**NOTA DE FUNDAMENTARE**

**la proiectul Hotărîrii Guvernului cu privire la aprobarea proiectului Hotărîrii Parlamentului pentru aprobarea Programului național de securitate cibernetică pentru anii 2026-2030**

**1. Denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului normativ**

Proiectul Hotărîrii Guvernului cu privire la aprobarea proiectului Hotărîrii Parlamentului pentru aprobarea Programului național de securitate cibernetică pentru anii 2026-2030 a fost 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*

Proiectul Hotărîrii Guvernului cu privire la aprobarea proiectului Hotărîrii Parlamentului pentru aprobarea Programului național de securitate cibernetică pentru anii 2026-2030 este elaborat în conformitate cu prevederile art. 6 alin. (3) al Legii nr. 48/2023 privind securitatea cibernetică și Hotărârii Guvernului nr. 386/2020 cu privire la planificarea strategică.

Totodată, Programul contribuie la implemntarea unor obiective și direcții strategice ale următoarelor strategii:

- Strategia securității naționale a Republicii Moldova, aprobată prin Hotărârea Parlamentului nr. 391/2023;
- Strategia de transformare digitală a Republicii Moldova pentru anii 2023–2030, aprobată prin Hotărârea Guvernului nr. 650/2023;
- Strategia de apărare națională 2024–2034, aprobată prin Hotărârea Parlamentului nr. 319/2024;
- Strategia de dezvoltare "Educația 2030", aprobată prin Hotărârea Guvernului nr. 114/2023;
- Strategia de dezvoltare a domeniului afacerilor interne pentru anii 2022–2030, aprobată prin Hotărârea Guvernului nr. 658/2022.

Elaborarea proiectului de act normativ propus spre examinare este prevăzută și de următoarele documente strategice ale Republicii Moldova:

1) Agenda de reforme aferentă Planului de creștere al Republicii Moldova pentru 2025-2027 (Hotărârea Guvernului nr. 260/2025) – măsura 2.3.11, Condiția de plată și linia de referință: „Pentru a pune în aplicare noul său Program național de acțiuni în domeniul securității cibernetice pentru perioada 2025-2030, Moldova își face Agenția pentru Securitate Cibernetică pe deplin operațională și înființează Echipa națională de intervenție în caz de urgență informatică (CERT).”

2) Foaia de parcurs privind „Statul de drept” (criteriu de referință în procesul de aderare a Republicii Moldova la Uniunea Europeană) (Hotărârea Guvernului nr. 275/2025) – acț. 4.4 din Rezultatul strategic nr. 4. „Consolidarea capacității de prevenire și combatere a criminalității cibernetice”.

3) Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029 (Hotărârea Guvernului nr. 306/2025) – Cap.10, proiectul 40.

4) Planul național de reglementări pentru anul 2025 (Hotărârea Guvernului nr. 841/2024) – acțiunea 24.

5) Strategia de transformare digitală a Republicii Moldova (Hotărârea Guvernului nr. 650/2023) - Obiectivul general nr. 5. „Crearea unui mediu digital accesibil, sigur și incluziv”.

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

Digitalizarea a impulsionat dezvoltarea economică și interconectarea globală, dar a crescut și expunerea la riscuri cibernetice. La nivel european, numărul incidentelor cu impact semnificativ

este în creștere, iar costurile încălcărilor de securitate au atins niveluri record. Criminalitatea cibernetică generează pierderi economice considerabile, estimate la circa 0,3% din PIB, ceea ce pentru Republica Moldova ar însemna anual circa 49 milioane USD.

În plan intern, se observă o creștere alarmantă a atacurilor cibernetice asupra cetățenilor și instituțiilor statului. Conștientizarea publică este în creștere, dar nivelul de familiarizare cu tipurile de amenințări rămâne scăzut. Potrivit Indicelui Global de Securitate Cibernetică (UIT), Moldova se află la un nivel mediu de performanță, cu lacune la capitolele măsuri tehnice și dezvoltarea capacităților.

