# GUVERNUL REPUBLICII MOLDOVA

## HOTĂRÂRE nr. ____

**din 2026**

**Chișinău**

**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**

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 Centrul 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, ghidurilor, modelelor de documente sau procedurilor necesare aplicării 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 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

Anexa nr. 1
Aprobată
prin Hotărârea Guvernului nr. ___/2026

# Norme metodologice
## privind evaluarea riscurilor la adresa infrastructurilor critice naționale

**1. I. Dispoziții generale**Prezentele Norme metodologice privind evaluarea riscurilor la adresa infrastructurilor critice naționale reglementează modul de organizare, realizare, documentare și actualizare a evaluării 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 ori 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.

**4.** Prezentele Norme metodologice se aplică gestionarilor infrastructurilor critice naționale desemnate potrivit legii, indiferent de forma de proprietate, forma juridică de organizare sau sectorul de activitate.

**5.** Prezentele Norme metodologice 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 subsectorului, de serviciul esențial furnizat, de componentele critice, de amplasare, de mediul operațional, de dependențe, interdependențe și de nivelul de expunere la amenințări și pericole.

**7.** Evaluarea riscurilor constituie baza obligatorie pentru elaborarea, actualizarea și revizuirea Planului de securitate al gestionarului infrastructurii critice naționale.

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

**9.** Aplicarea prezentelor Norme metodologice 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.** Termenii și expresiile utilizate în prezentele Norme metodologice au semnificația prevăzută de Legea nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale, precum și de actele normative incidente în domeniul 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 gestionarul infrastructurii critice naționale, în cooperare cu autoritatea publică responsabilă din sectorul sau subsectorul de competență. Centrul Național de Coordonare a Protecției Infrastructurilor Critice acordă, după caz, suport metodologic autorităților publice responsabile și gestionarilor infrastructurilor critice naționale în aplicarea prezentelor Norme metodologice.

**12.** Autoritatea publică responsabilă poate stabili cerințe suplimentare privind evaluarea riscurilor, cu respectarea cadrului metodologic aprobat prin prezenta hotărâre și cu informarea Centrului Național de Coordonare a Protecției Infrastructurilor Critice.

**13.** Procesul de evaluare a riscurilor se inițiază:

13.1. după desemnarea infrastructurii drept infrastructură critică națională;

13.2. la elaborarea Planului de securitate al gestionarului infrastructurii critice naționale;

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 Centrului Național de Coordonare a Protecției Infrastructurilor Critice, în condițiile legii.

**14.** Gestionarul infrastructurii critice naționale 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 securitate fizică, securitate cibernetică, continuitatea activității, protecție civilă, situații de urgență, mentenanță, exploatare tehnică, logistică, resurse umane, juridic, comunicare și management operațional.

**16.** Pentru evaluarea riscurilor care necesită expertiză specializată, gestionarul infrastructurii critice naționale sau autoritatea publică responsabilă poate

solicita suportul unor experți ori 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, funcționare degradată și 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, activelor critice și proceselor esențiale;

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

20.4. identificarea vulnerabilităților;

20.5. identificarea dependențelor și interdependențelor;

20.6. elaborarea scenariilor de risc;

20.7. estimarea impactului;

20.8. estimarea probabilității;

20.9. determinarea scorului și 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, activelor critice și proceselor esențiale, gestionarul stabilește elementele fără de care infrastructura critică națională nu poate furniza sau relua serviciul esențial.

**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 ori serviciul esențial furnizat.

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

25.1. istoricului incidentelor și perturbărilor;

25.2. analizelor interne și sectoriale;

25.3. informațiilor furnizate de 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. Evaluarea Națională a Riscurilor, evaluărilor strategice și 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, competențe sau 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 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, activelor critice și serviciului esențial;

29.7. efectele de propagare și 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, energiei, comunicațiilor, suportului tehnic ori 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 infrastructuri critice naționale, precum și asupra rezilienței naționale.

**33.** În procesul de evaluare, 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 adecvată 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 afectări semnificative asupra 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 necesitatea unor măsuri operative și manageriale suplimentare;

36.4. nivelul 4 – impact înalt: perturbări majore, cu afectare gravă a funcțiilor critice, posibilitatea producerii de pierderi semnificative de vieți omenești, pagube economice considerabile, afectarea simultană a mai multor valori protejate sau propagare semnificativă 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, frecvența sau plauzibilitatea materializării acestuia și 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 materializării apar rar;

40.2. nivelul 2 – probabilitate scăzută: scenariul este posibil, dar puțin probabil; există puține indicii sau precedente limitate; condițiile necesare 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 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 ori 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 nivelului de risc

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

**Scorul de risc = Impact × Probabilitate**

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

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

1–4 – risc scăzut;
5–10 – risc moderat;
11–15 – risc înalt;
16–25 – risc critic.

**46.** Matricea de risc are format 5x5 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, efectele asupra serviciului esențial, vulnerabilitățile asociate și 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 riscului rezidual, cu justificare;

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 al gestionarului infrastructurii critice naționale 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 ori pentru fiecare 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 infrastructurii critice naționale 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 într-un raport de evaluare a riscurilor la adresa infrastructurii critice naționale.

**60.** Raportul de evaluare a riscurilor se aprobă de conducătorul gestionarului infrastructurii critice naționale sau de 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, 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 Centrului Național de Coordonare a Protecției Infrastructurilor Critice, în condițiile legii.

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

**65.** Nota de actualizare indică 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 numai persoanelor care au atribuții directe în procesul de evaluare, avizare, monitorizare, control sau implementare a măsurilor de securitate.

**69.** Gestionarul infrastructurii critice naționale 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 vor fi adaptate regimului de protecție a informațiilor clasificate, utilizând exclusiv canale securizate și personal autorizat potrivit legislației.

## XIII. Reguli comune de aplicare și 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, protecției, continuității și rezilienței infrastructurilor critice naționale.

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

**74.** Centrul Național de Coordonare a Protecției Infrastructurilor Critice elaborează și pune la dispoziția autorităților publice responsabile și a gestionarilor infrastructurilor critice naționale modele-tip și instrumente metodologice standardizate pentru aplicarea prezentelor Norme metodologice, 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 aplicării unitare a procesului de evaluare a riscurilor.

**75.** Rezultatele evaluării riscurilor fundamentează Planul de securitate al gestionarului infrastructurii critice naționale, măsurile de tratare a riscurilor și procesul de revizuire a acestuia.

Anexa nr. 2
Aprobată
prin Hotărârea Guvernului nr. ___/2026

# Norme metodologice
# privind elaborarea, avizarea și aprobarea planurilor de securitate ale gestionarilor infrastructurilor critice naționale

## I. Dispoziții generale

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

**2.** Planul de securitate al gestionarului infrastructurii critice naționale reprezintă documentul de planificare strategică, cu caracter operativ prin procedurile asociate, elaborat pentru fiecare infrastructură critică națională desemnată, prin care sunt stabilite obiectivele, măsurile, responsabilitățile, resursele și procedurile necesare pentru protecția, securitatea, continuitatea și reziliența acesteia.

**3.** Planul de securitate are drept 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 pentru fiecare infrastructură critică națională desemnată, de către gestionarul acesteia, 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:

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

5.2. elabora 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, funcțiilor critice, activelor critice, măsurilor de securitate, responsabilităților, resurselor, termenelor și 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;

7.2. cadrului normativ aplicabil sectorului sau subsectorului;

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

7.4. instrucțiunilor sectoriale emise de 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, exercițiilor, testărilor, auditurilor sau 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. Responsabilități 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 infrastructurii critice naționale.

**11.** Conducătorul gestionarului infrastructurii critice naționale asigură:

11.1. inițierea procesului de elaborare a Planului de securitate;

11.2. desemnarea persoanelor sau 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, testării, revizuirii și 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. continuitatea activității;

13.5. managementul riscurilor;

13.6. protecție civilă și situații de urgență;

13.7. resurse umane;

13.8. juridic;
13.9. achiziții, logistică, tehnic și mentenanță;
13.10. comunicare publică;
13.11. protecția 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 acordă suport metodologic autorităților publice responsabile și, după caz, gestionarilor infrastructurilor critice naționale, în vederea aplicării unitare a cerințelor privind planurile de securitate.

## III. Cerințe 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 include cel puțin:
18.1. date generale privind gestionarul și infrastructura critică națională;
18.2. descrierea serviciului esențial furnizat;
18.3. descrierea funcțiilor critice, activelor critice și 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 exerciții;
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 pentru implementare;

19.5. termenul de implementare sau 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, diminuare a impactului, asigurare a continuității și 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 infrastructurii critice naționale, 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, continuitate și 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 9 luni de la data desemnării infrastructurii drept infrastructură critică națională, cu posibilitatea extinderii acestui termen cu cel mult 6 luni, cu acordul Centrului Național de Coordonare a Protecției Infrastructurilor Critice, în condițiile art. 14 alin. (1) din Legea nr. 223/2025.

**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, termenelor și 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 probabilitate estimat;
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 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, atunci când acest lucru este necesar pentru completarea sau validarea unor măsuri privind:

38.1. interdependențele;

38.2. continuitatea serviciilor;

38.3. furnizarea de resurse critice;

38.4. reacția și coordonarea interinstituțională;

38.5. suportul tehnic sau contractual necesar funcționării infrastructurii critice naționale.

**39.** Consultarea externă nu poate conduce la divulgarea informațiilor sensibile, confidențiale sau clasificate decât în condițiile prevăzute de legislația aplicabilă.

## VI. Transmiterea Planului de securitate spre avizare

**40.** După aprobarea preliminară internă, gestionarul infrastructurii critice naționale 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 evaluării 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 asociate 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 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 Centrul Național de Coordonare a Protecției Infrastructurilor Critice. 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, termenelor și resurselor;
44.7. existența procedurilor de răspuns, continuitate și recuperare;
44.8. corelarea cu cerințele sectoriale aplicabile;
44.9. existența mecanismelor de instruire, testare, raportare și 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 documentelor, 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 evaluării 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 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 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, existența informațiilor clasificate ori 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 infrastructurii critice naționale sau de persoana competentă desemnată potrivit actelor interne aplicabile, 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 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 responsabilităților prevăzute;

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

64.4. asigurarea resurselor necesare, în limita 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 aplicare 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 5 zile lucrătoare de la data aprobării.

**68.** Autoritatea publică responsabilă poate transmite Centrului Național de Coordonare a Protecției Infrastructurilor Critice 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 infrastructurii critice naționale 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, testelor și exercițiilor;

70.6. monitorizarea realizării măsurilor;

70.7. raportarea internă asupra stadiului 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. soluții 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 asupra stadiului implementării, neconformităților identificate și necesității 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 infrastructurii critice naționale 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 2 ani, precum și ori de câte ori intervin modificări semnificative ale infrastructurii critice

naționale, ale serviciului esențial, ale riscurilor, procedurilor, responsabilităților ori resurselor prevăzute în plan sau în urma producerii unui incident relevant.

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

80.6. teste ale procedurilor de continuitate și 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 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;

82.9. concluziile și lecțiile identificate.

**83.** Constatările, concluziile și lecțiile identificate în urma testării Planului de securitate, gestionării situațiilor de criză, exercițiilor naționale și 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 se înscrie în evidența internă a documentelor aferente infrastructurii critice naționale.

**88.** Structurile interne relevante sunt informate asupra versiunii aplicabile a Planului de securitate, în limita 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 numai persoanelor care au atribuții directe și 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 infrastructurii critice naționale 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. Reguli 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 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, producerii unui incident, desfășurării unui exercițiu,

modificării infrastructurii sau schimbării mediului de risc, gestionarul inițiază revizuirea acestuia potrivit anexei nr. 5.

**98.** Autoritățile publice responsabile pot elabora, cu informarea Centrului Național de Coordonare a Protecției Infrastructurilor Critice, instrucțiuni sectoriale și modele de documente pentru aplicarea prezentelor Norme metodologice 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 numai persoanelor autorizate, prin mijloace corespunzătoare regimului juridic aplicabil informațiilor respective.

**100.** Centrul Național de Coordonare a Protecției Infrastructurilor Critice elaborează și pune la dispoziția autorităților publice responsabile și a gestionarilor infrastructurilor critice naționale modele-tip și instrumente metodologice standardizate pentru aplicarea prezentelor Norme metodologice, 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 aplicării unitare a procedurii de elaborare, avizare, aprobare, implementare, testare, revizuire și actualizare a Planului de securitate.

Anexa nr. 3
Aprobată
prin Hotărârea Guvernului nr. ___/2026

# Structura-cadru
# a Planului de securitate al gestionarului infrastructurii critice naționale

## Secțiunea 1.
## Date generale

**1.** Capitolul privind datele generale va cuprinde cel puțin:

1.1. denumirea completă a gestionarului;

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, 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 2.
## Scopul, obiectivele și domeniul de aplicare al Planului de securitate

**2.** Capitolul privind scopul, obiectivele și domeniul de aplicare va include 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 vor viza cel puțin:

3.1. prevenirea și reducerea riscurilor prioritare;

3.2. protecția funcțiilor critice, activelor critice și 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 alte entități relevante;

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

## Secțiunea 3.
## Descrierea infrastructurii critice naționale și a serviciului esențial

**4.** Capitolul privind descrierea infrastructurii critice naționale și a serviciului esențial va include 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 4.
## Funcții critice, active critice, procese esențiale și alte elemente importante

**5.** Capitolul privind funcțiile critice, activele critice, procesele esențiale și alte elemente importante pentru furnizarea serviciului esențial va include 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 funcționării;

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

5.8. impactul indisponibilității acestora asupra serviciului esențial.

## Secțiunea 5.
## Dependențe și interdependențe

**6.** Capitolul privind dependențele și interdependențele va include 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 6.
## Rezultatele evaluării riscurilor

**7.** Capitolul privind rezultatele evaluării riscurilor va include 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 7.
## Măsuri existente de securitate

**9.** Capitolul privind măsurile existente de securitate va 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 8.
## Măsuri suplimentare și plan de implementare

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

**12.** Pentru fiecare risc prioritar, Planul de securitate va prevedea cel puțin:
12.1. măsurile suplimentare necesare;

12.2. obiectivul fiecărei măsuri;

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

12.4. nivelul de prioritate;

12.5. responsabilul pentru 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, urgența intervenției, capacitatea reală de implementare a gestionarului și necesitatea asigurării continuității serviciului esențial.

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

| Nr. | Risc vizat | Măsura propusă | Tipul măsurii | Responsabil | Termen | Resurse necesare | Indicator de realizare | Stadiu |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |

## Secțiunea 9.
## Măsuri de continuitate a activității

**15.** Capitolul privind continuitatea activității va include 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 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 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, relocare, redundanță sau funcționare alternativă.

## Secțiunea 10.
## Măsuri de răspuns, notificare și recuperare

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

16.1. măsurile de reacție în cazul producerii unui incident;

16.2. procedurile de alertare, informare și 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, 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, continuitate și recuperare prevăzute în Planul de securitate în mecanismele de gestionare a unei crize la nivel național.

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

## Secțiunea 11.
## Organizarea, responsabilitățile și mecanismele de coordonare

**18.** Capitolul privind organizarea, responsabilitățile și mecanismele de coordonare va include 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, autoritățile competente și alte entități relevante;

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

18.8. procedurile de escaladare decizională în situații de perturbare sau 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 12.
## Comunicare, raportare și schimb de informații

**19.** Capitolul privind comunicarea, raportarea și schimbul de informații va include cel puțin:

19.1. mecanismele de comunicare internă;

19.2. mecanismele de comunicare cu autoritatea publică responsabilă;

19.3. mecanismele de comunicare cu Centrul Național de Coordonare a Protecției Infrastructurilor Critice, după caz;

19.4. mecanismele de comunicare cu alte autorități competente;

19.5. comunicarea cu furnizorii, prestatorii, partenerii și 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, perturbărilor și 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 infrastructurii critice naționale ori, după caz, din cadrul autorității publice responsabile sau al Centrului Național de Coordonare a Protecției Infrastructurilor Critice, 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, dezinformării sau afectării suplimentare a securității infrastructurii critice naționale.

## Secțiunea 13.
## Instruire, testare și exerciții

**21.** Capitolul privind instruirea, testarea și exercițiile va include 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 exerciții planificate;

21.4. frecvența testelor și 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, testelor și exercițiilor desfășurate;

21.9. modalitatea de testare a cooperării și coordonării dintre gestionarul infrastructurii critice naționale, alți gestionari relevanți și autoritățile competente din cadrul Sistemului național de management al crizelor.

## Secțiunea 14.
## Revizuirea și actualizarea Planului de securitate

**22.** Capitolul privind revizuirea și actualizarea Planului de securitate va include 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 asupra modificărilor operate;
22.8. mecanismul de retragere sau arhivare a versiunilor depășite.

### Secțiunea 15.
### Regimul documentului, păstrarea și circulația informațiilor

**23.** Capitolul privind regimul documentului va 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, arhivare și 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 structurilor care au acces la Planul de securitate;
23.8. responsabilul pentru păstrarea versiunii oficiale;
23.9. măsurile de retragere a versiunilor neactuale.

### Secțiunea 16.
### 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. scheme, hărți, planuri de amplasament și diagrame funcționale;
24.5. liste de contacte operaționale;
24.6. registre ale activelor critice și ale resurselor esențiale;
24.7. proceduri operaționale relevante;
24.8. planuri conexe sau extrase din acestea;
24.9. tabelul măsurilor suplimentare și al planului de implementare;
24.10. evidența instruirilor, testelor și exercițiilor;
24.11. note de actualizare și evidența modificărilor;
24.12. lista persoanelor sau structurilor cu acces la Planul de securitate;
24.13. evidența distribuirii Planului de securitate;
24.14. alte documente justificative necesare.

## III. Cerințe minime de formă și conținut

**25.** Planul de securitate trebuie să fie redactat clar, coerent și structurat astfel încât să permită utilizarea sa efectivă în condiții normale 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 măsuri concrete, responsabili, termene, resurse, indicatori și mecanisme de aplicare.

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

**29.** În cazul în care anumite informații nu sunt aplicabile infrastructurii critice naționale evaluate, gestionarul indică 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
Aprobată
prin Hotărârea Guvernului nr. ___/2026

# Norme metodologice
# privind echivalarea documentelor existente cu Planul de securitate al gestionarului infrastructurii critice naționale

## I. Dispoziții generale

**1.** Norme de echivalarea reprezintă reguli și proceduri prin care se constată că un document existent sau un set de documente existente, elaborate de gestionar, acoperă integral ori în mod suficient cerințele minime aplicabile Planului de securitate al gestionarului infrastructurii critice naționale.

**2.** Norme de echivalare 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.** Norme de echivalarea nu are caracter automat și nu rezultă din simpla existență a unui document intern anterior, indiferent de denumirea acestuia.

**4.** Echivalarea se apreciază 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 infrastructurii critice naționale 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 al gestionarului infrastructurii critice naționale se utilizează pentru verificarea corespondenței dintre documentele existente și Structura-cadru a Planului de securitate, prevăzută în anexa nr. 3.

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

## II. Documentele care pot fi propuse spre echivalare

**8.** Pot fi propuse spre echivalare, după caz:

8.1. planuri de securitate internă;

8.2. planuri de continuitate a activității;

8.3. planuri de răspuns la incidente;

8.4. planuri de protecție fizică;

8.5. planuri de securitate informațională sau cibernetică;

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

8.7. planuri de protecție antiteroristă, după caz;

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

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

8.10. documente 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.

## 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 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, 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 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 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, notificare și 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, actualizare și 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 al gestionarului infrastructurii critice naționale, 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 infrastructurii critice naționale.

**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 va indica cel puțin:

20.1. infrastructura critică națională pentru care se solicită echivalarea;

20.2. documentul ori 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 pentru 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 ori a documentelor propuse spre echivalare;

21.2. nota de sinteză privind echivalarea;

21.3. grila de echivalare completată;

21.4. dovada aprobării documentului ori a documentelor respective;

21.5. informații 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. informații 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 ori 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. | Element minim obligatoriu al Planului de securitate | Existența în documentul propus spre | Denumirea documentului/ | Aprecierea suficienței conținutului | Observații/ completări necesare |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | echivalare: Da/Nu/Parțial | documentelor și capitolul/punctul relevant | | |
| | Date generale privind gestionarul și infrastructura critică națională | | | | |
| | Scopul, obiectivele și domeniul de aplicare | | | | |
| | Descrierea infrastructurii critice naționale și a serviciului esențial | | | | |
| | Funcții critice, active critice și procese esențiale | | | | |
| | Dependențe și interdependențe | | | | |
| | Rezultatele evaluării riscurilor | | | | |
| | Scenarii de risc și vulnerabilități | | | | |
| | Măsuri existente de securitate | | | | |
| | Măsuri suplimentare și plan de implementare | | | | |
| | Măsuri de continuitate a activității | | | | |
| | Măsuri de răspuns, notificare și recuperare | | | | |
| | Organizare, responsabilități și mecanisme de coordonare | | | | |
| | Comunicare, raportare și schimb de informații | | | | |
| | Instruire, testare și exerciții | | | | |
| | Revizuire, actualizare și evidența versiunilor | | | | |
| | 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 „Observații/completări necesare” se consemnează elementele lipsă, necorelările, necesitatea actualizării ori orice altă condiție necesară pentru admiterea echivalării.

