GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. _____

din_____

privind aprobarea Regulamentului cu privire la elaborarea, actualizarea și implementarea Planului național de răspuns la incidentele cibernetice și crizele cibernetice

În temeiul art. 9 alin. (4) din Legea nr. 48/2023 privind securitatea cibernetică (Monitorul Oficial al Republicii Moldova, 2023, nr. 151-153), Guvernul HOTĂRĂȘTE:

1. Se aprobă Regulamentul cu privire la elaborarea, actualizarea și implementarea prevederilor planului național de răspuns la incidentele cibernetice și crizele în domeniul securității cibernetice.

2. Agenția pentru Securitate Cibernetică va elabora și va aproba Planul național de răspuns la incidentele cibernetice și crizele în domeniul securității cibernetice în termen de 12 luni de la data intrării în vigoare a prezentei hotărâri.

3. Autoritățile și instituțiile publice, furnizorii de servicii în sectoarele critice identificați în baza Hotărârii Guvernului nr. 860/2024 cu privire la identificarea furnizorilor de servicii vor acorda suportul necesar Agenției pentru Securitate Cibernetică în vederea elaborării și actualizării, precum și vor asigura implementarea Planului național de răspuns la incidentele cibernetice și crizele în domeniul securității cibernetice.

4. Controlul executării prezentei hotărâri se pune în sarcina Ministerului Dezvoltării Economice și Digitalizării.

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

Prim-ministru

Viceprim-ministru,
ministrul dezvoltării
economice și digitalizării

Anexă la Hotărârea Guvernului

nr._____din_____

REGULAMENTUL

cu privire la elaborarea, actualizarea și implementarea prevederilor Planului național de răspuns la incidentele cibernetice și crizele în domeniul securității cibernetice

Capitolul I. Dispoziții generale

1. Regulamentul cu privire la elaborarea, actualizarea și implementarea prevederilor Planului național de răspuns la incidente cibernetice și crize în domeniul securității cibernetice *(în continuare - Regulament*) are ca obiect de reglementare cerințele față de conținutul Planului național de răspuns la incidentele cibernetice și crizele în domeniul securității cibernetice *(în continuare – Plan)*, procesul de elaborare, inclusiv etapele acestui proces, modul de actualizare și implementare a Planului, atribuțiile autorităților și instituțiilor publice în acest proces, drepturile și obligațiile persoanelor juridice implicate în procesul de elaborare, actualizare și implementare a Planului, precum și procedurile de interacțiune dintre acestea.

2. În sensul prezentului Regulament noțiunile utilizate au următorul înțeles:

2.1. ***incident cibernetic*** – astfel cum este definit la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică;

2.2. ***incident cibernetic de mare amploare*** – înseamnă un incident care provoacă un nivel de perturbare semnificativ asupra serviciilor esențiale, securității naționale, economiei sau ordinii publice sau care are un impact semnificativ asupra unui alt stat;

2.3. ***criză*** – astfel cum este definită la art. 2 pct. 3 din Legea nr. 248/2025 privind managementul situațiilor de criză;

2.4. ***criză cibernetică*** - situație excepțională generată de un incident cibernetic de mare amploare, care afectează în mod semnificativ funcționarea serviciilor esențiale, securitatea națională, economia sau ordinea publică .

2.5. ***gestionare a crizei cibernetice*** - totalitatea măsurilor luate în mod coordonat la nivel strategic, operațional și tehnic de către autoritățile și instituțiile publice responsabile la etapele de prevenire, pregătire, răspuns și recuperare după situația de criză, în scopul reducerii impactului și a efectelor unuia sau mai multor incidente cibernetice asupra sănătății și vieții persoanelor, asupra bunurilor, asupra mediului înconjurător, sau ordinii constituționale;

2.6. ***conștientizare situațională*** – proces dinamic, multidimensional și interinstituțional prin care persoanele implicate în gestionarea unei crize cibernetice colectează, integrează și interpretează informații relevante pentru a construi o imagine operațională comună, care permite înțelegerea contextului, anticiparea evoluțiilor și sprijinirea deciziilor strategice în timp real.

3. Alte noțiuni sunt utilizate în prezentul Regulament în înțelesul atribuit acestora de prevederile cadrului normativ relevant, inclusiv Legea nr. 48/2023 privind securitatea cibernetică, Legea nr. 248/2025 privind managementul situațiilor de criză, cadrul normativ privind identificarea, desemnarea și protecția infrastructurilor critice naționale.

4. Principiile de bază ale procesului de elaborare, actualizare și implementare a Planului sunt:

4.1. ***planificare bazată pe riscuri*** – presupune că elaborarea, stabilirea priorităților și alocarea resurselor pentru implementarea Planului să se bazeze pe identificarea, evaluarea și tratarea sistematică a riscurilor cibernetice la adresa serviciilor esențiale și/sau a infrastructurii critice naționale;

4.2. ***structură de guvernanță clară*** – presupune că elaborarea și implementarea Planului trebuie să se bazeze pe un cadru organizațional, instituțional și funcțional de coordonare și cooperare în timp de criză, coerent, transparent și cu o ierarhie bine definită de autoritate și luare a deciziilor în timpul unei crize cibernetice.

4.3. ***îmbunătățire continuă*** – presupune că elaborarea, actualizarea și implementarea Planului trebuie să se desfășoare într-un proces sistematic și dinamic, astfel încât să se asigure că capacitățile naționale de gestionare a crizelor cibernetice rămân adaptabile, eficiente și aliniate la standardele europene și internaționale de reziliență cibernetică.

5. Atunci când elaborează Planul, Agenția pentru Securitate Cibernetică *(în continuare - Agenția)* trebuie să se asigure că procedurile de răspuns la incidentele cibernetice, inclusiv și în mod special cele la scară largă, și procedurile de gestionare a crizelor cibernetice trebuie să garanteze că autoritățile și instituțiile publice responsabile acționează în mod coordonat în gestionarea crizelor cibernetice în baza și cu respectarea cel puțin a următoarelor principii:

5.1. ***proporționalitate*** – care presupune corelarea și alinierea naturii și severității acțiunilor și măsurilor de soluționare a crizei cibernetice întreprinse de persoanele responsabile la amploarea acesteia;

5.2. ***subsidiaritate*** – care presupune că acțiunile coordonate ale autorităților și instituțiilor publice competente să soluționeze un incident cibernetic și/sau să răspundă la o criză cibernetică trebuie să se desfășoare în funcție de tipul și locul producerii incidentului cibernetic concret, care poate conduce sau a condus la o criză cibernetică;

5.3. ***complementaritate*** – care presupune utilizarea instrumentelor disponibile și de reglementare care se completează reciproc prin cadre sectoriale, naționale și internaționale;

5.4. ***confidențialitate*** - care presupune comunicarea între părțile implicate în gestionarea crizelor prin intermediul unei infrastructuri sigure și reziliente destinată schimbului de informații, precum și respectînd protocoalele pentru schimbul ulterior al acestora în cadrul și în afara autorităților și instituțiilor publice implicate în soluționarea crizei cibernetice.

Capitolul II. Conținutul Planului

Secțiunea 1. Dispoziții generale.

6. Planul este un document care stabilește cadrul național de coordonare și cooperare la nivel strategic, operațional și tehnic a proceselor de pregătire, detectare, escaladare, răspuns și recuperare în urma incidentelor cibernetice, inclusiv celor semnificative sau de mare amploare, și a crizelor cibernetice în scopul protecției serviciilor esențiale, a siguranței publice și a securității naționale.

7. Elaborarea, aprobarea și actualizarea Planului are ca scop determinarea, corelarea și delimitarea rolurilor, atribuțiilor și responsabilităților autorităților și instituțiilor publice precum și a altor persoane juridice responsabile, prin instituirea unor mecanisme testate care permit un răspuns unificat, eficient și în timp util la incidente și crize cibernetice.

8. Planul se elaborează, se aprobă și se actualizează de către Agenție.

9. Planul trebuie să fie corelat cu Planul național de management al crizelor, aprobat de Guvern în temeiul art. 7 alin. (1) din Legea nr. 248/2025 privind managementul situațiilor de criză.