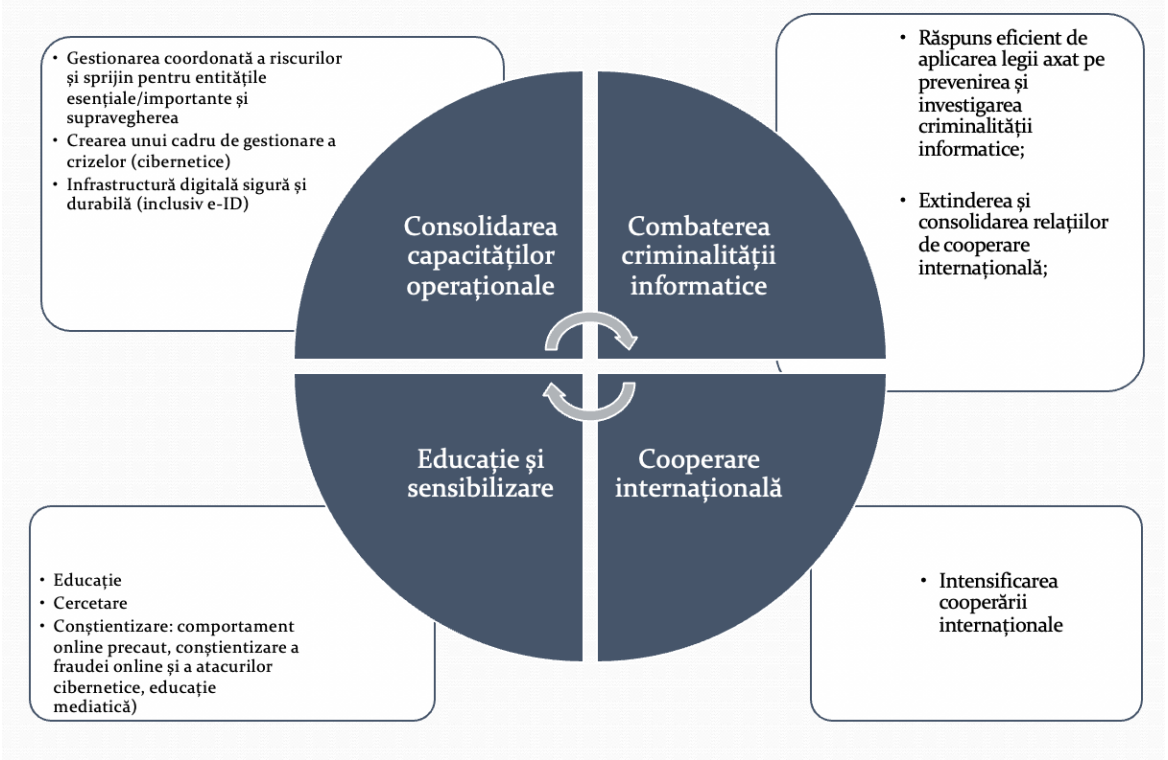
Sectorul TIC contribuie semnificativ la PIB, însă lipsa cadrelor calificate și investițiile reduse în cercetare și educație au impact asupra rezilienței digitale. Totodată, Strategia de securitate națională subliniază vulnerabilitatea țării la atacuri cibernetice și riscuri hibride, inclusiv dezinformare. În prezent, Moldova nu dispune de un cadru clar pentru gestionarea crizelor cibernetice, ceea ce o face dependentă de suport din partea instituțiilor UE.

Procesul de aderare la UE aduce noi obligații, în special punerea în aplicare a Legii 48/2023 și operaționalizarea Agenției pentru Securitate Cibernetică, inclusiv consolidarea capacităților furnizorilor de servicii critice și transpunerea cadrului normativ european (NIS2, Actul privind reziliența cibernetică, securitatea 5G).

Poate fi menționat că Republica Moldova se confruntă cu multiple provocări în domeniul securității cibernetice, dintre care se evidențiază următoarele:

- Creșterea numărului și complexității atacurilor cibernetice.
- Extinderea criminalității informatice și a fraudei online.
- Riscuri geopolitice și hibride, inclusiv dezinformare.
- Capacitate instituțională insuficientă.
- Nivel scăzut de conștientizare și educație digitală.
- Lipsa unui parteneriat public-privat funcțional.
- Vulnerabilitatea infrastructurilor critice.
- Cooperare internațională limitată.

