UE

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. ____

din 2025

Chișinău

Cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice

---

În temeiul art. 3 alin. (7), art. 11, art. 12 alin. (9), art. 14 alin. (2) și art. 23 alin. (2) lit. c) din Legea nr. 48/2023 privind securitatea cibernetică (Monitorul Oficial al Republicii Moldova, 2023, nr. 151-153, art. 225), cu modificările ulterioare, Guvernul HOTĂRĂȘTE:

Prezenta hotărâre transpune parțial Regulamentul de punere în aplicare (UE) 2024/2690 al Comisiei din 17 octombrie 2024 de stabilire a normelor de aplicare a Directivei (UE) 2022/2555 în ceea ce privește cerințele tehnice și metodologice ale măsurilor de gestionare a riscurilor în materie de securitate cibernetică și specificarea suplimentară a cazurilor în care un incident este considerat semnificativ referitor la furnizorii de servicii DNS, registrele de nume TLD, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea, precum și prestatorii de servicii de încredere, publicat în Jurnalul Oficial al Uniunii Europene L din 18 octombrie 2024, CELEX: 32024R2690.

1. Se aprobă Regulamentul cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice (se anexează).

2. Furnizorii esențiali de servicii:

2.1. vor asigura punerea în aplicare a prevederilor prezentei hotărâri în termen de 12 luni de la data intrării în vigoare a acesteia;

2.2. în termen de 6 luni de la data intrării în vigoare a prezentei hotărâri, în conformitate cu prevederile corespunzătoare ale Regulamentului cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice, vor efectua analiza riscurilor la adresa

securității rețelelor și a sistemelor informatice proprii și vor aproba rapoarte în acest sens, precum și vor aproba planuri de tratare a riscurilor identificate și evaluate;

2.3. vor prezenta Agenției pentru Securitate Cibernetică raportul de evaluare a riscurilor și planul de tratare a riscurilor, în termen de 10 zile de la data aprobării acestora;

2.4. vor prezenta Agenției pentru Securitate Cibernetică, în termen de 18 luni de la data intrării în vigoare a prezentei hotărâri, raportul primei evaluări a conformității cu cerințele prevăzute în Regulamentul menționat, efectuată de către persoane care dețin certificări în domeniul auditului securității informațiilor.

3. Furnizorii importanți de servicii:

3.1. vor asigura punerea în aplicare a prevederilor prezentei hotărâri în termen de 18 luni de la data intrării în vigoare a acesteia;

3.2. în termen de 9 luni de la data intrării în vigoare a prezentei hotărâri, în conformitate cu prevederile corespunzătoare ale Regulamentului cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice, vor efectua analiza riscurilor la adresa securității rețelelor și a sistemelor informatice proprii și vor aproba rapoarte în acest sens, precum și vor aproba planuri de tratare a riscurilor identificate și evaluate;

3.3. vor prezenta Agenției pentru Securitate Cibernetică rapoartele de evaluare a riscurilor și planurile de tratare a riscurilor, în termen de 10 zile de la data aprobării acestora;

3.4. vor prezenta Agenției pentru Securitate Cibernetică raportul primei evaluări a conformității cu cerințele prevăzute în Regulamentul menționat, în termen de 24 de luni de la data intrării în vigoare a prezentei hotărâri.

4. Agenția pentru Securitate Cibernetică:

4.1. în termen de 6 luni de la data publicării prezentei hotărâri, va asigura implementarea unor mecanisme, inclusiv prin utilizarea mijloacelor tehnice, destinate asigurării unui schimb direct, sistematic și imediat de informații în contextul realizării de către furnizorii de servicii a obligațiilor de raportare a incidentelor cibernetice cu impact semnificativ;

4.2. va acorda asistență consultativă furnizorilor de servicii, la solicitare, în procesul de evaluare a riscurilor;

4.3. în termen de 12 luni de la data expirării termenului prevăzut la subpunctul 2.4, va evalua nivelul de conformitate a furnizorilor esențiali de servicii și a operatorilor obiectivelor de infrastructură critică, inclusiv în baza rapoartelor de evaluare a riscurilor, a planurilor de tratare a riscurilor și a rapoartelor de evaluare a conformității, efectuate în temeiul subpunctelor 2.3 și 2.4, cu cerințele privind măsurile de securitate a rețelelor și a sistemelor informatice, prevăzute în Regulamentul cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în

sectoarele critice, și va înainta recomandările corespunzătoare furnizorilor de servicii evaluați;

4.4. în termen de 18 luni de la data expirării termenului prevăzut la subpunctul 3.4, va evalua nivelul de conformitate a furnizorilor importanți de servicii, inclusiv în baza rapoartelor de evaluare a riscurilor, a planurilor de tratare a riscurilor și a rapoartelor de evaluare a conformității, efectuate în temeiul subpunctelor 3.3 și 3.4, cu cerințele privind măsurile de securitate a rețelelor și a sistemelor informatice, prevăzute în Regulamentul nominalizat, și va înainta recomandările corespunzătoare furnizorilor de servicii evaluați.

5. Hotărârea Guvernului nr. 860/2024 cu privire identificarea furnizorilor de servicii (Monitorul Oficial al Republicii Moldova, 2024, nr. 548-551, art. 999) se modifică după cum urmează:

5.1. anexa nr. 1:

5.1.1. se completează cu punctul 9^1 cu următorul cuprins:

„**9^1.** Atât actul administrativ de desemnare în calitate de furnizor de servicii, cât și notificarea privind intenția de desemnare în calitate de furnizor de servicii constituie informație cu acces limitat. Modul de prelucrare a informației, precum și accesul la informația respectivă se stabilește prin ordin al directorului Agenției.”;

5.1.2. la punctul 28, textul „din Nomenclatorul național al infrastructurii critice,” se exclude;

5.2. punctul 10 din anexa nr. 3 va avea următorul cuprins:

„**10.** Lista constituie informație cu acces limitat. Modul de prelucrare a informației, precum și accesul la Listă se stabilește prin ordin al directorului Agenției.”

6. Se abrogă Hotărârea Guvernului nr. 201/2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică (Monitorul Oficial al Republicii Moldova, 2017, nr. 109-118, art. 277).

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

8. Prezenta hotărâre intră în vigoare la expirarea termenului de o lună de la data publicării în Monitorul Oficial al Republicii Moldova.

Prim-ministru **DORIN RECEAN**

Contrasemnează:

Viceprim-ministru,
ministrul dezvoltării
economice și digitalizării Doina NISTOR

Aprobat
prin Hotărârea Guvernului nr. /2025

REGULAMENT
cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice

Capitolul I
DISPOZIȚII GENERALE

1. Regulamentul cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice (în continuare – *Regulament*) are ca obiect de reglementare modul de aplicare a cerințelor privind măsurile de securitate a rețelelor și a sistemelor informatice utilizate la prestarea serviciilor esențiale, procedura de notificare a incidentelor cibernetice cu impact semnificativ, condițiile specifice pentru unele tipuri de furnizori de servicii în care un incident cibernetic urmează a fi calificat ca fiind semnificativ, precum și modul de evaluare a echivalenței efectelor legislației care reglementează activitatea furnizorilor de servicii și/sau sectoarele şi subsectoarele critice stabilite prin Hotărârea Guvernului nr. 860/2024 cu privire la identificarea furnizorilor de servicii (în continuare – *legislație sectorială*) în raport cu cele ale Legii nr. 48/2023 privind securitatea cibernetică.

2. Prezentul Regulament se aplică furnizorilor de servicii în sectoarele critice (în continuare – *furnizori de servicii*) identificați de către Agenția pentru Securitate Cibernetică (în continuare – *Agenți*e) în conformitate cu Hotărârea Guvernului nr. 860/2024 cu privire la identificarea furnizorilor de servicii.

3. În sensul prezentului Regulament, noțiunile utilizate au înțelesul stabilit în Legea nr. 48/2023 privind securitatea cibernetică și în Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat.

Capitolul II
MODUL DE APLICARE A CERINȚELOR PRIVIND MĂSURILE DE SECURITATE A REȚELELOR ȘI A SISTEMELOR INFORMATICE ALE FURNIZORILOR DE SERVICII ÎN SECTOARELE CRITICE

4. Furnizorii de servicii pot utiliza standarde și specificații tehnice naționale și internaționale, inclusiv europene, atunci când implementarea anumitor cerințe prevăzute în anexă implică necesitatea unor informații mai detaliate.

5. În baza cerințelor prevăzute în anexă, Agenția elaborează ghiduri de implementare cu caracter consultativ și furnizează orientări metodologice furnizorilor de servicii în sectoarele critice.

6. În implementarea și aplicarea măsurilor de gestionare a riscurilor în materie de securitate cibernetică, furnizorii de servicii asigură un nivel de securitate a rețelelor și a sistemelor informatice corespunzător și proporțional cu riscurile identificate.

7. Atunci când determină proporționalitatea măsurilor de securitate implementate pentru tratarea riscurilor identificate, furnizorii de servicii trebuie să țină cont în mod corespunzător de: gradul lor de expunere la riscuri, dimensiunea lor, probabilitatea apariției unor incidente, gravitatea acestora, inclusiv de impactul lor societal și economic.

8. În cazul în care anexa prevede că o cerință a unei măsuri de securitate a rețelelor și a sistemelor informatice se aplică dacă este adecvată, dacă este aplicabilă sau în măsura în care este fezabilă, iar furnizorul de servicii consideră că cerința respectivă nu este adecvată, nu este aplicabilă sau nu este fezabilă, acesta documentează într-un mod inteligibil motivarea în acest sens, informând Agenția în termen de 10 zile de la data documentării motivării de neimplementare a cerinței respective sau de aplicare a unei măsuri alternative.

9. Furnizorii de servicii efectuează audituri privind securitatea informațiilor, în vederea determinării nivelului de conformitate cu cerințele privind măsurile de securitate a rețelelor și a sistemelor informatice, prevăzute în anexă, cel puțin o dată la trei ani sau ori de câte ori este necesar în conformitate cu cerințele stabilite în anexă. Raportul de audit și rapoartele examinărilor independente, efectuate în conformitate cu capitolul II secțiunea a 3-a din anexă, se prezintă Agenției în termen de o lună de la data efectuării.

10. Cerințele prevăzute în anexă nu se aplică furnizorilor de servicii dacă măsurile de securitate implementate de furnizorul de servicii sunt conforme cu cerințele stabilite de standardul moldovenesc SM ISO/IEC 27001 și furnizorul de servicii a prezentat Agenției un certificat valabil care confirmă conformitatea cu standardul respectiv. Îndeplinirea de către furnizorul de servicii a condițiilor stabilite în prezentul punct nu exclude dreptul Agenției de a efectua o evaluare a conformității acestui furnizor de servicii cu cerințele prevăzute în anexă în exercitarea funcției de supraveghere și control de stat al modului în care sunt respectate prevederile cadrului normativ în domeniul securității cibernetice.

Capitolul III
MODUL DE EVALUARE A ECHIVALENȚEI EFECTELOR OBLIGAȚIILOR DE ASIGURARE A SECURITĂȚII CIBERNETICE

11. Dacă legislația sectorială impune furnizorilor de servicii cerințe ale măsurilor de securitate a rețelelor și a sistemelor informatice sau obligații de notificare a incidentelor cibernetice semnificative cel puțin echivalente cu cele prevăzute de Legea nr. 48/2023 privind securitatea cibernetică și de prezentul Regulament, furnizorii de servicii aplică prevederile legislației sectoriale.

12. Cerințele privind măsurile de securitate a rețelelor și a sistemelor informatice sau obligațiile de notificare a incidentelor cibernetice semnificative din legislația sectorială sunt considerate echivalente în privința efectului cu cele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și de prezentul Regulament în cazul în care:

12.1. măsurile de securitate a rețelelor și a sistemelor informatice sunt cel puțin echivalente în privința efectului cu cele prevăzute la articolul 11 alineatele (1), (2) și (3) din Legea nr. 48/2023 privind securitatea cibernetică și în prezentul Regulament;

12.2. legislația sectorială prevede accesul imediat, după caz automat și direct, al Agenției la notificările incidentelor cibernetice cu impact semnificativ și dacă obligațiile de notificare au un efect cel puțin echivalent cu cele prevăzute la articolul 12 din Legea nr. 48/2023 privind securitatea cibernetică.

13. Atunci când se evaluează dacă cerințele legislației sectoriale privind măsurile de securitate a rețelelor și a sistemelor informatice au un efect cel puțin echivalent cu cele prevăzute de Legea nr. 48/2023 privind securitatea cibernetică și de prezentul Regulament, cerințele legislației sectoriale trebuie:

13.1. cel puțin, să corespundă cerințelor prevederilor respective, să acopere toate problematicile prevăzute în anexă sau să aibă un caracter mai detaliat pe fond;

13.2. să se refere la toate operațiunile și serviciile furnizorului de servicii în cauză, nu numai la anumite active sau servicii informatice critice pe care acesta le furnizează;

13.3. să cuprindă măsuri de securitate orientate spre asigurarea securității rețelelor și a sistemelor informatice, inclusiv măsuri de securitate a hardware-ului, firmware-ului și software-ului utilizate în activitatea furnizorului de servicii;

13.4. să abordeze în mod specific securitatea fizică și de mediu a rețelelor și a sistemelor informatice în caz de defectare a sistemelor, de erori umane, de acte ilegale sau de fenomene naturale.

14. Atunci când se evaluează dacă cerințele legislației sectoriale privind notificarea incidentelor semnificative de către furnizorul de servicii către Agenție au un efect cel puțin echivalent cu cele prevăzute de Legea nr. 48/2023 privind securitatea cibernetică și de prezentul Regulament, trebuie să se țină cont de faptul că cerințele legislației sectoriale stabilesc cel puțin:

14.1. prevederi care să corespundă cerințelor Legii nr. 48/2023 privind securitatea cibernetică și ale prezentului Regulament sau să aibă un caracter mai detaliat pe fond;

14.2. obligativitatea raportării incidentelor cibernetice semnificative;

14.3. calificarea incidentelor cibernetice ca fiind semnificative, bazată pe condițiile minime stabilite la articolul 12 alineatul (5) din Legea nr. 48/2023 privind securitatea cibernetică și dezvoltate de prezentul Regulament;

14.4. prevederi privind raportarea incidentelor în mai multe etape, care să cuprindă cel puțin: o notificare, corespunzătoare informării prevăzute la articolul 12 alineatul (1), o actualizare a notificării, corespunzătoare articolului 12 alineatul (3), și un raport final, corespunzător articolului 12 alineatul (8) din Legea nr. 48/2023 privind securitatea cibernetică;

14.5. conținutul obligației de raportare, care include informațiile prevăzute la punctele 16, 17 și 18;

14.6. asigurarea accesului imediat prin mijloace automate și directe, care să asigure schimbul sistematic și imediat de informații cu Agenția.

Capitolul IV
PROCEDURA DE NOTIFICARE A INCIDENTELOR CIBERNETICE CU IMPACT SEMNIFICATIV

15. Pentru executarea obligațiilor stabilite în articolul 12 din Legea nr. 48/2023 privind securitatea cibernetică, furnizorii de servicii prezintă Agenției o notificare a incidentului cibernetic, o actualizare a notificării și un raport final. Informațiile prezentate Agenției în condițiile articolului 13 din Legea nr. 48/2023 privind securitatea cibernetică sunt supuse cerințelor stabilite de prevederile prezentului capitol.

16. Notificarea trebuie să includă, atunci când există, informații privind suspiciunile că incidentul semnificativ este cauzat de acte ilegale sau presupus ilegale sau dacă există probabilitatea că acest incident ar putea avea un impact transfrontalier. Notificarea trebuie să includă informațiile strict necesare pentru a aduce la cunoștința Agenției incidentul semnificativ și pentru a permite furnizorului de servicii în cauză să solicite asistență, la necesitate.

17. Actualizarea notificării trebuie să includă o evaluare inițială a incidentului semnificativ, inclusiv a gravității și a impactului acestuia, și, dacă

există, a indicatorilor de compromitere, precum și, atunci când există, o revizuire a informațiilor transmise prin notificare.

18. Raportul final trebuie să includă o descriere detaliată a incidentului cibernetic, inclusiv a gravității și a impactului acestuia, tipul de amenințare și/sau de cauză principală care a declanșat sau este probabil să fi declanșat incidentul, măsurile de atenuare aplicate și în curs de aplicare și, dacă este cazul, o descriere a impactului transfrontalier al incidentului cibernetic.

19. În cazul în care în momentul prezentării raportului final incidentul cibernetic este în desfășurare, furnizorul de servicii prezintă în momentul respectiv un raport privind progresele înregistrate, iar în termen de o lună de la finalizarea gestionării incidentului – un raport final.

20. În procesul gestionării incidentului cibernetic, la solicitarea Agenției, furnizorul de servicii prezintă actualizări ale informațiilor prezentate anterior sau, atunci când există, furnizează informații noi, relevante pentru procesul de gestionare a incidentului cibernetic și pentru asistența acordată de Agenție la solicitarea furnizorului de servicii.

21. Furnizorii de servicii persoane juridice de drept public, pentru executarea obligațiilor stabilite în articolul 12 din Legea nr. 48/2023 privind securitatea cibernetică, prezintă notificările, actualizările și rapoartele finale în modul stabilit în prezentul capitol Centrului guvernamental de răspuns la incidentele cibernetice. Centrul guvernamental de răspuns la incidentele cibernetice prezintă Agenției notificările, actualizările acestora și rapoartele finale în termenele stabilite de cadrul normativ. Furnizorii de servicii persoane juridice de drept public pot notifica Agenției incidentele cibernetice semnificative.

22. Modelul actului și formatul informațiilor prezentate în cadrul interacțiunii dintre furnizorii de servicii și Agenție în procesul de realizare de către aceștia a obligațiilor de notificare a incidentelor cibernetice cu impact semnificativ se aprobă de către directorul Agenției.

23. Incidentele care, în mod individual, nu sunt considerate drept un incident semnificativ în sensul articolului 12 alineatul (5) din Legea nr. 48/2023 privind securitatea cibernetică trebuie considerate toate împreună incidente recurente și calificate ca un unic incident cibernetic cu impact semnificativ, dacă îndeplinesc cumulativ următoarele condiții:

23.1. s-au produs cel puțin de două ori în decursul unei perioade de șase luni;

23.2. au aceeași cauză principală aparentă;

23.3. împreună au cauzat sau pot cauza pierderi financiare directe pentru furnizorul de servicii afectat care depășesc 5 % din cifra de afaceri anuală totală a acestuia aferentă exercițiului financiar anterior.

24. Nu sunt considerate a fi incidente cibernetice cu impact semnificativ întreruperile programate ale serviciului și consecințele planificate ale operațiunilor de întreținere programate, efectuate de către furnizorii de servicii sau de către terți în numele acestora.

25. Atunci când calculează numărul de utilizatori afectați de un incident cibernetic, furnizorii de servicii trebuie să țină cont cumulativ de următoarele elemente:

25.1. numărul de clienți care au un contract cu furnizorul de servicii care le acordă acces la rețeaua și la sistemele informatice ale furnizorului de servicii sau la serviciile oferite de rețeaua și de sistemele informatice respective ori accesibile prin intermediul acestora;

25.2. numărul de persoane fizice și juridice asociate clienților comerciali care utilizează rețeaua și sistemele informatice ale furnizorului de servicii sau serviciile oferite de rețeaua și de sistemele informatice respective ori accesibile prin intermediul acestora.

Capitolul V
CONDIȚII SPECIFICE PENTRU DETERMINAREA IMPACTULUI SEMNIFICATIV AL INCIDENTELOR CIBERNETICE PENTRU UNELE TIPURI DE FURNIZORI DE SERVICII

26. În sensul articolului 12 alineatul (5) litera d) din Legea nr. 48/2023 privind securitatea cibernetică, în ceea ce privește furnizorii de servicii de înregistrare a numelor de domenii şi furnizorii de servicii de sistem de nume de domenii (în continuare – *furnizori de servicii DNS*), Registratorul național al domeniului de nivel superior .md, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate și furnizorii de servicii de securitate gestionate, furnizorii de piețe online, furnizorii de motoare de căutare online, furnizorii de platforme de servicii de socializare în rețea și prestatorii de servicii de încredere, prejudiciile urmează a fi calificate ca fiind considerabile dacă sunt îndeplinite unul sau mai multe dintre următoarele criterii:

26.1. incidentul a cauzat sau poate cauza pierderi financiare directe pentru furnizorul de servicii afectat care depășesc 5 % din cifra de afaceri anuală totală a acestuia aferentă exercițiului financiar anterior;

26.2. incidentul a cauzat sau poate cauza exfiltrarea secretelor comerciale ale furnizorului de servicii, astfel cum acestea sunt definite la articolul 2 din Legea nr. 384/2023 privind protecția secretelor comerciale;

26.3. incidentul a cauzat sau poate cauza decesul unei persoane fizice;

26.4. incidentul a cauzat sau poate cauza daune considerabile sănătății unei persoane fizice;

26.5. s-a produs un acces reușit, presupus rău intenționat și neautorizat, la rețelele și la sistemele informatice, care poate cauza perturbări operaționale grave furnizorului de servicii;

26.6. incidentul este recurent în sensul punctului 23;

26.7. incidentul îndeplinește, în mod corespunzător, cel puțin una dintre condițiile prevăzute la punctele 27-36.

27. În sensul articolului 12 alineatul (5) literele a) și b) din Legea nr. 48/2023 privind securitatea cibernetică, în ceea ce privește furnizorii de servicii DNS, un incident cibernetic urmează a fi considerat ca având impact semnificativ și atunci când intervine una sau mai multe dintre următoarele condiții:

27.1. un serviciu de rezolvare recursivă sau autoritară a numelor de domenii este complet indisponibil timp de peste 30 de minute;

27.2. pentru o perioadă care depășește o oră, timpul mediu de răspuns al unui serviciu de rezolvare recursivă sau autoritară a numelor de domenii la cererile DNS este mai mare de 10 secunde;

27.3. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise ori prelucrate legate de furnizarea serviciului de rezolvare autoritară a numelor de domenii este compromisă, cu excepția cazurilor în care datele cu mai puțin de 1 000 de nume de domenii gestionate de furnizorul de servicii DNS, care nu depășesc 1 % din numele de domenii gestionate de furnizorul de servicii DNS, nu sunt corecte din cauza unei configurări eronate.

28. În sensul articolului 12 alineatul (5) literele a) și b) din Legea nr. 48/2023 privind securitatea cibernetică, în ceea ce privește Registratorul național al domeniului de nivel superior .md, gravitatea consecințelor unui incident cibernetic urmează a fi determinată ca fiind înaltă și, respectiv, imposibilitatea prestării serviciului ca fiind peste perioada maximă admisă, atunci când intervine cel puțin una dintre următoarele condiții:

28.1. un serviciu de rezolvare autoritară a numelor de domenii este complet indisponibil;

28.2. pentru o perioadă care depășește o oră, timpul mediu de răspuns al unui serviciu de rezolvare autoritară a numelor de domenii la cererile DNS este mai mare de 10 secunde;

28.3. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise ori prelucrate legate de funcționarea tehnică a domeniului de nivel superior este compromisă.

29. În sensul articolului 12 alineatul (5) literele a) și b) din Legea nr. 48/2023 privind securitatea cibernetică, în ceea ce privește furnizorii de servicii

de cloud computing, un incident cibernetic urmează a fi considerat ca având impact semnificativ și atunci când intervine una sau mai multe dintre următoarele condiții:

29.1. un serviciu de cloud computing furnizat este complet indisponibil timp de peste 30 de minute;

29.2. disponibilitatea unui serviciu de cloud computing al unui furnizor de servicii de cloud computing este limitată în cazul a peste 5 % dintre utilizatorii serviciului de cloud computing pentru o durată care depășește o oră;

29.3. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise ori prelucrate legate de furnizarea unui serviciu de cloud computing este compromisă ca urmare a unei acțiuni presupus ilegale;

29.4. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise ori prelucrate legate de furnizarea unui serviciu de cloud computing este compromisă, cu un impact asupra a peste 5 % dintre utilizatorii serviciului respectiv de cloud computing.

30. În sensul articolului 12 alineatul (5) literele a) și b) din Legea nr. 48/2023 privind securitatea cibernetică, în ceea ce privește furnizorii de servicii de centre de date, gravitatea consecințelor unui incident cibernetic urmează a fi determinată ca fiind înaltă și, respectiv, imposibilitatea prestării serviciului ca fiind peste perioada maximă admisă, atunci când intervine cel puțin una dintre următoarele condiții:

30.1. un serviciu de centru de date al unui centru de date operat de furnizor este complet indisponibil;

30.2. disponibilitatea unui serviciu de centru de date al unui centru de date operat de furnizor este limitată pentru o durată care depășește o oră;

30.3. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise ori prelucrate legate de furnizarea unui serviciu de centru de date este compromisă ca urmare a unei acțiuni presupus ilegale;

30.4. accesul fizic la un centru de date gestionat de furnizor este compromis.

31. În sensul articolului 12 alineatul (5) literele a) și b) din Legea nr. 48/2023 privind securitatea cibernetică, în ceea ce privește furnizorii de rețele de furnizare de conținut, gravitatea consecințelor unui incident cibernetic urmează a fi determinată ca fiind înaltă și, respectiv, imposibilitatea prestării serviciului ca fiind peste perioada maximă admisă, atunci când intervine cel puțin una dintre următoarele condiții:

31.1. o rețea de furnizare de conținut este complet indisponibilă timp de peste 30 de minute;

31.2. disponibilitatea unei rețele de furnizare de conținut este limitată în cazul a peste 5 % dintre utilizatorii rețelei de furnizare de conținut pentru o durată care depășește o oră;

31.3. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise ori prelucrate legate de furnizarea unei rețele de furnizare de conținut este compromisă ca urmare a unei acțiuni presupus ilegale;

31.4. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise ori prelucrate legate de furnizarea unei rețele de furnizare de conținut este compromisă, cu un impact asupra a peste 5 % dintre utilizatorii respectivei rețele de furnizare de conținut.

32. În sensul articolului 12 alineatul (5) literele a) și b) din Legea nr. 48/2023 privind securitatea cibernetică, în ceea ce privește furnizorii de servicii gestionate și furnizorii de servicii de securitate gestionate, gravitatea consecințelor unui incident cibernetic urmează a fi determinată ca fiind înaltă și, respectiv, imposibilitatea prestării serviciului ca fiind peste perioada maximă admisă, atunci când intervine cel puțin una dintre următoarele condiții:

32.1. un serviciu gestionat sau un serviciu de securitate gestionat este complet indisponibil timp de peste 30 de minute;

32.2. disponibilitatea unui serviciu gestionat sau a unui serviciu de securitate gestionat este limitată în cazul a peste 5 % dintre utilizatorii serviciului pentru o durată care depășește o oră;

32.3. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise ori prelucrate legate de furnizarea unui serviciu gestionat sau a unui serviciu de securitate gestionat este compromisă ca urmare a unei acțiuni presupus ilegale;

32.4. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise ori prelucrate legate de furnizarea unui serviciu gestionat sau a unui serviciu de securitate gestionat este compromisă, cu un impact asupra a peste 5 % dintre utilizatorii respectivului serviciu gestionat sau ai respectivului serviciu de securitate gestionat.

33. În sensul articolului 12 alineatul (5) literele a) și b) din Legea nr. 48/2023 privind securitatea cibernetică, în ceea ce privește furnizorii de piețe online, gravitatea consecințelor unui incident cibernetic urmează a fi determinată ca fiind înaltă și, respectiv, imposibilitatea prestării serviciului ca fiind peste perioada maximă admisă, atunci când intervine cel puțin una dintre următoarele condiții:

33.1. o piață online este complet indisponibilă pentru peste 5 % dintre utilizatorii din Republica Moldova ai respectivei piețe online;

33.2. peste 5 % dintre utilizatorii din Republica Moldova ai unei piețe online sunt afectați de disponibilitatea limitată a respectivei piețe online;

33.3. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise ori prelucrate legate de furnizarea unei piețe online este compromisă ca urmare a unei acțiuni presupus ilegale;

33.4. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise ori prelucrate legate de furnizarea unei piețe online este compromisă, cu un impact asupra a peste 5 % dintre utilizatorii din Republica Moldova ai respectivei piețe online.

34. În sensul articolului 12 alineatul (5) literele a) și b) din Legea nr. 48/2023 privind securitatea cibernetică, în ceea ce privește furnizorii de motoare de căutare online, gravitatea consecințelor unui incident cibernetic urmează a fi determinată ca fiind înaltă și, respectiv, imposibilitatea prestării serviciului ca fiind peste perioada maximă admisă, atunci când intervine cel puțin una dintre următoarele condiții:

34.1. un motor de căutare online este complet indisponibil pentru peste 5 % dintre utilizatorii din Republica Moldova ai respectivului motor de căutare online;

34.2. peste 5 % dintre utilizatorii din Republica Moldova ai unui motor de căutare online sunt afectați de disponibilitatea limitată a respectivului motor de căutare online;

34.3. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise ori prelucrate legate de furnizarea unui motor de căutare online este compromisă ca urmare a unei acțiuni presupus ilegale;

34.4. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise ori prelucrate legate de furnizarea unui motor de căutare online este compromisă, cu un impact asupra a peste 5 % dintre utilizatorii din Republica Moldova ai respectivului motor de căutare online.

35. În sensul articolului 12 alineatul (5) literele a) și b) din Legea nr. 48/2023 privind securitatea cibernetică, în ceea ce privește furnizorii de platforme de servicii de socializare în rețea, gravitatea consecințelor unui incident cibernetic urmează a fi determinată ca fiind înaltă și, respectiv, imposibilitatea prestării serviciului ca fiind peste perioada maximă admisă, atunci când intervine cel puțin una dintre următoarele condiții:

35.1. o platformă de servicii de socializare în rețea este complet indisponibilă pentru peste 5 % dintre utilizatorii din Republica Moldova ai respectivei platforme de servicii de socializare în rețea;

35.2. peste 5 % dintre utilizatorii din Republica Moldova ai unei platforme de servicii de socializare în rețea sunt afectați de disponibilitatea limitată a respectivei platforme de servicii de socializare în rețea;

35.3. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise ori prelucrate legate de furnizarea unei platforme de servicii de socializare în rețea este compromisă ca urmare a unei acțiuni presupus ilegale;

35.4. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise ori prelucrate legate de furnizarea unei platforme de servicii de socializare în rețea este compromisă, cu un impact asupra a peste 5 % dintre

utilizatorii din Republica Moldova ai respectivei platforme de servicii de socializare în rețea.

36. În sensul articolului 12 alineatul (5) literele a) și b) din Legea nr. 48/2023 privind securitatea cibernetică, în ceea ce privește prestatorii de servicii de încredere, gravitatea consecințelor unui incident cibernetic urmează a fi determinată ca fiind înaltă și, respectiv, imposibilitatea prestării serviciului ca fiind peste perioada maximă admisă, atunci când intervine cel puțin una dintre următoarele condiții:

36.1. un serviciu de încredere este complet indisponibil timp de peste 20 de minute;

36.2. un serviciu de încredere este indisponibil pentru utilizatori sau beneficiari timp de peste o oră, calcul efectuat pe baza unei săptămâni calendaristice;

36.3. peste 1 % dintre utilizatorii sau beneficiarii din Republica Moldova sunt afectați de disponibilitatea limitată a unui serviciu de încredere;

36.4. accesul fizic la o zonă în care sunt situate rețelele și sistemele informatice și la care accesul este limitat la personalul de încredere al prestatorului de servicii de încredere este compromis sau protecția unui astfel de acces fizic este compromisă;

36.5. integritatea, confidențialitatea sau autenticitatea datelor stocate, transmise ori prelucrate legate de furnizarea unui serviciu de încredere este compromisă, cu un impact asupra a peste 0,1 % dintre utilizatorii sau beneficiarii serviciului de încredere.

Anexă
la Regulamentul cu privire la modul de realizare
a obligațiilor de asigurare a securității cibernetice
de către furnizorii de servicii în sectoarele critice

CERINȚE
privind măsurile de securitate a rețelelor și a sistemelor informatice ale furnizorilor de servicii în sectoarele critice

Capitolul I
POLITICA PRIVIND SECURITATEA REȚELELOR ȘI A SISTEMELOR INFORMATICE

1. Furnizorii de servicii aprobă o politică privind securitatea rețelelor și a sistemelor informatice care trebuie să corespundă următoarelor cerințe:

1.1. stabilește abordarea furnizorilor de servicii în ceea ce privește gestionarea securității rețelelor și a sistemelor lor informatice;

1.2. este adecvată și complementară strategiei de afaceri și obiectivelor furnizorului de servicii;

1.3. stabilește obiective în materie de securitate a rețelelor și a informațiilor;

1.4. include un angajament de îmbunătățire continuă a securității rețelelor și a sistemelor informatice;

1.5. include un angajament de a furniza resursele adecvate necesare pentru punerea sa în aplicare, inclusiv personalul, resursele financiare, procesele, instrumentele și tehnologiile necesare;

1.6. este comunicată angajaților relevanți și părților externe interesate relevante care iau cunoștință de aceasta;

1.7. stabilește rolurile, responsabilitățile și atribuțiile în conformitate cu punctul 3;

1.8. enumeră documentația care trebuie păstrată și stabilește durata păstrării acesteia;

1.9. enumeră politicile tematice specifice;

1.10. stabilește indicatori și măsuri de monitorizare a punerii sale în aplicare și a stadiului actual al nivelului de maturitate al furnizorului de servicii în materie de securitate a rețelelor și a informațiilor;

1.11. precizează data aprobării oficiale de către organele de conducere ale furnizorului de servicii.

2. Politica privind securitatea rețelelor și a sistemelor informatice este revizuită și, dacă este adecvat, actualizată de către organele de conducere cel puțin anual și atunci când apar incidente cibernetice cu impact semnificativ sau modificări semnificative ale operațiunilor ori ale riscurilor. Rezultatul revizuirilor se documentează.

3. În cadrul politicii lor privind securitatea rețelelor și a sistemelor informatice, furnizorii de servicii:

3.1. stabilesc responsabilitățile și atribuțiile pentru securitatea rețelelor și a sistemelor informatice și le atribuie roluri, le alocă în funcție de nevoile lor și le comunică organelor de conducere;

3.2. solicită personalului și părților terțe să aplice securitatea rețelelor și a sistemelor informatice în conformitate cu politica stabilită privind securitatea rețelelor și a informațiilor și cu politicile și procedurile tematice specifice ale furnizorului de servicii;

3.3. asigură raportarea cel puțin a unei persoane direct organelor de conducere cu privire la aspecte legate de securitatea rețelelor și a sistemelor informatice;

3.4. asigură, în funcție de dimensiunea lor, acoperirea securității rețelelor și a sistemelor informatice cu roluri sau sarcini specifice îndeplinite în plus față de cele existente;

3.5. asigură separarea sarcinilor și a domeniilor de competență care intră în conflict, dacă este aplicabil.

4. Rolurile, responsabilitățile și atribuțiile se revizuiesc și, dacă este adecvat, se actualizează de către organele de conducere la intervale stabilite și atunci când apar incidente semnificative sau modificări semnificative ale operațiunilor ori ale riscurilor.

Capitolul II
POLITICA DE GESTIONARE A RISCURILOR LA ADRESA SECURITĂȚII REȚELELOR ȘI A SISTEMELOR INFORMATICE

Secțiunea 1
Cadrul de gestionare a riscurilor

5. Furnizorii de servicii efectuează și documentează evaluări ale riscurilor și, pe baza rezultatelor, stabilesc, pun în aplicare și monitorizează un plan de tratare a riscurilor. Rezultatele evaluării riscurilor și riscurile reziduale sunt acceptate de către organele de conducere sau, dacă este aplicabil, de către persoanele responsabile și care au autoritatea de a gestiona riscurile, cu condiția ca furnizorii de servicii să asigure raportarea adecvată către organele de conducere.

6. Furnizorii de servicii stabilesc proceduri de identificare, de analiză, de evaluare și de tratare a riscurilor, ceea ce constituie procesul de gestionare a riscurilor în materie de securitate cibernetică. Procesul de gestionare a riscurilor în materie de securitate cibernetică este parte integrantă a procesului general de gestionare a riscurilor furnizorului de servicii, dacă este aplicabil. Ca parte a

procesului de gestionare a riscurilor în materie de securitate cibernetică, furnizorii de servicii:

6.1. urmează o metodologie de gestionare a riscurilor;

6.2. stabilesc nivelul de toleranță la risc în conformitate cu apetitul la risc al furnizorului de servicii;

6.3. stabilesc și mențin criterii de risc relevante;

6.4. în conformitate cu o abordare care ține seama de toate riscurile, identifică riscurile la adresa securității rețelelor și a sistemelor informatice și le documentează, în special în ceea ce privește părțile terțe, și riscurile care ar putea conduce la perturbări ale disponibilității, integrității, autenticității și ale confidențialității rețelelor și a sistemelor informatice, inclusiv identificarea punctului unic de defecțiuni;

6.5. analizează riscurile la adresa securității rețelelor și a sistemelor informatice, inclusiv amenințările, probabilitatea, impactul și nivelul de risc, luând în considerare informațiile privind amenințările cibernetice și vulnerabilitățile;

6.6. evaluează riscurile identificate pe baza criteriilor de risc;

6.7. identifică și prioritizează opțiunile și măsurile adecvate de tratare a riscurilor;

6.8. monitorizează în permanență punerea în aplicare a măsurilor de tratare a riscurilor;

6.9. identifică cine are responsabilitatea punerii în aplicare a măsurilor de tratare a riscurilor și momentul în care acestea ar trebui puse în aplicare;

6.10. documentează măsurile de tratare a riscurilor alese într-un plan de tratare a riscurilor și motivele care justifică acceptarea riscurilor reziduale într-un mod inteligibil.

7. Atunci când identifică și ierarhizează opțiunile și măsurile adecvate de tratare a riscurilor, furnizorii de servicii țin seama de rezultatele evaluării riscurilor, de rezultatele procedurii de evaluare a eficacității măsurilor de gestionare a riscurilor în materie de securitate cibernetică, de costul punerii în aplicare în raport cu beneficiul preconizat, de clasificarea activelor menționată în capitolul XII secțiunea 1 și de analiza impactului asupra activității menționată la punctul 40.

8. Furnizorii de servicii examinează și, dacă este adecvat, actualizează rezultatele evaluării riscurilor și planul de tratare a riscurilor la intervale stabilite și cel puțin o dată pe an, precum și atunci când apar modificări semnificative ale operațiunilor, ale riscurilor sau incidente cibernetice cu impact semnificativ.

Secțiunea a 2-a
Monitorizarea conformității

9. Furnizorii de servicii examinează periodic conformitatea cu politicile lor privind securitatea rețelelor și a sistemelor informatice, cu politicile, normele și standardele tematice specifice. Organele de conducere sunt informate cu privire la situația securității rețelelor și a informațiilor pe baza evaluărilor conformității, prin intermediul unor rapoarte periodice.

10. Furnizorii de servicii instituie un sistem eficace de raportare a conformității, care trebuie să fie adecvat structurilor lor, mediilor de operare și situației amenințărilor. Sistemul de raportare a conformității trebuie să fie în măsură să ofere organelor de conducere o imagine în cunoștință de cauză a situației curente a gestionării riscurilor de către furnizorii de servicii.

11. Furnizorii de servicii efectuează monitorizarea conformității la intervale planificate și atunci când apar incidente cibernetice cu impact semnificativ sau modificări semnificative ale operațiunilor ori ale riscurilor.

Secțiunea a 3-a
Examinarea independentă a securității informațiilor și a rețelelor

12. Furnizorii de servicii examinează în mod independent abordarea în ceea ce privește gestionarea securității rețelelor și a sistemelor informatice și punerea în aplicare a acesteia, inclusiv în ceea ce privește persoanele, procesele și tehnologiile.

13. Furnizorii de servicii elaborează și mențin procese de efectuare a unor examinări independente, care sunt realizate de persoane care dețin certificări în domeniul auditului securității informațiilor. În cazul în care examinarea independentă este efectuată de către membri ai personalului furnizorului de servicii, aceștia nu trebuie să fie în linia ierarhică a personalului din domeniul examinat. În cazul în care dimensiunea furnizorului de servicii nu permite o astfel de separare a liniei ierarhice, furnizorul de servicii instituie măsuri alternative pentru a garanta imparțialitatea examinărilor.

14. Rezultatele examinărilor independente, inclusiv rezultatele monitorizării conformității în temeiul secțiunii a 2-a și ale monitorizării și măsurării în conformitate cu capitolul VII, se raportează organelor de conducere. Furnizorul de servicii ia măsuri corective sau acceptă riscuri reziduale în conformitate cu criteriile de acceptare a riscurilor ale furnizorului de servicii.

15. Examinările independente se efectuează la intervale planificate și atunci când apar incidente cibernetice cu impact semnificativ sau modificări semnificative ale operațiunilor ori ale riscurilor.

Capitolul III
GESTIONAREA INCIDENTELOR

Secțiunea 1
Politica de gestionare a incidentelor

16. Furnizorii de servicii elaborează și pun în aplicare o politică de gestionare a incidentelor cibernetice care stabilește rolurile, responsabilitățile și procedurile pentru detectarea, analizarea, limitarea incidentelor sau răspunsul la incidente, redresarea în urma incidentelor, documentarea și raportarea în timp util a incidentelor. Politica respectivă trebuie să fie coerentă cu planul de asigurare a continuității activității și de recuperare în caz de dezastru menționat în capitolul IV secțiunea 1.

17. Politica de gestionare a incidentelor cibernetice include:

17.1. un sistem de clasificare a incidentelor cibernetice care să fie în concordanță cu evaluarea și clasificarea evenimentelor, efectuate în temeiul punctului 28;

17.2. planuri de comunicare eficace, inclusiv pentru escaladare și raportare;

17.3. atribuirea rolurilor de detectare a incidentelor și de răspuns corespunzător în caz de incidente angajaților competenți;

17.4. documente care trebuie să fie utilizate în cursul detectării incidentelor și al răspunsului la incidente, cum ar fi manuale de răspuns la incidente, grafice privind sesizarea nivelurilor competente, liste de contacte și modele.

18. Rolurile, responsabilitățile și procedurile stabilite în cadrul politicii sunt testate și revizuite și, dacă este adecvat, actualizate la intervale planificate și în urma unor incidente cibernetice cu impact semnificativ sau modificări semnificative ale operațiunilor ori ale riscurilor.

Secțiunea a 2-a
Monitorizare și jurnalizare

19. Furnizorii de servicii stabilesc proceduri și utilizează instrumente pentru monitorizarea și jurnalizarea activităților în rețelele și sistemele lor informatice pentru a detecta evenimentele care ar putea fi considerate incidente cibernetice și pentru a răspunde în consecință în vederea atenuării impactului.

20. În măsura în care este fezabil, monitorizarea trebuie să fie automată și să se efectueze fie în mod continuu, fie la intervale periodice, în funcție de capacitățile operaționale. Furnizorii de servicii își pun în aplicare activitățile de monitorizare într-un mod care să reducă la minimum rezultatele fals pozitive și fals negative.

21. Pe baza procedurilor menționate la punctul 19, furnizorii de servicii păstrează, documentează și revizuiesc jurnalele. Furnizorii de servicii întocmesc o listă a activelor care urmează să facă obiectul jurnalizării pe baza rezultatelor evaluării riscurilor efectuate potrivit capitolului II secțiunea 1. Jurnalele includ, dacă este adecvat:

21.1. traficul de rețea relevant la ieșire și la intrare;

21.2. crearea, modificarea sau eliminarea utilizatorilor rețelelor și sistemelor informatice ale furnizorului de servicii și extinderea permisiunilor;

21.3. accesul la sisteme și aplicații;

21.4. evenimentele legate de autentificare;

21.5. toate accesurile privilegiate la sisteme și aplicații, precum și toate activitățile desfășurate de conturile administrative;

21.6. accesul sau modificările la fișierele configurației critice și la fișierele backup;

21.7. jurnalele de evenimente și jurnalele de la instrumente de securitate, cum ar fi antivirus, sisteme de detectare a intruziunilor sau firewall;

21.8. utilizarea resurselor sistemului, precum și performanța acestora;

21.9. accesul fizic la instalații;

21.10. accesul la echipamentele și dispozitivele lor de rețea și utilizarea acestora;

21.11. activarea, oprirea și întreruperea diferitelor jurnale;

21.12. evenimente de mediu.

22. Jurnalele sunt reexaminate periodic pentru a identifica orice tendință neobișnuită sau nedorită. Dacă este adecvat, furnizorii de servicii stabilesc valori corespunzătoare pentru pragurile de alarmă. În cazul în care valorile stabilite pentru pragul de alarmă sunt depășite, o alarmă urmează să se declanșeze, dacă este adecvat, în mod automat. Furnizorii de servicii se asigură că, în cazul declanșării unei alarme, se inițiază în timp util un răspuns calificat și adecvat.

23. Furnizorii de servicii păstrează jurnalele și realizează copii de rezervă ale acestora pentru o perioadă predefinită, dar nu mai mică de 12 luni, și le protejează împotriva accesului neautorizat și a modificărilor neautorizate.

24. În măsura în care este fezabil, furnizorii de servicii se asigură că toate sistemele dispun de surse ale orei sincronizate pentru a putea corela jurnalele între sisteme pentru evaluarea evenimentelor. Furnizorii de servicii întocmesc și

păstrează o listă a tuturor activelor jurnalizate și se asigură că sistemele de monitorizare și de jurnalizare sunt redundante. Disponibilitatea sistemelor de monitorizare și de jurnalizare este monitorizată independent de sistemele pe care le monitorizează.

25. Procedurile și lista activelor jurnalizate sunt revizuite și, dacă este adecvat, actualizate la intervale regulate și după incidente cibernetice cu impact semnificativ.