10. La solicitarea Agenției, Centrul Național de Management al Crizelor furnizează orientări metodologice pentru corelarea și integrarea Planului cu Planul național de management al crizelor.

11. Planurile de răspuns la incidente cibernetice și gestionare a crizelor cibernetice ale furnizorilor de servicii urmează a fi corelate cu Planul național de răspuns la incidentele cibernetice și crizele în domeniul securității cibernetice. La solicitarea furnizorilor de servicii în sectoarele critice, Agenția oferă suport consultativ și orientare metodologică pentru corelarea și sincronizarea planurilor de gestionare a crizelor, elaborate de către aceștia în conformitate cu Cerințele privind măsurile de securitate a rețelelor și a sistemelor informatice ale furnizorilor de servicii în sectoarele critice**.**

12. În conformitate cu art. 9 alin. (3) din Legea nr. 48/2023 privind securitatea cibernetică, Planul trebuie să includă cel puțin:

12.1. obiectivele măsurilor și ale activităților de pregătire la nivel național;

12.2. sarcinile și atribuțiile autorităților și instituțiilor publice responsabile;

12.3. procedurile de gestionare a crizelor și căile de schimb de informații;

12.4. măsurile de pregătire, inclusiv exercițiile și activitățile de formare;

12.5. furnizorii de servicii, interacțiunea dintre aceștia și autoritățile și instituțiile publice responsabile, precum și infrastructura implicată;

12.6. alte părți interesate relevante;

12.7. procedurile și mecanismele de interacțiune dintre autoritățile și instituțiile publice responsabile, precum și de interacțiune coordonată a acestora în gestionarea incidentelor cibernetice și a crizelor în domeniul securității cibernetice de mare amploare, inclusiv a celor la nivel european și internațional.

Secțiunea 2 . Obiectivele măsurilor și ale activităților de pregătire la nivel național

13. În Plan urmează a fi determinate și descrise clar obiectivele măsurilor și ale activităților de pregătire la nivel național.

14. Obiectivele trebuie să decurgă din viziunea strategică a statului în gestionarea unei situații de criză, bazate pe o abordare a implicării tuturor autorităților și instituțiilor publice și care ia în considerare toate pericolele indiferent de natura acestora, având ca finalitate prevenirea, protecția, diminuarea impactului, răspunsul la și recuperarea în urma materializării amenințărilor cibernetice.

Secțiunea 3. Sarcinile și atribuțiile autorităților și instituțiilor publice responsabile

15. Planul trebuie să descrie în mod clar sarcinile și atribuțiile care urmează a fi îndeplinite de fiecare autoritate și instituție publică desemnată în timpul gestionării crizelor cibernetice la nivel strategic, operațional și tehnic, precum și structura de guvernanță care trebuie să îndeplinească aceste sarcini și atribuții.

16. La nivel strategic, Planul urmează să determine autoritățile și instituțiile publice care sunt responsabile de:

16.1. identificarea impactului perturbărilor cauzate de criză;

16.2. asigurarea disponibilității sprijinului de urgență, atunci când e necesar, inclusiv prin suplimentarea competențelor de răspuns cibernetic, care ar putea include utilizarea forțelor de rezervă cibernetice, inclusiv ale mediului privat; activarea mecanismelor suplimentare de gestionare a crizelor, în funcție de natura și impactul incidentului cibernetic, inclusiv mecanismele de protecție civilă;

16.3. luarea măsurilor diplomatice pentru a răspunde la criza cibernetică națională;

16.4. cooperarea și coordonarea cu organizațiile europene, internaționale și țările partenere, inclusiv cu Rețeaua europeană a organizațiilor de legătură în materie de crize cibernetice (EU - CyCLONe);

16.5. determinarea strategiei comune de comunicare către public.

17. La nivel operațional, în Plan urmează a fi determinate autoritățile și instituțiile publice care sunt responsabile de:

17.1. asigurarea informațională, în vederea susținerii procesului decizional la nivel strategic;

17.2. coordonarea gestionării crizei de securitate cibernetică, prin implicarea altor părți necesare în asigurarea răspunsului la incidentele cibernetice, după caz, a gestionarilor de infrastructură critică, echipelor sectoriale sau organizaționale de răspuns la incidentele cibernetice, autorităților publice responsabile de combaterea criminalității informatice și cele responsabile de apărarea națională.

17.3. alertarea persoanelor afectate de incidentul cibernetic sau a celor care pot contribui la răspuns și furnizarea către aceste persoane a informațiilor necesare.

17.4. evaluarea consecințelor și a impactului la nivel național și propunerea de posibile măsuri de remediere.

18. La nivel tehnic, Planul trebuie să stabilească autoritățile și instituțiile publice care sunt responsabile de:

18.1. gestionarea incidentelor cibernetice pe perioada crizei cibernetice;

18.2. monitorizarea și supravegherea incidentelor cibernetice, inclusiv analiza continuă a amenințărilor și riscurilor în materie de securitate cibernetică.

19. În Plan urmează a fi descrisă structura de guvernanță din perspectiva categorizării autorităților și instituțiilor publice după rolurile și responsabilitățile pe care le au în gestionarea crizei cibernetice, inclusiv autoritățile principale și cele de sprijin, precum și rolurile și responsabilitățile de coordonare la nivel strategic, operațional și tehnic.

Secțiunea 4. Procedurile de gestionare a crizelor și căile de schimb de informații

20. Procedurile de gestionare a crizelor și căile de schimb de informații au ca scop sistematizarea metodelor și protocoalelor de interacțiune pentru a facilita schimbul de informații și coordonarea în timpul crizelor cibernetice, în vederea sprijinirii cooperării și pregătirii la nivel operațional, detectării și analizei, izolării, eradicării, recuperării în

urma unor incidente, precum și a activităților ulterioare analizei post-incident. Procedurile trebuie să cuprindă cel puțin:

20.1. modul de distribuire a informației către părțile relevante, descrierea informației, termenii de prezentare, căile și mijloacele de distribuire a acesteia;

20.2. modul de raportare a situației privind starea securității, care trebuie să descrie procesul de furnizare a informațiilor în vederea asigurării unei conștientizări situaționale și pentru a obține o imagine comună, actualizată și coerentă asupra situației de criză, care să permită luarea deciziilor adecvate la nivel tactic, operațional și strategic;

20.3. modul de comunicare a deciziilor strategice, care trebuie să includă descrierea procedurilor de informare a părților interesate relevante despre deciziile aprobate și despre impactul crizei asupra societății și statului.

20.4. modul de escaladare a răspunsului la incidente sau crize cibernetice la nivel național și internațional, inclusiv criterii și sau praguri de escaladare;

20.5. descrierea nivelurilor de operare în regim normal, în regim de alertă și în regim de criză, inclusiv criteriile și pragurile de escaladare către nivelurile de operare superioare, cel de alertă și, respectiv cel de criză;

20.6. taxonomia și clasificarea incidentelor cibernetice, inclusiv a celor semnificative și a celor de mare amploare, descrierea elementelor constitutive ale crizei cibernetice în vederea asigurării bazei de declanșare a escaladării în conformitate cu procedurile operaționale;

20.7. procedurile operaționale standard ce urmează a fi utilizate în regimurile de operare respective;

20.8. modul de inițiere de către autoritatea națională responsabilă pentru gestionarea crizelor cibernetice a cooperării transfrontaliere cu echipele de răspuns la incidente cibernetice, autoritățile competente în domeniul securității cibernetice, precum și cu organizații internaționale și organizațiile Uniunii Europene în materie de gestionare a crizelor, inclusiv a celor cibernetice.

20.9. canalele de schimb de informații, categoriile de informații și nivelul de confidențialitate a acestora.