Ca răspuns la aceste provocări, Programul prevede 4 subdomenii principale de intervenție:




**Consolidarea capacităților operaționale**

Modelul instituțional de securitate cibernetică din Republica Moldova este fragmentat, cu multiple autorități implicate în proces, dar cu o coordonare limitată și resurse insuficiente.

În ultimii ani, Republica Moldova a dezvoltat un cadru strategic, normativ și organizațional, pentru protecția spațiului său cibernetic și asigurarea securității rețelelor și sistemelor informatice, în vederea creșterii nivelului de reziliență cibernetică. Procedurile de raportare și gestionare a incidentelor în autoritățile publice sunt încă într-un stadiu de dezvoltare și este nevoie de un cadru interinstituțional mai bine structurat și funcțional, care să includă toți actorii relevanți, pentru a asigura un răspuns eficient și coordonat la atacurile cibernetice.

În prezent, principalele provocări sunt legate de lipsa resurselor umane specializate și a infrastructurii tehnice adecvate, dar și de dependența de proiecte externe pentru formare și echipamente. Responsabilitățile sunt dispersate între instituții, iar cooperarea și schimbul de date rămân reduse. Registrul național al incidentelor cibernetice nu este încă funcțional, fiind în dezvoltare, ceea ce face ca raportarea să fie fragmentară și incompletă, limitând capacitatea de prevenire și reacție. În același timp, mulți furnizori de servicii critice nu aplică încă proceduri de securitate bazate pe risc, iar Republica Moldova nu dispune de un mecanism integrat pentru gestionarea crizelor cibernetice la nivel național. Infrastructurile digitale, inclusiv identitatea digitală și semnătura electronică, rămân vulnerabile, cu un nivel scăzut de utilizare și încredere.

**Combaterea criminalității informatice**

Republica Moldova se confruntă cu o expunere ridicată la criminalitatea informatică, reflectată atât prin atacurile directe asupra instituțiilor și infrastructurilor critice, cât și prin rolul său de bază operațională pentru grupări infracționale transnaționale. Poziționarea țării pe locul 15 în clasamentul „World Cybercrime Index" indică vulnerabilități în mecanismele de prevenire și combatere, dar și asocierea nedorită cu state implicate activ în criminalitate cibernetică.

Principalele provocări sunt legate de atacurile sponsorizate de actori statali care vizează destabilizarea proceselor democratice și afectarea încrederii publice. Creșterea incidentelor de tip ransomware și fraudă online pune presiune pe instituțiile statului și mediul privat, în timp ce atacurile asupra infrastructurii critice subminează funcționarea serviciilor esențiale și generează percepții de insecuritate. În paralel, crima organizată online se dezvoltă rapid, alimentată de noi tehnologii precum inteligența artificială.

Un deficit structural îl reprezintă lipsa de profesioniști pe întreg lanțul de prevenire, investigare și urmărire penală a infracțiunilor informatice, accentuat de exodul de competențe către alte jurisdicții. Această slăbiciune afectează capacitatea autorităților de a reacționa eficient la incidente și de a construi o practică judiciară uniforme. Întreprinderile mici și mijlocii sunt în mod special vulnerabile la atacuri, din cauza resurselor limitate și a nivelului scăzut de conștientizare.

Deși Republica Moldova participă la parteneriate internaționale și este parte la Convenția de la Budapesta, nivelul de integrare în schimburile globale de informații și exerciții rămâne insuficient pentru a contracara complexitatea fenomenului.

**Educație și sensibilizare**

În prezent, Republica Moldova se confruntă cu un nivel scăzut de conștientizare în rândul autorităților publice, mediului privat, societății civile și al cetățenilor cu privire la riscurile cibernetice și măsurile de protecție. Există, de asemenea, un deficit de personal specializat, ceea ce afectează prevenirea, detectarea și gestionarea incidentelor cibernetice. Accesul la educație digitală de calitate și la programe de securitate cibernetică în instituțiile de învățământ formal și non-formal este încă limitat, iar resursele disponibile nu sunt suficiente pentru formarea unor specialiști competenți.

Igiena cibernetică și siguranța online nu sunt gestionate strategic la nivel național, iar inițiativele de sensibilizare existente au avut un impact redus, nefiind coordonate între actorii publici și cei privați.