Secțiunea a 3-a
Raportarea evenimentelor

26. Furnizorii de servicii instituie un mecanism simplu care să le permită angajaților, furnizorilor și clienților lor să raporteze evenimentele suspecte.

27. Furnizorii de servicii comunică, dacă este adecvat, mecanismul de raportare a evenimentelor furnizorilor și clienților lor și își instruiesc periodic angajații cu privire la modul de utilizare a mecanismului.

Secțiunea a 4-a
Evaluarea și clasificarea evenimentelor

28. Furnizorii de servicii evaluează evenimentele suspecte pentru a stabili dacă acestea constituie incidente și, în caz afirmativ, determină natura și gravitatea lor.

29. În sensul punctului 28, furnizorii de servicii acționează în modul următor:

29.1. efectuează evaluarea pe baza unor criterii predefinite, stabilite în prealabil, și a unei trieri pentru a stabili ordinea de prioritate a limitării și a eradicării incidentelor;

29.2. evaluează trimestrial existența incidentelor recurente menționate în punctul 15 din Regulament;

29.3. examinează jurnalele corespunzătoare în scopul evaluării și al clasificării evenimentelor;

29.4. instituie un proces de corelare și de analiză a jurnalelor;

29.5. reevaluează și reclasifică evenimentele în cazul în care devin disponibile noi informații sau după analizarea informațiilor disponibile anterior.

Secțiunea a 5-a
Răspunsul la incidente

30. Furnizorii de servicii trebuie să răspundă la incidente în conformitate cu procedurile documentate și în timp util.

31. Procedurile de răspuns la incidente includ următoarele etape:

31.1. limitarea incidentului, pentru a preveni răspândirea consecințelor incidentului;

31.2. eradicarea, pentru a preveni continuarea sau reapariția incidentului;

31.3. redresarea în urma incidentului, dacă este necesar.

32. Furnizorii de servicii sunt obligați să stabilească planuri și proceduri de comunicare:

32.1. cu echipa de răspuns la incidentele cibernetice la nivel național a Agenției pentru Securitate Cibernetică în legătură cu notificarea incidentelor;

32.2. pentru comunicarea între membrii personalului furnizorului de servicii și pentru comunicarea cu părțile interesate relevante, externe furnizorului de servicii.

33. Furnizorii de servicii jurnalizează activitățile de răspuns la incidente în conformitate cu procedurile menționate la punctul 19 și înregistrează dovezile.

34. Furnizorii de servicii testează la intervale planificate procedurile lor de răspuns la incidente.

Secțiunea a 6-a
Analizele postincident

35. Dacă este adecvat, furnizorii de servicii efectuează analize post-incident după redresarea în urma incidentelor. Analizele post-incident identifică, atunci când este posibil, cauza principală a incidentului și au drept rezultat învățăminte documentate pentru a reduce apariția și consecințele incidentelor viitoare.

36. Furnizorii de servicii se asigură că analizele post-incident contribuie la îmbunătățirea abordării lor în ceea ce privește securitatea rețelelor și a informațiilor, măsurile de tratare a riscurilor și procedurile de gestionare, de detectare și de răspuns la incidente.

37. Furnizorii de servicii trebuie să examineze la intervale planificate dacă incidentele au condus la analize post-incident.

Capitolul IV
CONTINUITATEA ACTIVITĂȚII ȘI GESTIONAREA CRIZELOR

Secțiunea 1
Planul de continuitate a activității și de recuperare în caz de dezastru

38. Furnizorii de servicii stabilesc și mențin un plan de continuitate a activității și de recuperare în caz de dezastru, care se aplică atunci când intervin incidente cibernetice.

39. Operațiunile furnizorilor de servicii se restabilesc în conformitate cu planul de continuitate a activității și de recuperare în caz de dezastru. Planul se bazează pe rezultatele evaluării riscurilor și include, dacă este adecvat, următoarele:

39.1. scopul, domeniul de aplicare și publicul;

39.2. rolurile și responsabilitățile;

39.3. principalele contacte și canale de comunicare (interne și externe);

39.4. condițiile pentru activarea și dezactivarea planului;

39.5. ordinea de recuperare pentru operațiuni;

39.6. planurile de recuperare pentru operațiuni specifice, inclusiv obiectivele de recuperare;

39.7. resursele necesare, inclusiv copii de rezervă și redundanțe;

39.8. restabilirea și reluarea activităților în baza măsurilor temporare.

40. Furnizorii de servicii efectuează o analiză a impactului asupra activității pentru a evalua impactul potențial al perturbărilor grave asupra operațiunilor lor și, pe baza rezultatelor acestei analize, stabilesc cerințe de continuitate pentru rețelele și sistemele informatice.

41. Planul de continuitate a activității și planul de recuperare în caz de dezastru sunt testate și revizuite și, dacă este adecvat, actualizate la intervale planificate și în urma incidentelor cibernetice cu impact semnificativ sau a modificărilor semnificative ale operațiunilor ori ale riscurilor. Furnizorii de servicii se asigură că planurile includ învățămintele desprinse în urma unor astfel de teste.

Secțiunea a 2-a
Gestionarea copiilor de rezervă și a redundanței

42. Furnizorii de servicii păstrează copii de rezervă ale datelor și furnizează suficiente resurse disponibile, inclusiv instalații, rețele și sisteme informatice și personal, pentru a asigura un nivel adecvat de redundanță.

43. Pe baza rezultatelor evaluării riscurilor și a planului de continuitate a activității, furnizorii de servicii stabilesc planuri de rezervă, care includ următoarele:

43.1. termenele de recuperare;

43.2. asigurarea privind caracterul complet și exactitudinea copiilor de rezervă, inclusiv a datelor de configurare și a datelor stocate în mediul serviciilor de cloud computing;

43.3. stocarea de copii de rezervă (online sau offline) într-un loc sau în locuri sigure, care nu se află în aceeași rețea cu sistemul și care se află la o distanță suficientă pentru a scăpa de orice daune cauzate de un dezastru la locul principal;

43.4. controale adecvate ale accesului fizic și logic la copiile de rezervă, în conformitate cu nivelul de clasificare a activelor;

43.5. restabilirea datelor din copiile de rezervă;

43.6. perioade de păstrare bazate pe cerințe comerciale și normative.

44. Furnizorii de servicii efectuează verificări periodice ale integrității copiilor de rezervă.

45. Pe baza rezultatelor evaluării riscurilor și a planului de continuitate a activității, furnizorii de servicii asigură disponibilitatea suficientă a resurselor prin redundanța, cel puțin parțială, a următoarelor:

45.1. rețele și sisteme informatice;

45.2. active, inclusiv instalații, echipamente și materiale;

45.3. personal care are responsabilitatea, atribuțiile și competența necesară;

45.4. canale de comunicare adecvate.

46. Dacă este adecvat, furnizorii de servicii se asigură că monitorizarea și ajustarea resurselor, inclusiv a instalațiilor, a sistemelor și a personalului, se întemeiază în mod corespunzător pe cerințele privind copiile de rezervă și redundanța.

47. Furnizorii de servicii testează periodic recuperarea copiilor de rezervă și a redundanțelor pentru a se asigura că, în condiții de recuperare, se pot baza pe acestea și că acoperă copiile, procesele și cunoștințele pentru realizarea unei recuperări efective. Furnizorii de servicii documentează rezultatele testelor și, dacă este necesar, iau măsuri corective.

Secțiunea a 3-a
Gestionarea crizelor

48. Furnizorii de servicii instituie un proces de gestionare a crizelor.

49. Furnizorii de servicii se asigură că procesul de gestionare a crizelor abordează cel puțin următoarele elemente:

49.1. rolurile și responsabilitățile personalului și, dacă este adecvat, ale furnizorilor și ale prestatorilor de servicii, specificând alocarea rolurilor în situații de criză, inclusiv etapele specifice care trebuie să fie urmate;

49.2. mijloacele de comunicare adecvate între furnizorul de servicii și autoritățile competente relevante;

49.3. aplicarea unor măsuri adecvate pentru a asigura menținerea securității rețelelor și a sistemelor informatice în situații de criză.

50. În sensul subpunctului 49.2, fluxul de informații dintre furnizorul de servicii și autoritățile competente relevante include atât comunicările obligatorii, cum ar fi rapoartele privind incidentele și termenele aferente, cât și comunicările neobligatorii.

51. Furnizorii de servicii instituie un proces de gestionare și de utilizare a informațiilor primite de la Agenția pentru Securitate Cibernetică cu privire la incidente, vulnerabilități, amenințări sau posibile măsuri de atenuare.

52. Furnizorii de servicii testează, revizuiesc și, dacă este adecvat, actualizează planul de gestionare a crizelor în mod regulat sau în urma unor incidente cibernetice cu impact semnificativ ori a unor modificări semnificative ale operațiunilor sau riscurilor.

Capitolul V
SECURITATEA LANȚULUI DE APROVIZIONARE

53. Furnizorii de servicii instituie, implementează și aplică o politică de securitate a lanțului de aprovizionare care reglementează relațiile cu furnizorii și prestatorii lor de servicii direcți pentru a atenua riscurile identificate la adresa securității rețelelor și a sistemelor informatice. În cadrul politicii de securitate a lanțului de aprovizionare, furnizorii de servicii identifică rolul lor în lanțul de aprovizionare și îl comunică furnizorilor și prestatorilor lor de servicii direcți.

54. Ca parte a politicii de securitate a lanțului de aprovizionare menționate la punctul 53, furnizorii de servicii stabilesc criterii pentru selectarea și contractarea furnizorilor și a prestatorilor de servicii. Aceste criterii includ următoarele:

54.1. practicile în materie de securitate cibernetică ale furnizorilor și ale prestatorilor de servicii, inclusiv procedurile lor securizate de dezvoltare;

54.2. capacitatea furnizorilor și a prestatorilor de servicii de a respecta specificațiile în materie de securitate cibernetică stabilite de furnizorul de servicii;

54.3. calitatea și reziliența generală a produselor TIC (tehnologie a informației și comunicațiilor) și a serviciilor TIC și măsurile de gestionare a riscurilor în materie de securitate cibernetică încorporate în acestea, inclusiv riscurile și nivelul de clasificare a produselor TIC și a serviciilor TIC;

54.4. capacitatea furnizorului de servicii de a diversifica sursele de aprovizionare și de a limita dependența de furnizor, dacă este aplicabil.

55. Pe baza politicii de securitate a lanțului de aprovizionare și ținând seama de rezultatele evaluării riscurilor, furnizorii de servicii se asigură că contractele lor cu furnizorii și prestatorii de servicii specifică, dacă este adecvat, prin acorduri privind nivelul serviciilor, următoarele:

55.1. cerințele în materie de securitate cibernetică pentru furnizorii sau prestatorii de servicii, inclusiv cerințele în ceea ce privește securitatea achiziționării serviciilor TIC sau a produselor TIC prevăzute în capitolul VI secțiunea 1;

55.2. cerințele privind sensibilizarea, competențele și formarea și, dacă este adecvat, certificările impuse angajaților furnizorilor sau ai prestatorilor de servicii;

55.3. cerințele privind verificarea antecedentelor angajaților furnizorilor și ai prestatorilor de servicii;

55.4. obligația furnizorilor și a prestatorilor de servicii de a notifica, fără întârzieri nejustificate, furnizorilor de servicii incidentele care prezintă un risc pentru securitatea rețelelor și a sistemelor informatice ale acestora;

55.5. dreptul de a efectua audituri sau dreptul de a primi rapoarte de audit;

55.6. obligația furnizorilor și a prestatorilor de servicii de a gestiona vulnerabilitățile care prezintă un risc pentru securitatea rețelelor și a sistemelor informatice ale furnizorilor respectivi de servicii;

55.7. cerințele privind subcontractarea și, în cazul în care furnizorul de servicii permite subcontractarea, cerințele în materie de securitate cibernetică pentru subcontractanți în conformitate cu cerințele în materie de securitate cibernetică menționate la subpunctul 55.1;

55.8. obligațiile furnizorilor și ale prestatorilor de servicii în cazul rezilierii contractului, cum ar fi extragerea și distrugerea informațiilor obținute de către furnizori și prestatorii de servicii în exercitarea sarcinilor lor.

56. Furnizorii de servicii iau în considerare elementele menționate la punctul 54 ca parte a procesului de selecție a noilor furnizori și prestatori de servicii, precum și ca parte a procesului de achiziții publice menționat în capitolul VI secțiunea 1.

57. Furnizorii de servicii trebuie să-și revizuiască politica de securitate a lanțului de aprovizionare și să monitorizeze, să evalueze și, dacă este necesar, să acționeze ca urmare a modificărilor aduse practicilor în materie de securitate cibernetică ale furnizorilor și ale prestatorilor de servicii, la intervale planificate și

atunci când au loc modificări semnificative ale operațiunilor sau ale riscurilor ori incidente cibernetice cu impact semnificativ legate de furnizarea de servicii TIC sau care au un impact asupra securității produselor TIC de la furnizori și prestatorii de servicii.

58. În sensul punctului 57, furnizorii de servicii:

58.1. monitorizează periodic rapoartele privind punerea în aplicare a acordurilor privind nivelul serviciilor, dacă este aplicabil;

58.2. examinează incidentele legate de produsele TIC și de serviciile TIC de la furnizorii și prestatorii de servicii;

58.3. evaluează necesitatea unor examinări neprogramate și documentează constatările într-un mod inteligibil;

58.4. analizează riscurile prezentate de modificările legate de produsele TIC și de serviciile TIC de la furnizorii și prestatorii de servicii și, dacă este adecvat, iau măsuri de atenuare în timp util.

59. Furnizorii de servicii mențin și actualizează un registru al furnizorilor lor și al prestatorilor lor de servicii direcți, care include:

59.1. punctele de contact pentru fiecare furnizor și prestator de servicii direct;

59.2. lista produselor TIC, a serviciilor TIC și a proceselor TIC livrate furnizorului de servicii de către furnizorul sau prestatorul de servicii direct.

Capitolul VI
SECURITATEA ÎN ACHIZIȚIONAREA, DEZVOLTAREA ȘI ÎNTREȚINEREA REȚELELOR ȘI A SISTEMELOR INFORMATICE

Secțiunea 1
Securitatea în achiziționarea serviciilor TIC sau a produselor TIC

60. Furnizorii de servicii stabilesc și pun în aplicare, pe baza evaluării riscurilor, efectuate potrivit capitolului II, procese de gestionare a riscurilor care decurg din achiziționarea a serviciilor TIC sau a produselor TIC de la furnizori sau prestatori de servicii pentru componente care sunt critice pentru securitatea rețelelor și a sistemelor informatice ale furnizorului de servicii pe parcursul întregului lor ciclu de viață.

61. Procesele menționate la punctul 60 trebuie să includă:

61.1. cerințe de securitate aplicabile serviciilor TIC sau produselor TIC care urmează să fie achiziționate;

61.2. cerințe privind actualizările de securitate pe întreaga durată de viață a serviciilor TIC sau a produselor TIC ori înlocuirea după încheierea perioadei de asistență;

61.3. informații care descriu componentele hardware și software utilizate în serviciile TIC sau în produsele TIC;

61.4. informații care descriu funcțiile de securitate cibernetică puse în aplicare ale serviciilor TIC sau ale produselor TIC și configurația necesară pentru funcționarea lor în condiții de siguranță;

61.5. asigurarea faptului că serviciile TIC sau produsele TIC respectă cerințele de securitate în conformitate cu subpunctul 61.1;

61.6. metode de validare a conformității serviciilor TIC sau a produselor TIC livrate cu cerințele de securitate declarate, precum și documentarea rezultatelor validării.

62. Furnizorii de servicii revizuiesc și, dacă este adecvat, actualizează procesele la intervale planificate și atunci când apar incidente semnificative.

Secțiunea a 2-a
Ciclul de viață al dezvoltării securizate

63. Înainte de a dezvolta o rețea și un sistem informatic, inclusiv un software, furnizorii de servicii stabilesc reguli pentru dezvoltarea securizată de rețele și sisteme informatice și le aplică atunci când dezvoltă rețele și sisteme informatice la nivel intern sau atunci când externalizează dezvoltarea rețelelor și a sistemelor informatice. Regulile acoperă toate etapele dezvoltării, inclusiv specificațiile, proiectarea, dezvoltarea, punerea în aplicare și testarea.

64. În sensul punctului 63, furnizorii de servicii:

64.1. efectuează o analiză a cerințelor de securitate în etapele referitoare la specificațiile și proiectarea oricărui proiect de dezvoltare sau de achiziție întreprins de furnizorul de servicii sau în numele acestuia;

64.2. aplică principii de creare a sistemelor securizate și principii de programare securizată oricărei activități de dezvoltare a sistemelor informatice, cum ar fi promovarea securității cibernetice din faza de proiectare, a arhitecturilor de tip „încredere zero”;

64.3. stabilesc cerințe de securitate privind mediile de dezvoltare;

64.4. instituie și pun în aplicare procese de testare a securității în ciclul de viață al dezvoltării;

64.5. selectează, protejează și gestionează în mod corespunzător datele privind testele de securitate;

64.6. sanitizează și anonimizează datele privind testele în conformitate cu evaluarea riscurilor.

65. În cazul în care dezvoltarea rețelelor și a sistemelor informatice este externalizată, furnizorul de servicii aplică inclusiv politicile și procedurile menționate în capitolul V și în secțiunea 1 din prezentul capitol.

66. Furnizorii de servicii își revizuiesc și, dacă este necesar, își actualizează normele de dezvoltare securizată la intervale planificate.

Secțiunea a 3-a
Gestionarea configurației

67. Furnizorii de servicii iau măsurile adecvate pentru a stabili, a documenta, a pune în aplicare și a monitoriza configurațiile, inclusiv configurațiile de securitate ale hardware-ului, software-ului, serviciilor și rețelelor.

68. În acest scop, furnizorii de servicii:

68.1. stabilesc și asigură securitatea configurațiilor pentru hardware, software, servicii și rețele;

68.2. stabilesc și pun în aplicare procese și instrumente pentru a asigura respectarea configurațiilor securizate stabilite pentru hardware, software, servicii și rețele, pentru sistemele nou-instalate, precum și pentru sistemele aflate în funcțiune pe durata lor de viață.

69. Furnizorii de servicii revizuiesc și, dacă este adecvat, actualizează configurațiile la intervale planificate și atunci când apar incidente cibernetice cu impact semnificativ sau modificări semnificative ale operațiunilor ori ale riscurilor.

Secțiunea a 4-a
Gestionarea schimbărilor, reparații și întreținere

70. Furnizorii de servicii aplică proceduri de gestionare a schimbărilor pentru a controla modificările aduse rețelelor și sistemelor informatice. Dacă este aplicabil, procedurile trebuie să fie în concordanță cu politicile generale privind gestionarea schimbărilor ale furnizorului de servicii.

71. Procedurile de gestionare a schimbărilor se aplică noilor versiuni, modificărilor și modificărilor de urgență ale oricărui software și hardware în exploatare și modificărilor configurației. Aceste proceduri asigură faptul că modificările respective sunt documentate și, pe baza evaluării riscurilor, sunt testate și evaluate având în vedere impactul potențial înainte de a fi puse în aplicare.

72. În cazul în care procedurile obișnuite de gestionare a schimbărilor nu au putut fi urmate din cauza unei urgențe, furnizorul de servicii documentează rezultatul modificării și explicația motivului pentru care procedurile nu au putut fi urmate.

73. Furnizorii de servicii revizuiesc și, dacă este adecvat, actualizează procedurile la intervale planificate și atunci când apar incidente cibernetice cu impact semnificativ sau modificări semnificative ale operațiunilor ori ale riscurilor.

Secțiunea a 5-a
Teste de securitate

74. Furnizorii de servicii stabilesc, implementează și aplică o politică și proceduri pentru testele de securitate.

75. Furnizorii de servicii:

75.1. stabilesc, pe baza evaluării riscurilor, necesitatea, sfera, frecvența și tipul testelor de securitate;

75.2. efectuează teste de securitate în conformitate cu o metodologie de testare documentată, care acoperă componentele identificate în cadrul unei analize a riscurilor ca fiind relevante pentru operarea în condiții de siguranță;

75.3. documentează tipul, sfera, ora și rezultatele testelor, inclusiv evaluarea criticalității și acțiunile de atenuare pentru fiecare constatare;

75.4. aplică măsuri de atenuare în cazul constatărilor critice.

76. Furnizorii de servicii își revizuiesc și, dacă este adecvat, își actualizează politicile privind testele de securitate la intervale planificate.

Secțiunea a 6-a
Gestionarea corecțiilor de securitate

77. Furnizorii de servicii specifică și aplică proceduri coerente cu procedurile de gestionare a modificărilor, precum și cu gestionarea vulnerabilităților, gestionarea riscurilor și cu alte proceduri de gestionare relevante, pentru a se asigura că:

77.1. corecțiile de securitate se aplică într-un termen rezonabil de la data la care devin disponibile;

77.2. corecțiile de securitate se testează înainte de a fi aplicate în sistemele de producție;

77.3. corecțiile de securitate provin din surse de încredere și sunt verificate din punctul de vedere al integrității;

77.4. în cazurile în care o corecție nu este disponibilă sau nu se aplică în temeiul punctului 78, se pun în aplicare măsuri suplimentare și se acceptă riscuri reziduale.

78. Furnizorii de servicii pot alege să nu aplice corecții de securitate atunci când dezavantajele aplicării corecțiilor de securitate sunt mai mari decât beneficiile în materie de securitate cibernetică. Furnizorii de servicii documentează și justifică în mod corespunzător motivele unei astfel de decizii.

Secțiunea a 7-a
Securitatea rețelelor

79. Furnizorii de servicii iau măsurile adecvate pentru a-și proteja rețelele și sistemele informatice împotriva amenințărilor cibernetice.

80. În acest sens, furnizorii de servicii:

80.1. documentează arhitectura rețelei într-un mod inteligibil și actualizat;

80.2. stabilesc și aplică controale pentru a-și proteja domeniile rețelei interne împotriva accesului neautorizat;

80.3. configurează controale pentru a preveni accesul și comunicarea în rețea care nu sunt necesare pentru funcționarea furnizorului de servicii;

80.4. stabilesc și aplică controale pentru accesul de la distanță la rețelele și la sistemele informatice, inclusiv accesul prestatorilor de servicii;

80.5. nu utilizează în alte scopuri sistemele folosite pentru administrarea punerii în aplicare a politicii de securitate;

80.6. interzic sau dezactivează în mod explicit conexiunile și serviciile care nu sunt necesare;

80.7. dacă este adecvat, permit exclusiv accesul la rețelele și sistemele lor informatice prin intermediul unor dispozitive autorizate de furnizorul de servicii;

80.8. permit conectarea prestatorilor de servicii numai după o cerere de autorizare și pentru o perioadă stabilită, cum ar fi durata unei operațiuni de întreținere;

80.9. stabilesc comunicarea între sisteme distincte numai prin canale de încredere care sunt izolate prin separare logică, criptografică sau fizică de alte canale de comunicare și garantează identificarea punctelor lor finale și protecția datelor canalului împotriva modificării sau divulgării;

80.10. adoptă un plan de punere în aplicare pentru tranziția completă către protocoale de comunicare la nivel de rețea de ultimă generație într-un mod sigur, adecvat și treptat și stabilesc măsuri de accelerare a acestei tranziții;

80.11. adoptă un plan de punere în aplicare pentru implementarea unor standarde moderne de comunicații prin e-mail convenite la nivel internațional și interoperabile pentru a securiza comunicațiile prin e-mail în vederea atenuării

vulnerabilităților legate de amenințările privind e-mailurile și stabilesc măsuri pentru accelerarea unei astfel de implementări;

80.12. aplică cele mai bune practici pentru securitatea DNS, pentru securitatea rutării pe internet și pentru igiena rutării traficului care provine din rețea și care este destinat acesteia.

81. Furnizorii de servicii revizuiesc și, dacă este adecvat, actualizează aceste măsuri la intervale planificate și atunci când apar incidente cibernetice cu impact semnificativ sau modificări semnificative ale operațiunilor ori ale riscurilor.

Secțiunea a 8-a
Segmentarea rețelei

82. Furnizorii de servicii segmentează sistemele în rețele sau zone în conformitate cu rezultatele evaluării riscurilor. Furnizorii de servicii își segmentează sistemele și rețelele de sistemele și rețelele terților.

83. În acest scop, furnizorii de servicii:

83.1. iau în considerare relația funcțională, logică și fizică, inclusiv localizarea, dintre sisteme și servicii fiabile;

83.2. acordă acces la o rețea sau la o zonă pe baza unei evaluări a cerințelor sale de securitate;

83.3. păstrează sistemele care sunt critice pentru funcționarea furnizorului de servicii sau pentru siguranță în zone securizate;

83.4. instalează o zonă demilitarizată în cadrul rețelelor lor de comunicare pentru a asigura o comunicare securizată care provine de la rețelele lor sau care este destinată acestora;

83.5. restricționează accesul și comunicațiile dintre zone și în interiorul acestora la cele necesare pentru funcționarea furnizorului de servicii sau pentru siguranță;

83.6. separă rețeaua dedicată administrării rețelelor și sistemelor informatice de rețeaua operațională a furnizorului de servicii;

83.7. separă canalele de administrare a rețelei de alte tipuri de trafic de rețea;

83.8. separă sistemele de producție pentru serviciile furnizorului de servicii de sistemele utilizate pentru dezvoltare și testare, inclusiv copii de rezervă.

84. Furnizorii de servicii revizuiesc și, dacă este adecvat, actualizează segmentarea rețelei la intervale planificate și atunci când apar incidente cibernetice cu impact semnificativ sau modificări semnificative ale operațiunilor ori ale riscurilor.

Secțiunea a 9-a
Protecția împotriva software-ului rău intenționat și neautorizat

85. Furnizorii de servicii își protejează rețelele și sistemele informatice împotriva software-ului rău intenționat și neautorizat.

86. În acest scop, furnizorii de servicii pun în aplicare, în special, măsuri de detectare sau de prevenire a utilizării programelor informatice rău intenționate sau neautorizate. Furnizorii de servicii se asigură, dacă este adecvat, că rețelele și sistemele lor informatice sunt echipate cu software de detectare și de răspuns, care este actualizat periodic în conformitate cu evaluarea riscurilor și cu acordurile contractuale cu furnizorii.

Secțiunea a 10-a
Gestionarea și divulgarea vulnerabilităților

87. Furnizorii de servicii obțin informații cu privire la vulnerabilitățile tehnice din rețelele și sistemele lor informatice, evaluează expunerea lor la astfel de vulnerabilități și iau măsurile adecvate pentru gestionarea vulnerabilităților.

88. În acest sens, furnizorii de servicii:

88.1. monitorizează informațiile privind vulnerabilitățile prin canale adecvate, cum ar fi anunțurile echipelor de răspuns la incidentele cibernetice, inclusiv ale echipei de răspuns la incidentele cibernetice la nivel național a Agenției pentru Securitate Cibernetică, ale altor autorități competente, sau informațiile furnizate de furnizori sau de prestatorii de servicii;

88.2. efectuează, dacă este adecvat, scanări ale vulnerabilității și consemnează rezultatele scanărilor la intervale planificate;

88.3. abordează, fără întârzieri nejustificate, vulnerabilitățile identificate ca fiind critice pentru operațiunile lor;

88.4. se asigură că gestionarea vulnerabilităților este compatibilă cu procedurile lor de gestionare a modificărilor, a corecțiilor de securitate, a riscurilor și a incidentelor;

88.5. stabilesc o procedură pentru divulgarea vulnerabilităților în conformitate cu politica națională coordonată aplicabilă în materie de divulgare a vulnerabilităților.

89. Atunci când acest lucru este justificat de impactul potențial al vulnerabilității, furnizorii de servicii elaborează și pun în aplicare un plan de atenuare a vulnerabilității. În alte cazuri, furnizorii de servicii documentează și justifică motivul pentru care vulnerabilitatea nu necesită remediere.

90. Furnizorii de servicii revizuiesc și, dacă este adecvat, actualizează la intervale planificate canalele pe care le utilizează pentru monitorizarea informațiilor privind vulnerabilitatea.

Capitolul VII
POLITICI ȘI PROCEDURI PENTRU EVALUAREA EFICACITĂȚII MĂSURILOR DE GESTIONARE A RISCURILOR ÎN MATERIE DE SECURITATE CIBERNETICĂ

91. Furnizorii de servicii stabilesc, implementează și aplică o politică și proceduri pentru a evalua dacă măsurile de gestionare a riscurilor în materie de securitate cibernetică luate sunt puse în aplicare și menținute în mod eficace.

92. Politica și procedurile menționate la punctul 91 trebuie să țină cont de rezultatele evaluării riscurilor și de incidentele cibernetice cu impact semnificativ din trecut. Furnizorii de servicii stabilesc:

92.1. măsurile de gestionare a riscurilor în materie de securitate cibernetică ce urmează să fie monitorizate și măsurate, inclusiv procese și controale;

92.2. metodele pentru monitorizare, măsurare, analiză și evaluare, dacă acest lucru se aplică, pentru a asigura validitatea rezultatelor;

92.3. momentul în care trebuie să fie efectuate monitorizarea și măsurarea;

92.4. persoana/entitatea responsabilă de monitorizarea și măsurarea eficacității măsurilor de gestionare a riscurilor în materie de securitate cibernetică;

92.5. momentul în care trebuie să fie analizate și evaluate rezultatele monitorizării și măsurării;

92.6. persoana/entitatea responsabilă de analiza și evaluarea acestor rezultate.

93. Furnizorii de servicii revizuiesc și, dacă este adecvat, actualizează politicile și procedurile la intervale planificate și atunci când apar incidente cibernetice cu impact semnificativ sau modificări semnificative ale operațiunilor ori ale riscurilor.

Capitolul VIII
PRACTICI DE BAZĂ ÎN MATERIE DE IGIENĂ CIBERNETICĂ ȘI FORMARE ÎN DOMENIUL SECURITĂȚII CIBERNETICE

Secțiunea 1
Sensibilizare și practici de bază în materie de igienă cibernetică

94. Furnizorii de servicii se asigură că angajații lor, inclusiv membrii organelor de conducere, precum și furnizorii și prestatorii de servicii direcți sunt

sensibilizați cu privire la riscuri, sunt informați cu privire la importanța securității cibernetice și aplică practici de igienă cibernetică.

95. În acest scop, furnizorii de servicii oferă angajaților lor, inclusiv membrilor organelor de conducere, precum și furnizorilor și prestatorilor de servicii direcți, dacă este adecvat, un program de sensibilizare, care:

95.1. este planificat în timp, astfel încât activitățile să fie repetate și să acopere noii angajați;

95.2. este stabilit în conformitate cu politica de securitate a rețelelor și a informațiilor, cu politicile tematice specifice și cu procedurile relevante privind securitatea rețelelor și a informațiilor;

95.3. acoperă amenințările cibernetice relevante, măsurile existente de gestionare a riscurilor în materie de securitate cibernetică, punctele de contact și resursele pentru obținerea de informații și de consiliere suplimentare cu privire la aspectele legate de securitatea cibernetică, precum și practicile de igienă cibernetică pentru utilizatori.

96. Dacă este adecvat, programul de sensibilizare este testat din punctul de vedere al eficacității. Programul de sensibilizare este actualizat și oferit la intervale planificate, ținând seama de modificările practicilor de igienă cibernetică, precum și de situația actuală a amenințărilor și de riscurile pentru furnizorul de servicii.

Secțiunea a 2-a
Formare în domeniul securității

97. Furnizorii de servicii identifică angajații ale căror roluri necesită seturi de competențe și expertiză relevante în materie de securitate și se asigură că aceștia beneficiază de formare periodică privind securitatea rețelelor și a sistemelor informatice.

98. Furnizorii de servicii stabilesc, implementează și aplică un program de formare în conformitate cu politica de securitate a rețelelor și a informațiilor, cu politicile tematice specifice și cu alte proceduri relevante privind securitatea rețelelor și a informațiilor, care determină nevoile de formare pentru anumite roluri și funcții pe baza unor criterii.

99. Formarea trebuie să fie relevantă pentru funcția postului angajatului, iar eficacitatea sa trebuie să fie evaluată. Formarea ia în considerare măsurile de securitate instituite și acoperă următoarele aspecte:

99.1. instrucțiuni privind configurarea și funcționarea în condiții de siguranță a rețelei și a sistemelor informatice, inclusiv a dispozitivelor mobile;

99.2. informare cu privire la amenințările cibernetice cunoscute;

99.3. formare cu privire la comportamentul care trebuie să fie adoptat atunci când au loc evenimente relevante pentru securitate.

100. Furnizorii de servicii asigură cursuri de formare membrilor personalului care se transferă în posturi sau roluri noi ce necesită seturi de competențe și expertiză relevante în materie de securitate.

101. Programul se actualizează și se desfășoară periodic, ținând seama de politicile și normele aplicabile, de rolurile și responsabilitățile atribuite, precum și de amenințările cibernetice cunoscute și de evoluțiile tehnologice.

Capitolul IX
CRIPTOGRAFIE

102. Furnizorii de servicii stabilesc, implementează și aplică o politică și proceduri legate de criptografie, cu scopul de a asigura utilizarea adecvată și eficace a criptografiei pentru a proteja confidențialitatea, autenticitatea și integritatea datelor în conformitate cu clasificarea activelor furnizorului de servicii și cu rezultatele evaluării riscurilor efectuate potrivit prezentelor cerințe.

103. Politica și procedurile cu privire la criptografie urmează să stabilească:

103.1. tipul, puterea și calitatea măsurilor criptografice necesare pentru a proteja activele furnizorului de servicii, inclusiv datele în repaus și datele în tranzit;

103.2. pe baza subpunctului 103.1, protocoalele sau familiile de protocoale de adoptat, precum și algoritmii criptografici, puterea de criptare, soluțiile criptografice și practicile de utilizare care urmează să fie aprobate și care sunt necesare pentru a fi utilizate în cadrul furnizorului de servicii, urmând, dacă este adecvat, o abordare bazată pe agilitate criptografică;

103.3. abordarea furnizorului de servicii în ceea ce privește gestionarea cheilor, inclusiv, dacă este adecvat, metodele pentru:

103.3.1. generarea de chei diferite pentru sistemele și aplicațiile criptografice;

103.3.2. emiterea și obținerea de certificate de cheie publică;

103.3.3. distribuirea cheilor către entitățile vizate, inclusiv modul de activare a cheilor atunci când sunt primite;

103.3.4. stocarea cheilor, inclusiv modul în care utilizatorii autorizați obțin acces la chei;

103.3.5. modificarea sau actualizarea cheilor, inclusiv normele privind momentul și modul de modificare a cheilor;

103.3.6. gestionarea cheilor compromise;

103.3.7. revocarea cheilor, inclusiv modul de retragere sau de dezactivare a cheilor;

103.3.8. recuperarea cheilor pierdute sau corupte;

103.3.9. crearea copiilor de rezervă sau arhivarea cheilor;

103.3.10. distrugerea cheilor;

103.3.11. jurnalizarea și auditarea activităților legate de gestionarea cheilor;

103.3.12. stabilirea datelor de activare și de dezactivare a cheilor, astfel încât cheile să poată fi utilizate numai pentru perioada specificată, în conformitate cu normele organizației privind gestionarea cheilor.

104. Furnizorii de servicii își revizuiesc și, dacă este adecvat, își actualizează politicile și procedurile la intervale planificate, ținând seama de stadiul de dezvoltare al criptografiei.

Capitolul X
SECURITATEA RESURSELOR UMANE

Secțiunea 1
Securitatea resurselor umane

105. Furnizorii de servicii se asigură că angajații lor și furnizorii și prestatorii lor de servicii direcți, dacă este aplicabil, înțeleg și își asumă responsabilitățile în materie de securitate, astfel cum este adecvat pentru serviciile oferite și postul ocupat și în conformitate cu politica furnizorului de servicii privind securitatea rețelelor și a sistemelor informatice.

106. Cerința menționată la punctul 105 include:

106.1. mecanisme prin care să se asigure că toți angajații, furnizorii și prestatorii de servicii direcți, dacă acest lucru este aplicabil, înțeleg și urmează practicile standard de igienă cibernetică pe care furnizorul de servicii le aplică în conformitate cu capitolul VIII secțiunea 1;

106.2. mecanisme prin care să se asigure că toți utilizatorii cu acces administrativ sau privilegiat cunosc și acționează în conformitate cu rolurile, responsabilitățile și atribuțiile lor;

106.3. mecanisme prin care să se asigure că membrii organelor de conducere înțeleg și acționează în conformitate cu rolul, responsabilitățile și atribuțiile lor în ceea ce privește securitatea rețelelor și a sistemelor informatice;

106.4. mecanisme de angajare a personalului calificat pentru rolurile respective, cum ar fi verificările referințelor, procedurile de verificare, validarea certificărilor sau testele scrise.

107. Furnizorii de servicii revizuiesc alocarea personalului în roluri specifice, astfel cum este descris în politica privind securitatea rețelelor și a sistemelor informatice, precum și gradul de mobilizare a resurselor umane în

această privință, la intervale planificate și cel puțin o dată pe an. Furnizorii de servicii actualizează alocarea dacă este necesar.

Secțiunea a 2-a
Verificarea antecedentelor

108. Furnizorii de servicii se asigură că se efectuează, în măsura în care este fezabil, verificări ale antecedentelor angajaților lor și, dacă este aplicabil, ale furnizorilor și prestatorilor lor de servicii direcți, în conformitate cu punctul 55, în cazul în care este necesar pentru rolul, responsabilitățile și autorizările lor.

109. În sensul punctului 108, furnizorii de servicii:

109.1. instituie criterii care stabilesc rolurile, responsabilitățile și atribuțiile care sunt exercitate numai de către persoane cărora le-au fost verificate antecedentele;

109.2. se asigură că verificările se efectuează pentru persoanele respective înainte ca ele să înceapă să exercite aceste roluri, responsabilități și atribuții, corespund prevederilor actelor normative, reglementărilor și normelor deontologice aplicabile în raport cu cerințele comerciale, clasificarea activelor menționată în capitolul XII secțiunea 1 și rețelele și sistemele informatice la care urmează să fie asigurat accesul, precum și cu riscurile percepute.

110. Furnizorii de servicii trebuie să revizuiască și, dacă este adecvat, să actualizeze politica la intervale planificate și la necesitate.

Secțiunea a 3-a
Procedura în caz de încetare sau de modificare a raporturilor de muncă

111. Furnizorii de servicii se asigură că responsabilitățile și sarcinile în materie de securitate a rețelelor și a sistemelor informatice care rămân valabile după încetarea sau după modificarea raporturilor de muncă ale angajaților lor sunt definite și puse în aplicare prin contract.

112. În sensul punctului 111, furnizorii de servicii trebuie să includă în condițiile de muncă, în contractul sau în acordul încheiat cu persoana în cauză responsabilitățile și sarcinile care sunt încă valabile după încetarea raporturilor de muncă sau a contractului, cum ar fi clauzele de confidențialitate.

Secțiunea a 4-a
Procesul disciplinar

113. Furnizorii de servicii instituie, comunică și mențin un proces disciplinar pentru gestionarea încălcărilor politicilor de securitate a rețelelor și a sistemelor informatice. Procesul ține seama de cerințele juridice, statutare, contractuale și comerciale relevante.

114. Furnizorii de servicii revizuiesc și, dacă este adecvat, actualizează procesul disciplinar la intervale planificate și atunci când este necesar ca urmare a unor schimbări legislative sau a unor modificări semnificative ale operațiunilor ori ale riscurilor.

Capitolul XI
CONTROLUL ACCESULUI

Secțiunea 1
Politica de control al accesului

115. Furnizorii de servicii stabilesc, documentează și pun în aplicare politici de control al accesului logic și fizic pentru accesul la rețelele și sistemele lor informatice, pe baza cerințelor comerciale, precum și a cerințelor de securitate a rețelelor și a sistemelor informatice.

116. Politicile menționate la punctul 115 trebuie:

116.1. să abordeze accesul persoanelor, inclusiv al personalului, al vizitatorilor și al entităților externe, cum ar fi furnizorii și prestatorii de servicii;

116.2. să abordeze accesul rețelelor și al sistemelor informatice;

116.3. să asigure faptul că accesul este acordat numai utilizatorilor care au fost autentificați în mod corespunzător.

117. Furnizorii de servicii revizuiesc și, dacă este adecvat, actualizează politicile la intervale planificate și atunci când apar incidente semnificative sau modificări semnificative ale operațiunilor ori ale riscurilor.

Secțiunea a 2-a
Gestionarea drepturilor de acces

118. Furnizorii de servicii trebuie să acorde, să modifice, să elimine și să documenteze drepturile de acces la rețelele și la sistemele informatice în conformitate cu politica de control al accesului menționată în secțiunea 1.

119. Furnizorii de servicii:

119.1. atribuie și revocă drepturile de acces pe baza principiilor necesității de a cunoaște, privilegiului minim și separării sarcinilor;

119.2. se asigură că drepturile de acces sunt modificate în mod corespunzător la încetarea sau la modificarea raporturilor de muncă;

119.3. se asigură că accesul la rețelele și la sistemele informatice este autorizat de către persoanele relevante;

119.4. se asigură că drepturile de acces abordează în mod corespunzător accesul terților, cum ar fi vizitatorii, furnizorii și prestatorii de servicii, în special prin limitarea drepturilor de acces în ceea ce privește sfera și durata acestora;

119.5. țin un registru al drepturilor de acces acordate;

119.6. aplică jurnalizarea gestionării drepturilor de acces.

120. Furnizorii de servicii revizuiesc drepturile de acces la intervale planificate și le modifică în conformitate cu schimbările organizaționale, precum și documentează rezultatele revizuirii, inclusiv modificările necesare ale drepturilor de acces.

Secțiunea a 3-a
Conturile privilegiate și conturile de administrare a sistemului

121. Furnizorii de servicii mențin politici de gestionare a conturilor privilegiate și a conturilor de administrare a sistemului ca parte a politicii de control al accesului menționate în secțiunea 1.

122. Politicile menționate la punctul 121:

122.1. instituie proceduri riguroase de identificare, de autentificare, cum ar fi autentificarea multifactorială, și de autorizare pentru conturile privilegiate și conturile de administrare a sistemului;

122.2. creează conturi specifice care să fie utilizate exclusiv pentru operațiunile de administrare a sistemului, cum ar fi instalarea, configurarea, gestionarea sau întreținerea;

122.3. individualizează și restricționează privilegiile de administrare a sistemului în cea mai mare măsură posibilă;

122.4. prevăd faptul că sunt utilizate conturile de administrare a sistemului numai pentru conectarea la sistemele de administrare a sistemului.

123. Furnizorii de servicii revizuiesc drepturile de acces aferente conturilor privilegiate și conturilor de administrare a sistemului la intervale planificate, le modifică în conformitate cu schimbările organizaționale și documentează rezultatele revizuirii, inclusiv modificările necesare ale drepturilor de acces.

Secțiunea a 4-a
Sisteme de administrare

124. Furnizorii de servicii restricționează și controlează utilizarea sistemelor de administrare a sistemului în conformitate cu politica de control al accesului.

125. În acest scop, furnizorii de servicii:

125.1. utilizează sistemele de administrare a sistemului numai în scopul administrării sistemului, și nu pentru alte operațiuni;

125.2. separă în mod logic astfel de sisteme de aplicațiile software care nu sunt utilizate în scopul administrării sistemului;

125.3. protejează accesul la sistemele de administrare a sistemului prin autentificare și criptare.

Secțiunea a 5-a
Identificare

126. Furnizorii de servicii gestionează întregul ciclu de viață al identităților rețelelor și sistemelor informatice și ale utilizatorilor acestora.

127. În acest scop, furnizorii de servicii:

127.1. stabilesc identități unice pentru rețelele și sistemele informatice și pentru utilizatorii acestora;

127.2. asociază identitatea utilizatorilor cu o singură persoană;

127.3. asigură supravegherea identităților rețelei și sistemelor informatice;

127.4. aplică jurnalizarea gestionării identităților.

128. Furnizorii de servicii permit identitățile atribuite mai multor persoane, cum ar fi identitățile comune, numai în cazul în care acestea sunt necesare din motive comerciale sau operaționale și fac obiectul unui proces de aprobare și al unei documentări explicite. Furnizorii de servicii țin seama de identitățile atribuite mai multor persoane în cadrul de gestionare a riscurilor de securitate cibernetică.

129. Furnizorii de servicii revizuiesc periodic identitățile rețelelor și sistemelor informatice și ale utilizatorilor acestora și, dacă nu mai sunt necesare, le dezactivează fără întârziere.

Secțiunea a 6-a
Autentificare

130. Furnizorii de servicii pun în aplicare proceduri și tehnologii de autentificare securizată bazate pe restricții de acces și pe politica privind controlul accesului.

131. În acest scop, furnizorii de servicii:

131.1. se asigură că puterea autentificării este adecvată pentru clasificarea activului care urmează să fie accesat;

131.2. controlează alocarea către utilizatori și gestionarea informațiilor secrete de autentificare printr-un proces care să asigure confidențialitatea informațiilor, inclusiv consilierea personalului cu privire la gestionarea adecvată a informațiilor de autentificare;

131.3. solicită modificarea acreditărilor de autentificare inițiale la intervale predefinite și în cazul în care se suspectează că respectivele acreditări au fost compromise;

131.4. solicită resetarea acreditărilor de autentificare și blocarea utilizatorilor după un număr predefinit de încercări nereușite de conectare;

131.5. pun capăt sesiunilor inactive după o perioadă prestabilită de inactivitate;

131.6. solicită acreditări separate pentru a obține acces privilegiat sau a avea acces la conturi administrative.