Secțiunea 5. Măsurile de pregătire, inclusiv exercițiile și activitățile de formare

21. Măsurile de pregătire din Plan trebuie să includă, fără însă a se limita la acestea, o descriere a:

21.1. activităților de consolidare a capacităților operaționale în domeniul securității cibernetice, inclusiv a platformelor tehnologice necesare;

21.2. modului de organizare și de participare la exerciții de securitate cibernetică, inclusiv de nivel național și internațional pentru testarea procedurilor de răspuns la incidente cibernetice și gestionare a crizelor cibernetice;

21.3. activităților de organizare a cursurilor de formare, interne și/sau externe relevante, opționale și obligatorii;

21.4. activităților de testare la nivel procedural, a gradului de pregătire al participanților de a comunica eficient și de a face schimb de informații, precum și a timpului de răspuns.

21.5. activităților de schimb de experiență, inclusiv partajare și punerea în aplicare a lecțiilor învățate din incidentele și crizele cibernetice și exercițiile anterioare;

21.6. activităților de planificare și punere în aplicare a măsurilor de testare a pregătirii autorităților și instituțiilor publice în domeniul securității cibernetice.

Secțiunea 6. Furnizorii de servicii și alte părți interesate relevante, interacțiunea dintre aceștia și autoritățile și instituțiile publice responsabile, precum și infrastructura implicată

22. Planul stabilește procedurile de acces, conform drepturilor atribuite, la datele privind furnizorii de servicii esențiali și importanți, alte părți interesate relevante procesului de răspuns la incidentele cibernetice și/sau de gestionare a crizelor cibernetice, precum și procedurile de schimb de date privind infrastructura, capacitățile umane și tehnice relevante procesului de răspuns la incidente cibernetice și de gestionare a crizelor cibernetice.

23. Alte părți interesate relevante procesului de răspuns la incidentele cibernetice și/sau de gestionare a unei crizelor cibernetice, menționate la pct. 22 sunt:

23.1. entitățile academice și de cercetare din perspectiva capacității acestora de a implementa activități educaționale, de a adapta programele de instruire și de formare existente și de dezvoltare a noilor programe educaționale, precum și din perspectiva potențialului acestor entități de a dezvolta tehnologii și instrumente avansate de securitate cibernetică;

23.2. reprezentanți ai sectorului privat, sau ai asociațiilor profesionale care reprezintă sectorul privat și care, prin intermediul parteneriatelor public-private, ar putea facilita implicarea reprezentanților relevanți ai sectorului privat în procesul național de gestionare a crizelor cibernetice;

23.3. persoanele juridice de drept privat, care nu au fost identificate în calitate de furnizor de servicii în baza Hotărârii Guvernului nr. 860/2024 „Cu privire la identificarea furnizorilor de servicii”, dar care dețin capacități tehnice, tehnologice, umane sau de altă natură și care at putea contribui la realizarea obiectivelor Planului.

24. Planul trebuie să determine în mod explicit procedurile de interacțiune dintre părțile interesate relevante și modul de utilizare a infrastructurii implicate în răspunsul la incidente și în gestionarea crizelor cibernetice.

Secțiunea 7. Procedurile și mecanismele de interacțiune la nivel național și internațional

25. Procedurile și mecanismele de interacțiune la nivel național și internațional trebuie să vizeze cel puțin următoarele:

25.1. procedurile naționale și angajamentele internaționale ale Republicii Moldova sau ale autorităților și instituțiilor publice, responsabile în cadrul procesului de gestionare a crizelor, care stabilesc participarea Republicii Moldova la mecanisme, disponibile la nivel internațional, inclusiv european, regional sau bilateral, de răspuns la incidentele cibernetice și de gestionare a crizelor cibernetice;

25.2. modul de escaladare a răspunsului la crizele cibernetice în cadrul mecanismelor internaționale, inclusiv europene disponibile sau la care Republica Moldova este parte în baza tratatelor internaționale.

Capitolul III. Elaborarea Planului

Secțiunea 1. Etapele de elaborare a Planului

26. Procesul de elaborare a Planului se desfășoară în următoarele etape:

26.1. inițierea elaborării;

26.2. colectarea și analizarea informațiilor;

26.3. întocmirea textului proiectului Planului;

26.4. consultarea proiectului Planului cu părțile interesate;

26.5. aprobarea Planului.

27. Agenția este responsabilă de asigurarea materială și logistică a procesului de elaborare a Planului, precum și documentarea activității administrative, desfășurate în cadrul acestui proces în conformitate cu prevederile cadrul normativ aplicabil.

Secțiunea 2. Etapa de inițiere a elaborării Planului.

28. Etapa de inițiere include definirea cadrului instituțional și metodologic, constituirea, la nivel operațional, a Grupului de lucru interinstituțional pentru elaborarea și actualizarea Planului, precum și planificarea activităților de elaborare cu determinarea acțiunilor, responsabililor și termenelor de realizare.

29. Agenția prin act administrativ constituie Grupul de lucru interinstituțional pentru elaborarea și actualizarea Planului *(în continuare – Grupul de lucru*).

30. În componența Grupului de lucru intră din oficiu reprezentanții: Centrului Național pentru Managementul Crizelor, Inspectoratului pentru Management Operațional al Ministerului Afacerilor Interne, Instituției publice „Serviciul Tehnologia Informației și Securitate Cibernetică", Serviciului de Informație și Securitate, ministerelor responsabile de realizarea politicii statului în sectoarele și subsectoarele prevăzute în anexa nr. 2 la Hotărârea Guvernului nr. 860/2024 „Cu privire la identificarea furnizorilor de servicii".

31. În componența Grupului de lucru pot fi incluși și reprezentanți ai persoanelor juridice menționate la pct. 23.

32. Președinția Grupului de lucru se asigură de către un funcționar public de conducere din cadrul Agenției.

33. În ordinul de constituire a Grupului de lucru se desemnează secretarul Grupului de lucru din rândul funcționarilor publici, angajați ai Agenției, care nu este membru al Grupului de lucru, și subdiviziunea structurală a Agenției care va exercita lucrările de secretariat ale Grupului de lucru.

Secțiunea 3. Etapa de colectare și analizare a informațiilor

34. Etapa de colectare și analizare a informațiilor include:

34.1. analizarea cadrului juridico-normativ, instituțional și de planificare strategică în domeniul securității cibernetice;

34.2. analiza informației disponibile privind evaluarea riscurilor la nivel național în domeniul securității cibernetice, a amenințărilor cibernetice și a vulnerabilităților;

34.3. colectarea informațiilor despre capacitățile existente, infrastructurile critice și interdependențele dintre acestea;

34.4. organizarea de consultări cu părțile interesate relevante.

35. Autoritățile și instituțiile publice și furnizorii de servicii în sectoarele critice identificați de către Agenție potrivit cadrului normativ în domeniul securității cibernetice, prezintă Agenției la solicitare informațiile disponibile necesare întocmirii textului Planului și relevante cadrului de fundamentare a prevederilor Planului.

Secțiunea 4. Etapa de întocmire a textului Planului

36. La această etapă Grupul de lucru determină structura Planului și întocmește textul versiunii inițiale a acestuia.

37. Proiectul Planului este un document cu accesibilitate limitată, regimul de protecție aplicabil fiecărei categorii de informații conținute în proiect fiind determinat de către Grupul de lucru potrivit cadrului normativ aplicabil.

38. Conținutul Planului trebuie să includă cel puțin problematicile abordate în Capitolul II din prezentul Regulament.

Secțiunea 5. Etapa consultării proiectului Planului cu părțile interesate

39. Proiectul Planului se remite spre consultarea opiniei autorităților și instituțiilor publice responsabile de răspunsul la incidentele cibernetice și gestionarea crizelor cibernetice, persoanelor juridice care dețin infrastructuri critice și altor părți interesate, vizate în proiectul Planului sau cu competențe conexe cu procesul de gestionare a crizelor cibernetice.

40. Secretariatul Grupului de lucru definitivează proiectul Planului în conformitate cu propunerile acceptate ale opiniilor recepționate, pregătește sinteza acestor opinii, care trebuie să conțină rezultatul examinării propunerilor înaintate.

41. Atunci când e necesar, Agenția poate organiza, pe platforma Grupului de lucru, ședințe de lucru cu autoritățile și instituțiile publice și alte părți interesate, ale căror propuneri la proiectul Planului nu au fost acceptate, pentru a soluționa divergențele apărute. După definitivare, proiectul Planului se supune validării în cadrului Grupului de lucru și se înaintează spre aprobare directorului Agenției.