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

## VIII. Analiza solicitării de echivalare

**30.** Echivalarea se analizează de 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 propuse 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, termenelor și mecanismelor de implementare;

31.9. existența regulilor de revizuire și 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. documente sau anexe lipsă;

34.3. actualizarea unor informații;

34.4. completarea grilei de echivalare;

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

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

**36.** Gestionarul transmite completările solicitate în termen de 5 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 atunci când 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 atunci când 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 atunci când:

41.1. anumite elemente sunt parțial suficiente;

41.2. lipsesc elemente neesențiale ori completabile 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 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 ori 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 atunci când:

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

43.2. lipsesc elemente 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, responsabilităților și 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 transmite spre avizare Planul de securitate în termenul prevăzut de Normele metodologice din anexa nr. 2 la prezenta hotărâre. 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 respingere a echivalării

**45.** Rezultatul examinării se consemnează într-un act de recunoaștere sau respingere a echivalării, emis de autoritatea publică responsabilă.

**46.** Actul de recunoaștere sau respingere a echivalării va 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 completare, actualizare sau corelare;

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 al gestionarului infrastructurii critice naționale.

**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 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 ori 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 exclude obligația gestionarului de a completa ori actualiza documentele respective atunci când intervin schimbări semnificative.

## XII. Revizuirea documentelor recunoscute ca echivalente

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

**54.** Gestionarul infrastructurii critice naționale notifică autoritatea publică responsabilă despre orice modificare a documentului sau a setului de documente recunoscute ca echivalente, în termen de cel mult 10 zile lucrătoare de la data aprobării sau intrării în vigoare a modificării. Modificările substanțiale se reflectă în documentația de echivalare actualizată și se transmit autorității publice responsabile odată cu notificarea.

**55.** Dacă, 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 atunci când:

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, controlului, auditului sau 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 recunoscute ca echivalente.

## XIII. Nota de sinteză privind echivalarea

**58.** Solicitarea de echivalare se însoțește de o notă de sinteză întocmită de gestionar.

**59.** Nota de sinteză privind echivalarea va cuprinde cel puțin:

59.1. datele de identificare ale gestionarului;

59.2. denumirea infrastructurii critice naționale;

59.3. lista documentului sau a 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 respingere a echivalării 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 numai 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, potrivit regimului 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. Reguli comune de aplicare și corelare metodologică

**65.** Procedura de echivalare se aplică în mod proporțional, fără a diminua nivelul de protecție, securitate și continuitate necesar infrastructurii critice naționale.

**66.** În toate cazurile, prevalează cerința ca documentul ori setul de documente recunoscut ca echivalent să permită:

65.1. identificarea clară a riscurilor relevante;

65.2. organizarea măsurilor de securitate;

65.3. asigurarea continuității serviciului esențial;

65.4. coordonarea răspunsului și recuperării;

65.5. verificarea, actualizarea și revizuirea periodică.

**67.** Echivalarea documentelor existente cu Planul de securitate nu exclude obligația gestionarului 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 metodologice, cu informarea Centrului Național de Coordonare a Protecției Infrastructurilor Critice.

**69.** Centrul Național de Coordonare a Protecției Infrastructurilor Critice emite recomandări metodologice privind aplicarea unitară a procedurii de echivalare.

**70.** În toate cazurile, 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 infrastructurii critice naționale 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 tabel de corespondență, care indică documentele, secțiunile, procedurile ori anexele prin care fiecare cerință este acoperită integral sau parțial.

Anexa nr. 5
Aprobată
prin Hotărârea Guvernului nr. ___/2026

# Norme metodologice privind revizuirea și actualizarea Planului de securitate al gestionarului infrastructurii critice naționale

## I. Dispoziții generale

**1.** Prezentele Norme metodologice stabilesc modul de revizuire și actualizare a Planului de securitate al gestionarului infrastructurii critice naționale.

**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 controalelor.

**3.** În sensul prezentei anexe:

3.1. actualizarea Planului de securitate reprezintă modificarea punctuală a unor date, capitole, anexe, proceduri, responsabilități sau măsuri din Planul de securitate, fără schimbarea arhitecturii generale a acestuia;

3.2. revizuirea Planului de securitate reprezintă procesul 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. revizuirea periodică reprezintă revizuirea realizată la intervale regulate, potrivit termenului stabilit de prezenta anexă sau de reglementările sectoriale aplicabile;

3.4. revizuirea extraordinară reprezintă revizuirea 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, în cooperare cu structurile interne relevante și, după caz, cu autoritatea publică responsabilă din sectorul sau subsectorul de competență.

**5.** Ofițerul de legătură pentru securitatea infrastructurii critice naționale coordonează, la nivel operațional, procesul de revizuire și actualizare a Planului de securitate, 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 2 ani, dacă prin lege, prin actul de desemnare a infrastructurii critice naționale sau prin reglementări sectoriale nu este stabilit 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 actualizare a acestuia.

**9.** Revizuirea periodică urmărește verificarea:

9.1. actualității datelor privind gestionarul și infrastructura critică națională;

9.2. actualității descrierii serviciului esențial furnizat;

9.3. actualității evaluării riscurilor și a nivelurilor de risc stabilite;

9.4. menținerii relevanței riscurilor identificate;

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

9.6. actualității dependențelor și 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, responsabilităților și procedurilor asociate;

9.12. rezultatelor instruirilor, testelor și exercițiilor desfășurate;

9.13. necesității de completare, modificare sau eliminare a unor capitole, secțiuni ori anexe.

**10.** Revizuirea periodică se documentează printr-o notă de actualizare/ revizuire, întocmită de gestionar.

**11.** În cazul în care revizuirea periodică nu identifică necesitatea unor modificări, 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 ori 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, activelor critice sau proceselor esențiale;

13.8. modificarea dependențelor sau interdependențelor relevante;

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

13.10. rezultate relevante ale auditurilor, controalelor, testărilor, exercițiilor sau simulărilor;

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

13.12. modificări ale cadrului normativ aplicabil sau ale 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, în condițiile legii;

13.17. declararea unei stări de criză sau modificarea nivelului de alertă la nivel național, atunci când aceasta afectează ori poate afecta funcționarea infrastructurii critice naționale sau continuitatea serviciului esențial furnizat;

13.18. constatarea 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 actualizare

**16.** Procesul de revizuire sau actualizare se inițiază prin decizia conducerii gestionarului infrastructurii critice naționale 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 revizuirii sau actualizării stabilește, după caz:

18.1. temeiul revizuirii sau actualizării;

18.2. obiectul revizuirii sau 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 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 continuitate a activității;
20.8. măsurile de răspuns, notificare și recuperare;
20.9. responsabilitățile interne și mecanismele de coordonare;
20.10. mecanismele de comunicare, raportare și schimb de informații;
20.11. programul de instruire, testare și exerciții;
20.12. anexele, registrele, listele de contacte și procedurile asociate;
20.13. regimul documentului și protecția 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 structurile responsabile;
21.10. necesită modificări, completări sau actualizări.

**22.** În cazul în care revizuirea indică modificarea profilului de risc, gestionarul actualizează evaluarea riscurilor potrivit Normelor metodologice prevăzute în anexa nr. 1.

**23.** În cazul în care revizuirea indică necesitatea modificării conținutului Planului de securitate, gestionarul actualizează capitolele, secțiunile, anexele sau procedurile afectate.

## VI. Clasificarea modificărilor

**24.** Modificările operate asupra Planului 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 unor structuri interne, fără schimbarea atribuțiilor;

26.3. corectarea erorilor materiale;

26.4. actualizarea listelor operaționale, fără afectarea mecanismelor principale;

26.5. ajustări redacționale sau de formă.

**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 prezenta anexă.

**32.** Rezultatele procesului de actualizare sau revizuire se consemnează într-o notă de actualizare/revizuire, întocmită de gestionar.

**33.** Nota de actualizare/revizuire include cel puțin:

33.1. temeiul actualizării sau 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, situațiilor de criză și 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 conducătorul gestionarului infrastructurii critice naționale sau de persoana competentă desemnată potrivit actelor interne aplicabile.

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

## VIII. Reavizarea Planului de securitate

**37.** Planul de securitate actualizat se transmite spre reavizare autorității publice responsabile atunci când 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 protecția informațiilor, atunci când 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.** Nu necesită reavizare modificările minore care nu afectează elementele prevăzute la pct. 37, cu condiția consemnării acestora în evidența modificărilor Planului de securitate.

**39.** Autoritatea publică responsabilă examinează forma actualizată a Planului de securitate potrivit procedurii de avizare prevăzute în anexa nr. 2.

**40.** În cazul în care autoritatea publică responsabilă constată că modificările nu impun reavizarea, 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 Planului de securitate 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.** Dacă 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 infrastructurii critice naționale notifică autoritatea publică responsabilă despre încetarea, suspendarea sau modificarea substanțială a documentului ori a setului de documente recunoscute ca echivalente, în termen de cel mult 10 zile lucrătoare de la data intervenirii acesteia.

## X. Evidența și trasabilitatea revizuirii

**45.** Gestionarul infrastructurii critice naționale asigură evidența și trasabilitatea tuturor revizuirilor și actualizărilor Planului de securitate.

**46.** Evidența revizuirilor și actualizărilor include cel puțin:

46.1. data inițierii revizuirii sau actualizării;

46.2. temeiul revizuirii sau 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 asupra versiunii aplicabile.

**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 actualizare

**49.** Documentele întocmite în procesul de revizuire și 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 actualizare se acordă numai 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. Reguli comune de aplicare și corelare metodologică

**53.** Revizuirea și actualizarea Planului de securitate nu exonerează gestionarul de obligația de a aplica măsurile de securitate, continuitate, răspuns și recuperare aflate 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, continuitate și 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 metodologice, cu informarea Centrului Național de Coordonare a Protecției Infrastructurilor Critice.

**57.** Centrul Național de Coordonare a Protecției Infrastructurilor Critice pune la dispoziția autorităților publice responsabile și gestionarilor infrastructurilor critice naționale modele de note de actualizare/revizuire, registre de evidență a modificărilor și alte instrumente metodologice de suport.

**58.** Prevederile prezentei anexe se aplică corespunzător și documentelor recunoscute ca echivalente cu Planul de securitate al gestionarului infrastructurii critice naționale.

Anexa nr. 6
Aprobată
prin Hotărârea Guvernului nr. ___/2026

# Norme metodologice
# privind desemnarea, statutul funcțional și atribuțiile ofițerului de legătură pentru securitatea infrastructurii critice naționale

## I. Dispoziții generale

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

**2.** Ofițerul de legătură pentru securitatea infrastructurii critice naționale 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 infrastructurii critice naționale și nici atribuțiile structurilor interne competente, ci asigură legătura funcțională dintre acestea, autoritatea publică responsabilă și, după caz, Centrul Național de Coordonare a Protecției Infrastructurilor Critice.

**4.** În sensul prezentei anexe, prin ofițer de legătură se înțelege persoana desemnată de gestionarul infrastructurii critice naționale 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 pentru cooperarea cu gestionarii infrastructurilor critice naționale din sectorul sau subsectorul de competență și cu Centrul Național de Coordonare a Protecției Infrastructurilor Critice.

## II. Desemnarea ofițerului de legătură la nivelul gestionarului infrastructurii critice naționale

**6.** Gestionarul infrastructurii critice naționale desemnează un ofițer de legătură pentru securitatea infrastructurii critice naționale.

**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 infrastructurii critice naționale.

**10.** Actul intern de desemnare include 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. persoana desemnată 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 7 zile lucrătoare de la data producerii modificării.

**12.** Autoritatea publică responsabilă poate transmite Centrului Național de Coordonare a Protecției Infrastructurilor Critice 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 prezenta anexă, prin actul intern de desemnare și prin documentele interne ale gestionarului infrastructurii critice naționale.

**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 prezenta anexă 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 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 conducerea gestionarului sau de 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 Centrul Național de Coordonare a Protecției Infrastructurilor Critice, prin intermediul autorității publice responsabile sau potrivit mecanismelor stabilite;

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

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

18.5. sprijină conducerea gestionarului în monitorizarea obligațiilor aferente infrastructurii critice naționale;

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

18.7. facilitează schimbul de informații între structurile interne responsabile;

18.8. contribuie la pregătirea documentelor, informațiilor și rapoartelor solicitate de 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. Atribuții 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 evaluării riscurilor;

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

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

19.5. contribuie la actualizarea registrului riscurilor, fișelor de risc și 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. Atribuții 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 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, perturbărilor, vulnerabilităților sau modificărilor relevante, fără instituirea unui mecanism paralel de notificare;

22.5. facilitează comunicarea cu furnizorii, prestatorii, partenerii și 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 nu transmite informații sensibile, confidențiale sau clasificate decât în condițiile legislației aplicabile și potrivit mandatului acordat de conducerea gestionarului.

## VII. Atribuții 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, simulărilor și exercițiilor aferente Planului de securitate;

24.4. participă, după caz, la exerciții 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 actualizare a Planului de securitate;

24.7. facilitează informarea personalului relevant asupra modificărilor Planului de securitate.

## VIII. Cerințe minime pentru desemnarea ofițerului de legătură

**25.** Persoana desemnată ca ofițer de legătură trebuie să îndeplinească cel puțin următoarele cerințe:

25.1. să fie angajat al gestionarului infrastructurii critice naționale 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 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 infrastructurii critice naționale 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, dacă natura atribuțiilor o impune.

**27.** Gestionarul infrastructurii critice naționale asigură participarea periodică a ofițerului de legătură la programe de instruire, perfecționare sau exerciții relevante,

inclusiv în domeniul managementului riscurilor, managementului situațiilor de criză, cooperării interinstituționale și protecției infrastructurilor critice naționale, în vederea menținerii și dezvoltării competențelor necesare exercitării 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. Obligații de conduită și confidențialitate

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

**30.** Ofițerul de legătură are obligația:

30.1. să păstreze confidențialitatea informațiilor la care are acces;

30.2. să utilizeze informațiile numai 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 prezenta anexă, 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 raportului 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 5 zile lucrătoare.

**34.** În cazul absenței temporare a ofițerului de legătură, atribuțiile acestuia sunt exercitate de 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 infrastructurilor critice naționale, cu ofițerii de legătură ai acestora și cu Centrul Național de Coordonare a Protecției Infrastructurilor Critice.

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

38.1. menține evidența ofițerilor de legătură desemnați de gestionarii infrastructurilor critice naționale 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 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 informații de sinteză privind stadiul elaborării, avizării, implementării, testării, revizuirii și actualizării planurilor de securitate;

38.8. asigură transmiterea către Centrul Național de Coordonare a Protecției Infrastructurilor Critice 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 dificultăți, riscuri, neconformități sau necesități de suport identificate în relația cu gestionarii.

**39.** Autoritatea publică responsabilă informează Centrul Național de Coordonare a Protecției Infrastructurilor Critice despre desemnarea, înlocuirea sau modificarea datelor de contact ale punctului de contact, în termen de 5 zile lucrătoare de la data producerii modificării.

## XII. Evidența ofițerilor de legătură și schimbul de informații

**40.** Gestionarul infrastructurii critice naționale ține evidența internă a ofițerului de legătură, a înlocuitorului acestuia și a datelor de contact aferente.

**41.** Autoritatea publică responsabilă ține evidența ofițerilor de legătură desemnați de gestionarii infrastructurilor critice naționale din sectorul sau subsectorul de competență.

**42.** Evidența prevăzută la pct. 40 include 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 Centrul Național de Coordonare a Protecției Infrastructurilor Critice 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 infrastructurii critice naționale și autoritatea publică responsabilă verifică periodic, cel puțin o dată pe an, actualitatea datelor de contact, a funcțiilor și a statutului 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. Reguli comune de aplicare și 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 prezenta anexă.

**48.** Desemnarea ofițerului de legătură nu exonerează gestionarul infrastructurii critice naționale 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 prezentei anexe, cu informarea Centrului Național de Coordonare a Protecției Infrastructurilor Critice.

**50.** Centrul Național de Coordonare a Protecției Infrastructurilor Critice va elabora modele orientative de fișe de atribuții, registre de evidență, formulare de notificare și alte instrumente metodologice necesare pentru aplicarea unitară a prezentei anexe.

**51.** Prevederile prezentei anexe 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.

**NOTA DE FUNDAMENTARE**

**la proiectul hotărârii de Guvern 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**

| |
|---|
| **1. Denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului normativ** |
| Proiectul hotărârii de Guvern 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 a fost elaborat de către Inspectoratul de Management Operațional din subordinea Ministerului Afacerilor Interne. |
| **2. Condițiile ce au impus elaborarea proiectului actului normativ** |
| 2.1. Temeiul legal sau, după caz, sursa proiectului actului normativ |
| Proiectul hotărârii de Guvern 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 este elaborat în temeiul art. 7 alin. (2) lit. b) din Legea nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale. |
| 2.2. Descrierea situației actuale și a problemelor care impun intervenția, inclusiv a cadrului normativ aplicabil și a deficiențelor/lacunelor normative |
| Legea nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale stabilește cadrul juridic primar pentru identificarea, desemnarea și protecția infrastructurilor critice naționale, precum și procedura etapizată de identificare a acestora.<br>Prin aprobarea Legii nr. 223/2025, legiuitorul a creat premisele juridice necesare la nivel național pentru inițierea și realizarea procesului de transpunere a Directivei (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE. În prima etapă, aplicarea cadrului legal presupune operaționalizarea mecanismelor instituționale și metodologice necesare identificării, desemnării și protecției infrastructurilor critice naționale, inclusiv prin desemnarea autorităților și instituțiilor publice cu atribuții specifice în sectoarele și subsectoarele prevăzute de lege.<br>Cadrul legal primar stabilește că protecția infrastructurilor critice naționale presupune identificarea și desemnarea infrastructurilor relevante, evaluarea riscurilor, stabilirea măsurilor de securitate, elaborarea Planului de securitate al gestionarului infrastructurii critice naționale, precum și testarea, revizuirea și actualizarea periodică a acestuia.<br>În prezent, la nivel național există reglementări sectoriale și proceduri interne care vizează anumite aspecte ale securității, continuității activității, protecției fizice, securității cibernetice, protecției civile, apărării împotriva incendiilor, răspunsului la incidente sau protecției informațiilor. Totuși, aceste reglementări nu formează un cadru metodologic unitar, aplicabil tuturor sectoarelor și subsectoarelor în care pot fi desemnate infrastructuri critice naționale.<br>Situația actuală evidențiază următoarele probleme principale:<br>a) lipsa unei metodologii unitare pentru evaluarea riscurilor la adresa infrastructurilor critice naționale, care să permită identificarea, analizarea, aprecierea și ierarhizarea riscurilor într-un mod comparabil și verificabil;<br>b) lipsa unei structuri-cadru obligatorii pentru Planul de securitate al gestionarului infrastructurii critice naționale, ceea ce poate genera diferențe de conținut, calitate și aplicabilitate între planurile elaborate de diferiți gestionari; |

c) lipsa unei proceduri clare privind elaborarea, transmiterea spre avizare, examinarea, aprobarea și implementarea Planului de securitate;

d) lipsa unui mecanism normativ clar pentru echivalarea documentelor existente cu Planul de securitate, deși unii gestionari pot deține deja planuri, proceduri sau documente interne relevante privind securitatea, continuitatea, răspunsul la incidente ori recuperarea;

e) lipsa unor reguli uniforme privind revizuirea periodică și extraordinară a Planului de securitate, inclusiv în cazul apariției unor riscuri noi, producerii unor incidente, modificării infrastructurii, schimbării dependențelor sau constatării unor deficiențe în urma testărilor, auditurilor ori controalelor;

f) lipsa unei reglementări metodologice privind rolul, statutul funcțional și atribuțiile ofițerului de legătură pentru securitatea infrastructurii critice naționale, atât la nivelul gestionarilor, cât și în relația cu autoritățile publice responsabile;

g) riscul aplicării neuniforme a obligațiilor legale de către autoritățile publice responsabile și gestionarii infrastructurilor critice naționale;

h) lipsa unui cadru comun pentru trasabilitatea măsurilor, documentarea deciziilor, protecția informațiilor sensibile și monitorizarea implementării măsurilor de securitate.

Deficiențele menționate pot afecta capacitatea autorităților publice responsabile și a gestionarilor de a asigura un nivel minim comun de protecție, securitate, continuitate și reziliență a infrastructurilor critice naționale. În lipsa normelor metodologice, evaluările de risc pot fi realizate pe baze diferite, Planurile de securitate pot avea conținut neuniform, iar mecanismele de avizare, echivalare, revizuire și monitorizare pot fi aplicate diferit de la un sector la altul.

Totodată, domeniul infrastructurilor critice naționale are un caracter multisectorial și interdependent. Infrastructurile din sectoare precum energia, transporturile, comunicațiile electronice, sectorul financiar, sănătatea, alimentarea cu apă, administrația publică, securitatea publică sau alte domenii relevante pot genera efecte în lanț în cazul perturbării, indisponibilizării, compromiterii sau distrugerii acestora. Această realitate impune existența unui cadru metodologic comun, dar suficient de flexibil pentru aplicare sectorială.

Proiectul intervine pentru acoperirea lacunelor normative identificate, prin instituirea unui cadru metodologic unitar, coerent și aplicabil privind evaluarea riscurilor, elaborarea, avizarea, aprobarea, echivalarea, revizuirea și actualizarea Planului de securitate, precum și atribuțiile ofițerului de legătură pentru securitatea infrastructurii critice naționale. Acesta urmărește aplicarea unitară a Legii nr. 223/2025, consolidarea responsabilităților autorităților publice responsabile și ale gestionarilor, precum și creșterea rezilienței și continuității serviciilor esențiale.