În lipsa unor mecanisme centralizate și a unor evaluări periodice ale impactului programelor de educație și campaniilor de conștientizare, Republica Moldova întâmpină dificultăți în creșterea

gradului de pregătire a cetățenilor și a instituțiilor pentru prevenirea și gestionarea incidentelor cibernetice.

**Cooperare internațională**

În plan internațional, Republica Moldova este tot mai integrată în programe și inițiative UE și NATO, participă la schimburi de formare și face parte din rețele multilaterale de reziliență. Totodată, diplomația cibernetică rămâne insuficient dezvoltată, lipsind unitățile specializate responsabile, inclusiv, de negocierea acordurilor internaționale pe segmentul dat.

Provocările majore includ armonizarea legislației naționale cu reglementările UE și integrarea în formatele internaționale de cooperare, precum și natura transnațională a amenințărilor cibernetice. Majoritatea incidentelor și infracțiunilor cibernetice implică autori și victime din jurisdicții diferite, ceea ce face prevenirea și combaterea acestora dependentă de cooperarea internațională eficientă. De asemenea, tehnologiile de securitate și metodele de atac sunt similare la nivel global, iar grupările de crimă organizată operează adesea dincolo de granițele naționale, accentuând necesitatea unor relații strânse și schimburi constante de informații cu autorități și organizații internaționale.

O altă provocare este coordonarea internă și valorificarea eficientă a resurselor limitate. Colaborarea între entitățile guvernamentale, mediul de afaceri și comunitatea de cercetare este esențială pentru maximizarea expertizei în securitate cibernetică și consolidarea rezilienței țării.

Toate cele 4 subdomenii de intervenție sunt descrise în capitolul „Analiza situației” din partea descriptivă a Programului.

## 3. Obiectivele urmărite și soluțiile propuse

*3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi*

Programul își propune să contribuie la realizarea obiectivelor și direcțiilor prioritare stabilite în documentele de politici publice de nivel superior, în special în Strategia națională de securitate a Republicii Moldova, Strategia de transformare digitală 2023–2030, precum și în alte documente strategice și de planificare, cum ar fi Strategia de dezvoltare „Educație 2030”, Strategia de dezvoltare a domeniului afacerilor interne 2022–2030, Strategia națională de apărare 2024–2034, Programul de prevenire și combatere a criminalității 2022–2025 (și proiectul pentru perioada 2026–2030) și Programul național de aderare a Republicii Moldova la UE 2025–2029.

În urma analizei acestor documente strategice și a realizării unui inventar detaliat al situației în domeniul securității cibernetice, au fost formulate patru obiective generale, prezentate în tabelul de mai jos.

Fiecare obiectiv general este detaliat în mai multe obiective specifice care oferă o direcție mai focusată cu privire la modul în care urmează a fi obținute rezultatele așteptate. Toate aceste obiective sunt însoțite de acțiuni, care sunt reflectate în Planul de acțiuni al Programului.

| **Obiectiv general** | **Obiectiv specific** | **Indicator** | **Valoarea de referință (2025)** | **Țintă(2028)** | **Țintă(2030)** |
|---|---|---|---|---|---|
| 1.Consolidarea capacităților operaționale | 1.1 Consolidarea capacităților de răspuns la incidentele cibernetice ale Agenției pentru Securitate Cibernetică | Creșterea scorului de țară la capitolul “dezvoltarea capacităților”<br><br>*Sursa: Indicele global de securitate cibernetică (GCI) al UIT* | 8,04 (2024) | 12.5 | 17,5 |