Secțiunea 6. Etapa aprobării Planului

42. Directorul Agenției aprobă și distribuie Planul tuturor persoanelor juridice de drept public și privat, cărora le sunt atribuite roluri și responsabilități în răspunsul la incidente cibernetice și gestionarea crizelor cibernetice vizate de Plan.

43. Persoanele juridice menționate la pct.42 nu au dreptul să distribuie mai departe Planul sau prevederi din cadrul acestuia și sunt obligate să asigure protecția accesului la Plan.

44. Directorul Agenției poate decide motivat distribuirea Planului sau anumitor părți ale acestuia și altor persoane juridice care nu sunt vizate direct în Plan, însă a căror participare la răspunsul la incidentul cibernetic și gestionarea crizei cibernetice ar putea fi justificată operațional din perspectiva rezultatelor evaluării riscurilor și a posibilelor scenarii de escaladare în răspunsul la criză.

Capitolul IV. Actualizarea Planului

45. Planul se actualizează o dată la doi ani, în baza rezultatelor evaluării naționale de risc efectuate în temeiul prevederilor art. 6 din Legea nr. 248/2025 privind managementul situațiilor de criză, evaluării riscurilor în domeniul securității cibernetice la nivel național și evaluării riscurilor la nivelul sectoarelor și subsectoarelor critice, efectuate de către autoritățile administrației publice centrale de specialitate responsabile de realizarea politicii de stat în sectoarele și/sau subsectoarele respective, precum și atunci când intervine cel puțin una dintre următoarele circumstanțe:

45.1. modificări ale cadrului normativ și schimbări organizaționale și structurale care vizează domeniile securității cibernetice, managementului situațiilor de urgență, protecției datelor sau securității naționale, inclusiv:

45.1.1. modificări în competența autorităților și instituțiilor publice și în mecanismele de coordonare pentru gestionarea crizelor;

45.1.2. restructurări instituționale care redefinesc modelele de guvernanță în gestionarea crizelor cibernetice și răspunsul la incidentele cibernetice;

45.2. producerea unor incidente cibernetice sau crize cibernetice din analiza cărora rezultă deficiențe semnificative în procedurile și mecanismele de gestionare a crizelor cibernetice și răspuns la incidentele cibernetice.

45.3. Schimbări ale mecanismelor existente sau apariția unor noi mecanisme de cooperare la nivel bilateral, regional sau internațional, la care Republica Moldova este parte.

46. Agenția inițiază actualizarea Planului în termen de 30 de zile din momentul survenirii cel puțin a uneia dintre circumstanțele ce constituie temei de actualizare a Planului, și asigură aprobarea și distribuirea Planului actualizat în termen de 6 luni de la data inițierii actualizării.

47. Autoritățile și instituțiile publice cu responsabilități în răspunsul la incidentele cibernetice și gestionarea crizelor de securitate cibernetică remit Agenției o notificare motivată privind necesitatea inițiereii actualizării Planului în cazul apariției unor circumstanțe care ar putea constitui temei de actualizare a acestuia, în termen de 5 zile de la constatarea circumstanțelor respective.

48. Divergențele dintre autoritățile și instituțiile publice responsabile conform Planului de răspunsul la incidentele cibernetice și gestionarea crizelor cibernetice, inclusiv refuzul Agenției de a iniția actualizarea Planului urmare a unei notificări înaintate potrivit pct. 47, se soluționează de către Centrul Național de Management al Crizelor prin decizie motivată a directorului general.

Capitolul V. Implementarea Planului

49. Activitățile de implementare a Planului au ca scop operaționalizarea măsurilor prevăzute de acesta prin stabilirea unui sistem coerent de acțiuni și mecanisme eficiente de cooperare interinstituțională, cu roluri și responsabilități clare, orientate spre atingerea obiectivelor stabilite de Plan.

50. Implementarea prevederilor Planului presupune un proces cu caracter continuu aferent gestionării crizelor cibernetice urmând a fi aplicate în toate fazele: de prevenire, pregătire, răspuns și recuperare.

51. În faza de prevenire, implementarea Planului are ca scop diminuarea probabilității producerii unor incidente cibernetice și escaladării acestora în crize cibernetice prin consolidarea rezilienței și a mecanismelor de protecție, inclusiv prin:

51.1. Dezvoltarea unor programe naționale de reducere a riscurilor de securitate cibernetică, în baza rezultatelor evaluării riscurilor la nivel național, sectorial sau subsectorial și a priorităților strategice ale sectoarelor critice;

51.2. Implementarea mecanismelor de monitorizare și avertizare timpurie pentru identificarea și semnalarea activităților cibernetice anormale;

51.3. Consolidarea capacităților echipei naționale, echipei guvernamentale, echipelor sectoriale de răspuns la incidente cibernetice sau echipelor instituite la nivelul furnizorilor de servicii

52. În faza de pregătire, implementarea Planului presupune creșterea nivelului de pregătire a autorităților și instituțiilor publice și a altor părți interesate responsabile de gestionarea crizelor și include, dar fără a se limita la acțiuni privind:

52.1. testarea și actualizarea procedurilor standard de operare;

52.2. aprobarea unui program multianual de exerciții de răspuns la incidente cibernetice semnificative și de mare amploare și de gestionare a crizelor cibernetice;

52.3. crearea și menținerea unei baze de date naționale a resurselor (experți, echipamente, infrastructuri) care ar putea fi mobilizate pentru răspunsul la incidente cibernetice și gestionarea crizelor cibernetice;

52.4. elaborarea unor planuri sectoriale de răspuns la incidente cibernetice și crize cibernetice, corelate și integrate cu Planul național;

52.5. organizarea și desfășurarea în mod planificat a programelor de formare și certificare profesională în domeniul securității cibernetice pentru personalul autorităților și instituțiilor publice implicat în gestionarea crizelor cibernetice;

53. În faza de răspuns, implementarea Planului presupune executarea procedurilor operaționale stabilite de acesta, prin convocarea structurilor de coordonare necesare.

54. Implementarea Planului în faza de recuperare după criza cibernetică include cel puțin:

54.1. evaluarea impactului crizei cibernetice,

54.2. restabilirea rețelelor și sistemelor informatice afectate,

54.3. asigurarea continuității serviciilor esențiale,

54.4. întocmirea unui raport post-incident și/sau post-criză

54.5. înaintarea propunerilor de actualizare a Planului, după necesitate;

54.6. asigurarea schimbului de bune practici.

55. Agenția asigură coordonarea măsurilor de implementare printr-o abordare sistemică, conform prevederilor Planului și în corelare cu analiza dinamicii și evoluției riscurilor, amenințărilor și vulnerabilităților în domeniul securității cibernetice.

56. Autoritățile și instituțiile publice cu roluri și responsabilități în răspunsul la incidente și crize cibernetice sunt responsabile de întreprinderea măsurilor necesare pentru a asigura implementarea prevederilor Planului, în conformitate cu competența cu care sunt învestite potrivit cadrului normativ.

57. Furnizorii de servicii în sectoarele critice și alte părți interesate sunt responsabili de asigurarea implementării Planului în limitele stabilite de acesta și cadrului normativ relevant.

58. Agenția asigură implementarea unor mecanisme de monitorizare continuă, evaluare și raportare a procesului de implementare a Planului.