Proiectul contribuie la consolidarea cadrului național de reziliență, la clarificarea responsabilităților autorităților publice responsabile și ale gestionarilor infrastructurilor critice naționale, precum și la asigurarea unei abordări coordonate în domeniul protecției infrastructurilor critice naționale.

Totodată, proiectul sprijină armonizarea cadrului național cu direcțiile europene și bunele practici internaționale în domeniul rezilienței, managementului riscurilor, continuității serviciilor esențiale și protecției infrastructurilor critice.

Intrarea în vigoare a hotărârii la data publicării în Monitorul Oficial al Republicii Moldova se justifică prin necesitatea asigurării unui cadru unitar pentru evaluarea riscurilor, elaborarea, avizarea, aprobarea, echivalarea, revizuirea și actualizarea Planurilor de securitate ale gestionarilor infrastructurilor critice naționale.

Prin urmare, intervenția normativă este necesară pentru asigurarea aplicării unitare a Legii nr. 223/2025, pentru consolidarea responsabilităților autorităților publice responsabile și ale gestionarilor infrastructurilor critice naționale, precum și pentru crearea unui mecanism funcțional de evaluare, planificare, implementare, monitorizare, testare și revizuire a măsurilor de securitate aplicabile infrastructurilor critice naționale.

**3. Obiectivele urmărite și soluțiile propuse**

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

Proiectul hotărârii Guvernului stabilește cadrul metodologic necesar pentru aplicarea unitară a prevederilor Legii nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale, în partea ce ține de evaluarea riscurilor, elaborarea, avizarea, aprobarea, echivalarea, revizuirea și actualizarea Planului de securitate al gestionarului infrastructurii critice naționale, precum și de desemnarea și atribuțiile ofițerului de legătură pentru securitatea infrastructurii critice naționale.

Prin proiect se propune aprobarea unui set de norme metodologice structurate în șase anexe, fiecare reglementând o componentă distinctă a mecanismului de protecție a infrastructurilor critice naționale.

Prin anexa nr. 1 se aprobă normele metodologice privind evaluarea riscurilor la adresa infrastructurilor critice naționale. Acestea stabilesc principiile, etapele și instrumentele necesare pentru identificarea amenințărilor, vulnerabilităților, scenariilor de risc, impactului, probabilității, nivelului de risc și riscului rezidual. Elementul nou constă în instituirea unei abordări metodologice unitare, care permite evaluarea riscurilor într-un mod comparabil, documentat și verificabil, indiferent de sectorul sau subsectorul în care este încadrată infrastructura critică națională.

Anexa nr. 2 aprobă normele metodologice privind elaborarea, avizarea și aprobarea Planului de securitate al gestionarului infrastructurii critice naționale. Acestea reglementează modul de elaborare a Planului de securitate, transmiterea acestuia spre avizare, examinarea de către autoritatea publică responsabilă, aprobarea de către gestionar, implementarea, monitorizarea și testarea măsurilor prevăzute. Elementul nou constă în clarificarea circuitului procedural al Planului de securitate, inclusiv a rolurilor gestionarului, autorității publice responsabile și Centrului Național de Coordonare a Protecției Infrastructurilor Critice.

Prin anexa nr. 3 se aprobă structura-cadru a Planului de securitate al gestionarului infrastructurii critice naționale. Aceasta stabilește conținutul minim obligatoriu al Planului de securitate, incluzând datele generale, descrierea infrastructurii și a serviciului esențial, funcțiile critice, activele critice, procesele esențiale, dependențele și interdependențele, rezultatele evaluării riscurilor, măsurile de securitate, continuitate, răspuns, recuperare, comunicare, instruire, testare și revizuire. Elementul nou constă în crearea unui model comun de structurare a Planului de securitate, care reduce riscul unor documente incomplete, neuniforme sau exclusiv declarative.

Anexa nr. 4 aprobă normele metodologice privind echivalarea documentelor existente cu Planul de securitate al gestionarului infrastructurii critice naționale. Acestea permit recunoașterea integrală, parțială sau condiționată a unor documente existente, cum ar fi planurile de continuitate, planurile de răspuns la incidente, planurile de protecție fizică, documentele de securitate cibernetică, procedurile interne sau alte documente relevante. Elementul nou constă în instituirea unui mecanism de echivalare care evită duplicarea nejustificată a documentelor interne, cu condiția ca acestea să acopere cerințele minime ale Planului de securitate.

Prin anexa nr. 5 se aprobă normele metodologice privind revizuirea și actualizarea Planului de securitate al gestionarului infrastructurii critice naționale. Acestea stabilesc regulile privind revizuirea periodică, revizuirea extraordinară, clasificarea modificărilor, reavizarea Planului de securitate, evidența modificărilor și efectele revizuirii asupra documentelor echivalate. Elementul nou constă în introducerea unui mecanism clar de menținere a Planului de securitate într-o formă actuală, aplicabilă și corelată cu evoluția riscurilor, schimbările tehnologice, operaționale, organizaționale sau legislative.

Ultima anexă aprobă Normele metodologice privind desemnarea, statutul funcțional și atribuțiile ofițerului de legătură pentru securitatea infrastructurii critice naționale. Acestea stabilesc modul de desemnare a ofițerului de legătură la nivelul gestionarului infrastructurii

critice naționale, cerințele minime pentru desemnare, atribuțiile privind evaluarea riscurilor, Planul de securitate, cooperarea, raportarea, instruirea și testarea, precum și rolul punctului de contact la nivelul autorității publice responsabile. Elementul nou constă în instituirea unei funcții operaționale de legătură, necesare pentru asigurarea comunicării, coordonării și schimbului de informații între gestionari, autoritățile publice responsabile și Centrul Național de Coordonare a Protecției Infrastructurilor Critice.

Totodată, proiectul se corelează cu Hotărârea Guvernului nr. 185/2026 cu privire la desemnarea autorităților publice responsabile de sectoarele și subsectoarele infrastructurii critice naționale, prin care au fost stabilite autoritățile competente pentru coordonarea proceselor de identificare, evaluare a riscurilor, examinare și monitorizare la nivelul sectoarelor și subsectoarelor respective.

De asemenea, proiectul stabilește atribuțiile generale ale Ministerului Afacerilor Interne, prin Centrul Național de Coordonare a Protecției Infrastructurilor Critice, în ceea ce privește coordonarea metodologică, monitorizarea și acordarea suportului de specialitate pentru aplicarea hotărârii.

Proiectul vizează, în esență:

a) instituirea unei metodologii unitare de evaluare a riscurilor la adresa infrastructurilor critice naționale;

b) stabilirea procedurii de elaborare, avizare și aprobare a Planului de securitate;

c) aprobarea unei structuri-cadru minime obligatorii pentru Planul de securitate;

d) instituirea mecanismului de echivalare a documentelor existente cu Planul de securitate;

e) reglementarea revizuirii și actualizării periodice sau extraordinare a Planului de securitate;

f) clarificarea statutului și atribuțiilor ofițerului de legătură pentru securitatea infrastructurii critice naționale;

g) consolidarea rolului autorităților publice responsabile în avizarea și monitorizarea Planurilor de securitate;

h) asigurarea trasabilității deciziilor, modificărilor, măsurilor și responsabilităților stabilite în domeniul protecției infrastructurilor critice naționale.

Prin urmare, proiectul nu creează doar obligații formale, ci instituie un mecanism practic de lucru pentru autoritățile publice responsabile și gestionarii infrastructurilor critice naționale, orientat spre evaluarea riscurilor, planificarea măsurilor de securitate, asigurarea continuității serviciilor esențiale, răspunsul la incidente, recuperarea și consolidarea rezilienței infrastructurilor critice naționale.

Mecanismele de comunicare și schimb de informații prevăzute de proiect reprezintă ansamblul procedurilor, responsabilităților, fluxurilor de notificare, canalelor și mijloacelor organizatorice sau tehnice utilizate pentru transmiterea, recepționarea, confirmarea și protejarea informațiilor relevante. Implementarea acestora se va realiza, la etapa inițială, prin utilizarea resurselor, canalelor de comunicare și sistemelor informaționale existente. Proiectul nu instituie obligația creării unor platforme sau sisteme informaționale noi. Eventuala dezvoltare a unor soluții tehnice suplimentare va fi realizată în baza unor decizii distincte, cu evaluarea impactului financiar și identificarea surselor de finanțare.

3.2. Opțiunile alternative analizate și motivele pentru care acestea nu au fost luate în considerare

Nu este aplicabil

**4. Analiza impactului de reglementare**

4.1. Impactul asupra sectorului public

Proiectul va avea un impact pozitiv asupra sectorului public, prin instituirea unui cadru metodologic unitar pentru aplicarea prevederilor Legii nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale, în partea ce ține de evaluarea

riscurilor, elaborarea, avizarea, aprobarea, echivalarea, revizuirea și actualizarea Planului de securitate al gestionarului infrastructurii critice naționale.

Prin aprobarea proiectului, autoritățile publice responsabile vor dispune de reguli clare pentru examinarea evaluărilor de risc, avizarea Planurilor de securitate, monitorizarea conformării gestionarilor infrastructurilor critice naționale și coordonarea sectorială a măsurilor de protecție, continuitate, răspuns și recuperare.

Proiectul va contribui la aplicarea uniformă a Legii nr. 223/2025 și la reducerea riscului de interpretări neunitare între sectoare și subsectoare, prin stabilirea unor cerințe metodologice comune privind conținutul Planului de securitate, procedura de avizare, mecanismul de echivalare a documentelor existente, regulile de revizuire și actualizare, precum și atribuțiile ofițerului de legătură pentru securitatea infrastructurii critice naționale.

Totodată, proiectul va sprijini activitatea Centrului Național de Coordonare a Protecției Infrastructurilor Critice în exercitarea rolului de coordonare metodologică, monitorizare și acordare a suportului de specialitate autorităților publice responsabile și gestionarilor infrastructurilor critice naționale.

Impactul asupra sectorului public este preponderent organizatoric, procedural și metodologic. Proiectul nu presupune crearea unor structuri noi, ci valorificarea competențelor instituționale existente și clarificarea mecanismelor de cooperare dintre Ministerul Afacerilor Interne, Centrul Național de Coordonare a Protecției Infrastructurilor Critice, autoritățile publice responsabile și gestionarii infrastructurilor critice naționale.

4.2. Impactul financiar și argumentarea costurilor estimative

Implementarea prevederilor proiectului hotărârii Guvernului nu implică alocarea unor resurse financiare suplimentare directe de la bugetul de stat.

Aplicarea normelor metodologice propuse se va realiza de către autoritățile publice responsabile și gestionarii infrastructurilor critice naționale în limita competențelor funcționale și a resurselor instituționale existente.

Proiectul stabilește cadrul metodologic pentru evaluarea riscurilor și planificarea măsurilor de securitate, continuitate, răspuns și recuperare. Eventualele costuri aferente implementării măsurilor concrete identificate în urma evaluării riscurilor vor fi determinate individual, la nivelul fiecărui gestionar, în funcție de specificul infrastructurii critice naționale, nivelul riscurilor, măsurile existente și necesitatea unor măsuri suplimentare.

Prin urmare, proiectul nu generează prin sine cheltuieli bugetare imediate, ci creează mecanismul de identificare, fundamentare și planificare a măsurilor necesare pentru protecția infrastructurilor critice naționale.

4.3. Impactul asupra sectorului privat

Proiectul are impact asupra sectorului privat în măsura în care anumite persoane juridice de drept privat pot avea calitatea de gestionari ai infrastructurilor critice naționale sau pot administra ori opera infrastructuri, sisteme, instalații, rețele, servicii ori active relevante pentru furnizarea serviciilor esențiale de interes național.

Impactul principal constă în instituirea unui cadru clar și previzibil pentru obligațiile metodologice ale gestionarilor infrastructurilor critice naționale, inclusiv în ceea ce privește:

a) realizarea evaluării riscurilor;

b) elaborarea Planului de securitate;

c) transmiterea Planului spre avizare;

d) implementarea măsurilor de securitate, continuitate, răspuns și recuperare;

e) desemnarea ofițerului de legătură;

f) revizuirea și actualizarea Planului de securitate;

g) posibilitatea echivalării documentelor existente cu Planul de securitate.

Proiectul nu instituie obligații investiționale directe și uniforme pentru toate entitățile private. Măsurile concrete care pot presupune costuri vor rezulta din evaluarea riscurilor și

din Planul de securitate al fiecărui gestionar, fiind stabilite proporțional cu nivelul riscurilor, specificul infrastructurii și măsurile deja existente.

Un element pozitiv pentru sectorul privat îl constituie mecanismul de echivalare a documentelor existente, care permite recunoașterea integrală sau parțială a unor planuri, proceduri sau documente interne deja aprobate și aplicate, evitând duplicarea nejustificată a documentației administrative.

Pe termen mediu, proiectul poate contribui la consolidarea cooperării public-private, la îmbunătățirea schimbului de informații relevante, la creșterea nivelului de pregătire al gestionarilor și la consolidarea rezilienței serviciilor esențiale furnizate populației, economiei și instituțiilor statului.

4.4. Impactul social

Proiectul are un impact social pozitiv, prin contribuția la consolidarea rezilienței infrastructurilor critice naționale și a serviciilor esențiale de interes național, precum și la creșterea capacității autorităților publice responsabile și a gestionarilor de a preveni, gestiona și depăși incidentele care pot afecta populația, economia și funcțiile vitale ale societății.

Aplicarea unui cadru metodologic unitar pentru evaluarea riscurilor și elaborarea Planurilor de securitate va contribui la îmbunătățirea capacității de prevenire, pregătire, răspuns și recuperare în cazul perturbării, indisponibilizării, compromiterii sau distrugerii infrastructurilor critice naționale.

Prin stabilirea unor cerințe unitare privind evaluarea riscurilor, identificarea vulnerabilităților, planificarea măsurilor de securitate, continuitate, răspuns și recuperare, proiectul creează cadrul necesar pentru menținerea continuității furnizării serviciilor esențiale către populație, inclusiv în domenii precum energia, alimentarea cu apă, transportul, sănătatea și comunicațiile. Aplicarea acestor măsuri permite identificarea anticipată a riscurilor și pregătirea unor mecanisme de continuitate și recuperare, contribuind astfel la reducerea duratei și amplorii eventualelor întreruperi ale serviciilor esențiale în situații de criză sau incidente majore.

Prin consolidarea măsurilor de securitate, continuitate, notificare, răspuns și recuperare, proiectul contribuie indirect la protejarea populației, la limitarea consecințelor sociale și economice ale incidentelor și la menținerea stabilității și funcționării normale a comunităților.

4.4.1. Impactul asupra datelor cu caracter personal

Proiectul nu instituie, prin sine, mecanisme noi de colectare sau prelucrare sistematică a datelor cu caracter personal. Totodată, în procesul de aplicare a normelor metodologice pot fi prelucrate anumite date profesionale sau de contact ale persoanelor desemnate în calitate de ofițeri de legătură, puncte de contact, responsabili de securitate ori membri ai structurilor interne implicate în evaluarea riscurilor și aplicarea Planului de securitate.

Prelucrarea acestor date se va realiza exclusiv în scopul aplicării Legii nr. 223/2025 și a hotărârii Guvernului, cu respectarea legislației privind protecția datelor cu caracter personal și a principiilor de legalitate, proporționalitate, minimizare și securitate a datelor.

Proiectul conține prevederi privind protecția informațiilor și limitarea accesului la documentele care pot conține date sensibile, vulnerabilități, scenarii de risc, măsuri de securitate, puncte sensibile sau alte informații protejate de lege.

4.4.2. Impactul asupra echității și egalității de gen

Din perspectiva echității și egalității de gen, proiectul nu conține prevederi care să genereze discriminare directă sau indirectă. Normele propuse se aplică în mod uniform autorităților publice responsabile și gestionarilor infrastructurilor critice naționale și nu produc impact diferențiat asupra femeilor și bărbaților.

Totodată, proiectul nu limitează participarea femeilor sau bărbaților în exercitarea atribuțiilor privind evaluarea riscurilor, elaborarea Planurilor de securitate, desemnarea ofițerilor de legătură, participarea la instruiri, exerciții, testări sau alte activități relevante pentru protecția infrastructurilor critice naționale.

4.5. Impactul asupra mediului

Proiectul nu are un impact direct asupra mediului, întrucât reglementează aspecte metodologice privind evaluarea riscurilor, elaborarea, avizarea, aprobarea, echivalarea, revizuirea și actualizarea Planurilor de securitate ale gestionarilor infrastructurilor critice naționale.

Totodată, metodologia propusă permite includerea riscurilor de mediu, a efectelor negative asupra mediului și a consecințelor ecologice ale perturbării, indisponibilizării, compromiterii sau distrugerii infrastructurilor critice naționale în cadrul procesului de evaluare a riscurilor și de planificare a măsurilor de securitate, continuitate, răspuns și recuperare.

Prin consolidarea mecanismelor de evaluare a riscurilor și de planificare a măsurilor de protecție, proiectul poate contribui indirect la reducerea riscurilor asociate incidentelor cu impact asupra mediului și la creșterea capacității de prevenire, limitare și gestionare a efectelor generate de perturbarea serviciilor esențiale.

4.6. Alte impacturi și informații relevante

Nu este aplicabil

**5. Compatibilitatea proiectului actului normativ cu legislația UE**

5.1. Măsuri normative necesare pentru transpunerea actelor juridice ale UE în legislația națională

Nu este aplicabil

5.2. Măsuri normative care urmăresc crearea cadrului juridic intern necesar pentru implementarea legislației UE

Proiectul nu constituie un act de transpunere directă a dreptului Uniunii Europene. Totodată, acesta contribuie la implementarea progresivă a standardelor europene relevante în domeniul rezilienței entităților critice, inclusiv a principiilor și abordărilor prevăzute de Directiva (UE) 2022/2557 privind reziliența entităților critice, prin instituirea unui cadru metodologic național privind evaluarea riscurilor, planificarea măsurilor de securitate, continuitatea serviciilor esențiale și protecția infrastructurilor critice naționale.

**6. Avizarea și consultarea publică a proiectului actului normativ**

În conformitate cu prevederile privind etapele principale ale legiferării, la 6 martie 2026, atât pe site-ul web oficial al Ministerului Afacerilor Interne, la compartimentul „Transparență”, subcompartimentul „Consultări publice”, secțiunea „Inițierea elaborării actelor normative”, cât și pe portalul particip.gov.md, a fost plasată informația despre inițierea procesului de elaborare a actului normativ și oferite detalii despre modalitatea înaintării propunerilor din partea părților cointeresate.

Confirmarea poate fi identificată la următoarele adrese web:

https://mai.gov.md/ro/consultari-publice

https://particip.gov.md/ro/document/stages/proiectul-hotarare-a-guvernului-privind-evaluarea-riscurilor-aferente-infrastructurii-critice-nation/16342

**7. Concluziile expertizelor**

Proiectul a fost supus expertizei juridice de către Ministerul Justiției și expertizei anticorupție de către Centrul Național Anticorupție.

Ministerul Justiției a formulat observații și recomandări privind claritatea și corelarea unor norme, tehnica legislativă, termenele procedurale, caracterul obligatoriu al unor documente, evitarea dublărilor normative și corelarea sistematică a anexelor proiectului. Observațiile și recomandările formulate au fost examinate și, după caz, acceptate, acceptate

parțial sau argumentat neacceptate, modificările corespunzătoare fiind operate în proiect și reflectate în Sinteza obiecțiilor și propunerilor.

Centrul Național Anticorupție a efectuat expertiza anticorupție a proiectului, fiind formulate recomandări pentru eliminarea unor norme redundante, corelarea unor prevederi cu conținut similar, clarificarea efectelor respingerii echivalării documentelor și corelarea periodicității testării și revizuirii Planului de securitate. Recomandările formulate au fost examinate și valorificate la definitivarea proiectului, în vederea diminuării riscurilor de interpretare neuniformă și a asigurării clarității și previzibilității normelor.

În urma expertizelor, proiectul a fost revizuit și definitivat, iar modul de examinare și încorporare a observațiilor și recomandărilor este reflectat în Sinteza obiecțiilor și propunerilor.

**8. Modul de încorporare a actului în cadrul normativ existent**

Proiectul hotărârii Guvernului se încorporează în cadrul normativ existent ca act normativ subsecvent Legii nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale.

Prin proiect se asigură dezvoltarea cadrului normativ secundar necesar pentru aplicarea prevederilor Legii nr. 223/2025, în partea ce ține de evaluarea riscurilor la adresa infrastructurilor critice naționale, elaborarea, avizarea, aprobarea, echivalarea, revizuirea și actualizarea Planului de securitate al gestionarului infrastructurii critice naționale, precum și stabilirea atribuțiilor ofițerului de legătură pentru securitatea infrastructurii critice naționale.

Actul normativ propus nu modifică și nu abrogă acte normative în vigoare, ci instituie cadrul metodologic necesar pentru aplicarea unitară a obligațiilor prevăzute de Legea nr. 223/2025. Prevederile proiectului urmează a fi aplicate în corelare cu legislația privind securitatea națională, protecția informațiilor atribuite la secret de stat, protecția datelor cu caracter personal, securitatea cibernetică, protecția civilă, situațiile excepționale, prevenirea și combaterea terorismului, precum și cu reglementările sectoriale aplicabile domeniilor în care pot fi desemnate infrastructuri critice naționale.