132. Furnizorii de servicii utilizează, în măsura în care este fezabil, metode de autentificare de ultimă generație, în conformitate cu riscul evaluat asociat și cu clasificarea activului care urmează să fie accesat, precum și informații de autentificare unice.

133. Furnizorii de servicii revizuiesc procedurile și tehnologiile de autentificare la intervale planificate.

Secțiunea a 7-a
Autentificarea multifactor

134. Furnizorii de servicii se asigură că utilizatorii sunt autentificați prin factori de autentificare multipli sau prin mecanisme de autentificare continuă pentru accesarea rețelelor și a sistemelor informatice ale furnizorului de servicii, dacă este adecvat, în conformitate cu clasificarea activului care urmează să fie accesat.

135. Furnizorii de servicii se asigură că puterea autentificării este adecvată pentru clasificarea activului care urmează să fie accesat.

Capitolul XII
GESTIONAREA ACTIVELOR

Secțiunea 1
Clasificarea activelor

136. Furnizorii de servicii stabilesc niveluri de clasificare a tuturor activelor, inclusiv a informațiilor, care intră în domeniul de aplicare al rețelelor și al sistemelor lor informatice corespunzătoare nivelului de protecție necesar.

137. În acest scop, furnizorii de servicii:

137.1. stabilesc un sistem de niveluri de clasificare a activelor;

137.2. asociază tuturor activelor un nivel de clasificare, bazat pe cerințe de confidențialitate, integritate, autenticitate și disponibilitate, pentru a indica protecția necesară în funcție de sensibilitatea, criticalitatea, riscul și valoarea lor comercială;

137.3. aliniază cerințele privind disponibilitatea activelor la obiectivele de livrare și de recuperare stabilite în planurile lor de continuitate a activității și de recuperare în caz de dezastru.

138. Furnizorii de servicii efectuează revizuiri periodice ale nivelurilor de clasificare a activelor și le actualizează, dacă este adecvat.

Secțiunea a 2-a
Gestionarea activelor

139. Furnizorii de servicii stabilesc, implementează și aplică o politică pentru gestionarea corespunzătoare a activelor, inclusiv a informațiilor, în conformitate cu politica lor de securitate a rețelelor și a informațiilor și comunică politica privind gestionarea corespunzătoare a activelor oricărei persoane care utilizează sau gestionează aceste active.

140. Politica de gestionare a activelor:

140.1. acoperă întregul ciclu de viață al activelor, inclusiv achiziționarea, utilizarea, depozitarea, transportul și eliminarea acestora;

140.2. prevede norme privind utilizarea, depozitarea și transportul în condiții de siguranță, precum și ștergerea și distrugerea iremediabilă a activelor;

140.3. prevede că transferul trebuie să aibă loc în condiții de siguranță, în funcție de tipul de activ care urmează să fie transferat.

141. Furnizorii de servicii revizuiesc și, dacă este adecvat, actualizează politica la intervale planificate și atunci când apar incidente cibernetice cu impact semnificativ sau modificări semnificative ale operațiunilor ori ale riscurilor.

Secțiunea a 3-a
Politica privind suporturile amovibile

142. Furnizorii de servicii stabilesc, implementează și aplică o politică de gestionare a suporturilor de stocare amovibile și o comunică angajaților lor și părților terțe care gestionează suporturi de stocare amovibile în incintele furnizorului de servicii sau în alte locuri în care suporturile amovibile sunt conectate la rețelele și sistemele informatice ale furnizorului de servicii.

143. Politica de gestionare a suporturilor de stocare amovibile:

143.1. prevede o interdicție tehnică de conectare a suporturilor amovibile, cu excepția cazului în care există un motiv organizațional pentru utilizarea acestora;

143.2. prevede dezactivarea autoexecutării din aceste suporturi și scanarea suporturilor pentru coduri rău intenționate înainte de a fi utilizate în sistemele furnizorului de servicii;

143.3. prevede măsuri de control și de protecție a dispozitivelor portabile de stocare care conțin date în timpul tranzitului și al stocării;

143.4. dacă este adecvat, prevede măsuri pentru utilizarea tehnicilor criptografice pentru a proteja datele de pe suporturile de stocare amovibile.

144. Furnizorii de servicii revizuiesc și, dacă este adecvat, actualizează politica la intervale planificate și atunci când apar incidente cibernetice cu impact semnificativ sau modificări semnificative ale operațiunilor ori ale riscurilor.

Secțiunea a 4-a
Inventarul activelor

145. Furnizorii de servicii elaborează și mențin un inventar complet, exact, actualizat și consecvent al activelor lor. Furnizorii de servicii consemnează modificările aduse înregistrărilor din inventar într-un mod care să poată fi urmărit.

146. Granularitatea inventarului activelor trebuie să fie la un nivel adecvat nevoilor furnizorilor de servicii. Inventarul include următoarele:

146.1. lista operațiunilor și a serviciilor și descrierea acestora;

146.2. lista rețelelor și a sistemelor informatice și a altor active asociate care sprijină operațiunile și serviciile entităților relevante.

147. Furnizorii de servicii trebuie să revizuiască și să actualizeze periodic inventarul și activele lor și să documenteze istoricul modificărilor.

148. Furnizorii de servicii stabilesc, implementează și aplică proceduri care garantează că activele lor, aflate în custodia personalului, sunt depozitate, restituite sau eliminate la încetarea raporturilor de muncă, precum și documentează depozitarea, returnarea și eliminarea activelor respective.

149. În cazul în care nu este posibilă depozitarea, returnarea sau eliminarea activelor, furnizorii de servicii se asigură că activele nu mai pot accesa rețelele și sistemele informatice ale acestora în conformitate cu politica pentru gestionarea corespunzătoare a activelor, prevăzută în secțiunea a 2-a.

Capitolul XIII
SECURITATEA MEDIULUI ȘI SECURITATEA FIZICĂ

Secțiunea 1
Utilități de sprijin

150. Furnizorii de servicii previn pierderea, deteriorarea sau compromiterea rețelelor și a sistemelor informatice sau întreruperea funcționării acestora din cauza defectării și a perturbării utilităților de sprijin.

151. În acest scop, furnizorii de servicii, dacă este adecvat:

151.1. protejează instalațiile împotriva întreruperii alimentării cu energie electrică și a altor perturbări cauzate de defecțiuni în ceea ce privește utilitățile de sprijin, cum ar fi energia electrică, telecomunicațiile, alimentarea cu apă, gazele, apele uzate, ventilarea și aerul condiționat;

151.2. iau în considerare utilizarea redundanței în ceea ce privește serviciile de utilități;

151.3. protejează serviciile de utilități pentru energie electrică și telecomunicații, care transportă date sau furnizează rețele și sisteme informatice, împotriva interceptării și a deteriorării;

151.4. monitorizează serviciile de utilități menționate la subpunctul 151.3 și raportează personalului intern sau extern competent evenimentele din afara pragurilor minime și maxime de control menționate la subpunctul 154.2 care afectează serviciile de utilități;

151.5. încheie contracte pentru aprovizionarea de urgență cu servicii corespunzătoare, cum ar fi pentru combustibilul pentru alimentarea cu energie electrică în situații de urgență;

151.6. asigură eficacitatea continuă, monitorizează, întreține și testează alimentarea rețelelor și a sistemelor informatice necesare pentru funcționarea

serviciului oferit, în special energia electrică, controlul temperaturii și al umidității, telecomunicațiile și conexiunea la internet.

152. Furnizorii de servicii testează, revizuiesc și, dacă este adecvat, actualizează măsurile de protecție în mod regulat sau în urma unor incidente cibernetice cu impact semnificativ ori a unor modificări semnificative ale operațiunilor sau ale riscurilor.

Secțiunea a 2-a
Protecția împotriva amenințărilor fizice și de mediu
+

153. Furnizorii de servicii previn sau reduc consecințele evenimentelor generate de amenințări fizice și de mediu, cum ar fi dezastrele naturale și alte amenințări intenționate sau neintenționate, pe baza rezultatelor evaluării riscurilor.

154. În acest scop, furnizorii de servicii, dacă este adecvat:

154.1. concep și pun în aplicare măsuri de protecție împotriva amenințărilor fizice și de mediu;

154.2. determină pragurile minime și maxime de control pentru amenințările fizice și de mediu;

154.3. monitorizează parametrii de mediu și raportează personalului intern sau extern competent evenimentele din afara pragurilor minime și maxime de control menționate la subpunctul 154.2.

155. Furnizorii de servicii testează, revizuiesc și, dacă este adecvat, actualizează măsurile de protecție împotriva amenințărilor fizice și de mediu în mod regulat sau în urma unor incidente cu impact semnificativ ori a unor modificări semnificative ale operațiunilor sau ale riscurilor.

Secțiunea a 3-a
Controlul perimetrului și al accesului fizic

156. Furnizorii de servicii previn și monitorizează accesul fizic neautorizat la rețelele și sistemele lor informatice, precum și deteriorarea acestora și interferențele cu acestea.

157. În acest scop, furnizorii de servicii:

157.1. pe baza evaluării riscurilor, stabilesc și utilizează perimetre de securitate pentru a proteja zonele în care sunt situate rețelele și sistemele informatice și alte active asociate;

157.2. protejează zonele menționate la subpunctul 157.1 prin controale de intrare și puncte de acces adecvate;

157.3. concep și pun în aplicare securitatea fizică pentru birouri, încăperi și instalații;

157.4. își monitorizează permanent incintele pentru a depista accesul fizic neautorizat.

158. Furnizorii de servicii testează, revizuiesc și, dacă este adecvat, actualizează măsurile de control al accesului fizic în mod regulat sau în urma unor incidente cu impact semnificativ ori a unor modificări semnificative ale operațiunilor sau ale riscurilor.

Nota de fundamentare
la proiectul hotărârii Guvernului cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice

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 proiectului de act normativ este constituit din prevederile art. 11 alin. (4), art. 12 alin. (9) și art. 14 alin. (2) din Legea nr. 48/2023 privind securitatea cibernetică (în continuare – Legea nr. 48/2023). Aceste norme stabilesc corespunzător în competența Guvernului reglementarea următoarelor aspecte:

- aprobarea standardelor naționale în domeniul securității informației și al securității cibernetice în baza standardelor și a specificațiilor tehnice europene și celor internaționale relevante pentru securitatea rețelelor și a sistemelor informatice
- aprobarea cerințelor specifice de securitate privind rețelele și sistemele informatice în funcție de sectorul, subsectorul, categoria și/sau tipul furnizorului de servicii.
- stabilirea procedurii de notificare a incidentelor cibernetice, inclusiv a interacțiunii dintre furnizorul de servicii și autoritatea competentă, a modul de stabilire a impactului unui incident cibernetic și formatul informațiilor, evaluărilor și rapoartelor prezentate în procesul de gestionare a unui incident cibernetic;
- aprobarea măsurilor de securitate minime obligatorii pentru persoanele juridice de drept public.

Proiectul de act normativ propus spre examinare concentrează aceste aspecte într-o singură inițiativă de intervenție normativă, pe de o parte, din motivul multiplelor interconexiuni dintre cele două componente a obligațiilor de asigurare a securității cibernetice: măsurile de gestionare a riscurilor și notificarea incidentelor cibernetice semnificative și, în acest context, evitarea eventualelor dublări în cazul divizării reglementărilor în diferite acte, iar, pe de altă parte, unificarea abordării în ce privește sectorul public și sectorul privat pentru a evita potențialele conflicte în interpretarea de către entitățile din sectorul public a aplicabilității unor reglementări ce vizează măsurile de gestionare a riscurilor și obligațiile de notificare.

De asemenea proiectul are ca sursă:

- Regulamentul de punere în aplicare (UE) 2024/2690[1] al Comisiei din 17 octombrie 2024 de stabilire a normelor de aplicare a Directivei (UE) 2022/2555 în ceea ce privește cerințele tehnice și metodologice ale măsurilor de gestionare a riscurilor în materie de securitate cibernetică și specificarea suplimentară a cazurilor în care un incident este considerat semnificativ referitor la furnizorii de servicii DNS, registrele de nume TLD, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea, precum și prestatorii de servicii de încredere, și

[1] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32024R2690

- Comunicarea Comisiei Orientările[2] Comisiei privind aplicarea articolului 4 alineatele (1) și (2) din Directiva (UE) 2022/2555 (Directiva NIS 2) 2023/C 328/02.

2.2. Descrierea situației actuale și a problemelor care impun intervenția, inclusiv a cadrului normativ aplicabil și a deficiențelor/lacunelor normative

Similar cum este prezentat în analizele de impact asociate proiectului de Lege privind securitatea cibernetică și legilor conexe, inclusiv proiectul de hotărâre de Guvern referitoare la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică, potrivit datelor actualizate, în perioada 2018-2023, statele membre ale Uniunii Europene au înregistrat un total de 3251 incidente cibernetice cu impact semnificativ, conform criteriilor stabilite de Directiva NIS1, Codul european al comunicațiilor electronice și Regulamentul eIDAS. Din acest număr, 26% au fost considerate acțiuni rău intenționate. Sectorul cel mai afectate a fost cel privat, în special domeniile comunicațiilor, bancar, sănătate, servicii de încredere, transport și energie. Deși numărul incidentelor a înregistrat o scădere în 2023 comparativ cu 2022, tendința generală este de creștere a incidentelor cu impact semnificativ, conform *Figurii 1*. Din cele 847 de incidente rău intenționate raportate, majoritatea au fost clasificate ca infracțiuni cibernetice, conform graficului de cauzalitate tehnică prezentat în *Figura 2*. Aceste date subliniază necesitatea unei abordări riguroase, comprehensive și bine coordonate pentru prevenirea și gestionarea incidentelor cibernetice cu impact semnificativ.

Fig.1 Numărul de incidente (anual)

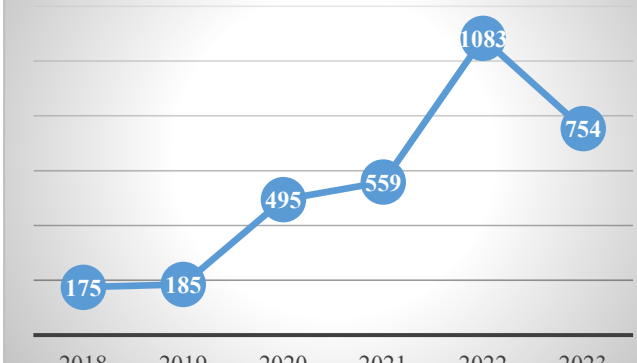
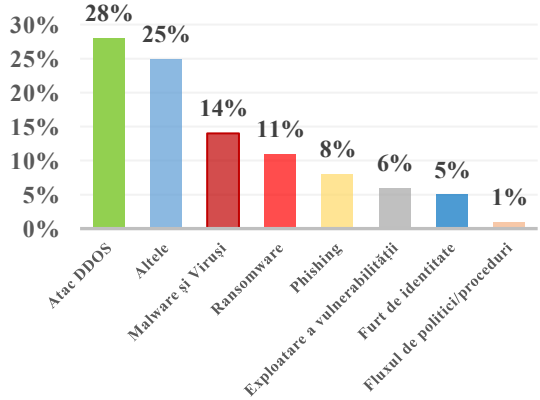


Fig. 2 Cauzalitatea tehnică

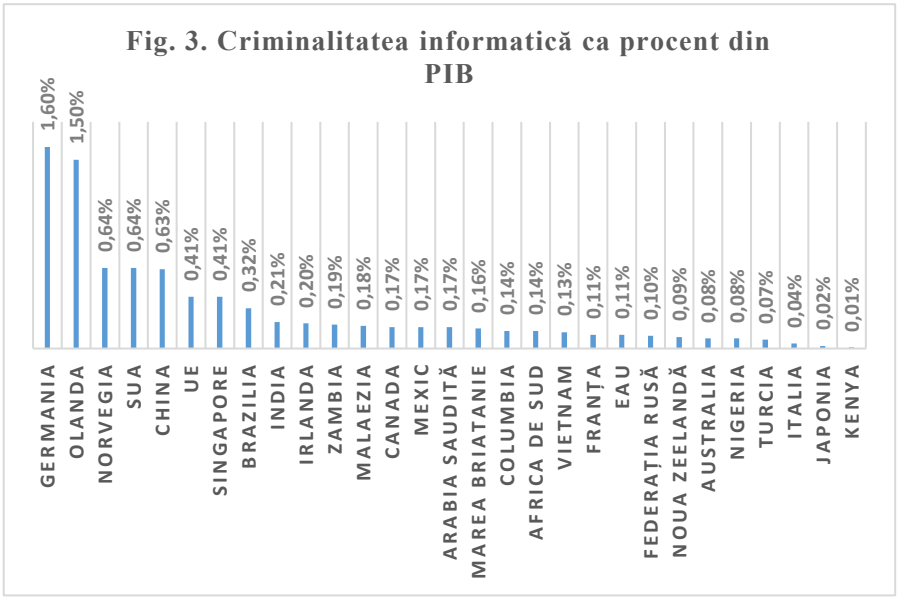


Conform raportului IBM *Cost of a Data Breach*[3] actualizat pentru anul 2023, impactul financiar al încălcării datelor este și mai mare pentru entitățile critice. Raportul arată că în 2023, costul mediu global al unei încălcări de date a atins un nivel record de 4,45 milioane de dolari americani, înregistrând o creștere cu 2,3% față de anul 2022 și o creștere cu 15,3% față de 2020. Comparând aceste date cu cele prezentate în analizele de impact anterioare, putem constata că de la instituirea cadrului normativ primar în domeniul securității cibernetice în Republica Moldova, impactul incidentelor cibernetice a devenit și mai pronunțat.

[2] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52023XC0918(01)
[3] https://www.ibm.com/reports/data-breach

În plus, relevăm studiul global realizat de compania McAfee[4], care a evaluat pierderile economice cauzate de criminalitatea cibernetică. Acest studiu, intitulat *Net Losses: Estimating the Global Cost of Cybercrime*, furnizează o estimare a impactului economic al infracțiunilor informatice pentru diferite țări, exprimate ca procent din PIB. Graficul prezentat în *Figura 3* evidențiază țările cel mai grav afectate în funcție de proporția prejudiciului monetizat în raport cu PIB-ul lor. În medie, pierderile cauzate de infracțiunile cibernetice reprezintă aproximativ 0,3% din PIB. Extrapolând aceste date pentru Republica Moldova, având în vedere că Produsul Intern Brut al acesteia a fost de aproximativ 16,5 miliarde de dolari SUA în 2023, se poate estima un prejudiciu potențial anual de aproximativ 49 de milioane de dolari, bazat pe media de 0,3% din PIB.

Fig. 3. Criminalitatea informatică ca procent din PIB



Potrivit Strategiei de transformare digitală a Republicii Moldova pentru anii 2023-2030[5], sectorul TIC a devenit principalul motor al digitalizării și inovării în Republica Moldova și este în creștere rapidă. În 2021, industria IT a atins o pondere de peste 4,2% din produsul intern brut (PIB), depășind 10 mlrd. lei vânzări, ponderea sectorului TIC fiind de peste 7,6 % din PIB, cu peste 18 mlrd. lei vânzări în anul 2021, realizate de circa 2000 de companii cu peste 30 000 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.

Prin urmare, deși Legea nr. 48/2023 privind securitatea cibernetică stabilește un cadru normativ de bază în domeniul securității cibernetice, absența unor reglementări complete la nivel sectorial pune în pericol funcționarea economiei Republicii Moldova, în special a celei digitale. În acest context, reziliența cibernetică a persoanelor juridice (atât publice, cât și private), care sunt furnizori de servicii esențiale și critice pentru funcționarea economiei naționale și a statului în ansamblu, devine un aspect de importanță majoră.

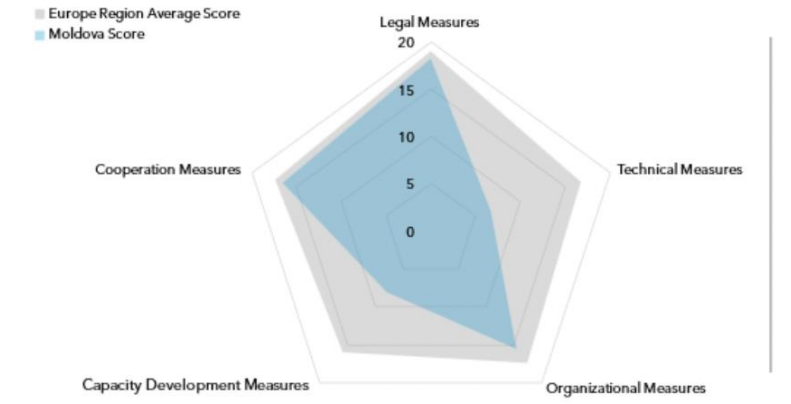
[4] https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis

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

Conform Indicelui Global de Securitate Cibernetică (GCI) al Uniunii Internaționale a Telecomunicațiilor (ITU) pentru anul 2024, scorul general al Republicii Moldova este de 65,09, iar performanța țării este descrisă ca fiind de nivel 3 - „Stabilire". Acest nivel reprezintă țările care au obținut un scor general de cel puțin 55/100, demonstrând un angajament de bază în materie de securitate cibernetică prin acțiuni guvernamentale care includ evaluarea, stabilirea sau implementarea anumitor măsuri de securitate cibernetică general acceptate într-un număr moderat de piloni sau indicatori. Acest indice evaluează angajamentul a 172 de țări în domeniul securității cibernetice, analizând gradul de conștientizare a importanței și dimensiunilor problemelor de securitate cibernetică, precum și rezistența și fiabilitatea sectorului TIC din fiecare țară.

Conform raportului ITU privind echipa de răspuns la incidente de securitate cibernetică la nivel național, performanța Republicii Moldova în cadrul GCI pentru 2024, în comparație cu anul 2020 a înregistrat o creștere a măsurilor juridice, organizatorice și de cooperare. Cu toate acestea, însă se remarcă o scădere notabilă a măsurilor tehnice și de dezvoltare a capacităților, însă acest lucru poate fi atribuit parțial ajustărilor metodologice și a ponderărilor GCI, precum și modificărilor aduse întrebărilor. Cu toate acestea, acest indice poate fi îmbunătățit prin armonizarea legislației naționale cu cea a UE și prin implementarea corespunzătoare a legislației naționale, inclusiv prin stabilirea unei autorități competente responsabile de gestionarea acestui sector.

Graficul de mai jos (*Figura 4*) evidențiază performanța Republicii Moldova în cadrul GCI pentru anul 2020, subliniind că măsurile organizaționale și consolidarea capacităților sunt punctele cele mai slabe ale Republicii Moldova în acest domeniu.



Domenii relativ consolidate:
Măsurile legale, de cooperare și organizaționale

Domenii cu potențial de creștere:
Măsurile tehnice și dezvoltarea capacităților

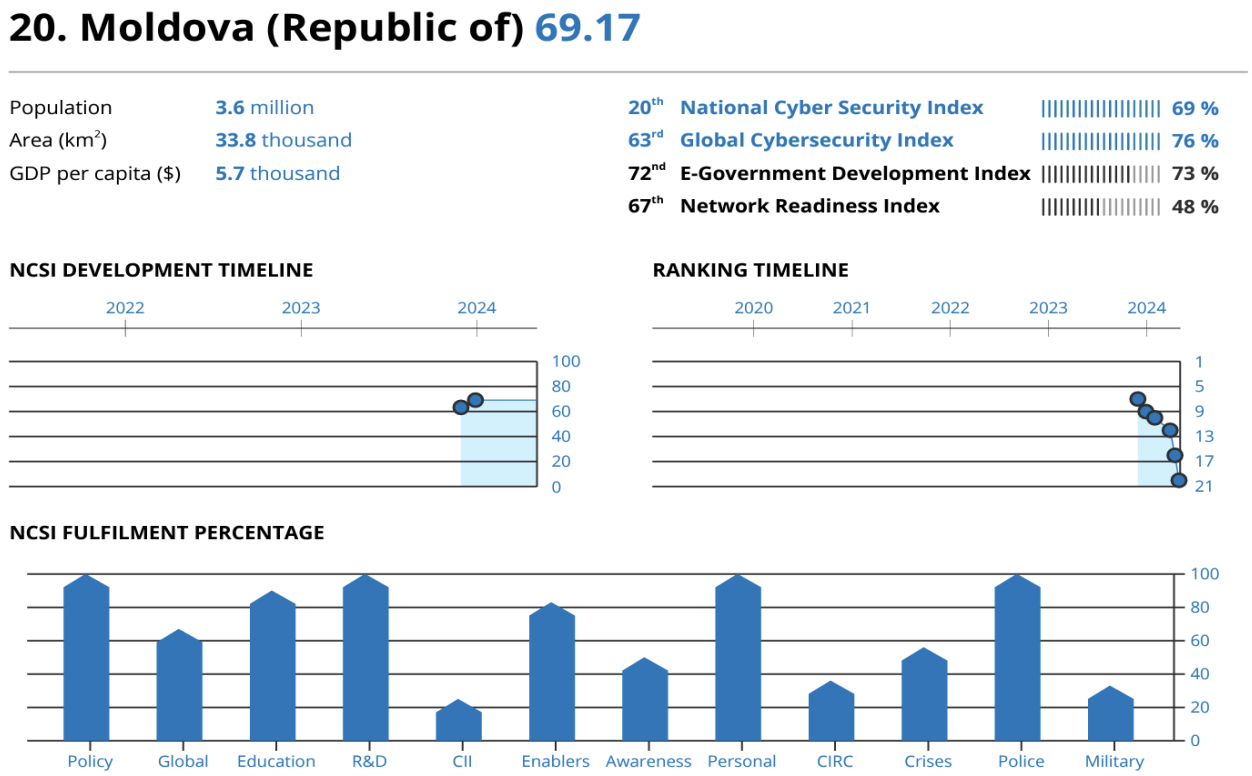
Scorul total	Măsurile legale	Măsurile tehnice	Măsurile organizaționale	Dezvoltarea capacităților	Măsuri de cooperare
65,09	18,28	6,68	15,51	8,04	16,58

De asemenea, trebuie să evidențiem că Republica Moldova este evaluată și în ceea ce privește maturitatea în domeniul securității cibernetice prin intermediul Indicelui Național de Securitate Cibernetică (NCSI)[6]. Acesta este un indice global în timp real, care măsoară gradul de pregătire a țărilor pentru a preveni amenințările cibernetice și a gestiona incidentele cibernetice. NCSI este, de asemenea, o bază de date cu materiale de evidență disponibile publicului și un instrument pentru consolidarea capacităților naționale în domeniul securității cibernetice.

[6] https://ncsi.ega.ee/

În figura de mai jos (Fig. 5.) este reflectată poziția Republicii Moldova și principalii indicatori care reflectă maturitatea țării în materie de securitate cibernetică. Potrivit NCSI, există restanțe semnificative în ceea ce privește protecția infrastructurilor critice (care constituie 25%), răspunsul la incidente cibernetice și asigurarea apărării cibernetice (ambii indicatori situându-se sub 40%)[7].

Fig. 5. Gradul de maturitate a Republicii Moldova în domeniul securității cibernetice conform NCSI



Astfel, la data de 16 martie 2023, Parlamentul a adoptat Legea nr. 48/2023 privind securitatea cibernetică, care urmează să intre în vigoare la data de 1 ianuarie 2025. 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, deși doar parțial, armonizarea cadrului normativ național la prevederile Directivei NIS2[8] și, implicit, a unor elemente esențiale ale Directivei NIS1[9].

[7] https://ncsi.ega.ee/country/md/

[8] ***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;

[9] ***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;

Astfel, Legea privind securitatea cibernetică cuprinde un set de reglementări care au ca scop în principal:

a) stabilirea cadrului general privind cooperarea și coordonarea strategică la nivel național și internațional, prin reglementarea expresă a constituirii unui consiliul coordonator cu rol consultativ al Guvernului, dedicat exclusiv domeniului securității cibernetice și stabilirea obligativității adoptării unei strategii naționale în acest domeniu;

b) desemnarea/instituirea de către Guvern a unei autorități competente în domeniul securității cibernetice la nivel național, care să includă în competența sa, de rând cu funcțiile de coordonare, cooperare internă, supraveghere și control de stat, și pe cele de echipă națională de răspuns la incidentele cibernetice și de punct unic de contact la nivel național;

c) reglementarea legală primară a procesului de coordonare și gestionare a crizelor în domeniul securității cibernetice și atribuirea competenței legale în această materie viitoarei autorități responsabile;

d) stabilirea cadrului legal primar în ce privește obligațiile de asigurare a securității cibernetice nu doar de către persoanele juridice de drept public, ci și de către cele de drept privat, în mod special în ceea ce privește obligațiile de implementare a măsurilor de securitate și în ceea ce privește obligațiile de notificare a incidentelor cibernetice semnificative, și împuternicirea autorității competente la nivel național în acest domeniu cu exercitarea funcțiilor de supraveghere și control de stat al modului în care persoanele vizate îndeplinesc aceste obligații;

e) determinarea cadrului normativ primar pentru identificarea persoanelor juridice ca fiind furnizori de servicii esențiale, împuternicire atribuită, de asemenea, autorității respective, ca parte componentă a funcției de supraveghere etc.

Potrivit prevederilor Legii privind securitatea cibernetică, Guvernul este învestit cu competență de intervenție, de diferită natură (normativă, organizatorică și tehnică), pe un șir de chestiuni în vederea punerii în aplicare a prevederilor acesteia, dintre care în mod special ținem să le evidențiem pe cele care sunt pertinente obiectului de reglementare a proiectului propus spre avizare și anume punerea în aplicare a cadrului legal primar în ce privește obligațiile de asigurare a securității cibernetice de către persoanele juridice de drept public și cele de drept privat, în mod special în ceea ce privește obligațiile de implementare a măsurilor de securitate și în ceea ce privește obligațiile de notificare a incidentelor cibernetice cu impact semnificativ.

Cadrul de politici de securitate cibernetică este oferit de un set de documente de politici publice adoptate de Parlament sau Guvern și care oferă viziunea strategică pentru țară cu privire la modul de înființare, consolidare și asigurare a rezilienței sistemului de securitate cibernetică pentru spațiul informațional al Republicii Moldova.

Din perspectiva **cadrului strategic** următoarele documente de politici cuprind obiective ce condiționează intervenția statului:

Concepția securității informaționale[10], aprobată prin Legea nr. 299/2017

Concepția reprezintă o viziune de ansamblu asupra scopului, obiectivelor, principiilor și direcțiilor de bază ale activității de asigurare a unui nivel înalt al securității informaționale a Republicii Moldova, securitatea informațională fiind parte componentă a sistemului național de securitate. Potrivit acestei concepții măsurile de prevenire, depistare și contracarare a amenințărilor complexe și persistente la adresa securității informaționale pot fi întreprinse doar cu condiția existenței și funcționării unui cadru normativ corespunzător în domeniu, a unor instrumente și metode bine definite, a unor mecanisme de colaborare la nivel național și internațional. Concepția

[10] https://www.legis.md/cautare/getResults?doc_id=105660&lang=ro

securității informaționale a Republicii Moldova este determinată de necesitatea protejării intereselor statului, ale societății și ale persoanei, a obiectivelor vitale și de importanță strategică pentru securitatea națională, de necesitatea asigurării protecției informației atribuite la secret de stat, precum și de necesitatea prevenirii și combaterii criminalității informatice.

Concepția constituie baza pentru elaborarea Strategiei securității informaționale a Republicii Moldova și a Planului de acțiuni pentru implementarea strategiei respective. În primul capitol Concepția descrie situația în domeniu și definește problemele din acest sector, stabilește obiectivele de bază, amenințările la adresa securității informaționale, realizarea cărora are ca scop asigurarea protecției, în spațiul informațional, a drepturilor și libertăților fundamentale, a democrației și a statului de drept. În partea a doua Concepția descrie instrumentele și căile de soluționare a problemelor identificate, inclusiv direcțiile strategice și tactice de asigurare a securității informaționale, principiile și principalele sarcini ale autorităților competente, metodele de asigurare a securității informaționale (juridice, tehnico-organizatorice, economice, contrainformative și de securitate), cooperarea internațională în acest domeniu și organizarea sistemului de asigurare a securității informaționale. În ce privește aspectul organizării sistemului respectiv, concepția desemnează Serviciul de Informații și Securitate ca fiind, în limitele competenței atribuite prin lege, autoritatea națională de coordonare a activității autorităților publice desfășurate în domeniul securității informaționale.

Strategia securității informaționale[11] a Republicii Moldova pentru anii 2019-2024 și Planul de acțiuni pentru implementarea acesteia, aprobate prin Hotărârea Parlamentului nr. 257/2018

După cum s-a menționat mai sus, Concepția securității informaționale reprezintă documentul de bază pentru elaborarea acestei Strategii și documentul de politici ce integrează domeniile centrale și asociate spațiului informațional, ce oferă noțiuni, definește principiile de organizare la nivel de stat, societate și persoană, precum și detaliază metodele juridice, tehnico-organizatorice, economice și contrainformative pentru asigurarea securității informaționale a Republicii Moldova. În acest context, **scopul principal** al Strategiei de securitate informațională este de a lega și integra din punct de vedere juridic domeniile prioritare cu responsabilități și competențe de asigurare a securității informațiilor la nivel național, bazată inclusiv pe reziliența cibernetică. Scopul și obiectivele acestei Strategii se realizează în baza Planului de acțiuni pentru implementarea acesteia. Astfel, în contextul definirii problemelor și al descrierii situației la momentul adoptării strategiei, acest document evidențiază un spectru larg de probleme cu care se confruntă până acum Republica Moldova. Problemele abordate de Strategie se referă la cinci componente de bază ale securității cibernetice și investigației criminalității cibernetice, securitatea spațiului media, componenta de contrainformații și securitate, aspectele juridice și, în final, problemele de conștientizare a maselor. Dintre acestea, Strategia evidențiază problemele cele mai proeminente cum ar fi lipsa unui CERT național (Centrul de răspuns la incidente de securitate cibernetică), responsabil de prevenirea și răspunsul la incidente din domeniul securității cibernetice la scară largă la nivel național, lipsa unui sistem integrat de management al securității cibernetice și un mecanism viabil de audit al securității cibernetice, precum și lipsa de specialiști calificați, programe de formare specializată adresate angajaților organelor de drept, dotarea insuficientă cu echipamente și software, finanțare redusă pentru participarea specialiștilor la proiecte internaționale și evenimente pentru consolidarea capacităților și schimbul de bune practici etc. Strategia include mai multe cerințe fundamentale pentru a obține o

[11] https://www.legis.md/cautare/getResults?doc_id=111979&lang=ro

mai bună guvernare a securității cibernetice la nivel național, precum și o listă de acțiuni propuse și indicatori de progres.

Strategia de transformare digitală a Republicii Moldova pentru anii 2023-2030, aprobată prin Hotărârea Guvernului nr. 650/2023[12]

Unul dintre obiectivele Strategiei de transformare digitală 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. Astfel, 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 responsabilitatea și angajamentul comun pentru susținerea și cooperarea în asigurarea securității cibernetice.

Diverse aspecte ale securității cibernetice sunt abordate și în Strategia securității naționale a Republicii Moldova, aprobată prin Hotărârea Parlamentului nr. 391/2023[13].

Din perspectiva cadrului normativ privind măsurile de securitate a rețelelor și sistemelor informatice, ***Legea nr. 48/2023 privind securitatea cibernetică*** reprezintă cadrul normativ general primar în domeniul securității cibernetice. Implementarea cerințelor, măsurilor și mecanismelor instituite în această lege are ca obiectiv să garanteze un nivel înalt de securitate a rețelelor și sistemelor informatice din Republica Moldova, oferind protecție pentru interesele vitale ale persoanelor fizice și juridice, ale societății și ale statului, precum și ale intereselor naționale ale Republicii Moldova.

Pentru punerea în aplicare a acestei legi au fost adoptate deja un set de acte normative după cum urmează:

Legea nr.58/2024 pentru modificarea unor acte normative, care are ca obiectiv aducerea în concordanță a cadrului normativ primar cu Legea nr. 48/2023;

Hotărârea Guvernului nr. 1028/2023 cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică;

Hotărârea Guvernului nr. 333/2024 cu privire la instituirea, organizarea și funcționarea Consiliului coordonator în domeniul securității cibernetice;

Hotărârea Guvernului nr. 860/2024 cu privire la identificarea furnizorilor de servicii.

Legea nr. 467/2003[14] ***cu privire la informatizare si resursele informaționale de stat*** (art.23) și **Legea nr. 71/2007**[15] **cu privire la registre** (art.24) reglementează, pe de o parte, responsabilitățile autorităților publice în asigurarea securității cibernetice a sistemelor și resurselor informaționale ale statului, iar pe de altă parte, responsabilitățile entităților, inclusiv private, în protecția informațiilor conținute de resursele și prelucrate de sistemele informaționale pe care le creează.

În același timp, cerințele de securitate pentru rețelele publice de comunicații electronice și serviciile de comunicații electronice accesibile publicului sunt prevăzute în ***Legea comunicațiilor electronice nr. 241/2007***[16]. Această lege reglementează activitatea în domeniul comunicațiilor electronice civile a tuturor furnizorilor de rețele sau servicii de comunicații electronice, fie din sectorul public sau privat, și stabilește drepturile și obligațiile utilizatorilor. Legea nu se extinde la rețelele de comunicații speciale. Din punct de vedere al securității rețelelor și serviciilor de comunicații electronice, Agenția Națională pentru Reglementare în Comunicațiile Electronice și

[12] https://www.legis.md/cautare/getResults?doc_id=139408&lang=ro
[13] https://www.legis.md/cautare/getResults?doc_id=141253&lang=ro
[14] https://www.legis.md/cautare/getResults?doc_id=132933&lang=ro
[15] https://www.legis.md/cautare/getResults?doc_id=131038&lang=ro
[16] https://www.legis.md/cautare/getResults?doc_id=133262&lang=ro

Tehnologia Informației este responsabilă de verificarea conformității din perspectiva autorizării a modului de implementare a măsurilor minime de securitate.

De asemenea, **Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate** are ca scop să faciliteze și să eficientizeze schimbul de date și interoperabilitatea în cadrul sectorului public, precum și între sectorul public și cel privat, în vederea creșterii calității serviciilor publice prestate, a creării noilor servicii publice electronice și a asigurării securității informaționale.

Pentru punerea în aplicare a acestor legi, Guvernul a aprobat:

– **Hotărârea Guvernului nr. 201/2017**[17] privind aprobarea cerințelor minime obligatorii de securitate cibernetică, care se adresează atât autorităților guvernamentale, cât și autorităților care nu intră în structura administrativă a Guvernului;

– **Hotărârea Guvernului nr. 482/2020**[18] privind aprobarea măsurilor necesare asigurării securității cibernetice la nivel guvernamental, care completează, în special, cu măsuri organizatorice decizia sus-menționată, dar numai pentru autoritățile și instituțiile publice care fac parte din structura administrativă guvernamentală;

– **Hotărârea Guvernului nr. 388/2022** [19] privind aprobarea Concepției Sistemului Informațional „Registrul de Stat al Incidentelor de Securitate Cibernetică", care este una dintre măsurile preliminare pentru stabilirea unei platforme informaționale pentru comunicarea strategică cu entitățile publice, precum și pentru asigurarea evidenței amenințărilor, vulnerabilităților în spațiul cibernetic și a incidentelor de securitate cibernetică identificate sau raportate.

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

1. ***Guvernul și autoritatea 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;

2. ***Persoanele juridice de drept public***, inclusiv ***autoritățile administrației publice locale*** – categorie care prin efectul legii sunt identificate furnizori esențiali sau importanți de servicii;

3. ***Persoanele juridice de drept privat, inclusiv întreprinderile de stat,*** care cad sub incidența prevederilor proiectului de act normativ;

4. ***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.

Prezentul proiect de hotărâre de Guvern este parte indispensabilă a setului de acte care stau la soluționarea problemei definite la pct. 1 a) din prezenta analiză de impact. Astfel, problematica enunțată și descrisă în subcompartimentele anterioare, rezumată la reziliența cibernetică scăzută a actorilor esențiali, perturbarea activității cărora ar putea prejudicia considerabil viața economică și socială caracterizată în mod special printr-un nivel insuficient de protecție împotriva incidentelor, riscurilor și amenințărilor la securitatea rețelelor și a sistemelor informatice ale acestora are la bază o serie de **cauze**, principalele dintre care constau în următoarele:

1. lipsa unui cadru normativ complet, de gestionare a crizelor la nivel național, inclusiv în caz de incidente cibernetice de mare amploare sau care ar putea sau au impact semnificativ asupra sectoarelor critice sau societății;

[17] https://www.legis.md/cautare/getResults?doc_id=98644&lang=ro
[18] https://www.legis.md/cautare/getResults?doc_id=122272&lang=ro
[19] https://www.legis.md/cautare/getResults?doc_id=132011&lang=ro

2. măsuri implementate insuficiente de securitate a rețelelor și sistemelor informatice sau chiar lipsa acestora, ale unor actori din sectorul privat, a căror activitate poate fi calificată ca fiind esențială în prestarea unor servicii;

3. schimbul insuficient de informații cu privire la incidente, riscuri și amenințări de securitate cibernetică în ambele sectoare, public și privat, și lipsa unei platforme digitale pentru schimbul de informații fiabile privind amenințările, riscurile și incidentele de securitate, conform prevederilor Legii nr. 48/2023 privind securitatea cibernetică. Majoritatea breșelor de securitate nu sunt raportate și trec neobservate, în principal din cauza reticenței companiilor de a împărtăși aceste informații, de teama daunelor aduse reputației sau a răspunderii. De cele mai multe ori, persoanele responsabile de securitatea rețelelor și a sistemelor informatice împărtășesc informațiile relevante doar cu grupuri mici pe care le consideră de încredere, mai degrabă decât să treacă prin canalele oficiale.

4. există în prezent un cadru instituțional, procedural și normativ-juridic incomplet pentru schimbul de informații de încredere privind amenințările, riscurile și incidentele de securitate între sectorul public și cel privat.

3. Obiectivele urmărite şi soluţiile propuse

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

Prezentul 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 prezentului proiect de hotărâre de Guvern, care odată realizate vor contribui la atingerea obiectivului general enunțat mai sus, ținem să evidențiem următoarele:

– instituirea unei abordări uniforme în gestionarea riscurilor în materie de securitate cibernetică prin elaborarea și adoptarea unui set unic de norme și proceduri aplicabile tuturor entităților vizate de prezenta hotărâre de Guvern;

– reglementarea unor chestiuni generale privind procesul de notificare a incidentelor cibernetice cu impact semnificativ de către furnizorii de servicii către Agenția pentru Securitate Cibernetică

– stabilirea unei bazei juridice clare pentru determinarea sincronizată a impactului semnificativ al unor incidente cibernetice, cu accent pe unele tipuri de furnizori din cadrul sectorului infrastructurii digitale, gestionarea serviciilor TIC și cel al furnizorilor digitali;

– clarificarea și aplicarea principiului proporționalității în implementarea măsurilor de securitate cibernetică prin dezvoltarea unui cadru metodologic care să asigure corelarea măsurilor respective cu riscurile identificate, precum și echivalența dintre legislația sectorială și cea privind securitatea cibernetică.

Proiectul de act normativ propus spre examinare are ca **obiect de reglementare**:

a) cerințele privind măsurile de gestionare a riscurilor la adresa securității rețelelor și sistemelor informatice pe care le utilizează furnizorii de servicii la prestarea serviciilor esențiale;

b) aspecte generale privind procedura de notificare a incidentelor cibernetice cu impact semnificativ, precum și condiții specifice pentru unele tipuri de furnizori de servicii în care un incident cibernetic urmează a fi calificat ca fiind semnificativ;

c) modul de evaluare a echivalenței efectelor legislației sectoriale în raport cu cele ale Legii nr. 48/2023 privind securitatea cibernetică, prevăzut în art. 3 alineatele (5) și (6) din Legea nr.48/2023 privind securitatea cibernetică.

Art. 23 alin. (2) lit. c) din Legea nr. 48/2023 stabilește în sarcina Guvernului obligația de a asigura elaborarea și adoptarea actelor normative necesare punerii în aplicare a prevederilor acestei legi. Articolul 11 din legea respectivă prevede obligațiile furnizorilor de servicii în contextul asigurării securității cibernetice prin implementarea măsurilor de securitate ale rețelelor și sistemelor informatice pe care le utilizează la prestarea serviciilor esențiale, adecvate și proporționale riscurilor identificate și evaluate. Alineatul (2) din același articol la pct. 2 enumeră tematicile care trebuie abordate atunci când furnizorul de servicii își evaluează riscurile și implementează astfel de măsuri. Tematicile respective sunt preluate din art. 21 alin. (2) din Directiva NIS2 în contextul armonizării legislației naționale la cea a UE. În temeiul alin. (5) din art. 21 al Directivei NIS2 Comisia Europeană a fost împuternicită să adopte un act de punere în aplicare în ce privește cerințe de gestionare a riscurilor în materie de securitate cibernetică pentru furnizorii de servicii DNS, registrele de nume TLD, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea și prestatorii de servicii de încredere. În consecință Comisia a adoptat Regulamentul de punere în aplicare (UE) 2024/2690. Analiza prevederilor Regulamentului respectiv, efectuată de către experți internaționali și naționali a relevat pertinența și concludența aplicării prevederilor acestuia în raport cu toate persoanele juridice care vor fi identificate de către Agenția pentru Securitate Cibernetică în calitate de furnizori de servicii în sensul Legii nr. 48/2023. În consecință **domeniul de aplicare al proiectului** propus spre examinare se extinde asupra tuturor furnizorilor de servicii, esențiali sau importanți, care vor fi identificați de Agenția pentru Securitate Cibernetică în conformitate cu prevederile Hotărârii Guvernului nr. 860/2024. Totuși, trebuie relevat faptul că această extindere nu este una arbitrară, ci este susținută de reglementări privind aplicarea principiului proporționalității, inclusiv a unei marje discreționare motivate și limitate a furnizorului de servicii în aplicarea măsurilor respective, precum și de reglementări de punere în aplicare treptată a prevederilor acestui act normativ, prevăzute de partea dispozitivă a proiectului de hotărâre a Guvernului.