Nota de fundamentare

la proiectul hotărârii Guvernului privind aprobarea Regulamentului cu privire la elaborarea, actualizarea și implementarea prevederilor planului național de răspuns la incidentele cibernetice și crizele în domeniul securității cibernetice

1. Denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului normativ
Proiectul hotărârii Guvernului este elaborat de către Ministerul Dezvoltării Economice și Digitalizării, în calitate de autoritate a administrației publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul securității cibernetice.
2. Condițiile ce au impus elaborarea proiectului actului normativ
2.1. Temeiul legal sau, după caz, sursa proiectului actului normativ
Temeiul legal al elaborării și adoptării proiectului de act normativ îl constituie prevederile art. 9 alin. (3) din Legea nr. 48/2023 privind securitatea cibernetică (în continuare – Legea nr. 48/2023). Aceste norme stabilesc în competența Guvernului stabilirea cadrului normativ metodologic privind elaborarea, actualizarea și implementarea prevederilor planului național de răspuns la incidentele cibernetice și crizele în domeniul securității cibernetice, privind interacțiunea dintre autoritățile și instituțiile publice cu responsabilități în procesul de elaborare și actualizare a planului respectiv și interacțiunea acestora cu sectorul privat. Proiectului de act normativ este prevăzut și de punctul 53 nr. 33 din capitolul 10 - Societatea informațională și mass-media al Clusterului 3 – Competitivitate și creștere incluzivă din Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029.
2.2. Descrierea situației actuale și a problemelor care impun intervenția, inclusiv a cadrului normativ aplicabil și a deficiențelor/lacunelor normative
Între anii 2018 și 2024, statele membre ale Uniunii Europene au raportat un total de 5108 de incidente cibernetice cu impact semnificativ[1], conform criteriilor stabilite de Directiva NIS1[2], Codul[3] european al comunicațiilor electronice și Regulamentul eIDAS[4]. Dintre acestea, 29 % au fost considerate acțiuni rău intenționate. Cel mai afectat sector a fost sectorul privat, în special domeniile comunicațiilor, bancar, sănătate, servicii de încredere, transporturi și energie. Datele indică o tendință generală de creștere a numărului de incidente cu impact semnificativ (figura 1). Din cele 1402 de incidente rău intenționate raportate, majoritatea

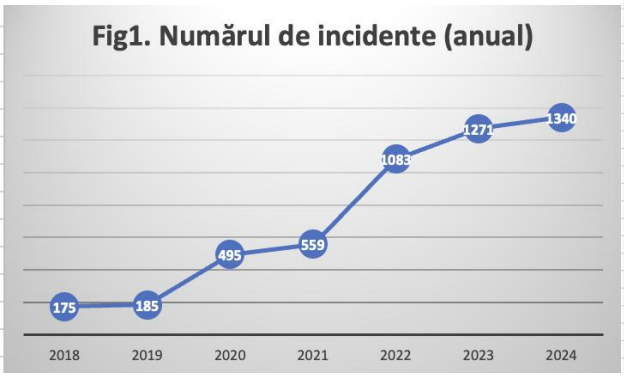
[1] https://ciras.enisa.europa.eu/ciras-consolidated-reporting

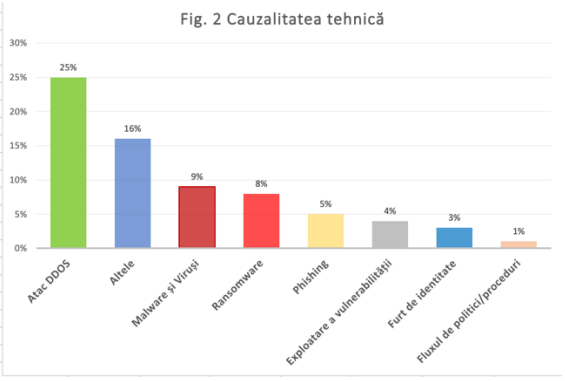
[2] Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32016L1148

[3] Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018 de instituire a Codului european al comunicațiilor electronice: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:02018L1972-20241018

[4] Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:02014R0910-20241018

au fost clasificate ca infracțiuni cibernetice, conform graficului de cauzalitate tehnică prezentat în figura 2.



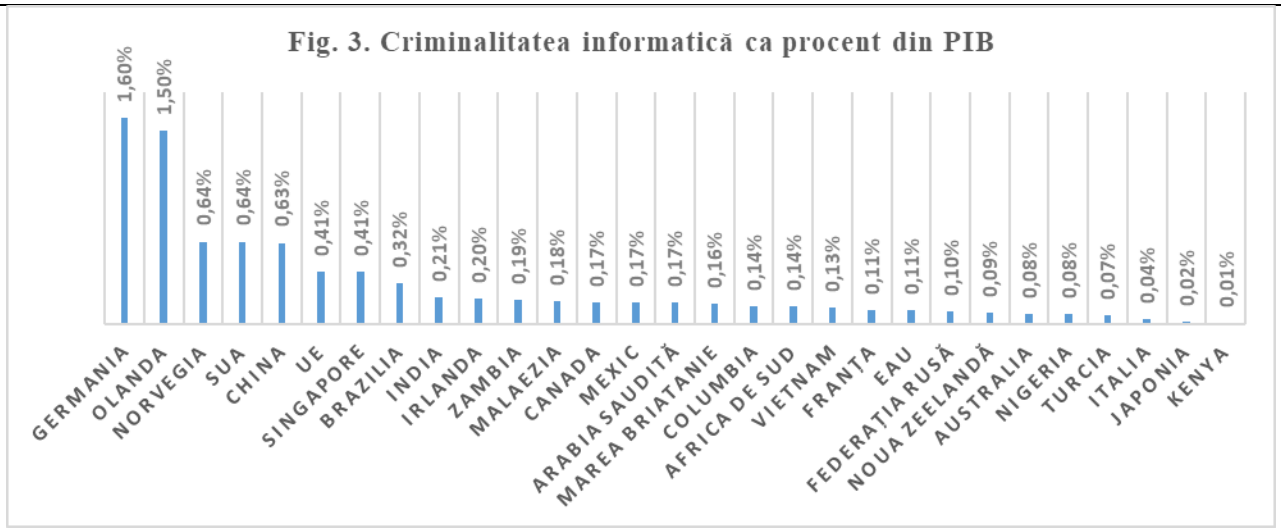


Sursa: Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA)

Conform *raportului actualizat al IBM privind costul unei încălcări a securității datelor în 2024*[5] , impactul financiar al încălcărilor securității datelor este și mai mare pentru entitățile critice. Raportul indică faptul că, în 2024, costul mediu global al unei încălcări a securității datelor a atins un nivel record de 4,88 milioane de dolari SUA, înregistrând o creștere de 10% față de 2023

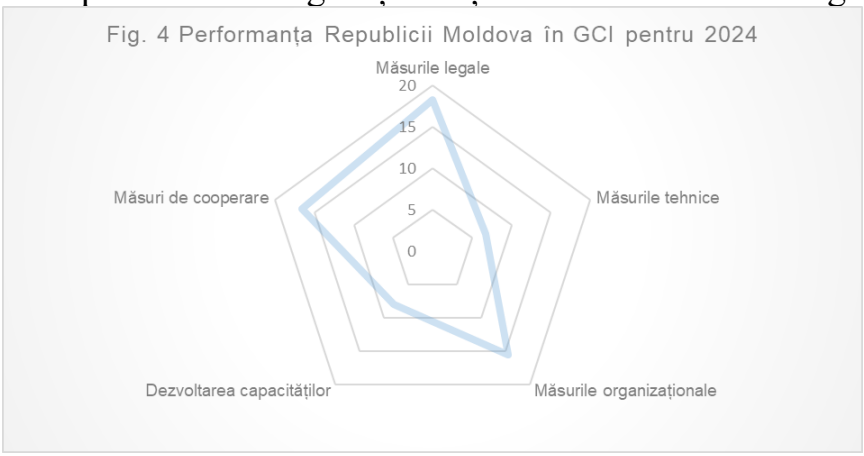
Studiul global realizat de compania McAfee[6] , care a evaluat pierderile economice cauzate de criminalitatea informatică, intitulat "Pierderi nete: estimarea costului global al criminalității informatice", oferă o estimare a impactului economic al criminalității informatice pentru diferite țări, exprimat ca procent din PIB. Graficul prezentat în figura 3 evidențiază țările cele mai grav afectate în funcție de proporția daunelor monetizate în raport cu PIB-ul lor. În medie, pierderile cauzate de criminalitatea cibernetică reprezintă aproximativ 0,3% din PIB. Extrapolând aceste date pentru Republica Moldova, având în vedere că produsul intern brut al țării a fost de aproximativ 16,5 miliarde de dolari americani în 2023, se poate estima un prejudiciu anual potențial de aproximativ 49 de milioane de dolari, pe baza mediei de 0,3% din PIB.