Totodată, proiectul prevede obligația ministerelor, altor autorități administrative centrale și instituțiilor publice responsabile de a aduce actele normative departamentale, procedurile interne și documentele aplicabile în concordanță cu prevederile hotărârii, în termenul stabilit de aceasta.

În vederea implementării unitare a actului normativ, autoritățile publice responsabile vor putea elabora instrucțiuni sectoriale, ghiduri, modele de documente sau proceduri interne, cu respectarea cadrului metodologic aprobat prin hotărâre și cu informarea Centrului Național de Coordonare a Protecției Infrastructurilor Critice.

Totodată, proiectul este compatibil cu:

- cadrul național de evaluare a riscurilor la adresa securității naționale;
- cadrul normativ privind protecția informațiilor sensibile și clasificate;
- documentele strategice și obligațiile asumate de Republica Moldova în contextul procesului de aderare la Uniunea Europeană.

**9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ**

Implementarea prevederilor proiectului hotărârii Guvernului va fi realizată de Ministerul Afacerilor Interne, prin intermediul Centrului Național de Coordonare a Protecției Infrastructurilor Critice, de autoritățile publice responsabile și de gestionarii infrastructurilor critice naționale, potrivit competențelor stabilite de Legea nr. 223/2025 și de cadrul metodologic aprobat prin proiect.

Pentru aplicarea prevederilor proiectului vor fi necesare următoarele măsuri:

a) informarea autorităților publice responsabile și, după caz, a gestionarilor infrastructurilor critice naționale cu privire la cadrul metodologic aprobat;

b) desemnarea sau actualizarea punctelor de contact la nivelul autorităților publice responsabile și a ofițerilor de legătură pentru securitatea infrastructurii critice naționale la nivelul gestionarilor;

c) organizarea, după caz, a unor activități de instruire, consultare sau suport metodologic privind evaluarea riscurilor, elaborarea Planului de securitate, echivalarea documentelor existente, revizuirea și actualizarea Planului;

d) elaborarea sau ajustarea procedurilor interne ale autorităților publice responsabile privind examinarea, avizarea, monitorizarea și evidența Planurilor de securitate;

e) elaborarea, avizarea și aprobarea Planurilor de securitate ale gestionarilor infrastructurilor critice naționale, în condițiile prevăzute de cadrul metodologic;

f) examinarea documentelor existente ale gestionarilor care pot fi recunoscute, integral sau parțial, ca echivalente ale Planului de securitate;

g) instituirea evidenței Planurilor de securitate, a documentelor echivalate, a revizuirilor, actualizărilor și măsurilor de implementare;

h) asigurarea protecției informațiilor atribuite la secret de stat, datelor cu caracter personal, informațiilor sensibile privind infrastructurile critice naționale și altor categorii de informații protejate de lege;

i) monitorizarea implementării măsurilor de securitate, continuitate, răspuns și recuperare stabilite în Planurile de securitate;

j) aducerea actelor normative departamentale, procedurilor interne și documentelor aplicabile în concordanță cu prevederile hotărârii, în termenul stabilit de aceasta.

Implementarea proiectului nu necesită crearea unor structuri instituționale noi, ci presupune valorificarea mecanismelor și competențelor existente la nivelul Ministerului Afacerilor Interne, autorităților publice responsabile și gestionarilor infrastructurilor critice naționale.

Centrul Național de Coordonare a Protecției Infrastructurilor Critice va asigura coordonarea metodologică, monitorizarea și suportul de specialitate necesar pentru aplicarea unitară a prevederilor hotărârii.

**Ministru** **Daniella MISAIL-NICHITIN**

**SINTEZA**
**proiectul hotărârii de Guvern 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**

| Participantul la avizare, consultare publică, expertizare | Nr. crt. | Conținutul obiecției, propunerii, recomandării, concluziei | Argumentarea autorului proiectului |
|---|---|---|---|
| **Avizare și consultare publică** | | | |
| **Cancelaria de Stat (aviz nr. 12-69-8657 din 23.07.2026)** | 1 | Denumirea proiectului și formularea dispoziției de aprobare urmează a fi corelate terminologic, astfel încât să rezulte cu claritate că prin hotărâre se aprobă ansamblul anexelor care constituie cadrul metodologic, nu doar o parte a acestuia. | **Se acceptă.** Denumirea proiectului și pct. 1 din proiectul hotărârii au fost corelate terminologic, fiind precizat că cadrul metodologic aprobat este constituit din ansamblul celor șase anexe privind evaluarea riscurilor, elaborarea, avizarea și aprobarea Planului de securitate, structura-cadru a acestuia, echivalarea documentelor existente, revizuirea și actualizarea Planului de securitate, precum și statutul și atribuțiile ofițerului de legătură pentru securitatea infrastructurii critice naționale. |
| | | Se recomandă verificarea uniformității utilizării noțiunilor „Planul de securitate”, „planurile de securitate”, „cadrul metodologic”, „norme metodologice”, precum și a sintagmelor referitoare la „autoritățile publice responsabile”, pentru evitarea oscilațiilor terminologice în textul hotărârii și în anexele acesteia. | **Se acceptă.** Terminologia utilizată în proiectul hotărârii și în anexele acestuia a fost revizuită și uniformizată, astfel încât noțiunile „Planul de securitate”, „cadrul metodologic”, „Normele metodologice” și „autoritățile publice responsabile” să fie utilizate consecvent și în concordanță cu |

| | | | |
|---|---|---|---|
| | | | obiectul de reglementare al fiecărui element structural. |
| | | În textul anexei nr. 1 se identifică unele formulări care necesită corectare redacțională ori completare, inclusiv:<br>• formularea „obligațiilor specific prevăzute”, care urmează a fi ajustată gramatical;<br>• propoziția referitoare la „Evaluarea Națională a Riscurilor, evaluărilor strategice și altor documente relevante...”, care apare incompletă și necesită reformulare;<br>• formularea „pericole ori hazarde, constând în evenimente, procese sau independente de intenția ostilă a unui actor”, care necesită completare pentru a exprima clar ipoteza normativă. | **Se acceptă parțial.** Formulările din anexa nr. 1 au fost revizuite și corectate redacțional. Astfel, sintagma „obligațiilor specific prevăzute” a fost ajustată gramatical.<br><br>Nu se acceptă observația referitoare la formularea privind „Evaluarea Națională a Riscurilor, evaluărilor strategice și altor documente relevante”, întrucât aceasta face parte din enumerarea surselor utilizate pentru identificarea amenințărilor, pericolelor și surselor de risc, iar sensul normei rezultă în mod clar din coroborarea subpct. 26.7 cu partea introductivă a pct. 26 din anexa nr. 1.<br><br>Se acceptă observația privind formularea „pericole ori hazarde, constând în evenimente, procese sau independente de intenția ostilă a unui actor”. Prevederea a fost completată prin introducerea termenului „fenomene”, astfel încât formularea să prevadă expres „evenimente, procese sau fenomene independente de intenția ostilă a unui actor”. |

| | | | |
|---|---|---|---|
| | | În anexa nr. 2, pct. 5, formularea „în cazul în care același gestionar administrează sau operează mai mult infrastructuri critice naționale” necesită corectare gramaticală. | **Se acceptă.** Formularea de la pct. 5 din anexa nr. 2 a fost corectată gramatical, |
| | | Se recomandă verificarea tuturor trimiterilor interne din anexe, pentru a se asigura concordanța dintre punctele, subpunctele și anexele la care se face referire, precum și pentru a evita eventuale inadvertențe de numerotare ori autoreferințe eronate. | **Se acceptă.** Modificările au fost operate**.** |
| | | Din perspectiva delimitării competențelor, se recomandă reevaluarea formulărilor prin care Centrului Național de Coordonare a Protecției Infrastructurilor Critice i se atribuie competențe de „aprobare” a unor modele-tip și instrumente metodologice, în vederea corelării stricte a acestora cu temeiul legal din Legea nr. 223/2025 și cu competențele stabilite pentru autoritățile publice implicate. | **Se acceptă.** Formulările referitoare la competențele Centrului Național de Coordonare a Protecției Infrastructurilor Critice au fost revizuite și corelate cu prevederile art. 7 alin. (2) din Legea nr. 223/2025. |
| | | Norma prin care ministerele, alte autorități administrative centrale și instituțiile publice responsabile urmează să își aducă actele departamentale și procedurile interne în concordanță cu hotărârea necesită o corelare mai clară cu termenele și obligațiile aplicabile gestionarilor infrastructurilor critice naționale, pentru a evita neclarități în procesul de implementare. | **Se acceptă.** Pct. 9 din proiect a fost completat pentru a delimita expres termenul de 12 luni acordat autorităților pentru aducerea actelor normative departamentale, procedurilor interne și documentelor aplicabile în concordanță cu prevederile hotărârii de obligația gestionarilor infrastructurilor critice naționale de a elabora și transmite spre avizare Planul de securitate în termenul prevăzut de cadrul metodologic. |
| | | Se recomandă examinarea suplimentară a caracterului suficient de determinat al unor formulări cu grad ridicat de generalitate, precum „alte riscuri relevante”, „alte instrumente necesare” sau „alte măsuri relevante”, astfel încât textul să păstreze flexibilitatea necesară, fără a afecta previzibilitatea normei. | **Nu se acceptă.** Formulările menționate sunt utilizate pentru a asigura flexibilitatea aplicării cadrului metodologic în raport cu specificul diferitelor sectoare, subsectoare și infrastructuri critice naționale. Acestea nu instituie obligații autonome și nedeterminate, ci se aplică în contextul criteriilor, procedurilor și competențelor expres prevăzute de proiect. Limitarea exhaustivă a categoriilor de riscuri, măsuri sau instrumente ar putea exclude situații relevante care nu pot fi anticipate în mod |

| | | | |
|---|---|---|---|
| | | | complet la momentul aprobării cadrului metodologic. În consecință, se menține redacția actuală. |
| | | Se recomandă completarea proiectului cu prevederi exprese privind efectele juridice ale nerespectării termenelor procedurale, întrucât textul nu stabilește ce se întâmplă în situația în care autoritatea publică responsabilă nu emite avizul în termen, nu clarifică dacă actul de restituire sau de respingere poate fi contestat și nu reglementează consecințele depășirii termenului de 6 luni. În vederea asigurării previzibilității și aplicării uniforme a normei, aceste aspecte urmează a fi reglementate expres. | **Nu se acceptă**. Proiectul stabilește termene clare pentru verificarea plenitudinii dosarului, examinarea în fond, solicitarea completărilor, retransmiterea și reexaminarea Planului de securitate, precum și posibilitatea prelungirii motivate a termenului de examinare. Depășirea termenului de către autoritatea publică responsabilă nu poate produce efectul avizării tacite în lipsa unui temei legal expres, obligația acesteia de a finaliza examinarea și de a emite o soluție menținându-se.<br><br>În ceea ce privește contestarea actelor emise în cadrul procedurii, aceasta se realizează potrivit cadrului normativ general aplicabil procedurii administrative, nefiind necesară instituirea unei căi speciale de contestare prin prezentul proiect.<br><br>Totodată, depășirea termenului prevăzut pentru elaborarea și transmiterea Planului de securitate nu înlătură obligația gestionarului de a executa această obligație, iar eventualele consecințe ale neexecutării se stabilesc potrivit legislației aplicabile. Introducerea unor norme suplimentare în proiect ar dubla reglementările generale și ar depăși obiectul metodologic al hotărârii. |

| | | | |
|---|---|---|---|
| | | Se recomandă completarea proiectului cu prevederi exprese privind participarea autorităților administrației publice locale în procesul reglementat. Potrivit pct. 9 din anexa nr. 1 la Legea nr. 223/2025, „administrația publică” este clasificată ca sector al infrastructurii critice naționale, iar „autoritățile administrației publice locale” sunt prevăzute în calitate de furnizori de servicii. Cu toate acestea, proiectul nu stabilește în mod clar rolul, atribuțiile și modalitatea de implicare a acestora în procesul de aplicare a normelor propuse, nici mecanismele de conlucrare cu autoritățile publice responsabile și cu celelalte autorități implicate. Se recomandă reglementarea expresă a etapelor în care participă autoritățile administrației publice locale, a obligațiilor care le revin și a modului de coordonare și schimb de informații cu celelalte autorități competente | **Nu se acceptă.** Autoritățile administrației publice locale participă la aplicarea cadrului metodologic în măsura în care dețin calitatea de gestionar al unei infrastructuri critice naționale sau exercită atribuții stabilite de cadrul normativ aplicabil sectorului ori subsectorului respectiv. Proiectul reglementează obligațiile în funcție de calitatea juridică și rolul entității în mecanismul de protecție a infrastructurilor critice naționale, fără a institui regimuri procedurale distincte pentru fiecare categorie de furnizor de servicii prevăzută în anexa nr. 1 la Legea nr. 223/2025.<br><br>Totodată, mecanismele de cooperare, coordonare și schimb de informații sunt reglementate prin raportare la autoritățile publice responsabile, gestionarii infrastructurilor critice naționale și celelalte autorități competente, acestea fiind aplicabile și autorităților administrației publice locale atunci când participă în una dintre aceste calități. Introducerea unor prevederi distincte exclusiv pentru autoritățile administrației publice locale ar dubla normele generale deja aplicabile și nu se justifică prin obiectul metodologic al proiectului. |
| | | Nota de fundamentare urmează a fi revizuită sub aspect redacțional și al coerenței interne, inclusiv pentru:<br>• uniformizarea terminologiei utilizate în raport cu textul proiectului;<br>• clarificarea unor secțiuni în care formulările sunt excesiv descriptive și repetitive; | **Se acceptă.** Nota de fundamentare a fost revizuită sub aspect redacțional și al coerenței interne, |

| | | | |
|---|---|---|---|
| | | • verificarea prezentării distincte a impactului social, inclusiv a subsecțiunilor privind datele cu caracter personal și egalitatea de gen. | |
| **Centrul Național de Management al Crizelor (aviz nr. 3-221 din 09.07.2026.)** | 2 | Cu referire la proiectul hotărârii, se recomandă precizarea mai clară a delimitării competențelor între autoritățile sectoriale și Centrul Național de Coordonare a Protecției Infrastructurilor Critice, pentru evitarea suprapunerilor funcționale; este necesară detalierea procedurii de avizare a planurilor de securitate, inclusiv a termenelor și etapelor administrative; se propune armonizarea prevederilor cu alte domenii conexe (securitate cibernetică, protecție civilă, continuitatea guvernării), pentru asigurarea coerenței normative. | **Se acceptă.** Proiectul a fost revizuit pentru delimitarea mai clară a competențelor dintre autoritățile publice responsabile și Centrul Național de Coordonare a Protecției Infrastructurilor Critice. Astfel, autoritățile publice responsabile asigură coordonarea la nivelul sectorului sau subsectorului de competență, examinarea și avizarea Planurilor de securitate, monitorizarea implementării măsurilor și emiterea instrucțiunilor sectoriale, iar Centrul asigură coordonarea metodologică la nivel național, elaborarea modelelor-tip și a instrumentelor standardizate, precum și suportul metodologic necesar aplicării unitare a cadrului.<br><br>Totodată, procedura de avizare a Planurilor de securitate a fost detaliată prin stabilirea etapelor administrative, a termenelor pentru verificarea plenitudinii dosarului, examinarea în fond, solicitarea completărilor, restituirea pentru revizuire și reexaminarea documentelor.<br><br>Prevederile proiectului au fost, de asemenea, corelate cu normele aplicabile în domeniile conexe, |

| | | | |
|---|---|---|---|
| | | | inclusiv securitatea cibernetică, protecția civilă, managementul crizelor și continuitatea guvernării, pentru evitarea suprapunerilor și asigurarea coerenței normative. |
| | | Referitor la proiectul Normelor metodologice privind evaluarea riscurilor la adresa infrastructurilor critice naționale (Anexa nr. 1), se propune:<br>Completarea pct. 26 cu prevederea că, identificarea amenințărilor și a riscurilor se realizează inclusiv în baza Evaluării Naționale a Riscurilor, a evaluărilor strategice și a altor documente elaborate în cadrul Sistemului național de management al crizelor. | **Se acceptă.** Pct. 26 din anexa nr. 1 a fost completat cu subpct. 26.7, prin includerea Evaluării Naționale a Riscurilor, a evaluărilor strategice și a altor documente relevante elaborate în cadrul Sistemului național de management al crizelor printre sursele utilizate la identificarea amenințărilor, pericolelor și surselor de risc. |
| | | Completarea pct. 32, astfel încât, la evaluarea riscurilor hibride și a riscurilor cu impact sistemic, să fie analizate și efectele asupra continuității funcțiilor vitale ale statului și asupra rezilienței naționale. | **Se acceptă.** Anexa nr. 1, la pct. 32.4 a fost completată cu un punct distinct, potrivit căruia, în cazul riscurilor hibride și al riscurilor cu impact sistemic, evaluarea include analiza efectelor potențiale asupra continuității funcțiilor vitale ale statului, asupra altor sectoare și infrastructuri critice naționale, precum și asupra rezilienței naționale. Prevederea a fost introdusă separat de clasificarea riscurilor, întrucât aspectele menționate reprezintă efecte și consecințe ale materializării riscurilor, nu categorii distincte de risc. |
| | | Completarea pct. 63, prin includerea actualizării evaluării riscurilor și în cazul modificării nivelului de alertă sau al declarării unei stări de criză, dacă aceasta afectează infrastructura critică națională ori serviciile esențiale. | **Se acceptă.** În urma renumerotării proiectului, prevederea vizată se regăsește la pct. 64 din anexa nr. 1. |

| | | | |
|---|---|---|---|
| | | | Subpct. 64.7 a fost completat cu un temei suplimentar pentru actualizarea evaluării riscurilor, respectiv modificarea nivelului de alertă sau declararea unei stări de criză, atunci când aceasta afectează ori poate afecta infrastructura critică națională sau continuitatea serviciului esențial furnizat. |
| | | Completarea pct. 74, prin prevederea că, modelele metodologice elaborate de Centrul Național de Coordonare a Protecției Infrastructurilor Critice vor fi dezvoltate în coordonare cu autoritățile competente în domeniul managementului crizelor, pentru asigurarea unei abordări unitare la nivel național. | **Se acceptă.** Pct. 74 a fost completat prin precizarea că modelele-tip și instrumentele metodologice se elaborează, după caz, în coordonare cu autoritățile competente în domeniu, pentru asigurarea unei abordări coerente și unitare la nivel național. |
| | | Referitor la proiectul Normelor metodologice privind elaborarea, avizarea și aprobarea Planurilor de securitate ale gestionarilor infrastructurilor critice naționale (Anexa nr. 2), se propune:<br>La pct. 18 (conținutul Planului de securitate), se propune completarea cu obligația includerii mecanismelor de coordonare și cooperare cu autoritățile competente în gestionarea<br>situațiilor de criză, în cazul producerii unor incidente cu impact sistemic. | **Se acceptă.** Pct. 18 din anexa nr. 2 se completează cu un subpunct distinct privind mecanismele de coordonare și cooperare cu autoritățile competente în gestionarea situațiilor de criză, aplicabile în cazul incidentelor care depășesc capacitatea de răspuns a gestionarului sau produc efecte sistemice ori intersectoriale.<br><br>Se introduce următorul subpunct:<br>„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;” |

| | | | |
|---|---|---|---|
| | | La pct. 31 și pct. 86, se recomandă ca Planul de securitate să fie corelat nu doar cu documentele interne ale gestionarului, ci și cu documentele naționale privind continuitatea<br>funcțiilor vitale ale statului, reziliența națională și managementul crizelor, după caz. | **Se acceptă.** În urma renumerotării proiectului, prevederea vizată se regăsește la pct. 32 din anexa nr. 2. Subpct. 32.7 din anexa nr. 2 a fost completat prin includerea, între documentele valorificate la elaborarea Planului de securitate, a documentelor naționale relevante privind continuitatea funcțiilor vitale ale statului, reziliența națională și managementul crizelor, după caz.<br><br>Totodată, în urma renumerotării anexei nr. 2, prevederea vizată inițial la pct. 86 se regăsește la pct. 95. Pct. 95 a fost completat prin introducerea obligației de corelare a Planului de securitate, după caz, cu documentele naționale privind continuitatea funcțiilor vitale ale statului, reziliența națională și managementul crizelor. |
| | | La Capitolul X – Testarea Planului de securitate, se propune completarea cu prevederea că exercițiile privind scenariile cu impact major asupra serviciilor esențiale se desfășoară, după caz, cu participarea autorităților competente din cadrul Sistemului național de management al crizelor, pentru verificarea mecanismelor de coordonare interinstituțională. Se recomandă completarea metodologiei cu prevederi privind valorificarea lecțiilor învățate rezultate din gestionarea situațiilor de criză, exerciții naționale și incidente majore, ca element obligatoriu în procesul de revizuire și actualizare a Planului de securitate. Deși documentul face referire la incidente și exerciții, nu stabilește obligația integrării sistematice a lecțiilor învățate în ciclul de planificare. | **Se acceptă.** Capitolul X din anexa nr. 2 a fost completat prin introducerea pct. 82, cu următorul cuprins:<br><br>**„**82. 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.”<br><br>Totodată, prevederea privind valorificarea rezultatelor testării a fost revizuită, prin introducerea pct. 84 cu următorul cuprins:<br><br>„84. Constatările, concluziile și lecțiile identificate în urma testării Planului de securitate, gestionării situațiilor de criză, exercițiilor naționale și 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 la prezenta hotărâre.” |
| | | Planul de securitate nu conține prevederi privind integrarea în mecanismele naționale de management al crizelor în cazul incidentelor care depășesc capacitatea de răspuns a gestionarului sau generează efecte intersectoriale. În acest sens, lipsesc reglementări referitoare la escaladarea strategică a incidentelor, inclusiv criteriile de informare a Centrului Național de Management al Crizelor, activarea coordonării interinstituționale și integrarea planului de securitate în managementul unei crize la nivel național. | **Se acceptă.** Anexa nr. 3 a fost completată la Secțiunea 10 „Măsuri de răspuns, notificare și recuperare”, prin introducerea unor prevederi privind criteriile și nivelurile de escaladare a incidentelor care depășesc capacitatea de răspuns a gestionarului sau generează efecte sistemice ori intersectoriale, procedura de informare a Centrului Național de Management al Crizelor, activarea coordonării interinstituționale și integrarea măsurilor de răspuns, continuitate și |