| | | | | | |
|---|---|---|---|---|---|
| | 1.2 Consolidarea rezilienței furnizorilor de servicii în sectoarele critice împotriva amenințărilor cibernetice și a incidentelor cibernetice. | Creșterea scorului de țară la capitolul "măsurile tehnice"<br><br>*Sursa: Indicele global de securitate cibernetică (GCI) al UIT* | 6,68 (2024) | 10,5 | 15,5 |
| | 1.3 Îmbunătățirea răspunsului la crizele cibernetice prin asigurarea unei abordări coordonate și prin valorificarea structurilor existente pentru menținerea funcțiilor societale vitale | Creșterea scorului de țară la capitolul "măsurile tehnice"<br><br>*Sursa: Indicele global de securitate cibernetică (GCI) al UIT* | 6,68 (2024) | 10,5 | 15,5 |
| 2.Consolidarea rezilienței țării împotriva criminalității informatice | 2.1 Consolidarea competențelor și abilităților autorităților de aplicare a legii în ceea ce privește investigarea infracțiunilor informatice şi infracţiunilor în domeniul comunicaţiilor electronice | Creșterea numărului de cauze cu privire la infracțiunile informatice şi infracțiunile în domeniul comunicaţiilor electronice remise în judecată<br><br>*Sursa: Ministerul Afacerilor Interne* | N/A | Creșterea cu 15% | Creșterea cu 30% |
| | 2.2. Crearea de instrumente tehnologice eficace și avansate pentru prevenirea, detectarea și investigarea eficientă a criminalității informatice | Dotarea cu instrumente și soluții inteligente de investigare<br><br>*Sursa: Ministerul Afacerilor Interne* | 8 instrumente (2024) | Minim 9 instrumente | Creștere cu 25% (minim 10 soluții) |

| | | | | | |
|---|---|---|---|---|---|
| 3. Dezvoltarea competențelor și a culturii de securitate cibernetică în societate | 3.1 Dezvoltarea unei forțe de muncă calificate în domeniul securității cibernetice prin extinderea oportunităților educaționale | Ponderea specialiștilor în TIC în rândul populației ocupate<br><br>*Sursa: Ministerul Educației și Cercetării, Biroul Național de Statistică* | 2,7 % (2022) | 3,3 % | 4% |
| | | Ponderea absolvenților STEAM în rezerva totală de absolvenți de studii universitare<br><br>*Sursa: Ministerul Educației și Cercetării, Biroul Național de Statistică* | 13,7 % (2022) | 15 % | 16% |
| | 3.2 Dezvoltarea unui mecanism național de monitorizare continuă și evaluare a dezvoltării societății digitale | Ponderea populație cu competențe digitale de bază<br><br>*Sursa: Ministerul Educației și Cercetării, Biroul Național de Statistică* | N/A | 40 % | 80% |
| | 3.3. Consolidarea cooperării interne între autoritățile și instituțiile publice, precum și cu mass-media pentru a combate eficient manipulările electorale și atacurile cibernetice. | Ponderea persoanelor care verifică veridicitatea informațiilor întâlnite pe internet<br><br>*Sursa: Ministerul Educației și Cercetării, Biroul Național de Statistică* | N/A | 40 % | 80% |
| | 3.4. Protejarea drepturilor și libertăților persoanelor atunci când datele lor cu caracter personal sunt prelucrate | Ponderea utilizatorilor de internet care aplică măsuri active de gestionare a confidențialității și a datelor personale<br><br>*Sursa: Ministerul Educației și Cercetării, Biroul Național de Statistică* | N/A | 40 % | 80% |
| 4. Cooperarea internațională pentru a deveni un partener de încredere în | 4.1 Consolidarea cooperării internaționale prin integrarea Republicii | Creșterea scorului de țară la capitolul "măsuri de cooperare" | 15,51 (2024) | 16,5 | 18,5 |

| | | | | | |
|---|---|---|---|---|---|
| comunitatea internațională de aplicare a legii și securitate cibernetică | Moldova în cadrele de cooperare în materie de aplicare a legii și securitate cibernetică la nivelul UE | *Sursa: Indicele global de securitate cibernetică al ITU* | | | |
| | 4.2 Dezvoltarea platformelor de comunicare strategică externă pentru asigurarea securității informaționale și promovarea intereselor naționale ale Republicii Moldova | Creșterea scorului de țară la capitolul "măsuri de cooperare" *Sursa: Indicele global de securitate cibernetică al ITU* | 15,51 (2024) | 16,5 | 18,5 |
| | 4.3 Consolidarea capacității de diplomație cibernetică internațională | Creșterea scorului de țară la capitolul "măsuri de cooperare" *Sursa: Indicele global de securitate cibernetică al ITU* | 15,51 (2024) | 16,5 | 18,5 |

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

Nu sunt opțiuni alternative.

