptează la regimul de protecție a informațiilor clasificate, utilizând exclusiv canale securizate și personal autorizat potrivit legislației.

XIII. REGULILE COMUNE DE APLICARE

ȘI DE CORELARE METODOLOGICĂ

72. Evaluarea riscurilor la adresa infrastructurilor critice naționale nu substituie evaluările de risc prevăzute de legislația specială, ci se corelează cu acestea în vederea asigurării unei abordări integrate a securității, a protecției, a continuității și a rezilienței infrastructurilor critice naționale.

73. Autoritățile publice responsabile și gestionarii cooperează pentru asigurarea unei abordări unitare, proporționale și coerente în procesul de evaluare a riscurilor.

74. CNCPIC elaborează și pune la dispoziția autorităților publice responsabile și a gestionarilor modele-tip și instrumente metodologice standardizate pentru aplicarea prezentelor Norme, inclusiv modele de evaluare a riscurilor, registre de risc, matrice de evaluare, fișe de risc, formulare-tip de raportare, modele de revizuire și alte instrumente necesare pentru aplicarea unitară a procesului de evaluare a riscurilor.

75. Rezultatele evaluării riscurilor fundamentează Planul de securitate, măsurile de tratare a riscurilor și procesul de revizuire a acestuia.

Anexa nr. 2

la Hotărârea Guvernului nr.483/2026

NORME

metodologice privind elaborarea, avizarea și aprobarea Planului

de securitate al gestionarului infrastructurii critice naționale

I. DISPOZIȚII GENERALE

1. Prezentele Norme reglementează modul de elaborare, de transmitere spre avizare, examinare și aprobare a Planului de securitate al gestionarului infrastructurii critice

naționale (denumit în continuare *Plan de securitate*).

2. Planul de securitate reprezintă documentul de planificare strategică, cu caracter operativ prin procedurile asociate, elaborat pentru fiecare infrastructură critică națională desemnată, care stabilește obiectivele, măsurile, responsabilitățile, resursele și procedurile necesare pentru protecția, securitatea, continuitatea și reziliența acesteia.

3. Planul de securitate are ca scop transpunerea rezultatelor evaluării riscurilor în măsuri organizatorice, tehnice, procedurale și operaționale, orientate spre prevenirea, reducerea, gestionarea și recuperarea în urma incidentelor care pot afecta infrastructura critică națională sau serviciul esențial furnizat prin intermediul acesteia.

4. Planul de securitate se elaborează de către gestionarul fiecărei infrastructuri critice naționale desemnate (denumit în continuare *gestionar*), indiferent de forma juridică de organizare, forma de proprietate sau sectorul de activitate.

5. În cazul în care același gestionar administrează sau operează mai multe infrastructuri critice naționale, acesta poate elabora:

5.1. planuri de securitate distincte pentru fiecare infrastructură critică națională; sau

5.2. un plan integrat, cu condiția delimitării clare, distincte și verificabile a elementelor specifice fiecărei infrastructuri critice naționale.

6. Planul integrat prevăzut la pct. 5 subpct. 5.2. trebuie să permită identificarea separată, pentru fiecare infrastructură critică națională, a riscurilor, a funcțiilor critice, a activelor critice, a măsurilor de securitate, a responsabilităților, a resurselor, a termenelor și a procedurilor aplicabile.

7. Planul de securitate se elaborează în baza:

7.1. evaluării riscurilor, realizate potrivit Normelor metodologice privind evaluarea riscurilor la adresa infrastructurilor critice naționale, prevăzute în anexa nr. 1;

7.2. cadrului normativ aplicabil sectorului sau subsectorului;

7.3. structurii-cadru prevăzute în anexa nr. 3;

7.4. instrucțiunilor sectoriale emise de către autoritatea publică responsabilă, după caz;

7.5. obligațiilor legale privind securitatea, continuitatea, protecția civilă, securitatea cibernetică, protecția antiteroristă, protecția informațiilor și alte domenii relevante;

7.6. lecțiilor identificate în urma incidentelor, a exercițiilor, a testărilor, a auditurilor sau a controalelor.

8. Planul de securitate nu substituie planurile, procedurile sau documentele prevăzute de legislația specială, ci se corelează cu acestea și le integrează, după caz, în cadrul unui mecanism unitar de protecție, continuitate și reziliență a infrastructurii critice

naționale.

9. Elaborarea, avizarea și aprobarea Planului de securitate se realizează cu respectarea principiilor legalității, proporționalității, abordării bazate pe risc, responsabilității gestionarului, cooperării instituționale, continuității serviciilor esențiale, trasabilității, confidențialității și protecției informațiilor sensibile sau clasificate.

II. RESPONSABILITĂȚILE ÎN PROCESUL

DE ELABORARE A PLANULUI DE SECURITATE

10. Responsabilitatea generală pentru elaborarea, transmiterea spre avizare, aprobarea finală, implementarea, testarea, revizuirea și actualizarea Planului de securitate revine gestionarului.

11. Conducătorul gestionarului asigură:

11.1. inițierea procesului de elaborare a Planului de securitate;

11.2. desemnarea persoanelor sau a structurilor responsabile;

11.3. alocarea resurselor necesare pentru elaborare, consultare, testare și actualizare;

11.4. aprobarea preliminară a proiectului Planului de securitate, în vederea transmiterii spre avizare;

11.5. transmiterea Planului de securitate spre avizare autorității publice responsabile;

11.6. aprobarea finală a Planului de securitate, după obținerea avizului autorității publice responsabile;

11.7. punerea în aplicare a măsurilor prevăzute în Planul de securitate;

11.8. monitorizarea implementării, a testării, a revizuirii și a actualizării Planului de securitate.

12. Ofițerul de legătură pentru securitatea infrastructurii critice naționale coordonează, la nivel operațional și metodologic, procesul de elaborare a Planului de securitate, fără a substitui responsabilitatea conducerii gestionarului.

13. La elaborarea Planului de securitate participă, după caz, structurile interne relevante ale gestionarului, inclusiv cele responsabile de:

13.1. operare și exploatare;

13.2. securitate fizică;

13.3. securitate informațională și cibernetică;

13.4. continuitate a activității;

13.5. management al riscurilor;

13.6. protecție civilă și situații de urgență;

13.7. resurse umane;

13.8. asigurarea cadrului juridic;

13.9. achiziții, logistică, tehnic și mentenanță;

13.10. comunicare publică;

13.11. protecție a informațiilor;

13.12. alte domenii relevante potrivit specificului infrastructurii critice naționale.

14. Autoritatea publică responsabilă asigură coordonarea sectorială a procesului de elaborare a planurilor de securitate, oferă clarificări metodologice gestionarilor din domeniul său de responsabilitate și examinează planurile transmise spre avizare.

15. Centrul Național de Coordonare a Protecției Infrastructurilor Critice (denumit în continuare *CNCPIC*) acordă suport metodologic autorităților publice responsabile și, după caz, gestionarilor, în vederea aplicării unitare a cerințelor privind planurile de securitate.

III. CERINȚELE GENERALE PRIVIND CONȚINUTUL

PLANULUI DE SECURITATE

16. Planul de securitate se elaborează potrivit structurii-cadru prevăzute în anexa nr. 3.

17. Planul de securitate trebuie să fie:

17.1. specific infrastructurii critice naționale pentru care este elaborat;

17.2. fundamentat pe evaluarea riscurilor;

17.3. aplicabil din punct de vedere operațional;

17.4. corelat cu documentele interne relevante ale gestionarului;

17.5. redactat într-o formă clară, coerentă și actualizabilă;

17.6. proporțional cu nivelul riscurilor identificate.

18. Planul de securitate cuprinde cel puțin:

18.1. datele generale privind gestionarul și infrastructura critică națională;

18.2. descrierea serviciului esențial furnizat;

18.3. descrierea funcțiilor critice, a activelor critice și a proceselor esențiale;

18.4. sinteza evaluării riscurilor;

18.5. măsurile existente de securitate și continuitate;

18.6. măsurile suplimentare de tratare a riscurilor;

18.7. procedurile de prevenire, protecție, detectare și avertizare;

18.8. procedurile de răspuns la incidente;

18.9. procedurile de continuitate și recuperare;

18.10. responsabilitățile interne și externe;

18.11. mecanismele de comunicare, notificare și raportare;

18.12. resursele necesare pentru implementarea măsurilor;

18.13. mecanismele de coordonare și cooperare cu autoritățile competente în gestionarea situațiilor de criză, în cazul incidentelor care depășesc capacitatea de răspuns a gestionarului sau produc efecte sistemice ori intersectoriale;

18.14. calendarul de implementare;

18.15. modul de instruire, testare și desfășurare a exercițiilor;

18.16. modalitatea de monitorizare, revizuire și actualizare;

18.17. anexele tehnice și documentele suport.

19. Pentru fiecare măsură relevantă prevăzută în Planul de securitate se indică:

19.1. descrierea măsurii;

19.2. scopul acesteia;

19.3. riscul, vulnerabilitatea, funcția critică sau activul critic vizat;

19.4. responsabilul de implementare;

19.5. termenul de implementare sau de aplicare;

19.6. resursele necesare, după caz;

19.7. indicatorul de realizare;

19.8. modalitatea de verificare.

20. Pentru riscurile încadrate ca înalte sau critice, Planul de securitate include în mod obligatoriu măsuri concrete de reducere a probabilității, de diminuare a impactului, precum și de asigurare a continuității și de recuperare.

21. Pentru riscurile moderate, Planul de securitate include măsuri proporționale de monitorizare, prevenire sau reducere, în funcție de specificul infrastructurii și de evoluția mediului de risc.

22. Pentru riscurile scăzute, gestionarul asigură monitorizarea periodică și reevaluarea acestora în cazul modificării contextului operațional, tehnic, organizațional sau de securitate.

23. În cazul în care un incident depășește capacitatea de răspuns a gestionarului, afectează ori poate afecta continuitatea unui serviciu esențial sau generează efecte sistemice ori intersectoriale, Planul de securitate stabilește cel puțin:

23.1. criteriile și nivelurile de escaladare a incidentului;

23.2. responsabilitățile privind evaluarea și inițierea escaladării;

23.3. procedura de informare a autorității publice responsabile, a Centrului Național de Management al Crizelor și a altor autorități competente, potrivit cadrului normativ aplicabil;

23.4. mecanismele de activare a cooperării și coordonării interinstituționale;

23.5. modalitatea de integrare a măsurilor proprii de răspuns, de continuitate și de recuperare în mecanismele naționale de management al crizelor;

23.6. datele de contact, canalele de comunicare și fluxurile de notificare aplicabile.

IV. ELABORAREA PLANULUI DE SECURITATE

24. Elaborarea Planului de securitate se inițiază după desemnarea infrastructurii drept infrastructură critică națională.

25. Planul de securitate se elaborează și se transmite spre avizare în termen de nouă luni de la data desemnării infrastructurii drept infrastructură critică națională, cu posibilitatea extinderii acestui termen cu cel mult șase luni, cu acordul CNCPIC, în condițiile art. 14 alin. (1) din Legea nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale.

26. Decizia internă de inițiere stabilește cel puțin:

26.1. infrastructura critică națională pentru care se elaborează Planul de securitate;

26.2. coordonatorul procesului de elaborare;

26.3. structurile și persoanele implicate;

26.4. calendarul intern de elaborare;

26.5. responsabilitățile principale;

26.6. modul de consultare și avizare internă.

27. Gestionarul poate constitui, după caz, un grup de lucru intern sau o comisie internă pentru elaborarea Planului de securitate.

28. Elaborarea Planului de securitate include cel puțin următoarele etape:

28.1. inițierea procesului de elaborare;

28.2. delimitarea infrastructurii critice naționale și a serviciului esențial vizat;

28.3. realizarea sau actualizarea evaluării riscurilor;

28.4. valorificarea rezultatelor evaluării riscurilor;

28.5. identificarea și sistematizarea măsurilor existente;

28.6. analiza documentelor interne relevante;

28.7. stabilirea măsurilor suplimentare necesare;

28.8. definirea măsurilor de continuitate și recuperare;

28.9. stabilirea responsabilităților, a termenelor și a resurselor;

28.10. redactarea proiectului Planului de securitate;

28.11. consultarea internă și, după caz, externă;

28.12. aprobarea preliminară a proiectului, în vederea transmiterii spre avizare;

28.13. transmiterea spre avizare autorității publice responsabile;

28.14. aprobarea finală a Planului de securitate, după obținerea avizului;

28.15. asigurarea evidenței versiunii aprobate și punerea în aplicare.

29. Etapele prevăzute la pct. 28 se realizează în mod proporțional cu complexitatea infrastructurii critice naționale și nivelul riscurilor identificate.

30. Planul de securitate se elaborează obligatoriu în baza unei evaluări actuale și documentate a riscurilor.

31. În procesul de elaborare a Planului de securitate se valorifică cel puțin:

31.1. riscurile prioritare identificate;

31.2. scenariile de risc relevante;

31.3. vulnerabilitățile și dependențele identificate;

31.4. funcțiile critice, activele critice și procesele esențiale;

31.5. nivelul de impact și probabilitatea estimate;

31.6. măsurile existente și deficiențele constatate;

31.7. documentele naționale relevante privind continuitatea funcțiilor vitale ale statului, reziliența națională și managementul crizelor, după caz.

32. În lipsa unei evaluări actuale a riscurilor sau în cazul în care evaluarea existentă nu mai corespunde situației reale, Planul de securitate nu poate fi considerat elaborat în mod corespunzător.

33. La elaborarea Planului de securitate, gestionarul valorifică, după caz, documentele interne existente relevante pentru:

33.1. continuitatea activității;

33.2. răspunsul la incidente;

33.3. protecția fizică;

33.4. securitatea informațională și cibernetică;

33.5. situațiile excepționale, protecția civilă sau apărarea împotriva incendiilor;

33.6. mentenanța și recuperarea tehnică;

33.7. comunicarea internă și externă;

33.8. alte domenii incidente.

34. Valorificarea documentelor prevăzute la pct. 33 nu exclude obligația de a asigura coerența, unitatea și completitudinea Planului de securitate.

35. În cazul în care documentele existente acoperă integral sau parțial cerințele Planului de securitate, gestionarul poate solicita echivalarea acestora potrivit Normelor metodologice prevăzute în anexa nr. 4.

V. CONSULTAREA ȘI VERIFICAREA INTERNĂ

36. Proiectul Planului de securitate se supune consultării interne cu structurile și persoanele relevante din cadrul gestionarului.