| | | | |
|---|---|---|---|
| | | | recuperare în mecanismele de gestionare a unei crize la nivel național.<br><br>Totodată, Secțiunea 11 „Organizarea, responsabilitățile și mecanismele de coordonare” a fost completată cu prevederi privind cooperarea și coordonarea cu Centrul Național de Management al Crizelor și cu alte autorități competente în cazul incidentelor cu impact sistemic ori intersectorial. |
| | | Referitor la proiectul Structurii-cadru a Planului de securitate al gestionarului infrastructurii critice naționale (Anexa nr. 3), în vederea asigurării compatibilității cu Sistemul național de management al crizelor, se propune:<br><br>Completarea pct. 8 cu un obiectiv distinct privind menținerea contribuției infrastructurii critice la continuitatea funcțiilor vitale ale statului și la consolidarea rezilienței naționale. | **Se acceptă.** În urma renumerotării anexei nr. 3, prevederea vizată se regăsește la pct. 11, care stabilește obiectivele Planului de securitate. Pct. 11 a fost completat cu un obiectiv distinct privind menținerea contribuției infrastructurii critice naționale la continuitatea funcțiilor vitale ale statului și la consolidarea rezilienței naționale.<br><br>Se introduce subpct. 11.8, cu următorul cuprins:<br>*„11.8. menținerea contribuției infrastructurii critice naționale la continuitatea funcțiilor vitale ale statului și la consolidarea rezilienței naționale.”* |
| | | Completarea pct. 12.10 astfel încât implicațiile evaluării riscurilor să fie analizate inclusiv din perspectiva impactului asupra funcțiilor vitale ale statului și a efectelor intersectoriale generate de indisponibilizarea infrastructurii critice. | **Se acceptă.** Subpct. 12.10 din anexa nr. 3 a fost completat astfel încât implicațiile evaluării riscurilor asupra |

| | | | |
|---|---|---|---|
| | | | măsurilor de securitate, continuitate, răspuns și recuperare să fie analizate inclusiv din perspectiva impactului potențial asupra continuității funcțiilor vitale ale statului și a efectelor sistemice sau intersectoriale generate de indisponibilizarea infrastructurii critice naționale. |
| | | Completarea pct. 20.7 prin includerea mecanismelor de coordonare cu autoritățile competente din cadrul Sistemului național de management al crizelor, în situațiile în care incidentele depășesc capacitatea de răspuns a gestionarului sau produc efecte sistemice. | **Nu se acceptă.** În urma corectării numerotării anexei nr. 3, prevederea vizată se regăsește la pct. 23 subpct. 23.7. Completarea propusă nu este necesară, întrucât mecanismele de coordonare cu autoritățile competente din cadrul Sistemului național de management al crizelor, aplicabile în situațiile în care incidentele depășesc capacitatea de răspuns a gestionarului sau produc efecte sistemice ori intersectoriale, sunt deja reglementate distinct la pct. 24 subpct. 24.13–24.16 și la pct. 26 subpct. 26.9 din anexa nr. 3. Introducerea aceleiași prevederi și la pct. 23 subpct. 23.7 ar genera dublarea reglementării. |
| | | Completarea pct. 21.2 și pct. 21.10 cu prevederi privind criteriile de escaladare și notificare în cazul incidentelor cu impact asupra continuității funcțiilor vitale ale statului, în conformitate cu mecanismele naționale de management al crizelor. | **Nu se acceptă.** În urma corectării numerotării anexei nr. 3, prevederile vizate se regăsesc la pct. 24 subpct. 24.2 și 24.10. Completarea acestora nu este necesară, întrucât criteriile și nivelurile de escaladare a incidentelor, procedura de informare a Centrului Național de Management al Crizelor, mecanismele de activare a coordonării |

| | | | |
|---|---|---|---|
| | | | interinstituționale și integrarea măsurilor de răspuns în mecanismele naționale de management al crizelor sunt deja prevăzute distinct la pct. 24 subpct. 24.13–24.16. Introducerea acelorași prevederi la subpct. 24.2 și 24.10 ar genera dublarea reglementării. |
| | | Completarea pct. 23.8 cu prevederi referitoare la procedurile de activare a mecanismelor de coordonare interinstituțională în cazul situațiilor de criză. | **Nu se acceptă.** În urma corectării numerotării anexei nr. 3, prevederea vizată se regăsește la pct. 26 subpct. 26.8, care reglementează procedurile de escaladare decizională în situații de perturbare sau incident. Completarea propusă nu este necesară, întrucât mecanismele de activare a coordonării interinstituționale în cadrul Sistemului național de management al crizelor sunt deja prevăzute distinct la pct. 24 subpct. 24.15, iar mecanismele de cooperare și coordonare cu Centrul Național de Management al Crizelor și cu alte autorități competente sunt reglementate la pct. 26 subpct. 26.9. Introducerea acelorași prevederi la subpct. 26.8 ar genera dublarea reglementării. |
| | | Completarea pct. 24.7 prin includerea obligativității corelării comunicării de criză cu mecanismele naționale de comunicare în situații de criză, pentru asigurarea unui mesaj instituțional unitar. | **Se acceptă.** În urma corectării numerotării anexei nr. 3, prevederea vizată se regăsește la pct. 27 subpct. 27.7. Subpunctul se completează prin introducerea obligației de corelare a comunicării de criză cu mecanismele naționale de comunicare în situații de |

| | | | |
|---|---|---|---|
| | | | criză, în vederea asigurării unui mesaj instituțional coerent și unitar. |
| | | Completarea pct. 26 astfel încât exercițiile să includă scenarii de criză cu caracter intersectorial și să permită testarea cooperării dintre gestionarii infrastructurilor critice și autoritățile competente din cadrul Sistemului național de management al crizelor. | **Se acceptă.** În urma corectării numerotării anexei nr. 3, prevederea vizată se regăsește la pct. 29 din Secțiunea 13 „Instruire, testare și exerciții". Pct. 29 a fost completat prin includerea, după caz, a scenariilor de criză cu caracter intersectorial și a modalității de testare a cooperării și coordonării dintre gestionarul infrastructurii critice naționale, alți gestionari relevanți și autoritățile competente din cadrul Sistemului național de management al crizelor.<br>În acest sens, subpct. 29.5 a fost expus în următoarea redacție:<br>**„29.5. scenariile de testare relevante, inclusiv, după caz, scenarii de criză cu caracter intersectorial;"**<br>Totodată, a fost introdus subpct. 29.9 cu următorul cuprins:<br>**„29.9. modalitatea de testare a cooperării și coordonării dintre gestionarul infrastructurii critice naționale, alți gestionari relevanți și autoritățile competente din cadrul Sistemului național de management al crizelor."** |
| | | Referitor la proiectul Normelor metodologice privind echivalarea documentelor existente cu Planul de securitate al gestionarului infrastructurii critice naționale (Anexa | **Se acceptă.**<br>Se introduce un subpunct nou: |

| | | | |
|---|---|---|---|
| | | nr. 4), în vederea asigurării unei abordări integrate cu Sistemul național de management al crizelor, se propune:<br><br>Completarea pct. 14 cu cerința ca documentele propuse spre echivalare să demonstreze, după caz, modul de asigurare a continuității funcțiilor vitale ale statului și mecanismele de coordonare în situații de criză. | „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;” |
| | | Completarea pct. 31 cu un criteriu suplimentar de evaluare privind verificarea compatibilității documentelor propuse spre echivalare cu mecanismele naționale de management al crizelor și cu procedurile de cooperare interinstituțională aplicabile. | **Se acceptă.** Pct. 31 din anexa nr. 4 a fost completat cu un criteriu suplimentar de evaluare privind verificarea compatibilității documentului sau setului de documente propuse spre echivalare cu mecanismele naționale de management al crizelor și cu procedurile de cooperare interinstituțională aplicabile, după caz. |
| | | Completarea pct. 57 prin includerea unui caz suplimentar de încetare a valabilității echivalării atunci când intervin modificări semnificative ale cadrului normativ național în domeniul managementului crizelor, rezilienței sau protecției infrastructurilor critice, care impun revizuirea documentelor recunoscute ca echivalente. | **Se acceptă.** Pct. 57 din anexa nr. 4 a fost completat cu un caz suplimentar de încetare a valabilității echivalării, aplicabil atunci când intervin modificări semnificative ale cadrului normativ național în domeniul managementului crizelor, rezilienței sau protecției infrastructurilor critice, iar documentele recunoscute ca echivalente nu mai corespund cerințelor aplicabile și necesită revizuire. |
| | | Completarea pct. 69 cu prevederea că documentele recunoscute ca echivalente trebuie să asigure nu doar același nivel de protecție, continuitate, răspuns și recuperare, ci și compatibilitatea cu mecanismele naționale de coordonare și gestionare a crizelor. | **Nu se acceptă.** Completarea pct. 69 nu este necesară, întrucât compatibilitatea documentelor recunoscute ca echivalente cu mecanismele naționale de coordonare și gestionare a crizelor |

| | | | |
|---|---|---|---|
| | | | este deja verificată în cadrul condițiilor minime de echivalare și al criteriilor de examinare prevăzute la pct. 14 și pct. 31 din anexa nr. 4. Totodată, pct. 69 stabilește cerința generală privind atingerea aceluiași nivel funcțional de protecție, continuitate, răspuns, recuperare și reziliență ca Planul de securitate. Reiterarea aceleiași obligații la pct. 69 ar genera dublarea reglementării. |
| | | Referitor la proiectul Normelor metodologice privind revizuirea și actualizarea Planului de securitate al gestionarului infrastructurii critice naționale (Anexa nr. 5), în vederea consolidării coerenței cu Sistemul național de management al crizelor, se propun următoarele completări:<br><br>Completarea pct. 12 cu un temei suplimentar pentru revizuirea extraordinară a Planului de securitate, și anume declararea unei stări de criză sau modificarea nivelului de alertă la nivel național, atunci când aceasta poate afecta funcționarea infrastructurii critice naționale ori serviciul esențial furnizat. | **Se acceptă.** În urma corectării numerotării anexei nr. 5, temeiurile concrete pentru inițierea revizuirii extraordinare sunt prevăzute la pct. 13. Pct. 13 a fost completat cu un temei suplimentar privind declararea unei stări de criză sau modificarea nivelului de alertă la nivel național, atunci când aceasta afectează ori poate afecta funcționarea infrastructurii critice naționale sau continuitatea serviciului esențial furnizat.<br>Se introduce un subpunct nou:<br>**„**13.17. declararea unei stări de criză sau modificarea nivelului de alertă la nivel național, atunci când aceasta afectează ori poate afecta funcționarea infrastructurii critice naționale sau continuitatea serviciului esențial furnizat;” |

| | | | |
|---|---|---|---|
| | | Completarea pct. 19 și pct. 20 cu obligația evaluării impactului modificărilor asupra continuității funcțiilor vitale ale statului și asupra efectelor intersectoriale pe care le poate genera indisponibilizarea infrastructurii critice. | **Nu se acceptă.** În urma corectării numerotării anexei nr. 5, prevederile vizate se regăsesc la pct. 20 și pct. 21. Completarea propusă nu este necesară, întrucât revizuirea Planului de securitate include deja examinarea evaluării riscurilor, a scenariilor de risc, a dependențelor și interdependențelor, a măsurilor de continuitate, răspuns și recuperare, precum și verificarea capacității Planului de securitate de a asigura continuitatea serviciului esențial și recuperarea funcțiilor critice afectate. Impactul asupra funcțiilor vitale ale statului și efectele sistemice ori intersectoriale sunt evaluate în cadrul acestor elemente și al evaluării actualizate a riscurilor. Introducerea unor prevederi distincte la pct. 20 și pct. 21 ar genera dublarea reglementării. |
| | | Completarea pct. 32 astfel încât Nota de actualizare/revizuire să includă și concluziile rezultate din analiza lecțiilor identificate în urma gestionării incidentelor, situațiilor de criză și exercițiilor interinstituționale, precum și măsurile adoptate pentru implementarea acestora. | **Se acceptă.** În urma corectării numerotării anexei nr. 5, prevederea vizată se regăsește la pct. 33, care stabilește conținutul Notei de actualizare/revizuire. Pct. 33 a fost completat prin includerea concluziilor rezultate din analiza lecțiilor identificate în urma gestionării incidentelor, situațiilor de criză și exercițiilor interinstituționale, precum și a măsurilor stabilite pentru |

| | | | |
|---|---|---|---|
| | | | valorificarea și implementarea acestora.<br>Se introduc următoarele subpuncte:<br>**„**33.10. concluziile rezultate din analiza lecțiilor identificate în urma gestionării incidentelor, situațiilor de criză și exercițiilor interinstituționale, după caz;”<br>„33.11. măsurile stabilite pentru valorificarea și implementarea lecțiilor identificate, responsabilii și termenele aferente.” |
| | | Completarea pct. 36 cu prevederea că reavizarea Planului de securitate este necesară și în cazul modificării mecanismelor de cooperare și coordonare cu autoritățile competente din cadrul Sistemului național de management al crizelor. | **Se acceptă.** În urma corectării numerotării anexei nr. 5, prevederea vizată se regăsește la pct. 37, care stabilește cazurile în care Planul de securitate actualizat se transmite spre reavizare. Pct. 37 a fost completat prin includerea modificării mecanismelor de cooperare și coordonare cu autoritățile competente din cadrul Sistemului național de management al crizelor printre situațiile care impun reavizarea Planului de securitate.<br>Se introduce un subpunct nou:<br>„37.11. mecanismele de cooperare și coordonare cu autoritățile competente din cadrul Sistemului național de management al crizelor.” |
| | | Completarea pct. 54 cu mențiunea că procesul de revizuire și actualizare trebuie să contribuie la consolidarea rezilienței naționale și la asigurarea continuității funcțiilor | **Se acceptă.** În urma corectării numerotării anexei nr. 5, prevederea vizată se regăsește la pct. 55. Pct. 55 a |

| | | | |
|---|---|---|---|
| | | vitale ale statului, în conformitate cu cadrul normativ în domeniul managementului crizelor. | fost completat prin precizarea că revizuirea și actualizarea Planului de securitate trebuie să contribuie la consolidarea rezilienței naționale și la asigurarea continuității funcțiilor vitale ale statului, în conformitate cu cadrul normativ aplicabil în domeniul managementului crizelor. |
| | | Referitor la proiectul Normelor metodologice privind desemnarea, statutul funcțional și atribuțiile ofițerului de legătură pentru securitatea infrastructurii critice naționale (Anexa<br>nr. 6), se propune:<br>Cu referire la delimitarea atribuțiilor operaționale ale ofițerului de legătură, proiectul atribuie ofițerului de legătură un rol extins de coordonare operațională (pct. 2, pct. 18.3 și pct. 20.1), fără a delimita suficient competențele acestuia de atribuțiile conducerii gestionarului și ale structurilor responsabile de securitate, management al riscurilor și continuitatea activității. Se propune precizarea expresă că atribuțiile de coordonare exercitate de ofițerul de legătură au caracter tehnic și de coordonare administrativă, fără a implica competențe de conducere operațională sau decizională, acestea revenind exclusiv conducerii gestionarului și structurilor competente. | **Se acceptă parțial.** Pct. 17 din anexa nr. 6 a fost completat pentru a preciza expres că atribuțiile ofițerului de legătură nu conferă competențe de conducere operațională sau decizională, acestea revenind conducerii gestionarului și structurilor interne competente, potrivit atribuțiilor legale și interne.<br>Nu se acceptă modificarea pct. 2, subpct. 18.3 și subpct. 20.1, întrucât formulările privind coordonarea operațională descriu rolul funcțional al ofițerului de legătură în organizarea comunicării, corelarea activităților și facilitarea cooperării dintre structurile implicate, fără a-i atribui competențe de comandă sau decizie. Această delimitare rezultă deja din pct. 3 și este consolidată prin completarea pct. 17. Modificarea tuturor prevederilor menționate ar restrânge nejustificat rolul funcțional al ofițerului de legătură și ar crea riscul unei interpretări excesiv de administrative a atribuțiilor sale. |

| | | | |
|---|---|---|---|
| | | | |
| | | Corelarea cu mecanismele naționale de management al crizelor. În cuprinsul proiectului sunt prevăzute atribuții privind comunicarea și schimbul de informații cu autoritățile competente, însă nu este reglementată expres corelarea acestora cu mecanismele naționale de management al crizelor instituite potrivit legislației. Se propune completarea normelor cu prevederea că activitatea ofițerului de legătură privind notificarea, schimbul de informații și cooperarea operațională se realizează fără a aduce atingere mecanismelor de coordonare și raportare prevăzute de cadrul normativ privind managementul crizelor și continuitatea guvernării. | **Se acceptă.** Anexa nr. 6 a fost completată cu o prevedere distinctă prin care se precizează că activitățile ofițerului de legătură privind notificarea, schimbul de informații și cooperarea operațională se desfășoară cu respectarea mecanismelor naționale de coordonare, comunicare și raportare stabilite de cadrul normativ în domeniul managementului crizelor și al continuității guvernării.<br>În capitolul XIII „Reguli comune de aplicare și corelare metodologică” se introduce următorul punct:<br>**„**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.” |
| | | Clarificarea responsabilităților privind raportarea incidentelor. La pct. 22.4 este prevăzut că ofițerul de legătură contribuie la raportarea incidentelor, perturbărilor și vulnerabilităților. Pentru evitarea unor interpretări diferite, se recomandă precizarea că raportarea se realizează în limitele competențelor gestionarului și potrivit procedurilor normative aplicabile, fără instituirea unui mecanism paralel de notificare. | **Se acceptă.** Subpct. 22.4 din anexa nr. 6 a fost completat pentru a preciza că participarea ofițerului de legătură la raportarea incidentelor, perturbărilor, vulnerabilităților sau modificărilor relevante se realizează în limitele competențelor gestionarului și potrivit |

| | | | |
|---|---|---|---|
| | | | procedurilor prevăzute de cadrul normativ aplicabil, fără instituirea unui mecanism paralel de notificare. |
| | | Uniformizarea terminologiei. În cuprinsul proiectului sunt utilizate alternativ noțiunile: „coordonează”; „sprijină”; „facilitează”; „contribuie”. Se recomandă utilizarea consecventă a<br>acestor termeni, astfel încât nivelul responsabilităților atribuite ofițerului de legătură să fie clar<br>diferențiat și să nu creeze suprapuneri cu atribuțiile altor structuri interne. | **Se acceptă.** Terminologia utilizată în anexa nr. 6 a fost revizuită și uniformizată, astfel încât termenii „coordonează”, „sprijină”, „facilitează” și „contribuie” să reflecte în mod consecvent nivelul distinct al responsabilităților atribuite ofițerului de legătură și să nu genereze suprapuneri cu atribuțiile conducerii gestionarului sau ale structurilor interne competente.<br>În acest sens, termenul **„coordonează”** se utilizează exclusiv pentru activitățile în care ofițerul de legătură are un rol expres de organizare și corelare, în limitele mandatului acordat, iar termenii **„sprijină”**, **„facilitează”** și **„contribuie”** se utilizează pentru activitățile de suport, intermediere și participare, fără competențe de conducere operațională sau decizională. |
| | | Completarea cerințelor privind pregătirea profesională. La Capitolul VIII se stabilesc cerințele minime pentru desemnarea ofițerului de legătură. Se propune completarea acestora cu obligația participării periodice la programe de instruire privind: managementul riscurilor;<br>managementul situațiilor de criză; cooperarea interinstituțională; protecția infrastructurilor critice,<br>în vederea menținerii competențelor necesare exercitării atribuțiilor. | **Se acceptă.** Capitolul VIII din anexa nr. 6 a fost completat prin instituirea obligației gestionarului de a asigura participarea periodică a ofițerului de legătură la programe de instruire relevante pentru exercitarea atribuțiilor, inclusiv în domeniul managementului riscurilor, |

| | | | |
|---|---|---|---|
| | | | managementului situațiilor de criză, cooperării interinstituționale și protecției infrastructurilor critice naționale.<br>Se introduce un punct nou, după pct. 26:<br>„27. Gestionarul infrastructurii critice naționale asigură participarea periodică a ofițerului de legătură la programe de instruire, perfecționare sau exerciții relevante, inclusiv în domeniul managementului riscurilor, managementului situațiilor de criză, cooperării interinstituționale și protecției infrastructurilor critice naționale, în vederea menținerii și dezvoltării competențelor necesare exercitării atribuțiilor.” |
| | | Evidența și actualizarea datelor. Pct. 39–43 reglementează evidența ofițerilor de legătură. Se recomandă stabilirea expresă a obligației verificării periodice a actualității datelor de contact și a funcțiilor persoanelor desemnate, pentru asigurarea funcționalității mecanismelor de notificare și coordonare în situații de criză. | **Se acceptă.** Capitolul XII din anexa nr. 6 a fost completat prin instituirea obligației de verificare periodică a actualității datelor de contact, a funcțiilor și a statutului persoanelor desemnate ca ofițeri de legătură și înlocuitori, în vederea asigurării funcționalității mecanismelor de notificare, comunicare și coordonare, inclusiv în situații de criză.<br>Se introduce un punct nou după pct. 44:<br>„45. Gestionarul infrastructurii critice naționale și autoritatea publică responsabilă verifică periodic, cel puțin o dată pe an, actualitatea datelor de contact, a funcțiilor și a statutului |