[5] https://www.ibm.com/reports/data-breach
[6] https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis



Sursa: Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA)

Conform Indicelui Global de Securitate Cibernetică (GCI) al UIT pentru 2024, Republica Moldova are un scor general de 65,09, iar performanța țării este descrisă ca fiind de nivel 3 (nivelul 3 reprezintă țările care au obținut un scor general de cel puțin 55/100), demonstrând un angajament de bază în materie de securitate cibernetică, care include evaluarea, stabilirea sau implementarea anumitor măsuri de securitate cibernetică general acceptate, pe un număr moderat de piloni sau indicatori. Conform raportului UIT privind echipa națională de răspuns la incidente de securitate cibernetică, performanța Republicii Moldova pentru 2024, comparativ cu 2020, a înregistrat o creștere a măsurilor legale, organizaționale și de cooperare, însă o scădere notabilă a măsurilor tehnice și de dezvoltare a capacităților, dar acest lucru poate fi atribuit parțial ajustărilor metodologice și ponderilor GCI, precum și modificărilor aduse întrebărilor. Graficul de mai jos (Figura 4) evidențiază performanța Republicii Moldova în GCI pentru 2024, subliniind că măsurile tehnice și consolidarea capacităților sunt punctele slabe ale Republicii Moldova în acest domeniu. Cu toate acestea, acest indice poate fi îmbunătățit prin implementarea corespunzătoare a legislației naționale armonizate cu legislația UE.



Industria IT în Republica Moldova se dezvoltă rapid. În 2023, industria IT a atins o pondere de peste 5,3% din produsul intern brut, depășind 15 miliarde de lei în vânzări,

ponderea sectorului TIC este de peste 8,3% din PIB, cu peste 25 de miliarde de lei în vânzări în 2023, realizate de aproximativ 3 200 de companii cu peste 35 000 de angajați. Creșterea în sectorul IT a fost generată de avantajele pe care Moldova le oferă ca destinație pentru externalizarea serviciilor IT, beneficiind de costuri competitive, amplasare geografică favorabilă și calificări ale forței de muncă, alături de un cadru fiscal și administrativ facil pentru rezidenții Parcului IT Virtual Moldova. Rapoartele globale referitoare la digitalizare (cum ar fi Indicele UN DESA e-Guvernare, Indicele de Dezvoltare în Rețea NRI, Indicele Țării Digitale etc.), rapoartele emise de ANRCETI și sondajele anuale efectuate de Agenția de Guvernare Electronică (AGE) confirmă progresele semnificative ale Republicii Moldova în privința accesului la internet și utilizarea dispozitivelor IT, precum și dezvoltarea platformelor de e-guvernare.

Cu toate acestea, avansul rapid al tehnologiei informației și comunicațiilor electronice și al proceselor de transformare digitală, deși aduce beneficii incontestabile în diverse domenii, este însoțit de o creștere semnificativă și continuă a amenințărilor la adresa securității cibernetice. Reieșind din acestea, securitatea cibernetică a fost declarată ca fiind o prioritate la nivel național, acest aspect fiind reflectat într-un set de documente de politici, cum ar fi:

- ***Programul național de aderare a Republicii Moldova la Uniunea Europeană* pentru perioada 2025-2029**[7] acordă prioritate punerii în aplicare a Legii 48/2023 privind securitatea cibernetică, în special identificării furnizorilor de servicii critice și punerii în aplicare a cerințelor de securitate pentru rețele și sisteme informatice, precum și operaționalizării complete a Agenției pentru Securitate Cibernetică. Hotărârea Guvernului nr. 562/2025 „Cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice", care include în obiectul său de reglementare și cerințele de securitate pentru rețele și sisteme informatice, este în proces de promovare, urmând în timpul apropiat să fie supus examinării de către Guvern. Aceasta determină necesitatea consolidării capacităților furnizorilor de servicii din sectoarele critice, deoarece aceștia au nevoie de formare în ceea ce privește modul de punere în aplicare a cerințelor de securitate cibernetică și de respectare a cadrului normativ în domeniu.
- ***Strategia de transformare digitală a Republicii Moldova pentru anii 2023-2030***[8]***:*** unul dintre obiectivele acesteia este crearea unui mediu digital accesibil, sigur și incluziv, având ca scop asigurarea unei creșteri a nivelului de reziliență cibernetică a entităților-cheie din Republica Moldova. Aceste entități urmează fi gestionate mult mai eficient și transparent, iar incidentele cibernetice, precum și eventualele prejudicii materiale și reputaționale asociate acestora, vor fi evitate. În același timp, se urmărește implementarea unei abordări multidisciplinare, iar toate părțile interesate, inclusiv Guvernul, sectorul privat și societatea civilă, își vor asuma

[7] https://www.legis.md/cautare/getResults?doc_id=148720&lang=ro
[8] https://www.legis.md/cautare/getResults?doc_id=139408&lang=ro

responsabilitatea și angajamentul comun pentru susținerea și cooperarea în asigurarea securității cibernetice.

- ***Strategia securității naționale a Republicii Moldova***[9], care evidențiază riscurile cibernetice la care este expusă Republica Moldova, subliniind în principal atacurile cinetice sau cibernetice lansate de actori statali externi asupra infrastructurii critice naționale și regionale, atacurile cibernetice lansate asupra instituțiilor publice sau private de către structuri specializate în criminalitatea cibernetică, precum și riscurile asociate evoluțiilor din domeniul tehnologiilor precum blockchain și criptomonede, inteligența artificială, învățarea automată, internetul obiectelor, tehnologia 5G, big data, tehnologiile cuantice, internetul ascuns.

La data de 1 ianuarie 2025 a intrat în vigoare Legea nr. 48/2023 privind securitatea cibernetică. Legea are ca obiectiv general să asigure legalitatea în spațiul cibernetic prin reglementarea principalelor elemente indispensabile implementării unui model de guvernanță eficient la nivel național în vederea protecției și asigurării securității rețelelor și sistemelor informatice, utilizate de către persoanele juridice, publice sau private, în procesul de prestare a serviciilor considerate a fi esențiale pentru susținerea unor activități societale și economice critice. Un instrument juridic esențial asumat în procesul reglementării acestui domeniu a constituit legislația Uniunii Europene, inclusiv în contextul obținerii de către Republica Moldova a statutului de țară candidat la aderarea la Uniunea Europeană, prin Legea respectivă asigurându-se armonizarea parțială a cadrului normativ național la prevederile Directivei NIS2[10].

Unul dintre aspectele de bază concepute normativ la nivel primar în Legea nr. 48/2023 îl constituie reglementarea procesului de coordonare și gestionare a crizelor în domeniul securității cibernetice. Potrivit art. 9 alin. (1) autoritatea publică responsabilă de gestionarea incidentelor cibernetice și a crizelor în domeniul securității cibernetice la nivel național este Agenția pentru Securitate Cibernetică – autoritate competentă în domeniul securității cibernetice, constituită și desemnată de Guvern în această calitate prin Hotărârea Guvernului nr. 1028/2023 ”Cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică”.

Același articol 9 din Legea nr. 48/2023 în alineatul (2) învestește Agenția pentru Securitate Cibernetică cu prerogativa de elaborare și aprobare a planului național de răspuns la incidentele cibernetice și crizele în domeniul securității cibernetice în care urmează a fi stabilite obiectivele și modalitățile de gestionare a incidentelor și a crizelor respective la nivel național. Din perspectiva conținutului acestui plan, alineatul (3) determină în mod generic principalele problematici care urmează a fi abordate. Modalitatea în care planul național urmează a fi elaborat, procesul propriu-zis și

[9] https://www.legis.md/cautare/getResults?doc_id=141253&lang=ro

[10] ***Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului*** din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148;

prerogativele actorilor implicați în acesta, potrivit alin. (4) urmează a fi detaliate într-un act normativ de către Guvern.