37. În procesul de consultare internă se verifică cel puțin:

37.1. corectitudinea descrierii infrastructurii critice naționale și a serviciului esențial;

37.2. conformitatea cu evaluarea riscurilor;

37.3. caracterul complet al măsurilor prevăzute;

37.4. realismul termenelor și al resurselor;

37.5. claritatea responsabilităților;

37.6. coerența cu celelalte documente interne relevante;

37.7. respectarea structurii-cadru prevăzute în anexa nr. 3.

38. După caz, gestionarul poate consulta entități externe relevante, în limitele competențelor legale și ale regimului de protecție a informațiilor, dacă acest lucru este necesar pentru completarea sau validarea unor măsuri privind:

38.1. interdependențele;

38.2. continuitatea serviciilor;

38.3. furnizarea resurselor critice;

38.4. reacția și coordonarea interinstituțională;

38.5. suportul tehnic sau contractual necesar pentru funcționarea infrastructurii critice naționale.

39. Consultarea externă nu poate conduce la divulgarea informațiilor sensibile, confidențiale sau clasificate, cu excepția cazurilor prevăzute de legislația aplicabilă.

VI. TRANSMITEREA PLANULUI DE SECURITATE SPRE AVIZARE

40. După aprobarea preliminară internă, gestionarul transmite Planul de securitate spre avizare autorității publice responsabile din sectorul sau subsectorul de competență.

41. Dosarul transmis spre avizare include:

41.1. cererea de avizare;

41.2. Planul de securitate aprobat preliminar la nivel intern;

41.3. raportul de evaluare a riscurilor sau sinteza acestuia;

41.4. registrul riscurilor;

41.5. lista măsurilor prioritare;

41.6. tabelul de corelare cu structura-cadru prevăzută în anexa nr. 3;

41.7. lista documentelor anexate sau aferente Planului de securitate;

41.8. datele de contact ale ofițerului de legătură;

41.9. actul intern privind inițierea elaborării Planului de securitate sau aprobarea preliminară a acestuia;

41.10. alte documente solicitate de către autoritatea publică responsabilă, justificate de specificul sectorului.

42. Planul de securitate și documentele aferente se transmit în formatul și prin

mijloacele stabilite potrivit cerințelor tehnice și modelelor standardizate aprobate de către CNCPIC. Autoritatea publică responsabilă poate stabili cerințe suplimentare justificate de specificul sectorului sau subsectorului, cu respectarea cerințelor unitare și a regimului de protecție a informațiilor sensibile, confidențiale sau clasificate.

43. În cazul în care Planul de securitate conține informații atribuite la secret de stat sau alte categorii de informații protejate, transmiterea, accesarea și păstrarea acestuia se realizează potrivit regimului juridic aplicabil acestor informații.

VII. EXAMINAREA ȘI AVIZAREA PLANULUI DE SECURITATE

44. Autoritatea publică responsabilă examinează Planul de securitate în raport cu:

44.1. respectarea structurii-cadru prevăzute în anexa nr. 3;

44.2. existența și calitatea evaluării riscurilor;

44.3. corelarea măsurilor propuse cu riscurile identificate;

44.4. proporționalitatea măsurilor în raport cu nivelul de risc;

44.5. includerea măsurilor pentru riscurile înalte și critice;

44.6. claritatea responsabilităților, a termenelor și a resurselor;

44.7. existența procedurilor de răspuns, de continuitate și de recuperare;

44.8. corelarea cu cerințele sectoriale aplicabile;

44.9. existența mecanismelor de instruire, de testare, de raportare și de actualizare;

44.10. respectarea regimului de protecție a informațiilor.

45. Autoritatea publică responsabilă verifică plenitudinea dosarului în termen de cel mult 10 zile lucrătoare de la data recepționării acestuia.

46. În cazul în care dosarul este complet, autoritatea publică responsabilă informează gestionarul despre constatarea plenitudinii acestuia și examinează Planul de securitate în termen de cel mult 30 de zile lucrătoare de la data constatării plenitudinii dosarului.

47. În cazul în care dosarul este incomplet, autoritatea publică responsabilă solicită gestionarului completarea informațiilor sau a documentelor necesare, indicând în mod clar aspectele care urmează a fi remediate.

48. Gestionarul transmite completările solicitate în termen de 14 zile lucrătoare de la data recepționării solicitării, dacă autoritatea publică responsabilă nu stabilește un alt termen justificat.

49. Termenul pentru verificarea plenitudinii dosarului curge din nou de la data

recepționării completărilor solicitate.

50. În cazul în care gestionarul nu transmite completările solicitate în termenul prevăzut la pct. 48 și nu solicită, înainte de expirarea acestuia, prelungirea motivată a termenului, autoritatea publică responsabilă restituie dosarul fără finalizarea procedurii de avizare. Reluarea procedurii se realizează prin transmiterea unui dosar complet.

51. În cadrul examinării în fond, autoritatea publică responsabilă poate solicita clarificări sau informații suplimentare necesare pentru evaluarea Planului de securitate.

52. Termenul de examinare în fond se suspendă de la data transmiterii solicitării prevăzute la pct. 51 până la data recepționării clarificărilor sau a informațiilor solicitate. Gestionarul prezintă clarificările sau informațiile suplimentare în termen de 10 zile lucrătoare de la data recepționării solicitării. Suspendarea termenului de examinare în fond nu poate depăși 15 zile lucrătoare.

53. În urma examinării, autoritatea publică responsabilă emite una dintre următoarele soluții:

53.1. avizarea Planului de securitate;

53.2. avizarea condiționată, cu indicarea măsurilor sau a completărilor care urmează a fi realizate;

53.3. restituirea Planului de securitate pentru revizuire, cu indicarea motivelor.

54. Avizarea condiționată se poate acorda atunci când Planul de securitate corespunde în esență cerințelor, iar neconformitățile identificate nu afectează aplicabilitatea măsurilor principale de securitate, continuitate, răspuns și recuperare.

55. În cazul avizării condiționate, gestionarul prezintă autorității publice responsabile dovada remedierii neconformităților în termenul stabilit în aviz.

56. Restituirea Planului de securitate pentru revizuire se dispune atunci când lipsurile sau neconformitățile constatate afectează substanțial calitatea evaluării riscurilor, proporționalitatea măsurilor, aplicabilitatea planului sau capacitatea acestuia de a asigura protecția și continuitatea serviciului esențial.

57. Soluțiile prevăzute la pct. 53 se consemnează într-un aviz scris, care conține cel puțin:

57.1. datele de identificare ale gestionarului și ale infrastructurii critice naționale;

57.2. temeiul examinării;

57.3. documentele analizate;

57.4. concluzia examinării și soluția dispusă;

57.5. neconformitățile constatate, condițiile, recomandările sau măsurile de

remediere, după caz;

57.6. termenul de remediere sau de retransmitere a Planului de securitate revizuit, după caz;

57.7. data emiterii;

57.8. semnătura persoanei autorizate.

58. În cazul restituirii Planului de securitate pentru revizuire, gestionarul îl revizuiește și îl retransmite autorității publice responsabile în termen de 30 de zile lucrătoare de la data recepționării avizului, dacă prin aviz nu este stabilit un alt termen justificat de complexitatea modificărilor necesare.

59. Autoritatea publică responsabilă examinează Planul de securitate revizuit în termen de cel mult 30 de zile lucrătoare de la data constatării plenitudinii dosarului și emite una dintre soluțiile prevăzute la pct. 53.

60. Termenul de examinare în fond poate fi prelungit o singură dată, cu cel mult 15 zile lucrătoare, în situații justificate de complexitatea documentației, de existența informațiilor clasificate ori de necesitatea efectuării unor verificări suplimentare. Prelungirea se comunică în scris gestionarului înainte de expirarea termenului inițial, cu indicarea motivelor.

61. Autoritatea publică responsabilă ține evidența planurilor de securitate examinate și a avizelor emise pentru infrastructurile critice naționale din sectorul sau subsectorul de competență.

VIII. APROBAREA FINALĂ A PLANULUI DE SECURITATE

62. Planul de securitate se aprobă final de către conducătorul gestionarului sau de către persoana competentă desemnată potrivit actelor interne, după obținerea avizului autorității publice responsabile.

63. În cazul avizării condiționate, Planul de securitate poate fi aprobat final cu obligația implementării măsurilor indicate în aviz, în termenele stabilite de către autoritatea publică responsabilă.

64. Prin aprobarea finală a Planului de securitate, conducerea gestionarului confirmă:

64.1. asumarea conținutului Planului de securitate;

64.2. asumarea măsurilor și a responsabilităților prevăzute;

64.3. asumarea obligației de implementare, monitorizare, testare și actualizare;

64.4. asigurarea resurselor necesare, în limitele competențelor și posibilităților

instituționale.

65. Planul de securitate aprobat final conține cel puțin:

65.1. data aprobării;

65.2. semnătura persoanei competente;

65.3. numărul sau codul versiunii;

65.4. mențiunea privind intrarea în vigoare;

65.5. regimul de acces la document, potrivit legislației aplicabile.

66. Planul de securitate intră în vigoare la data aprobării finale sau la data prevăzută în cuprinsul acestuia.

67. Gestionarul transmite autorității publice responsabile o copie a actului intern de aprobare finală a Planului de securitate în termen de cinci zile lucrătoare de la data aprobării.

68. Autoritatea publică responsabilă poate transmite CNCPIC informații de sinteză privind planurile de securitate avizate, fără divulgarea informațiilor sensibile, confidențiale sau clasificate, dacă legislația aplicabilă nu prevede altfel.

IX. IMPLEMENTAREA ȘI MONITORIZAREA PLANULUI DE SECURITATE

69. După aprobarea finală, gestionarul asigură punerea în aplicare a măsurilor prevăzute în Planul de securitate potrivit responsabilităților și termenelor stabilite.

70. Punerea în aplicare a Planului de securitate include, după caz:

70.1. comunicarea internă a responsabilităților;

70.2. alocarea resurselor necesare;

70.3. inițierea măsurilor de implementare;

70.4. integrarea măsurilor în activitatea curentă a structurilor relevante;

70.5. programarea instruirilor, a testelor și a exercițiilor;

70.6. monitorizarea realizării măsurilor;

70.7. raportarea internă privind stadiul implementării.

71. Măsurile care vizează riscurile înalte sau critice se implementează și se monitorizează cu prioritate.

72. Pentru măsurile care necesită investiții, achiziții, lucrări, contracte sau resurse

suplimentare, gestionarul stabilește calendarul de implementare, sursele de finanțare disponibile, responsabilitățile interne și, după caz, măsurile temporare sau compensatorii.

73. În cazul în care unele măsuri necesare nu pot fi implementate imediat, gestionarul prevede:

73.1. soluțiile temporare sau compensatorii;

73.2. ordinea de prioritate a implementării;

73.3. responsabilitățile și termenele aferente;

73.4. justificarea neimplementării imediate;

73.5. riscul rezidual acceptat temporar.

74. Ofițerul de legătură urmărește, la nivel operațional, punerea în aplicare a Planului de securitate și informează conducerea gestionarului despre stadiul implementării, neconformitățile identificate și necesitatea unor măsuri suplimentare.

75. Gestionarul informează autoritatea publică responsabilă despre dificultățile majore care pot afecta implementarea măsurilor prevăzute pentru riscurile înalte sau critice.

76. Autoritatea publică responsabilă monitorizează, în limitele competențelor legale, modul de implementare a măsurilor prevăzute în planurile de securitate ale gestionarilor din sectorul sau subsectorul de competență.

X. TESTAREA PLANULUI DE SECURITATE

77. Gestionarul asigură testarea Planului de securitate prin exerciții, simulări, verificări funcționale sau alte forme adecvate specificului infrastructurii și riscurilor evaluate.

78. Testarea Planului de securitate se realizează cel puțin o dată la doi ani, precum și ori de câte ori intervin modificări semnificative ale infrastructurii critice naționale, ale serviciului esențial, ale riscurilor, ale procedurilor, ale responsabilităților ori ale resurselor prevăzute în plan sau în urma producerii unui incident relevant.

79. Testarea Planului de securitate are drept scop verificarea aplicabilității măsurilor, a clarității responsabilităților, a funcționalității procedurilor de răspuns, de continuitate și de recuperare, precum și identificarea vulnerabilităților sau a neconformităților.

80. Testarea poate fi realizată prin:

80.1. exerciții de tip tabletop;

80.2. exerciții funcționale;

80.3. exerciții operaționale;

80.4. simulări tehnice;

80.5. verificări ale canalelor de comunicare și de notificare;

80.6. teste ale procedurilor de continuitate și de recuperare;

80.7. alte forme de testare adecvate specificului infrastructurii.

81. Exercițiile care includ scenarii cu impact major asupra serviciilor esențiale, efecte sistemice sau intersectoriale se desfășoară, după caz, cu participarea autorităților competente din cadrul sistemului național de management al crizelor, în vederea verificării mecanismelor de notificare, cooperare și coordonare interinstituțională.

82. Rezultatele testării se consemnează într-un raport de testare sau de exercițiu, care include cel puțin:

82.1. obiectivele testării;

82.2. scenariul utilizat;

82.3. participanții;

82.4. procedurile testate;

82.5. constatările;

82.6. neconformitățile sau vulnerabilitățile identificate;

82.7. măsurile corective;

82.8. responsabilii și termenele de realizare;

82.9. concluziile și lecțiile identificate.

83. Constatările, concluziile și lecțiile identificate în urma testării Planului de securitate, a gestionării situațiilor de criză, a exercițiilor naționale și a incidentelor majore se analizează și se valorifică în mod obligatoriu la actualizarea evaluării riscurilor și, după caz, la revizuirea și actualizarea Planului de securitate, potrivit anexei nr. 5.

XI. EVIDENȚA VERSIUNILOR ȘI TRASABILITATEA MODIFICĂRILOR

84. Gestionarul asigură evidența tuturor versiunilor Planului de securitate.

85. Evidența versiunilor include cel puțin:

85.1. numărul sau codul versiunii;

85.2. data elaborării;

85.3. data avizării;

85.4. data aprobării finale;

85.5. descrierea modificărilor operate;

85.6. motivul modificării;

85.7. persoanele sau structurile responsabile;

85.8. regimul de acces la document.

86. Gestionarul asigură păstrarea versiunii în vigoare și a versiunilor anterioare, potrivit regimului juridic aplicabil documentului.