| | | | |
|---|---|---|---|
| | | | 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.” |
| **Ministerul Energiei (aviz nr. . 05-1761 din 03.07.2026)** | 3 | Revizuirea pct. 42 din anexa nr. 2, astfel încât formatul și modalitatea de transmitere a Planului de securitate și a documentelor aferente să fie stabilite unitar la nivel național, prin cerințe tehnice și formate standardizate, pentru a asigura interoperabilitatea și a evita soluțiile neuniforme. | **Se acceptă.** Pct. 43 din anexa nr. 2 se reformulează în vederea asigurării unei abordări unitare la nivel național privind formatul și modalitatea de transmitere a Planului de securitate și a documentelor aferente.<br><br>Pct. 43 va avea următorul cuprins:<br><br>„43. Planul de securitate și documentele aferente se transmit în formatul și prin mijloacele stabilite potrivit cerințelor tehnice și modelelor standardizate aprobate de Centrul Național de Coordonare a Protecției Infrastructurilor Critice. 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..” |

| | | | |
|---|---|---|---|
| | | Clarificarea în proiect și în Nota de fundamentare a sintagmelor „mecanisme de comunicare” și „mecanisme de schimb de informații”, inclusiv prin precizarea dacă acestea presupun proceduri interne, canale de comunicare, sisteme informaționale, platforme electronice, protocoale ori alte instrumente organizatorice și tehnice.<br><br>Completarea Notei de fundamentare cu evaluarea impactului financiar aferent implementării și menținerii mecanismelor de comunicare și schimb de informații, întrucât Ministerul Energiei nu dispune, la etapa actuală, de resurse financiare prevăzute pentru crearea și menținerea acestora. | **Se acceptă.** Nota de fundamentare se va completa cu precizarea că aplicarea prevederilor proiectului, în forma actuală, nu generează în mod direct cheltuieli obligatorii pentru crearea unor platforme sau sisteme informaționale noi, iar eventualele costuri suplimentare vor depinde de soluțiile tehnice adoptate ulterior de autoritățile competente.<br><br>În Nota de fundamentare s-a introdus următorul alineat:<br><br>„Mecanismele de comunicare și schimb de informații prevăzute de proiect reprezintă ansamblul procedurilor, responsabilităților, fluxurilor de notificare, canalelor și mijloacelor organizatorice sau tehnice utilizate pentru transmiterea, recepționarea, confirmarea și protejarea informațiilor relevante. Implementarea acestora se va realiza, la etapa inițială, prin utilizarea resurselor, canalelor de comunicare și sistemelor informaționale existente. Proiectul nu instituie obligația creării unor platforme sau sisteme informaționale noi. Eventuala dezvoltare a unor soluții tehnice suplimentare va fi realizată în baza unor decizii distincte, cu evaluarea |

| | | | |
|---|---|---|---|
| | | | impactului financiar și identificarea surselor de finanțare.” |
| | | Revizuirea termenului de 6 luni prevăzut la pct. 7 din proiectul hotărârii pentru aducerea actelor normative departamentale, procedurilor interne și documentelor aplicabile în concordanță cu noul cadru metodologic, astfel încât termenul să fie corelat cu volumul de lucru și capacitățile reale ale autorităților. Completarea Notei de fundamentare cu o analiză detaliată a impactului administrativ și financiar asupra autorităților publice responsabile, inclusiv sub aspectul resurselor umane, financiare și tehnice necesare implementării noilor obligații. | **Se acceptă.** Termenul de 6 luni prevăzut la pct. 9 nu este stabilit expres de Legea nr. 223/2025 pentru aducerea actelor normative departamentale, procedurilor interne și documentelor aplicabile în concordanță cu cadrul metodologic aprobat. Având în vedere volumul și complexitatea activităților necesare, termenul a fost extins la 12 luni de la data intrării în vigoare a hotărârii. |
| | | Completarea Notei de fundamentare cu o analiză detaliată a impactului administrativ și financiar asupra autorităților publice responsabile, inclusiv sub aspectul resurselor umane, financiare și tehnice necesare implementării noilor obligații. | **Nu se acceptă.** Proiectul nu instituie în mod direct obligația creării unor structuri noi, sisteme informaționale, platforme tehnice sau mecanisme care să genereze cheltuieli obligatorii suplimentare. Implementarea cadrului metodologic urmează a fi realizată de autoritățile publice responsabile în limitele competențelor și ale resurselor umane, financiare și tehnice existente.<br><br>O analiză financiară detaliată și cuantificată nu poate fi realizată la această etapă, întrucât necesarul efectiv de resurse va depinde de numărul infrastructurilor critice naționale desemnate, specificul fiecărui sector, documentele și capacitățile deja existente, precum și de soluțiile |

| | | | |
|---|---|---|---|
| | | | concrete de implementare adoptate ulterior. Eventualele necesități suplimentare de resurse vor fi evaluate și fundamentate separat, în cadrul procedurilor bugetare și normative aplicabile. |
| **Ministerul Apărării (aviz nr. 11-1005 din 29.06.2026)** | 4 | Pentru infrastructura militară administrată de Ministerul Apărării, aplicarea cadrului metodologic să se realizeze cu respectarea legislației speciale din domeniul apărării naționale, secretului de stat, regimului armamentului și munițiilor, precum și a dispozitivelor militare.<br><br>În cazul Aeroportului Internațional Liber „Mărculești”, evaluarea riscurilor și actualizarea Planului de securitate să fie realizate de administratorul aeroportului — Ministerul Infrastructurii și Dezvoltării Regionale — în coordonare cu Ministerul Apărării și autoritatea competentă în domeniul aeronauticii civile.<br><br>Pentru infrastructura sistemului național de apărare administrată de alte autorități publice, evaluarea riscurilor și măsurile de securitate să fie realizate de autoritățile publice responsabile pentru sectorul sau subsectorul respectiv, în coordonare cu Ministerul Apărării.<br><br>Completarea capitolului I „Dispoziții generale” din anexa nr. 1 cu o normă expresă referitoare la infrastructura militară și infrastructura sistemului național de apărare, cu următorul conținut:<br><br>„În cazul infrastructurii militare aflate în administrarea Ministerului Apărării și al infrastructurii sistemului național de apărare aflate în administrarea altor autorități publice responsabile sectoriale, aplicarea prevederilor hotărârii se realizează cu respectarea Legii nr. 345/2003 cu privire la apărarea națională, Legii nr. 245/2008 cu privire la secretul de stat, Legii nr. 178/2008 cu privire la Aeroportul Internațional Liber «Mărculești» și Legii nr. 147/2017 privind regimul armamentului și munițiilor | **Nu se acceptă.** Proiectul hotărârii Guvernului stabilește un cadru metodologic general, aplicabil tuturor sectoarelor și gestionarilor infrastructurilor critice naționale, fără a aduce atingere normelor speciale aplicabile domeniului apărării naționale, regimului informațiilor atribuite la secret de stat, regimului armamentului și munițiilor, precum și altor domenii incidente.<br><br>Prevederile proiectului nu contravin aspectelor expuse în avizul Ministerului Apărării, acestea urmând a fi aplicate în coroborare cu actele normative speciale și în limitele competențelor legale ale autorităților implicate. Totodată, proiectul conține deja norme generale privind aplicarea cerințelor speciale și protecția informațiilor atribuite la secret de stat.<br><br>În aceste condiții, introducerea unei norme distincte, aplicabile exclusiv infrastructurii militare și infrastructurii |

| | | | |
|---|---|---|---|
| | | convenționale, al mijloacelor speciale și dispozitivelor militare deținute de Armata Națională și de forțele militare străine aflate legal pe teritoriul Republicii Moldova.” | sistemului național de apărare, nu este necesară. |
| **Ministerul Dezvoltării Economice și Digitalizării (aviz nr. 03-2371 din 13.07.2026)** | 5 | Se propune reexaminarea pct. 3 și pct. 6 din proiect, prin prisma principiului delimitării funcțiilor de elaborare și promovare a politicilor publice de funcțiile de implementare, supraveghere și control.<br><br>Ministerul Dezvoltării Economice și Digitalizării consideră că atribuțiile privind avizarea Planurilor de securitate ale gestionarilor infrastructurilor critice naționale, monitorizarea conformării acestora cu cerințele legale și metodologice, precum și elaborarea instrucțiunilor sectoriale, ghidurilor, modelelor de documente și procedurilor interne au un caracter preponderent operațional și nu corespund rolului ministerelor în calitate de organe centrale de specialitate responsabile de elaborarea politicilor publice.<br><br>Totodată, se menționează că exercitarea acestor atribuții necesită resurse umane și financiare suplimentare, precum și expertiză tehnică specializată, de care ministerele nu dispun în prezent. În opinia autorului avizului, funcțiile de monitorizare, supraveghere și implementare ar trebui exercitate de autoritățile administrative și instituțiile publice specializate, potrivit competențelor acestora | **Nu se acceptă.** Atribuțiile prevăzute la pct. 4 și pct. 7 din proiect nu reprezintă atribuții noi instituite prin proiectul hotărârii, ci concretizează responsabilitățile care decurg din Legea nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale și din Hotărârea Guvernului nr. 185/2026 privind desemnarea autorităților publice responsabile de sectoarele și subsectoarele infrastructurii critice naționale.<br><br>Avizarea Planurilor de securitate, coordonarea sectorială și monitorizarea conformării gestionarilor cu cerințele legale și metodologice constituie componente indispensabile exercitării rolului de autoritate publică responsabilă. Monitorizarea prevăzută de proiect are caracter metodologic și sectorial și nu echivalează cu exercitarea unor funcții de control sau supraveghere specifice autorităților de reglementare ori organelor de control.<br><br>Totodată, elaborarea instrucțiunilor sectoriale, a ghidurilor, a modelelor de documente și a procedurilor necesare |

| | | | |
|---|---|---|---|
| | | | aplicării cadrului metodologic reprezintă o activitate de concretizare și aplicare unitară a politicilor sectoriale. Autoritățile publice responsabile pot realiza aceste atribuții cu implicarea autorităților administrative, instituțiilor publice și structurilor specializate din domeniul lor de competență, fără a substitui atribuțiile legale ale autorităților de reglementare, supraveghere sau control.<br><br>Prin urmare, prevederile pct. 4 și pct. 7 nu contravin principiului delimitării funcțiilor de elaborare și promovare a politicilor publice de funcțiile de implementare, consacrat de Legea nr. 98/2012. |
| **Ministerul Mediului (aviz nr.13-05/2213 din 06.07.2026)** | 6 | Completarea pct. 8 din anexa nr. 1 cu referire expresă la **legislația din domeniul protecției mediului** și la **prevenirea și controlul riscurilor de mediu**, având în vedere că evaluarea riscurilor include impactul asupra mediului, prevăzut la pct. 35.4 din aceeași anexă | **Se acceptă.** Pct. 8 din anexa nr. 1 se completează prin includerea expresă a legislației din domeniul protecției mediului și al prevenirii și controlului riscurilor de mediu, în vederea corelării cu prevederile privind evaluarea impactului asupra mediului. |
| **Ministerul Educației și Cercetării (aviz nr. 06/897/26 din 03.07.2026)** | 7 | Ministerul Educației și Cercetării avizează pozitiv proiectul, fără a formula propuneri sau obiecții. | |
| **Agenția Națională pentru Cercetare și Dezvoltare** | 8 | Instituția a avizat pozitiv proiectul, fără obiecții și propuneri. | |

| | | | |
|---|---|---|---|
| **Ministerul Infrastructurii și Dezvoltării Regionale (aviz nr. nr. 04-3893 din 09.07.2026 )** | 9 | Completarea anexei nr. 4 la proiect prin includerea expresă a **planurilor de localizare și lichidare a situațiilor de avarie** în lista documentelor propuse spre echivalare, în calitate de documente conexe. | Se acceptă. La pct. 8 din anexa nr. 4 a fost introdus subpct. **8.8**, cu următorul cuprins:<br>„8.8. planurile de localizare și lichidare a situațiilor de avarie, elaborate potrivit legislației din domeniul securității industriale.” |
| | | În structura-cadru a Planului de securitate, procedurile de răspuns în caz de incident sau avarie în domeniul securității industriale să fie prevăzute cu caracter opțional, pentru a evita dublarea responsabilităților personalului operativ. | **Se acceptă parțial.** Nu se acceptă atribuirea caracterului opțional procedurilor de răspuns la incidente sau avarii, întrucât acestea reprezintă un element esențial al Planului de securitate.<br><br>Pentru evitarea dublării măsurilor, responsabilităților și procedurilor deja stabilite prin legislația specială aplicabilă, capitolul I „Dispoziții generale” din anexa nr. 3 a fost completat cu pct. 6 și 7, care prevăd integrarea, anexarea sau indicarea prin trimitere expresă a procedurilor, planurilor ori altor documente existente, precum și includerea în Planul de securitate doar a elementelor suplimentare necesare pentru protecția, continuitatea și reziliența infrastructurii critice naționale.<br><br>Totodată, precizarea nu este limitată exclusiv la legislația din domeniul securității industriale. Hotărârea Guvernului are caracter general și se |

| | | | |
|---|---|---|---|
| | | | aplică tuturor sectoarelor și gestionarilor infrastructurilor critice naționale, motiv pentru care soluția a fost formulată în raport cu orice legislație specială aplicabilă. Legislația privind securitatea industrială reprezintă doar unul dintre domeniile în care asemenea documente și proceduri pot exista deja. |
| | | Evaluarea riscurilor industriale aferente infrastructurii critice naționale să nu instituie indicatori sau cerințe paralele ori contradictorii cu normele din domeniul securității industriale, a căror respectare este supusă controlului Inspectoratului Național pentru Supraveghere Tehnică | **S-a luat act.** Observația este deja reflectată la pct. 9 din anexa nr. 1, care prevede aplicarea cerințelor suplimentare ori mai stricte stabilite prin legislația specială aplicabilă sectorului sau subsectorului respectiv. Prin urmare, evaluarea riscurilor la adresa infrastructurilor critice naționale se realizează în corelare cu normele speciale incidente și nu substituie cerințele din domeniul securității industriale sau competențele de control ale Inspectoratului Național pentru Supraveghere Tehnică. Nu sunt necesare modificări suplimentare ale proiectului. |
| **Autoritatea Aeronautică Civilă (aviz nr. nr. 2411 din 07.07.2026)** | 10 | Comunică lipsa obiecțiilor și/sau propunerilor asupra proiectulu | |
| **Agenția Feroviară (aviz nr. nr. 01-146 din 30.06.2026)** | 11 | Comunică lipsa propunerilor de modificare sau completare a proiectulu | |

| | | | |
|---|---|---|---|
| **Ministerul Sănătății (aviz nr 09/2477 din 10 iulie 2026** | 12 | Comunică lipsa de propuneri și obiecții la proiect. | |
| **Agenția Națională pentru Sănătate Publică (aviz nr. nr. 01-1-3450 din 23.06.2026.)** | 13 | Comunică lipsa obiecțiilor și acordă aviz pozitiv asupra proiectului. | |
| **Agenția Națională pentru Siguranța Alimentelor (aviz nr. 15-3618 din 30.06.2026)** | 14 | Comunică lipsa de propuneri și obiecții la proiect. | |
| **Agenția Medicamentului și Dispozitivelor Medicale (aviz nr.** nr. Rg02-3134 din 24.06.2026 **)** | 15 | Comunică lipsa de propuneri și obiecții asupra proiectului. | |
| **Agenția Națională pentru Reglementare în Comunicații (aviz nr. 01-DRA/1315 din 08.07.2026)** | 16 | Agenția avizează pozitiv proiectul, fără propuneri și observații, și susține promovarea acestuia. | |
| **Banca Națională a Moldovei (aviz nr. 31-002/113/3631 din 07.07.2026; aviz nr. 31-002/101/3386 din 30.06.2026)** | 17 | BNM solicită precizarea modului de exercitare a obligațiilor prevăzute la pct. 3 și 6 din proiect în situația în care pentru același sector sau subsector sunt desemnate două ori mai multe autorități publice responsabile, inclusiv dacă aceste obligații se exercită în comun sau individual de către fiecare autoritate. | **Se acceptă.** În vederea clarificării modului de exercitare a obligațiilor în cazul desemnării mai multor autorități publice responsabile pentru același sector sau subsector, proiectul hotărârii se completează cu pct. 8, cu următorul cuprins: |

| | | | |
|---|---|---|---|
| | | | „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, ghidurilor, modelelor de documente sau procedurilor necesare aplicării prezentei hotărâri, cu informarea Centrului Național de Coordonare a Protecției Infrastructurilor Critice.” |
| | | Cu referire la periodicitatea actualizării evaluării riscurilor de către gestionarul infrastructurii critice naționale, considerăm necesară corelarea acestui exercițiu cu periodicitatea anuală prevăzută la art. 6 alin. (2) și (3) din Legea nr. 223/2025, stabilită pentru elaborarea, de către autoritățile publice responsabile împreună cu gestionarii infrastructurilor critice naționale, a rapoartelor de evaluare privind riscurile și incidentele semnificative, precum și privind evoluția amenințărilor și existența unor vulnerabilități în sectoarele și subsectoarele infrastructurii critice naționale (evaluări sectoriale). Subsecvent, având în vedere că evaluările sectoriale se transmit Centrului Național de Coordonare a Protecției Infrastructurilor Critice până la data de 15 ianuarie a anului următor, în vederea elaborării raportului anual privind stadiul de protecție a infrastructurilor critice la nivel național, se impune ca evaluările instituționale ale riscurilor să fie actualizate într-un termen care să permită valorificarea rezultatelor acestora în cadrul evaluărilor sectoriale și, implicit, în procesul de elaborare a | **Se acceptă.** Propunerea este justificată, întrucât pct. 62 din anexa nr. 1 prevede actualizarea periodică a evaluării riscurilor, fără a stabili expres periodicitatea minimă. În vederea corelării cu raportarea anuală prevăzută la art. 6 alin. (2) și (3) din Legea nr. 223/2025, pct. 63 va fi completat cu mențiunea că evaluarea riscurilor se actualizează cel puțin o dată pe an, într-un termen care să permită valorificarea rezultatelor acesteia la elaborarea rapoartelor sectoriale și a raportului |

| | | | |
|---|---|---|---|
| | | rapoartelor anuale. În caz contrar, există riscul ca analiza inclusă în respectivele rapoarte să nu reflecte situația actuală a riscurilor și vulnerabilităților identificate. | anual privind stadiul protecției infrastructurilor critice naționale. Pct. 63 va avea următorul conținut: „63. 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, precum și ori de câte ori intervin schimbări semnificative privind infrastructura critică națională, serviciul esențial, mediul de risc, dependențele, interdependențele ori vulnerabilitățile relevante.” |
| | | Cu referire la anexa nr. 1<br>La pct. 2, propunem substituirea sintagmei „identificate, analizate, apreciate și prioritizate” cu sintagma „identificate, analizate, evaluate, prioritizate, monitorizate și raportate”, întrucât, în conformitate cu principiile și cerințele prevăzute de standardele ISO 31000 și COSO ERM, managementul riscurilor reprezintă un proces continuu, care nu se limitează la identificarea și evaluarea riscurilor, ci include și monitorizarea permanentă a evoluției acestora, precum și raportarea informațiilor relevante către factorii decizionali. Completarea propusă asigură o abordare integrată a gestionării riscurilor la adresa infrastructurilor critice naționale. | **Se acceptă.** Modificările au fost operate. |
| | | La pct. 8, propunem revizuirea sintagmei „legislație sectorială” în vederea asigurării cerințelor de claritate și previzibilitate prevăzute în art. 3 din Legea nr. 100/2017 cu privire la actele normative (cadrul normativ național nu diferențiază categoria de act legislativ sectorial). | **Se acceptă.** În vederea asigurării clarității și previzibilității normei, precum și pentru evitarea utilizării unei sintagme care nu este definită distinct de cadrul normativ național, la pct. 8 sintagma „legislația sectorială” se substituie cu sintagma „legislația |