Cadrul normativ prevede în mod imperativ obligativitatea elaborării unui document de politici în domeniul securității cibernetice, aspect reflectat într-un șir de strategii, printre care Strategia securității naționale a Republicii Moldova, Strategia de transformare digitală a Republicii Moldova pentru anii 2023–2030 etc.

## 4. Analiza impactului de reglementare

*4.1. Impactul asupra sectorului public*

Implementarea Programului va produce un impact sistemic asupra sectorului public, având impact direct asupra modului în care autoritățile și instituțiile publice își gestionează resursele, riscurile și responsabilitățile în domeniul securității cibernetice.

Impactul asupra sectorului public este vizibil prin mai multe dimensiuni esențiale precum:

- ***Consolidarea cadrului instituțional și a guvernanței*** - va fi consolidat mecanismul de coordonare între autoritățile și instituțiile publice cu responsabilități în domeniul securității cibernetice.
- ***Creșterea rezilienței operaționale*** – toate autoritățile și instituțiile publice vor fi obligate să implementeze un set minim de măsuri de securitate, ceea ce va reduce vulnerabilitatea sistemelor guvernamentale.
- ***Instruirea și formarea funcționarilor publici*** - programul prevede instruirea funcționarilor și angajaților din autoritățile și instituțiile publice, ceea ce va ridica nivelul de alfabetizare cibernetică.
- ***Îmbunătățirea transparenței și responsabilității*** - raportarea obligatorie a incidentelor cibernetice către autoritățile competente va genera o imagine clară asupra nivelului real de

amenințări și va permite o planificare mai eficientă a resurselor. Publicarea rapoartelor anuale privind nivelul de maturitate cibernetică va responsabiliza instituțiile și va încuraja respectarea standardelor minime.

- ***Eficiență financiară și utilizarea optimă a resurselor*** - investițiile coordonate în soluții comune (licențe, infrastructură SOC/SIEM, servicii de audit) vor permite economii, reducând cheltuielile individuale ale instituțiilor. Prin prevenirea incidentelor majore, se vor diminua costurile de remediere post-incident și pierderile asociate întreruperii serviciilor publice.
- ***Aliniere la standardele europene și integrare internațională*** – transpunerea legislației Uniunii Europene la nivel național și a altor instrumente europene va facilita interoperabilitatea instituțiilor naționale cu instituțiile partenere europene. Participarea instituțiilor publice la exerciții comune și la mecanisme de schimb de informații va contribui la recunoașterea Republicii Moldova ca partener de încredere în domeniul securității cibernetice.

*4.2. Impactul financiar și argumentarea costurilor estimative*

Implementarea Programului se va realiza din contul și în limitele alocațiilor aprobate în bugetele autorităților responsabile, precum și prin intermediul asistenței financiare și tehnice acordate de organizațiile internaționale și partenerii de dezvoltare, și din alte surse permise de legislație.

În urma evaluării costurilor, cheltuielile necesare pentru realizarea acțiunilor planificate sunt estimate la circa 79,9 milioane lei. Dezagregarea pe obiective specifice și ani este prezentată la capitolul costuri în proiectul Programului, precum și la nivel de acțiuni în Planul de acțiuni al Programului.

Deși aproximativ 2/3 din aceste cheltuieli nu dispune, la acest moment, de acoperire financiară din partea partenerilor de dezvoltare și urmează a fi reflectată în Cadrul Bugetar pe Termen Mediu și bugetul de stat, autoritățile și instituțiile responsabile vor continua dialogul cu partenerii de dezvoltare și alți actori relevanți, în vederea identificării și mobilizării surselor externe de finanțare. Acest proces va contribui la diminuarea presiunii asupra bugetului național.

Implementarea Programului se va realiza preponderent prin următoarele programe bugetare:

- Programul „03. Executivul și serviciile de suport”
  - Subprogramul „0303. e-Transformare a Guvernării”
- Programul „15. Edificarea societății informaționale”
  - Subprogramul „1501. Politici și management în domeniul dezvoltării informaționale”
  - Subprogramul „1504. Tehnologii informaționale”
- Programul „50. Servicii generale economice și comerciale”
  - Subprogramul “5001-Politici și management în domeniul macroeconomic și de dezvoltare a economiei”

*4.3. Impactul asupra sectorului privat*

Realizarea acțiunilor în baza implementării Programului va avea un impact asupra mediului privat, în special asupra furnizorilor de servicii identificați de Agenția pentru Securitate Cibernetică conform Hotărîrii Guvernului nr. 860/2024.