La data de 1 septembrie a intrat în vigoare Legea nr. 248/2025 privind managementul situațiilor de urgență. Legea instituie cadrul legal pentru asigurarea managementului situațiilor de criză și stabilește modul de realizare și de coordonare a măsurilor întreprinse de autoritățile și instituțiile publice, operatorii economici și de organizațiile necomerciale pentru a asigura prevenirea, pregătirea, răspunsul la și recuperarea după situații de criză în beneficiul protejării populației, a ordinii publice și a altor domenii ale securității naționale. În contextul fazelor de prevenire și pregătire pentru crize, legea respectivă stabilește în responsabilitatea autorităților și instituțiilor publice elaborarea și aprobarea planurilor sectoriale de management al crizelor, în baza unei metodologii de întocmire a planurilor sectoriale de management al crizelor, ce urmează a fi aprobată de Guvern.

Convergența prevederilor acestor două legi în reglementarea modului de elaborare a planurilor sectoriale de management al crizelor trebuie privită prin prisma relației lege generală - lege specială, în acest caz, prevederile citate mai sus ale Legii securității cibernetice fiind o lege specială în raport cu prevederile similare ale Legii privind managementul situațiilor de criză.

Proiectul de act normativ propus nu este generat ca urmare a identificării unei probleme noi, ci este o măsură care se înscrie în spectrul de acțiuni orientate spre constituirea cadrului normativ în domeniul securității cibernetice necesar asigurării implementării prevederilor Legii nr. 48/2023. **Problema principală** care urmează a fi soluționată prin inițiativa propusă este cea stabilită în analiza de impact la proiectul de lege privind securitatea cibernetică și rezidă în nivelul general insuficient de protecție împotriva incidentelor, riscurilor și amenințărilor legate de securitatea rețelelor și a sistemelor informatice, ceea ce poate submina buna funcționare, pe de o parte, a activității administrative, în mod special prestarea serviciilor publice, de către administrația publică centrală și locală, iar pe de altă parte buna funcționare a activității economice desfășurată de către întreprinderile din mediul privat, ceea ce afectează în consecință întreaga economie națională și, implicit, activitatea socială. În legătură directă cu obiectul de reglementare a proiectului de act normativ propus spre examinare, următoarele principale **probleme specifice** ce urmează a fi soluționate prin acesta intervenție ar putea fi evidențiate următoarele:

- Mecanisme insuficiente de coordonare a activităților de răspuns la incidentele cibernetice și gestionarea crizelor cibernetice;
- Lipsa unei definiri cuprinzătoare a conceptului de incident cibernetic, incident cibernetic semnificativ, incident cibernetic de mare amploare și criză cibernetică care constituie fundamentul primordial al activării diferitelor moduri de operare și escaladării la nivelurile corespunzătoare de gestionare.
- Capacități și mecanisme de cooperare limitate în procesul de răspuns la crizele cibernetice;

- Lipsa unei integrări efective a mecanismelor și instrumentelor de răspuns la incidentele și cibernetice și gestionare a crizelor cibernetice în sistemul național de management al crizelor.

Cercul de subiecți interesați în intervenția propusă poate fi grupat în următoarele categorii:

1. ***Guvernul și Ministerul Dezvoltării Economice și Digitalizării, în calitatea sa de autoritate a administrației publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul securității cibernetice*** – din perspectiva, pe de o parte, a necesității instituirii unui mecanism instituțional și organizațional viabil de implementare a politicii de stat în domeniul securității cibernetice, în vederea asigurării rezilienței cibernetice a cercului de subiecți care cad sub incidența actului normativ, iar, pe de altă parte – necesitatea armonizării cadrului normativ național la aquis-ul Uniunii Europene;
2. ***Autoritățile și instituțiile publice și autoritățile publice locale*** – atât din perspectiva determinării clare a responsabilităților partajate în cadrul mecanismelor de gestionare a crizelor, cât și din punctul de vedere a formalizării unor procedurilor operaționale de interacțiune atât în interiorul sectorului public, cât și cu
3. ***Furnizorii de servicii în sectoarele critice***, din perspectiva rolului și responsabilității primordiale pe care îl au în răspunsul la incidente și crize cibernetice, inclusiv din punctul de vedere al aplicării principiului subsidiarității;
4. ***Persoanele juridice de drept privat,*** altele decât furnizorii de servicii, care, deși nu intră în domeniul de aplicare a Legii securității cibernetice, din punctul de vedere al resurselor disponibile ar putea avea u rol în gestionarea crizelor de securitate cibernetic**.**
5. ***Utilizatorii finali ai serviciilor*** prestate de furnizorii de servicii, esențiali sau importanți, din perspectiva interesului pe care îl au în creșterea calității serviciilor de care beneficiază, în mod special din punctul de vedere al securității și protecției datelor cu caracter personal, dar și a continuității prestării acestor servicii în situații de criză cibernetică sau incidente cibernetice.

3. Obiectivele urmărite şi soluţiile propuse

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

Proiect de hotărâre de Guvern va contribui la realizarea **obiectivul general al întregului cadru normativ în domeniul securității cibernetice** și anume de creștere a nivelului de reziliență cibernetică a furnizorilor de servicii, privați sau publici, asigurând un nivel ridicat de protecție a rețelelor și sistemelor informatice ale acestor furnizori utilizate în procesul de prestare de către aceștia a serviciilor esențiale.

Ca **obiective specifice** ale proiectului de hotărâre de Guvern sunt crearea mecanismelor de interacțiune între entitățile cu competențe sau activități în domeniul securității cibernetice și protecției infrastructurii critice, în vederea elaborării, menținerii în stare de actualitate și implementare a Planului național de răspuns la incidente cibernetice și gestionare a crizelor în domeniul securității cibernetice.

Proiectul de act normativ are ca **obiect de reglementare** cerințele față de conținutul Planului național de răspuns la incidentele cibernetice și crizele în domeniul securității cibernetice, procesul de elaborare, inclusiv etapele acestui proces, modul de actualizare și implementare a Planului, atribuțiile autorităților și instituțiilor publice în acest proces, drepturile și obligațiile persoanelor juridice implicate în procesul de elaborare, actualizare și implementare a Planului, precum și procedurile de interacțiune dintre acestea.

Domeniul de aplicare al proiectului propus spre examinare se extinde asupra autorităților și instituțiilor publice cu competențe în gestionarea crizelor de securitate cibernetică, furnizorilor de servicii, esențiali sau importanți, asupra altor persoane juridice de drept privat, care deși nu sunt identificate în calitate de furnizori de servicii, totuși ar putea dispune de resurse pertinente procesului de răspuns la un incidente cibernetic semnificativ sau de mare amploare care poate escalada într-o criză cibernetică.

Din punct de vedere structural, proiectul include partea dispozitivă a hotărârii de Guvern și anexa.

Partea dispozitivă cuprinde decizia Guvernului de adoptare a regulamentului în speță și sarcini Agenției pentru Securitate Cibernetică de elaborare și aprobare a Planul în termen de 12 luni de la data intrării în vigoare a actului normativ, precum și entităților publice și private relevante să acorde suportul necesar Agenției pentru Securitate Cibernetică în acest proces.

De asemenea, se prevede intrarea în vigoare a hotărârii de Guvern la data publicării în Monitorul Oficial al Republicii Moldova, reieșind din faptul că proiectul menționat este inclus în documentele strategice ale Republicii Moldova, și anume Agenda de reforme aferente Planului de creștere al Republicii Moldova pentru anii 2025–2027 (aprobat prin Hotărârea Guvernului nr. 260/2025) și Foaia de parcurs privind „Statul de drept”, care constituie un criteriu de referință în procesul de aderare a Republicii Moldova la Uniunea Europeană (aprobată prin Hotărârea Guvernului nr. 275/2025), având termen de realizare anul 2025.

Anexa cuprinde Regulamentul privind aprobarea Regulamentului cu privire la elaborarea, actualizarea și implementarea Planului național de răspuns la incidentele cibernetice și crizele cibernetice. Acesta include patru capitole.