87. Orice versiune nouă a Planului de securitate sau orice actualizare substanțială a acestuia se înscrie în evidența internă a documentelor aferente infrastructurii critice naționale.

88. Structurile interne relevante sunt informate cu privire la versiunea aplicabilă a Planului de securitate, în limitele atribuțiilor și a necesității de a lucra cu informațiile respective.

XII. PROTECȚIA INFORMAȚIILOR

89. Planul de securitate și documentele aferente acestuia se gestionează cu respectarea regimului juridic aplicabil informațiilor atribuite la secret de stat, datelor cu caracter personal, informațiilor sensibile privind infrastructurile critice naționale și altor categorii de informații protejate de lege.

90. Accesul la Planul de securitate și la documentele aferente se acordă exclusiv persoanelor care au atribuții directe și care justifică necesitatea de a lucra cu informațiile respective, cu respectarea regimului juridic aplicabil informațiilor sensibile, confidențiale, informațiilor atribuite la secret de stat și altor categorii de informații protejate de lege.

91. Gestionarul stabilește măsuri interne pentru evidența, păstrarea, accesarea, multiplicarea, transmiterea, arhivarea și protecția Planului de securitate și a documentelor asociate.

92. Informațiile privind vulnerabilitățile, scenariile de risc, măsurile de securitate, capacitățile de răspuns, punctele sensibile și interdependențele critice se protejează corespunzător nivelului de risc generat de divulgarea acestora.

93. Transmiterea Planului de securitate către autoritatea publică responsabilă sau către alte entități abilitate se realizează prin mijloace care asigură protecția corespunzătoare a informațiilor, potrivit regimului juridic aplicabil.

XIII. REGULILE COMUNE DE APLICARE

ȘI CORELARE METODOLOGICĂ

94. Planul de securitate se corelează cu evaluarea riscurilor, planurile de continuitate, planurile de protecție fizică, planurile de protecție civilă, planurile de securitate cibernetică, planurile de intervenție, procedurile operaționale și alte documente

relevante ale gestionarului, precum și, după caz, cu documentele naționale privind continuitatea funcțiilor vitale ale statului, reziliența națională și managementul crizelor.

95. În cazul infrastructurilor critice naționale care implică interdependențe semnificative cu alte entități, gestionarul asigură includerea în Planul de securitate a mecanismelor de coordonare și de cooperare necesare.

96. Elaborarea și aprobarea Planului de securitate nu exclud obligația gestionarului de a respecta și celelalte cerințe legale, sectoriale, tehnice și procedurale aplicabile infrastructurii critice naționale.

97. În cazul în care Planul de securitate necesită modificări ca urmare a actualizării evaluării riscurilor, a producerii unui incident, a desfășurării unui exercițiu, a modificării infrastructurii sau a schimbării mediului de risc, gestionarul inițiază revizuirea acestuia potrivit anexei nr. 5.

98. Autoritățile publice responsabile pot elabora, cu informarea CNCPIC, instrucțiuni sectoriale și modele de documente pentru aplicarea prezentelor Norme în sectoarele și subsectoarele de competență.

99. Elaborarea, transmiterea, examinarea, avizarea, aprobarea și păstrarea Planului de securitate aferent infrastructurilor critice naționale din domeniul apărării, ordinii publice și securității statului se realizează cu respectarea regimului juridic aplicabil informațiilor atribuite la secret de stat, informațiilor sensibile privind infrastructurile critice naționale și altor categorii de informații protejate de lege. Accesul la Planul de securitate și la documentele aferente se acordă exclusiv persoanelor autorizate, prin mijloace corespunzătoare regimului juridic aplicabil informațiilor respective.

100. CNCPIC elaborează și pune la dispoziția autorităților publice responsabile și a gestionarilor modele-tip și instrumente metodologice standardizate pentru aplicarea prezentelor Norme, inclusiv formulare-cadru pentru Planul de securitate, modele de tabele de corelare, formulare-tip de raportare, modele de avizare, modele de revizuire și alte instrumente necesare pentru aplicarea unitară a procedurii de elaborare, avizare, aprobare, implementare, testare, revizuire și actualizare a Planului de securitate.

Anexa nr. 3

la Hotărârea Guvernului nr.483/2026

STRUCTURA-CADRU

a Planului de securitate al gestionarului

infrastructurii critice naționale

Secțiunea 1

Date generale

1. Capitolul privind datele generale cuprinde cel puțin:

1.1. denumirea completă a gestionarului infrastructurii critice naționale (denumit în continuare *gestionar*);

1.2. forma juridică de organizare;

1.3. sediul și datele de contact;

1.4. denumirea infrastructurii critice naționale;

1.5. sectorul și subsectorul în care aceasta se încadrează;

1.6. temeiul legal al desemnării infrastructurii critice naționale;

1.7. versiunea Planului de securitate al gestionarului (denumit în continuare *Plan de securitate*), data elaborării și data aprobării;

1.8. nivelul de acces, regimul de păstrare și circuitul documentului;

1.9. persoanele responsabile de elaborarea, actualizarea și păstrarea Planului de securitate;

1.10. datele de contact ale ofițerului de legătură pentru securitatea infrastructurii critice naționale.

Secțiunea a 2-a

Scopul, obiectivele și domeniul de aplicare

al Planului de securitate

2. Capitolul privind scopul, obiectivele și domeniul de aplicare cuprinde cel puțin:

2.1. scopul Planului de securitate;

2.2. obiectivele generale și specifice de securitate;

2.3. domeniul de aplicare al Planului de securitate;

2.4. infrastructura critică națională, serviciile, procesele, amplasamentele și structurile vizate;

2.5. limitele de aplicare ale Planului de securitate;

2.6. relația Planului de securitate cu alte planuri, proceduri și documente interne sau sectoriale;

2.7. ipotezele de lucru utilizate la elaborarea Planului de securitate.

3. Obiectivele Planului de securitate vizează cel puțin:

3.1. prevenirea și reducerea riscurilor prioritare;

3.2. protecția funcțiilor critice, a activelor critice și a proceselor esențiale;

3.3. menținerea sau reluarea serviciului esențial la un nivel minim acceptabil;

3.4. asigurarea răspunsului coordonat în cazul incidentelor;

3.5. recuperarea și restabilirea funcționării infrastructurii critice naționale;

3.6. protecția informațiilor sensibile, confidențiale sau clasificate;

3.7. cooperarea cu autoritățile publice responsabile și cu alte entități relevante;

3.8. menținerea contribuției infrastructurii critice naționale la continuitatea funcțiilor vitale ale statului și la consolidarea rezilienței naționale.

Secțiunea a 3-a

Descrierea infrastructurii critice naționale

și a serviciului esențial

4. Capitolul privind descrierea infrastructurii critice naționale și a serviciului esențial conține cel puțin:

4.1. descrierea generală a infrastructurii critice naționale;

4.2. localizarea, amplasamentele și componentele principale;

4.3. descrierea serviciului esențial furnizat;

4.4. importanța infrastructurii pentru continuitatea serviciului esențial;

4.5. principalele procese operaționale și fluxuri funcționale;

4.6. parametrii minimi de funcționare acceptabili;

4.7. condițiile în care se consideră afectată continuitatea serviciului esențial;

4.8. timpul maxim tolerabil de întrerupere, dacă acesta este stabilit;

4.9. nivelul minim de funcționare acceptabil în regim degradat;

4.10. implicațiile evaluării riscurilor asupra măsurilor de securitate, continuitate, răspuns și recuperare, inclusiv din perspectiva impactului potențial asupra continuității funcțiilor vitale ale statului și a efectelor sistemice sau intersectoriale generate de indisponibilizarea infrastructurii critice naționale.

Secțiunea a 4-a

Funcțiile critice, activele critice, procesele esențiale

și alte elemente importante

5. Capitolul privind funcțiile critice, activele critice, procesele esențiale și alte elemente importante pentru furnizarea serviciului esențial cuprinde cel puțin:

5.1. identificarea funcțiilor critice;

5.2. identificarea activelor critice;

5.3. identificarea proceselor esențiale;

5.4. identificarea altor elemente importante pentru menținerea sau reluarea serviciului esențial;

5.5. personalul-cheie și competențele indispensabile;

5.6. resursele critice necesare pentru funcționare;

5.7. ordinea de prioritate a funcțiilor critice, a activelor critice și a proceselor esențiale;

5.8. impactul indisponibilității acestora asupra serviciului esențial.

Secțiunea a 5-a

Dependențele și interdependențele

6. Capitolul privind dependențele și interdependențele cuprinde cel puțin:

6.1. dependențele interne dintre funcții, procese, sisteme și componente;

6.2. dependențele externe față de furnizori, prestatori, operatori și parteneri;

6.3. dependențele față de energie, apă, comunicații, sisteme informaționale, transport sau alte resurse critice;

6.4. interdependențele cu alte infrastructuri critice sau servicii esențiale;

6.5. vulnerabilitățile generate de aceste dependențe;

6.6. posibilele efecte în lanț sau în cascadă;

6.7. măsurile de reducere a dependențelor critice, după caz;

6.8. mecanismele de coordonare cu entitățile de care depinde funcționarea infrastructurii critice naționale.

Secțiunea a 6-a

Rezultatele evaluării riscurilor

7. Capitolul privind rezultatele evaluării riscurilor cuprinde cel puțin:

7.1. sinteza evaluării riscurilor efectuate;

7.2. riscurile identificate, grupate pe categorii;

7.3. scenariile de risc relevante;

7.4. vulnerabilitățile identificate;

7.5. evaluarea impactului și a probabilității;

7.6. scorurile și nivelurile de risc;

7.7. riscurile prioritare;

7.8. riscurile reziduale, după caz;

7.9. concluziile principale ale evaluării;

7.10. implicațiile evaluării riscurilor asupra măsurilor de securitate, continuitate, răspuns și recuperare.

8. La Planul de securitate se anexează fișele de evaluare a riscurilor, registrul riscurilor, matricea de risc și documentele-suport relevante, în condițiile regimului de acces aplicabil.

Secțiunea a 7-a

Măsurile existente de securitate

9. Capitolul privind măsurile existente de securitate descrie cel puțin:

9.1. măsurile fizice de protecție;

9.2. măsurile tehnice și tehnologice de protecție;

9.3. măsurile organizatorice și procedurale;

9.4. măsurile informaționale și cibernetice;

9.5. măsurile privind controlul accesului;

9.6. măsurile privind securitatea personalului;

9.7. măsurile privind detectarea, alertarea și reacția inițială;

9.8. măsurile privind monitorizarea și raportarea incidentelor;

9.9. măsurile privind protecția informațiilor;

9.10. măsurile privind redundanța și funcționarea alternativă, după caz.

10. Măsurile existente se descriu în raport cu riscurile, vulnerabilitățile, funcțiile

critice, activele critice sau procesele esențiale pe care le protejează.

Secțiunea a 8-a

Măsurile suplimentare și planul de implementare

11. Capitolul privind măsurile suplimentare și planul de implementare cuprinde măsurile necesare pentru tratarea riscurilor prioritare și remedierea vulnerabilităților identificate.

12. Pentru fiecare risc prioritar, Planul de securitate prevede cel puțin:

12.1. măsurile suplimentare necesare;

12.2. obiectivul fiecărei măsuri;

12.3. tipul măsurii: organizatorică, tehnică, procedurală, fizică, cibernetică, de continuitate, de răspuns, de recuperare sau alt tip relevant;

12.4. nivelul de prioritate;

12.5. responsabilul de implementare;

12.6. resursele necesare;

12.7. termenul de implementare;

12.8. indicatorii de realizare;

12.9. modalitatea de verificare;

12.10. riscul rezidual acceptat, după caz.

13. Măsurile suplimentare se stabilesc în funcție de nivelul de risc, de urgența intervenției, de capacitatea reală de implementare a gestionarului și de necesitatea asigurării continuității serviciului esențial.

14. Măsurile suplimentare se prezintă, de regulă, într-un tabel de implementare care conține cel puțin următoarele rubrici:

Nr. crt.	Risc vizat	Măsură propusă	Tip al măsurii	Responsabil	Termen	Resurse necesare	Indicator de realizare	Stadiu

Secțiunea a 9-a

Măsurile de continuitate a activității

15. Capitolul privind continuitatea activității cuprinde cel puțin:

15.1. măsurile de menținere a funcțiilor critice;

15.2. soluțiile de funcționare degradată, alternativă sau de rezervă;

15.3. prioritățile de menținere și de reluare a serviciului esențial;

15.4. resursele minime necesare pentru continuitate;

15.5. procedurile de activare a măsurilor de continuitate;

15.6. responsabilitățile structurilor și ale persoanelor implicate;

15.7. mecanismele de coordonare internă și externă;

15.8. timpul maxim tolerabil de întrerupere, dacă este stabilit;

15.9. obiectivele de timp pentru reluarea funcțiilor critice, după caz;

15.10. soluțiile de substituire, de relocare, de redundanță sau de funcționare alternativă.

Secțiunea a 10-a

Măsurile de răspuns, de notificare și de recuperare

16. Capitolul privind răspunsul, notificarea și recuperarea cuprinde cel puțin:

16.1. măsurile de reacție în cazul producerii unui incident;

16.2. procedurile de alertare, de informare și de escaladare;

16.3. măsurile de limitare a efectelor;

16.4. măsurile de restabilire treptată sau integrală a funcționării;

16.5. prioritățile de recuperare;

16.6. resursele necesare pentru recuperare;

16.7. modul de documentare a incidentelor și de valorificare a lecțiilor identificate;

16.8. fluxul intern de notificare a conducerii gestionarului;

16.9. fluxul de notificare a autorității publice responsabile;

16.10. fluxul de notificare a Centrului Național de Coordonare a Protecției Infrastructurilor Critice (denumit în continuare *CNCPIC*), după caz;

16.11. fluxul de notificare a altor autorități competente sau entități relevante, potrivit legislației aplicabile;

16.12. persoanele sau structurile responsabile de gestionarea incidentelor;

16.13. criteriile și nivelurile de escaladare a incidentelor care depășesc capacitatea

de răspuns a gestionarului sau generează efecte sistemice ori intersectoriale;

16.14. criteriile și procedura de informare a Centrului Național de Management al Crizelor, potrivit cadrului normativ aplicabil;

16.15. mecanismele de activare a coordonării interinstituționale în cadrul sistemului național de management al crizelor;

16.16. modalitatea de integrare a măsurilor de răspuns, de continuitate și de recuperare prevăzute în Planul de securitate în mecanismele de gestionare a unei crize la nivel național.