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, termenul de implementare a cerințelor privind măsurile de gestionare a riscurilor în materie de securitate cibernetică de către furnizorii de servicii și sarcini pentru Agenția pentru Securitate Cibernetică. Termenul de implementare este diferit pentru cele două categorii de furnizori de servicii: pentru cei esențiali – 12 luni, iar pentru cei importanți 18 de luni din data intrării în vigoare a hotărârii. Intrarea în vigoare urmând să aibă loc în baza regulii generale, stabilită de art. 56 alin. (1) din Legea nr. 100/2017 privind actele normative, adică la o lună din data publicării. În partea dispozitivă a proiectului de act normativ, de asemenea sunt stabilite un set de sarcini atât furnizorilor de servicii, cât și Agenției orientate spre inițierea primei iterații de evaluare a maturității furnizorilor de servicii și determinarea inconsistențelor, implementarea îmbunătățirilor, în baza recomandărilor evaluatorilor, inclusiv ale Agenției pentru Securitate Cibernetică.

În anexă este dat Regulamentul cu privire la modul de aplicare a măsurilor de securitate a rețelelor și sistemelor informatice de către furnizorii de servicii în sectoarele critice. Acesta include trei capitole și o anexă.

Capitolul I „Dispoziții generale” cuprinde prevederi care determină obiectul de reglementare al proiectului, actele legislative relevante care cuprind definițiile unor noțiuni utilizate în textul proiectului de act normativ și cercul de subiecți care cad sub incidența prevederilor actului normativ.

Capitolul II „Modul de aplicare a cerințelor privind măsurile de securitate a rețelelor și sistemelor informatice a furnizorilor de servicii în sectoarele critice” stabilește reglementări ale unor aspecte generale privind implementarea cerințelor privind măsurile de securitate stabilite în anexa la proiectul de Regulament. În mod specific este acordată o marjă discreționară largă furnizorilor de servicii în utilizarea standardelor naționale și internaționale, atunci când un nivel de detaliere mai înaltă este necesar pentru implementarea adecvată a anumitor cerințe. De asemenea Agenția pentru Securitate Cibernetică urmează să vină cu orientări metodologice și explicații furnizorilor de servicii atunci când aceștia au nevoie în procesul de aplicare a cerințelor respective, inclusiv în ce privește aplicarea principiului proporționalității. De asemenea, în acest capitol este reglementat și modul de aplicare a principiului proporționalității de către furnizorii de servicii atunci când determină relevanța unei anumite cerințe de securitate pentru tratarea riscurilor identificate și condițiile când cerința aplicată este considerată ca fiind proporțională (dacă este adecvată, dacă este aplicabilă și în măsura în care este fezabilă.) Atunci când identifică și prioritizează măsurile adecvate pentru abordarea riscurilor, furnizorii de servicii trebuie să ia în considerare rezultatele evaluării riscurilor, eficacitatea măsurilor și costul punerii în aplicare în raport cu beneficiile preconizate. Dacă un furnizor de servicii consideră că nu este adecvat, nu este aplicabil sau nu este fezabil ca acesta să aplice anumite cerințe din anexa la proiectul regulamentului, furnizorul respectiv de servicii trebuie să motiveze documentat această neaplicare. În context trebuie menționat că acest principiu al proporționalității va constitui și un instrument pentru Agenția pentru Securitate Cibernetică atunci când își exercită atribuțiile de supraveghere. Aceasta va trebui să țină cont de raționamentele de neaplicare ale furnizorului de servicii și de timpul rezonabil care este necesar pentru punerea în aplicare a unei anumite cerințe.

Acest capitol cuprinde și reglementări care stabilesc în sarcina furnizorilor de servicii efectuarea, o dată la 3 ani, a unor audituri externe de securitate cibernetică în vederea determinării nivelului de conformitate cu cerințele privind măsurile de securitate a rețelelor și sistemelor informatice. Totodată, în acest capitol este propusă o prevedere care exonerează furnizorii de servicii, care sunt conformi cu standardul național de securitate a informației și cele internaționale corespunzătoare, de la aplicarea cerințelor de securitate stabilite de proiect. Totuși aceasta nu exclude competența Agenției de a verifica conformitate cu aceste cerințe în totalitate sau în parte în contextul exercitării de către aceasta a funcției de supraveghere și control de stat.

Capitolul III „Modul de evaluare a echivalenței efectelor obligațiilor de asigurare a securității cibernetice” din proiectul Regulamentului cuprinde prevederi care stabilesc condițiile privind dispozițiile minime pe care trebuie să le includă legislația sectorială din punctul de vedere al reglementării aspectelor ce țin de măsurile de gestionare a riscurilor și obligațiile de raportare a incidentelor cibernetice cu impact semnificativ, în raport cu Legea nr. 48/2023, pentru a fi aplicabilă furnizorilor de servicii în materie de gestionare a riscurilor și raportare a incidentelor. Acest capitol vine cu un set de clarificări necesare atât pentru furnizorii de servicii, cât și pentru Agenția pentru Securitate Cibernetică în procesul de determinare a cerințelor de securitate aplicabile. Reglementările propuse în acest capitol sunt bazate pe Orientările Comisiei privind aplicarea articolului 4 alineatele (1) și (2) din Directiva (UE) 2022/2555 (Directiva NIS 2)[20].

Capitolul IV Procedura de notificare a incidentelor cibernetice cu impact semnificativ din proiectul Regulamentului include prevederi, întemeiate pe art. 12 din Legea nr. 48/2023, și reglementează aspecte generale privind procedura de notificare incidentelor cibernetice cu impact semnificativ, inclusiv, interacțiunea dintre subiecții acestui proces. Este important de menționat că

[20] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52023XC0918(01)

aspectul general al acestor prevederi este datorat faptului că acestea vor fi completate de prevederi ale actelor interne ale furnizorilor de servicii și ale Agenției pentru Securitate Cibernetică aprobate în legătură cu necesitatea implementării cerințelor privind măsurile de securitate ce vizează gestionarea incidentelor.

În acest capitol este stabilit și conținutul notificărilor privind incidentele cibernetice cu impact semnificativ transmise de către furnizorii de servicii către Agenția pentru Securitate Cibernetică. Astfel raportarea incidentelor semnificative către Agenție urmează a fi realizată în trei etape:

- prin transmiterea unei notificări care să includă în cazul în care există, informații privind suspiciunile că incidentul semnificativ este cauzat de acte ilegale sau răuvoitoare sau dacă există probabilitatea că acest incident ar putea avea un impact transfrontalier;

- printr-o actualizare a notificării incidentului, care să cuprindă o evaluare inițială a incidentului semnificativ, inclusiv a gravității și a impactului acestuia, precum și, dacă există, a indicatorilor de compromitere. Suplimentar actualizarea notificării incidentului, atunci când există, trebuie să conțină o actualizare a informațiilor transmise în cadrul notificării.

- printr-un raport final care să includă o descriere detaliată a incidentului, inclusiv a gravității și a impactului acestuia; tipul de amenințare sau de cauză principală care este probabil să fi declanșat incidentul; măsurile de atenuare aplicate și în curs de aplicare și, dacă este cazul, o descriere a impactului transfrontalier al incidentului.

Agenția potrivit prevederilor părții dispozitive a proiectului de hotărâre urmează să implementeze, în termen de 6 luni, mecanisme, inclusiv prin utilizarea mijloacelor tehnice, care să asigure un schimb direct, sistematic și imediat de informații în contextul realizării de către furnizorii de servicii a obligațiilor de raportare a incidentelor cibernetice cu impact semnificativ. Această sarcină a Agenției decurge din prevederile art. 7 alin. (4) punctele 5) și 7) ale Legii nr. 48/2023, conform cărora Agenția acordă asistență furnizorilor de servicii în procesul de răspuns la incidentele cibernetice, precum și creează platforme de management al incidentelor cibernetice și pentru schimbul de informații. De asemenea, în procesul de implementarea a prevederilor proiectului de act normativ, Agenția trebuie să țină cont și să faciliteze și schimbul voluntar de informații în contextul punerii în aplicare a prevederilor art. 17 din Legea nr. 48/2023.

Prevederile cuprinse de **Capitolul V „Condiții specifice pentru determinarea impactului semnificativ al incidentelor cibernetice pentru unele tipuri de furnizori de servicii”** vizează condiții de determinare a impactului semnificativ al unui incident cibernetic și au ca obiectiv punerea în aplicare a art. 12 alin. (5) din Legea nr. 48/2023, în ce privește furnizorii de servicii DNS, Registratorul național al domeniului de nivel superior .md, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate și furnizorii de servicii de securitate gestionate, furnizorii de piețe online, furnizorii de motoare de căutare online, furnizorii de platforme de servicii de socializare în rețea și prestatorii de servicii de încredere, în vederea clarificării unor aspecte ce vizează modul de determinare a unui incident cibernetic pentru. Astfel, art. 12 alin. (5) din Legea nr. 48/2023 stabilește condițiile când un incident cibernetic se consideră că are un impact semnificativ, și anume atunci când:

a) gravitatea consecințelor incidentului cibernetic este determinată ca fiind cel puțin înaltă în raportul de evaluare a riscurilor de securitate a rețelelor și sistemelor informatice, întocmit în conformitate cu prevederile art.11 alin.(2) pct.1) din lege sau cu cerințele prevăzute de actele aprobate potrivit art.11 alin.(4) din Legea nr. 8/2023;

b) din cauza incidentului cibernetic, prestarea serviciului nu poate fi continuată după expirarea perioadei maxime admise prevăzute în acordul privind nivelul agreat al serviciilor, încheiat în cadrul

relațiilor contractuale ale furnizorului de servicii cu alte persoane, sau prevăzute de cerințele privind continuitatea serviciului stabilite în documentația indicată la art.11 alin.(2) pct.1)–3);

c) continuitatea serviciului altui furnizor de servicii este perturbată de incidentul cibernetic;

d) furnizorului de servicii care notifică incidentul cibernetic, altui furnizor de servicii sau utilizatorilor serviciilor le-au fost cauzate sau le-ar putea fi cauzate prejudicii materiale sau nonmateriale considerabile din cauza incidentului cibernetic.

Punctulv25 din acest capitol asigură transpunerea art. 3 din Regulamentul de punere în aplicare (UE) 2024/2690, prin prisma prevederilor art. 12 alin. (5) lit. d) din Legea nr.48/2023, stabilind cerințe pentru toți furnizorii de servicii în determinarea caracterului considerabil al prejudiciilor materiale și non-materiale la determinarea caracterului semnificativ al unui incident cibernetic. În continuare punctele 26-35 asigură transpunerea prevederilor art. 5-14 din Regulamentul de punere în aplicare (UE) 2024/2690 prin prisma prevederilor art. 12 alin. (5) literele a) și b) din Legea securității cibernetice, stabilind cerințe pentru anumite categorii de furnizori de servicii, atunci când determină caracterul semnificativ al unui incident cibernetic, în ce privește gradul de indisponibilitate a serviciului, gradul de compromitere a integrității, confidențialității sau autenticității informațiilor sau datelor, nivelul de compromitere a accesului fizic sau protecția fizică a unor anumite infrastructuri critice.

În **Anexa la proiectul Regulamentului** sunt prevăzute **Cerințele privind măsurile de securitate a rețelelor și sistemelor informatice ale furnizorilor de servicii în sectoarele critice.** Scopul acestor cerințe este să asigure un nivel uniform și suficient de maturitate a furnizorilor de servicii în procesul de asigurare a securității rețelelor și sistemelor informatice pe are aceștia le dețin. Cerințele transpun practic în totalitate prevederile anexei la Regulamentul de punere în aplicare (UE) 2024/2690 cu limitările ce țin de terminologia legislației moldovenești și de extinderea domeniului de aplicare a cerințelor la toți furnizorii de servicii. Problematicile abordate în cele 13 capitole ale anexei se fundamentează pe prevederile art. 11 alin. (2) pct. 2) și vizează:

1. ***Politica privind securitatea rețelelor și a sistemelor informatice*****,** inclusiv rolurile, responsabilitățile și autoritățile în cadrul furnizorului de servicii;
2. ***Politica de gestionare a riscurilor*** la adresa securității rețelelor și sistemelor informatice: cadrul de gestionare a riscurilor; monitorizarea conformității și examinarea independentă a securității informațiilor și rețelelor;
3. ***Gestionarea incidentelor:*** politica de gestionare a incidentelor, monitorizare și jurnalizare a activităților în rețelele și sistemele informatice, raportarea evenimentelor, evaluarea și clasificarea evenimentelor, răspunsul la incidente, analizele post-incident;
4. ***Continuitatea activității și gestionarea crizelor:*** planurile de continuitate a activității și de recuperare în caz de dezastru, gestionarea copiilor de rezervă și a redundanței, procesul de gestionare a crizelor;
5. ***Securitatea lanțului de aprovizionare:*** politica de securitate a lanțului de aprovizionare și registrul furnizorilor și al prestatorilor de servicii direcți ai furnizorului de servicii;
6. ***Securitatea în achiziționarea, dezvoltarea și întreținerea rețelelor și a sistemelor informatice:*** securitatea în achiziționarea de servicii TIC sau de produse TIC; ciclul de viață al dezvoltării securizate; gestionarea configurației; gestionarea modificărilor, reparații și întreținere; testele de securitate; gestionarea corecțiilor de securitate; securitatea rețelelor; segmentarea rețelei; protecția împotriva software-ului rău-intenționat și neautorizat, gestionarea și divulgarea vulnerabilităților;
7. ***Politici și proceduri pentru a evalua eficacitatea măsurilor de gestionare a riscurilor în materie de securitate cibernetică;***

8. ***Practici de bază în materie de igienă cibernetică și formare în domeniul securității cibernetice:*** sensibilizare și practici de bază în materie de igienă cibernetică; formare în domeniul securității;
9. ***Criptografie:*** politica și procedurile legate de criptografie cu scopul de a asigura utilizarea adecvată și eficace a criptografiei pentru a proteja confidențialitatea, autenticitatea și integritatea datelor în conformitate cu clasificarea activelor;
10. ***Securitatea resurselor umane,*** inclusiv verificarea antecedentelor, procedura în caz de încetare sau modificare a raporturilor de muncă și procesul disciplinar;
11. ***Controlul accesului,*** inclusiv politica de control al accesului, gestionarea drepturilor de acces, conturile privilegiate și conturile de administrare a sistemului, sisteme de administrare, identificarea, autentificarea, inclusiv multifactor,
12. ***Gestionarea activelor*****,** inclusiv clasificarea acestora, politica privind suporturile amovibile, inventarul activelor;
13. ***Securitatea mediului și fizică,*** inclusiv utilități de sprijin, protecția împotriva amenințărilor fizice și de mediu, controlul perimetrului și al accesului fizic.

Astfel, art. 11 alin. (1) din Legea nr. 48/2023 stabilește că aceste cerințe ale măsurilor de securitate urmează a fi implementate în mod continuu de către furnizorii de servicii în scopul prevenirii incidentelor cibernetice, soluționării incidentelor cibernetice, prevenirii și atenuării impactului asupra continuității serviciului ori asupra securității rețelei și/sau sistemului informatic, cauzat de un incident cibernetic, precum și prevenirii și atenuării impactului potențial asupra continuității serviciilor ori asupra securității rețelelor și sistemelor informatice dependente de cele ale furnizorului de servicii. Abordarea bazată pe risc reflectată de alineatul (2) al aceluiași articol impune furnizorilor de servicii să efectueze și să documenteze o evaluare a riscurilor de securitate a rețelelor și sistemelor informatice și să descrie măsurile pentru soluționarea unui potențial incident cibernetic, precum și să implementeze măsuri de securitate corespunzătoare și proporționale pentru a gestiona riscurile de securitate a rețelelor și a sistemelor informatice.

Din punctul de vedere al elementelor noi care vor fi introduse în legislația națională prin adoptarea proiectului respectiv de act normativ relevăm în mod special unificarea într-un singur act a reglementărilor privind gestionarea riscurilor în materie de securitatea cibernetică atât sub aspectul relației domeniul public - domeniul privat, cât și din perspectiva sectoarelor critice în care sunt prestate servicii esențiale pentru funcționarea activităților societale și economice critice. Cu toate acestea, această unificare este una care decurge din necesitatea asigurării punerii în aplicare a prevederilor Legii nr. 48/2023, măsurile de securitate în sine nefiind un element de o noutate absolută pentru o bună parte a potențialilor furnizori de servicii. Spre exemplu, majoritatea cerințelor din anexa la proiectul Regulamentului sunt deja obiectul reglementării Hotărârii Guvernului nr. 201/2017, care are ca subiecți toate personale juridice de drept public cu competență la nivel național. De asemenea, unor categorii distincte de furnizori de servicii, cum sunt, spre exemplu, furnizorii de rețele publice de comunicații electronice și/sau de servicii de comunicații electronice accesibile publicului, le sunt în prezent aplicabile cerințe, într-o anumită măsură similare, prin Hotărârea ANRCETI nr. 60/2019 pentru aprobarea Modalității de implementare a măsurilor minime de securitate și integritate a rețelelor publice de comunicații electronice și/sau serviciilor de comunicații electronice accesibile publicului.

Totodată, propunerea privind modificarea Hotărârii Guvernului 860/2024 cu privire la identificarea furnizorilor de servicii derivă în general din necesitatea eficientizării procesului de identificare a furnizorilor de servicii , precum și din cea de protejare a siguranței publice prin

restricționarea accesului la actele administrative emise de către Agenția pentru Securitate Cibernetică în raport cu furnizorii de servicii.

Astfel, în particular, se propune completarea Anexei 1 cu un punct nou ce urmează să restricționeze accesul la notificarea prealabilă și la actul administrativ emis de către Agenție în cadrul procedurii administrative cu potențialii furnizori de servicii pentru a nu prejudicia procedura administrativă și nemijlocit siguranța națională.

În altă ordine de idei, modificarea anexei 3 la Hotărârea Guvernului nr. 860/2024 este necesară deoarece, în urma aplicării acesteia, s-a constatat că formularea actuală a punctului 10 din anexa 3 permite interpretări duale, generând dificultăți în întocmirea Listei furnizorilor de servicii care este esențială în contextul asigurării securității cibernetice a furnizorilor de servicii esențiali și importanți. Mai mult, includerea listei la informație atribuită la secret de stat creează blocaje în activitatea Agenției, din perspectiva identificării și urmării amenințărilor și vulnerabilităților cibernetice asupra entităților esențiale și importante. Totodată, atribuirea la secret de stat a listei este lipsită de sens deoarece această listă poate fi dedusă din criteriile ce sunt stabilite de către Guvern care sunt stipulate într-un act normativ public.

Pentru a evita blocajele de întocmire și menținere a listei, se propune revizuirea punctului 10, oferindu-i o formulare mai clară. Conform articolului 34 din Constituție, dreptul la informație de interes public nu poate fi îngrădit, însă acesta trebuie să fie exercitat fără a compromite siguranța națională sau protecția cetățenilor.

Totodată, având în vedere caracterul sensibil al listei furnizorilor de servicii, aceasta nu poate fi pusă la dispoziția publicului fără restricții. Se propune, așadar, ca accesul la listă să fie limitat, iar modul de gestionare și utilizare a acestor informații să fie stabilit prin Ordinul Directorului Agenției pentru Securitate Cibernetică.

Această modificare este în concordanță cu practicile europene, unde, deși accesul la astfel de liste este restricționat, acestea nu sunt clasificate drept secret de stat. Regimuri similare se regăsesc în Germania, Belgia, Estonia, Spania și alte state europene.

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

Determinarea unei valori absolute a **impactului financiar asupra mediului de afaceri** nu poate fi determinată în prealabil. Numărul mare de indicatori necunoscuți sau variabili nu permite o evaluare a distribuției costurilor de securitate cibernetică. Dintre acești indicatori ar putea fi relevați cel puțin următorii: starea actuală de securitate a fiecărei organizații în parte; numărul exact de furnizori de servicii care vor cădea sub incidența prevederilor Legii nr. 48/2023 și implicit a obligațiilor privind implementarea măsurilor de securitate a rețelelor și sistemelor lor informatice; variabilitatea mare a domeniului de aplicare a măsurilor de securitate cibernetică, care poate fi foarte diferit de la o organizație la alta, inclusiv în funcție de tipul acesteia, dimensiunea acestea, sectorul și subsectorul în care activează; ponderea cheltuielilor destinate asigurării securității cibernetice în totalul cheltuielilor destinate dezvoltării tehnologiei informației și comunicațiilor în cadrul

organizației; variabilitatea costurilor în timp legată de aspecte macroeconomice și de evoluția tehnologiei, etc.

Totuși unele puncte de referință sunt oferite de studiile și rapoartele realizate la nivel european și internațional care permit având anumite date la nivel național determinarea estimativă a impactului financiar asupra mediului de afaceri. Astfel, potrivit Raportului [21] de evaluare a impactului la propunerea de Directivă a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în întreaga Uniune, de abrogare a Directivei (UE) 2016/1148 (Directiva NIS2): „Pe baza previziunilor periodice ale Gartner din 2012 până în 2020 privind procentajul cheltuielilor globale cu securitatea TIC din cheltuielile TIC și din veniturile totale, precum și ținând seama de cele mai recente date sectoriale ale Gartner disponibile Comisiei, în scopul evaluării impactului s-a presupus că media cheltuielilor pentru securitatea TIC pe sector în 2020 este de aproximativ **9,14%** din cheltuielile totale TIC. În funcție de nivelul de maturitate și de capacitățile de securitate cibernetică ale sectorului, precum și de nivelul de digitalizare, această medie ar putea fi ajustată cu +/-3%. În plus, cheltuielile medii TIC pe sector sunt estimate la aproximativ **5,69% din cifra de afaceri** totală și, prin urmare, cheltuielile medii cu securitatea TIC din cifra de afaceri totală pe sector în 2020 sunt estimate la **aprox. 0.52%**.„

Cu toate acestea aceste estimări au fost considerate ca fiind destul de prudente. „Un studiu privind investițiile NIS comandat de ENISA și realizat de Gartner indică un nivel mai scăzut al cheltuielilor pentru securitatea TIC în Europa, de aproximativ 6 % din bugetul TIC începând cu 2016, organizațiile din sectorul bancar, al serviciilor financiare și al produselor farmaceutice având un raport mai mare de 5 %, în timp ce sectoare precum transporturile, educația și comerțul cu amănuntul ar avea cele mai mici astfel de raporturi, sub 2,5 %.”

Din perspectiva rezultatelor celor două analize efectuate de către Comisia Europeană și ENISA, odată cu finalizarea procesului de identificare a furnizorilor de servicii de către Agenția pentru Securitate Cibernetică conform Hotărârii Guvernului nr. 860/2024 „Cu privire la identificarea furnizorilor de servicii”, va fi cunoscută lista furnizorilor de servicii și fiecare caz aparte, cunoscând cifra de afaceri al acestor entități prin aplicarea procentului de 0,52% va fi posibil de determinat costurile aproximative ale implementării măsurilor de securitate. Cu toate aceste, chiar și valorile respective vor fi destul de aproximative nefiind cunoscut nivelul actual de maturitate al fiecărui furnizori în parte.

Suplimentar considerăm relevant să menționăm că în 2024 ENISA a produs cel de-al cincilea Raport privind investițiile în securitatea rețelelor și informațiilor (NIS Investments 2024Report)[22] oferind un set de concluzii relevante pentru estimarea globală a impactului asupra sectorului privat, bazate pe procesare datelor de la „1 350 de organizații din toate cele 27 de state membre ale UE, acoperind toate sectoarele NIS 2 de mare importanță, precum și sectorul de producție”. Raportul oferă o „perspectivă asupra pregătirii entităților de a se conforma noilor cerințe, precum și asupra provocărilor cu care se confruntă acestea”. Principalele concluzii relevante ale raportului care pot oferi furnizorilor de servicii o suficientă bază pentru a-și estima costurile de implementare sunt următoarele:

„a) Organizațiile alocă 9,0% din investițiile lor IT pentru securitatea informațiilor, o creștere semnificativă de 1,9 puncte procentuale față de anul trecut.

b) Organizațiile alocă 11,1 % din ENI (echivalent normă întreagă) pentru securitatea informațiilor, ceea ce reprezintă o scădere de 0,8 % față de anul trecut, în ciuda creșterii generale a

[21] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020SC0345, pag. 71

[22] https://www.enisa.europa.eu/publications/nis-investments-2024

cheltuielilor cu securitatea cibernetică și al patrulea an consecutiv în care se observă o scădere a acestui indicator.

c) 89% dintre organizații vor avea nevoie de mai mult personal în domeniul securității cibernetice pentru a se conforma NIS 2, în special în domeniile arhitecturii și ingineriei securității cibernetice (46%) și operațiunilor de securitate cibernetică (40%).

d) Organizațiile vor avea nevoie, de asemenea, de ENI suplimentare pentru a se conforma altor acte legislative orizontale (CRA - 85%) sau verticale (DORA - 84%; NCCS - 81%) privind securitatea cibernetică.

e) Majoritatea organizațiilor anticipează o creștere punctuală sau permanentă a bugetelor de securitate cibernetică pentru conformitatea cu NIS 2, deși un număr substanțial de entități nu vor putea solicita bugetul suplimentar necesar, un procent care este deosebit de ridicat pentru IMM-uri (34%)...".

De asemenea, din perspectiva impactului financiar asupra sectorului privat trebuie să relevăm și informațiile aduse în analiza de impact la proiectul de Lege privind securitatea cibernetică la orientările pe această dimensiune oferite de Comisia Europeană în procesul de evaluare a costurilor de conformare pentru mediul privat în procesul de pregătire a propunerii de Directivă NIS1: „Pornind de la costurile totale de conformare pentru sectorul privat, care variază între 360 și 720 de milioane de euro, costul de conformare pentru fiecare întreprindere mică și mijlocie s-ar situa între 2 500 și 5 000 de euro. La efectuarea calculului, s-a presupus că întreprinderile mici și mijlocii reprezintă 20% din cifra de afaceri a întreprinderilor private vizate de regulament și reprezintă 68% din toate întreprinderile afectate, adică puțin peste 28 000 de întreprinderi. Acesta este costul mediu estimat pentru fiecare IMM pentru atingerea nivelului actual de "cel mai bun din clasă" în ceea ce privește protecția NIS. Pe măsură ce tehnologiile evoluează, riscurile, pe de o parte, și măsurile de protecție, pe de altă parte, vor continua să evolueze și ele. Astfel, vor fi necesare investiții continue pentru a ține pasul cu stadiul actual al tehnologiei, dar este foarte dificil, în acest stadiu, să se prevadă care vor fi costurile pe care le implică menținerea pasului cu evoluțiile tehnologice. Cu toate acestea, aceste investiții vor garanta că atât întreprinderile mari și mici, cât și economia europeană vor fi bine poziționate pentru a profita de avantajele pieței globale a securității cibernetice, care, potrivit estimărilor, se va număra printre segmentele cu cea mai rapidă creștere din sectorul tehnologiei informației (IT) în următorii 3-5 ani; în 2011, piața securității cibernetice valora 63,7 miliarde de dolari și se preconizează că va crește între 80 și 120,1 miliarde de dolari până în 2017."

În ce privește costurile pentru entitățile administrației publice și furnizorii de servicii asociați cu raportarea obligatorie a unui incident semnificativ, Comisia Europeană a estimat în aceeași analiză de impact următoarele:

„Pentru a evalua costurile de raportare a incidentelor grave din NIS, a fost extrapolată o estimare a notificărilor care ar trebui efectuate pe parcursul unui an, pe baza datelor existente privind punerea în aplicare a articolului 13a din directiva-cadru privind comunicațiile electronice. Pe această bază, numărul de notificări de incidente NIS preconizate s-ar ridica la aproximativ 1 700 pe an. Presupunând că un angajat ar trebui să aloce 0,5 zile lucrătoare pentru notificare și că notificarea ca atare ar avea costuri neglijabile (de exemplu, ar fi efectuată prin intermediul unui e-mail), costul preconizat pentru fiecare notificare de încălcare ar fi de 125 EUR, ceea ce ar duce la un cost total pentru notificarea încălcărilor pe bază anuală de 212 500 EUR la nivelul UE. În ceea ce privește posibilele investigații care pot fi inițiate de către autoritățile competente din NIS cu privire la respectarea obligațiilor de gestionare a riscurilor și de notificare a incidentelor NIS, nu este posibil în acest stadiu să se estimeze dacă și câte investigații ar putea fi inițiate. Cu toate acestea, se poate presupune în mod rezonabil că între 10 și 20% din notificările de incidente NIS ar putea fi urmate

de o investigație, ceea ce corespunde unei valori absolute de 170-340 de investigații preconizate pe an. Ținând cont de costul salarial standard, costul maxim pentru entitatea afectată ar fi de maximum 25 000 EUR pe investigație…".

Cu toate acestea, trebuie remarcat că acestea nu sunt cheltuieli care ar trebui efectuate într-un interval scurt de timp. Având în vedere prevederile punctelor 6 și 7 ale proiectului de Regulament costurile necesare pentru implementarea cerințelor de securitatea pot fi eșalonate de-a lungul anilor, în funcție de prioritizarea activelor critice vizate și de capacitatea financiară a furnizorului de servicii. În plus, trebuie să se țină cont de faptul că punerea în aplicare a măsurilor de securitate nu este un proiect unic cu costuri introductive, ci un proces continuu în cadrul fiecărei entități, având în vedere că multe măsuri de securitate necesită actualizări regulate, monitorizare și îmbunătățire continuă.

Sub aspectul **impactului financiar asupra sectorului public** acesta trebuie examinat din perspectiva a două componente: costurile de implementare ce urmează a fi suportate de către Agenția pentru Securitatea Cibernetică din punctul de vedere al măsurilor de implementare descrise în punctul 9 din prezenta notă și costurile și cheltuielile ce urmează a fi suportate de către furnizorii de servicii – persoane juridice de drept public pentru implementarea cerințelor privind măsurile de gestionare a riscurilor în materie de securitate cibernetică și a celor de raportare a incidentelor cibernetice cu impact semnificativ.

Astfel, în ce privește prima componentă, realizarea de către Agenție a activităților de implementare nu implică cheltuieli suplimentare la cele care sunt deja prevăzute în bugetul de stat. Astfel, în Legea bugetului de stat pentru anul 2025, Ministerului Dezvoltării Economice și Digitalizării în subprogramul bugetar 1504 "Tehnologii informaționale" îi sunt prevăzute cheltuieli în valoare de 20416,5 mii lei. Aceste cheltuieli sunt asociate realizării de către Agenție a competenței sale în ce privește implementarea politicii de stat în domeniul securității cibernetice, inclusiv exercitarea funcției de supraveghere și control al modului în care sunt respectate prevederile cadrului normativ în acest domeniul, oferirea de asistență, inclusiv metodologică furnizorilor de servicii în sectoarele critice în vederea implementării măsurilor de securitate.

În ceea ce privește cea de-a doua componentă costurile de implementare a măsurilor de securitate pentru furnizorii de servicii din sectorul public, relevăm următoarele. În prezent o parte dintre aceste entități publice sunt obligate să implementeze măsurile de securitate stabilite de Hotărârea Guvernului nr. 201/2017 „Cu privire la aprobarea Cerințelor minime obligatorii de securitate cibernetică", și anume Cancelaria de Stat, ministerele, alte autorități administrative centrale subordonate Guvernului, inclusiv al structurilor organizaționale din sfera lor de competență (autoritățile administrative din subordine, serviciile publice desconcentrate și cele aflate în subordine, instituțiile publice în care Cancelaria de Stat, ministerul sau altă autoritate administrativă centrală are calitatea de fondator), al autorităților administrative autonome și unităților cu autonomie financiară. Se presupune că toate aceste autorități și instituții publice au deja prevăzute anumite mijloace financiare în bugetul de stat pentru realizarea obligațiilor prevăzute de Hotărârea Guvernului nr. 201/2023. Având în vedere că obligațiile impuse de această hotărâre de Guvern și cele propuse în proiectul de hotărâre propus spre examinare nu diferă fundamental sub aspectul conceptului și obiectivelor urmărite prin implementarea măsurilor de securitate, dar și într-o anumită măsură a conținutului acestor măsuri, este de presupus să nu fie necesară o creștere substanțială a cuantumului mijloacelor financiare la cele deja planificate în bugetul de stat pentru asigurarea conformității cu cerințe privind măsurile de gestionare a riscurilor în materie de securitate cibernetică. În principiu, putem conchide că implementarea măsurilor de securitate cibernetică

pentru furnizorii de servicii din sectorul public urmează să se asigure din contul și în limita mijloacelor financiare alocate în legile bugetare anuale.

Cu toate acestea considerăm important de relevat unele aspecte abordate de către Comisia Europeană în Analiza [23] de impact la propunerea de Directivă NIS2. Astfel, *Datele pentru administrația publică se referă la costurile de funcționare. Cheltuielile TIC în sectorul public sunt de obicei exprimate ca procent din cheltuielile de funcționare în loc de venituri sau cifra de afaceri. Conform Eurostat , în 2019, cheltuielile totale la nivelul administrației centrale în UE-27 au fost de 22% din PIB, în timp ce veniturile totale au fost de 21,7% din PIB. La nivelul administrației locale, cheltuielile totale au fost la fel ca veniturile totale: 10,9% din PIB. Studiul privind investițiile NIS indică o* ***medie anuală a cheltuielilor pentru securitatea TIC de 4% din bugetul TIC pentru guvernele din Europa****. În conformitate cu estimările menționate anterior privind o creștere cu 22% a cheltuielilor pentru securitatea TIC în cei 3-4 ani care urmează intrării în vigoare a Directivei NIS revizuite ...., cheltuielile pentru securitatea TIC ale guvernelor ar trebui, prin urmare, să crească la* ***4,88%****...."*

De asemenea, considerăm relevante exercițiului nostru constatările analizei de impact[24] efectuate de către Agenția Republicii Cehe pentru Securitate Cibernetică și Informațională (NUKIB) la proiectul de lege privind securitate cibernetică care transpune prevederile Directivei NIS2. Astfel, Agenția respectivă a efectuat o analiză în baza mai multor studii privind investițiile în securitatea cibernetică ale ENISA, în baza estimărilor anterioare în procesul de transpunere a Directivei NIS1 și a unui sondaj a unui grup de entități selectate. Această analiză *a condus la un calcul orientativ al costurilor pentru implementarea și punerea în aplicare ulterioară a principalelor măsuri de securitate* ***pentru un sistem securizat*** *sub forma unor estimări foarte aproximative, cuprinse între 800 000 CZK și 1 500 000 CZK (aproximativ între* ***30000 și 60000 euro****). Schimbările în abordarea reglementării introduse de directivă, variabilele menționate mai sus (în special starea diferită a securității actuale în organizațiile reglementate), distribuția obligațiilor impuse acestor entități, precum și agregarea unui număr de măsuri de securitate în mai multe sisteme din cadrul unei organizații pot influența aceste valori, dar, având în vedere cele de mai sus, este posibil să se aștepte la cerințe bugetare publice în acest interval aproximativ. Prin urmare, variabila esențială va fi numărul de sisteme individuale pentru fiecare organizație în parte și multiplicarea sumei de mai sus care va trebui alocată organizațiilor în bugetele publice."* În aceeași analiză NUKIB însă constată că rezultatele sondajului *demonstrează că, din perspectiva autorității de reglementare, nu este posibil să se cuantifice impactul asupra bugetelor sub forma unui număr absolut care să fie suficient de precis*.

Și în acest caz evidențiem faptul că acestea nu sunt cheltuieli care ar trebui efectuate într-un interval de un an bugetar. Implementarea cerințelor de securitate și în sectorul public ar putea fi eșalonate de-a lungul mai multor ani, în funcție de prioritizarea activelor critice vizate și de disponibilitatea mijloacelor financiare ale furnizorului de servicii.

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: Soluția propusă va îmbunătăți securitatea cibernetică prin detectarea și blocarea eficientă a atacurilor, protejând datele și informațiile sensibile și asigurând reacții rapide.

[23] https://eur-lex.europa.eu/legal-content/EN/TXT/DOC/?uri=CELEX:52020SC0345

[24] https://odok.cz/portal/veklep/material/ALBSCSSFKU7S/

- 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.

- Reducerea costurilor asociate incidentelor cibernetice: Soluția va reduce riscurile, impactul și costurile financiare legate de incidentele cibernetice, cum ar fi pierderile de date și daunele reputației sau perturbarea serviciilor, economisind astfel resursele necesare pentru recuperare și remediere.

- Îmbunătățirea încrederii și reputației: O securitate cibernetică mai puternică va crește încrederea utilizatorilor și clienților în mediul privat și stat, consolidând reputația acestora.

- Siguranța infrastructurii critice: Soluția va proteja infrastructura critică, cum ar fi rețelele energetice, sistemul bancar și transportul, reducând riscul de întreruperi majore și asigurând continuitatea serviciilor vitale.

- Stimularea inovării și cercetării: Implementarea soluției va impulsiona inovația și cercetarea în domeniul securității cibernetice, contribuind la dezvoltarea economică și colaborarea internațională.

4.4. Impactul social

4.4.1. Impactul asupra datelor cu caracter personal

Din perspectiva datelor cu caracter personal prevederile proiectului de act normativ ar trebui să aibă 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. Iar aceste rețele și sisteme informatice în mare partea, mai ales în cazul furnizorilor de servicii mari, procesează date cu caracter personal.

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

Un nivel mai ridicat de securitate ar îmbunătăți încrederea cetățenilor în mediul on-line, care ar putea profita pe deplin de avantajele lumii digitale, în mod special în ce privește serviciile digitale guvernamentale. Aceste servicii esențiale ar deveni mai atractive datorită fiabilității și disponibilității ridicate. Acest lucru le poate conferi cetățenilor din regiunile rurale sau îndepărtate cu acces limitat la serviciile offline o mai mare încredere. În cele din urmă, este foarte probabil ca această opțiune să stimuleze crearea unui corp de profesioniști în domeniul asigurării securității rețelelor și sistemelor informatice și, implicit al ocupării forței de muncă a personalului din acest domeniu, inclusiv datorită cerințelor de a efectua evaluări ale riscurilor de securitate cibernetică și de a adopta măsuri de securitate adecvate.

5. Compatibilitatea proiectului actului normativ cu legislația UE

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

Proiectul de act normativ propus spre examinare transpune parțial prevederile Regulamentului de punere în aplicare (UE) 2024/2690 al Comisiei din 17 octombrie 2024[25], precum

[25] Regulamentul de punere în aplicare (UE) 2024/2690 al Comisiei din 17 octombrie 2024 de stabilire a normelor de aplicare a Directivei (UE) 2022/2555 în ceea ce privește cerințele tehnice și metodologice ale măsurilor de gestionare a riscurilor în materie de securitate cibernetică și specificarea suplimentară a cazurilor în care un incident este considerat semnificativ referitor la furnizorii de servicii DNS, registrele de nume TLD, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, furnizorii de piețe online, de motoare de căutare online și de platforme de

și ia în considerare dispozițiile Comunicării[26] Comisiei referitoare la Orientările Comisiei privind aplicarea articolului 4 alineatele (1) și (2) din Directiva (UE) 2022/2555[27] (Directiva NIS 2) 2023/C 328/02.

Obiectivul Regulamentului de punere în aplicare (UE) 2024/2690 al Comisiei din 17 octombrie 2024 constă în stabilirea cerințelor tehnice și metodologice ale măsurilor de gestionare a riscurilor în materie de securitate cibernetică, menționate la articolul 21 alineatul (2) din Directiva (UE) 2022/2555, și să precizeze mai în detaliu cazurile în care un incident ar trebui considerat semnificativ, astfel cum se menționează la articolul 23 alineatul (3) din Directiva (UE) 2022/2555.

Domeniul de aplicare al actului juridic european este limitat la *furnizorii de servicii DNS, registrele de nume TLD, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea, precum și prestatorii de servicii de încredere.* Actul UE acoperă două sectoare cu o importanță critică ridicată (anexa nr. 1 la Directiva NIS2): infrastructura digitală *(cu excepția furnizorilor de puncte de schimb de internet (IXP - internet exchange point) și furnizorii de rețele publice de comunicații electronice și/sau de servicii de comunicații electronice accesibile publicului)* și gestionarea serviciilor TIC, și un sector de importanță critică (anexa nr. II la Directiva NIS): sectorul furnizori digitali. Proiectul de act normativ însă extinde domeniul de aplicare al prevederilor transpuse la întregul spectru de subiecți ai Legii nr 48/2023 privind securitatea cibernetică. Această extensie este datorată pe de o parte de necesitatea punerii în aplicare a prevederilor art. 11 din Legea nr. 48/2023 care reglementează obligațiile furnizorilor de servicii în ce privește implementarea măsurilor de securitate a rețelelor și sistemelor informatice pe care le dețin și, pe de altă parte, de faptul că cerințele reglementate de actul UE sunt cerințe minime necesare pentru asigurarea unei reziliențe din punct de vedere cibernetic atât a entităților din sectorul public, cât și a entităților din sectorul privat. În acest sens, trebuie evidențiat faptul că actul UE *„se bazează pe standarde europene și internaționale, cum ar fi ISO/IEC 27001, ISO/IEC 27002 și ETSI EN 319401, precum și pe specificații tehnice, cum ar fi CEN/TS 18026:2024, care sunt relevante pentru securitatea rețelelor și a sistemelor informatice*"[28] relevante pentru toate tipurile de entități care activează în sectoarele critice.

Actul UE a cărui transpunere se urmărește prin adoptarea proiectului de act normativ propus spre examinare este unul recent adoptat și nu a constituit anterior obiect al transpunerii în legislația națională.

Referitor la reglementările similare existente în legislația statelor membre ale Uniunii Europene, a fost efectuată o evaluare a legislației a cinci State membre ale UE: Belgia, Cehia, Estonia, Germania și România.

Toate cadrele de securitate cibernetică ce se folosesc, se referă la sau au fost inspirate de cele mai comune standarde internaționale, cum ar fi cele ale familiei ISO 27000 și NIST. Unele țări au optat să emită un standard național autonom, altele stabilesc măsurile de securitate în reglementări de implementare, în timp ce a treia categorie utilizează încă certificarea internațională ca dovadă a conformității.

servicii de socializare în rețea, precum și prestatorii de servicii de încredere: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32024R2690

[26] Comunicare a Comisiei Orientările Comisiei privind aplicarea articolului 4 alineatele (1) și (2) din Directiva (UE) 2022/2555 (Directiva NIS 2) 2023/C 328/02: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52023XC0918(01)

[27] 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: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2555.

[28] Considerentul (3) din preambulul la Regulamentul de punere în aplicare UE) 2024/2690 al Comisiei din 17 octombrie 2024;

În Belgia, decretul regal din 9 iunie 2024 de executare a legii de transpunere a Directivei NIS2 introduce două cadre de referință din care să aleagă entitățile reglementate. În primul rând, certificarea ISO 27001 și, în al doilea rând Cyber Fundamentals (CyFun), cadrul dezvoltat de Centrul național de securitate cibernetică belgian. Acesta din urmă combină patru cadre de securitate cibernetică utilizate în mod obișnuit (NIST, CSF, ISO 27001/ISO 27002, CIS Controls și IEC 62443), împreună cu date anonimizate ale atacurilor cibernetice anterioare. Cadrul belgian oferă trei niveluri de asigurare: de bază, importantă și esențială, completate de nivelul de pornire „mic". Cu toate acestea, metodologia care stă la baza diferențierii măsurilor de securitate între cele trei niveluri nu este evidentă.

România, la rândul ei, aplică standarde și/sau specificații europene și internaționale individual sau grupate în funcție de domeniile, subdomeniile, măsurile și cerințele de securitate, stabilite în conformitate cu regulile tehnice privind cerințele minime pentru asigurarea securității rețelelor și sistemelor informatice. Aceste standarde și/sau specificații europene și internaționale se găsesc în Lista standardelor și specificațiilor europene și internaționale, adoptată de Guvern. Proiectul de Ordonanță de urgență de transpunere a Directivei NIS2 nu precizează nicio cerință și lasă la latitudinea Directoratului Național de Securitate Cibernetică (DSNC) stabilirea oricărei legislații secundare corespunzătoare între 15 și 180 de zile de la data publicării ordonanței în Monitorul Oficial, în funcție de subtema corespunzătoare. În timp ce adoptarea respectivei ordonanțe de urgență va abroga actuala Lege privind securitatea cibernetică, măsurile adoptate sau impuse în temeiul prevederilor dispozițiilor acesteia din urmă privind securitatea rețelelor și sistemelor informatice, auditurilor și certificărilor, precum și a legislației secundare corespunzătoare, rămân în vigoare până la revizuirea acestora, în conformitate cu perioada menționată mai sus de la data publicării ordonanței. În plus, proiectul menționează o listă de standarde și specificații europene și internaționale, supuse elaborării și aprobării de către DNSC.

În Cehia, Legea securității cibernetice face distincție între cerințele de securitate organizațională și cea tehnică și oferă o listă enumerativă a acelor cerințe sau măsuri. Ca urmare a obligației legale de punere în aplicare a măsurilor de securitate, NUKIB emite și este responsabil de actualizarea decretelor care detaliază măsurile de securitate și modalitățile de punere în aplicare și audit a acestora. NUKIB publică în continuare materiale metodice fără caracter obligatoriu care ajută entitățile reglementate să înțeleagă și să pună în aplicare în mod corect cadrul juridic. Cerințele se bazează pe familia ISO 27k și în special pe standardul ISO 27001. În cazul în care legislația sectorială (națională sau a UE) reglementează gestionarea securității și a incidentelor, legea privind securitatea cibernetică recunoaște aceste norme sectoriale ca lex specialis, cu condiția ca acestea să garanteze un nivel de securitate comparabil cu cel al legii privind securitatea cibernetică. În mod obișnuit, o astfel de legislație se găsește în sectoarele energetice, financiare sau de telecomunicații. Legea de transpunere a Directivei NIS2 adoptă aceeași abordare.