Capitolul I – Dispoziții generale – determină noțiunile și definițiile acestora utilizate în textul proiectului de act normativ, precum și principiile de bază care guvernează nemijlocit procesul de elaborare, actualizare și implementare a Planului.

Capitolul II – Conținutul Planului – detaliază prevederile art. 9 alin. (3) ale Legii nr. 48/2023 privind securitatea cibernetică, prevederi care la rândul lor constituie o materializare a procesului de armonizare a legislației naționale la Directiva NIS2, în speță art. 9 alin. (4) din această Directivă.

Capitolul este divizat în șapte secțiuni, câte o secțiune dedicată fiecărei problematici abordate în art. 9 alin. (3) din legea nr. 48/2023. În context, ținem să evidențiem faptul că descrierea conținutului planului conform problematicilor abordate de lege, în consecutivitatea propusă în proiect nu constituie vreo limitare a discreției Agenției în

organizarea conținutului Planului conform unei structuri prestabilite. Agenția dispune de o marjă discreționară destul de largă în alegerea opțiunii celei mai viabile pentru structurarea acestui conținut. În același timp este important de relevat faptul că Agenția nu este constrânsă în a include în plan și alte problematici relevante obiectului de reglementare al Planului și nici de anvergura detalierii problematicilor abordate deja în proiectul de act normativ.

Capitolul III – Elaborarea Planului – determină și descrie cele 5 etape de elaborare a Planului:

a) *Etapa de inițiere a elaborării care include definirea cadrului instituțional și metodologic, constituirea, la nivel operațional, a Grupului de lucru interinstituțional pentru elaborarea și actualizarea Planului;*

b) *Etapa de colectare și analizare a informațiilor care include activități de analiză a cadrului juridico-normativ, instituțional și de planificare strategică, evaluare a riscurilor amenințărilor cibernetice și a vulnerabilităților, colectare a informațiilor despre capacitățile existente, infrastructurile critice și interdependențele dintre acestea, organizarea de consultări cu părțile interesate relevante;*

c) *Etapa de întocmire a textului Planului – în cadrul căreia se întocmește textul propriu-zis al planului;*

d) *Etapa aprobării Planului – include aspecte de aprobare de către directorul Agenției a Planului, precum și aspecte privind aducerea la cunoștință a textului Planului părților interesate.*

Capitolul IV - Actualizarea Planului – stabilește termenul maxim de actualizare care este doi ani. Totodată, excepție de la această regulă o constituie intervenirea anumitor circumstanțe care constituie temeiuri de revizuire și actualizare a planului.

Capitolul V - Implementarea Planului – cuprinde reglementări care vizează activitatea autorităților și instituțiilor responsabile de punere în aplicare a prevederilor Planului. Reglementările sunt structurate în funcție de fazele de gestionare a unei crize: prevenire, pregătire, răspuns și recuperare.

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

Opțiunile alternative nu au fost luate în considerare deoarece la nivel de lege este stabilită obligația Guvernului de a aproba cerințe privind măsurile de securitate a rețelelor și sistemelor informatice ale furnizorilor de servicii.

4. Analiza impactului de reglementare

4.1. Impactul asupra sectorului public

Proiectul de act normativ nu implică impacturi structurale și instituționale asupra sistemului administrației publice, inclusiv acțiuni de reformă structurală sau instituțională.

4.2. Impactul financiar și argumentarea costurilor estimative

Proiectul de act normativ nu implică un impactul financiar direct asupra mediului de afaceri și nici costurile administrative directe ce urmează a fi suportate de către agenții economici. Informațiile necesare pentru elaborarea planului național de răspuns la

incidentele cibernetice și crizele cibernetice, disponibile la furnizorii de servicii în sectoarele critice, urmează a fi prezentate în contextul realizării de către aceștia a obligațiilor de asigurare a securității cibernetice, stabilite de Legea nr. 48/2025 și dezvoltate în Hotărârea Guvernului nr. 562/2025.

Activitatea Agenției în exercitarea rolului său de coordonare în elaborarea planului și ale altor autorități și instituții publice urmează a se efectua în limita mijloacelor financiare aprobate acestor autorități și instituții publice în bugetul de stat.

4.3. Impactul asupra sectorului privat

Sub aspectul impacturilor non-financiare asupra sectorului privat ținem să relevăm în mod special că proiectul de act normativ propus spre examinare va contribui la:

- Consolidarea rezilienței și securității cibernetice în ansamblu: proiectul de act normativ va contribui la crearea unor mecanisme eficiente de coordonare la nivel național a situațiilor de criză în domeniul securității cibernetice, ceea ce va îmbunătăți interacțiunea dintre diferite entități implicate în răspunsul la incidente și crize cibernetice;
- Protecția informațiilor și a drepturilor utilizatorilor: implementarea soluției va spori protecția informațiilor personale și a drepturilor utilizatorilor, prevenind accesul neautorizat și utilizarea abuzivă a datelor;
- Siguranța infrastructurii critice: proiectul va contribui într-un mod indirect la protecția infrastructurii critice, reducând riscul de întreruperi majore și asigurând continuitatea serviciilor esențiale;
- Îmbunătățirea cooperării dintre autoritățile publice responsabile și furnizorii de servicii în sectorul privat în implementarea cerințelor de securitate a rețelelor și sistemelor informatice, aprobate prin Hotărârea Guvernului nr. 562/2025, în vederea asigurării unei pregătiri corespunzătoare pentru situații în care va fi necesar răspunsul la incidente semnificative, de mare amploare și la crize cibernetice.

4.4. Impactul social

4.4.1. Impactul asupra datelor cu caracter personal

Din perspectiva datelor cu caracter personal prevederile proiectului de act normativ va avea un impact pozitiv, având în vedere că acesta are ca obiectiv ridicarea nivelului de securitate a rețelelor și sistemelor informatice ale furnizorilor de servicii esențiale.

4.4.2. Impactul asupra echității și egalității de gen

Nu este aplicabil.

4.5. Impactul asupra mediului

Nu este aplicabil.

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
Nu este aplicabil.
6. Avizarea și consultarea publică a proiectului actului normativ
În conformitate cu prevederile art. 9 din Legea nr. 239/2008 privind transparența în procesul decizional, la data de 27.10.2025 a fost publicat anunțul referitor la inițierea procesului de elaborare a proiectului de hotărâre de Guvern pe pagina web oficială a Ministerului Dezvoltării Economice și Digitalizării mded.gov.md și pe platforma de consultare particip.gov.md (https://particip.gov.md/ro/document/stages/anunt-privind-initierea-procesului-de-elaborare-a-proiectului-hotararii-de-guvern-cu-privire-la-aprobarea-cadrului-normativ-privind-elaborarea-actualizarea-si-implementarea-prevederilor-planului-national-de-raspuns-la-incidentele-cibernetice-si-crizele-in-domeniul-securitatii-cibernetice/15367).
7. Concluziile expertizelor
Proiectul de act normativ urmează a fi supus expertizei anticorupție și expertizei juridice conform procedurii stabilite de cadrul normativ.
8. Modul de încorporare a actului în cadrul normativ existent
Adoptarea și intrarea în vigoare a proiectului nu va necesita modificarea cadrului normativ existent. Pentru implementarea proiectului de act normativ Agenția urmează să elaboreze și să adopte Planul național de răspuns la incidente și crize cibernetice și să emită un act administrativ de constituie a Grupului de lucru pentru elaborarea Planului respectiv.
9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ
Autoritatea publică principală responsabilă de asigurarea implementării proiectului de act normativ este Agenția pentru Securitate Cibernetică. Pentru a asigura punerea în aplicare a prevederilor proiectului propus spre examinare, Agenția urmează, inclusiv în comun cu alte autorități și instituții publice: - să elaboreze și să aprobe Planul național de răspuns la incidentele cibernetice și crizele în domeniul securității cibernetice; - să constituie Grupul de lucru pentru elaborarea planului respectiv și să-i asigure activitatea prin exercitarea rolului de secretariat al acestuia; - să desfășoare consultări preliminare elaborării planului; - să aprobe proceduri operaționale necesare pentru implementarea prevederilor Planului.

Secretar de Stat **Michelle ILIEV**