17. Procedurile de răspuns și de recuperare trebuie corelate cu scenariile de risc relevante și cu măsurile de continuitate prevăzute în Planul de securitate.

Secțiunea a 11-a

Organizarea, responsabilitățile și mecanismele

de coordonare

18. Capitolul privind organizarea, responsabilitățile și mecanismele de coordonare cuprinde cel puțin:

18.1. structurile interne implicate în aplicarea Planului de securitate;

18.2. atribuțiile conducerii gestionarului;

18.3. atribuțiile ofițerului de legătură;

18.4. atribuțiile structurilor operaționale, tehnice, administrative și de suport;

18.5. mecanismele de coordonare internă;

18.6. mecanismele de cooperare cu autoritățile publice responsabile, cu autoritățile competente și cu alte entități relevante;

18.7. mecanismele de coordonare cu furnizorii, cu prestatorii și cu partenerii critici;

18.8. procedurile de escaladare decizională în situații de perturbare sau de incident;

18.9. mecanismele de cooperare și coordonare cu Centrul Național de Management al Crizelor și cu alte autorități competente, în cazul incidentelor cu impact sistemic ori intersectorial.

Secțiunea a 12-a

Comunicarea, raportarea și schimbul de informații

19. Capitolul privind comunicarea, raportarea și schimbul de informații cuprinde cel puțin:

19.1. mecanismele de comunicare internă;

19.2. mecanismele de comunicare cu autoritatea publică responsabilă;

19.3. mecanismele de comunicare cu CNCPIC, după caz;

19.4. mecanismele de comunicare cu alte autorități competente;

19.5. comunicarea cu furnizorii, cu prestatorii, cu partenerii și cu alte entități relevante;

19.6. persoanele autorizate să transmită informații;

19.7. regulile privind comunicarea publică și comunicarea de criză, inclusiv corelarea acestora, după caz, cu mecanismele naționale de comunicare în situații de criză, în vederea asigurării unui mesaj instituțional coerent și unitar;

19.8. procedurile de raportare a incidentelor, a perturbărilor și a vulnerabilităților relevante;

19.9. mecanismele de schimb de informații privind riscurile, amenințările, vulnerabilitățile și măsurile de securitate.

20. Comunicarea publică privind incidentele care afectează infrastructura critică națională se realizează exclusiv de către persoanele desemnate sau autorizate în acest scop din cadrul gestionarului ori, după caz, din cadrul autorității publice responsabile sau al CNCPIC, în limitele competențelor legale și cu respectarea mecanismelor de coordonare interinstituțională, a legislației aplicabile, a regimului informațiilor protejate și a necesității de evitare a panicii, a dezinformării sau a afectării suplimentare a securității infrastructurii critice naționale.

Secțiunea a 13-a

Instruirea, testarea și exercițiile

21. Capitolul privind instruirea, testarea și exercițiile cuprinde cel puțin:

21.1. programul de instruire a personalului relevant;

21.2. instruirea ofițerului de legătură și a personalului-cheie;

21.3. tipurile de teste și de exerciții planificate;

21.4. frecvența testelor și a exercițiilor;

21.5. scenariile de testare relevante, inclusiv, după caz, scenarii de criză cu caracter intersectorial;

21.6. modul de evaluare a rezultatelor;

21.7. măsurile de remediere a deficiențelor constatate;

21.8. evidența instruirilor, a testelor și a exercițiilor desfășurate;

21.9. modalitatea de testare a cooperării și coordonării dintre gestionar, alți gestionari relevanți și autoritățile competente din cadrul sistemului național de management al crizelor.

Secțiunea a 14-a

Revizuirea și actualizarea Planului de securitate

22. Capitolul privind revizuirea și actualizarea Planului de securitate cuprinde cel puțin:

22.1. periodicitatea revizuirii Planului de securitate;

22.2. cazurile care determină revizuirea extraordinară;

22.3. persoanele și structurile responsabile de actualizare;

22.4. modul de aprobare a modificărilor;

22.5. evidența versiunilor și a modificărilor;

22.6. modul de reflectare în Planul de securitate a modificărilor rezultate din actualizarea evaluării riscurilor;

22.7. modul de informare a structurilor interne relevante cu privire la modificările operate;

22.8. mecanismul de retragere sau de arhivare a versiunilor depășite.

Secțiunea a 15-a

Regimul documentului, păstrarea

și circulația informațiilor

23. Capitolul privind regimul documentului cuprinde cel puțin:

23.1. nivelul de acces și regimul de confidențialitate;

23.2. persoanele autorizate să consulte, să utilizeze și să modifice Planul de securitate;

23.3. regulile de păstrare, de arhivare și de multiplicare;

23.4. modul de transmitere internă și externă;

23.5. protecția informațiilor sensibile, confidențiale sau clasificate, după caz;

23.6. evidența distribuirii Planului de securitate;

23.7. lista persoanelor sau a structurilor care au acces la Planul de securitate;

23.8. responsabilul de păstrarea versiunii oficiale;

23.9. măsurile de retragere a versiunilor neactuale.

Secțiunea a 16-a

Anexele Planului de securitate

24. La Planul de securitate se atașează, după caz, următoarele anexe:

24.1. fișele de evaluare a riscurilor;

24.2. registrul riscurilor;

24.3. matricea de risc;

24.4. schemele, hărțile, planurile de amplasament și diagramele funcționale;

24.5. listele contactelor operaționale;

24.6. registrele activelor critice și ale resurselor esențiale;

24.7. procedurile operaționale relevante;

24.8. planurile conexe sau extrase din acestea;

24.9. tabelul măsurilor suplimentare și al planului de implementare;

24.10. evidența instruirilor, a testelor și a exercițiilor;

24.11. notele de actualizare și evidența modificărilor;

24.12. lista persoanelor sau a structurilor cu acces la Planul de securitate;

24.13. evidența distribuirii Planului de securitate;

24.14. alte documente justificative necesare.

Secțiunea a 17-a

Cerințele minime de formă și de conținut

25. Planul de securitate trebuie să fie redactat clar, coerent și structurat astfel încât să permită utilizarea sa efectivă în condiții normale, precum și în situații de perturbare.

26. Informațiile incluse în Planul de securitate trebuie să fie actuale, verificabile, corelate între ele și conforme cu rezultatele evaluării riscurilor.

27. Planul de securitate nu poate avea caracter exclusiv descriptiv sau declarativ, ci trebuie să includă măsurile concrete, lista responsabililor, termenele, resursele, indicatorii

și mecanismele de aplicare.

28. Lipsa unuia sau a mai multe elemente esențiale prevăzute de prezenta anexă atrage necesitatea completării Planului de securitate ori, după caz, imposibilitatea avizării sau a recunoașterii echivalării acestuia.

29. În cazul în care anumite informații nu sunt aplicabile infrastructurii critice naționale evaluate, gestionarul indică în mod expres acest fapt și motivează neaplicabilitatea.

30. Planul de securitate se redactează în formă scrisă și se păstrează în condiții care asigură protecția informațiilor incluse în acesta.

Anexa nr. 4

la Hotărârea Guvernului nr.483/2026

NORME

metodologice privind echivalarea documentelor existente

cu Planul de securitate al gestionarului infrastructurii critice naționale

I. DISPOZIȚII GENERALE

1. Prezentele Norme stabilesc regulile și procedurile în baza cărora se constată dacă un document existent sau un set de documente existente, elaborate de către gestionarul infrastructurii critice naționale (denumit în continuare *gestionar*), acoperă integral ori în mod suficient cerințele minime aplicabile Planului de securitate al gestionarului (denumit în continuare *Plan de securitate*).

2. Prezentele Norme au ca scop evitarea duplicării nejustificate a documentelor interne deja existente, cu condiția ca acestea să fie relevante, actuale, aplicabile și conforme cu cerințele prezentei hotărâri.

3. Echivalarea nu are caracter automat și nu rezultă din simpla existență a unui document intern anterior, indiferent de denumirea acestuia.

4. Echivalarea se stabilește în funcție de conținutul efectiv al documentului sau al setului de documente, iar nu exclusiv în funcție de denumirea acestuia.

5. Recunoașterea echivalării nu exonerează gestionarul de obligația de a asigura caracterul complet, actual, aplicabil și verificabil al documentelor recunoscute ca echivalente.

6. Grila de echivalare a documentelor existente cu Planul de securitate se utilizează pentru verificarea corespondenței dintre documentele existente și structura-cadru prevăzută în anexa nr.3.

7. Documentele recunoscute ca echivalente produc efecte în limitele și în condițiile stabilite în actul de recunoaștere a echivalării.

II. DOCUMENTELE CARE POT FI PROPUSE SPRE ECHIVALARE

8. Pot fi propuse spre echivalare, după caz:

8.1. planurile de securitate internă;

8.2. planurile de continuitate a activității;

8.3. planurile de răspuns la incidente;

8.4. planurile de protecție fizică;

8.5. planurile de securitate informațională sau cibernetică;

8.6. planurile privind gestionarea situațiilor excepționale, protecția civilă ori apărarea împotriva incendiilor;

8.7. planurile de protecție antiteroristă, după caz;

8.8. planurile de localizare și lichidare a situațiilor de avarie, elaborate potrivit legislației din domeniul securității industriale;

8.9. seturile integrate de proceduri, regulamente, registre, instrucțiuni și alte documente interne relevante;

8.10. documentele privind managementul riscurilor, continuitatea, recuperarea și reziliența;

8.11. alte documente care, prin conținutul lor, acoperă cerințele minime ale Planului de securitate.

9. Echivalarea poate fi solicitată:

9.1. pentru un singur document;

9.2. pentru un set de documente, dacă acestea acoperă cumulativ cerințele minime aplicabile Planului de securitate;

9.3. pentru anumite capitole, secțiuni sau elemente ale Planului de securitate.

10. În cazul echivalării unui set de documente, gestionarul prezintă modul de corelare dintre documente și rolul fiecărui document în acoperirea structurii-cadru a Planului de securitate, prevăzută în anexa nr. 3.

III. CONDIȚIILE GENERALE ALE ECHIVALĂRII

11. Echivalarea se admite numai dacă documentul existent sau setul de documente existente:

11.1. este în vigoare la data solicitării;

11.2. este aprobat în mod legal de către organul sau persoana competentă;

11.3. este aplicabil infrastructurii critice naționale concrete pentru care se solicită echivalarea;

11.4. este corelat cu serviciul esențial furnizat prin infrastructura critică națională;

11.5. are un conținut clar, coerent și operațional;

11.6. este fundamentat, după caz, pe evaluarea riscurilor ori este compatibil cu rezultatele acesteia;

11.7. include măsuri concrete de securitate, continuitate, răspuns sau recuperare, după caz;

11.8. stabilește responsabilități, termene și mecanisme de implementare;

11.9. permite verificarea conformității sale cu cerințele minime aplicabile Planului de securitate;

11.10. poate fi examinat de către autoritatea publică responsabilă, în condițiile regimului de acces aplicabil.

12. Nu poate fi recunoscut drept echivalent un document care:

12.1. are caracter exclusiv descriptiv, declarativ ori general;

12.2. nu conține măsuri concrete, responsabilități și mecanisme de aplicare;

12.3. nu este adaptat infrastructurii critice naționale concrete;

12.4. nu reflectă serviciul esențial furnizat prin infrastructura critică națională;

12.5. este depășit, incomplet ori inaplicabil;

12.6. nu este corelat cu evaluarea riscurilor;

12.7. nu permite verificarea conformității sale cu cerințele minime aplicabile Planului de securitate;

12.8. nu poate fi pus la dispoziția autorității publice responsabile în condițiile legii.

13. În cazul în care unul sau mai multe elemente lipsesc ori sunt insuficient dezvoltate, echivalarea poate fi:

13.1. admisă parțial;

13.2. admisă condiționat, cu obligația completării documentului ori a setului de documente într-un termen stabilit;

13.3. respinsă.

IV. CERINȚELE MINIME

CARE TREBUIE ACOPERITE PRIN ECHIVALARE

14. Pentru a putea fi recunoscut drept echivalent integral, documentul existent sau setul de documente existente trebuie să acopere cel puțin următoarele elemente:

14.1. identificarea gestionarului, a infrastructurii critice naționale și a serviciului esențial furnizat;

14.2. scopul, obiectivele și domeniul de aplicare;

14.3. descrierea funcțiilor critice, a activelor critice, a proceselor esențiale și a elementelor importante;

14.4. identificarea dependențelor și a interdependențelor relevante;

14.5. existența unei evaluări documentate a riscurilor sau a unor elemente echivalente acesteia;

14.6. identificarea riscurilor relevante, a scenariilor de risc și a vulnerabilităților;

14.7. măsurile existente de securitate;

14.8. măsurile suplimentare necesare și modul de implementare a acestora;

14.9. măsurile de continuitate;

14.10. măsurile de răspuns, de notificare și de recuperare;

14.11. organizarea internă, responsabilitățile și mecanismele de coordonare;

14.12. comunicarea, raportarea și schimbul de informații;

14.13. modul de asigurare, după caz, a contribuției infrastructurii critice naționale la continuitatea funcțiilor vitale ale statului și mecanismele de coordonare cu autoritățile competente în situații de criză;

14.14. instruirea, testarea și exercițiile, după caz;

14.15. regulile de revizuire, de actualizare și de evidență a modificărilor;

14.16. regimul documentului și protecția informațiilor relevante.

15. Cerințele minime prevăzute la pct. 14 se analizează prin raportare la structura-cadru a Planului de securitate, prevăzută în anexa nr. 3.

16. În cazul în care documentul sau setul de documente acoperă doar o parte dintre cerințele minime, echivalarea poate fi admisă parțial, cu obligația completării elementelor neacoperite.

17. Pentru elementele neacoperite sau acoperite insuficient, gestionarul elaborează completări, secțiuni, anexe, proceduri ori documente suplimentare.

V. INIȚIEREA PROCEDURII DE ECHIVALARE

18. Procedura de echivalare se inițiază la solicitarea gestionarului.

19. Solicitarea de echivalare se formulează în scris și se depune la autoritatea publică responsabilă din sectorul sau subsectorul de competență.

20. Solicitarea de echivalare indică cel puțin:

20.1. infrastructura critică națională pentru care se solicită echivalarea;

20.2. documentul sau documentele propuse spre echivalare;

20.3. tipul echivalării solicitate: integrală, parțială sau condiționată;

20.4. justificarea solicitării;

20.5. mențiunea privind aprobarea și valabilitatea documentelor respective;

20.6. persoana responsabilă din partea gestionarului de susținerea procedurii de echivalare;

20.7. datele de contact ale ofițerului de legătură pentru securitatea infrastructurii critice naționale.