| | | | |
|---|---|---|---|
| | | | specială aplicabilă sectorului sau subsectorului respectiv”. |
| | | La pct. 9, atenționăm că redacția prevederii pare să contravină normei de la art. 5 alin. (4)-(5) din Legea nr. 100/2017 care reglementează expres aplicarea normei speciale în caz de divergență între o normă generală și o normă specială. Propunem revizuirea pct. 9 în acest sens. | **Se acceptă.** În vederea corelării cu art. 5 alin. (3) și (4) din Legea nr. 100/2017 cu privire la actele normative și pentru evitarea unei interpretări potrivit căreia prezentele Norme metodologice ar prevala asupra normelor speciale sau derogatorii de același nivel, pct. 9 va fi reformulat: „ Cerințele suplimentare ori mai stricte privind evaluarea riscurilor, stabilite prin norme speciale sau derogatorii aplicabile sectorului ori subsectorului respectiv, se aplică în condițiile art. 5 alin. (3) și (4) din Legea nr. 100/2017 cu privire la actele normative |
| | | La pct. 12, propunem:<br>a) completarea cu o noțiune nouă cu următorul cuprins: „Riscul inerent este riscul care survine în absența oricăror acțiuni directe sau specifice pentru a-i modifica severitatea”.<br><br>b) revizuirea definiției de „risc” luând în considerare standardul COSO (Committee of Sponsoring Organizations of the Treadway Commission) pentru definirea riscului. În acest context, propunem următoarea redacție: „risc – posibilitatea producerii unui eveniment, incident, perturbări sau situații care poate afecta obiectivele de securitate, funcționalitate, integritate, disponibilitate sau continuitate a infrastructurii critice naționale ori a serviciului esențial furnizat”.<br>c) revizuirea definiției de „probabilitate” în conformitate cu standardul ISO31000 și COSO. În acest context, propunem următoarea redacție: „probabilitate - este eventualitatea producerii unui risc, care poate fi definită, determinată sau măsurată în mod obiectiv sau subiectiv și poate fi exprimată calitativ sau cantitativ (numeric), în termeni de posibilitate sau frecvență”. | **S-a luat act.** Pct. 12 la care se referă propunerea a fost exclus din proiect în urma avizării prealabile. Prin urmare, propunerile privind completarea și revizuirea noțiunilor „risc inerent”, „risc”, „probabilitate” și „măsuri de tratare a riscului” nu mai sunt aplicabile redacției actuale a proiectului. |

| | | | |
|---|---|---|---|
| | | d) precizarea dacă definiția de „măsuri de tratare a riscului” se referă la măsurile existente sau și la măsurile suplimentare propuse, astfel cum este reglementat la definiția de „fișă de evaluare a riscului”. | |
| | | La pct. 15, propunem excluderea cuvântului „sectoriale”, opinăm în acest sens că, norma reglementează clar că autoritatea publică responsabilă poate stabili cerințe suplimentare privind evaluarea riscurilor. | **Se acceptă.** În urma avizării prealabile, prevederea de la pct. 15 a fost renumerotată și se regăsește la pct. 13 din proiect. Pentru evitarea redundanței și asigurarea clarității normei, cuvântul „sectoriale” se exclude. |

| | | | |
|---|---|---|---|
| | | La pct. 23, întru asigurarea concordanței cu definiția „evaluării riscurilor” prevăzută la pct. 2, propunem completarea și revizuirea etapelor procesului de evaluare a riscurilor, inclusiv prin reflectarea propunerilor formulate în aviz la pct. 2. Totodată, se consideră necesară reconsiderarea structurii etapelor prevăzute la lit. a)–e), întrucât acestea nu reprezintă etape distincte ale procesului de evaluare a riscurilor, ci elemente și criterii de analiză utilizate în cadrul identificării și analizei riscurilor, care stau la baza estimării impactului și probabilității și, ulterior, a determinării nivelului de risc.<br><br>Suplimentar, la pct. 23, propunem:<br>a) la lit. i), după cuvântul „risc”, completarea cu cuvintele „inerent și rezidual”.<br>b) la lit. j), după cuvintele „prioritizarea riscurilor”, completarea cu cuvintele „ținând cont de nivelul riscului rezidual”.<br>c) la lit. k), după cuvântul „riscurilor”, completarea cu cuvintele „existente și celor suplimentare”. | **Se acceptă parțial.** În urma avizării prealabile, prevederea de la pct. 23 a fost renumerotată și se regăsește la pct. 21 din proiect.<br><br>Propunerea privind reconsiderarea subpct. 21.1–21.5 nu se acceptă, întrucât delimitarea obiectului evaluării, identificarea serviciului esențial și a elementelor critice, identificarea amenințărilor, vulnerabilităților, dependențelor și interdependențelor reprezintă operațiuni distincte și succesive ale procesului de evaluare. Menținerea acestora ca etape separate asigură trasabilitatea evaluării și documentarea individuală a elementelor care fundamentează scenariile de risc, estimarea impactului și estimarea probabilității.<br><br>Propunerile privind completarea subpct. 21.9 și 21.10 cu referiri la riscul inerent și riscul rezidual nu se acceptă. În redacția actuală, metodologia stabilește determinarea scorului și nivelului riscului evaluat, iar riscul rezidual este documentat ulterior aplicării măsurilor de tratare, potrivit pct. 53. Introducerea determinării distincte a scorurilor pentru riscul inerent și riscul rezidual ar presupune modificarea întregului mecanism de |

| | | | |
|---|---|---|---|
| | | Corespunzător modificărilor propuse supra la pct. 23, urmează a fi ajustate prevederile capitolelor IX–XI, în special cele referitoare la determinarea scorului și nivelului de risc, prioritizarea și tratarea riscurilor, fișa de evaluare a riscului și registrul riscurilor. | evaluare, inclusiv a matricei de risc, fișei de evaluare și registrului riscurilor.<br><br>Se acceptă propunerea privind delimitarea măsurilor existente de măsurile suplimentare. În acest sens, subpct. 21.11 va avea următorul cuprins:<br>„21.11. identificarea măsurilor existente și evaluarea eficacității acestora, precum și identificarea și prioritizarea măsurilor suplimentare de tratare a riscurilor;”.<br><br>În consecință, nu este necesară ajustarea capitolelor IX–XI sub aspectul introducerii unei evaluări distincte a riscului inerent și rezidual, urmând a fi operate doar modificările necesare pentru corelarea terminologică privind măsurile existente și măsurile suplimentare. |

| | | | |
|---|---|---|---|
| | | Observăm că la capitolul VI se enumeră mai mult tipuri de riscuri fără a le clasifica, în acest context, propunem clasificarea acestor riscuri aplicând cele 4 tipuri de factori declanșatori ai riscului și tipurile de evenimente ce pot fi produse ca urmare a materializării (oameni, procese/guvernare internă, sisteme/infrastructură, mediul extern). Aceasta clasificare va permite alinierea textului metodologiei la standardele COSO. | **Nu se acceptă.** În urma avizării prealabile, capitolul VI a fost renumerotat și se regăsește la **capitolul V** din proiect. Acesta clasifică deja riscurile în categorii distincte, relevante pentru protecția infrastructurilor critice naționale: riscuri naturale, tehnologice și industriale, antropice intenționate, hibride, cibernetice, organizaționale și de personal, riscuri aferente lanțului de aprovizionare și dependențelor externe, precum și riscuri reputaționale sau informaționale.<br><br>Clasificarea propusă potrivit celor patru categorii „oameni, procese/guvernare internă, sisteme/infrastructură și mediul extern” este specifică preponderent cadrului de management al riscurilor organizaționale COSO și nu reflectă integral specificul riscurilor la adresa infrastructurilor critice naționale, în special riscurile naturale, hibride, cibernetice, tehnologice și intersectoriale.<br><br>Totodată, pct. 32.9 permite includerea altor riscuri relevante pentru sectorul și specificul infrastructurii critice naționale evaluate, iar autoritățile publice responsabile pot stabili cerințe suplimentare privind evaluarea riscurilor, potrivit pct. 13 din proiect. |

| | | | |
|---|---|---|---|
| | | | Prin urmare, clasificarea COSO poate fi utilizată, după caz, ca instrument complementar la nivel sectorial sau instituțional, fără a fi instituită ca structură generală obligatorie a metodologiei. |
| | | La pct. 47, propunem următoarea clasificare „1-4 – risc scăzut; 5-10 – risc moderat”, în acest context, având în vedere descrierea nivelurilor impactului riscului conform prevederilor proiectului, constatăm că riscul de nivel 5 (probabilitate - 1, impact - 5) poate avea un efect mai mare decât în cazul unui risc de nivel 6 (probabilitate - 3, impact - 2). | **Se acceptă.** În urma avizării prealabile, prevederea de la pct. 47 a fost renumerotată și se regăsește la **pct. 46** din proiect.<br><br>Observația este întemeiată, întrucât încadrarea scorului 5 în categoria „risc scăzut” poate conduce la subevaluarea unor scenarii cu impact critic, chiar dacă probabilitatea producerii acestora este foarte scăzută. Astfel, un risc cu impact de nivel 5 și probabilitate de nivel 1 nu poate fi tratat în aceeași categorie cu riscurile care generează consecințe reduse.<br><br>În vederea asigurării unei clasificări proporționale cu gravitatea consecințelor și a unei prioritizări adecvate a măsurilor de tratare, pct. 46 va fi modificat după cum urmează:<br><br>„46. În scopul clasificării și prioritizării, nivelurile de risc se stabilesc după cum urmează: |

| | | | |
|---|---|---|---|
| | | | 1–4 – risc scăzut;<br>5–10 – risc moderat;<br>11–15 – risc înalt;<br>16–25 – risc critic.” |
| | | Având în vedere prevederile de la pct. 75, propunem evaluarea oportunității de completare a normelor metodologice cu un model de Registru al riscurilor aferente infrastructurii critice naționale, care ar contribui la aplicarea unitară a metodologiei, la trasabilitatea deciziilor și la monitorizarea implementării măsurilor de securitate, continuitate, răspuns și recuperare. | **S-a luat act.** Propunerea este deja reflectată în redacția actuală, care prevede că Centrul Național de Coordonare a Protecției Infrastructurilor Critice elaborează, aprobă și pune la dispoziția autorităților publice responsabile și a gestionarilor infrastructurilor critice naționale modele-tip și instrumente metodologice standardizate, inclusiv **modele de registre de risc**.<br><br>Prin urmare, nu este necesară completarea suplimentară a normelor metodologice. |
| | | Cu referire la anexa nr. 2<br><br>La pct.18, propunem următoarea redacție pentru literele d) și f): „d) sinteza evaluării riscurilor inerente și reziduale” și „f) măsurile suplimentare de tratare a riscurilor, stabilite în funcție de nivelul riscurilor reziduale”. | **Nu se acceptă.** Propunerea este condiționată de instituirea, în cadrul normelor metodologice privind evaluarea riscurilor, a unui mecanism distinct de determinare și cuantificare a riscului inerent și a riscului rezidual. Or, proiectul stabilește un mecanism unitar de evaluare a riscurilor, iar la pct. 18.4 și 18.6 din anexa nr. 2 sunt prevăzute, în mod distinct, „sinteza evaluării riscurilor” și „măsurile |

| | | | |
|---|---|---|---|
| | | | suplimentare de tratare a riscurilor”. Totodată, pct. 32.1–32.6 stabilește elementele care se valorifică la elaborarea Planului de securitate, inclusiv riscurile prioritare, nivelul de impact și probabilitate, măsurile existente și deficiențele constatate. Introducerea expresă a noțiunilor de risc inerent și risc rezidual ar necesita revizuirea corespunzătoare a întregului mecanism de evaluare, inclusiv a etapelor, matricei de risc, fișei de evaluare și registrului riscurilor. În consecință, se menține redacția actuală a pct. 18.4 și 18.6. |
| | | La pct. 21, 22, 23, după cuvântul „riscurile” propunem completarea cu cuvântul „reziduale”. Prin aceste ajustări se va corela conținutul planului de securitate cu prevederile pct. 23 din proiectul Normelor metodologice privind evaluarea riscurilor la adresa infrastructurilor critice naționale. | **Nu se acceptă.** Propunerea este corelată cu introducerea unei evaluări distincte a riscului rezidual în cadrul Normelor metodologice privind evaluarea riscurilor, propunere care nu a fost acceptată.<br><br>Pct. 21–23 din anexa nr. 2 stabilesc măsurile aplicabile în funcție de nivelul |
| | | | riscurilor rezultat din mecanismul unitar de evaluare prevăzut de proiect: măsuri obligatorii pentru riscurile înalte sau critice, măsuri proporționale pentru riscurile moderate și monitorizare periodică pentru riscurile scăzute. Completarea acestora cu termenul „reziduale” ar crea neconcordanțe cu metodologia de evaluare, care nu prevede determinarea |

| | | | |
|---|---|---|---|
| | | | distinctă a scorului și nivelului riscului rezidual.<br><br>Totodată, prevederea invocată de autorul avizului, anterior numerotată la pct. 23, se regăsește după avizarea prealabilă la pct. 21 din Normele metodologice privind evaluarea riscurilor. În consecință, se menține redacția actuală a pct. 21–23 din anexa nr. 2. |
| | | La pct. 46, propunem instituirea unui termen de cel puțin 10 zile pentru verificarea plenitudinii dosarului recepționat de către autoritatea publică responsabilă de la gestionarul infrastructurii critice naționale (ICN). Totodată, având în vedere complexitatea informațiilor ce necesită a fi examinate de către autoritatea publică responsabilă, propunem extinderea termenului de examinare prevăzut la acest punct (de exemplu: de la 14 zile lucrătoare - la 30 de zile lucrătoare). | **Se acceptă parțial.** Se acceptă instituirea unui termen distinct pentru verificarea plenitudinii dosarului, însă acesta urmează a fi stabilit ca termen maxim, respectiv **„în cel mult 10 zile lucrătoare”**, și nu „de cel puțin 10 zile”, pentru a evita tergiversarea procedurii.<br><br>De asemenea, se acceptă extinderea termenului de examinare a Planului de securitate de la 14 la **30 de zile lucrătoare**, având în vedere complexitatea evaluării documentației, necesitatea verificării corelării măsurilor cu riscurile identificate și specificul fiecărui sector sau subsector.<br><br>Prevederile vor fi reformulate după cum urmează:<br><br>„46. Autoritatea publică responsabilă verifică plenitudinea dosarului în |

| | | | |
|---|---|---|---|
| | | | termen de cel mult 10 zile lucrătoare de la data recepționării acestuia.”<br><br>„47. În cazul în care dosarul este complet, autoritatea publică responsabilă examinează Planul de securitate în termen de 30 de zile lucrătoare de la data constatării plenitudinii dosarului.”<br><br>„48. În cazul în care dosarul este incomplet sau sunt necesare clarificări, autoritatea publică responsabilă solicită gestionarului completarea informațiilor sau documentelor, indicând aspectele care urmează a fi remediate.” |
| | | La pct. 49, propunem completarea prevederii cu acțiunile ce necesită a fi întreprinse de autoritatea publică responsabilă în cazul în care gestionarul ICN nu transmite completările solicitate în termenul stabilit (de exemplu: reluarea integrală a procedurii într-un anumit interval de timp sau alte acțiuni necesare). | **Se acceptă.** Prevederile actuale stabilesc termenul în care gestionarul trebuie să transmită completările solicitate, fără a reglementa consecințele nerespectării acestuia. Pentru evitarea suspendării procedurii pe termen nedeterminat, după pct. 49 se va introduce o prevedere potrivit căreia, în cazul netransmiterii completărilor în termen și în lipsa unei solicitări motivate de prelungire, autoritatea publică responsabilă restituie dosarul fără finalizarea procedurii de avizare, iar reluarea procedurii se realizează prin depunerea unui dosar complet. |

| | | | |
|---|---|---|---|
| | | | „51. În cazul în care gestionarul nu transmite completările solicitate în termenul prevăzut la pct. 49 și nu solicită, înainte de expirarea acestuia, prelungirea motivată a termenului, autoritatea publică responsabilă restituie dosarul fără finalizarea procedurii de avizare. Gestionarul poate relua procedura prin transmiterea unui dosar complet, termenele de examinare urmând să curgă de la data recepționării acestuia.” |
| | | La pct. 50, propunem a se preciza dacă restituirea planului de securitate cu indicarea motivelor, presupune, similar situațiilor prevăzute la pct. 50 lit. a) și lit. b), elaborarea unui aviz conform structurii prevăzute la pct. 54. Suplimentar, considerăm oportună consemnarea acțiunilor ulterioare ce necesită a fi întreprinse (și termenele prevăzute) de către autoritatea publică responsabilă și respectiv, de către gestionarul ICN în cazul în care este dispusă restituirea planului de securitate prevăzută la pct. 50 lit. c). | **Se acceptă parțial.** Se acceptă instituirea unui termen distinct pentru verificarea plenitudinii dosarului, stabilit la cel mult 10 zile lucrătoare, precum și extinderea termenului de examinare în fond a Planului de securitate la 30 de zile lucrătoare. Totodată, se acceptă reglementarea consecințelor netransmiterii completărilor solicitate, a procedurii aplicabile în cazul restituirii Planului de securitate pentru revizuire și a termenelor de retransmitere și reexaminare.<br><br>Pentru asigurarea coerenței procedurii, prevederile au fost reformulate astfel încât să se distingă între verificarea plenitudinii dosarului și examinarea în fond. Termenul de examinare în fond începe să curgă de la data constatării plenitudinii dosarului, iar perioada în |

| | | | |
|---|---|---|---|
| | | | care gestionarul transmite completări sau clarificări nu se include în acest termen. În situații justificate de complexitatea documentației, existența informațiilor clasificate ori necesitatea unor verificări suplimentare, termenul de examinare poate fi prelungit o singură dată, cu cel mult 15 zile lucrătoare, cu informarea motivată în scris a gestionarului. |
| | | Cu referire la anexa nr. 3<br><br>La pct.12, propunem evaluarea oportunității delimitării lit. f) și h) în patru litere distincte cu următorul conținut: „f) scorurile și nivelurile riscurilor inerente; h) măsurile existente și evaluarea eficacității acestora; f¹) scorurile și nivelurile riscurilor reziduale; h¹) riscurile reziduale prioritare”. O astfel de reglementare este necesară pentru ca planul de securitate să reflecte clar diferența dintre riscul evaluat inițial și riscul rămas după măsurile existente de securitate. | **Nu se acceptă.** Propunerea presupune introducerea, în cadrul Normelor metodologice privind evaluarea riscurilor, a unui mecanism distinct de determinare a scorurilor și nivelurilor riscurilor inerente și reziduale, propunere care nu a fost acceptată.<br><br>În redacția actuală, structura-cadru a Planului de securitate reflectă rezultatele mecanismului unitar de evaluare a riscurilor, măsurile existente, deficiențele constatate și măsurile suplimentare necesare. Delimitarea propusă ar crea neconcordanțe cu metodologia de evaluare, care nu reglementează calcularea separată a riscului inerent și a riscului rezidual.<br><br>Totodată, evaluarea eficacității măsurilor existente și identificarea riscurilor care necesită măsuri suplimentare pot fi reflectate în |

| | | | |
|---|---|---|---|
| | | | conținutul Planului de securitate fără instituirea unor categorii distincte de scor și nivel pentru riscul inerent și cel rezidual. Prin urmare, se menține redacția actuală a pct. 12 din anexa nr. 3. |
| | | La pct. 25, propunem inserarea unei precizări cu privire la apartenența instituțională a persoanelor autorizate să comunice public incidentele care afectează ICN (din cadrul gestionarului ICN, a autorității publice responsabile sau din cadrul Centrului Naţional de Coordonare a Protecţiei Infrastructurilor Critice). | **Se acceptă.** Pct. 28 a fost completat prin precizarea apartenenței instituționale a persoanelor autorizate să comunice public incidentele care afectează infrastructura critică națională. Astfel, comunicarea publică se realizează exclusiv de către persoanele desemnate sau autorizate din cadrul gestionarului infrastructurii critice naționale ori, după caz, din cadrul autorității publice responsabile sau al Centrului Național de Coordonare a Protecției Infrastructurilor Critice, în limitele competențelor legale și cu respectarea mecanismelor de coordonare interinstituțională, a legislației aplicabile și a regimului informațiilor protejate. |
| | | La anexa nr. 4<br><br>La pct. 31 lit. e) urmează a fi precizat ce se corelează cu evaluarea riscurilor în procesul de analiză a solicitării de echivalare. La fel, după cuvântul „riscurilor”, propunem completarea cu cuvintele „inerente și reziduale”. Suplimentar, propunem evaluarea oportunității de completare a pct. 31 cu două litere distincte cu următorul | **Se acceptă parțial.** Pct. 31 a fost completat prin precizarea că obiectul corelării îl constituie documentul sau setul de documente propuse spre echivalare, în raport cu evaluarea riscurilor aferente infrastructurii critice |

| | | | |
|---|---|---|---|
| | | conținut: „evaluarea măsurilor existente și a eficacității acestora și existența Registrului riscurilor”. Această completare va asigura coerența cu propunerile de modificare expuse supra. | naționale. Totodată, au fost introduse criterii distincte privind reflectarea măsurilor existente și evaluarea eficacității acestora, precum și existența și actualitatea Registrului riscurilor, după caz. Nu a fost acceptată completarea cu sintagma „riscurilor inerente și reziduale”, întrucât metodologia nu reglementează determinarea distinctă a scorurilor și nivelurilor acestor categorii de risc. |
| | | La pct. 54, propunem precizarea termenului maxim în care gestionarul ICN este obligat să notifice autoritatea publică responsabilă despre modificarea documentului sau setului de documente recunoscute ca echivalente. Propunerea este valabilă și pentru prevederea de la pct. 43 din anexa nr. 5. | **Se acceptă.** Pct. 54 a fost completat prin stabilirea termenului de cel mult 10 zile lucrătoare pentru notificarea autorității publice responsabile despre modificarea documentului sau a setului de documente recunoscute ca echivalente.<br>A fost actualizat si pct. 44 din anexa 5. |
| | | La anexa nr. 5. La pct. 8, propunem evaluarea oportunității completării acestui punct cu trei litere distincte cu următorul conținut: „actualitatea nivelului riscurilor inerente și reziduale; actualitatea măsurilor existente de securitate, prevenire, continuitate, răspuns și recuperare; actualitatea Registrului riscurilor aferente infrastructurii critice naționale”. Menționăm că o astfel de completare va asigura coerența cu propunerile de modificare expuse supra. | **Se acceptă parțial.** Urmare renumerotării, Pct. 8 a devenit pct.9 din anexa nr. 5, și a fost completat prin includerea verificării actualității evaluării riscurilor și a nivelurilor de risc stabilite, a actualității și eficacității măsurilor existente de securitate, prevenire, continuitate, răspuns și recuperare, precum și a existenței și actualității Registrului riscurilor aferente infrastructurii critice naționale.<br><br>Sintagma „riscurilor inerente și reziduale” nu a fost preluată, întrucât |