Implementarea de către Germania a Directivei NIS și Directivei NIS2 aderă în general la cadrele internaționale de securitate cibernetică și la cele mai bune practici, cum ar fi ISO 27001, dar cu cerințe suplimentare. De exemplu, măsurile trebuie să fie adaptate pentru a aborda riscurile de mediu, amenințările fizice și tehnologiile de ultimă generație. Țara încorporează în continuare cele mai bune practici internaționale și standarde specifice industriei. Astfel, anumite sectoare urmează linii directoare personalizate care reflectă nevoi operaționale unice, cum ar fi catalogul de securitate BNetzA pentru telecomunicații sau cerințele de infrastructură critică conform BSI- KritisV . Acestea sunt personalizate în funcție de riscurile inerente fiecărei industrii. Anumite industrii precum energia, telecomunicațiile și serviciile financiare sunt reglementate prin instrumente juridice suplimentare, cum ar fi Legea industriei energetice (EnWG) și Legea telecomunicațiilor (TKG), care includ

mandate de securitate cibernetică specifice sectorului, aliniate cu Directiva NIS2. Pentru entitățile care nu sunt acoperite de standarde specifice sectorului, legea pune accent pe alinierea la cadrele internaționale mai largi. ISO 27001 este menționat ca fundație, deși este adesea considerat insuficient fără măsuri suplimentare prescrise de Directiva NIS2. Cadrul juridic general oferit de BSIG asigură, prin urmare, o bază de referință, în timp ce industriile specifice aderă la standarde personalizate pentru a aborda riscurile unice. Alegând această abordare hibridă, Germania depune eforturi pentru o acoperire cuprinzătoare a cerințelor de securitate cibernetică în toate sectoarele.

În Estonia, toate entitățile reglementate intră sub supravegherea autorității competente, Autoritatea Estoniană pentru Sisteme Informaționale sau RIA. Drepturile și obligațiile acestei autorități sunt descrise în capitolele 4 și 5 din actul de securitate cibernetică. Prevederile Standardului Estonian de Securitate a Informațiilor sunt de natură generală și se aplică tuturor entităților obligate. Legea nu face diferențe între sectoare (privat vs public sau altfel). Scopul implementării continue a măsurilor de securitate cibernetică este de a permite și de a contribui la prevenirea incidentelor cibernetice, rezolvarea incidentelor cibernetice, prevenirea și atenuarea impactului unui incident asupra continuității unui serviciu sau securității unui sistem sau a altui serviciu dependent sau securitatea unui sistem. Abordarea bazată pe riscuri impune tuturor entităților reglementate să pregătească o evaluare a riscurilor sistemului și să descrie măsurile de soluționare a unui incident cibernetic, să asigure existența și actualitatea unei evaluări documentate a riscurilor sistemului, a reglementărilor de securitate și a descrierii aplicării măsurilor de securitate, să asigure monitorizarea sistemului pentru detectarea acțiunilor sau a programelor informatice care compromit securitatea acestuia și să comunice RIA informații privind acțiunile sau programele informatice care compromit securitatea sistemului, să ia măsuri pentru reducerea impactului și răspândirii unui incident cibernetic, inclusiv restricționarea utilizării sau a accesului la sistem, dacă este necesar.

În conformitate cu prevederile Regulamentului privind armonizarea legislației Republicii Moldova cu legislația Uniunii Europene, aprobat prin Hotărârea Guvernului nr. 1171/2018, a fost elaborat tabelul de concordanță care este parte a dosarului de însoțire a proiectului de act normativ.

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, pe pagina web oficială a Ministerului Dezvoltării Economice și Digitalizării mded.gov.md și pe platforma de consultare particip.gov.md, la data de 25.09.2024 a fost publicat anunțul referitor la inițierea procesului de elaborare a proiectului de hotărâre de Guvern link, - (https://particip.gov.md/ro/document/stages/*/13240).

Anunț privind consultarea publică a proiectului hotărârii de Guvern a fost plasat la data de 04.02.2025, link - (https://particip.gov.md/ro/document/stages/*/13896)

7. Concluziile expertizelor

Proiectul de act normativ a fost supus expertizei anticorupție și expertizei juridice conform procedurii stabilite de cadrul normativ.

Conform expertizei anticorupție proiectul nu conține factori de risc care să genereze apariția riscurilor de corupție.

Totodată, proiectul a fost definitivat conform obiecțiilor și propunerilor din expertiza juridică.

8. Modul de încorporare a actului în cadrul normativ existent

Prin proiectul de act normativ se propune abrogarea Hotărârii Guvernului 201/2017 privind cerințele minime obligatorii de securitate cibernetică. Abrogarea este determinată pe de o parte de faptul că toate persoanele juridice de drept public în temeiul art. 3 alin. (2) lit. i) intră în sfera de aplicare a Legii nr. 48/2023 și cerințele respective le vor fi aplicabile, iar pe de altă parte cerințele prevăzute în Hotărârea Guvernului nr. 201/2017 sunt cuprinse de cerințele propuse în proiect.

În principiu adoptarea și intrarea în vigoare a proiectului nu va necesita modificarea cadrului normativ existent, dat fiind caracterul de lege specială a legislației sectoriale în raport cu legislația privind securitatea cibernetică, inclusiv prevederile proiectului în speță, dacă legislația sectorială stabilește cerințe cel puți echivalente în efecte cu cele ale actelor normative adoptate pentru punerea în aplicare a Legii nr. 48/2023 și lega propriu-zisă.

Deși proiectul nu implică adoptarea unor acte normative noi, totuși trebuie notat că Agenția pentru Securitate Cibernetică urmează să vină cu modele de notificare a incidentelor de către furnizorii de servicii care să le faciliteze raportarea incidentelor cibernetice cu impact semnificativ.

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. Potrivit prevederilor art. 7 alin. (3) lit. e), Agenția exercită supravegherea și controlul respectării de către furnizorii de servicii a obligațiilor ce le revin conform Legii nr. 48/2023. Modul de exercitarea a acestor funcții ale Agenției urmează a fi reglementat prin-un act normativ separat aprobat de către Guvern în temeiul prevederilor art. 18 alin. (3) și 19 alin (5). Însă prevederile proiectului actului normativ urmează a fi aplicate de către furnizorii de servicii în mod treptat în termenele stabilite. În această perioadă de timp, Agenția urmează:

- să finalizeze operaționalizarea în volum deplin a subdiviziunii responsabile de identificarea, evidența și relaționarea cu furnizorii de servicii și a subdiviziunii responsabile de supraveghere și controlul executării prevederilor legale de către furnizorii de servicii;
- să aprobe ghiduri și orientări metodologice pentru furnizorii de servicii în vederea sprijinirii acestora în implementarea cerințelor privind măsurile de gestionare a riscurilor care ajută furnizorii de servicii să înțeleagă și să pună în aplicare corect cerințele privind măsurile de securitate;
- să acorde suport consultativ furnizorilor de servicii privind evaluarea nivelului de maturitate și conformitate a acestora cu cerințele de asigurare a securității cibernetice;
- în baza constatărilor acestor evaluări acordarea suportului consultativ entităților în prioritizarea pentru implementare, în mod special în baza principiului proporționalității, a măsurilor de securitate în funcție de capacitatea furnizorilor de servicii, atingerea obiectivelor de reziliență, raportul cost-beneficiu.
- să stabilească formate și să instituie mecanisme, inclusiv sprijinite de mijloace digitale, pentru a înlesni îndeplinirea de către furnizorii de servicii a obligațiilor de raportare a incidentelor cibernetice cu impact semnificativ;
- să întreprindă alte acțiuni menite să faciliteze schimbul de informații în timp real cu furnizorii de servicii în vederea creșterii nivelului de reziliență al acestora.

Secretar de stat **Michelle ILIEV**

SINTEZA

obiecțiilor și propunerilor/recomandărilor la proiectul de hotărâre de Guvern

„Cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice” (număr unic 49/MDED/2025)

PRIMA AVIZARE

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
1.	**Cancelaria de Stat** *(Nr. 14-93-1860 din 19.02.2025)*		Lipsa de propuneri și obiecții.	
2.	**Cancelaria de Stat (Grupul de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător)** *(Nr. 38-78-1661 din 14.02.2025)*		***Evaluarea proiectului de act normativ*** ***Decizia Grupului de lucru în privința proiectului de act normativ și notei de fundamentare:*** Nu se susține proiectul de act normativ și nota de fundamentare. ***Concluzia:*** Proiectul conține prevederi contradictorii cu principiile de reglementare a activității de întreprinzător.	
		1.	Comentarii, recomandări:	
		2.	Proiectul este elaborat în procesul de armonizare, ceea ce presupune că preluarea limbajului din Regulamentul UE poate rezulta în norme vagi, care necesită corelare cu prevederile în vigoare ale cadrului normativ național și mai multe detalii pentru a asigura înțelegerea și aplicarea corectă a drepturilor și obligațiilor stipulate. Cerințele privind măsurile de gestionare a riscurilor în materie de securitate cibernetică din anexă în marea majoritate a cazurilor sunt expuse foarte vag și interpretabil. Cerințele expuse abundă în formulări de genul - a efectua/realiza în mod „adecvat”, a revizui „la intervale stabilite” sau „planificate”, a aplica în „termen rezonabil”, a asigura „expertiză relevantă” ș.a.m.d. În acest mod, aplicarea normelor în cauză este	**Nu se acceptă** Proiectul de act normativ, după cum este formulat, **transpune prevederile Regulamentului de punere în aplicare (UE) 2024/2690** al Comisiei din 17 octombrie 2024. Totodată, menționăm că în prezent cadrul normativ național nu include un act normativ care să abordeze problematica măsurilor în materie de securitate cibernetică într-un mod la fel de detaliat și de cuprinzător. Proiectul de act normativ propus spre examinare cuprinde subiecți de drept atât din sectorul public, cât și din sectorul privat, apartenența acestora la cercul

			imprevizibilă și poate duce fie la abuzuri din partea organului de control sau la eschivare de unii agenți economici de la aplicarea normelor în cauză. Pentru a asigura claritatea obligațiilor și previzibilitatea aplicării normelor în cauză, este important de a evita expuneri ambigui, în special în lipsa unor posibile acte normative subsidiare care ar putea veni cu clarificările tehnice necesare	de subiecți ai Legii nr. 48/2023 fiind determinată de caracterul critic al sectoarelor în care entitățile respective prestează servicii esențiale. Un obiectiv specific al acestui proiect de act normativ, strâns legat de obiectivul de punere în aplicare a prevederilor Legii nr. 48/2023, este uniformizarea cerințelor în materie de securitate cibernetică pentru entitățile respective, un aspect important al acestui exercițiu fiind și consfințirea unei terminologii unice în acest domeniu, armonizată la terminologia utilizată de legislația europeană. De asemenea, ținem să relevăm că estimarea nivelului corespunzător de detaliere a unor astfel de cerințe este destul de complicată în contextul în care abordarea bazată pe riscuri este principiul fundamental în determinarea măsurilor de intervenție corespunzătoare riscurilor identificate. Mai mult, peisajul destul de pestriț din punctul de vedere al caracterului critic, al dimensiunii, al capacităților financiare, al maturității din punctul de vedere al rezilienței, al furnizorilor de servicii face practic imposibilă stabilirea unor cerințe de securitate stricte și rigide cu un grad înalt de detaliere. Ceea ce pentru unii furnizori de servicii, chiar din aceeași categorie sau de același tip, ar putea să constituie un minim necesar, pentru alții ar putea constitui un obstacol insurmontabil și, implicit ar putea duce la încetarea activității. În textul proiectului anexei la proiectul de Regulament sintagma „termen rezonabil” este utilizată doar la pct. 77.1 și vizează aplicarea

				corecțiilor de securitate într-un termen rezonabil de la data la care devin disponibile. Stabilirea unui termen cuantificabil în proiectul de hotărâre este imposibil, deoarece aplicarea acestei măsuri implică un set de variabile, cum ar fi spre exemplu: - acțiuni de corecție care pot varia în funcție de sistem; de exemplu, patch-uri obligatorii pentru sistemele expuse (de exemplu, dispozitive conectate la internet precum firewall-uri și routere) și patch-uri limitate pentru sistemele izolate sau moștenite; - Aplicarea de corecții ar trebui să constituie o activitate standard în cadrul întreținerii normale și al planificării întreruperii serviciilor. Cu toate acestea, unele defecțiuni pot necesita aplicarea imediată de patch-uri, în funcție de gravitatea lor; - furnizorii de servicii ar trebui să aplice corecțiile după aprobare sau testare într-un mediu izolat, urmând procedura de gestionare a modificărilor. Rezonabilitatea termenelor respective trebuie apreciată atât de furnizorul de servicii, cât și de autoritatea competentă de supraveghere ținând cont de următoarele: În ce privește sintagma „în mod adecvat”. Aceasta este utilizată în cazul prevederilor implementarea cărora și verificarea conformității implementării cărora urmează a se efectua prin aplicarea principiului proporționalității. Acest principiu este statuat de prevederile art. 11 alin. (2) punctul 2) conform căruia furnizorii de

				servicii sunt obligați să implementeze măsuri de securitate corespunzătoare și proporționale riscurilor identificate ca urmare a evaluării efectuate în temeiul punctului 1) alin. (2) din același articol. Acest principiu al proporționalității este reflectat și de Directiva NIS2 și, pe cale de consecință, dezvoltat de Regulamentul de punerea în aplicare (UE) 2024/2690 al Comisiei din 17 octombrie 2024 a acestei Directive. Aceeași abordare atât din perspectiva conceptului abordării bazate pe riscuri, cât și din punctul de vedere al obiectivelor de armonizare a legislației naționale la aquis-ul comunitar, este preluată și de proiectul de act normativ național. Astfel, din punct de vedere tehnic, sintagmele „*dacă este adecvat”, „dacă este aplicabil”* și *„în măsura în care este fezabil”* din Anexa la proiectul de regulament sunt conectate cu prevederea de la pct. 8 din proiectul Regulamentului. Astfel dacă un furnizor de servicii va considera că o anumită cerință de securitatea nu este adecvată și/sau nu este aplicabilă și/sau nu este fezabilă, acesta va trebui să vină cu o motivare documentată în acest sens. Cuvântul planificat este utilizat în mai multe prevederi din proiectul Cerințelor și în contexte diverse legate în mod specific de prevederile care stabilesc aprobarea de către furnizorul de servicii a anumitor documente: politici, proceduri, planuri. Spre exemplu, în cazul cuvântului *„planificate”* utilizat în sintagma *„intervale planificate”* de la punctul 11 din proiectul

				Cerințelor, intervalele respective nu pot fi mai mici de un an, deoarece, conform punctului 9, furnizorii de servicii trebuie să examineze periodic conformitatea cu politicile privind securitatea rețelelor și sistemelor informatice, care potrivit punctului 2 se revizuiește și se actualizează cel puțin anual.
		3.	În aceiași ordine de idei, conform pct.6 din Regulament (și celor indicate în Notă) nu sunt preconizate alte acte normative cu mai multe detalii privind cerințele din anexă. Adică, contrar prevederilor din art.11 din Legea nr.48/2023, care prevede existența standardelor aprobate de Institutul Național de Standardizare, se propune ca obligațiile din prezentul proiect să fie desfășurate și clarificate în ghidurile elaborate și aprobate de Agenție. Cu toate că legea nu prevede atribuția Agenției de a aproba ghiduri prin care se vor pune în aplicare actele normative aprobate de Guvern și Parlament, dar și nici nu vine să clarifice că standardele (menționate la art.11) vor avea cumva aplicabilitate obligatorie. Astfel situația în care Agenția urmează să vină cu detaliile tehnice necesare în baza unor ghiduri (elaborate și aprobate de Agenție) nu creează doar un conflict evident de interese, odată ce Agenția are și funcții de organ de control, dar este o încălcare gravă a principiului prevăzut la art.5 din Legea nr.235/2006, conform căruia activitatea agenților economici poate fi reglementată doar prin acte normative, în limitele stabilite de lege (pe când Agenția nu are nici funcții de reglementare în principiu). Spre exemplu în domeniul construcțiilor sau securității industriale se aprobă de către ministerele de ramură Norme (NRS) și Normative (NCM) care, în dependență de caz sau categoria obiectului reglementat, stabilesc suficiente detalii tehnice și parametri necesari de respectat pentru a asigura punerea în aplicare a obligațiilor generale stabilite de Guvern sau Parlament. Pentru	**Nu se acceptă** Este eronată interpretarea conform căreia faptul că Agenția poate elabora ghiduri sau furniza orientări metodologice furnizorilor de servicii ar contraveni prevederilor art. 11 din Legea nr.48/2023 . Agenția, conform prevederilor, art. 7 alin. (3) lit. b); f) și ale alin. (4) punctele 2), 3), 5) și 6) din Legea nr.48/2023 poate elabora și pune la dispoziția celor interesați ghiduri sau orientări metodologice pentru punerea în aplicare a prevederilor actelor normative. Mai mult, o astfel de atribuție este specifică și organelor de control, art. 32 din Legea nr. 131/2012 privind controlul de stat fiind relevant în acest sens.

			a evita încălcarea menționată, este necesar ca proiectul să conțină toate detaliile tehnice și toți parametrii pentru a putea pune în aplicare obligațiile prevăzute sau, cel puțin Legea nr.48/2023 să prevadă o categorie de norme/documente cu caracter tehnic, care vor fi aprobate printr-un act normativ al ministerului de ramură, în care se vor conține detaliile tehnice necesare.	
		4.	În privința conținutului incert, incomplet și vag, pot fi în special, în calitate de exemplu, aduse următoarele obiecții: - În linii generale, în proiect lipsesc prevederi pentru Sistemele de control industrial SCADA / Rețele OT și IoT. Principiul de funcționare și metodele de asigurare a securității și vizibilității acestor rețele diferă de cel al rețelelor/sistemelor IT. Totodată, anume pe aceste sisteme/rețele se bazează serviciile critice prestate de Furnizori.	**Nu se acceptă** **Precizare.** Cerințele propuse în proiect sunt general aplicabile tuturor furnizorilor de servicii și fiind bazate în principal pe standardele de securitate a informației din seria 27000, pun accentul pe confidențialitatea informației. Cerințele de securitate cibernetică pentru sisteme de control industrial și tehnologie operațională cum sunt spre exemplu cele prevăzute de standardul IEC 62443 au ca accent disponibilitatea sistemelor respective. Proiectul propus spre avizare are ca obiectiv stabilirea unor cerințe de bază. Ulterior, în temeiul art. 11 alin. (4) din Legea nr. 48/2023 privind securitatea cibernetică vor putea fi adoptate sau actualizate cerințe de securitate specifice sectoarelor și subsectoarelor critice prevăzute de Hotărârea Guvernului nr. 860/2024. Astfel de cerințe specifice există actualmente pentru anumite categorii de furnizori de servicii.
		5.	- La pct.6 din Regulament, este necesară stabilirea unor criterii conform cărora nivelul de securitate va fi clasificat “corespunzător”. Pot apărea situații când ASC va considera că urmează a fi implementate măsuri mai avansate/sofisticate de securizare iar agenția de reglementare (in cazul sectorului energetic ANRE) nu va aproba/nu va fi de acord cu acestea.	**Se acceptă parțial.** Evaluarea caracterului corespunzător al măsurilor de securitate implementate trebuie realizată conform principiului proporționalității. Acesta este descris la punctul următor și urmează fi înțeles împreună cu prevederile din anexă care

				stabilesc condițiile proporționalității pentru fiecare cerință de securitate în parte. Totodată, la acest aspect urmează a fi luat în considerare faptul că stabilirea unor criterii uniforme este imposibilă din cauza diversității mari a cazurilor de aplicabilitate. Pentru fiecare caz concret și pentru fiecare organizație anumite măsuri pot fi implementate diferit. Totodată, evaluarea de către ASC a faptului dacă măsura este corespunzătoare are ca punct de referință documentele aprobate de către furnizorul de servicii în temeiul prevederilor anexei, inclusiv raportul de evaluare a riscurilor, planul de tratare a riscurilor. Cu toate acestea, în proiect au fost incluse prevederi mai detaliate privind procesul de punere în aplicare a actului normativ (a se vedea partea dispozitivă a hotărârii de Guvern).
		6.	- La pct.7 din Regulament, se propune excluderea sintagmei "inclusiv de impactul lor societal și economic". Aceste cerințe nu se regăsesc în prevederile standardului ISO 27001:2023, capitolul 6 (referința la standard se face în pct. 4 al proiectului Regulamentului). Fie este necesar de făcut referință la o metodologie/document oficial aprobat și Se acceptă pe teritoriul Republicii Moldova, care conține asemenea cerințe și descrie cum determină/stabilesc acești parametri.	**Nu se acceptă.** Menționăm că referința la standard a fost exclusă din pct. 4. Totuși, referința la acest standard nu înseamnă că regulamentul urmează să urmeze fidel prevederile acestuia. Totodată, punctul 4 nu are ca scop impunerea obligativității aplicării acestora standarde, ci, în baza constatării că acestea stau la baza cerințelor de securitate propuse în proiect, oferă furnizorilor de servicii oportunitatea de a le utiliza atunci când o cred de cuviință pentru a asigura implementarea corespunzătoare a măsurilor de securitate. În ceea privește punctul 7, sintagma la care se face referire în obiecție este o concretizare a criteriului gravității incidentului cibernetic, criteriu necesar pentru a identifica măsurile de

				securitate corespunzătoare pentru a trata eventualele riscuri în caz de apariție a unor astfel de incidente. Impactul societal și cel economic sunt importante de evidențiat, datorită valorilor pe care le poate afecta incidentul cibernetic și pentru a hiperboliza importanța identificării și tratării unor riscuri reieșind din probabilitatea apariției unor astfel de incidente.
		7.	- La pct.6.1 din Anexă, la final, se propune adăugarea sintagmei conform căreia metodologia să fie aprobată prin actul normativ al autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice. Totodată, urmează să fie asigurata o uniformizare a tipului/conținutului/structurii rapoartelor de analiză a riscurilor și predictibilitatea pentru furnizori.	**Nu se acceptă.** Agenția, conform punctului 5 din proiectul Regulamentului, urmează să vină cu orientări metodologice și ghiduri de implementare și să furnizeze, la solicitare, pentru cazuri aparte orientări metodologice furnizorilor de servicii în sectoarele critice. Totodată, „încorsetarea" opțiunilor metodologice ale furnizorilor de servicii într-un act normativ departamental implică anumite provocări de punere în aplicare, dat fiind peisajul foarte divers al furnizorilor de servicii și a infrastructurii informaționale critice, gestionată de aceștia. Spectrul de metodologii care ar putea fi aplicate variază destul de mult: *care pot fi aplicate oricărui tip de organizație (ISO 27005; NIST SP 800-37, SP 800-30 & SP 800-39; BSI 100-3; OCTAVE S, Allegro & FORTE, Open FAIR etc.), cadre și metodologii aplicabile în sectoare specifice (IMO MSC, Guidelines on Cyber Security Onboard Ships), standarde orientate către anumite industrii (NIST 800-82, ANSI/ISA-62443-3-2-2020), metodologii mai structurate care urmează faze sau pași specifici pentru implementarea proceselor de management al*

				riscurilor ETSI TVRA, MONARC, MAGERIT, EBIOS, EU ITSRM, CORAS etc.)[1] ENISA a publicat în 2022 în acest context un Compendiu al cadrelor de management al riscurilor cu potențial de interoperabilitate.
		8.	- La pct.75 din Anexă, cu scopul de a asigura uniformizarea cerințelor și predictibilitatea pentru Furnizori, se propune adăugarea unui subpunct care va face referință la metodologiile de testare a securității, aprobate prin actul normativ al autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice.	**Nu se acceptă.** Nu este clar de ce se invocă scopul uniformizării cerințelor în ce privește metodologiile de testare a securității. Un astfel de obiectiv nu este pertinent pentru exercițiul respectiv. Metodologiile utilizate variază în funcție de tipul testului de securitate, de obiectivele pe care aceste teste le urmăresc, de activele asupra cărora se efectuează. Furnizorul de servicii urmează să aibă aceste metodologii descrise documentar și alese în funcție de obiectivele pe care le stabilește politica de securitate în cadrul organizației, infrastructura testată, etc. La nivel european și mondial există diverse standarde și metodologii utilizate. Uniformizarea metodologică la nivel național o considerăm nejudicioasă.
		9.	- La pct.108 – 110 din Anexă, în privința antecedentelor este necesară o descriere mai detaliată a acțiunilor de întreprins fie trimitere la un act normativ subsidiar prin care vor fi aprobate normele care vor conține detaliile necesare.	**Precizare**. Detaliile privind procesul și mecanismele de implementare urmează a constitui obiectul viitoarelor ghiduri și orientări metodologice pe care le va furniza Agenția pentru Securitate Cibernetică în procesul de acordare a asistenței furnizorilor de servicii în sectoarele critice, în procesul de implementare a prevederilor Legii nr. 48/2023. La punctul 5 din proiectul de

[1] https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks

				Regulament se stabilește obligația Agenției pentru Securitate Cibernetică de a elabora și publica aceste orientări și ghiduri și de a oferi asistența necesară furnizorilor de servicii.
		10.	Pe lângă cele menționate, proiectul mai vine cu unele obligații cu caracter primar, care creează costuri vădite pentru agenții economici însă care nu sunt prevăzute în mod cert de lege și, în lipsa unor prevederi exprese în lege, nu ar putea fi consfințite într-un act al Guvernului (conform art.14 din Legea nr.235/2006), și anume: - În secțiunea 3, Cap.2 din anexă se impune efectuarea periodică a „examinării independente a securității” de către o persoană „certificată”. Nu doar obligația acestei examinări nu este prevăzută de lege dar și faptul că această examinare trebuie să fie efectuată anume de o persoană certificată într-un anumit mod; - Secțiunea 2, Cap.3 impune obligația de „jurnalizare” într-un anumit mod și volum, cu toate că însăși conținutul jurnalelor rămâne incert și interpretabil, fiind impus în măsura în care „este adecvat”; - Secțiunea 2, Cap.8 impune formarea continuă a personalului, în lipsa unei astfel de obligații clare în lege. Cu atât mai mult, în lipsa unor clarificări în lege dar și în proiect cu privire la modul de formare, periodicitatea și alte detalii importante, nu este clar cum aceasta trebuie să se realizeze și cum se va	**Precizare** Prevederile actului normativ detaliază prevederile art. 11 alin. (2). Cerințele de securitate propuse în proiectul de act normativ sunt bazate pe problematicile stabilite la art. 11 alin. (2) punctul 2) din Legea nr. 48/2023. Această obligație este expres prevăzută de art. 11 alin (2) punctul 6); Această cerință decurge din obligațiile stabilite la art. 11 alin (2) punctul 2) lit. b) și punctul 4) Obligația respectivă este clar specificată la nivel primar la art. 11 alin. (2) punctul 2) litera i). Verificarea conformității măsurilor de securitate implementate în acest domeniu de către furnizorul de servicii urmează a fi efectuată, în primul rând, în baza informațiilor documentate privind existența programului de formare în cadrul organizației, care să detalieze obiectivele pentru diferite roluri și modul de atingere a acestora, conținutul și frecvența formării. De asemenea, rezultatele evaluării în urma oricăror

			constata de către organul de control că obligația în cauză este respectată.	teste sau evaluări efectuate pentru a măsura înțelegerea de către angajați a subiectelor abordate; certificate de absolvire sau confirmări acordate angajaților la finalizarea formării în acest domeniu, materiale de formare distribuite angajaților, inclusiv broșuri, prezentări și module online, etc. urmează să constituie probe ale furnizorului de servicii.
		11.	Cu toate că proiectul propus vine cu un set de cerințe formulate în mod vag și incert, care necesită eforturi enorme pentru înțelegere și punere în aplicare, corespunzător vor necesita și alte acte normative conexe, totuși în proiect nu se propune un termen pentru intrare în vigoare. Nu este suficient doar de a indica obligația pentru furnizori de a pune în aplicare pe parcursul a trei ani cerințele prevăzute în proiect, dar este important de a stabili și termene de intrare treptată în vigoare a diverselor categorii de cerințe. În caz contrar, cel puțin pe parcursul termenului de 3 ani, se admite că furnizorii permanent vor încălca normele prevăzute în proiect și, corespunzător, aceștia constant vor fi sub riscul sancționării sau abuzurilor din partea organului de control. Astfel, proiectul necesită să intre în vigoare în mod treptat, în măsura în care autoritățile responsabile vor putea crea instrumentele necesare pentru punerea în aplicare a cerințelor și agenții economici vor avea suficient timp pentru a demonstra conformarea cu cerințele în cauză.	**Se acceptă.** În partea dispozitivă a proiectului de act normativ au fost incluse prevederi care stabilesc obligativitatea furnizorilor de servicii de a efectua și de a documenta în mod corespunzător evaluarea riscurilor la adresa securității rețelelor și sistemelor lor informatice în termen de cel mult un an din data intrării în vigoare a actului normativ (a se vedea completările la pct.3 din partea dispozitivă a proiectului de act normativ).
			Evaluarea notei de fundamentare (analizei impactului de reglementare) ***Concluzia:*** Nota de fundamentare conține suficiente informații pentru a stabili de principiu necesitatea intervenției din perspectiva procesului de armonizare, cu toate că nu conține informația și analiza suficientă pentru a ilustra impactul soluțiilor propuse în proiect, astfel corespunde parțial cu	

			cerințele metodologice prevăzute de Legea nr.100/2017 cu privire la actele normative.	
			Comentarii, recomandări:	
		12.	Cu toate că în descrierea situației (definirea problemei) se expune destul de multă informație despre importanța securității cibernetice, impactul incidentelor cibernetice și locul Moldovei în diverse clasamente internaționale, totuși această analiză nu este suficientă. În cazul în care se invocă riscuri de incidente și prejudicii potențiale datorate unui nivel de protecție insuficient la nivel național, atunci este deosebit de important la analiza situației curente, în baza interviurilor și datelor colectate, să se estimeze în mod argumentat care este nivelul de risc, care sunt prejudiciile reale și potențiale anume pentru Moldova în realitățile economice și tehnologice existente la întreprinderi sau instituții relevante. În baza câtorva exemple relevante este extrem de important de a efectua analiza nivelului actual de securitate cibernetică a întreprinderilor (celor mai relevante întreprinderi) care vor fi vizate direct de proiectul preconizat. În urma acestei analize se va identifica ce elemente și practici lipsesc sau nu sunt dezvoltate suficient, comparativ cu exigențele din proiect. Corespunzător, se va putea identifica nivelul real de riscuri existent dar și, mai jos la analiza impacturilor, se va putea estima impactul real pentru conformarea mediului de afaceri la noul proiect sau cel puțin va fi posibil de identificat cele mai importante costuri de conformare care nu pot fi evitate.	**Precizare** Pentru colectarea a astfel de informații este necesară efectuarea unor analize ale riscurilor nu doar la aspecte ce au tangență cu domeniul securității cibernetice. Analiza riscurilor la nivel național, sectorial, subsectorial intersectorial, etc., urmează să abordeze aspecte mult mai largi care vizează nu doar protecția cibernetică a infrastructurii informaționale critice, ci și cea fizică. Această activitate este una complexă și urmează a fi realizată comprehensiv, începând cu nivelul național și terminând cu analiza riscurilor la nivel de entitate critică (care trebuie realizată de către entitate sau cu acordul acesteia). Directiva NIS2 este un „standard” european care stabilește cerințe minime la nivel național și organizațional, realizarea cărora trebuie să atingă obiectivele de reziliență, iar cerințele de bază privind măsurile de gestionare a riscurilor în materie de securitate cibernetică sunt o componentă a acestui „standard”. În context notăm că o astfel de analiză a riscurilor urmează a fi efectuată în contextul implementării noii legislații care va asigura armonizarea legislației naționale cu Directiva CER. Art. 5 din această Directivă stabilește că statele membre urmează să realizeze astfel de evaluări a riscurilor către data de 17.01.2026 și ulterior ori de câte ori e necesar, însă cel puțin o dată la 4 ani. Armonizarea legislației naționale la Directiva

				CER este, de asemenea, o necesitate și pentru domeniul securității cibernetice, având în vedere caracterul complementar conform căruia urmează a fi puse în aplicare ambele directive NIS2 și CER. De asemenea, ținem să relevăm că efectuarea analizei nivelului actual de securitate cibernetică la o anumită întreprindere este o activitate destul de complexă. În esență, aceasta ar însemna un audit de securitate cibernetică. O astfel de activitate, pe de o parte, implică acceptul furnizorului de servicii de a accesa anumite aspecte sensibile ale activității, iar pe de altă parte, resurse consistente de timp și de mijloace financiare.
		13.	La stabilirea obiectivelor este necesar ca acestea să fie racordate la cauzele problemelor, să fie măsurabile, tangibile și expuse în timp. O mare parte din „obiectivele specifice” sunt de fapt mai mult acțiuni ce urmează a fi întreprinse.	**Se acceptă.** Obiectivele specifice au fost reformulate și expuse într-o manieră măsurabilă, tangibilă și fixată în timp.
		14.	În raport cu beneficiile potențiale nu se estimează direct impactul soluțiilor din proiectul propus, adică, estimativ, cu cât ar putea scădea riscul de incidente cibernetice și cum se traduce în valori monetare scăderea acestui risc (sau schimbarea tendinței de creștere). Ori prejudiciile care au fost evitate pot fi calificate ca și potențiale beneficii, chiar și prin scăderea doar a riscului în puncte procentuale, unde fiecare punct procentual poate avea o valoarea monetară destul de tangibilă.	**Precizare** Răspunsul la astfel de întrebări este posibil după evaluarea primei iterații de implementare a prevederilor proiectului de act normativ, care în baza anumitor criterii uniforme ar putea oferi suficiente date, inclusiv statistice, care comparate cu o a doua iterație de implementare, ar putea oferi anumite informații concludente. Astfel spus, pentru a putea determina cu cât ar putea scădea riscul de incidente este necesar de stabilit condițiile în care acest risc se evaluează, perioada, criteriile de clasificare a incidentelor, taxonomia, existența anumitor măsuri

				obligatorii. Aceste informații și date lipsesc la moment.
		15.	În partea ce se referă la costuri este insuficient dezvoltat impactul asupra întreprinderilor. Sunt prezentate unele cifre din experiența altor state în privința cheltuielilor necesare pentru mentenanța unui sistem de securitate și prudență cibernetică. Totuși este necesar ca acestea să fie extrapolate la realitățile Moldovei, nivelul real de securitate existent și la numărul concret de întreprinderi care vor fi vizate. În special este important de a clarifica costurile instituirii și dezvoltării celor mai importante obligații din proiect – costul instruirilor, examinărilor independente de securitate, jurnalizării standardizate, elaborării protocoalelor și diverselor documente de politici ș.a.m.d.	**Nu se acceptă** Nota informativă nu prezintă doar cifre din experiența altor state, ci propune un model de estimare a costurilor în funcție de cifra de afaceri. Acest model a fost furnizat de către Comisia Europeană în raportul său de evaluare a impactului la propunerea de directivă NIS2. Astfel, în scopul evaluării impactului s-a presupus că media cheltuielilor pentru securitatea TIC pe sector în 2020 este de aproximativ 9,14% din cheltuielile totale TIC, acestea din urmă, la rândul lor, în funcție de nivelul de maturitate și de capacitățile de securitate cibernetică ale sectorului, precum și de nivelul de digitalizare, această medie ar putea fi ajustată cu +/-3%. În plus, cheltuielile medii TIC pe sector sunt estimate la aproximativ 5,69% din cifra de afaceri totală și, prin urmare, cheltuielile medii cu securitatea TIC din cifra de afaceri totală pe sector în 2020 sunt estimate la aprox. 0.52%. Totodată, menționăm că procesul de identificare a persoanelor juridice care vor cădea sub incidența prevederilor Legii nr. 48/2023 privind securitatea cibernetică nu a fost încă finalizat. Estimări mai aprofundate și realiste a nivelului de maturitate a furnizorilor de servicii vor fi posibile după primele evaluări ale conformității acestora cu cerințele de securitatea stabilite de cadrul normativ, inclusiv rezultatele auditurilor de securitate cibernetică.

		16.	Nu în ultimul rând, luând în calcul nivelul actual de conformare, costurile conformării și posibilitățile financiare reale ale celor mai importante instituții și întreprinderi, este important de a examina și expune în detalii strategia de implementare a proiectului propus. Reieșind din această strategie, să fie argumentate normele tranzitorii și cele care prevăd modul de intrare în vigoare a proiectului.	**Se acceptă.** Nota de fundamentare a fost completată cu indicatori de performanță, precum și cu mențiuni privind mecanismul ce va fi implementat pentru monitorizarea și evaluarea impactului prezentei Hotărâri de Guvern.
		17.	Atenționăm că, contrar cerințelor Metodologiei, nu este reflectat un proces de consultări, ori deja în timpul elaborării proiectului și analizei de impact, acest proces trebuia derulat. Corespunzător este important ca la această etapă să fie reflectată poziția persoanelor afectate, în special a agenților economici.	**Nu se acceptă** Procesul de consultare publică a proiectului a fost demarat la data 04.02.2025 prin plasarea pe pagina web oficială a ministerului, precum și pe platforma participip.gov.md a anunțului privind consultarea publică a proiectului hotărârii de Guvern „Cu privire la modul de implementare a măsurilor de securitate a rețelelor și sistemelor informatice de către furnizorii de servicii în sectoarele critice”.
3.	**Cancelaria de Stat (Centrul de Armonizare a Legislației)** *(Nr. 14-93-1860 din 19.02.2025)*		***Observații de compatibilitate cu Regulamentul 2024/2690/UE***	
		18.	Pct. 27 din proiectul Regulamentului, care reflectă criteriile de pentru calificarea incidentelor ca fiind semnificative, se va completa și cu criteriile stabilite de art. 3 (1) (f) și (g) din actul UE, prin operarea cu trimiteri la incidentele descise de pct. 17 – 27 din proiectul Regulamentului.	**Se acceptă.** Punctul 25 din proiectul Regulamentului, care stabilește criteriile generale de determinare a caracterului considerabil a prejudiciilor cauzate de către un incident cibernetic cu impact semnificativ, a fost completat cu subpunctele 25.6 și 25.7, în următoarea redacție: „ 25.5 incidentul este recurent în sensul punctului 22; 25.6 incidentul îndeplinește cel puțin una dintre condițiile prevăzute la punctele 26-35.”.
		19.	De asemenea, pct. 16, lit. (a) din proiectul Regulamentului reflectă doar criteriul cifrei de afaceri și nu reflectă alternativ și criteriul financiar al pierderilor ”care depășesc 500 000 EUR”	**Nu se acceptă.** Condițiile stabilite în articolul din actul UE se referă doar la tipurile de furnizori care intră în

			de la art. 3 (1) (a) din actul UE, ori urmează a fi luată în considerare ”valoarea cea mai mică” a unuia din criterii.	sfera de aplicare al acestuia. În proiectul de act național însă aceste condiții sunt extinse, în mod justificat asupra întregului cerc de subiecți ai Legii nr. 48/2023. În acest context, în situația stabilirii sumei respective aceasta ar avea un caracter disproporționat față de condiția procentuală, având în vedere caracterul pestriț din punct de vedere a dimensiunii și a cifrei de afacere ale subiecților Legii nr. 48/2023.
		20.	Cu referile la pct. 20 și pct. 22 – 26 din proiectul Regulamentului, constatăm că nu au fost preluate la calificarea caracterului semnificativ al incidentului, în speță, la criteriul disponibilității serviciului respectiv, ca alternativă, disponibilitatea serviciului la ”peste 1 milion de utilizatori ai serviciului...din UE”, ori urmează a fi luată în considerare cifra cea mai mică, pentru o durată care depășește o oră potrivit normelor corespondente de la art. 7 și art. 9 – 14 din actul UE.	**Nu se acceptă.** După cum s-a menționat și în tabelul de concordanță referitor la literele b) și d) din actul UE, condiția alternativă de 1 milion de utilizatori nu a fost preluată în proiectul de act normativ național, deoarece în actul UE cifra este utilizată proporțional anumitor calificative ale statelor membre ale UE (cifra de afaceri ale entităților din sectoarele infrastructură digitală și servicii digitale, populație, număr de utilizatori), ceea ce nu este aplicabil Republicii Moldova, iar la nivel național nu sunt date disponibile care ar permite stabilirea unei cifre realiste.
			Obiecții privind clauza de armonizare	
		21.	Proiectul național nu conține clauza de armonizare, care este obligatorie pentru toate actele normative care au ca scop transpunerea legislației UE. Astfel, ținând cont de prevederile art. 31 din Legea nr. 100/2017 cu privire la actele normative și pct. 30 din Regulamentul privind armonizarea legislației Republicii Moldova cu legislația Uniunii Europene, aprobat prin HG ne. 1171/2018, după clauza de adoptare a proiectului național urmează a fi inserată clauza de armonizare în următoarea redacție:	**Se acceptă.**

			”Prezenta Hotărâre transpune Regulamentul de punere în aplicare (UE) 2024/2690 al Comisiei din 17 octombrie 2024 de stabilire a normelor de aplicare a Directivei (UE) 2022/2555 în ceea ce privește cerințele tehnice și metodologice ale măsurilor de gestionare a riscurilor în materie de securitate cibernetică și specificarea suplimentară a cazurilor în care un incident este considerat semnificativ referitor la furnizorii de servicii DNS, registrele de nume TLD, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea, precum și prestatorii de servicii de încredere, CELEX: 32024R2690, publicat în Jurnalul Oficial al Uniunii Europene L din 18 octombrie 2024”.	
			Obiecții privind sigla UE	
		22.	Totodată, pentru respectarea cerințelor înaintate față de proiectele de acte normative cu relevanță UE stabilite de art. 31 din Legea nr. 100/2017 și pct. 36 și 37 din Regulamentul, aprobat prin HG nr. 1171/2018, proiectul național urmează a fi marcat pe prima pagină în colțul drept de sus cu sigla UE (se indică cu litere mari, cu caractere aldine, fontul Times New Roman și mărimea corpului de literă 16).	**Se acceptă.**
		23.	**Concluzii:** Ca urmare a expertizei de compatibilitate realizate, proiectul național și clauza de armonizare vor fi revizuite potrivit celor expuse mai sus.	**Se acceptă,** cu excepțiile menționate mai sus.
4.	**Aparatul Președintelui Republicii Moldova**		Comunică lipsa obiecțiilor și susține promovarea proiectului.	