VI. DOCUMENTELE NECESARE

PENTRU ECHIVALARE

21. Solicitarea de echivalare se însoțește cel puțin de:

21.1. copia documentului sau a documentelor propuse spre echivalare;

21.2. nota de sinteză privind echivalarea;

21.3. grila de echivalare completată;

21.4. dovada aprobării documentului sau a documentelor respective;

21.5. informațiile privind versiunea în vigoare și data ultimei actualizări;

21.6. raportul evaluării riscurilor sau sinteza acestuia;

21.7. lista documentelor propuse spre echivalare;

21.8. informațiile privind aplicarea, testarea sau actualizarea documentelor, după caz;

21.9. alte documente justificative relevante, după caz.

22. În cazul în care se solicită echivalarea unui set de documente, gestionarul prezintă suplimentar:

22.1. lista integrală a documentelor;

22.2. rolul fiecărui document în acoperirea structurii-cadru a Planului de securitate;

22.3. modul de corelare dintre documente;

22.4. documentul central sau nota de sinteză care asigură unitatea și utilizarea coerentă a setului de documente.

23. În lipsa unei corelări clare între documentele prezentate, echivalarea nu poate fi admisă integral.

VII. GRILA DE ECHIVALARE

24. Echivalarea se analizează prin completarea unei grile de corespondență între structura-cadru a Planului de securitate și documentul existent sau setul de documente existente.

25. Grila de echivalare are următoarea structură minimă:

Nr. crt.	**Elementul minim obligatoriu al Planului de securitate**	**Existența în documentul propus spre echivalare: Da/Nu/Parțial**	**Denumirea documentului/ documentelor și capitolul/punctulconținutului relevant**	**Aprecierea suficienței**	**Observațiile/ completările necesare**
1.	Datele generale privind gestionarul și infrastructura critică națională				
2.	Scopul, obiectivele și domeniul de aplicare				
3.	Descrierea infrastructurii critice naționale și a serviciului esențial				
4.	Funcțiile critice, activele critice și procesele esențiale				

5. Dependențele și interdependențele
6. Rezultatele evaluării riscurilor
7. Scenariile de risc și vulnerabilitățile
8. Măsurile existente de securitate
9. Măsurile suplimentare și planul de implementare
10. Măsurile de continuitate a activității
11. Măsurile de răspuns, de notificare și de recuperare
12. Organizarea, responsabilitățile și mecanismele de coordonare
13. Comunicarea, raportarea și schimbul de informații
14. Instruirea, testarea și exercițiile
15. Revizuirea, actualizarea și evidența versiunilor
16. Regimul documentului, păstrarea și circulația informațiilor

26. În rubrica „Existența în documentul propus spre echivalare” se indică una dintre următoarele opțiuni:

26.1. „Da”, dacă elementul este acoperit integral;

26.2. „Parțial”, dacă elementul este acoperit incomplet sau necesită completări;

26.3. „Nu”, dacă elementul nu este acoperit.

27. În rubrica „Aprecierea suficienței conținutului” se indică, după caz:

27.1. „Suficient”;

27.2. „Parțial suficient”;

27.3. „Insuficient”.

28. În rubrica „Observațiile/completările necesare” se consemnează elementele lipsă, necorelările, necesitatea actualizării sau orice altă condiție necesară pentru admiterea echivalării.

29. Grila de echivalare se completează inițial de către gestionar și se verifică de către autoritatea publică responsabilă în procesul de examinare a solicitării de echivalare.

VIII. ANALIZA SOLICITĂRII DE ECHIVALARE

30. Echivalarea se analizează de către autoritatea publică responsabilă, în limitele competențelor legale.

31. În procesul de analiză se verifică cel puțin:

31.1. relevanța documentului pentru infrastructura critică națională vizată;

31.2. actualitatea și valabilitatea documentului;

31.3. integralitatea și suficiența conținutului;

31.4. caracterul operațional și aplicabil al măsurilor prevăzute;

31.5. corelarea documentului sau a setului de documente propus spre echivalare cu evaluarea riscurilor aferente infrastructurii critice naționale;

31.6. reflectarea măsurilor existente și a evaluării eficacității acestora;

31.7. existența și actualitatea registrului riscurilor, după caz;

31.8. existența responsabilităților, a termenelor și a mecanismelor de implementare;

31.9. existența regulilor de revizuire și de actualizare;

31.10. conformitatea cu structura-cadru prevăzută în anexa nr. 3;

31.11. regimul de protecție a informațiilor;

31.12. compatibilitatea documentului sau a setului de documente propuse spre echivalare, după caz, cu mecanismele naționale de management al crizelor și cu procedurile de cooperare interinstituțională aplicabile;

31.13. posibilitatea verificării documentului și a anexelor sale.

32. Analiza echivalării se realizează prin completarea și examinarea grilei de echivalare.

33. Autoritatea publică responsabilă examinează solicitarea de echivalare în termen de 14 zile lucrătoare de la data recepționării dosarului complet.

34. În cadrul procedurii de echivalare pot fi solicitate gestionarului:

34.1. clarificări suplimentare;

34.2. documentele sau anexele lipsă;

34.3. actualizarea unor informații;

34.4. completarea grilei de echivalare;

34.5. prezentarea modului practic de aplicare a documentului sau a documentelor propuse spre echivalare.

35. Termenul de examinare se suspendă de la data solicitării completărilor până la data recepționării informațiilor sau a documentelor solicitate.

36. Gestionarul transmite completările solicitate în termen de cinci zile lucrătoare de la data recepționării solicitării, dacă autoritatea publică responsabilă nu stabilește un alt termen justificat.

IX. REZULTATUL PROCEDURII DE ECHIVALARE

37. În urma analizei, rezultatul procedurii de echivalare poate fi:

37.1. echivalare admisă integral;

37.2. echivalare admisă parțial;

37.3. echivalare admisă condiționat;

37.4. echivalare respinsă.

38. Echivalarea se admite integral în cazul în care toate elementele esențiale prevăzute de prezenta hotărâre și de structura-cadru a Planului de securitate sunt identificate și apreciate ca fiind suficiente.

39. Echivalarea se admite parțial în cazul în care documentul sau setul de documente acoperă numai anumite capitole, secțiuni ori cerințe ale Planului de securitate.

40. În cazul echivalării admise parțial, gestionarul completează elementele neacoperite prin elaborarea unor secțiuni, anexe sau documente suplimentare.

41. Echivalarea se admite condiționat în cazul în care:

41.1. anumite elemente sunt parțial suficiente;

41.2. lipsesc elemente neesențiale sau care pot fi completate într-un termen rezonabil;

41.3. este necesară completarea ori corelarea unor documente existente;

41.4. documentul sau setul de documente poate deveni conform prin aplicarea unor măsuri de remediere clar determinate.

42. În cazul echivalării admise condiționat se stabilesc în mod expres:

42.1. elementele care urmează a fi completate, corectate sau actualizate;

42.2. termenul de remediere;

42.3. documentele sau dovezile care urmează a fi prezentate ulterior;

42.4. consecințele neîndeplinirii condițiilor stabilite.

43. Echivalarea se respinge în cazul în care:

43.1. documentul sau setul de documente nu este relevant pentru infrastructura critică națională concretă;

43.2. lipsesc elementele esențiale;

43.3. documentul este depășit, incomplet ori inaplicabil;

43.4. documentul nu este corelat cu evaluarea riscurilor;

43.5. documentul nu permite verificarea măsurilor, a responsabilităților și a mecanismelor de aplicare;

43.6. documentul nu poate fi examinat în condițiile regimului de acces aplicabil.

44. Respingerea echivalării nu exonerează gestionarul de obligația de a elabora și a transmite spre avizare Planul de securitate în termenul prevăzut de Normele din anexa nr. 2. Inițierea și desfășurarea procedurii de echivalare nu suspendă și nu prelungește termenul stabilit pentru elaborarea și transmiterea spre avizare a Planului de securitate.

X. ACTUL DE RECUNOAȘTERE

SAU DE RESPINGERE A ECHIVALĂRII

45. Rezultatul examinării se consemnează în actul de recunoaștere sau de respingere a echivalării, emis de către autoritatea publică responsabilă.

46. Actul de recunoaștere sau de respingere a echivalării cuprinde cel puțin:

46.1. datele de identificare ale gestionarului;

46.2. denumirea infrastructurii critice naționale;

46.3. sectorul sau subsectorul de competență;

46.4. documentele analizate;

46.5. temeiul solicitării;

46.6. grila de echivalare sau sinteza acesteia;

46.7. concluzia examinării;

46.8. forma echivalării admise, după caz: integrală, parțială sau condiționată;

46.9. elementele recunoscute ca echivalente;

46.10. elementele care necesită a fi completate, actualizate sau corelate;

46.11. termenul de remediere, după caz;

46.12. obligațiile gestionarului privind aplicarea, testarea, revizuirea și actualizarea documentelor recunoscute ca echivalente;

46.13. data emiterii;

46.14. semnătura persoanei autorizate.

47. În cazul echivalării admise integral, documentul sau setul de documente recunoscut ca echivalent produce aceleași efecte funcționale ca Planul de securitate.

48. În cazul echivalării admise parțial sau condiționat, documentele recunoscute ca echivalente se completează cu secțiunile, anexele sau documentele necesare pentru acoperirea integrală a cerințelor minime ale Planului de securitate.

49. Autoritatea publică responsabilă ține evidența solicitărilor de echivalare, a documentelor analizate și a actelor emise.

XI. EFECTELE ECHIVALĂRII

50. Documentul sau setul de documente recunoscut ca echivalent produce efectele funcționale ale Planului de securitate, în limitele și în condițiile stabilite prin actul de recunoaștere a echivalării.

51. În cazul echivalării admise, gestionarului îi revine obligația de a asigura:

51.1. menținerea valabilității documentului sau a documentelor recunoscute;

51.2. aplicarea efectivă a măsurilor prevăzute;

51.3. actualizarea și revizuirea acestora în condițiile prevăzute de lege și de prezenta hotărâre;

51.4. păstrarea coerenței între documentele recunoscute ca echivalente și situația reală a infrastructurii critice naționale;

51.5. protecția informațiilor conținute în documentele recunoscute ca echivalente.

52. Recunoașterea echivalării nu exonerează gestionarul de obligația de a completa sau de a actualiza documentele recunoscute ca echivalente în cazul în care intervin schimbări semnificative.

XII. REVIZUIREA DOCUMENTELOR RECUNOSCUTE CA ECHIVALENTE

53. Documentele recunoscute ca echivalente se supun acelorași cerințe privind revizuirea periodică și revizuirea extraordinară aplicabile Planului de securitate.

54. Gestionarul notifică autorității publice responsabile orice modificare a documentului sau a setului de documente recunoscut ca echivalent, în termen de cel mult 10 zile lucrătoare de la data aprobării sau a intrării în vigoare a modificării. Modificările substanțiale se reflectă în documentația de echivalare actualizată și se transmit autorității publice responsabile odată cu notificarea.

55. În cazul în care, în urma revizuirii sau a modificărilor intervenite, documentele recunoscute ca echivalente nu mai acoperă cerințele minime aplicabile Planului de securitate, echivalarea se reconsideră.

56. În cazul prevăzut la pct. 55, autoritatea publică responsabilă poate dispune, după caz:

56.1. menținerea echivalării, dacă neconformitățile sunt minore și remediabile;

56.2. acordarea unui termen de remediere;

56.3. încetarea recunoașterii echivalării și obligarea gestionarului la elaborarea ori completarea Planului de securitate în formă distinctă.

57. Echivalarea își pierde valabilitatea în cazul în care:

57.1. documentul recunoscut ca echivalent este abrogat, înlocuit sau își încetează aplicabilitatea;

57.2. infrastructura critică națională suferă modificări substanțiale;

57.3. evaluarea riscurilor indică riscuri noi sau modificări semnificative ale profilului de risc;

57.4. documentul nu mai acoperă cerințele minime ale Planului de securitate;

57.5. documentul nu mai este implementat sau verificabil;

57.6. sunt constatate deficiențe majore în urma testării, a controlului, a auditului sau

a incidentelor;

57.7. intervin modificări semnificative ale cadrului normativ național în domeniul managementului crizelor, rezilienței sau protecției infrastructurilor critice, care impun revizuirea documentului ori a setului de documente recunoscut ca echivalent.

XIII. NOTA DE SINTEZĂ PRIVIND ECHIVALAREA

58. Solicitarea de echivalare se însoțește de nota de sinteză întocmită de către gestionar.

59. Nota de sinteză privind echivalarea cuprinde cel puțin:

59.1. datele de identificare ale gestionarului;

59.2. denumirea infrastructurii critice naționale;

59.3. lista documentelor propuse spre echivalare;

59.4. justificarea solicitării;

59.5. descrierea succintă a conținutului relevant al documentelor;

59.6. mențiunea privind aprobarea și valabilitatea acestora;

59.7. modul de corelare a documentelor cu structura-cadru a Planului de securitate;

59.8. confirmarea asumării de către conducerea gestionarului.

XIV. PROTECȚIA INFORMAȚIILOR

60. Documentele propuse spre echivalare, grila de echivalare, nota de sinteză, actul de recunoaștere sau de respingere a echivalării, precum și documentele aferente se gestionează cu respectarea regimului juridic aplicabil informațiilor atribuite la secret de stat, datelor cu caracter personal, informațiilor sensibile privind infrastructurile critice naționale și altor categorii de informații protejate de lege.

61. Examinarea și recunoașterea echivalenței documentelor aferente infrastructurilor critice naționale din domeniul apărării, ordinii publice și securității statului se realizează cu respectarea regimului juridic aplicabil informațiilor atribuite la secret de stat, informațiilor sensibile privind infrastructurile critice naționale și altor categorii de informații protejate de lege. Transmiterea, consultarea, verificarea, păstrarea și restituirea documentelor propuse spre echivalare se efectuează prin mijloace și de către persoane autorizate, în condițiile cadrului normativ aplicabil.

62. Accesul la documentele propuse spre echivalare se acordă exclusiv persoanelor care au atribuții directe și justifică necesitatea de a lucra cu informațiile respective.

63. Transmiterea documentelor propuse spre echivalare se realizează prin mijloace care asigură protecția corespunzătoare a informațiilor, în conformitate cu regimul juridic

aplicabil.