| | | | |
|---|---|---|---|
| | | | Normele metodologice privind evaluarea riscurilor nu reglementează determinarea distinctă a scorurilor și nivelurilor pentru aceste două categorii de risc. În consecință, pct. 9.3 a fost formulat prin referire generală la actualitatea evaluării riscurilor și a nivelurilor de risc stabilite. |
| | | Propunerea este valabilă și pentru prevederea de la pct. 43 din anexa nr. 5.- propunem precizarea termenului maxim în care gestionarul ICN este obligat să notifice autoritatea publică responsabilă despre modificarea documentului sau setului de documente recunoscute ca echivalente. | **Se acceptă.** Pct. 43 din anexa nr. 5 se completează prin stabilirea termenului maxim în care gestionarul infrastructurii critice naționale este obligat să notifice autoritatea publică responsabilă despre încetarea, suspendarea sau modificarea substanțială a documentului ori a setului de documente recunoscute ca echivalente. |
| **Comisia Națională a Pieței Financiare (aviz nr. 06-4/2954 din 10.07.2026)** | 18 | Comunică lipsa de obiecții și propuneri asupra proiectului. | |
| **Ministerul Justiției (aviz nr. nr. 04/1-7784 din 13.07.2026 )** | 19 | La pct. 2.1 din Nota de fundamentare, trimiterile la Legea nr. 223/2025 să fie corelate cu temeiul legal indicat în clauza de adoptare. | Se acceptă. Modificările au fost operate. |
| | | În anexa nr. 1, la pct. 22, trimiterea la pct. 23 să fie înlocuită cu trimiterea la pct. 21. | Se acceptă. Modificările au fost operate. |
| | | La pct. 40 din anexa nr. 1, să fie corectată numerotarea subpunctelor, iar descrierea de la subpct. 40.4 să fie integrată la subpct. 40.3. | Se acceptă. Modificările au fost operate, în pct. 41. |
| | | La pct. 62 din anexa nr. 1, să fie indicată expres periodicitatea minimă de actualizare a evaluării riscurilor. | Se acceptă. Modificările au fost operate, în pct.63 |

| | | | |
|---|---|---|---|
| | | La pct. 58 din anexa nr. 1, să fie clarificat dacă Registrul riscurilor este obligatoriu sau facultativ și în ce condiții poate lipsi. | Se acceptă. Modificările au fost operate.<br>Pct. 59 va avea următorul text: „ Gestionarul întocmește un registru al riscurilor, care include riscurile identificate, scorul acestora, nivelul de risc, măsurile existente, măsurile suplimentare și stadiul implementării acestora” |
| | | La pct. 22 din anexa nr. 6, să fie rectificată numerotarea subpunctelor. | S-a luat act. |
| | | La pct. 59 din anexa nr. 1, să fie reevaluată expresia „după caz”, astfel încât să fie clarificat caracterul obligatoriu sau facultativ al raportului de evaluare a riscurilor. | Se acceptă. Modificările au fost operate. Pct. 60 va avea următorul text: „ Rezultatele evaluării riscurilor se includ într-un raport de evaluare a riscurilor la adresa infrastructurii critice naționale”. |
| | | La pct. 71 din anexa nr. 1, norma privind infrastructurile din domeniul apărării, ordinii publice și securității statului să fie plasată într-o dispoziție generală aplicabilă întregului cadru metodologic sau să fie reflectată și în anexele nr. 2, 4 și 5. | **Se acceptă.** Norma prevăzută la pct. 72 din anexa nr. 1 a fost adaptată și inclusă în toate anexele relevante ale proiectului, în funcție de obiectul de reglementare al fiecăreia. Prevederile introduse asigură respectarea regimului juridic aplicabil informațiilor atribuite la secret de stat, informațiilor sensibile privind infrastructurile critice naționale și altor categorii de informații protejate de lege pe parcursul evaluării riscurilor, elaborării și avizării Planului de securitate, echivalării documentelor, revizuirii și actualizării planului. |

| | | | |
|---|---|---|---|
| | | | Anexa 2: pct.100 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 numai persoanelor autorizate, prin mijloace corespunzătoare regimului juridic aplicabil informațiilor respective.”<br><br>Anexa 4, pct. 60: „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.”<br><br>Anexa 5, pct. 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.” |
| | | La pct. 54 din anexa nr. 2, să fie stabilită durata maximă de prelungire a termenului de examinare și avizare a Planului de securitate. | **Se acceptă.** În urma revizuirii și renumerotării prevederilor anexei nr. 2, norma vizată se regăsește la pct. 60. Aceasta a fost completată prin stabilirea duratei maxime de prelungire a termenului de examinare în fond a Planului de securitate. Astfel, termenul poate fi prelungit o singură dată, cu cel mult 15 zile lucrătoare, numai în situații justificate, cu informarea motivată în scris a gestionarului înainte de expirarea termenului inițial. |
| | | Capitolul X din anexa nr. 2 să fie completat cu o periodicitate minimă pentru testarea Planului de securitate sau cu o corelare expresă cu termenul de revizuire periodică. | **Se acceptă.** Capitolul X din anexa nr. 2 a fost completat prin introducerea unui punct nou, care stabilește periodicitatea |

| | | | |
|---|---|---|---|
| | | | minimă pentru testarea Planului de securitate.<br><br>Se introduce următorul punct:<br><br>„79. Testarea Planului de securitate se realizează cel puțin o dată la 2 ani, precum și ori de câte ori intervin modificări semnificative ale infrastructurii critice naționale, ale serviciului esențial, ale riscurilor, procedurilor, responsabilităților ori resurselor prevăzute în plan sau în urma producerii unui incident relevant.” |
| | | În anexa nr. 6, la pct. 25.7, sintagma „incompatibilitate evidentă” să fie concretizată. | **Se acceptă.** Pct. 25.7 din anexa nr. 6 a fost reformulat pentru concretizarea sintagmei „incompatibilitate evidentă” și asigurarea clarității și previzibilității normei.<br><br>Pct. 25.7 va avea următorul cuprins:<br><br>„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 infrastructurii critice naționale pot afecta imparțialitatea, independența ori exercitarea |

| | | | |
|---|---|---|---|
| | | | corespunzătoare a atribuțiilor de ofițer de legătură.” |
| **Ministerul Muncii și Protecției Sociale (aviz nr. nr. 16/3680 din 06.07.2026)** | 20 | Comunică lipsa de obiecții și propuneri asupra proiectului. | |
| **Serviciul de Informații și Securitate (aviz nr. nr. IE/7019 din 13.07.2026)** | 21 | Comunică lipsa de obiecții și propuneri asupra proiectului. | |
| **Agenția Geodezie, Cartografie și Cadastru (aviz nr. 36/01-05/896 din 29.06.2026)** | 22 | Reevaluarea sau argumentarea termenului de 6 luni prevăzut la pct. 7 din proiect pentru aducerea în concordanță a actelor normative departamentale și a procedurilor interne. | **Se acceptă.** În urma revizuirii și renumerotării proiectului, prevederea vizată inițial la pct. 7 se regăsește la **pct. 9**. Termenul a fost reevaluat, având în vedere volumul și complexitatea activităților necesare pentru inventarierea și revizuirea actelor normative departamentale, a procedurilor interne și a documentelor aplicabile. În consecință, termenul a fost extins de la **6 luni la 12 luni** de la data intrării în vigoare a hotărârii. |
| | | La pct. 2 din anexa nr. 1, substituirea sintagmei „procesul structurat prin care sunt identificate, analizate, apreciate și prioritizate riscurile” cu formularea: „procesul structurat de identificare, analiză, evaluare și prioritizare a riscurilor”. | **Se acceptă.** Pct. 2 din anexa nr. 1 a fost revizuit pentru eliminarea redundanțelor și clarificarea etapelor procesului de evaluare a riscurilor. |
| | | Corectarea denumirii capitolului I din anexa nr. 2 din „I,Dispoziții generale” în „I. Dispoziții generale”. | **Se acceptă.** Denumirea capitolului I din anexa nr. 2 a fost corectată din „I,Dispoziții generale” în:„I. Dispoziții generale”. |

| | | | |
|---|---|---|---|
| | | Delimitarea mai clară a atribuțiilor Centrului Național de Coordonare a Protecției Infrastructurilor Critice și ale autorităților publice responsabile în ceea ce privește coordonarea metodologică, emiterea ghidurilor și modelelor de documente, monitorizarea implementării și verificarea conformității. | **Se acceptă.** Delimitarea atribuțiilor a fost clarificată în proiectul hotărârii, la pct. 2, 4 și 7, precum și în anexa nr. 2, la pct. 14, 15, 45, 77, 99 și 101. Autoritățile publice responsabile asigură coordonarea sectorială, examinarea și avizarea Planurilor de securitate, monitorizarea implementării măsurilor și elaborarea instrucțiunilor sectoriale, iar Centrul Național de Coordonare a Protecției Infrastructurilor Critice asigură coordonarea metodologică la nivel național, acordarea suportului metodologic și elaborarea modelelor-tip și a instrumentelor metodologice standardizate. |
| | | Completarea Notei de fundamentare cu informații suplimentare privind sursele de finanțare și resursele necesare implementării proiectului, inclusiv necesarul de personal, impactul asupra volumului de activitate, instruirea personalului și costurile administrative. | **Se acceptă parțial.** Nota de fundamentare a fost completată cu informații privind impactul administrativ al implementării proiectului, activitățile suplimentare ce revin autorităților publice responsabile și utilizarea, la etapa inițială, a resurselor umane, financiare și tehnice existente.<br><br>Nu a fost realizată o estimare financiară detaliată și cuantificată, întrucât necesarul efectiv de personal, instruire și resurse financiare va depinde de specificul fiecărui sector, de numărul infrastructurilor critice naționale desemnate, de capacitățile |

| | | | |
|---|---|---|---|
| | | | instituționale existente și de soluțiile concrete adoptate în procesul implementării. Eventualele necesități suplimentare vor fi evaluate, fundamentate și planificate separat, potrivit cadrului bugetar aplicabil. |
| | | Introducerea în proiect și în Nota de fundamentare a unei referințe exprese la Hotărârea Guvernului nr. 185/2026 privind desemnarea autorităților publice responsabile de sectoarele și subsectoarele infrastructurii critice naționale | **Se acceptă.** În proiectul hotărârii, la pct. 3, a fost introdusă precizarea potrivit căreia autoritățile publice responsabile sunt cele desemnate prin Hotărârea Guvernului nr. 185/2026 cu privire la desemnarea autorităților publice responsabile de sectoarele și subsectoarele infrastructurii critice naționale.<br><br>Totodată, Nota de fundamentare a fost completată la compartimentul „Principalele prevederi ale proiectului și evidențierea elementelor noi” cu referința expresă la Hotărârea Guvernului nr. 185/2026 și cu precizarea rolului autorităților desemnate în procesele de identificare, evaluare a riscurilor, examinare și monitorizare la nivelul sectoarelor și subsectoarelor respective. |
| **Ministerul Agriculturii și** | 23 | Comunică lipsa de propuneri și obiecții asupra proiectului. | |

| | | | |
|---|---|---|---|
| **Industriei Alimentare ( aviz** nr. 2026PHG-**2036 din 16.07.2026)** | | | |
| **Administrația Națională a Penitenciarelor (aviz nr. 7-2136 din 03.08.2026)** | 24 | Comunică lipsa de propuneri și obiecții asupra proiectului. | |
| **Agenția pentru Securitate Cibernetică (scrisoare din 5.08.2026)** | 25 | Agenția pentru Securitate Cibernetică a comunicat că proiectul a fost avizat prealabil fără obiecții și propuneri, cu informarea Ministerului Dezvoltării Economice și Digitalizării. Totodată, în cadrul procedurii de avizare repetată, poziția Agenției a fost reflectată prin avizul general al Ministerului Dezvoltării Economice și Digitalizării, autoritatea în subordinea căreia se află Agenția. | S-a luat act. |
| **Agenția Națională Transport Auto (aviz nr. 15/1-4065 din 06.08.2026)** | 26 | Comunică lipsa obiecțiilor și propunerilor asupra proiectului. | |
| **Agenția Navală (aviz nr. 03-301 din 22.07.2026)** | 27 | Comunică lipsa obiecțiilor și propunerilor asupra proiectului. | |
| **Expertizare** | | | |
| **Raportul de expertiză anticorupție al CNA nr. EHG26/11754 din 06.08.2026** | 1 | Se recomandă excluderea pct. 9 din anexa nr. 1, întrucât prevederea are caracter redundant, principiul aplicării normelor speciale fiind deja reflectat în proiect și reglementat de Legea nr. 100/2017 cu privire la actele normative. | **Se acceptă.** Pct. 9 din anexa nr. 1 a fost exclus. |
| | | Se recomandă corelarea cerințelor minime privind forma și conținutul Planului de securitate prevăzute la pct. 35 din anexa nr. 3 cu cele prevăzute la pct. 19 din anexa nr. 2, în vederea evitării eventualelor neconcordanțe între dispozițiile proiectului referitoare la planurile de securitate. În cazul în care cele două dispoziții reglementează același conținut, una dintre acestea urmează a fi exclusă, pentru a evita dublarea reglementării și repetarea inutilă a normelor. | **Se acceptă.** Pentru evitarea dublării reglementării, pct. 19 din anexa nr. 2 a fost exclus, cerința privind caracterul concret și aplicabil al Planului de securitate fiind menținută în anexa nr. 3, care reglementează în mod distinct structura-cadru și cerințele minime de |

| | | | |
|---|---|---|---|
| | | | formă și conținut ale Planului de securitate. |
| | | Norma de la pct. 44 prevede că respingerea echivalării nu exonerează gestionarul de obligația de a elabora și transmite spre avizare Planul de securitate. CNA consideră că formularea nu stabilește suficient de clar dacă această obligație devine imediat exigibilă după respingerea echivalării și nici termenul în care trebuie executată, nefiind clar dacă se aplică termenul prevăzut în anexa nr. 2 sau un alt termen. CNA recomandă reconsiderarea pct. 44. | **Se acceptă.** Pct. 44 din anexa nr. 4 a fost completat pentru a preciza expres că, în cazul respingerii echivalării, obligația de elaborare și transmitere spre avizare a Planului de securitate se execută în termenul stabilit de anexa nr. 2. Totodată, s-a precizat că inițierea și desfășurarea procedurii de echivalare nu suspendă și nu prelungește termenul general aplicabil elaborării și transmiterii spre avizare a Planului de securitate. |
| | | Se recomandă corelarea prevederilor privind periodicitatea testării Planului de securitate, prevăzută în anexa nr. 2, cu periodicitatea revizuirii acestuia, prevăzută în anexa nr. 5, astfel încât să fie exclusă orice neclaritate privind raportul dintre cele două obligații și termenele aplicabile. | **Se acceptă.** Prevederile referitoare la periodicitatea testării și revizuirii Planului de securitate au fost corelate. În acest sens, pct. 8 din anexa nr. 5 a fost completat cu prevederea potrivit căreia 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 actualizare a acestuia. Termenul de cel puțin o dată la 2 ani se menține pentru ambele procese. |
| **Raportul de expertiză al Ministerului Justiției nr. 04/1-8836 din 04.08.2026** | 2 | La subpct. 7.3, se vor exclude cuvintele **„la prezenta hotărâre”**, deoarece, potrivit art. 55 alin. (4) din Legea nr. 100/2017, atunci când se face trimitere la o normă juridică din același act normativ sau element structural, trimiterea se face fără precizarea că aceasta face parte din același act, cu excepția cazului în care precizarea este necesară pentru evitarea unui echivoc. | **Se acceptă.** La subpct. 7.3 din anexa nr. 2 au fost excluse cuvintele „la prezenta hotărâre”, în vederea conformării cu prevederile art. 55 alin. (4) din Legea nr. 100/2017 cu privire la actele normative. Totodată, au fost |

| | | | |
|---|---|---|---|
| | | Ministerul Justiției menționează că observația este valabilă pentru toate cazurile similare din proiect. | verificate și ajustate corespunzător cazurile similare din cuprinsul proiectului. |
| | | Se recomandă precizarea expresă a momentului de la care curge termenul de 9 luni pentru elaborarea și transmiterea spre avizare a Planului de securitate, astfel încât să rezulte fără echivoc că termenul se calculează de la data desemnării infrastructurii drept infrastructură critică națională. | **Se acceptă.** Pct. 25 din anexa nr. 2 a fost completat pentru a preciza expres că termenul de 9 luni pentru elaborarea și transmiterea spre avizare a Planului de securitate curge de la data desemnării infrastructurii drept infrastructură critică națională, în vederea eliminării oricărui echivoc privind momentul de început al termenului. |
| | | La anexa nr. 2, subpct. 42.4, se recomandă excluderea sintagmei „după caz” din formularea referitoare la registrul riscurilor, întrucât întocmirea registrului riscurilor reprezintă o obligație stabilită prin anexa nr. 1, iar prezentarea acestuia în dosarul transmis spre avizare nu poate avea caracter facultativ. | Se acceptă. Sintagma „după caz” a fost exclusă de la subpct. 41.4 din anexa nr. 2, urmare renumerotării, având în vedere că întocmirea registrului riscurilor reprezintă o obligație prevăzută de anexa nr. 1, iar includerea acestuia în dosarul transmis spre avizare nu are caracter opțional. |
| | | La **anexa nr. 2, pct. 53**, se recomandă stabilirea unui termen maxim pentru suspendarea termenului de examinare în fond și, concomitent, stabilirea termenului în care gestionarul urmează să prezinte clarificările sau informațiile suplimentare solicitate de autoritatea publică responsabilă, în vederea asigurării previzibilității procedurii și evitării suspendării acesteia pe o perioadă nedeterminată. | **Se acceptă.** Pct. 52 din anexa nr. 2, urmare renumerotării, a fost completat prin stabilirea unui termen de 10 zile lucrătoare pentru prezentarea clarificărilor sau informațiilor suplimentare solicitate de autoritatea publică responsabilă și a unei durate maxime de 15 zile lucrătoare pentru suspendarea termenului de examinare în fond, în vederea asigurării previzibilității și celerității procedurii de avizare. |

| | | | |
|---|---|---|---|
| | | Cu referire la normele prevăzute la **pct. 1–7 din anexa nr. 3**, dispozițiile care reiau normele generale din anexa nr. 2 referitoare la definiția, scopul și cerințele Planului de securitate se vor exclude. Întrucât anexa nr. 3 reglementează structura-cadru a Planului, aceasta urmează să cuprindă exclusiv elementele structurale și conținutul minim al documentului, în vederea evitării dublajului normativ. | **Se acceptă.** Urmare discuțiilor purtate cu Ministerul Justiției, recomandarea a fost reexaminată și acceptată. În vederea evitării dublajului normativ, au fost excluse din anexa nr. 3 dispozițiile de la pct. 1–7 care reiau normele generale deja reglementate în anexa nr. 2 referitoare la definiția, scopul și cerințele Planului de securitate.<br><br>Anexa nr. 3 a fost revizuită astfel încât să cuprindă exclusiv prevederile care țin nemijlocit de Structura-cadru a Planului de securitate, respectiv elementele structurale, conținutul minim obligatoriu și cerințele necesare pentru utilizarea acesteia la elaborarea Planului de securitate.<br><br>Modificările operate asigură delimitarea clară a obiectului anexei nr. 3 față de normele metodologice din anexa nr. 2 și elimină suprapunerile de reglementare. |
| | | Prevederea de la pct. 8 din anexa nr. 3, referitoare la examinarea și recunoașterea echivalenței documentelor aferente infrastructurilor critice naționale din domeniul apărării, ordinii publice și securității statului, urmează a fi transferată în anexa nr. 4, întrucât aceasta reglementează procedura de echivalare a documentelor existente cu Planul de securitate. Menținerea normei în anexa nr. 3 nu corespunde obiectului acesteia, care vizează structura-cadru a Planului de securitate. | **Se acceptă.** Prevederea de la pct. 8 din anexa nr. 3 a fost exclusă și transferată în anexa nr. 4, care reglementează în mod distinct procedura de echivalare a documentelor existente cu Planul de securitate. Prevederea a fost introdusă |

| | | | |
|---|---|---|---|
| | | | în anexa nr. 4, capitolul XIV „Protecția informațiilor” |
| | | La pct. 38 din anexa nr. 5, trimiterea la pct. 36 urmează a fi substituită cu trimiterea la pct. 37, întrucât pct. 37 stabilește cazurile în care modificările operate asupra Planului de securitate impun reavizarea acestuia. | **Se acceptă.** Trimiterea internă de la pct. 38 din anexa nr. 5 a fost corectată, prin substituirea trimiterii la pct. 36 cu trimiterea la pct. 37, care reglementează elementele a căror modificare determină necesitatea reavizării Planului de securitate. |

**Ministru** **Daniella MISAIL-NICHITIN**