	(Nr.2/2-06-386 din 28.02.2025)			
5.	**Ministerul Infrastructurii și Dezvoltării Regionale** *(05-878 din 19.02.2025)*	Comunică despre susținerea proiectului, cu următoarele propuneri.		
		24.	Pct. 1 din proiectul de hotărîre a Guvernului de completat cu cuvintele (se anexează).	**Se acceptă.**
		25.	II. La proiectul regulamentului: a) la textul „Anexa nr.1” de exclus cuvintele „nr.1”;	**Se acceptă.**
		26.	b) textul urmează a fi ajustat conform prevederilor art. 52 din Legea nr.100/2017 cu privire la actele normative;	**Se acceptă.**
		27.	c) prevederile pct. 3.1, 3.3, 6.2 urmează a fi reformulate/ajustate în conformitate cu prevederile art.54 alin.(1) lit. a) din Legea nr.100/2017 cu privire la actele normative potrivit căreia conținutul proiectului actului normativ trebuie expus într-un limbaj simplu, clar și concis, pentru a se exclude orice echivoc.	**Precizare.** Presupunem că obiecția se referă la anexa la Regulament și nu la proiectul de Regulament propriu-zis, având în vedere că în textul proiectului de regulament nu există o astfel de numerotare. În acest caz, ar fi utilă motivarea obiecției cu referire la cazurile concrete și nu doar invocarea prevederilor legale aplicabile textului la care se obiectează. Limbajul utilizat este bazat pe terminologia consfințită în acest domeniu și este similar textului oficial în limba română al punctelor 1.2.1, 1.2.4 și, respectiv, 2.1.2 lit. b) din anexa la Regulamentul de punere în aplicare (UE) 2024/2690 al Comisiei din 17 octombrie 2024 de stabilire a normelor de aplicare a Directivei (UE) 2022/2555.
6.	**Ministerul Energiei** *(Nr. 02-439 din 18.02.2025)*		**La proiect de act normativ:**	
		28.	La p.1. se propune ca după ”Legii nr. 48/2023 privind securitatea cibernetică” în loc de punct să fie virgulă.	**Se acceptă.**
		29.	La p.5 se propune cuvântul ”implementarea” să fie schimbat cu ”implementare”.	**Se acceptă.**
		30.	La p.11 se propune între cuvintele ”evaluează” și ”dacă” să fie adăugat ”cazul” pentru o mai bună înțelegere.	**Nu se acceptă.**

				Includerea cuvântului propus ar distorsiona sensul și ideea de bază a redacției propuse a punctului respectiv.
		31.	La p.12 se propune între cuvintele ”evaluează” și ”dacă” să fie adăugat ”cazul” pentru o mai bună înțelegere.	**Nu se acceptă.** Includerea cuvântului propus ar distorsiona sensul și ideea de bază a redacției propuse a punctului respectiv.
		32.	La p.16 este indicat să fie schimbat anul la Legea nr.48 din ”20203” în ”2023”. Tot aici la subpunctul a) este indicat să fie virgulă după cuvântul ”afectat”.	**Se acceptă.**
		33.	La p.17 este indicat formularea la singular ”Incidentul,” iar virgula să fie în fața cuvântului ”care” fiind o propoziție explicativă. Tot aici, îmbinarea de cuvinte ”nu sunt considerate” să fie schimbate cu ”nu este considerat”.	**Nu se acceptă.** Conform regulilor gramaticale, incidența („în mod individual” în acest caz) urmează a fi izolate prin virgulă. Totodată, este oportună păstrarea formei la plural a cuvântului incident, având în vedere că aceasta decurge din necesitatea explicării contextului în care multe incidente cu caracter recurent sunt considerate ca fiind unul singur incident cu impact semnificativ.
		34.	La p.21 se propune ca la subpunctul a) să fie înlocuit ”un serviciu de centru de date al unui centru de date operat” cu ”un serviciu al unui centru de date gestionat”. Tot aici, la subpunctul b) se propune simplificarea prin eliminarea după cuvântul serviciu ”de centru de date”.	**Nu se acceptă.** Redacția din proiect corespunde terminologiei juridice date în particular de prevederile Regulamentului cu privire la identificarea furnizorilor de servicii, aprobat prin Hotărârea Guvernului nr. 860/2024. Conform punctului 2.7. *serviciu de centre de date* este o noțiune unică care semnifică un serviciu care cuprinde structuri sau grupuri de structuri dedicate găzduirii, interconectării și exploatării centralizate a tehnologiei informației și a echipamentelor de rețea, care furnizează servicii de stocare, prelucrare și transport de date,

				împreună cu toate instalațiile și infrastructura de distribuție a energiei electrice și de control al mediului.
			La anexă	
		35.	La p. 22 se propune revizuirea propozițiilor ”Dacă este adecvat, furnizorii de servicii stabilesc valori corespunzătoare pentru pragurile de alarmă. În cazul în care valorile stabilite pentru pragul de alarmă sunt depășite, o alarmă urmează să se declanșeze automat, dacă este adecvat.” din care nu este clar obiectivul către ce anume trebuie să fie ”adecvat”. Sau se propune înlocuirea îmbinării de cuvinte ”dacă este adecvat” cu îmbinarea de cuvinte ”dacă este cazul/oportun”.	**Nu se acceptă.** Proiectul de act normativ, după cum este formulat, transpune prevederile Regulamentului de punere în aplicare (UE) 2024/2690 al Comisiei din 17 octombrie 2024. Sintagma „dacă este adecvat” în contextul acestei propoziții urmează a fi interpretată din perspectiva principiului proporționalității măsurilor de securitate în raport cu riscurile identificate la adresa securității rețelelor și sistemelor informatice ale furnizorului de servicii. Modul de aplicare a acestui principiu este dat la punctele 7 și 8 din proiectul Regulamentului. Totuși, propoziția a treia a fost revizuită rezultând următoarea redacție: *În cazul în care valorile stabilite pentru pragul de alarmă sunt depășite, o alarmă urmează să se declanșeze**, dacă este adecvat,** în mod automat.*
		36.	La p.53 se propune ca să fie modificată expresia ”furnizorii și prestatorii lor de servicii direcți” cu ”furnizorii și prestatorii direcți de servicii” pentru o percepere mai facilă.	**Se acceptă.**
		37.	La p.71 se propune în loc de ”Procedurile de gestionare a modificărilor se aplică noilor versiuni, modificărilor și modificărilor de urgență ale oricărui software și hardware în exploatare și modificărilor configurației.” să fie utilizat ”Procedurile de gestionare a modificațiilor se aplică noilor versiuni, la modificări și modificări de urgență ale oricărui software și hardware în exploatare și modificărilor configurației.”	**Se acceptă.** Sintagma „gestionarea modificărilor” a fost substituită cu sintagma „gestionarea schimbărilor”.

		38.	La p.92.1. se propune în loc de ”ce măsuri” să fie folosit ”măsurile”	**Se acceptă.**
		39.	La p.92.4. se propune în loc de ”cine este responsabil” să fie folosit ”persoana/entitatea responsabilă”	**Se acceptă.**
		40.	La p.92.6. se propune în loc de ”cine trebuie să analizeze și să evalueze aceste” să fie folosit ”persoana/entitatea responsabilă de analiza și evaluarea acestor”	**Se acceptă.**
		41.	La p.109.2. se propune ca în expresia ”clasificarea activelor menționată la în capitolul” să fie eliminată prepoziția ”la”.	**Se acceptă.**
		42.	La p.156 se propune la sfârșitul propoziției în loc de ”cu acestea” să fie utilizat ”lor”.	**Nu se acceptă.** Acceptarea propunerii ar implica deficiențe semantice.
			La nota de fundamentare:	
		43.	La p.2.1. se propune ca în ”(în continuare – Legea nr. 48.2023)” să fie ”(în continuare Legea nr. 48/2023)”.	**Se acceptă.**
		44.	La pag.8 aliniatul 2 se propune corectarea ”Astfel, aceste entități urmează fi gestionate” cu ”Astfel, aceste entități urmează a fi gestionate”	**Precizare.** Autorul obiecției propune substituirea unor texte identice.
		45.	La pag.11 se propune corectarea la subpunctul ”– oferirea bazei juridice pentru determinarea în mod sincronizare” cu ”– oferirea bazei juridice pentru determinarea în mod de sincronizare”.	**Precizare** Sintagma a fost reformulată pentru o redare mai clară
		46.	La pag. 13 se propune în cazul subpunctului ”- printr-o notificare a incidentului evaluare inițială a incidentului semnificativ” folostrea virgulei ”- printr-o notificare a incidentului, evaluare inițială a incidentului semnificativ”.	**Precizare** Sintagma a fost exclusă
		47.	La pag.14. primul alianiat se propune corectarea ”Legea nr. 48/20203” cu ”Legea nr. 48/2023”.	**Se acceptă.**
		48.	La pag.14. se propune la subpunctul d) în cazul ”altui furnizor de servicii sau utilizatorilor serviciilor le-au fost cauzate” să fie folosit ”altui furnizor de servicii sau utilizatorilor serviciilor, cărora le-au fost cauzate”.	**Nu se acceptă.** Textul literei d) este preluat din art. 12 alin. (5) din Legea nr. 48/2023.

		49.	La pag.14. ultimul aliniat se propune în cazul ”de asigurare a securității rețelelor și sistemelor informatice pe are aceștia le dețin.” folosirea expresiei ”de asigurare a securității rețelelor și sistemelor informatice pe care aceștia le dețin.”	**Se acceptă**
		50.	La pag.18. se propune la aliniatul 5 în loc de ”pe care le implică menținerea pasului” să se folosească ”necesare corespunderii”.	**Nu se acceptă.** Textul respectiv este un citat.
		51.	La pg.19. se propune în aliniatul 5 în loc de ”inclusiv al structurile organizaționale” să se folosească ”inclusiv al structurilor organizaționale”.	**Se acceptă.**
		52.	La pag.21 subpunctul 4.4.1. se propune ca să fie modificată expresia ”ar trebuie aibă un” cu expresia ”ar trebui să aibă un”.	**Se acceptă.**
		53.	La pag. 21 punctul 4.6. se propune ca în loc de expresia ”îmbunătăți încrederea on-line a cetățenilor” să se folosească ”îmbunătăți încrederea în serviciile on-line a cetățenilor”.	**Se acceptă.** Textul „încrederea on-line a cetățenilor” a fost substituit cu textul „încrederea cetățenilor în mediul on-line”
		54.	La pag.22 punctul 5.1 aliniatul doi se propune ca în loc de ”constă în stabilească cerințelor” să se folosească ”constă în stabilirea cerințelor”.	**Se acceptă.**
		55.	La pag.23 aliniatul trei se propune ca în loc de ”Toate cadrele folosesc” să fie folosit ”Toate cadrele ce se folosesc”.	**Se acceptă.**
		56.	La pag.23 aliniatul cinci se propune ca în expresia ”rămân în vigoare.” punctul să fie exclus.	**Se acceptă.**
		57.	La pag.26 la subpunctul trei se propune în loc de ” -să acorde suport furnizorilor de servicii prin evaluarea nivelului de maturitate și conformitate a acestora cu cerințele de asigurarea a securității cibernetice;” să fie ” -să acorde suport furnizorilor de servicii prin evaluarea nivelului de maturitate și conformitate a acestora cu cerințele de asigurare a securității cibernetice;”	**Se acceptă.**
7.	**Ministerul Finanțelor**	**58.**	În informațiile prezentate la compartimentul 4.2 al notei de fundamentare privind impactul financiar și argumentarea costurilor estimative, autorul indică că autoritățile/instituțiile	**Se acceptă.** Nota de fundamentare a fost completată cu textul propus.

	(Nr. 07/3-03-33/247 din 21.02.2025)		publice au deja prevăzute anumite mijloace financiare în bugetul de stat pentru realizarea cerinţelor minime obligatorii de securitate cibernetică, și se presupune să nu fie necesară o creștere substanțială a cuantumului mijloacelor finaciare la cele deja planificate. Respectiv, se propune după text de completat cu următoarea propoziție: „Implementarea măsurilor de securitate cibernetică pentru furnizorii de servicii din sectorul public se va asigura din contul și în limita mijloacelor financiare alocate în legile bugetare anuale”.	
		59.	Totodată, autorul menționează că costurile necesare pentru implementarea acțiunilor ce urmează a fi suportate de Agenția Securitatea Cibernetică (ASC) nu implică cheltuieli suplimentare din bugetul de stat, însă fără prezentarea detaliilor în acest sens. Astfel, urmează a fi indicat subprogramul bugetar 1504 ”Tehnologii informaționale” și suma alocațiilor aprobate în bugetul de stat pentru anul 2025 în vederea asigurării implementării acțiunilor de către ASC. Reieșind din cele relatate, autorul urmează să ajusteze nota de fundamentare a proiectului privind impactul financiar și argumentarea costurilor estimative prin prisma celor expuse mai sus.	**Se acceptă.** Nota de fundamentare a fost completată, la pct. 4.2, cu textul următor: „Astfel, în Legea bugetului de stat pentru anul 2025, Ministerului Dezvoltării Economice și Digitalizării în subprogramul bugetar 1504 „Tehnologii informaționale” îi sunt prevăzute cheltuieli în valoare de 20416,5 mii lei. Aceste cheltuieli sunt asociate realizării de către Agenție a competenței sale în ce privește implementarea politicii de stat în domeniul securității cibernetice, inclusiv exercitarea funcției de supraveghere și control al modului în care sunt respectate prevederile cadrului normativ în acest domeniu, oferirea de asistență, inclusiv metodologică furnizorilor de servicii în sectoarele critice în vederea implementării măsurilor de securitate.”
8.	**Ministerul Mediului** *(Nr. 12/2-07/433 din 17.02.2025)*		Lipsa obiecțiilor și propunerilor.	
9.	**Ministerul Sănătății**		Lipsa obiecțiilor sau propunerilor.	

	(Nr. 27/877 din 13.03.2025)			
10.	**Ministerul Agriculturii și Industriei Alimentare** *(Nr. 2025PHG-444 din 25.02.2025)*	**Obiecţii argumentate şi explicite pe marginea cărora trebuie să se ajungă la un acord:**		
		60.	*În hotărîre:* În clauza de emitere, referința la articolul 11 alineatul (4) litera a) din Legea nr. 48/2023 privind securitatea cibernetică, urmează a fi substituită că referința la articolul 11 alineatul (4) litera b), întrucît litera a) prevede competența Guvernului de a aproba, prin intermediul organismului național de standardizare, „standardelor naţionale în domeniul securităţii informaţiei şi al securităţii cibernetice”, pe cînd litera b) prevede competența Guvernului de a aproba „cerinţele specifice de securitate privind reţelele și sistemele informatice”, ceea ce face obiectul proiectului supus avizării.	**Se acceptă.** În clauza de adoptare a fost menținută doar referința la articolul 11 din Legea nr. 48/2023. De asemenea, clauza de adoptare a fost completată cu referința la art. 14. alin (2) din Legea nr. 48/2023, conform căreia Guvernul aprobă cerințele minime de securitate pentru furnizorii de servicii persoane juridice de drept public.
		61.	*La anexa nr. 1:* Pct. 17 litera c), observăm că nu este indicat actul normativ al referinței la articolul 3 alineatul (1) litera a).	**Precizare** Punctul respectiv a fost exclus
		Propuneri care poartă caracter de recomandare:		
		62.	*La anexa nr. 1:* Pct. 10 propunem autorului reformularea literei b), întrucît textul „au efect cel puțin echivalent cu cele prevăzute la articolul 12 din Legea nr. 48/2023 privind securitatea cibernetică” nu are legătură logică cu prima parte a prevederilor acestei litere.	**Se acceptă.** La litera respectivă, după cuvintele „impact semnificativ” s-a completat cu textul „și dacă obligațiile de notificare”.
		63.	*La pct. 3.1 din Anexa la Regulament*, propunem substituirea cuvîntului „autoritățile” prin cuvîntul „împuternicirile” sau „atribuțiile”, pentru a exclude posibilitatea interpretării că furnizorii de servicii, care pot fi atît persoane juridice de public cît și de drept privat, dispun de careva autoritate, în sensul de „putere de stat”.	**Se acceptă.** Cuvântul „autoritățile” a fost substituit cu cuvântul „atribuțiile” în tot textul anexei la Regulament.
11.	**Ministerul Apărării**		Lipsa obiecțiilor.	

	(Nr. 11/181 din 12.02.2025)			
12.	**Ministerul Afacerilor Interne** *(Nr. 38/537 din 18.022025)*	Comunică despre susținerea conceptuală a proiectului cu menționarea următoarelor considerente. Cu referire la conceptul proiectului prenotat, se înaintează propuneri și recomandări, după cum urmează.		
		64.	În tot conținutul proiectului se recomandă revizuirea cuvintelor *„legislația sectorială”*, deoarece acestea nu sunt adaptate terminologiei juridice autohtone, fapt ce poate genera interpretări extensive în procesul de aplicare a normelor juridice.	**Se acceptă.** La pct. 1 din proiectul regulamentului cuvintele „legislație sectorială” au fost substituite cu textul „legislației care reglementează activitatea furnizorilor de servicii și/sau sectoarele şi subsectoarele critice stabilite prin Hotărârea Guvernului nr. 860/2023 cu privire la identificarea furnizorilor de servicii *(în continuare - legislație sectorială)*”. Soluția propusă se bazează pe formula textuală prevăzută la art. 3 alin (5) din Legea nr. 48/2023.
		65.	În tot conținutul proiectului apare o incertitudine cu referire la cuvântul *„răuvoitoare”*, inclusiv în partea ce ține de sintagmele ce îl înglobează. Din acest motiv, se propune reformularea acestuia, astfel încât conținutul normativ al proiectului să corespundă prioritar reglementărilor din Codul contravențional nr. 218/2008, Codul penal nr. 985/2002 și, după caz, celor din alte acte normative care reglementează acțiunile ilegale în domeniul securității cibernetice.	**Se acceptă.** Cuvântul „răuvoitor” a fost substituit cu cuvântul „ilegal”.
		66.	La pct. 16 din proiectul regulamentului nu sunt clare limitele noțiunii *„prejudicii nonmateriale”*, deoarece legislația națională operează exclusiv cu noțiunile de *„prejudiciu fizic”*, *„prejudiciu material”* și *„prejudiciu moral”*. Prin urmare, cuvântul „nonmaterial” este utilizat cu sens ambiguu, fapt ce determină apariția unor confuzii în procesul de calificare a tipologiei prejudiciului cauzat în cazul unui incident cibernetic.	**Se acceptă.** Textul „materiale și nonmateriale” a fost exclus.
		Cu referire la aspectele de tehnică legislativă, se înaintează observații, în ordinea ce succede.		

		67.	Se atrage atenția că dosarul proiectului de act normativ include tabelul de concordanță. Totuși, proiectul de act normativ nu reglementează clauza de armonizare, ce indică tipul, numărul şi denumirea oficială a actelor Uniunii Europene care se transpun în actul normativ, seria, numărul şi data Jurnalului Oficial al Uniunii Europene în care au fost publicate actele respective, precum și măsura în care acestea sunt transpuse.	**Se acceptă.**
		68.	Se specifică că potrivit art. 44 alin. (4) din Legea nr. 100/2017 cu privire la actele normative, clauza de armonizare este obligatorie pentru toate proiectele actelor normative cu relevanță UE. Mai mult, conform art. 31 alin. (2) din legea prenotată, actele normative cu relevanță UE sunt marcate cu sigla „UE” și conțin clauza de armonizare conform modelului stabilit în Hotărârea Guvernului nr. 1171/2018 pentru aprobarea Regulamentului privind armonizarea legislației Republicii Moldova cu legislația Uniunii Europene.	**Se acceptă.**
		69.	În tot conținutul proiectului regulamentului, este necesară a fi revizuită gruparea elementelor structurale a punctelor, deoarece conform art. 52 alin. (3) din Legea nr. 100/2017, pentru interpretare corectă și aplicare comodă, punctele pot fi divizate în subpuncte care se numerotează prin adăugarea consecutivă a cifrelor arabe, până la gradul de detaliere necesar.	**Se acceptă.**
		70.	Se recomandă completarea proiectului cu lista de abrevieri utilizate, inclusiv cu explicația acestora, întrucât autorul proiectului utilizează o multitudine de acronime și neologisme, a căror înțelesuri nu sunt definite la prima utilizare.	**Se acceptă.** În textul proiectului de act normativ au fost introduse, acolo unde este cazul explicarea abrevierilor.
		71.	Se propune completarea pct. 1 din proiectul de hotărâre cu cuvintele *„conform anexei”*, întrucât conținutul regulamentului care urmează a fi aprobat este prevăzut în conținutul anexei. Concomitent, din preambulul anexei, textul *„nr. 1”* se va exclude ca fiind inutil, deoarece proiectul de hotărâre conține o anexă unică. Or, potrivit art. 49 alin. (4) din Legea nr.	**Se acceptă.**

			100/2017, dacă un act normativ are mai multe anexe, acestea sunt însemnate cu numere ordinare, exprimate prin cifre arabe, în ordinea în care au fost enunțate în textul actului. În concluzie, se solicită respecuos revizuirea proiectului prin prisma recomandărilor și propunerilor formulate mai sus.	
13.	**Ministerul Afacerilor Externe** *(Nr. DI/3/041.1-1487 din 14.02.2025)*	**72.**	În conformitate cu art. 31, alin. (2) din Legea nr. 100/2017 cu privire la actele normative, precum și potrivit pct. 13, alin. (4), pct. a) și b) din Regulamentul privind armonizarea legislației Republicii Moldova cu legislația UE, aprobat prin Hotărârea Guvernului nr. 1171/2018 (în continuare – *Regulament*), proiectul de act normativ care are ca scop transpunerea actelor juridice europene conține în mod obligatoriu clauza de armonizare, care indică gradul de transpunere a actului juridic european și este marcat cu sigla „UE”. Astfel, proiectul supus examinării urmează a fi ajustat corespunzător celor menționate supra, clauza de armonizare urmând a fi inclusă după preambulul și clauza de adoptare ale proiectului, în conformitate cu modelele stabilite în anexa nr.1 la Regulament.	**Se acceptă.**
14.	**Ministerul Educației și Cercetării** *(Nr. 08/3-09/1591 din 10.03.2025)*		Lipsa de obiecții şi propuneri.	
15.	**Ministerul Muncii și Protecției Sociale** *(Nr. 22/888 din 21.02.2025)*		Lipsa obiecţiilor şi propunerilor.	
16.	**Ministerul Culturii**		Lipsa de obiecţii şi propuneri.	

	(Nr. 05/4-09/370 din 06.02.2025)			
17.	**Serviciul de Informații și Securitate** *(Nr. IE/1459 din 18.02.2025)*	**Cu referire la textul proiectului Hotărârii de Guvern:**		
		73.	Punctul 2 stabilește că, măsurile de securitate a rețelelor și sistemelor informatice urmează a fi implementate pe parcursul a 3 ani în baza analizei riscurilor. Astfel, Serviciul constată că termenul este unul mult prea mare și va afecta securitatea cibernetică a furnizorilor de servicii – care reprezintă entități critice pentru asigurarea funcțiilor vitale ale societății și statului. În acest sens, propunem limitarea termenului de la 3 ani la 2 ani și includerea unei norme suplimentare prin care se va coordona cu Agenția pentru Securitate Cibernetică (*în continuare - Agenția*), analiza de riscuri efectuată și Planul de implementare a măsurilor de securitate cibernetică. Corespunzător, Agenția va deține informații privind deficiențele din infrastructurile TIC ale furnizorilor, va superviza și acorda suport acolo unde este necesar la realizarea Planului de implementare a măsurilor.	**Se acceptă.** Partea dispozitivă a hotărârii Guvernului a fost revizuită corespunzător.
		74.	La punctul 4, de abrogă Cerințele minime obligatorii de securitate cibernetică (HG 201/2017), cerințe ce sunt obligatorii pentru Cancelaria de Stat, Ministere, entități subordonate Guvernului și structurile organizaționale din sfera lor de competență. Astfel, pentru a nu crea un vid normativ, și pentru a asigura continuitatea aplicării măsurilor de securitate cibernetică în entitățile publice, Serviciul propune completarea punctului 2 și anume, după sintagma „Furnizorii de servicii” adăugarea cuvintelor „și persoanele juridice de drept public”.	**Nu se acceptă.** Noțiunea „furnizori de servicii” cuprinde și persoanele juridice de drept public. Potrivit art. 2 din Legea nr. 48/2023, furnizor de servicii – persoană juridică de drept public sau de drept privat, înregistrată în Republica Moldova, care prestează servicii în unul sau mai multe sectoare şi/sau subsectoare critice, stabilite de către Guvern, şi care este identificată de autoritatea competentă în conformitate cu prevederile prezentei legi şi ale actelor normative pentru punerea acesteia în aplicare. Persoanele juridice de drept public intră în domeniul de aplicare al

				Legii nr. 48/2023 în temeiul prevederilor art. 3 alin. (2) lit. i) din legea menționată.
		75.	Punctul 8 din *Regulamentul cu privire la modul de aplicare a măsurilor de securitate a rețelelor și sistemelor informatice de către furnizorii de servicii în sectoarele critice (Anexa nr. 1 la proiectul Hotărârii de Guvern)*, stabilește că furnizorul poate să nu aplice o cerință dacă o consideră nefezabilă (neadecvată, neaplicabilă etc.), în asemenea circumstanțe Serviciul consideră necesar, notificarea obligatorie a Agenției pentru analiza impactului de neaplicare. Totodată, considerăm că decizia de neaplicare a unei cerințe necesită a fi coordonată cu specialiștii Agenției, pentru a minimiza probabilitatea de producere a unor incidente majore de securitate cibernetică din motivul unor omisiuni.	**Se acceptă.** Punctul 8 a fost completat cu textul: „informând Agenția pentru Securitate Cibernetică în termen de 10 zile din data documentării motivării de neimplementare a cerinței respective.”.
		76.	La secțiunea 3 din *Cerințele privind măsurile de gestionare a riscurilor în materie de securitate cibernetică (Anexa nr. 2 la proiectul Hotărârii de Guvern)*, s-ar presupune din punct de vedere logic, efectuarea unor audituri externe privind respectarea cerințelor de securitate cibernetică stabilite în prezentul proiect de Hotărâre de Guvern. Totuși, în realitate, din textul secțiunii reiese că auditul este unul intern, respectiv independența acestuia este subiectivă, la fel ca și rezultatele. În acest sens, Serviciul consideră necesară revizuirea prevederilor Secțiunii, în scopul introducerii unor norme obligatorii de efectuare a auditului extern privind respectarea cerințelor de securitate cibernetică, prin contracararea unor entități/specialiști autorizați de Agenție.	**Se acceptă.** Proiectul Regulamentului a fost completat cu un punct nou în următoarea redacție: „9. Furnizorii de servicii efectuează audituri externe privind securitatea informațiilor, în vederea determinării nivelului de conformitate cu cerințele privind măsurile de securitate a rețelelor și sistemelor informatice, prevăzute în anexa la prezentul Regulament, cel puțin o dată la trei ani sau ori de câte ori este necesar în conformitate cu cerințele stabilite de anexa la prezentul Regulament. Raportul de audit extern și rapoartele examinărilor independente, efectuate în conformitate cu secțiunea 2 a capitolului 2 din anexa la prezentul Regulament se prezintă Agenției pentru Securitate Cibernetică în termen de o lună de la data efectuării”.
		77.	Totodată, Serviciul consideră necesară instituirea unei norme de prezentare a raportului de audit în adresa Agenției. În felul	**Se acceptă.**

			dat Agenția va cunoaște și monitoriza respectarea de către furnizori a cerințelor de securitate. Nu în ultimul rând, cele menționate vor facilita dezvoltarea unei industrii de securitate cibernetică în Republica Moldova.	Proiectul Regulamentului a fost completat cu un punct nou în următoarea redacție: „9. Furnizorii de servicii efectuează audituri externe privind securitatea informațiilor, în vederea determinării nivelului de conformitate cu cerințele privind măsurile de securitate a rețelelor și sistemelor informatice, prevăzute în anexa la prezentul Regulament, cel puțin o dată la trei ani sau ori de câte ori este necesar în conformitate cu cerințele stabilite de anexa la prezentul Regulament. Raportul de audit extern și rapoartele examinărilor independente, efectuate în conformitate cu secțiunea 2 a capitolului 2 din anexa la prezentul Regulament se prezintă Agenției pentru Securitate Cibernetică în termen de o lună de la data efectuării.”.
18.	**Serviciul Tehnologia Informației și Securitate Cibernetică** *(Nr. 1.4/387/25 din 18.02.2025)*	**Obiecții și propuneri la proiectul hotărârii.**		
		78.	Potrivit Notei de fundamentare, temei juridic pentru aprobarea hotărârii este articolul 14 alin. (2) din Legea nr. 48/2023, care stabilește că Guvernul va aproba măsurile de securitate minime obligatorii pentru persoanele juridice de drept public. Examinând proiectul constatăm că acesta stabilește generic aceleași reguli pentru toți furnizorii de servicii, concentrîndu-se de asemenea pe reglementarea mai multor raporturi juridice care apar în procesul de implementare a Legii 48/2023. Astfel reieșind din obiectul larg de reglementare a proiectului, considerăm necesară reformularea titlului hotărârii de guvern, și ca propunere vă prezentăm următorul text „Hotărâre cu privire la aprobarea unor acte normative pentru implementarea Legii nr. 48/2023 privind securitatea cibernetică”.	**Se acceptă parțial.** Titlul proiectului de act normativ a fost expus într-o nouă redacție care reflectă esența proiectului.
		79.	În continuarea ideii de mai sus, propunem ca Cerințele privind măsurile de gestionare a riscurilor în materie de securitate cibernetică, anexă la Regulament, să constituie un act normativ	**Nu se acceptă.** Regulamentul cuprinde prevederi care sunt în legătură cu cerințele specificate în anexă.

			separat, anexa nr. 2 la proiectul hotărârii. Urmare se va revedea numerotația punctelor din hotărâre.	Proiectul de Regulament cuprinde în mod specific un set de reglementări care au ca obiectiv facilitatea și asigurarea punerii corecte în aplicare a anexei, aceasta din urmă fiind o continuare logică a expunerii textului juridic cuprins în proiectul de Regulament.
		80.	Totodată, textul „cerințele privind măsurile de gestionare a riscurilor la adresa securității rețelelor și sistemelor informatice" din tot textul proiectului, se va reformula, deoarece utilizarea în același context atât a cuvântului „cerințe" cât și a cuvântului "măsuri" este de prisos, fie sunt „cerințe de gestionare...", fie „măsuri de gestionare....", în acest scop se va consulta art. 11 alin. (2). pct. 2 din Legea 48/2023, care operează cu textul „măsuri tehnice și organizatorice...".	**Se acceptă parțial.** Textul proiectului a fost modificat fiind utilizată următoarea sintagmă *cerințe privind măsurile de securitate a rețelelor și sistemelor informatice.* Au fost păstrate ambele noțiuni având în vedere că în raport cu măsurile de securitate cerințele presupun anumite operațiuni/activități/acțiuni componente mai detaliate și specifice atât de ordin tehnic, cât și organizatoric.
		81.	Potrivit art. 11 alin. (4) al Legii nr. 48/2023 privind securitatea cibernetică *„(4) În vederea asigurării îndeplinirii obligaţiilor prevăzute de prezentul articol şi asigurării securităţii reţelelor şi sistemelor informatice ale furnizorilor de servicii, Guvernul:* ***a) prin intermediul organismului naţional de standardizare, asigură aprobarea standardelor naţionale*** *în domeniul securităţii informaţiei şi al securităţii cibernetice în baza standardelor şi a specificaţiilor tehnice europene şi celor internaţionale relevante pentru securitatea reţelelor şi a sistemelor informatice;* *b) la propunerea autorităţii administraţiei publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securităţii cibernetice,* ***aprobă cerinţele specifice de securitate privind reţelele şi sistemele informatice în funcţie de sectorul, subsectorul, categoria şi/sau tipul furnizorului de servicii.***	**Se acceptă parțial.** Clauza de fundamentare a fost revizuită, prin excluderea referinței la alin. (4) al art. 11. Totuși, referința la art. 11 a fost păstrată având în vedere că proiectul are ca scop punerea în aplicare a acestui articol în mod cuprinzător, în particular prin detalierea prevederilor alineatului (2).

			Articolul citat nu poate constitui temei juridic de aprobare a prezentului proiect de hotărâre de guvern, or standardul național nu se aprobă de Guvern, ci de organismul național de standardizare, în Republica Moldova acest rol îl exercită Institutul de Standardizare din Moldova, iar la lit. b) Guvernul trebuie să aprobe cerințe **specifice** în funcție de sector/subsector, pe când prezentul proiect reglementează cadrul de măsuri generale pentru toți furnizorii de servicii indiferent de sector/subsector. Prin urmare din temeiul de aprobare al proiectului Hotărârii se va exclude textul „art. 11 alin. (4) lit. a)”, totodată, prin această prismă se va modifica și pct. 2.1. din Nota de fundamentare.	
		82.	La pct. 2 textul „pe parcursul a trei ani” induce în eroare privind termenul de realizare a obligației privind implementarea cerințelor, și poate fi interpretat că doar pe parcursul a 3 ani furnizorii sunt obligați să implementeze cerințele, pentru a evita interpretări eronate se va modifica cu textul „în termen de 3 ani”.	**Se acceptă.** Partea dispozitivă a proiectului de act normativ a fost revizuită.
		83.	La punctul 4 se va institui termen similar de abrogare a Hotărârii Guvernului nr. 201/2017 „cu privire la aprobarea Cerințelor minime obligatorii de securitate cibernetică” cu termenul de implementare a prezentului proiect, fiind absolut necesar reglementarea și menținerea pe parcursul următorilor 3 ani, până la implementarea măsurilor de securitate conform prezentului act normativ, a cerințelor minime de securitate cibernetică instituie conform cadrului normativ în vigoare.	**Nu se acceptă.** Proiectul de act normativ urmează să intre în vigoare conform termenului general, adică într-o lună din data publicării, însă implementarea și punerea prevederilor acestuia în aplicarea se va realiza conform algoritmului propus în partea dispozitivă a proiectului. Abrogarea Hotărârii Guvernului nr. 201/2017 trebuie realizată la data intrării în vigoare a proiectului de act propus spre examinare, în caz contrar vor exista două acte normative cu un obiect de reglementare similar pentru subiecții din sectorul public, ceea ce ar putea crea confuzii la interpretarea aplicabilității actelor. Totodată, partea

				dispozitivă a proiectului de hotărâre a fost revizuită în mod corespunzător.
		84.	În altă ordine de idei, conceptul propus în pct. 3, care presupune realizarea de către furnizori a obligațiilor de raportare, creează blocaj în realizarea atribuțiilor legale a Centrului Guvernamental de răspuns la incidentele cibernetice stabilite în art. 8 alin (3) și art. 12 alin. (11) din Legea nr. 48/2023 privind securitatea cibernetică. Astfel, se propune expunerea pct. 3 în următoare redacție :„ Agenția pentru Securitate Cibernetică va asigura implementarea, în termen de 6 luni, a unor mecanisme, inclusiv prin utilizarea mijloacelor tehnice, care să asigure un schimb sistematic, sigur și imediat de informații în contextul realizării de către furnizorii de servicii, cu excepția celor stabiliți la art. 12 alin. (11) din Legea 48/2023, a obligațiilor de raportare a incidentelor cibernetice cu impact semnificativ”.	**Nu se acceptă.** Prevederea respectivă nu are ca obiect de reglementare determinarea competenței ASC, ci stabilirea unor sarcini realizarea cărora va facilita și eficientiza punerea în aplicare a prevederilor legale.
		II. Obiecții și propuneri la Regulament.		
		85.	La pct. 1 având în vedere denumirea Regulamentului, în obiectul de reglementare a acestuia trebuie să se includă <u>modul de aplicare a măsurilor de securitate stabilite de art. 11 alin. (1) din Legea 48/2023</u>, care prevede *„Furnizorul de servicii este obligat să aplice continuu măsuri de securitate în scopul: a)* ***prevenirii incidentelor cibernetice****; b)* ***soluţionării incidentelor cibernetice****; c) prevenirii şi atenuării impactului asupra continuităţii serviciului ori asupra securităţii reţelei şi/sau sistemului informatic, cauzat de un incident cibernetic; d)* ***prevenirii şi atenuării impactului potenţial asupra continuităţii serviciilor*** *ori asupra securităţii reţelelor şi/sau sistemelor informatice dependente de cele ale furnizorului de servicii.*	**Se acceptă.** Punctul a fost revizuit corespunzător.
		86.	Se propune revizuirea pct. 4 prin prisma Legii nr. 20/2016 cu privire la standardizarea națională, în special art. 15 alin. (5), care prevede că în actele normative pot fi făcute referinţe	**Se acceptă.** Punctul 4 a fost revizuit prin excluderea primei propoziții.

			directe numai la standardele moldovenești publicate în limba română.	
		87.	Totodată, se propune revizuirea textului „legislația sectorială” din întregul proiect, or art. 6 din Legea nr. 100/2017 cu privire la actele normative, nu stabilește așa categorie de acte normative. Suplimentar, fiecare utilizare a textului „legislația sectorială” care presupune trimitere la anumite acte normative, urmează a fi realizată în conformitate cu art. 55 din Legea nr. 100/2017 cu privire la actele normative, potrivit cărui, în cazul în care proiectul actului normativ cuprinde prevederi ce se regăsesc în alte acte normative, se face trimitere expresă la actul normativ care le conține.	**Se acceptă.** La punctul 1 din proiect a fost dată explicarea acestui termen, utilizând-se formularea din art. 3 alin. (5) din Legea nr. 48/2023.
		88.	Capitolul II se va exclude deoarece este inoportun, or art. 3 alin. (5) din Legea 48/2023 clar reglementează acest aspect și nu necesită reglementări suplimentare. Astfel, întrucât la art. 11 sunt stabilite măsurile de securitate și la art. 12 obligația de notificare, pentru stabilirea echivalenței este necesară doar compararea prevederilor Legii nr. 48/2023 cu prevederile din alte legi speciale.	**Nu se acceptă.** Prevederile propuse în Capitolul II asigură clarificarea și detalierea prevederilor art. 3 alin. (5) pentru o mai bună aplicare. Totodată, aceste prevederi au ca obiectiv alinierea cadrului normativ național la Comunicarea Comisiei Orientările Comisiei privind aplicarea articolului 4 alineatele (1) și (2) din Directiva (UE) 2022/2555..
		89.	La pct. 17: - se va exclude textul *„și a punctului 16”* deoarece acesta nu stabilește dacă incidentul este semnificativ, ci prejudiciile considerabile în sensul art. 12 alin. (5) lit. d) din Legea 48/2023;	**Precizare.** Punctul respectiv a fost exclus
		90.	- textul „în mod colectiv” se va exclude, iar după textul „ca incidente recurente” se va adăuga textul „dar sunt considerate în mod colectiv”;	**Precizare.** Punctul respectiv a fost exclus
		91.	- după textul “articolul 3 alineatul (1) litera (a)” se va nominaliza legea la care se face referire, atragem atenția ca art. 3 alin. (1) Legea 48/2023 nu conține litere.	**Precizare.** Punctul respectiv a fost exclus

		92.	Reieșind din faptul, că criteriile și condițiile de determinare a impactului semnificativ al unui incident cibernetic, stabilite în Capitolul III (pct. 16-29) în mare parte se repetă, se consideră a fi oportună revizuirea și optimizarea formei de clasificare a acestei, fiind grupate în tabel.	**Nu se acceptă.** Prevederile acestor puncte sunt grupate din punctul de vedere al tipului furnizorului de servicii și expuse din perspectiva formulării unor norme juridice, conform cerințelor stabilite de cadrul normativ.
		III. Obiecții și propuneri la Anexa Regulamentului.		
		93.	La pct. 3 în primul enunț de exclus cuvântul „lor”, iar cuvântul „autoritățile” din pct. 3 și pct. 4, sbpct. 109.1 de modificat cu cuvântul „competențe”, după caz „funcții”, deoarece „authorities” din Regulamentul UE a fost eronat tradus ca „autorități”, și pentru a evita neînțelegeri la interpretarea normei juridice este necesară această modificare.	**Se acceptă parțial.** Cuvântul *autoritățile* a fost înlocuit cu cuvântul *atribuțiile*.
		94.	La pct. 32 textul „sunt obligați să stabilească” se va substitui cu textul „stabilesc”, iar la sbpct. 32.1 se va adăuga cuvântul „împreună” înainte de textul „cu echipa de răspuns”.	**Nu se acceptă.** Considerăm formularea textului din perspectiva obligativității este mai clară în varianta proiectului. În ce privește inserarea cuvântului „împreună”, aceasta ar distorsiona sensul reglementării.
		IV. Obiecție la Nota de fundamentare.		
		95.	Este absolut important a se completa pct. 4 Analiza impactului de reglementare, cu informație relevantă, în mod special pct. 4.1. Impactul asupra sectorului public, 4.2. Impactul financiar și argumentarea costurilor estimative și pct. 4.3. Impactul asupra sectorului privat, or lipsa unei analize adecvate a costurilor estimative privind implementarea proiectului, a impactului asupra sectorului public și privat creează imprevizibilitate și incertitudine privind posibilitatea furnizorilor de servicii de drept privat, și chiar și a celor de drept public, de a asigura respectarea hotărârii de guvern care urmează să fie aprobată.	**Nu se acceptă.** Nota de fundamentare cuprinde suficientă informație care permite estimarea cheltuielilor pe care urmează să le suporte un furnizor de servicii pentru a asigura conformitatea cu cerințele de securitate respective. Astfel, în ce privește sectorul public, trebuie să ținem cont de faptul că majoritatea prevederilor proiectului sunt executorii pentru autoritățile publice și instituțiile publice încă din anul 2017 când a fost aprobată Hotărârea Guvernului nr. 201/2017. Totodată, estimările realizate și furnizate la nivelul Statelor Membre ale UE

				arată că cheltuielile cu securitatea TIC a guvernelor ar trebui estimată la aproximativ 4,88 % din bugetul de cheltuieli pentru TIC. În ce privește sectorul privat această cifră se situează la aproximativ 0,52% din cifra de afaceri a furnizorului de servicii.
19.	**Agenția pentru Securitate Cibernetică**	**96.**	Agenția pentru Securitate Cibernetică propune completarea proiectului de Hotărâre a Guvernului privind modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii din sectoarele critice (număr unic 49/MDED/2025), prin introducerea unui punct nou care să modifice Anexa nr. 1 și Anexa nr. 3 la Hotărârea Guvernului nr. 860/2024 privind identificarea furnizorilor de servicii, cu următorul conținut: - Anexa 1 la hotărâre se completează cu pct. 91- în următoarea redacție: „Actul administrativ de desemnare în calitate de furnizor de servicii, cât și notificarea privind intenția de desemnare în calitate de furnizor de servicii constituie informație cu acces limitat. Modul de prelucrare a informației precum și acces la informația dată urmează a fi reglementat prin Ordinul Directorului Agenției pentru Securitate Cibernetică. – - Punctul 10 din Anexa nr.3 va avea următorul cuprins: „10. Lista constituie informație cu acces limitat. Modul de prelucrare a informației precum și accesul la listă urmează a fi reglementat prin Ordinul Directorului Agenției pentru Securitate Cibernetică.” Aceste propuneri de completare și modificare în general derivă din necesitatea de continuare a identificării furnizorilor de servicii fără limitări, precum și din cea de protejare a siguranței publice prin restricționarea accesului la actele administrative emise de către Agenția pentru Securitate Cibernetică în raport cu furnizorii de servicii.	**Se acceptă** Proiectul și nota informativă au fost completate.

			Astfel, în particular, se propune completarea Anexei 1 cu un punct nou ce urmează să restricționeze accesul la notificarea prealabilă și la actul administrativ emis de către Agenție în cadrul procedurii administrative cu potențialii furnizori de servicii pentru a nu prejudicia procedura administrativă și nemijlocit siguranța națională. În altă ordine de idei, modificarea anexei 3 la Hotărârea Guvernului nr. 860/2024 este necesară deoarece, în urma aplicării acesteia, s-a constatat că formularea actuală a punctului 10 din anexa 3 permite interpretări duale, generând dificultăți în întocmirea Listei furnizorilor de servicii care este esențială în contextual asigurării securității cibernetice a furnizorilor de servicii esențiale și importante. Mai mult, includerea listei la informație atribuită la secret de stat creează blocaje în activitatea Agenției, din perspectiva identificării și urmării amenințărilor și vulnerabilităților cibernetice asupraentităților esențiale și importante. Totodată, atribuirea la secret de stat al listei creează riscuri de compromitere a Regimului secret, reieșind din faptul că această listă poate fi dedusă din criteriile ce sunt stabilite de către Guvern care sunt stipulate într-un act normativ public. Pentru a evita blocajele de întocmire și menținerea listei, se propune revizuirea punctului 10, oferindu-i o formulare mai clară. Conform articolului 34 din Constituție, dreptul la informație de interes public nu poate fi îngrădit, însă acesta trebuie să fie exercitat fără a compromite siguranța națională sau protecția cetățenilor. Având în vedere caracterul sensibil al listei furnizorilor de servicii, aceasta nu poate fi pusă la dispoziția publicului fără restricții. Se propune, așadar, ca accesul la listă să fie limitat, iar modul de gestionare și utilizare a acestor informații să fie stabilit prin Ordinul Directorului Agenției pentru Securitate Cibernetică.	

			Această modificare este în concordanță cu practicile europene, unde, deși accesul la astfel de liste este restricționat, acestea nu sunt clasificate drept secret de stat. Regimuri similare se regăsesc în Germania, Belgia, Estonia, Spania și alte state europene.	
20.	**Agenția de Guvernare Electronică** *(Nr. 3007-021 din 12.02.2025)*	**97.**	Comunică avizarea favorabilă a proiectului și lipsa obiecții. Totodată, după analiza obiectului de reglementare al proiectului, constatăm că implementarea măsurilor de securitate cibernetică ce vor fi impuse de cadrul normativ nou în domeniu, după abrogarea Hotărârii Guvernului nr.201/2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică, va avea un impact financiar semnificativ atât asupra sectorului privat, cât și asupra *sectorului public*. Deși, în secțiunea 4.1. din Nota de fundamentare la proiect, se precizează că „proiectul de act normativ nu implică impacturi structurale și instituționale asupra sistemului administrației publice", este evident că autoritățile și instituțiile publice, vor trebui să suporte costuri asociate inclusiv pentru: • evaluări periodice ale infrastructurii TI, pentru identificarea și gestionarea riscurilor; • implementarea soluțiilor tehnice avansate, cum ar fi sisteme de monitorizare, gestionare a vulnerabilităților, criptare și alte măsuri de securitate cibernetică; • angajarea sau externalizarea personalului specializat în securitate cibernetică, care să asigure conformitatea și operarea sistemelor; • mentenanța și actualizarea continuă a sistemelor implementate, pentru a menține nivelul de securitate conform standardelor actualizate. În concluzie, implementarea cerințelor privind măsurile de gestionare a riscurilor în materie de securitate cibernetică implică un impact financiar direct asupra sectorului public, care trebuie evaluat și gestionat proactiv. Este important ca aceste	**Precizare.** Nota informativă analizează impactul asupra sectorului public din punct de vedere financiar, deoarece anumite schimbări fundamentale de ordin structural sau instituțional aceste cerințe nu implică. Într-o măsură destul de extinsă obligațiunile prescrise de proiectul de act normativ pentru autoritățile și instituțiile publice sunt acoperite deja de acte normative care sunt în vigoare. În cea mai mare parte, aceste obligații sunt stabilite de Hotărârea Guvernului nr. 201/2017 privind cerințele minime de securitate cibernetică. Aceste reglementări sunt executorii pentru autoritățile și instituțiile publice de o perioadă destul de extinsă de timp, începând cu aprilie 2017, când această hotărâre a intrat în vigoare. În același context, trebuie să evidențiem faptul că activitățile care sunt listate de către autorul obiecției sunt activități curente ale autorităților și instituțiilor publice. Stabilirea termenului de implementare în partea dispozitivă a proiectului de act normativ urmează anume raționamentul oferirii oportunității unei implementări etapizate, conform prioritizărilor determinate de către furnizorul de servicii, în funcție de

			cheltuieli să fie integrate în bugetele autorităților și instituțiilor publice, cu o planificare treptată și prioritizare a activelor critice. În acest context, la definitivarea proiectului, recomandăm autorului să examineze aspectele respective suplimentar și să reconsidere ***secțiunea 4.2. din Nota de fundamentare la proiect***, eventual prin descrierea impactului financiar asupra bugetelor, cu indicarea costurilor necesare pentru punerea în aplicare a actului normativ respectiv, reflectate pe bugete componente ale bugetului public național și pe ani bugetari, inclusiv a resurselor de la partenerii de dezvoltare, sau cu identificarea economiilor în cadrul bugetelor actuale care ar putea fi realocate în scopuri propuse și, după caz, cu prezentarea informațiilor privind veniturile generate/ratate în baza noilor reglementări – conform cerințelor din note la Anexa nr.1 la Legea nr.100/2017 cu privire la actele normative.	serviciile care le prestează, sectorul în care își desfășoară activitatea, tipul entității, etc. Nota de fundamentare la proiect, deși vine cu informații generice și orizontale în ce privește impactul asupra sectorului public, aceasta însă oferă suficientă bază pentru estimarea cheltuielilor ce vor fi necesare pentru implementarea acestor măsuri într-un termen de 2 -3 ani. În această ordine de idei, ar trebui să ținem cont de faptul că implementarea măsurilor de securitate este un proces continuu, acesta nu se va termina odată cu expirarea termenului menționat în partea dispozitivă a actului normativ (vezi art. 11 alin. (1) din Legea nr. 48/2023: *furnizorul de servicii este obligat să aplice continuu măsuri de securitate...)*. Termenul de implementare propus în partea dispozitivă este o perioadă de grație pentru furnizorii de servicii din perspectiva asigurării conformității și pregătirii pentru exercitarea de către ASC a funcției de supraveghere și control.
21.	**Agenția Servicii Publice** *(Nr. 01/2381 din 20.02.2025)*	**98.**	La **Capitolul 3 Gestionarea incidentelor, Secțiunea 2 Monitorizare și jurnalizare** – impune o influență majoră la deținerea resurselor tehnice pentru păstrarea registrelor și logourilor curente. Dacă să examinăm aspectul dat prin prisma Hotărârii Guvernului nr.414/2018, atunci responsabil de gestionarea resurselor menționate și anume integritatea și păstrarea copiilor de rezervă – ține de competența IP STISC. În caz contrar, fiecare Instituție de Stat va fi nevoită să-și achiziționeze independent echipamente corespunzătoare pentru gestionarea acestui proces, fapt ce contravine prevederilor legii.	**Nu se acceptă.** Aceste obligațiuni sunt în prezent în vigoare pentru autoritățile și instituțiile publice și sunt cuprinse de Hotărârea Guvernului nr. 201/2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică și de Hotărârea Guvernului nr.482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental.