64. Informațiile privind vulnerabilitățile, scenariile de risc, măsurile de securitate, capacitățile de răspuns, punctele sensibile și interdependențele critice se protejează corespunzător nivelului de risc generat de divulgarea acestora.

XV. REGULILE COMUNE DE APLICARE

ȘI DE CORELARE METODOLOGICĂ

65. Procedura de echivalare se aplică în mod proporțional, fără a diminua nivelul de protecție, securitate și continuitate necesar pentru infrastructura critică națională.

66. Documentul sau setul de documente recunoscut ca echivalent trebuie să permită:

66.1. identificarea clară a riscurilor relevante;

66.2. organizarea măsurilor de securitate;

66.3. asigurarea continuității serviciului esențial;

66.4. coordonarea răspunsului și a recuperării;

66.5. verificarea, actualizarea și revizuirea periodică.

67. Echivalarea documentelor existente cu Planul de securitate nu exonerează gestionarul de obligația de a respecta cerințele legale, sectoriale, tehnice și procedurale aplicabile infrastructurii critice naționale.

68. Autoritățile publice responsabile pot elabora modele de grile, instrucțiuni sectoriale sau recomandări pentru aplicarea prezentelor Norme, cu informarea Centrului Național de Coordonare a Protecției Infrastructurilor Critice.

69. Centrul Național de Coordonare a Protecției Infrastructurilor Critice emite recomandări metodologice în vederea asigurării aplicării unitare a procedurii de echivalare.

70. Documentele recunoscute ca echivalente trebuie să permită atingerea aceluiași nivel de protecție, continuitate, răspuns, recuperare și reziliență ca Planul de securitate elaborat potrivit structurii-cadru prevăzute în anexa nr. 3.

71. Gestionarul asigură trasabilitatea corespondenței dintre cerințele minime ale Planului de securitate și documentele existente propuse spre echivalare, inclusiv prin întocmirea și menținerea unui registru intern sau a unui tabel de corespondență, în care se indică documentele, secțiunile, procedurile ori anexele prin care fiecare cerință este acoperită integral sau parțial.

Anexa nr. 5

la Hotărârea Guvernului nr.483/2026

NORME

metodologice privind revizuirea și actualizarea Planului de securitate

al gestionarului infrastructurii critice naționale

I. DISPOZIȚII GENERALE

1. Prezentele Norme stabilesc modul de revizuire și de actualizare a Planului de securitate al gestionarului infrastructurii critice naționale (denumit în continuare *Plan de securitate*).

2. Revizuirea și actualizarea Planului de securitate au drept scop menținerea caracterului actual, aplicabil, coerent și eficient al acestuia, în raport cu evoluția riscurilor, modificările infrastructurii critice naționale, schimbările operaționale, tehnologice, organizaționale, legislative sau sectoriale, precum și cu lecțiile identificate în urma incidentelor, testărilor, exercițiilor, auditurilor ori a controalelor.

3. În sensul prezentelor Norme, următorii termeni se definesc după cum urmează:

3.1. *actualizare* – modificare punctuală a unor date, capitole, anexe, proceduri, responsabilități sau măsuri din Planul de securitate, fără schimbarea arhitecturii generale a acestuia;

3.2. *revizuire* – proces de reexaminare sistematică a Planului de securitate în vederea verificării actualității, aplicabilității, conformității și corelării acestuia cu evaluarea riscurilor și cu situația reală a infrastructurii critice naționale;

3.3. *revizuire periodică* – revizuire realizată la intervale regulate, potrivit termenelor stabilite de prezentele Norme sau de reglementările sectoriale aplicabile;

3.4. *revizuire extraordinară* – revizuire inițiată ca urmare a producerii unui incident, a apariției unor riscuri, vulnerabilități ori modificări semnificative sau la solicitarea autorității publice responsabile.

4. Revizuirea și actualizarea Planului de securitate se realizează de către gestionarul infrastructurii critice naționale (denumit în continuare *gestionar*), în cooperare cu structurile interne relevante și, după caz, cu autoritatea publică responsabilă din sectorul sau subsectorul de competență.

5. Coordonarea operațională a procesului de revizuire și actualizare a Planului de securitate se realizează de către ofițerul de legătură pentru securitatea infrastructurii critice naționale, fără a substitui responsabilitatea conducerii gestionarului.

6. Revizuirea și actualizarea Planului de securitate se realizează cu respectarea cerințelor privind protecția informațiilor atribuite la secret de stat, datelor cu caracter personal, informațiilor sensibile privind infrastructurile critice naționale și altor categorii de informații protejate de lege.

7. Revizuirea și actualizarea Planului de securitate aferent infrastructurilor critice

naționale din domeniul apărării, ordinii publice și securității statului se realizează cu respectarea regimului juridic aplicabil informațiilor atribuite la secret de stat, informațiilor sensibile privind infrastructurile critice naționale și altor categorii de informații protejate de lege. Transmiterea, examinarea, aprobarea și păstrarea versiunilor revizuite sau actualizate se efectuează prin mijloace și de către persoane autorizate.

II. REVIZUIREA PERIODICĂ

8. Planul de securitate se revizuiește periodic, cel puțin o dată la doi ani, cu excepția cazurilor în care prin lege, prin actul de desemnare a infrastructurii critice naționale sau prin reglementări sectoriale este prevăzut un termen mai scurt. Revizuirea periodică se realizează în corelare cu testarea periodică a Planului de securitate prevăzută în anexa nr. 2, iar rezultatele testărilor, exercițiilor și simulărilor se valorifică în procesul de revizuire și de actualizare a acestuia.

9. Revizuirea periodică urmărește verificarea:

9.1. datelor privind gestionarul și infrastructura critică națională;

9.2. descrierii serviciului esențial furnizat;

9.3. evaluării riscurilor și a nivelurilor de risc stabilite;

9.4. relevanței riscurilor identificate;

9.5. funcțiilor critice, a activelor critice și a proceselor esențiale;

9.6. dependențelor și a interdependențelor;

9.7. actualității și eficacității măsurilor existente de securitate, prevenire, continuitate, răspuns și recuperare;

9.8. existenței și actualității registrului riscurilor aferente infrastructurii critice naționale;

9.9. gradului de implementare a măsurilor prevăzute în Planul de securitate;

9.10. funcționalității mecanismelor de notificare, comunicare și coordonare;

9.11. actualității listelor de contacte, a responsabilităților și a procedurilor asociate;

9.12. rezultatelor instruirilor, testelor și exercițiilor desfășurate;

9.13. necesității completării, a modificării sau a eliminării unor capitole, secțiuni ori anexe.

10. Revizuirea periodică se consemnează în nota de actualizare/revizuire, întocmită de către gestionar.

11. În cazul în care revizuirea periodică nu identifică necesitatea modificării Planului de securitate, acest fapt se consemnează în nota de actualizare/revizuire, cu indicarea

motivelor.

III. REVIZUIREA EXTRAORDINARĂ

12. Revizuirea extraordinară se inițiază ori de câte ori intervin evenimente, modificări sau constatări care pot afecta actualitatea, aplicabilitatea, conformitatea sau eficiența Planului de securitate.

13. Revizuirea extraordinară se inițiază, în special, în următoarele situații:

13.1. producerea unui incident major care afectează sau poate afecta infrastructura critică națională ori serviciul esențial furnizat;

13.2. producerea unei perturbări semnificative a funcționării infrastructurii critice naționale;

13.3. identificarea unor riscuri, amenințări, vulnerabilități sau scenarii de risc noi;

13.4. modificarea nivelului riscurilor existente;

13.5. modificarea evaluării riscurilor sau a registrului riscurilor;

13.6. modificări structurale, tehnologice, funcționale sau organizaționale ale infrastructurii critice naționale;

13.7. modificarea funcțiilor critice, a activelor critice sau a proceselor esențiale;

13.8. modificarea dependențelor sau a interdependențelor relevante;

13.9. schimbarea furnizorilor critici, a prestatorilor, a lanțurilor de aprovizionare sau a mecanismelor de suport tehnic;

13.10. obținerea unor rezultate relevante în urma auditurilor, controalelor, testărilor, exercițiilor sau simulărilor;

13.11. constatarea unor deficiențe în aplicarea măsurilor de securitate, continuitate, răspuns sau recuperare;

13.12. modificarea cadrului normativ aplicabil sau a cerințelor sectoriale;

13.13. modificarea actului de desemnare a infrastructurii critice naționale;

13.14. schimbarea regimului de proprietate, administrare, operare sau control asupra infrastructurii critice naționale;

13.15. solicitarea autorității publice responsabile;

13.16. solicitarea Centrului Național de Coordonare a Protecției Infrastructurilor Critice (denumit în continuare *CNCPIC*), în condițiile legii;

13.17. declararea unei stări de criză sau modificarea nivelului de alertă la nivel

național, în cazul în care aceasta afectează ori poate afecta funcționarea infrastructurii critice naționale sau continuitatea serviciului esențial furnizat;

13.18. constatarea faptului că documentele recunoscute ca echivalente nu mai acoperă cerințele minime ale Planului de securitate;

13.19. orice altă situație care poate afecta protecția, securitatea, continuitatea, răspunsul, recuperarea sau reziliența infrastructurii critice naționale.

14. Revizuirea extraordinară se inițiază fără întârziere după constatarea situației care o determină.

15. În cazul producerii unui incident major sau al identificării unei vulnerabilități semnificative, gestionarul poate aplica măsuri temporare sau compensatorii până la finalizarea revizuirii Planului de securitate.

IV. INIȚIEREA PROCESULUI DE REVIZUIRE

SAU DE ACTUALIZARE

16. Procesul de revizuire sau de actualizare a Planului de securitate se inițiază prin decizia conducerii gestionarului sau la propunerea ofițerului de legătură, a structurii responsabile de securitate, continuitate, managementul riscurilor ori a altei structuri interne relevante.

17. Revizuirea sau actualizarea poate fi inițiată și ca urmare a solicitării autorității publice responsabile, în limitele competențelor legale.

18. Decizia de inițiere a procesului de revizuire sau de actualizare stabilește, după caz:

18.1. temeiul revizuirii sau al actualizării;

18.2. obiectul revizuirii sau al actualizării;

18.3. capitolele, secțiunile, anexele sau procedurile vizate;

18.4. structurile și persoanele implicate;

18.5. coordonatorul procesului;

18.6. termenul de realizare;

18.7. modul de documentare a rezultatelor.

19. În funcție de complexitatea modificărilor, gestionarul poate constitui un grup de lucru intern sau o comisie internă pentru revizuirea ori actualizarea Planului de securitate.

V. DESFĂȘURAREA REVIZUIRII

20. Revizuirea Planului de securitate include examinarea cel puțin a următoarelor

elemente:

20.1. evaluarea riscurilor și registrul riscurilor;

20.2. scenariile de risc relevante;

20.3. funcțiile critice, activele critice și procesele esențiale;

20.4. dependențele și interdependențele;

20.5. măsurile existente de securitate;

20.6. măsurile suplimentare și stadiul implementării acestora;

20.7. măsurile de asigurare a continuității activității;

20.8. măsurile de răspuns, de notificare și de recuperare;

20.9. responsabilitățile interne și mecanismele de coordonare;

20.10. mecanismele de comunicare, de raportare și de schimb de informații;

20.11. programul de instruire, de testare și de desfășurare a exercițiilor;

20.12. anexele, registrele, listele de contacte și procedurile asociate;

20.13. regimul documentului și măsurile de protecție a informațiilor.

21. În cadrul revizuirii se verifică dacă Planul de securitate:

21.1. corespunde situației reale a infrastructurii critice naționale;

21.2. este corelat cu evaluarea actuală a riscurilor;

21.3. conține măsuri proporționale cu nivelul riscurilor;

21.4. stabilește responsabilități clare;

21.5. prevede termene, resurse și indicatori de realizare;

21.6. permite răspunsul coordonat în caz de incident;

21.7. asigură continuitatea serviciului esențial;

21.8. permite recuperarea funcțiilor critice afectate;

21.9. este cunoscut și aplicabil de către structurile responsabile;

21.10. necesită modificări, completări sau actualizări.

22. În cazul în care, în urma revizuirii, se constată modificarea profilului de risc, gestionarul actualizează evaluarea riscurilor potrivit Normelor metodologice privind

evaluarea riscurilor la adresa infrastructurilor critice naționale prevăzute în anexa nr. 1.

23. În cazul în care, în urma revizuirii, se constată necesitatea modificării conținutului Planului de securitate, gestionarul actualizează capitolele, secțiunile, anexele sau procedurile afectate.

VI. CLASIFICAREA MODIFICĂRILOR

24. Modificările operate în Planul de securitate se clasifică, după caz, în:

24.1. modificări minore;

24.2. modificări semnificative;

24.3. modificări substanțiale.

25. Modificările minore sunt modificările care nu afectează conținutul de fond al Planului de securitate, profilul de risc, măsurile esențiale, responsabilitățile principale sau mecanismele de notificare și coordonare.

26. Pot constitui modificări minore:

26.1. actualizarea datelor de contact;

26.2. actualizarea denumirilor structurilor interne, fără schimbarea atribuțiilor;

26.3. corectarea erorilor materiale;

26.4. actualizarea listelor operaționale, fără afectarea mecanismelor principale;

26.5. efectuarea unor ajustări redacționale sau de formă care nu afectează conținutul de fond al Planului de securitate.

27. Modificările semnificative sunt modificările care afectează anumite capitole, secțiuni, anexe, măsuri, responsabilități sau proceduri ale Planului de securitate, fără a impune revizuirea integrală a acestuia.

28. Pot constitui modificări semnificative:

28.1. introducerea sau modificarea unor măsuri de securitate, continuitate, răspuns ori recuperare;

28.2. modificarea responsabilităților operaționale principale;

28.3. modificarea unor proceduri de notificare, comunicare sau escaladare;

28.4. modificarea unor dependențe sau interdependențe relevante;

28.5. modificarea unor anexe tehnice importante;

28.6. modificarea unor termene, resurse sau indicatori de implementare.

29. Modificările substanțiale sunt modificările care afectează arhitectura generală a Planului de securitate, profilul de risc, funcțiile critice, activele critice, serviciul esențial, măsurile principale de securitate sau capacitatea de continuitate și recuperare.

30. Modificările substanțiale impun revizuirea integrală a Planului de securitate sau, după caz, elaborarea unei versiuni noi a acestuia.