Totodată, impactul acțiunilor din proiectul Programului ce țin de crearea cadrului normativ va fi evaluat la etapa elaborării actelor normative în cauză.

Impactul asupra sectorului privat este vizibil prin mai multe dimensiuni esențiale, precum:

- ***Creșterea nivelului de conformitate și securitate*** – furnizorii de servicii implementând cerințe minime de securitate și respectând procedurile standardizate de raportare a incidentelor vor reduce expunerea la riscuri și vor asigura continuitatea serviciilor esențiale furnizate cetățenilor și economiei.

- ***Stimularea investițiilor în securitatea cibernetică*** - prin implementarea cerințelor de securitate obligatorii, mediul privat va fi motivat să investească în infrastructuri, soluții și personal specializat, ceea ce va permite prevenirea pierderilor financiare și va spori competitivitatea companiilor pe piață.
- ***Crearea de mecanisme de cooperare public–privat*** - instituirea mecanismelor de cooperare va permite schimbul regulat de informații despre amenințări și bune practici între autorități și furnizorii de servicii, ceea ce va contribui la detectarea timpurie a atacurilor și o reacție mai rapidă și coordonată.
- ***Dezvoltarea capitalului uman în sectorul privat*** - Programul prevede instruirea și certificarea unui număr semnificativ de specialiști IT din mediul privat, ceea ce va contribui la reducerea deficitului de competențe și la creșterea calității serviciilor de securitate cibernetică oferite pe piață.
- ***Creșterea încrederii consumatorilor și a partenerilor*** - consolidarea securității infrastructurilor și a serviciilor private va spori încrederea clienților și a partenerilor internaționali. Aceasta va facilita atragerea de investiții străine directe și integrarea companiilor naționale în lanțurile valorice la nivel internațional.

*4.4. Impactul social*

Implementarea Programului va avea impact asupra societății în ansamblu, contribuind la protecția drepturilor cetățenilor, care vor beneficia de servicii reziliente din partea statului și a mediului privat. Printre cele importante rezultate se numără:

- ***Creșterea alfabetizării digitale și a culturii de securitate*** - campaniile de informare, instruirile și introducerea elementelor de igienă cibernetică în educația formală și non-formală vor contribui la ridicarea nivelului de conștientizare al populației.
- ***Reducerea fraudei și a escrocheriilor online*** - crearea unor mecanisme accesibile de raportare și instruirea cetățenilor vor duce la scăderea numărului de victime ale fraudelor cibernetice.
- ***Creșterea încrederii în serviciile digitale*** - consolidarea securității cibernetice va încuraja populația să utilizeze mai activ serviciile electronice din sănătate, educație, plăți și comerț electronic, ceea ce va fi stimulată incluziunea digitală și va crește calitatea vieții.
- ***Consolidarea responsabilității colective*** - Programul promovează ideea că securitatea cibernetică este o responsabilitate comună a statului, companiilor și cetățenilor. Astfel, se va crea o cultură socială de prevenire și reacție rapidă la incidente.

*4.4.1. Impactul asupra datelor cu caracter personal*

Programul va contribui direct la îmbunătățirea protecției datelor cu caracter personal, reducând riscurile de compromitere și sporind încrederea cetățenilor în mediul digital. Printre cele mai importante rezultate se numără:

- ***Reducerea riscului de incidente de securitate -*** implementarea cerințelor minime obligatorii va diminua probabilitatea accesului neautorizat la date personale.
- ***Raportare și transparență*** - obligația instituțiilor și operatorilor privați de a raporta incidentele cibernetice în termene stricte va permite o reacție rapidă și va contribui la protejarea drepturilor persoanelor vizate.
- ***Creșterea capacității instituționale a autorităților de supraveghere*** - Programul prevede crearea de mecanisme de cooperare între Agenția pentru Securitate Cibernetic și Centrul Național pentru Protecția Datelor cu Caracter Personal, ceea ce va întări capacitatea de monitorizare și sancționare.
- ***Responsabilizarea operatorilor și a angajaților*** - prin instruiri și mecanisme, operatorii de date vor fi obligați să adopte practici mai stricte de protecție, reducând riscul de scurgeri cauzate de erori umane sau neglijență.