		99.	**Secțiunea 4 Evaluarea și clasificarea evenime**ntelor – impune Instituțiilor de Stat extinderea statelor de personal angajat și crearea unei structuri interne de securitate informațională. Sarcinile structurii(subdiviziunii) vor cuprinde toate cerințele indicate în **Secțiunea 5 Răspunsul la incidente** și respectiv din **Capitolul 5 Securitatea lanțului de aprovizionare**. Totodată, Structura menționată va interacționa cu Agenția pentru Securitate Cibernetică și va implementa acțiunile descrise în secțiunile și capitolul enumerate mai sus (teste, audit, etc.).	**Nu se acceptă.** Aceste obligațiuni sunt în prezent în vigoare pentru autoritățile și instituțiile publice și sunt cuprinse de Hotărârea Guvernului nr. 201/2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică și de Hotărârea Guvernului nr.482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental.
		100.	La **Capitolul 6 Securitatea în achiziționarea, dezvoltarea și întreținerea rețelelor și a sistemelor informatice** – invocă două aspecte. În primul rând, fiecare Instituție de Stat va fi nevoită să reglementeze pe intern lista echipamentelor și producătorilor (vendori) aplicabili în participarea la achiziții, însă aceste acțiuni vor fi în contradicție cu prevederile Legii nr.131/2015 privind achizițiile publice, care interzice favorizarea. Pornind de la acest considerent, derivă aspectul doi, prin care Instituția Pubică Agenția pentru Securitate Cibernetică selectează independent și aprobă lista producătorilor și a echipamentelor propuse spre achiziționare Instituțiilor de Stat. În același timp, listele menționate necesită să fie Se acceptăe de către Agenția de Guvernare Electronică și Agenția Achiziții Publice.	**Nu se acceptă.** Ținem să menționăm că acest capitol nu impune furnizorilor de servicii așa-numita „reglementare pe intern a listei echipamentelor și producătorilor (vendorilor) aplicabili în participarea la achiziții”. Acest capitol, în mod deosebit secțiunea 1 (la care în principiu face referire autorul obiecției), stabilește cerințe pentru furnizorii de servicii în ce privește gestionarea riscurilor în procesul de achiziții, în funcție și în baza rezultatelor evaluării riscurilor. Nu este clar care prevedere a acestui capitol în mod specific intră în contradicție cu prevederile Legii nr. 131/2015 privind achizițiile publice.
		101.	La **Capitolul 10 Securitatea resurselor umane, Secțiunea 1 Securitatea resurselor umane** – Invocând informația, sectorul IT guvernamental se regăsește într-o criză de personal. Pentru menținerea unui personal calificat sunt necesare salarii decente și măsuri suplimentare de motivare. Acest lucru este, de asemenea, important pentru atragerea de noi specialiști sau pentru crearea unui mediu atractiv pentru profesioniștii din sectorul privat, aspect care lipsește în sectorul de stat. Totodată,	**Se acceptă,** însă problematica respectivă depășește obiectul de reglementare al proiectului de act normativ propus spre avizare și vizează problematici ce țin de politica de personal în sectorul public.

			birocratizarea excesivă exclude posibilitatea atragerii de personal calificat nou, dar și motivarea celor existenți. În acest context, menționăm că acest proiect este necesar, însă implementarea sa va întâmpina dificultăți atât din punct de vedere tehnic, cât și uman.	
22.	**Agenția Națională pentru Siguranța Alimentelor** *(Nr. 18-670 din 07.02.2025)*		Lipsa de propuneri și obiecții.	
23.	**Agenția Medicamentului și Dispozitivelor Medicale** *(Nr. Rg02 – 001042 din 04.03.2025)*		Lipsa obiecțiilor.	
24.	**Agenția Națională pentru Cercetare și Dezvoltare** *(Nr. 50 din 18.02.2025)*		Comunică avizarea pozitivă precum și lipsa obiecțiilor și a propunerilor.	
25.	**Agenția Națională pentru Reglementare în Energetică** *(Nr. 06-01/835 din 17.02.2025)*	**102.**	**La pct. 2** din proiectul de Hotărâre, considerăm oportun etapizarea detaliată a procesului de implementare a cerințelor privind măsurile de gestionare a riscurilor la adresa securității rețelelor și sistemelor informatice. ***Argumentare:*** Luând în considerare termenul de 3 ani pentru implementarea cerințelor de securitate, se impune descrierea/etapizarea procesului, ținând cont de capacitatea financiară a operatorilor economici și de impactul asupra tarifelor reglementate. Aceasta înseamnă că aceștia vor trebui	**Se acceptă parțial.** Partea dispozitivă a fost revizuită substanțial în vederea oferirii unei clarități mai mari procesului de implementare. Totuși, ținem să menționăm cu referire la „etapizarea detaliată a procesului de implementare”, că stabilirea termenului de implementare în partea dispozitivă a proiectului de act normativ urmează anume raționamentul oferirii

			să investească în soluții de securitate care sunt accesibile, dar și adecvate nivelului de risc, or evaluarea impactului economic al noilor obligații asupra furnizorilor de servicii în domeniul energetic necesită a fi clarificat în anexa la Regulament.	oportunității unei implementări treptate, conform prioritizărilor determinate de către furnizorul de servicii: în funcție de serviciile care le prestează, sectorul în care își desfășoară activitatea, tipul entității, mijloacele financiare disponibile etc. Totodată, ar trebui să ținem cont de faptul că implementarea măsurilor de securitate este un proces continuu, acesta nu se va termina odată cu expirarea termenului menționat în partea dispozitivă a actului normativ (vezi art. 11 alin. (1) din Legea nr. 48/2023: *furnizorul de servicii este obligat să aplice continuu măsuri de securitate...)*. Termenul de implementare propus în partea dispozitivă este „o perioadă de grație" pentru furnizorii de servicii din perspectiva asigurării conformității și pregătirii pentru exercitarea de către ASC a funcției de supraveghere și control.
		103.	**La proiectul Regulamentului**, este necesară o evaluare a impactului noilor cerințe asupra operatorilor din sectorului energetic în vederea asigurării implementării eficiente și sustenabile a noilor cerințe. ***Argumentare:*** La pct. 4 din proiectul de Hotărâre se face mențiunea privind abrogarea Hotărârii Guvernului nr. 201/2017 cu privire la aprobarea Cerințelor minime obligatorii de securitate cibernetică, însă proiectul înaintat spre avizare nu prevede evaluarea impactului noilor cerințe, astfel încât să nu pună o presiune administrativă excesivă asupra operatorilor, în special în contextul resurselor financiare și umane limitate.	**Nu se acceptă.** În nota de fundamentare a proiectului de act normativ sunt date informații suficiente pentru a putea determina impactul financiar asupra furnizorilor de servicii, inclusiv celor din sectorul energetic. Astfel, potrivit Raportului de evaluare a impactului la propunerea de Directivă a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în întreaga Uniune, de abrogare a Directivei (UE) 2016/1148 (Directiva NIS2): „Pe baza previziunilor periodice ale Gartner din 2012 până în 2020 privind procentajul cheltuielilor globale cu

				securitatea TIC din cheltuielile TIC și din veniturile totale, precum și ținând seama de cele mai recente date sectoriale ale Gartner disponibile Comisiei, în scopul evaluării impactului s-a presupus că media cheltuielilor pentru securitatea TIC pe sector în 2020 este de aproximativ 9,14% din cheltuielile totale TIC. În funcție de nivelul de maturitate și de capacitățile de securitate cibernetică ale sectorului, precum și de nivelul de digitalizare, această medie ar putea fi ajustată cu +/-3%. În plus, cheltuielile medii TIC pe sector sunt estimate la aproximativ 5,69% din cifra de afaceri totală și, prin urmare, cheltuielile medii cu securitatea TIC din cifra de afaceri totală pe sector în 2020 sunt estimate la aprox. 0.52%.”.
		104.	**La proiectul Regulamentului**, propunem completarea cerințelor de securitate cibernetică prin includerea unor standarde specifice aplicabile sectorului energetic, cum ar fi NIST SP 800-82 pentru sistemele SCADA și IEC 62443. ***Argumentare:*** Completarea cerințelor de securitate cibernetică prin includerea unor standarde specifice precum NIST SP 800-82 pentru sistemele SCADA și IEC 62443 pentru infrastructurile industriale ar reprezenta un pas esențial în protejarea sectorului energetic de riscurile cibernetice. Aceste standarde sunt esențiale pentru asigurarea unui nivel ridicat de securitate în fața amenințărilor cibernetice tot mai complexe, contribuind astfel la protejarea infrastructurilor critice, la prevenirea atacurilor și la menținerea continuității furnizării serviciilor energetice.	**Nu se acceptă.** În temeiul prevederilor art. 11 alin. 4 lit. b) din Legea nr. 48/2023 privind securitatea cibernetică, autoritățile publice centrale de specialitate responsabile de realizarea politicii de stat în sectoarele sau subsectoarele critice în comun cu autoritate publică responsabilă de realizarea politicii de stat în domeniul securității cibernetice urmează să înainteze propuneri de instituire a anumitor cerințe de securitate cibernetică specifice sectoarelor sau subsectoarelor critice. Proiectul propus spre avizare vine cu un set de cerințe orizontale ce urmează a fi implementate de toate persoanele juridice care cad sub incidența Legii nr. 48/2023.

		105.	**La proiectul Regulamentului,** propunem detalierea impactului financiar al noilor măsuri asupra furnizorilor de servicii energetice și corelarea acestora cu reglementările tarifare existente, pentru a preveni majorările nejustificate ale costurilor, protejând astfel consumatorii. ***Argumentare:*** Detalierea impactului financiar al noilor măsuri de securitate cibernetică asupra furnizorilor de servicii energetice și corelarea acestora cu reglementările tarifare existente sunt esențiale pentru a asigura că măsurile sunt implementate în mod eficient și echitabil. Acest proces implică mai multe etape și reprezintă aspecte importante care trebuie abordate cu atenție pentru a preveni creșterea prețurilor și tarifelor în mod nejustificat.	**Nu se acceptă.** În nota de fundamentare a proiectului de act normativ sunt date informații suficiente pentru a putea determina impactul financiar asupra furnizorilor de servicii, inclusiv celor din sectorul energetic. Astfel, potrivit Raportului de evaluare a impactului la propunerea de Directivă a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în întreaga Uniune, de abrogare a Directivei (UE) 2016/1148 (Directiva NIS2): „Pe baza previziunilor periodice ale Gartner din 2012 până în 2020 privind procentajul cheltuielilor globale cu securitatea TIC din cheltuielile TIC și din veniturile totale, precum și ținând seama de cele mai recente date sectoriale ale Gartner disponibile Comisiei, în scopul evaluării impactului s-a presupus că media cheltuielilor pentru securitatea TIC pe sector în 2020 este de aproximativ 9,14% din cheltuielile totale TIC. În funcție de nivelul de maturitate și de capacitățile de securitate cibernetică ale sectorului, precum și de nivelul de digitalizare, această medie ar putea fi ajustată cu +/-3%. În plus, cheltuielile medii TIC pe sector sunt estimate la aproximativ 5,69% din cifra de afaceri totală și, prin urmare, cheltuielile medii cu securitatea TIC din cifra de afaceri totală pe sector în 2020 sunt estimate la aprox. 0.52%.”.

26.	**Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informație** *(Nr. 01-DRA/331 din 17.02.2025)*		Lipsa de propuneri și obiecții.	
27.	**Agenția Națională Transport Auto** *(Nr. 10/1-1-1036 din 26.02.2025)*		Lipsa propunerilor și obiecțiilor.	
28.	**Agenția Navală a Republicii Moldova** *(Nr. 03-72 din 17.02.2025)*	**106.**	Punctul 2 din PHG stabilește că furnizorii de servicii vor asigura implementarea măsurilor de gestionare a riscurilor „în funcție de rezultatele evaluării riscurilor, de nivelul caracterului critic al activelor și capacitățile financiare ale furnizorului de servicii". Această formulare ridică întrebarea dacă furnizorii care nu dispun de resurse financiare suficiente vor fi exceptați, în practică, de la obligația de a implementa aceste măsuri. Lipsa unei clarificări explicite poate duce la aplicări neuniforme, iar unele entități ar putea să nu își poată îndeplini obligațiile din motive financiare. Considerăm necesară o precizare clară privind măsurile alternative disponibile sau posibilitatea unui sprijin în astfel de situații, pentru a asigura un nivel minim de conformitate în toate sectoarele vizate.	**Se acceptă.** Partea dispozitivă a fost completată cu reglementări care precizează modul de punere în aplicare a cerințelor privind măsurile de gestionare a riscurilor.
		107.	Cu referire la punctul 26 al proiectului Regulamentului, având în vedere că furnizorul de servicii asociat Serviciilor de Trafic Maritim (STM) se află în responsabilitatea exclusivă a ANRM, dorim să înțelegem modul în care obligațiile privind raportarea incidentelor cibernetice se aplică în acest context. Aceasta, deoarece PHG prevede că furnizorii de servicii trebuie să	**Precizare.** Punctul 26 din anexa la proiectul Regulamentului stabilește obligația furnizorului de servicii, inclusiv a celor care sunt persoane juridice de drept public, să instituie mecanisme de raportare a evenimentelor suspecte. Această

			instituie un mecanism simplu pentru raportarea evenimentelor suspecte și să îl comunice furnizorilor și clienților, „dacă este adecvat”. Totuși, nu este clar dacă există deja mecanisme standardizate care pot fi utilizate sau dacă fiecare furnizor va trebui să dezvolte un sistem propriu. În acest sens, considerăm că aceste mecanisme ar trebui uniformizate pentru a asigura o aplicare coerentă a prevederilor. În ceea ce privește expresia „dacă este adecvat” utilizată în punctul 27, este necesar să se precizeze criteriile pe baza cărora se stabilește această *adecvare*.	obligație se înscrie într-un proces mai larg de gestionare a incidentelor. Potrivit pct. 16 furnizorul de servicii, în cazul dat ANRM, urmează să adopte și să pună în aplicare o procedură de gestionare a incidentelor cibernetice. Cele care nu au impact semnificativ urmează a fi raportate în mod obligatoriu către CERT-Gov, iar cele care au sau ar putea avea un impact semnificativ – către ASC care exercită funcția de CERT-MD sau CSIRT național. În acest proces, etapa de raportare a evenimentelor suspecte este un instrument util pentru furnizorul de servicii în procesul de monitorizare a rețelelor și sistemelor informatice proprii sau celor care stau la baza prestării serviciilor esențiale. Referindu-ne la speța în cauză, menționăm că ANRM va trebui să integreze în procedurile sale de raportare a evenimentelor suspecte și procesele și mecanismele de raportare a evenimentelor suspecte ce țin de activitățile de prestare a serviciilor de trafic maritim. În ceea ce privește expresia „dacă este adecvat” de la punctul 27 din anexa la proiectul Regulamentului, aceasta urmează a fi înțeleasă și interpretată în coroborare cu prevederile punctelor 6-8 din proiectul Regulamentului, care reglementează aspecte ce țin de aplicarea principiului proporționalității măsurilor de securitate cu riscurile identificate la adresa rețelelor și sistemelor informatice ale furnizorilor de servicii.

		108.	PHG prevede că măsurile de securitate vor fi implementate pe o perioadă de trei ani, însă nu este clar dacă există deja un plan detaliat al etapelor de aplicare sau dacă acesta urmează să fie elaborat. Având în vedere caracterul specific al PHG și expertiza necesară pentru implementarea măsurilor prevăzute, ar fi util să înțelegem dacă furnizorii de servicii vor avea la dispoziție un ghid clar sau un set de etape structurate care să faciliteze aplicarea acestor cerințe. Nu toți furnizorii de servicii dispun de capacități și expertiză tehnică pentru a transpune direct prevederile PHG în practică, motiv pentru care un plan etapizat ar putea contribui la o implementare coerentă și eficientă.	**Precizare.** Punctul 5 din proiectul de Regulament stabilește în sarcina Agenției pentru Securitate Cibernetică aprobarea ghidurilor și orientărilor metodologice pentru punerea în aplicare a acestor cerințe și acordare suportului necesar furnizorilor de servicii în acest proces pe cazuri și situații specifice.
		109.	Secțiunea 3 al Capitolului 2 din Anexa la proiectul Regulamentului stabilește că furnizorii de servicii trebuie să examineze în mod independent gestionarea securității rețelelor și sistemelor informatice, inclusiv procesele, persoanele și tehnologiile utilizate (punctul 12). De asemenea, punctul 13 prevede că aceste examinări trebuie realizate de persoane care dețin certificări corespunzătoare în domeniul auditului securității informațiilor, menționând ca exemplu standarde internaționale precum ISO/IEC 27001. Totuși, nu este clar dacă există criterii specifice pentru recunoașterea acestor certificări sau dacă fiecare furnizor poate decide ce standarde aplică, atâta timp cât sunt „similare”. De asemenea, nu este specificat dacă va exista un mecanism prin care o autoritate competentă poate verifica validitatea certificărilor utilizate. În plus, punctul 13 stabilește că, dacă examinarea independentă este realizată de personalul propriu al furnizorului de servicii, aceștia *nu trebuie să fie în linia ierarhică a personalului din domeniul examinat*. În situațiile în care dimensiunea furnizorului nu permite această separare, furnizorul trebuie să instituie măsuri alternative pentru a garanta imparțialitatea examinărilor. Nu este clar însă ce tipuri de măsuri alternative	**Precizare**. Condițiile esențiale pentru aceste examinări independente ale conformității sunt următoarele: a) entitatea care evaluează este competentă și b) este asigurată imparțialitatea evaluării. În ce privește prima condiție, furnizorul de servicii trebuie să se asigure că persoana care efectuează examinarea dispune de cunoștințele tehnice de securitate cibernetică, de exemplu, cadrele de securitate cibernetică (ISO/IEC 27001, NIST etc.), are cunoștințe în domeniul sectorului critic; dispune de competențe de evaluare a riscurilor, cunoaște reglementările, de exemplu NIS2, GDPR, DORA etc. și înțelege bune practici în domeniul auditului. În ce privește cea de-a doua condiție, pentru ca să asigure imparțialitate evaluării conformității, este necesar să fie aprobat și implementat un proces clar al evaluării care să includă, fără însă a se limita la acestea: scopul și obiectul

			sunt considerate acceptabile și dacă acestea vor necesita aprobarea unei autorități competente.	examinării, metodologia aplicată, frecvența evaluării, anumite modele de evaluare, etc., având în vedere că asigurarea independenței este esențială, furnizorul de servicii trebuie să determine cine va efectua evaluarea (cineva din interior sau din exterior). Atunci când dimensiunea întreprinderii nu o permite furnizorul de servicii ar trebui să aplice măsuri alternative cum ar fi spre exemplu: rotația personalului, înființarea unei comisii sau grup de lucru de evaluare cu membri din diferite departamente; apelarea la un prestator extern de servicii evaluare a conformității (o parte terță). În ce privește „*mecanismele de verificare a validității certificărilor”*, menționăm că în funcție de sistemul de certificare urmează a fi utilizate mecanismele de verificare oferite de entități care efectuează certificarea, disponibile public inclusiv, pe paginile web ale acestora.
		110.	Urmează a fi ajustate erorile de natură redacțională, cum ar fi eliminarea expresiei „cel puțin” de la litera a) a punctului 12 din proiectul Regulamentului, unde apare superfluu.	**Se acceptă.**
29.	**Autoritatea Aeronautică Civilă** *(Nr. 268 din 07.02.2025)*		Lipsa de obiecţii şi propuneri.	
30.	**Agenția de Mediu** *(Nr. 08/1825/2025 din 05.02.2025)*		Lipsa de obiecții și propuneri.	
31.	**Agenția Națională de**		Lipsa de obiecţii şi propuneri.	

	Reglementare a Activităților Nucleare și Radiologice *(Nr. 18-69-1113 din 03.02.2025)*			
32.	**Agenția Proprietății Publice** *(Nr. 05-04-780 din 05.02.2025)*		Lipsa obiecțiilor. Totodată, reieșind din faptul că proiectul a fost expediat spre avizare și întreprinderilor de stat „Calea Ferată din Moldova” și „Administrația de Stat a Drumurilor”, considerăm oportun să se țină cont de propunerile acestora la definitivarea proiectului.	
33.	**ÎS „Administrația de Stat al Drumurilor”** *(Nr. 06/01-01/736 din 12.02.2025)*	**111.**	Lipsa obiecțiilor şi propunerilor.	
34.	**ÎS „Calea Ferată din Moldova”** *(Nr. H-4/413 din 25.02.2025)*		Informează că susține în general acest proiect. Analizând proiectul prezentat în conexiune cu prevederile Codului transportului feroviar, Î.S. „Calea Ferată din Moldova” avizează pozitiv proiectul de hotărâre a Guvernului „Cu privire la modul de implementare a măsurilor de securitate a rețelelor și sistemelor informatice de către furnizorii de servicii în sectoarele critice” cu număr unic 49/MDED/2025.	
35.	**Comisia Națională a Pieței Financiare** *(Nr. 06-4/720 din 19.02.2025)*		Lipsa de obiecţii şi propuneri.	
36.	**Biroul Național de Statistică**		Lipsa de obiecții şi propuneri.	

	(Nr. 24-01/02 din 18.02.2025)			
37.	**Banca Națională a Moldovei** *(Nr. 31-002/35/1217 din 05.03.2025)*	**112.**	Observăm că în proiectul Regulamentului privind modul de aplicare a măsurilor de securitate a rețelelor și sistemelor informatice de către furnizorii de servicii în sectoarele critice (capitolul II) autorul reglementează criteriile de stabilire a echivalenței între prevederile legilor care reglementează activitatea furnizorilor de servicii și cele ale Legii nr. 48/2023 privind securitatea cibernetică. În acest sens, sesizăm că Legea nr. 48/2023 nu pare să abiliteze Guvernul cu competențe de stabilire a unor astfel de criterii în cadrul normativ subsecvent Legii nr. 48/2023. Opinăm, că modul și criteriile de evaluare a echivalenței efectelor obligațiilor de asigurare a securității cibernetice și de determinare a legii aplicabile urmează a fi detaliate în Legea nr. 48/2023, care la art. 3 alin. (5) stabilește cerința de echivalență a efectelor obligațiilor legale, fără însă a reglementa modul și criteriile de evaluare a întrunirii acestei cerințe.	**Precizare.** Prevederile proiectului de Regulament nu instituie norme care depășesc limitele stabilite de art. 3 alin. (5) din Legea nr. 48/2023. Acestea doar detaliază normele primare deja stabilite și vin cu clarificările necesare privind aplicarea dispozițiilor legale respective, clarificări necesare, în primul rând ASC, dar și furnizorilor de servicii din perspectiva garanțiilor, certitudinii și predictibilității reglementărilor primare. Totodată, reiterăm că aceste reglementări decurg din Comunicarea Comisiei Orientările Comisiei privind aplicarea articolului 4 alineatele (1) și (2) din Directiva (UE) 2022/2555 (Directiva NIS 2)[2].
		113.	Având în vedere prevederile art. 3 alin. (7) din Legea nr. 48/2023, înțelegem că evaluarea echivalenței obligațiilor de asigurare a securității cibernetice, prevăzute în legile care reglementează activitatea furnizorilor de servicii, în raport cu cele stabilite în Legea nr. 48/2023, se efectuează la etapa de identificare a furnizorilor de servicii. În acest sens, considerăm necesar a se ține cont de faptul, că legislația care reglementează sectorul bancar prevede cerințe privind măsurile de securitate și de notificare a incidentelor cibernetice cu impact semnificativ, care sunt echivalente cu obligațiile stabilite de Legea nr. 48/2023. Astfel, menționăm că reglementările primare privind gestionarea riscurilor în materie de securitate cibernetică se	**Precizare.** Într-adevăr, în procesul de identificare la etapa deciziei includerii în Lista furnizorilor de servicii în sectoarele critice, ASC va trebui să determine și legislația aplicabilă furnizorului de servicii pentru determinarea cerințelor de securitate cibernetică aplicabile. În principiu, tocmai din considerentele existenței unor astfel de reglementări sectoriale specifice, descrise destul de desfășurat pentru sectorul bancar de autorul obiecției, și sunt necesare clarificările de rigoare într-un act subordonat legii.

[2] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52023XC0918(01)

			regăsesc în Legea nr. 202/2017 privind activitatea băncilor și Legea nr. 114/2012 cu privire la serviciile de plată și moneda electronică. În acest context, constatăm, că Legea nr. 202/2017 conține, la art. 382, prevederi detaliate cu privire la asigurarea securității cibernetice de către bănci (băncile trebuie să dispună de un cadru de administrare a riscurilor aferente tehnologiei informației și comunicațiilor (TIC) și securității informației care să conțină procese și proceduri pentru a asigura identificarea, analizarea, evaluarea, diminuarea, monitorizarea, raportarea și menținerea riscurilor în limitele toleranței la risc; să instituie un cadru de administrare a continuității activității, în măsură să asigure capacitatea de funcționare în mod continuu, cu asigurarea protejării tuturor informațiilor; să stabilească procese de revizuire a riscurilor, procese de testare a securității informației și continuității activității care să valideze eficacitatea măsurilor de control și aplicabilitatea planurilor de asigurare a continuității activității etc.). La fel, Legea nr. 114/2012 reglementează, la art. 321 și art. 322, modul de gestionare a riscurilor operaționale și de securitate de către prestatorii de servicii de plată, inclusiv de către bănci, precum și obligația de raportare la BNM a incidentelor care au generat disfuncționalități la nivelul funcțiilor semnificative, au afectat integritatea, confidențialitatea, autenticitatea informațiilor, continuitatea serviciilor - cel târziu în următoarea zi lucrătoare după producerea incidentului. În continuare, menționăm, că reglementările secundare aferente gestionării riscurilor în materie de securitate cibernetică de către sectorul bancar se regăsesc în Regulamentul privind cerințele minime pentru gestionarea riscurilor aferente TIC, securității informației și continuității activității, aprobat recent de Banca Națională a Moldovei (Hotărârea Comitetului Executiv nr. 29 din 12.02.2025). Remarcăm în acest sens, că prevederile acestui regulament aliniază cerințele prevăzute în	De altfel, sectorul financiar bancar este unicul care, pe dimensiunea evaluării echivalenței efectelor și a aplicabilității cerințelor de securitate este expres menționat în apendicele la orientările Comisiei. Cu toate acestea, această evaluare urmează a fi efectuată într-un cadru definit normativ și de către o autoritate împuternicită corespunzător.

			reglementările BNM la standardele internaționale în domeniu (spre exemplu: Standardul ISO/IEC 27001 „Securitatea informațională, securitatea cibernetică și protecția confidențialității. Sisteme de management al securității informației”; Standardul ISO/IEC 27002 „Securitatea informației, securitatea cibernetică și protecția vieții private”) precum și transpune parțial prevederile Ghidului EBA/GL/2019/04 privind administrarea riscurilor tehnologiei informației și comunicațiilor și de securitate și a Regulamentului UE nr. 2022/2554 privind reziliența operațională digitală a sectorului financiar. În același context, menționăm că, prin Regulamentul nr. 29/2025, BNM a prescris băncilor implementarea unui șir de măsuri în vederea gestiunii eficiente a riscurilor TIC (cerințe privind guvernanța, cadrul intern TIC și securitatea informației; cerințe minime privind desfășurarea operațiunilor TIC și gestionarea incidentelor și a proiectelor TIC; cerințe privind dublarea echipamentelor critice și a elementelor principale din cadrul infrastructurii; cerințe privind efectuarea anuală a testărilor de securitate și testărilor de disponibilitate și continuitatea pentru sistemele/serviciile TIC critice; cerințe privind informarea BNM la finele fiecărui an privind incidentele produse pe parcursul anului etc.). Totodată, precizăm că, în cazul băncilor, Regulamentul nr. 29/2025 detaliază unele cerințe referitoare la riscurile TIC prevăzute în Regulamentul nr. 322/2018 privind cadrul de administrare a activității băncilor. În temeiul legislației menționate supra, BNM evaluează cadrul intern aferent TIC în fiecare bancă, în raport cu natura, amploarea și complexitatea riscurilor inerente modelului de afaceri și activităților desfășurate de bancă și cu profilul/apetitul de risc în cadrul controalelor desfășurate la bancă și poate aplica măsuri de supraveghere și sancțiuni în cazul identificării riscurilor sau încălcărilor în acest domeniu.	

			În această ordine de idei, semnalăm că unele competențe de reglementare, supraveghere și control ale Agenția de Securitate Cibernetică (prevăzute în Legea nr. 48/2023), în raport cu băncile, s-ar putea suprapune cu competențele BNM. Mai mult, opinăm că o astfel de suprapunere de competențe ar putea crea impedimente procesului de supraveghere efectuat atât de BNM, cât și de către Agenția de Securitate Cibernetică. Astfel, menționăm că monitorizarea și supravegherea respectării atât a prevederilor primare, cât și a celor secundare de către sectorul bancar este apanajul exclusiv al BNM. Totodată, ținând cont de obiectivul comun de asigurare a unui cadru național uniform și robust de asigurare a securității cibernetice, precum și în vederea asigurării capacității Agenției de Securitate Cibernetică de a accesa informațiile necesare pentru realizarea atribuțiilor acesteia, reiterăm propunerea de creare a unui mecanism fiabil de coordonare a eforturilor în procesul de asigurare a respectării prevederilor Legii nr. 48/2023 și a cadrului normativ subsecvent acestei legi. Mecanismul respectiv urmează să asigure schimbul de informații dintre BNM și Agenția de Securitate Cibernetică, evitarea suprapunerii de competențe dintre aceste două autorități și, intruziunile reciproce nejustificate. Manifestăm în acest sens disponibilitate pentru conlucrare în vederea atingerii acestui obiectiv comun. Cu referire la asigurarea securității cibernetice de către BNM, menționăm, că întru aplicarea prevederilor art. 74 din Legea nr. 548/1995 cu privire la Banca Națională a Moldovei, intitulat „standarde privind gestionarea adecvată”, cadrul de reglementare al BNM, inclusiv privind asigurarea securității cibernetice (politica de securitate, standardele de securitate, cerințe de securitate, instrucțiunile și proceduri interne aferente protecției securității cibernetice) este elaborat având la bază Standardul ISO/IEC 27001 „Securitatea informațională,	

			securitatea cibernetică şi protecția confidențialității. Sisteme de management al securității informației", Standardul ISO/IEC 27002 „Securitatea informației, securitatea cibernetică și protecția vieții private", Standardele Institutului Național de Standarde și Tehnologii, precum și alte standarde relevante domeniilor reglementate (gestiunea riscurilor, gestiunea incidentelor, managementul vulnerabilităților, continuitatea activității, etc.). Astfel, cadrul robust de reglementare al BNM instituie un regim de securitate cibernetică cel puțin echivalent cu cel stabilit în Legea nr. 48/2023 și actele normative de punere în aplicare a acesteia.	
		114.	Cu referire la conținutul proiectului Hotărârii de Guvern cu privire la modul de implementare a măsurilor de securitate a rețelelor și sistemelor informatice de către furnizorii de servicii în sectoarele critice, observăm că prin această hotărâre nu se aprobă și standardele naţionale în domeniul securităţii informaţiei şi al securităţii cibernetice, așa cum prevede art. 11 alin. (4) lit. a) din Legea nr. 48/2023 (prevăzut de autor ca temei legal pentru elaborare acestei hotărâri). Constatăm în acest sens, că art. 11 alin. (4) lit. a) din Legea nr. 48/2023 prevede că „Guvernul prin intermediul organismului naţional de standardizare, asigură aprobarea standardelor naţionale în domeniul securităţii informaţiei şi al securităţii cibernetice în baza standardelor şi a specificaţiilor tehnice europene şi celor internaţionale relevante pentru securitatea reţelelor şi a sistemelor informatice". Astfel, înțelegem că aceste standarde vor fi aprobate ulterior de către Institutul de Standardizare din Moldova conform prevederilor Legii nr. 20/2016 cu privire la standardizarea națională (spre exemplu, art. 11, 12 etc.). În acest context, în clauza de adoptare a proiectului Hotărârii de Guvern propunem revizuirea trimiterii la art. 11 alin. (4) lit. a) din Legea nr. 48/2023 ca temei de adoptare a acestei hotărâri. Suplimentar, atenționăm, că în conformitate cu art. 14 alin. (1)	**Se acceptă**. Clauza de adoptare a proiectului a fost revizuită corespunzător.

			din Legea nr. 20/2016, aplicarea standardelor moldovenești are caracter voluntar, totodată, alin. (2) din același articol prevede expres că: „Aplicarea unui standard moldovenesc poate deveni obligatorie, în totalitate sau în parte, pe întreg teritoriul ţării sau pe plan local, numai printr-un act normativ în care se face referinţă directă la acest standard, în cazul în care considerentele de ordin public, de protecţie a vieţii, a sănătăţii şi a securităţii oamenilor, a mediului şi a intereselor consumatorilor fac necesară o astfel de măsură”. Suplimentar celor menționate în prezentul aviz, reiterăm susținerea pentru eforturile consolidate ale autorităților în fortificarea cadrului legal privind securitatea cibernetică și suntem disponibili pentru a discuta în comun potențialele soluții de ordin legislativ și practic în vederea atingerii acestui obiectiv.	
38.	**Centrul Naţional pentru Protecţia Datelor cu Caracter Personal** *(Nr. 04-01/442 din 14.02.2025)*		Lipsa obiecțiilor.	
39.	**Asociația Națională a Companiilor din Domeniul TIC** *(Nr. 109/2025-LA din 18.02.2025)*	**115.**	Prin prezenta, Asociația Națională a Companiilor din Domeniul TIC salută eforturile depuse de MDED pentru elaborarea și promovarea proiectului hotărârii de Guvern „Cu privire la modul de implementare a măsurilor de securitate a rețelelor și sistemelor informatice de către furnizorii de servicii în sectoarele critice” (număr unic 49/MDED/2025), elaborat în conformitate cu art. 11 alin. (4) lit. b) din Legea nr. 48/2023 privind securitatea cibernetică. Prin urmare, ATIC vine să contribuie cu câteva observații esențiale pentru îmbunătățirea cadrului legislativ menționat supra.	**Nu se acceptă.**

			Conform pct. 20. lit. a) din Regulamentul cu privire la modul de aplicare a măsurilor de securitate a rețelelor și sistemelor informatice de către furnizorii de servicii în sectoarele critice, un incident cibernetic urmează a fi considerat ca având impact semnificativ și atunci când un serviciu de cloud computing furnizat este indisponibil timp de peste 30 de minute. **Propunem modificarea termenului de la 30 minute la 60 minute din următoarele considerente**: În multe state membre ale Uniunii Europene, un incident cibernetic este considerat a avea un impact semnificativ dacă un serviciu de cloud computing devine indisponibil pentru o perioadă de 60 de minute sau mai mult. Acest prag temporal este stabilit la nivel național, deoarece Directiva (UE) 2022/2555 (Directiva NIS 2) nu specifică un interval de timp exact pentru a defini impactul semnificativ al unui incident cibernetic. În schimb, directiva încurajează statele membre să stabilească propriile criterii și praguri, adaptate contextului și nevoilor locale. Astfel, unele state au optat pentru pragul de 60 de minute, considerând că o astfel de durată de indisponibilitate poate provoca perturbări semnificative în funcționarea serviciilor esențiale și poate afecta negativ utilizatorii și economia. De asemenea, SLA (Service Level Agreement) care este un Acord de Nivel de Serviciu între un furnizor și un client și care definește standardele de performanță și disponibilitate ale unui serviciu, procentul de 99,99% pentru un serviciu de cloud computing înseamnă că acesta poate fi indisponibil pentru aproximativ 4,38 minute pe săptămână sau 52,6 minute pe lună. Dacă să analizăm SLA pentru top operatori de cloud internationali, identificăm o perioadă de 52,6 minute per lună.	În primul rând, ținem să precizăm că disponibilitatea unui serviciu, ca o condiție inerentă unei stări normale de securitate și reziliență, este vizată nu doar de criteriul menționat la subpunctul 28.1 (în redacția inițială 20.1) ci și la subpunctele 23.2 și 23.3. Argumentarea autorului obiecției se înscrie plenar în și este acoperită din punct de vedere normativ de condiția prevăzută de subpunctul 28.2 (20.2 în redacția anterioară) care se referă la indisponibilitatea parțială a serviciului pentru o durată ce depășește 60 de minute (o oră) și nu de condiția stabilite la subpunctul 28.1. În al doilea rând, disponibilitatea de 99,99%, la care face referire autorul obiecției, care de regulă se stabilește în SLA-uri, include nu doar indisponibilitatea cauzată de acte malițioase, ci și perioadele de indisponibilitate datorate mentenanței sau altor acțiuni care nu pot fi în mod specific calificate ca incidente cibernetice în sensul Legii nr. 48/2023 (vezi definiția incidentului cibernetic de la art. 2 al legii menționate). De asemenea, perioada de indisponibilitate din SLA-uri este calculată sumativ pe când condiția în speță prevăzută la subpunctul 28.1 din proiectul Regulamentului urmează a fi interpretată ca o indisponibilitate continuă de cel puțin 30 de minute. Un alt aspect care e necesar de relevat este faptul că această condiție are ca obiectiv armonizarea legislației naționale la prevederile articolului 7 litera (a) din Regulamentul de punere în aplicare (UE) 2024/2690 al Comisiei

			Google Cloud https://cloud.google.com/compute/sla - Monthly Uptime Percentage = 99.99% AWS https://aws.amazon.com/compute/sla/ - Monthly Uptime Percentage of at least 99.99% Microsoft https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services?lang=1 - 99.99% Prin urmare, stabilirea pragului de 60 de minute pentru clasificarea unui incident cibernetic ca având impact semnificativ, în loc de 30 de minute, are la bază următoarele argumente: • Alinierea la standardele SLA utilizate în industrie. Majoritatea furnizorilor de servicii critice, inclusiv cei de cloud computing, operează cu acorduri de nivel de serviciu (SLA) de 99,99% disponibilitate, ceea ce corespunde unei indisponibilități lunare de aproximativ 52 de minute. Un prag de 60 de minute este o extensie logică și realistă a acestei limite, evitând clasificarea incidentelor minore ca fiind semnificative. • Reducerea alarmelor false și a raportărilor inutile. Stabilirea unui prag de 30 de minute ar putea duce la numeroase raportări pentru incidente care nu au un impact real asupra utilizatorilor sau operațiunilor. Aceasta ar putea supraîncărca autoritățile responsabile și ar diminua eficiența răspunsului la incidente cu adevărat critice. • Practici internaționale și armonizarea cu alte state. Unele state membre ale UE au adoptat deja un prag de 60 de minute pentru a defini impactul semnificativ al unui incident cibernetic. O astfel de armonizare ar permite aplicarea unor reguli uniforme în cadrul pieței digitale europene, facilitând conformitatea pentru furnizorii de servicii transnaționali.	din 17 octombrie 2024 de stabilire a normelor de aplicare a Directivei (UE) 2022/2555.

			• Reducerea impactului economic asupra furnizorilor de servicii. Clasificarea incidentelor de scurtă durată ca fiind „semnificative” ar impune cerințe suplimentare de raportare și măsuri de remediere costisitoare, fără un beneficiu clar pentru securitatea generală. Pragul de 60 de minute permite o mai bună echilibrare între securitate și sustenabilitatea economică. În concluzie, adoptarea pragului de 60 de minute în loc de 30 de minute este justificată prin standardele din industrie, eficiența raportărilor, impactul real asupra utilizatorilor și armonizarea cu alte state membre. Vă mulțumim anticipat pentru atenția acordată acestei propuneri	
40.	**Moldtelecom** *(Nr. 01-10/1529 din 25.02.2025)*	**116.**	În cadrul ședințelor de consultare, SA “Moldtelecom” a transmis sugestii privind implementarea măsurilor de securitate cibernetică, reflectând preocupările furnizorilor de servicii din sectoarele critice. Proiectul de hotărâre aduce beneficii semnificative pentru securitatea națională, aliniindu-se la standardele internaționale și conslidând protecția infrastructurilor critice împotriva atacurilor cibernetice. Prin responsabilizarea furnizorilor de servicii și impunerea unor cerințe stricte de gestionare a riscurilor, proiectul contribuie la creșterea încrederii în serviciile digitale și la stabilitatea operațională. Cu toate acestea, implementarea sa poate aduce mai multe provocări, și anume pe segmentul cerințelor de monitorizare și jurnalizare detaliată prevăzute în documentul analizat, unde se impune furnizorilor de servicii din sectoarele critice să colecteze și să stocheze cantități semnificative de date despre activitățile desfășurate în rețelele și sistemele lor informatice. Această practică poate avea mai multe implicații asupra confidențialității datelor utilizatorilor, după cum urmează:	

			1. Volumul și natura datelor colectate: Regulamentul specifică păstrarea detaliată a jurnalelor, inclusiv: traficul de rețea la intrare și ieșire, accesul la sisteme și aplicații, accesul fizic la instalații și echipamente de rețea ș.a. Aceste informații pot conține date sensibile despre utilizatori, cum ar fi adrese IP, locații geografice, date de autentificare, tipare de comportament online și alte date personale.	**Precizare.** Categoriile de informații și date care urmează a fi stocate în procesul jurnalizării activităților referitoare la anumite active urmează a fi supuse acelorași cerințe de securitate ca și activele (datele și informațiile) utilizate în procesul prestării serviciilor esențiale de către furnizorul de servicii.
		117.	Riscuri de supraveghere excesivă: Monitorizarea continuă și detaliată a activităților utilizatorilor ar putea duce la o formă de supraveghere excesivă, ridicând întrebări legate de proporționalitatea și necesitatea colectării unor astfel de date. În special, există riscul ca monitorizarea extinsă să afecteze dreptul la viață privată al utilizatorilor, contravenind principiilor de minimizare a datelor prevăzute de Regulamentul General privind Protecția Datelor (GDPR).	**Nu se acceptă.** Nu este clară fundamentarea unei astfel de obiecții, atâta timp cât proiectul stabilește jurnalizarea doar a anumitor informații strict necesare pentru a detecta evenimentele care ar putea fi considerate incidente cibernetice și pentru a răspunde în consecință în vederea atenuării impactului. Furnizorul de servicii urmează să decidă de sine stătător ce active urmează să fie supuse jurnalizării. La punctul 21 furnizorului de servicii i se o oferă o marjă discreționară, ale cărei limite sunt stabilite de condițiile de aplicare ale principiului proporționalității în implementarea măsurilor de securitate în raport cu riscurile identificate și evaluate.
		118.	Potențial de abuz și utilizare neautorizată a datelor: Jurnalele detaliate stocate pe perioade lungi de timp pot deveni ținte atractive pentru atacatori cibernetici sau pot fi utilizate abuziv de către angajați neautorizați, ceea ce ar putea duce la breșe de securitate și încălcări ale confidențialității.	**Nu se acceptă.** Proiectul de act normativ stabilește și alte cerințe de securitate pe care furnizorul de servicii urmează să le întreprindă pentru a asigura securitatea informațiilor deținute, în particular controlul accesului, securitatea resurselor umane, segmentarea rețelelor, etc. Un astfel de *„potențial de abuz și utilizare neautorizată a datelor”* există și în prezent dacă

				măsurile adecvate de securitate nu sunt implementate.
		119.	Conformitatea cu legislația privind protecția datelor: În contextul legislației europene și naționale privind protecția datelor personale, furnizorii de servicii vor trebui să: - asigure că datele colectate sunt utilizate exclusiv pentru scopurile definite (detecția și răspunsul la incidente cibernetice) și nu în alte scopuri neautorizate. - notifice utilizatorii cu privire la colectarea datelor lor personale, în conformitate cu principiul transparenței. - obțină consimțământul utilizatorilor în anumite cazuri, ceea ce poate crea obstacole operaționale și juridice.	**Se acceptă.** Într-adevăr, furnizorii de servicii vor fi obligați de rând cu cerințele de securitate stabilite de proiectul de act normativ să respecte și cerințele altor acte normative, în particular legislația privind protecția datelor cu caracter personal. În general, obiectivul cerințelor de securitate propuse în proiectul de act normativ urmărește și creșterea nivelului de protecție a datelor cu caracter personal prin ridicarea nivelului de maturitate a furnizorului de servicii și asigurarea rezilienței acestuia, în mod special, din punct de vedere a securității informațiilor.
		120.	Provocări legate de stocarea și securitatea jurnalelor: Regulamentul impune păstrarea jurnalelor pentru cel puțin 12 luni și efectuarea de copii de rezervă. Aceasta poate crea provocări suplimentare, inclusiv: - necesitatea de a implementa măsuri avansate de securitate pentru protejarea acestor date împotriva accesului neautorizat, modificărilor sau pierderii. - riscul ca datele stocate pe termen lung să fie accesate în viitor prin atacuri avansate sau breșe de securitate, afectând astfel confidențialitatea utilizatorilor.	**Precizare.** După cum s-a menționat deja cerințele impun anumite măsuri de securitate pentru însăși datele de jurnalizare pentru a asigura protecția adecvată a acestora și minimizarea riscurilor de securitate, inclusiv a celor invocate de autorul obiecției.
		121.	Recomandări pentru atenuarea impactului: Pentru a minimiza impactul asupra confidențialității datelor utilizatorilor, ar putea fi necesar să se implementeze următoarele soluții: - anonimizarea/sau Pseudonimizarea datelor, pentru a reduce riscul identificării directe a utilizatorilor;	**Se acceptă.** Astfel de măsuri precum controlul accesului și criptarea datelor sunt deja prevăzute în proiectul de act normativ. După cum s-a menționat și mai sus, furnizorul de servicii urmează să asigure inclusiv respectarea și a prevederilor legislației privind protecția datelor cu caracter personal. Astfel,

			- controlul strict al accesului: limitarea accesului la jurnale doar pentru personalul autorizat, prin măsuri tehnice și organizatorice stricte; - criptarea datelor: protejarea datelor stocate prin metode avansate de criptare.	atunci când această legislație o impune datele urmează a fi anonimizate.
		122.	În concluzie, proiectul de hotărâre privind implementarea măsurilor de securitate a rețelelor și sistemelor informatice în Republica Moldova aduce beneficii semnificative pentru securitatea națională, aliniindu-se la standardele internaționale și consolidând protecția infrastructurilor critice împotriva atacurilor cibernetice. Prin responsabilizarea furnizorilor de servicii și impunerea unor cerințe stricte de gestionare a riscurilor, proiectul contribuie la creșterea încrederii în serviciile digitale și la stabilitatea operațională a sectoarelor critice. Cu toate acestea, implementarea sa poate aduce provocări considerabile, inclusiv costuri ridicate pentru conformare, complexitatea administrativă și riscuri pentru confidențialitatea datelor utilizatorilor din cauza cerințelor extinse de monitorizare și jurnalizare, ceea ce va necesita implicarea autorităților în oferirea de sprijin adecvat furnizorilor de servicii pentru conformare eficientă.	**Precizare.** În nota de fundamentare sunt oferite date suficiente privind cheltuielile estimative de conformare a furnizorilor de servicii la cerințele de securitate propuse în proiect. Termenul extins de implementare a acestor cerințe este datorat anume faptului ca furnizorul de servicii să poată planifica și prioritiza cheltuielile legate de implementarea măsurilor de securitate.