VII. REZULTATUL REVIZUIRII

ȘI APROBAREA MODIFICĂRILOR

31. În urma revizuirii, gestionarul poate decide, după caz:

31.1. menținerea Planului de securitate fără modificări;

31.2. actualizarea parțială a Planului de securitate;

31.3. revizuirea integrală a Planului de securitate;

31.4. elaborarea unei versiuni noi a Planului de securitate;

31.5. actualizarea evaluării riscurilor;

31.6. actualizarea documentelor recunoscute ca echivalente;

31.7. transmiterea Planului de securitate spre reavizare, în cazurile prevăzute de prezentele Norme.

32. Rezultatele procesului de actualizare sau de revizuire se consemnează în nota de actualizare/revizuire, întocmită de către gestionar.

33. Nota de actualizare/revizuire include cel puțin:

33.1. temeiul actualizării sau al revizuirii;

33.2. descrierea situației care a determinat modificarea;

33.3. elementele Planului de securitate afectate;

33.4. impactul asupra evaluării riscurilor;

33.5. modificările propuse;

33.6. concluzia;

33.7. responsabilii;

33.8. termenele de implementare;

33.9. necesitatea reavizării, după caz;

33.10. concluziile rezultate din analiza lecțiilor identificate în urma gestionării

incidentelor, a situațiilor de criză și a exercițiilor interinstituționale, după caz;

33.11. măsurile stabilite pentru valorificarea și implementarea lecțiilor identificate, responsabilii și termenele aferente.

34. Modificările minore se aprobă potrivit procedurilor interne ale gestionarului și se consemnează în evidența modificărilor Planului de securitate.

35. Modificările semnificative și modificările substanțiale se aprobă de către conducătorul gestionarului sau de către persoana competentă desemnată potrivit actelor interne aplicabile.

36. Versiunea actualizată a Planului de securitate indică în mod expres data intrării în vigoare, numărul versiunii și modificările operate față de versiunea anterioară.

VIII. REAVIZAREA PLANULUI DE SECURITATE

37. Planul de securitate actualizat se transmite spre reavizare autorității publice responsabile în cazul în care modificările afectează:

37.1. evaluarea riscurilor;

37.2. riscurile prioritare;

37.3. funcțiile critice, activele critice sau procesele esențiale;

37.4. serviciul esențial furnizat;

37.5. măsurile esențiale de securitate, continuitate, răspuns sau recuperare;

37.6. responsabilitățile principale;

37.7. mecanismele de notificare, comunicare, raportare sau coordonare;

37.8. dependențele ori interdependențele relevante;

37.9. documentele recunoscute ca echivalente;

37.10. regimul documentului sau măsurile de protecție a informațiilor, în cazul în care modificarea poate afecta accesul ori circulația informațiilor;

37.11. mecanismele de cooperare și coordonare cu autoritățile competente din cadrul sistemului național de management al crizelor.

38. Modificările minore care nu afectează elementele prevăzute la pct. 37 nu sunt supuse reavizării, cu condiția consemnării acestora în evidența modificărilor Planului de securitate.

39. Autoritatea publică responsabilă examinează Planul de securitate actualizat, în conformitate cu procedura de avizare prevăzută în anexa nr. 2.

40. În cazul în care autoritatea publică responsabilă constată că modificările efectuate nu impun reavizarea Planului de securitate, aceasta poate lua act de actualizare și poate solicita, după caz, păstrarea documentelor justificative în evidența gestionarului.

IX. EFECTELE REVIZUIRII ASUPRA DOCUMENTELOR ECHIVALATE

41. În cazul în care Planul de securitate este constituit integral sau parțial din documente recunoscute ca echivalente, revizuirea acestuia include și verificarea documentelor echivalate.

42. Documentele recunoscute ca echivalente se revizuiesc ori de câte ori intervin modificări care afectează actualitatea, aplicabilitatea sau conformitatea acestora cu cerințele minime prevăzute de structura-cadru a Planului de securitate, conform anexei nr. 3.

43. În cazul în care documentele recunoscute ca echivalente nu mai acoperă integral sau suficient cerințele Planului de securitate, gestionarul:

43.1. actualizează documentele respective;

43.2. completează documentele cu secțiuni sau anexe suplimentare;

43.3. solicită o nouă echivalare, după caz;

43.4. elaborează Planul de securitate în formă distinctă, dacă echivalarea nu mai poate fi menținută.

44. Gestionarul notifică autorității publice responsabile încetarea, suspendarea sau modificarea substanțială a documentului ori a setului de documente recunoscut ca echivalent, în termen de cel mult 10 zile lucrătoare de la data intervenirii acesteia.

X. EVIDENȚA ȘI TRASABILITATEA REVIZUIRII

45. Gestionarul asigură evidența și trasabilitatea tuturor revizuirilor și actualizărilor Planului de securitate.

46. Evidența revizuirilor și a actualizărilor cuprinde cel puțin:

46.1. data inițierii revizuirii sau a actualizării;

46.2. temeiul revizuirii sau a actualizării;

46.3. capitolele, secțiunile, anexele sau procedurile afectate;

46.4. descrierea modificărilor operate;

46.5. persoanele sau structurile responsabile;

46.6. data aprobării modificărilor;

46.7. necesitatea reavizării, după caz;

46.8. data transmiterii spre reavizare, după caz;

46.9. versiunea nouă a Planului de securitate;

46.10. documentele justificative.

47. Gestionarul asigură:

47.1. păstrarea notelor de actualizare/revizuire;

47.2. păstrarea versiunilor anterioare ale Planului de securitate;

47.3. evidența modificărilor operate;

47.4. păstrarea documentelor justificative care au stat la baza revizuirii;

47.5. retragerea sau arhivarea versiunilor depășite;

47.6. informarea structurilor interne relevante cu privire la versiunea aplicabilă a Planului de securitate.

48. Versiunile anterioare ale Planului de securitate se păstrează potrivit regimului juridic aplicabil documentului și regulilor interne privind arhivarea.

XI. PROTECȚIA INFORMAȚIILOR

ÎN PROCESUL DE REVIZUIRE ȘI DE ACTUALIZARE

49. Documentele întocmite în procesul de revizuire și de actualizare, inclusiv notele de actualizare/revizuire, versiunile anterioare, documentele justificative și anexele afectate, se gestionează cu respectarea regimului juridic aplicabil informațiilor atribuite la secret de stat, datelor cu caracter personal, informațiilor sensibile privind infrastructurile critice naționale și altor categorii de informații protejate de lege.

50. Accesul la documentele aferente procesului de revizuire și de actualizare se acordă exclusiv persoanelor care au atribuții directe și justifică necesitatea de a lucra cu informațiile respective.

51. Transmiterea documentelor aferente revizuirii și actualizării către autoritatea publică responsabilă sau către alte entități abilitate se realizează prin mijloace care asigură protecția corespunzătoare a informațiilor, potrivit regimului juridic aplicabil.

52. Informațiile privind vulnerabilitățile, scenariile de risc, măsurile de securitate, capacitățile de răspuns, punctele sensibile, interdependențele critice și deficiențele constatate în procesul de revizuire se protejează corespunzător nivelului de risc generat de divulgarea acestora.

XII. REGULILE COMUNE DE APLICARE

ȘI DE CORELARE METODOLOGICĂ

53. Revizuirea și actualizarea Planului de securitate nu exonerează gestionarul de obligația de a aplica măsurile de securitate, continuitate, răspuns și recuperare în vigoare.

54. În perioada revizuirii, gestionarul asigură continuitatea aplicării măsurilor existente și, după caz, aplicarea unor măsuri temporare sau compensatorii pentru riscurile identificate.

55. Revizuirea și actualizarea Planului de securitate se realizează fără a diminua nivelul de protecție, de continuitate și de reziliență al infrastructurii critice naționale și trebuie să contribuie, după caz, la consolidarea rezilienței naționale și la asigurarea continuității funcțiilor vitale ale statului, în conformitate cu cadrul normativ aplicabil în domeniul managementului crizelor.

56. Autoritățile publice responsabile pot elabora instrucțiuni sectoriale, recomandări, modele de registre sau instrumente de suport pentru aplicarea prezentelor Norme, cu informarea CNCPIC.

57. CNCPIC pune la dispoziția autorităților publice responsabile și a gestionarilor modele de note de actualizare/revizuire, registre de evidență a modificărilor și alte instrumente metodologice de suport.

58. Prevederile prezentelor Norme se aplică în mod corespunzător și documentelor recunoscute ca echivalente cu Planul de securitate.

Anexa nr. 6

la Hotărârea Guvernului nr.483/2026

NORME

metodologice privind desemnarea, statutul funcțional și atribuțiile

ofițerului de legătură pentru securitatea infrastructurii critice naționale

I. DISPOZIȚII GENERALE

1. Prezentele Norme stabilesc modul de desemnare, statutul funcțional, cerințele minime și atribuțiile ofițerului de legătură pentru securitatea infrastructurii critice naționale (denumit în continuare *ofițer de legătură*), desemnat la nivelul gestionarului infrastructurii critice naționale (denumit în continuare *gestionar*), precum și atribuțiile punctului de contact desemnat la nivelul autorității publice responsabile.

2. Ofițerul de legătură asigură coordonarea operațională, comunicarea și schimbul de informații relevante privind protecția, securitatea, continuitatea, răspunsul, recuperarea și reziliența infrastructurii critice naționale.

3. Ofițerul de legătură nu substituie responsabilitatea conducerii gestionarului și nici

atribuțiile structurilor interne competente, ci asigură coordonarea și legătura funcțională dintre acestea, autoritatea publică responsabilă și, după caz, Centrul Național de Coordonare a Protecției Infrastructurilor Critice (denumit în continuare *CNCPIC*).

4. În sensul prezentelor Norme, prin ofițer de legătură se înțelege persoana desemnată de către gestionar pentru exercitarea atribuțiilor de coordonare, comunicare și suport privind securitatea infrastructurii critice naționale.

5. La nivelul autorității publice responsabile se desemnează un punct de contact sau o persoană responsabilă de cooperarea cu gestionarii din sectorul sau subsectorul de competență și cu CNCPIC.

II. DESEMNAREA OFIȚERULUI DE LEGĂTURĂ

LA NIVELUL GESTIONARULUI

6. Ofițerul de legătură este desemnat de către gestionar.

7. În cazul în care același gestionar administrează sau operează mai multe infrastructuri critice naționale, acesta poate desemna:

7.1. un ofițer de legătură pentru fiecare infrastructură critică națională;

7.2. un ofițer de legătură pentru mai multe infrastructuri critice naționale, cu condiția asigurării capacității efective de exercitare a atribuțiilor;

7.3. un coordonator la nivel central și persoane responsabile la nivelul fiecărei infrastructuri critice naționale.

8. Pentru asigurarea continuității comunicării, gestionarul desemnează un înlocuitor al ofițerului de legătură.

9. Desemnarea ofițerului de legătură și a înlocuitorului acestuia se realizează prin act intern al gestionarului.

10. Actul intern de desemnare cuprinde cel puțin:

10.1. numele și prenumele persoanei desemnate;

10.2. funcția deținută în cadrul gestionarului;

10.3. infrastructura critică națională pentru care este desemnată;

10.4. atribuțiile principale;

10.5. datele de contact profesionale;

10.6. numele și prenumele persoanei desemnate ca înlocuitor;

10.7. data de la care desemnarea produce efecte;

10.8. obligațiile privind confidențialitatea și protecția informațiilor.

11. Gestionarul informează autoritatea publică responsabilă despre desemnarea, înlocuirea sau modificarea datelor de contact ale ofițerului de legătură și ale înlocuitorului acestuia, în termen de șapte zile lucrătoare de la data producerii modificării.

12. Autoritatea publică responsabilă poate transmite CNCPIC informații de sinteză privind ofițerii de legătură desemnați la nivelul gestionarilor din sectorul sau subsectorul de competență.

III. STATUTUL FUNCȚIONAL ȘI CONDIȚIILE DE EXERCITARE A ATRIBUȚIILOR

13. Ofițerul de legătură exercită atribuțiile stabilite prin prezentele Norme, prin actul intern de desemnare și prin documentele interne ale gestionarului.

14. Ofițerul de legătură trebuie să dispună de acces la informațiile, documentele, structurile și procesele relevante pentru exercitarea atribuțiilor sale, cu respectarea regimului juridic aplicabil informațiilor protejate.

15. Gestionarul asigură condițiile organizatorice necesare pentru exercitarea atribuțiilor ofițerului de legătură, inclusiv:

15.1. accesul la informațiile relevante;

15.2. includerea în procesele interne privind evaluarea riscurilor și Planul de securitate;

15.3. participarea la ședințe, exerciții, testări, instruiri și consultări relevante;

15.4. comunicarea cu autoritatea publică responsabilă;

15.5. comunicarea cu structurile interne responsabile de securitate, continuitate, răspuns și recuperare.

16. Ofițerul de legătură poate cumula atribuțiile prevăzute de prezentele Norme cu alte atribuții de serviciu, cu condiția ca acestea să nu afecteze exercitarea efectivă a responsabilităților privind securitatea infrastructurii critice naționale.

17. Atribuțiile ofițerului de legătură se exercită în limitele competențelor acordate de către gestionar și nu conferă drept de conducere operațională sau de decizie în afara mandatului stabilit prin actul intern de desemnare. Deciziile operative și măsurile obligatorii sunt dispuse de către conducerea gestionarului sau de către structurile interne competente, potrivit atribuțiilor acestora.

IV. ATRIBUȚIILE GENERALE ALE OFIȚERULUI DE LEGĂTURĂ

18. Ofițerul de legătură are următoarele atribuții generale:

18.1. asigură comunicarea operațională dintre gestionar și autoritatea publică responsabilă;

18.2. asigură, după caz, comunicarea cu CNCPIC, prin intermediul autorității publice responsabile sau potrivit mecanismelor stabilite;

18.3. coordonează, la nivel operațional, activitățile interne privind protecția, securitatea, continuitatea și reziliența infrastructurii critice naționale;

18.4. contribuie la colectarea, actualizarea și sistematizarea informațiilor relevante referitoare la infrastructura critică națională;

18.5. sprijină conducerea gestionarului în procesul de monitorizare a obligațiilor aferente infrastructurii critice naționale;

18.6. urmărește menținerea corelării între evaluarea riscurilor, Planul de securitate și măsurile implementate;

18.7. facilitează schimbul de informații dintre structurile interne responsabile;

18.8. contribuie la pregătirea documentelor, a informațiilor și a rapoartelor solicitate de către autoritatea publică responsabilă, în limitele competențelor legale;

18.9. informează conducerea gestionarului despre problemele relevante identificate în procesul de aplicare a măsurilor de securitate;

18.10. sprijină evidența și actualizarea datelor aferente infrastructurii critice naționale.