- ***Creșterea încrederii cetățenilor*** - o mai bună protecție a datelor va consolida încrederea populației în serviciile digitale publice și private, stimulând utilizarea lor mai largă și sprijinind transformarea digitală a Republicii Moldova.

*4.4.2. Impactul asupra echității și egalității de gen*

Implementarea Programului va contribui la promovarea echității și egalității de gen în sectorul digital și în domeniul securității cibernetice. Prin acțiunile planificate, Programul va stimula participarea activă a femeilor în formare, instruire și certificare, asigurând acces egal la oportunități profesionale.

*4.5. Impactul asupra mediului*

Programul nu are un impact direct asupra mediului înconjurător. Acțiunile prevăzute vizează în principal consolidarea cadrului instituțional, dezvoltarea capacităților tehnice, formarea capitalului uman și creșterea rezilienței digitale, fără a genera efecte semnificative asupra mediului.

Totuși, prin promovarea digitalizării serviciilor și utilizarea infrastructurilor partajate, Programul poate avea efecte indirecte pozitive, contribuind la reducerea consumului de resurse materiale. Aceste efecte sunt secundare și nu constituie obiectiv explicit al Programului.

*4.6. Alte impacturi și informații relevante*

Alte impacturi nu au fost identificate.

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

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

Prezentul proiect de Hotărîre a Guvernului nu conține norme privind transpunerea actelor juridice ale UE în legislația națională. Totodată, Programul include acțiuni specifice care vizează transpunerea ulterioară a actelor juridice ale UE în legislația națională, asigurând astfel alinierea cadrului normativ la cerințele europene.

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

În procesul elaborării proiectului Programului și, implicit, a planului de acțiuni, s-a luat în considerare prevederile Comunicării Comune către Parlamentul European și Consiliu „Strategia de securitate cibernetică a UE pentru deceniul digital".

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

În vederea respectării prevederilor art. 8 și 9 din Legea nr. 239/2008 privind transparența în procesul decizional, precum și conform prevederilor pct. 177 din Regulamentul Guvernului, aprobat prin Hotărârea Guvernului nr. 610/2018, a fost publicat anunțul privind inițierea procesului de elaborare a proiectului Programului național în domeniul securității cibernetice (https://particip.gov.md/ru/document/stages/anunt-privind-initierea-procesului-de-elaborare-a-proiectului-programului-national-in-domeniul-securitatii-cibernetice-pentru-anii-2026-2030/14107).

Totodată, în vederea respectării prevederilor pct. 63.8 al Regulamentului cu privire la planificarea strategică, aprobat prin Hotărârea Guvernului nr. 386/2020, conceptul revizuit Programului în baza opiniei Cancelariei de Stat a fost plasat pe site-ul web al Ministerului Dezvoltării Economice și Digitalizării și platforma particip.gov.md.

Adițional, în vederea respectării prevederilor 63.14 al aceluiași Regulament, proiectul a fost supus evaluării calității și a conformității de către Cancelaria de Stat și Ministerul Finanțelor. Ulterior, proiectul a fost definitivat în baza recomandărilor acestor autorități.

Suplimentar, la data de 11.11.2025, în vederea respectării pct. 63.5, proiectul a fost supus examinării în cadrul Consiliului pentru coordonarea dezvoltării durabile.

**7. Concluziile expertizelor**

| |
|---|
| Proiectul va fi supus expertizei juridice din partea Ministerului Justiției și expertizei anticorupție de către Centrul Național Anticorupție. |
| **8. Modul de încorporare a actului în cadrul normativ existent** |
| Proiectul se integrează în sistemul legislației, este corelat cu prevederile actelor normative conexe în vigoare, iar implementarea prevederilor acestui proiect nu necesită modificarea altor acte normative |
| **9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ** |
| Nu necesită careva măsuri pentru implementare. |

**Secretar de stat**

Digitally signed by Selevestru Natalia
Date: 2021.11.13 14:31:46 EET
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

**Natalia SELEVESTRU**