REAVIZARE

EXPERTIZARE

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
1.	**Ministerul Justiției** *(Nr. 04/2-5652 din 17.06.2025)*	***La proiectul hotărârii:***		
		1.	În clauza de adoptare, pentru o corectă informare juridică, textul „În scopul executării prevederilor art. 11 și în temeiul art. 12 alin. (9) și al art. 14 alin. (2)” se va substitui cu textul „În temeiul art. 11, art. 12 alin. (9) și art. 14 alin. (2)”. Totodată, izvorul publicării *Legii nr. 48/2023*, după textul „nr. 151-153” se va completa cu textul „art. 225”.	**Se acceptă**
		2.	La pct. 1, atragem atenția că, clauza de armonizare se inserează în cuprinsul proiectului fără numerotare. Prin urmare, proiectul necesită o renumerotare în fond.	**Se acceptă**
		3.	La pct. 3: • la sbp. 3.1 cuvintele „din data intrării în vigoare” se vor substitui cu cuvintele „de la data intrării în vigoare” (observația este valabilă inclusiv pentru sbp. 3.2, 3.3, 4.1-4.4);	**Se acceptă**
			La sbp. 7.1 și 7.2, în redacția propusă a punctului 9^1 din anexa nr. 1 și punctului 10 din anexa nr. 3, cuvintele „urmează a fi reglementat” se vor substitui cu cuvintele „se stabilește”.	**Se acceptă**
		4.	La pct. 8, sintagma „Controlul executării” se va substitui cu sintagma „Controlul asupra executării”.	**Se acceptă**
		La proiectul Regulamentului:		**Se acceptă**
		5.	Întru corectitudinea redactării, parafa de aprobare se va indica după cum urmează: „Aprobat	

			prin hotărârea Guvernului nr. ___/2025”.	
		6.	La pct. 4 cuvintele „în anexa la prezentul Regulament” se vor substitui cu cuvintele „în anexă”, or, potrivit art. 55 alin. (4) din *Legea nr. 100/2017 cu privire la actele normative*, în cazul în care se face trimitere la o normă juridică care este stabilită în același act normativ, pentru evitarea reproducerii acesteia, se face trimitere la elementul structural sau constitutiv respectiv, fără a se indica că elementul respectiv face parte din același act normativ (observația se referă inclusiv la pct. 5, pct. 8 – 10, sbp. 13.1).	**Se acceptă**
		7.	În parafa anexei la regulament textul „ , aprobat prin Hotărârea Guvernului nr._____din ” se va exclude ca fiind excedent.	**Se acceptă**
		8.	Conţinutul proiectului urmează a fi definitivat conform prevederilor art. 54 din *Legea nr. 100/2017 cu privire la actele normative*. Textul punctelor trebuie să aibă un caracter dispozitiv, să prezinte norma instituită fără explicaţii sau justificări. Verbele utilizate în text se vor expune la timpul prezent, forma afirmativă, pentru a se accentua caracterul imperativ al dispoziţiei respective. La utilizarea abrevierilor se va ține cont că, în conformitate cu art. 54 alin. (1) lit. i) al *Legii nr. 100/2017*, exprimarea prin abrevieri a unor denumiri sau termeni se poate face numai după explicarea acestora în text, la prima folosire (a se vedea: „DNS”, „TLD”).	**Se acceptă**
2.	**Centrul Național Anticorupție** *(Nr. 06/2/10487 din 20.06.2025)*	**9.**	Proiectul nu conține factori de risc care să genereze apariția riscurilor de corupție.	

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
1.	**Cancelaria de Stat** *(Nr. din .2025)*		Lipsa de propuneri și obiecții.	
2.	**Aparatul Președintelui Republicii Moldova** *(Nr. 2/2-06-912 din 16.06.2025)*		Comunică lipsa obiecțiilor și susține promovarea proiectului.	
3.	**Ministerul Infrastructurii și Dezvoltării Regionale** *(aviz plasat pe platforma legiferare.gov.md)*		Lipsa de propuneri sau obiecții suplimentare.	
4.	**Ministerul Energiei** *(Nr. 02–1851 din 04 iulie 2025)*		Lipsa obiecțiilor și a propunerilor suplimentare.	
5.	**Ministerul Finanțelor** *(Nr. 07/3-03-106/895 din 17.06.2025)*		Lipsa de obiecții și propuneri.	
6.	**Ministerul Mediului** *(Nr. 12/2-07/1800 din 24.06.2025)*		Lipsa obiecțiilor și propunerilor.	
7.	**Ministerul Sănătății** *(Nr. 27/2110 din 07.07.2025)*		Lipsa obiecțiilor sau propunerilor.	
8.	**Ministerul Agriculturii și Industriei Alimentare** *(Nr. 21-03/1587 din 10.06.2025)*		Lipsa de obiecții.	
9.	**Ministerul Apărării** *(Nr. 11/805 din 20.06.2025)*		Lipsa obiecțiilor.	
10.	**Ministerul Afacerilor Interne** *(Nr. 38/ 1985 din 05.06.2025)*		Lipsa de obiecții și propuneri.	

11.	**Ministerul Afacerilor Externe** *(Nr. DI/3/041.1-5891 din 09.06.2025)*		Lipsa de propuneri sau obiecții suplimentare.	
12.	**Ministerul Educației și Cercetării** *(Nr. 08/4-09/4377 din 19.06.2025)*		Lipsa de obiecții și propuneri.	
13.	**Ministerul Muncii și Protecției Sociale**		Nu a prezentat avizul	
14.	**Ministerul Culturii** *(Nr. 05/4-09/1895 din 25.06.2025)*		Lipsa de obiecţii şi propuneri.	
15.	**Agenția Națională Transport Auto** *(Nr. 2/1-1-3633 din 27.06.2025)*	**10.**	În limita competențelor funcționale, comunică despre susținerea proiectului, cu excepția:	
		11.	**1. Pct. 5 din Regulamentul cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice, anexă la proiectul Hotărîrii de Guvern (în continuare Regulament):** „Agenția elaborează ghiduri de implementare și furnizează, orientări metodologice...” **Obiecție:** Nu este clar regimul juridic al ghidurilor emise de Agenție. În lipsa unei norme legale explicite, acestea riscă să fie tratate ca având caracter obligatoriu de facto, ceea ce ar contraveni art. 5 din Legea nr. 235/2006. **Propunere:** Textul trebuie completat cu precizarea că aceste ghiduri au **doar caracter orientativ**, nefiind norme obligatorii.	**Se acceptă** După cuvintele „ghiduri de implementare” s-a completat cu cuvintele „cu caracter consultativ”.
		12.	**2. Pct. 6 și 7 din Regulament.** Se impune furnizorilor să implementeze măsuri „corespunzătoare și proporționale”, ținând cont de „impactul societal și economic”. **Obiecție:** Noțiunile de „impact societal” și „impact economic” sunt extrem de vagi și greu cuantificabile. În lipsa unor	**Nu se acceptă** Aceste puncte derivă din prevederile art. 21 alineatul al doilea al Directivei NIS2. Terminologia utilizată este una proprie reglementărilor în materie de

			metodologii aprobate, evaluarea acestora va rămâne subiectivă, creând risc de abuz sau aplicare inconsistentă. **Propunere:** Excluderea expresă a acestor noțiuni sau, alternativ, elaborarea de către o autoritate competentă a unei metodologii standard de evaluare, aprobată prin ordin al ministerului de resort.	securitate cibernetică. Unul din criteriile de determinare a proporționalității măsurilor de securitate aplicate în raport cu riscurile identificate este impactul pe care îl pot avea potențialele incidente cibernetice, adică gravitatea acestora. La estimarea acesteia din urmă se ține cont de consecințele și impactul pe care îl pot avea sau îl au asupra economiei și a societății în ansamblu. Spre exemplu, Legea nr. 48/2023 privind securitatea cibernetică stabilește condiții care califică un incident ca fiind semnificativ printre acestea se numără condiții care vizează indisponibilitatea serviciilor sau perturbarea continuității prestării acestuia (art. 12 alin. (5) lit. b) și c). Totodată, menționăm că proiectul transpune prevederile Regulamentului de punere în aplicare (UE) 2024/2690 al Comisiei din 17 octombrie 2024.
		13.	**3. Pct. 8 din Regulament.** Posibilitatea ca un furnizor să declare unilateral că o cerință „nu este adecvată/aplicabilă” și să trimită o simplă motivare documentată. **Obiecție:** Această prevedere lasă loc de abuzuri — se permite evitarea unor cerințe esențiale printr-o autoevaluare subiectivă, fără o validare externă sau un proces de aprobare.	**Nu se acceptă** Stabilirea unei proceduri detaliate de aplicare a principiului proporționalității în cazul implementării fiecărei cerințe de securitate este imposibilă. În fiecare caz concret furnizorul de servicii, ca

			Propunere: Introducerea unei proceduri clare de **aprobare a motivării** de către Agenție, nu doar de notificare.	principal responsabil de reziliența rețelelor și sistemelor sale informatice trebuie să decidă asupra măsurilor de securitate care trebuie aplicate pentru tratarea riscurilor respective. Informarea Agenției are ca obiectiv punerea în vedere unei stări de fapt, care la decizia acesteia, ar putea fi verificată în regim de supraveghere și control de stat, proceduri care adițional la cadrul normativ deja existent, vor fi detaliate într-o hotărâre de Guvern care vor avea ca obiect de reglementare aspectele menționate la art. 18 alin. (3) și art. 19 alin. (5) din Legea nr. 48/2023.
		14.	**4. Pct. 9 din Regulament.** Audit extern obligatoriu „cel puțin o dată la trei ani”. **Obiecție:** Nu se face distincție între dimensiunea furnizorului, complexitatea sistemului și resursele disponibile. Cerința poate fi excesivă pentru entitățile mici, generând costuri disproporționate. **Propunere:** Introducerea unui **prag de scutire** sau a unei opțiuni de autoevaluare pentru IMM-uri, cu confirmare de către ASC.	**Se acceptă** Cuvântul extern a fost exclus.
		15.	**5. Pct. 10 din Regulament.** Exceptarea de la cerințe dacă există certificare ISO/IEC 27001. **Obiecție:** Se creează o dublă măsură și un potențial tratament preferențial. Certificarea ISO nu echivalează neapărat cu conformitatea cu toate cerințele tehnice din regulament. **Propunere:** Introducerea unui mecanism de **validare**	**Se acceptă** Pct. 10 deja stabilește că „Îndeplinirea de către furnizorul de servicii a condițiilor stabilite de prezentul punct nu exclude dreptul Agenției de a efectua o evaluare a conformității acestui furnizor de

			prealabilă de către ASC a documentației aferente ISO, înainte de acordarea exceptării.	servicii cu cerințele prevăzute în anexă la prezentul regulament în exercitarea funcției de supraveghere și control de stat al modului în care sunt respectate prevederile cadrului normativ în domeniul securității cibernetice.”
		16.	**6. Pct. 3.2 și 4.2 din Hotărâre (partea dispozitivă)** Se impune analiza riscurilor și plan de tratare într-un termen de 6/9 luni. **Obiecție:** Pentru furnizori care pornesc de la un nivel minim de maturitate, acest termen este nerealist, mai ales în lipsa ghidurilor și metodologiilor care urmează să fie elaborate. **Propunere:** Extinderea termenului la **12 luni pentru toți**, cu o etapizare clară a obligațiilor: inițial doar analiza de risc, ulterior planuri și măsuri tehnice.	**Nu se acceptă** Evaluarea riscurilor și planul de tratare a acestora sunt activități de inițiere a procesului de implementare a cerințelor de securitate propuse în proiectul de act normativ. Termenul de 6 luni și respectiv 9 luni sunt termene rezonabile de realizare a acestei sarcini, având în vedere că această rezonabilitatea trebuie corelată cu stringența creșterii nivelului de maturitate a furnizorilor de servicii în capacitatea lor de a face față potențialelor amenințări. În cazul furnizorilor esențiali de servicii acest termen este unul mai restrâns din cauza nivelului înalt de criticalitate a sectoarelor în care activează și a serviciilor pe care le prestează.
		17.	**7. Pct. 75 din Anexă la Regulament (Testarea securității).** **Obiecție:** Cerințe privind testele de Securitate sunt stabilite fără specificarea metodologiilor. În lipsa unui cadru standard, fiecare furnizor poate aplica metode arbitrare, afectând calitatea și comparabilitatea rezultatelor.	**Nu se acceptă** Identificarea metodologiei de testare urmează a fi efectuată de către furnizorul de servicii în funcție de tipul său, sectorul în care activează, serviciile care le prestează, activele

			Propunere: Stabilirea unui cadru minimal de testare (de ex. OWASP, PTES, NIST) sau obligativitatea indicării metodei utilizate și justificării acesteia în documentația tehnică.	pe care le utilizează în prestarea acestor servicii, dimensiunea sa. Totodată este necesar de luat în considerare standardele recunoscute în industrie atunci când se elaborează politica de testare. Atunci când stabilesc politicile și procedurile de testare, inclusiv abordarea metodologică, furnizorii de servicii trebuie să ia în considerare standardele recunoscute în industrie. Obligativitatea indicării metodei utilizate și justificării acesteia în documentația tehnică este stabilită expres la pct. 75.2.
16.	**Agenția Navală a Republicii Moldova** *(Nr. 03-252 din 19.06.2025)*		Lipsa obiecțiilor și propunerilor suplimentare față de versiunea actualizată a proiectului de Hotărâre.	
17.	**Autoritatea Aeronautică Civilă** *(Nr. 1483 din 18.06.2025)*		Lipsa de obiecții sau propuneri.	
18.	**Agenția de Mediu** *(Nr. 08/1956/2025 din 05.06.2025)*		Lipsa de obiecții și propuneri.	
19.	**Agenția Națională de Reglementare a Activităților Nucleare și Radiologice** *(Nr. 01-04/401 din 06.06.2025)*		Lipsa de obiecții și propuneri.	
20.		*La Proiectul de Hotărâre,*		

	Agenția pentru Securitate Cibernetică *(Nr. 08-241 din 17.06.2025)*	**18.**	La pct. 3, propunem unificarea formulărilor cu privire la furnizorii de servicii esențiali, în acest sens, *Hotărîrea Guvernului nr. 860/2024 cu privire la identificarea furnizorilor de servicii* prevede noțiunea de „furnizor esențial". Sintagma „inclusiv operatorii obiectivelor de infrastructură critică" necesită exclusă, ori aceștia sunt furnizori de servicii esențiali sau importanți.	**Se acceptă**
		La Anexa la Regulament		
		19.	La pct. 23, propunem următorul conținut „23. Furnizorii de servicii păstrează jurnalele și realizează copii de rezervă ale acestora pentru o perioadă predefinită, dar nu mai mică de 12 luni, și le protejează împotriva accesului neautorizat sau a modificărilor neautorizate." În acest sens, dacă termenul de 12 luni nu va fi acceptat pentru toți furnizorii, atunci propunem impunerea obligației de 6 luni și 12 luni după cum urmează: 1. 6 luni- pentru furnizorii de servicii importanți, 2. 12 luni- pentru furnizorii de servicii esențiali. Menționăm că termenul de 6 luni pentru păstrarea jurnalului este unul prea mic, iar diferențele de cost pentru o perioadă suplimentară de 6 luni nu sunt esențiale.	**Se acceptă**
21.	**Serviciul de Informații și Securitate** *(Nr. IE/6126 din 18.06.2025)*	**20.**	1. Prin avizul nr. IE/1459 DIN 18.02.2025, Serviciul a obiectat la punctul 6 al textului proiectului hotărârii de Guvern, prin care se abrogă Cerințele minime obligatorii de securitate cibernetică *(Hotărârea Guvernului nr. 201/2017)*, cerințe obligatorii pentru Cancelaria de Stat, Ministere, entități subordonate Guvernului și structurile organizaționale din sfera lor de competență. Astfel, pentru a nu crea un vid normativ, și pentru a asigura continuitatea aplicării măsurilor de securitate cibernetică în entitățile publice, la punctul 3 al proiectul hotărârii de Guvern, Serviciul a propus adăugarea cuvintelor „*și persoanele juridice de drept public"*, după sintagma *„Furnizorii esențiali de servicii"*.	**Nu se acceptă** **Precizare** Proiectul prevede odată cu abrogarea hotărârii Guvernului nr.201/2017 - intrarea în vigoare a noilor Cerințe privind măsurile de securitate a rețelelor și sistemelor informatice ale furnizorilor de servicii în sectoarele critice (Anexă la proiectul Regulamentului cu privire la modul de aplicare de către furnizorii de servicii a măsurilor de securitate a rețelelor și sistemelor informatice).

			Argumentarea autorului de a nu accepta propunerea Serviciului, este noțiunea *„furnizori de servicii” care cuprinde și persoanele juridice de drept public. Potrivit art. 2 din Legea nr. 48/2023, furnizor de servicii – persoană juridică de drept public sau de drept privat, înregistrată în Republica Moldova, care prestează servicii în unul sau mai multe sectoare și/sau subsectoare critice, stabilite de către Guvern, și care este identificată de autoritatea competentă în conformitate cu prevederile prezentei legi și ale actelor normative pentru punerea acesteia în aplicare.* *Persoanele juridice de drept public intră în domeniul de aplicare al Legii nr. 48/2023 în temeiul prevederilor art. 3 alin. (2) lit. i) din legea menționată.”* Serviciul consideră că autorul a interpretat eronat prevederile legale, or, pentru a încadra o persoană de drept public în categoria de *„furnizor de servicii”*, initial, este necesară identificarea acesteia de către entitatea competentă. În acest sens, în procesul de identificare a furnizorilor de servicii, există probabilitatea ca aceștia să nu fie identificați din diverse motive, prin urmare, entitatea publică nu va fi obligată să aplice măsurile instituite în proiectul hotărârii de Guvern. Suplimentar, atragem atenția că art. 14 alin (2) din Legea nr. 48/2023 stabilește expres că ***„Măsurile de securitate minime obligatorii pentru persoanele juridice de drept public sunt stabilite de către Guvern”.***	Menționăm că intenția de reglementare nu poate fi condiționată de anumite situații ipotetice la nivel operațional. Pe de altă parte, în ipoteza în care toate persoanele juridice de drept public vor fi identificate în calitate de furnizori de servicii în timp util, și dacă hotărârea Guvernului nr.201/2017 nu va fi abrogată, vom avea situația în care sunt în vigoare două acte normative cu același obiect de reglementare. Suplimentar, propunerea de completare la punctul 2 (fostul punct 3) al proiectul hotărârii de Guvern, cu cuvintele „și persoanele juridice de drept public”, după sintagma „Furnizorii esențiali de servicii” ar contraveni Anexei nr. 2 la Hotărârea Guvernului nr.860/2024, care menționează la pct. 9 că: *persoanele juridice de drept public, cu excepția autorităților administrației publice locale sunt furnizori de servicii Esențiali, iar autoritățile ale administrației publice locale sunt furnizori de servicii Importanți.* Respectiv, Hotărârea Guvernului nr.860/2024 stabilește clar care sunt furnizori de servicii Esențiali și furnizori de servicii Importanți, iar, în dependență de acest fapt ei

				urmează a cădea sub incidența fie a punctului 2 sau 3 din proiectul de Hotărîre.
		21.	2. Potrivit pct. 7.2 din proiectul hotărârii de Guvern, punctul 10 din Anexa nr. 3 a hotărârii Guvernului nr. 860/2024, ar urma să aibă următorul cuprins *„10. Lista constituie informație cu acces limitat. Modul de prelucrare a informației precum și accesul la listă urmează a fi reglementat prin Ordinul Directorului Agenției pentru Securitate Cibernetică.”* Astfel, Serviciul comunică despre faptul că, o asemenea normă ar permite aplicarea unor măsuri de securitate inferioare pentru protecția Listei furnizorilor de servicii. Subsidiar, atragem atenția că, potrivit cadrului normativ în vigoare, Lista respectivă reprezintă informații atribuite la secret de stat, care necesită aplicarea unor măsuri speciale de protecție conform *Regulamentului cu privire la asigurarea regimului secret în cadrul autorităților publice și al altor persoane juridice, aprobat prin hotărârea de Guvern nr 1176/2010*, or, obținerea accesului la Listă a unor persoane care nu au perfectat dreptul de acces la secretul de stat, poate aduce un prejudiciu foarte grav securității naționale. Totodată, conform pct. 28 din hotărârea Guvernului nr. 860/2024, Lista se formează, inclusiv și în baza informațiilor din Nomenclatorul național al infrastructurii critice, furnizate de către Serviciul de Informații și Securitate al Republicii Moldova, care, de asemenea reprezintă informații atribuite la secret de stat. Respectiv, întru elucidarea acestor circumstanțe, Serviciul propune expunerea pct. 10 din Anexa nr. 3 a hotărârii Guvernului nr. 860/2024, în următoarea redacție *„10. Lista constituie informații atribuite la secret de stat. Modul de prelucrare a informației, se va efectua cu respectarea prevederilor Legii nr. 245/2008 cu privire la secretul de stat, iar*	**Se acceptă parțial** Proiectul a fost definitivat în comun cu SIS. S-a stabilit necesitatea inițierii procesului de organizare a regimului secret în cadrul Agenției pentru Securitate Cibernetică. Totodată, reieșind din conținutul datelor Listei furnizorilor de servicii, s-a stabilit de comun acord că nu este oportun ca această Listă să constituie informații atribuite la secret de stat. În același context, proiectul a fost completat cu prevederea privind excluderea la pct. 28 al Anexei nr. 1 la Hotărârea Guvernului nr. 860/2024 cu privire identificarea furnizorilor de servicii, a textului „din Nomenclatorul național al infrastructurii critice,”.

			accesul la listă urmează a fi reglementat prin Ordinul Directorului Agenției pentru Securitate Cibernetică." Suplimentar, Serviciul reiterează despre necesitatea inițierii procesului de organizare a regimului secret, în cadrul Agenției pentru Securitatea Cibernetică.	
22.	**Serviciul Tehnologia Informației și Securitate Cibernetică** *(Nr. 1.4/1037/25 din 20.06.2025)*		**Cu referire la proiectul hotărârii:**	
		22.	1) Se va modifica denumirea hotărârii, în scopul exprimării cu claritate a obiectului reglementării, având în vedere că proiectul modifică și abrogă alte hotărâri ale guvernului.	**Nu se acceptă** Titlul proiectului de act normativ exprimă sintetic obiectul de reglementare al proiectului propus spre avizare conform cerințelor stabilite de cadrul normativ. Prevederile părții dispozitive a proiectului de hotărâre au un caracter conex acestui obiect de reglementare.
		23.	2) În scopul unificării și optimizării procesului de prezentare a rapoartelor de evaluare a riscurilor, din partea furnizorilor, se propune completarea pct. 3.3. cu următorul conținut: „Elaborate în conformitate cu instrucțiunea și modelele aprobate de către Agenția pentru Securitate Cibernetică".	**Nu se acceptă** O astfel de activitate este pusă în sarcina Agenției prin punctul 5 din proiectul Regulamentului.
		24.	3) În scopul expunerii corecte din punct de vedere gramatical a prevederilor din pct. 3, subpct. 3.2. și pct. 4, subpct. 4.2., după cuvintele "în termen" se va completa cu prepoziția "de";	**Se acceptă**
		25.	4) La subpct. 4.4 se va indica entitatea care va efectua raportul evaluării a conformității cu cerințele menționate.	**Nu se acceptă** Acest aspect este reglementat de punctul 9 din proiectul Regulamentului și de capitolul 2 secțiunea 2 și 3 și capitolul 7 din anexa la proiectul de Regulament.
		26.	5) La punctul 5, subpct. 5.1 reiterăm obiecția expusă la prima avizare privind necesitatea de a reformulării acestui, or,	**Nu se acceptă**

			aprobarea normei juridice în redacția actuală, contravine art. 12 alin. (11) din Legea nr. 48/2023, totodată potrivit pct. 5 subpct. 3) din Hotărârea Guvernului nr. 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securităţii cibernetice la nivel guvernamental şi modificarea Hotărârii Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public şi de raţionalizare a administrării sistemelor informaţionale de stat, CERT Gov are atribuțiile de a asigura interacțiunea cu structurile de tip CERT departamentale din cadrul entităților publice, de asemenea, de a coopera cu acestea în cadrul unei platforme guvernamentale de management al incidentelor cibernetice, prin urmare solicităm ca acest subpunct să fie expus în modul următor: *„în termen de 6 luni de la data publicării prezentei hotărâri va stabili care sunt mecanismele, inclusiv mijloacele tehnice care se vor utiliza, pentru a asigura un schimb direct, sistematic şi imediat de informații în contextul realizării de către furnizorii de servicii a obligațiilor de raportare a incidentelor cibernetice cu impact semnificativ”.*	Implementarea mecanismelor respective vizează raportarea doar a incidentelor cibernetice cu impact semnificativ. Invocarea art. 12 alin. (11) de către autorul obiecției nu este justificată în primul rând deoarece către CERT-Gov urmează a fi notificate toate incidentele, iar în al doilea rând exonerarea furnizorilor de servicii din sectorul public de obligația de raportare a incidentelor semnificative (atunci când aceste sunt raportate de către CERT-Gov către CSIRT național) nu limitează dreptul acestora de a notifica și direct CSIRT național în mod voluntar, drept prevăzut la pct. 6^1 din Măsurile necesare pentru asigurarea securității cibernetice la nivel Guvernamental, aprobate prin HG nr.482/2020.
			Cu referire la proiectul Regulamentului:	
		27.	1) La pct. 1 textul „Hotărârea Guvernului nr. 860/2023”, se va substitui cu „Hotărârea Guvernului nr. 860/2024”;	**Se acceptă**
		28.	2) Pct. 2 se va expune în următoarea redacție: „Prezentul Regulament se aplică furnizorilor de servicii în sectoarele critice (în continuare furnizori de servicii) identificați de către Agenția pentru Securitate Cibernetică (în continuare - Agenția) în conformitate cu Hotărârea Guvernului nr. 860/2024 „Cu privire la identificarea furnizorilor de servicii”	**Acceptat**
		29.	3) La pct. 8 textul „cerință a unei măsuri de gestionare a riscurilor în materie de securitate cibernetică” se va reformula având în vedere denumirea Anexei Regulamentului cu privire la	**Se acceptă**

			modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice.	
		30.	4) Se va revizui pct. 10 prin prisma prevederilor Legii nr. 20/2016 cu privire la standardizarea națională, în special art. 15 alin. (5), care prevede că în actele normative pot fi făcute referințe directe numai la standardele moldovenești publicate în limba română.	**Se acceptă**
		31.	5) În capitolul III se folosește impropriu sintagma de „legislația sectorială”, or pct. 1 stabilește că legislația sectorială este Hotărârea Guvernului nr. 860/2024 cu privire la identificarea furnizorilor de servicii. Prin urmare, se denaturează intenția legislatorului expusă în art. 3 alin. (5) din Legea 48/2023 prin care se instituie o normă juridică care reglementează modul de implementare a măsurilor de securitate și îndeplinirea obligațiilor de notificare a incidentelor cibernetice, stabilite de alte legi care reglementează activitatea furnizorilor de servicii, sectoarele și subsectoarele. Astfel, este necesar a se stabili sensul termenului „legislația sectorială” utilizată în prezentul proiect, inclusiv de exclus la pct. 1 textul „(în continuare – legislație sectorială)” pentru a evita confuzia în utilizarea acestor noțiuni.	**Nu se acceptă** Sintagma *legislație sectorială* se referă la textul ***legislație care reglementează activitatea furnizorilor de servicii și/sau sectoarele şi subsectoarele critice stabilite prin Hotărârea Guvernului nr. 860/2023 cu privire la identificarea furnizorilor de servicii***
		32.	6) La pct. 12, subpct. 12.1 se va revedea sintagma „măsurile de gestionare a riscurilor în materie de securitate cibernetică”, or art. 11 alin. (1) –(3) nu se limitează doar la măsurile de gestionare a riscurilor, dar reglementează măsurile de securitate cibernetice, care include gestionarea riscurilor.	**Se acceptă**
		33.	7) În capitolul IV se va adăuga un nou punct cu următorul conținut: „Furnizorii de servicii persoane juridice de drept public, pentru executarea obligațiilor stabilite de art. 12 alin. (11) din Legea nr. 48/2023 prezintă notificările, actualizările și rapoartele finale în modul stabilit de prezentul capitol Centrului guvernamental de răspuns la incidentele cibernetice”.	**Se acceptă** S-a completat cu un punct nou, 21, cu următorul cuprins: 21. Furnizorii de servicii persoane juridice de drept public, pentru executarea obligațiilor stabilite de art. 12 din Legea nr. 48/2023

				prezintă notificările, actualizările și rapoartele finale în modul stabilit de prezentul capitol Centrului guvernamental de răspuns la incidentele cibernetice. Centrul guvernamental de răspuns la incidente cibernetice prezintă notificările, actualizările acestora și rapoartele finale Agenției în termenii stabiliți de cadrului normativ. Furnizorii de servicii persoane juridice de drept public pot notifica Agenția cu privire la incidentele cibernetice semnificative.
23.	**Agenția de Guvernare Electronică** *(Nr. 3007-118 din 17.06.2025)*		Lipsa obiecțiilor și propunerilor.	
24.	**Agenția Servicii Publice** *(Nr. 01/7839 din 17.06.2025)*		Lipsa de obiecții.	
25.	**Agenția Națională pentru Siguranța Alimentelor** *(Nr. 18-3412 din 18.06.2025)*		Lipsa de propuneri și obiecții.	
26.	**Agenția Medicamentului și Dispozitivelor Medicale** *(Nr. Rg02-002748 din 09.06.2025*		Inexistența obiecțiilor sau propunerilor.	
27.	**Agenția Națională pentru Cercetare și Dezvoltare** *(Nr. 195 din 17.06.2025)*		Își exprimă acordul față de conținutul proiectului și nu are obiecții sau propuneri de modificare.	

28.	**Agenția Națională pentru Reglementare în Energetică** *(Nr. 06-01/3348 din 17.06.2025)*	**34.**	La proiectul Regulamentului, reiterăm propunerea privind detalierea impactului financiar al noilor măsuri asupra furnizorilor de servicii energetice și corelarea acestora cu reglementările tarifare existente, în scopul prevenirii unor majorări nejustificate ale costurilor care ar putea afecta consumatorii. Considerăm esențial ca introducerea noilor măsuri de securitate cibernetică să fie însoțită de o analiză clară a implicațiilor financiare pentru operatorii economici din sectorul energetic, având în vedere că aceste costuri pot influența direct tarifele reglementate. În lipsa unei astfel de evaluări și a unei corelări explicite cu cadrul tarifar actual, există riscul transferării nejustificate a costurilor către consumatori. De asemenea, includerea acestor aspecte în documentul de reglementare va contribui șa transparența procesului de implementare, la menținerea echilibrului între securitatea rețelelor și sustenabilitatea financiară a operatorilor.	**Nu se acceptă** În nota de fundamentare a proiectului de act normativ sunt date informații suficiente pentru a putea determina impactul financiar asupra furnizorilor de servicii, inclusiv celor din sectorul energetic. Astfel, potrivit Raportului de evaluare a impactului la propunerea de Directivă a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în întreaga Uniune, de abrogare a Directivei (UE) 2016/1148 (Directiva NIS2): „Pe baza previziunilor periodice ale Gartner din 2012 până în 2020 privind procentajul cheltuielilor globale cu securitatea TIC din cheltuielile TIC și din veniturile totale, precum și ținând seama de cele mai recente date sectoriale ale Gartner disponibile Comisiei, în scopul evaluării impactului s-a presupus că media cheltuielilor pentru securitatea TIC pe sector în 2020 este de aproximativ 9,14% din cheltuielile totale TIC. În funcție de nivelul de maturitate și de capacitățile de securitate cibernetică ale sectorului, precum și de nivelul de digitalizare, această medie ar putea fi ajustată cu +/-3%. În plus, cheltuielile

				medii TIC pe sector sunt estimate la aproximativ 5,69% din cifra de afaceri totală și, prin urmare, cheltuielile medii cu securitatea TIC din cifra de afaceri totală pe sector în 2020 sunt estimate la aprox. 0.52%.„
29.	**Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației** *(Nr. 02-DRA/1219 din 25.06.2025)*		Lipsa de propuneri și obiecții.	
30.	**Agenția Proprietății Publice** *(Nr. 05-04-4289 din 05.06.2025)*		Lipsa obiecțiilor și propunerilor.	
31.	**ÎS „Administrația de Stat al Drumurilor”**		Lipsa obiecțiilor și propunerilor. *(Vezi avizul Agenției Proprietății Publice cu nr. 05-04-4289 din 05.06.2025).*	
32.	**ÎS „Calea Ferată din Moldova”**		Nu a prezentat avizul.	
33.	**Comisia Națională a Pieței Financiare** *(Nr. 06-4/2588 din 12.06.2025)*		Lipsa de obiecții și propuneri.	
34.	**Biroul Național de Statistică** *(aviz plasat pe platforma legiferare.gov.md)*		Lipsa de obiecții și propuneri.	
35.	**Banca Națională a Moldovei**	**35.**	1. Având în vedere că Legea nr. 202/2017 privind activitatea băncilor și Regulamentul privind cerinţele minime pentru gestionarea riscurilor aferente tehnologiei informaţiei şi comunicaţiilor, securităţii informaţiei şi continuităţii activităţii	**Nu se acceptă** Capitolul V din proiectul Regulamentului vine deja cu detalierile necesare privind

			(aprobat prin Hotărârea BNM nr. 29/2025) stabilesc cerințele de securitate în domeniul tehnologiei informației și comunicațiilor care urmează a fi aplicate de către bănci, precum și competența BNM de supraveghere a respectării acestor cerințe, reiterăm că implementarea proiectului hotărârii de Guvern, în redacția actuală, generează riscuri semnificative de suprapunere a competențelor și atribuțiilor între BNM și Agenția pentru Securitate Cibernetică (ASC) în partea ce ține de furnizorii de servicii din sectorul bancar. O astfel de suprapunere creează vulnerabilități în procesul de supraveghere și monitorizare a sectorului bancar, generând riscuri operaționale suplimentare, inclusiv raportări incomplete, duble sau eronate. În aceeași ordine de idei, susținem înțelegerea comună că cerințele stabilite de cadrul normativ special aplicabil băncilor au un caracter mai riguros decât cele prevăzute de Legea nr. 48/2023 privind securitatea cibernetică și prezentul proiect. În acest sens, propunem completarea proiectului hotărârii de Guvern cu o prevedere adițională care să menționeze că furnizorii de servicii din sectorul bancar aplică cerințele de asigurare a securității cibernetice prevăzute de Legea nr. 202/2017 privind activitatea băncilor și Regulamentul privind cerinţele minime pentru gestionarea riscurilor aferente tehnologiei informaţiei şi comunicaţiilor, securităţii informaţiei şi continuităţii activităţii, aprobat prin Hotărârea BNM nr. 29/2025.	determinarea cerințelor aplicabile furnizorilor de servicii în sectoarele critice, stabilind modul de evaluare a echivalenței dintre efectele produse de legislația sectorială și legislația în domeniul securității cibernetice. Acest principiu este reglementat la nivel primar de prevederile art. 3 alin. (5) din Legea securității cibernetice. În acest context relevăm că cerințele de securitate stabilite de proiectul propus spre avizare constituie un minim necesar pentru asigurarea unei maturități suficiente a tuturor furnizorilor de servicii în sectoarele critice și implicit o garanție orizontală de evitare a unor eventuale lacune sau cerințe mai indulgente în cadrul de reglementare sectorial care ar putea să nu asigure o reziliență minimă. De asemenea, având reglementările art. 3 alin. (5) din legea securității cibernetice și prevederile Capitolului V din proiectului Regulamentului, din punct de vedere formal juridico-normativ, completarea propusă este lipsită de utilitate juridică.
		36.	Suplimentar, comunicăm disponibilitatea de furnizare a informațiilor necesare ASC în exercitarea atribuțiilor sale (raportarea incidentelor semnificative din sectorul bancar) prin intermediul platformei centralizate de raportare a incidentelor gestionată de BNM, reducând astfel riscul operațional asociat	**Se acceptă în principiu** Aceste aspecte urmează a fi soluționate la nivel operațional și tehnic la momentul interconectării și integrării platformelor existente

			dublei raportări. Mecanismul respectiv urmează să contribuie la schimbul de informații dintre BNM și ASC, la evitarea suprapunerii de competențe dintre aceste două autorități și a intruziunilor reciproce nejustificate.	și/sau viitoare deținute de BNM, ASC sau alte autorități publice și organizații
		37.	Adițional, în vederea consolidării capacităților naționale în domeniul securității cibernetice, recomandăm organizarea periodică a unor exerciții comune de simulare între BNM și ASC, care să permită evaluarea continuă și îmbunătățirea capacității de reacție la incidentele majore.	**Se acceptă** Acesta este în principiu una din atribuțiile ASC care decurge din funcțiile (inclusiv cooperare, orientare metodologică, monitorizare și supraveghere a domeniului) acesteia stabilite de Legea nr. 48/2023 privind securitatea cibernetică, exercițiile comune, inclusiv tematice, fiind una din metodele prin care poate fi evaluată starea de lucruri în anumite sfere și maturitatea diferiților furnizori de servicii în sectoare critice. Astfel de exerciții, ar trebui organizate nu doar între ASC (CSIRT național) și BNM (CSIRT sectorial) ci și prin implicarea altor actori din acest domeniu inclusiv mediul universitar, guvernamental, militar.
		38.	2. Cu referire la pct. 3.4 din dispozitivul hotărârii de Guvern, considerăm că cerința de prezentare a raportului primei evaluări a conformității cu cerințele prevăzute în proiectul de regulament (efectuată de către o parte terță certificată în domeniul auditului securității informațiilor) presupune costuri suplimentare substanțiale pentru entități și crește riscul divulgării informațiilor sensibile referitoare la măsurile interne de securitate către terțe părți. În acest sens, propunem ajustarea prevederii pentru a permite efectuarea evaluărilor de	**Se acceptă parțial** Punctul 3.4 **(***în noua redacție punctul 2.4)* a fost expus în următoarea redacție: „2.4. vor prezenta Agenției pentru Securitate Cibernetică, în termen de 18 de luni de la data intrării în vigoare a prezentei hotărâri, raportul primei evaluări a conformității cu

			conformitate și de către auditori certificați independenți față de domeniul auditat (de exemplu CISA), fără referința exclusivă la părțile terțe externe. În acest context, propunem următoarea redacție pentru prevederea de la pct. 3.4: „3.4 vor prezenta Agenției pentru Securitate Cibernetică, în termen de 18 de luni de la data intrării în vigoare a prezentei hotărâri, raportul primei evaluări a conformității cu cerințele prevăzute în anexa la prezenta hotărâre, efectuată de auditori certificați în domeniul securității informațiilor (CISA), care sunt independenți față de domeniul auditat”. Menționăm că această ajustare este necesară pentru a preveni suprasaturarea inevitabilă a pieței locale de servicii de audit specializate în domeniul securității informațiilor, având în vedere numărul ridicat de entități care trebuie să se conformeze într-un termen relativ scurt (18 luni). O astfel de suprasaturare ar conduce la întârzieri semnificative în evaluarea conformității, cu potențiale efecte negative asupra eficacității generale a implementării cerințelor de securitate cibernetică. În schimb, prin includerea evaluării de către auditorii certificați independenți, dar nu neapărat externi, se optimizează utilizarea resurselor certificate disponibile, asigurându-se astfel o conformare promptă și eficientă a entităților vizate.	cerințele prevăzute în anexa la prezenta hotărâre, efectuată de către ***persoane care dețin certificări*** în domeniul auditului securității informațiilor.”, asigurând concomitent corelarea cu terminologia utilizată în pct. 13 din anexa la proiectul Regulamentului.
		39.	3. La capitolul III din proiectul regulamentului, recomandăm evaluarea suplimentară a temeiului legal privind reglementarea criteriilor de evaluare a echivalenței efectelor obligațiilor de asigurare a securității cibernetice. Opinăm, că criteriile de evaluare a echivalenței efectelor obligațiilor de asigurare a securității cibernetice urmează a fi detaliate în Legea nr. 48/2023. În acest sens, atragem atenția la constatările Curții Constituționale expuse în paragrafele 77-79 din Hotărârea nr. 23/2013. La fel, observăm că procedura de identificare a furnizorilor de servicii este reglementată prin Regulamentul cu privire la identificarea furnizorilor de servicii aprobat prin	**Se acceptă parțial** Clauza de adoptare a proiectului a fost modificată prin includerea referinței la art. 3 alin. (7) și art. 23 alin. (2) lit. c) din Legea nr. 48/2023 privind securitatea cibernetică. Această completare este importantă din perspectiva competenței Guvernului în reglementarea acestui aspect.

			Hotărârea de Guvern nr. 860/2024. Prin urmare, având în vedere că evaluarea echivalenței obligațiilor de asigurare a securității cibernetice se efectuează la etapa de identificare a furnizorilor de servicii, opinăm că procedura de evaluare a echivalenței efectelor obligațiilor de asigurare a securității cibernetice (în baza criteriilor de evaluare prevăzute de lege) se circumscrie obiectului de reglementare al Hotărârii de Guvern nr. 860/2024.	În special menționăm că în temeiul art. 23 alin. (2) lit. c) din Legea nr. 48/2023 Guvernul este obligat să adopte actele normative necesare punerii în aplicare a prevederilor legii.
36.	**Centrul Național pentru Protecția Datelor cu Caracter Personal** *(Nr. 04-01/1924 din 13.06.2025)*		Lipsa obiecțiilor.	
37.	**Centrul de Armonizare a Legislației**	**40**	CAL validează PHG. Totodată, clauza de armonizare se va expune imediat după clauza de adoptare a PHG, fiind exclusă din pct. 1 al HG.	**Se acceptă**

Secretar de stat **Michelle ILIEV**