V. ATRIBUȚIILE PRIVIND EVALUAREA RISCURILOR ȘI PLANUL DE SECURITATE

19. În domeniul evaluării riscurilor, ofițerul de legătură:

19.1. participă la organizarea procesului de evaluare a riscurilor;

19.2. facilitează colectarea informațiilor necesare pentru evaluarea riscurilor;

19.3. contribuie la identificarea funcțiilor critice, a activelor critice, a proceselor esențiale, a dependențelor și interdependențelor;

19.4. sprijină identificarea riscurilor, a amenințărilor, a vulnerabilităților și a scenariilor relevante;

19.5. contribuie la actualizarea registrului riscurilor, a fișelor de risc și a documentelor aferente;

19.6. semnalează conducerii gestionarului modificările care pot afecta profilul de risc

al infrastructurii critice naționale.

20. În domeniul Planului de securitate, ofițerul de legătură:

20.1. coordonează, la nivel operațional, elaborarea, actualizarea și revizuirea Planului de securitate;

20.2. facilitează corelarea Planului de securitate cu evaluarea riscurilor;

20.3. urmărește includerea în Planul de securitate a măsurilor aferente riscurilor identificate;

20.4. contribuie la completarea, actualizarea și sistematizarea anexelor Planului de securitate;

20.5. sprijină consultarea structurilor interne relevante;

20.6. urmărește evidența versiunilor Planului de securitate;

20.7. contribuie la pregătirea documentelor necesare pentru avizare, reavizare sau echivalare, după caz;

20.8. monitorizează, la nivel operațional, stadiul implementării măsurilor prevăzute în Planul de securitate;

20.9. informează conducerea gestionarului despre întârzieri, neconformități sau dificultăți în implementarea măsurilor.

21. Ofițerul de legătură contribuie la documentarea actualizărilor și revizuirilor Planului de securitate, inclusiv prin pregătirea sau coordonarea notei de actualizare/revizuire, după caz.

VI. ATRIBUȚIILE PRIVIND COOPERAREA,

RAPORTAREA ȘI MONITORIZAREA

22. În domeniul cooperării, raportării și monitorizării, ofițerul de legătură:

22.1. menține comunicarea cu autoritatea publică responsabilă;

22.2. transmite, potrivit mandatului acordat, informațiile solicitate de către autoritatea publică responsabilă;

22.3. sprijină pregătirea răspunsurilor la solicitările autorității publice responsabile;

22.4. contribuie, în limitele competențelor gestionarului și potrivit procedurilor prevăzute de cadrul normativ aplicabil, la raportarea incidentelor, a perturbărilor, a vulnerabilităților sau a modificărilor relevante, fără instituirea unui mecanism paralel de notificare;

22.5. facilitează comunicarea cu furnizorii, prestatorii, partenerii și cu alte entități

relevante, în limitele mandatului acordat;

22.6. sprijină monitorizarea măsurilor de securitate, continuitate, răspuns și recuperare;

22.7. informează conducerea gestionarului despre solicitările, recomandările sau observațiile primite de la autoritatea publică responsabilă;

22.8. contribuie la pregătirea informațiilor de sinteză privind stadiul implementării Planului de securitate;

22.9. urmărește, după caz, remedierea deficiențelor constatate în urma controalelor, auditurilor, exercițiilor sau incidentelor.

23. Ofițerul de legătură transmite informații sensibile, confidențiale sau clasificate exclusiv în condițiile prevăzute de legislația aplicabilă și în limitele mandatului acordat de către conducerea gestionarului.

VII. ATRIBUȚIILE PRIVIND INSTRUIREA,

TESTAREA ȘI EXERCIȚIILE

24. În domeniul instruirii, testării și exercițiilor, ofițerul de legătură:

24.1. contribuie la identificarea necesităților de instruire privind securitatea infrastructurii critice naționale;

24.2. sprijină organizarea instruirilor interne relevante;

24.3. contribuie la planificarea testelor, a simulărilor și a exercițiilor aferente Planului de securitate;

24.4. participă, după caz, la exercițiile organizate la nivel intern, sectorial sau interinstituțional;

24.5. sprijină documentarea rezultatelor exercițiilor, testărilor și simulărilor, contribuie la identificarea lecțiilor învățate și a măsurilor corective;

24.6. urmărește includerea constatărilor relevante în procesul de revizuire sau de actualizare a Planului de securitate;

24.7. facilitează informarea personalului relevant cu privire la modificările operate în Planul de securitate.

VIII. CERINȚELE MINIME PENTRU DESEMNAREA

OFIȚERULUI DE LEGĂTURĂ

25. Persoana desemnată în calitate de ofițer de legătură trebuie să îndeplinească cel puțin următoarele cerințe:

25.1. să fie angajat al gestionarului sau să exercite atribuții în cadrul acestuia în temeiul unui raport juridic corespunzător;

25.2. să cunoască specificul infrastructurii critice naționale și al serviciului esențial furnizat;

25.3. să aibă acces la structurile, procesele și informațiile relevante pentru exercitarea atribuțiilor;

25.4. să dețină capacitatea de a coordona comunicarea internă și externă;

25.5. să cunoască procedurile interne relevante privind securitatea, continuitatea, răspunsul și recuperarea;

25.6. să respecte cerințele de confidențialitate și protecție a informațiilor;

25.7. să nu se afle într-o situație de incompatibilitate stabilită de cadrul normativ aplicabil, într-un conflict de interese sau într-o situație în care atribuțiile exercitate în cadrul gestionarului pot afecta imparțialitatea, independența ori exercitarea corespunzătoare a atribuțiilor de ofițer de legătură.

26. În funcție de specificul infrastructurii critice naționale, gestionarul poate stabili cerințe suplimentare privind:

26.1. experiența profesională;

26.2. domeniul de specializare;

26.3. cunoașterea managementului riscurilor;

26.4. cunoașterea continuității activității;

26.5. cunoașterea securității fizice, informaționale, cibernetice sau operaționale;

26.6. participarea la instruiri specializate;

26.7. accesul la informații atribuite la secret de stat, în cazul în care natura atribuțiilor exercitate o impune.

27. Gestionarul asigură participarea periodică a ofițerului de legătură la programe de instruire, perfecționare sau exerciții relevante, inclusiv în domeniul managementului riscurilor, al managementului situațiilor de criză, al cooperării interinstituționale și protecției infrastructurilor critice naționale, în vederea menținerii și dezvoltării competențelor necesare pentru exercitarea atribuțiilor.

28. Accesul ofițerului de legătură la informații atribuite la secret de stat sau la alte informații protejate se realizează numai în condițiile legislației aplicabile.

IX. OBLIGAȚIILE DE CONDUITĂ

ȘI DE CONFIDENȚIALITATE

29. Ofițerul de legătură exercită atribuțiile cu responsabilitate, imparțialitate și diligență, cu respectarea interesului de securitate al infrastructurii critice naționale.

30. În exercitarea atribuțiilor, ofițerul de legătură are următoarele obligații:

30.1. să păstreze confidențialitatea informațiilor la care are acces;

30.2. să utilizeze informațiile exclusiv în scopul exercitării atribuțiilor;

30.3. să respecte regimul juridic al informațiilor protejate;

30.4. să evite divulgarea neautorizată a informațiilor privind vulnerabilități, riscuri, scenarii, măsuri de securitate, capacități de răspuns sau puncte sensibile;

30.5. să informeze conducerea gestionarului despre orice situație care poate afecta exercitarea atribuțiilor sale;

30.6. să respecte procedurile interne privind accesul, păstrarea, transmiterea și arhivarea informațiilor.

31. Ofițerul de legătură nu poate utiliza informațiile obținute în exercitarea atribuțiilor în alte scopuri decât cele prevăzute de prezentele Norme, de actul intern de desemnare și de legislația aplicabilă.

X. ÎNCETAREA, MODIFICAREA ȘI ACTUALIZAREA DESEMNĂRII

32. Desemnarea ofițerului de legătură încetează în următoarele cazuri:

32.1. încetarea raporturilor de muncă sau de serviciu cu gestionarul;

32.2. schimbarea funcției sau a atribuțiilor, dacă aceasta afectează exercitarea rolului de ofițer de legătură;

32.3. retragerea desemnării prin act intern al gestionarului;

32.4. imposibilitatea exercitării atribuțiilor pentru o perioadă îndelungată;

32.5. constatarea unei incompatibilități sau a imposibilității de exercitare corespunzătoare a atribuțiilor;

32.6. alte cazuri stabilite prin actele interne ale gestionarului sau prin legislația aplicabilă.

33. În cazul încetării desemnării, gestionarul desemnează un nou ofițer de legătură și informează autoritatea publică responsabilă în termen de cinci zile lucrătoare.

34. În cazul absenței temporare a ofițerului de legătură, atribuțiile acestuia sunt exercitate de către înlocuitorul desemnat.

35. Gestionarul actualizează datele ofițerului de legătură și ale înlocuitorului ori de câte ori intervin modificări privind funcția, datele de contact, atribuțiile sau capacitatea de exercitare a rolului.

XI. PUNCTUL DE CONTACT LA NIVELUL AUTORITĂȚII PUBLICE RESPONSABILE

36. Autoritatea publică responsabilă desemnează, la nivelul structurii specializate sau al structurii competente, un punct de contact pentru securitatea infrastructurilor critice naționale din sectorul sau subsectorul de competență.

37. Punctul de contact desemnat la nivelul autorității publice responsabile asigură legătura funcțională cu gestionarii, cu ofițerii de legătură ai acestora, precum și cu CNCPIC.

38. Punctul de contact al autorității publice responsabile are următoarele atribuții:

38.1. ține evidența ofițerilor de legătură desemnați de către gestionari din sectorul sau subsectorul de competență;

38.2. asigură comunicarea cu ofițerii de legătură ai gestionarilor;

38.3. recepționează informații, notificări, solicitări și documente transmise de către gestionari, potrivit competențelor legale;

38.4. sprijină examinarea planurilor de securitate transmise spre avizare sau reavizare;

38.5. sprijină examinarea solicitărilor de echivalare a documentelor existente cu Planul de securitate;

38.6. contribuie la monitorizarea conformării gestionarilor cu cerințele legale și metodologice;

38.7. centralizează informațiile de sinteză privind stadiul elaborării, avizării, implementării, testării, revizuirii și actualizării Planurilor de securitate;

38.8. asigură transmiterea către CNCPIC a informațiilor de sinteză necesare, fără divulgarea informațiilor sensibile, confidențiale sau clasificate, dacă legislația aplicabilă nu prevede altfel;

38.9. participă la ședințe, consultări, instruiri, exerciții și alte activități relevante privind protecția infrastructurilor critice naționale;

38.10. sprijină aplicarea unitară a cerințelor metodologice în sectorul sau subsectorul de competență;

38.11. informează conducerea autorității publice responsabile despre dificultățile, riscurile, neconformitățile sau necesitățile de suport identificate în relația cu gestionarii.

39. Autoritatea publică responsabilă informează CNCPIC despre desemnarea, înlocuirea sau modificarea datelor de contact ale punctului de contact, în termen de cinci zile lucrătoare de la data producerii modificării.

XII. EVIDENȚA OFIȚERILOR DE LEGĂTURĂ

ȘI SCHIMBUL DE INFORMAȚII

40. Gestionarul ține evidența internă a ofițerilor de legătură, a înlocuitorilor acestora, precum și a datelor de contact profesionale aferente.

41. Autoritatea publică responsabilă ține evidența ofițerilor de legătură desemnați de către gestionari din sectorul sau subsectorul de competență.

42. Evidența prevăzută la pct. 40 cuprinde cel puțin:

42.1. denumirea gestionarului;

42.2. denumirea infrastructurii critice naționale;

42.3. sectorul și subsectorul;

42.4. numele, prenumele și funcția ofițerului de legătură;

42.5. datele de contact profesionale;

42.6. numele, prenumele și funcția înlocuitorului;

42.7. data desemnării;

42.8. data actualizării informațiilor;

42.9. mențiuni privind modificarea sau încetarea desemnării.

43. Schimbul de informații dintre gestionari, autoritățile publice responsabile și CNCPIC se realizează cu respectarea regimului juridic aplicabil informațiilor transmise.

44. Informațiile privind ofițerii de legătură și punctele de contact se utilizează exclusiv în scopul cooperării privind protecția infrastructurilor critice naționale.

45. Gestionarul și autoritatea publică responsabilă verifică periodic, cel puțin o dată pe an, actualitatea datelor privind funcția, datele de contact și statutul ofițerilor de legătură, al înlocuitorilor acestora și al punctelor de contact desemnate și asigură actualizarea fără întârziere a evidențelor aferente, în vederea menținerii funcționalității mecanismelor de notificare, comunicare și coordonare, inclusiv în situații de criză.

XIII. REGULILE COMUNE DE APLICARE

ȘI DE CORELARE METODOLOGICĂ

46. Activitățile ofițerului de legătură privind notificarea, schimbul de informații și

cooperarea operațională se realizează cu respectarea și fără a aduce atingere mecanismelor de coordonare, comunicare și raportare prevăzute de cadrul normativ în domeniul managementului crizelor și al continuității guvernării.

47. Atribuțiile detaliate ale ofițerului de legătură se stabilesc prin actul intern de desemnare și, după caz, prin documentele interne ale gestionarului, cu respectarea cerințelor minime prevăzute de prezentele Norme.

48. Desemnarea ofițerului de legătură nu exonerează gestionarul de responsabilitățile legale privind protecția, securitatea, continuitatea, răspunsul, recuperarea și reziliența infrastructurii critice naționale.

49. Autoritățile publice responsabile pot elabora instrucțiuni sectoriale sau recomandări privind aplicarea prezentelor Norme, cu informarea CNCPIC.

50. CNCPIC poate elabora modele orientative de fișe de atribuții, registre de evidență, formulare de notificare și alte instrumente metodologice necesare pentru aplicarea unitară a prezentelor Norme.

51. Prevederile prezentelor Norme se aplică fără a aduce atingere regimului juridic al informațiilor atribuite la secret de stat, datelor cu caracter personal, informațiilor confidențiale și altor categorii de informații protejate de lege.