proiect

GUVERNUL

HOTĂRÂRE nr. din

privind aprobarea Conceptului Sistemului informațional "Registrul de stat al incidentelor cibernetice" și a Regulamentului Registrului de stat al incidentelor cibernetice

În temeiul art. 22 lit. d) din Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr. 6-12, art. 44), cu modificările ulterioare, art. 10 din Legea nr.48/2023 privind securitatea cibernetică (Monitorul Oficial al Republicii Moldova, 2023, nr. 151-153 art. 225) și al art. 16 din Legea nr. 71/2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr. 70-73, art. 314), cu modificările ulterioare, Guvernul HOTĂRĂȘTE:

1. Se aprobă:

1.1 Conceptul Sistemului informațional „Registrul de stat al incidentelor cibernetice" (anexa nr.1).

1.2 Regulamentul Registrului de stat al incidentelor cibernetice (anexa nr.2).

2. Se instituie Registrul de stat al incidentelor cibernetice.

3. Se desemnează Agenția pentru Securitate Cibernetică în calitate de posesor, deținător și administrator tehnic al Sistemului informațional „Registrul de stat al incidentelor cibernetice", care va asigura crearea, implementarea, funcționarea și dezvoltarea Sistemului informațional „Registrul de stat al incidentelor cibernetice".

4. Realizarea prevederilor prezentei hotărâri se va efectua din contul și în limitele mijloacelor financiare alocate din bugetul de stat și ale altor mijloace, conform legii.

5. Se abrogă Hotărîrea Guvernului nr.388/2022 cu privire la aprobarea Conceptului Sistemului informațional „Registrul de stat al incidentelor de securitate cibernetică"

PRIM-MINISTRU

Contrasemnează:

Viceprim-ministru, ministrul
dezvoltării economice și digitalizării

Anexa nr.1

CONCEPTUL

Sistemului informațional „Registrul de stat al incidentelor cibernetice”

I. INTRODUCERE

În scopul evidenței datelor privind apariția, evoluția și soluționarea incidentelor cibernetice, al automatizării proceselor de identificare, înregistrare, documentare, clasificare, analizare și gestionare a unor astfel de incidente, al monitorizării și evidenței alertelor cibernetice și vulnerabilităților, în conformitate cu prevederile art. 10 alin. (1) din Legea nr.48/2023 privind securitatea cibernetică, Guvernul a fost abilitat cu competențe privind crearea Registrului de stat al incidentelor cibernetice și sistemului informațional destinat ținerii registrului respectiv.

Prin Hotărîrea Guvernului nr.1028/2023 Agenția pentru Securitate Cibernetică (în continuare - ASC) a fost desemnată de către Guvern în calitate de autoritate competentă la nivel național în domeniul securității cibernetice și echipă de răspuns la incidente cibernetice la nivel național. Pentru exercitarea funcțiilor respective este necesar de a asigura crearea Registrului de stat al incidentelor cibernetice.

De asemenea, conform pct. 7 subpct. 3) și 5) din Regulamentul cu privire la organizarea și funcționarea Agenției pentru Securitate Cibernetică (aprobat prin Hotărârea Guvernului nr.1028/2023) ASC are atribuția de a oferi o platformă de management al incidentelor cibernetice și pentru schimbul de informații, în scopul cooperării cu echipele de răspuns la incidente cibernetice, precum și o platformă destinată intermedierii schimbului de informații între furnizorii de servicii și alte persoane juridice. Totodată, ASC asigură monitorizarea amenințărilor cibernetice, vulnerabilităților și incidentelor cibernetice la nivel național.

În prezent, pentru raportarea incidentelor cibernetice și datelor aferente acestora se utilizează procese semi-automatizate, ceea ce presupune eventuale riscuri privind securitatea informației, integritatea datelor, istoricul modificărilor la datele înregistrate precum și riscul de pierdere a datelor. Astfel, incidentele raportate sunt documentate conform unui șablon predefinit (formular de raportare a incidentelor cibernetice) și remise prin poșta electronică, fiind înregistrate manual într-o bază de date. Metoda actuală nu asigură realizarea unei analize comprehensive, care ar permite identificarea cauzelor și a ariilor expuse riscului de securitate.

Astfel, pentru evitarea riscurilor enunțate și automatizarea proceselor din cadrul ASC, a modului de gestiune a incidentelor cibernetice și interacțiune cu Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică” (în continuare I.P STISC) și echipele de răspuns la incidente cibernetice sectoriale (în continuare - CERT sectoriale), apare necesitatea creării și implementării Sistemului informațional „Registrul de stat al incidentelor cibernetice” (în continuare – SI RSIC).

Prezentul Concept stabilește scopurile, sarcinile și funcțiile SI RSIC, structura organizațională și baza normativă necesară pentru crearea și exploatarea lui, obiectele informaționale și lista datelor care se păstrează în acesta, infrastructura tehnologică și măsurile de securitate informațională. În cadrul implementării și exploatării SI RSIC, se

va respecta Reglementarea tehnică „Procesele ciclului de viață ale software-ului RT 38370656-002:2006, aprobată prin Ordinul ministrului dezvoltării informaționale nr. 78/2006.

Beneficiile implementării SI RSIC sunt:

1) optimizarea proceselor operaționale;

2) accesarea rapidă a datelor și a documentelor relevante pentru procesele de lucru ale ASC, I.P. STISC și CERT sectoriale;

3) crearea unei baze de date electronice naționale aferente incidentelor cibernetice, vulnerabilităților și amenințărilor cibernetice;

5) înregistrarea și evidența totalității documentelor aferente incidentelor cibernetice;

6) standardizarea datelor și precizia informațiilor gestionate în sistem;

7) reducerea birocrației, prin eliminarea evidenței manuale;

8) simplificarea procesului de introducere, modificare și actualizare a informațiilor aferente incidentelor cibernetice;

9) centralizarea, în format electronic, a informațiilor cu privire la incidentele cibernetice raportate;

10) asigurarea interoperabilității cu alte sisteme informaționale de stat pentru schimbul de date;

11) asigurarea schimbului de date cu privire la incidentele cibernetice, în format electronic, între ASC, I.P. STISC și CERT sectoriale, precum și furnizori de servicii din sectoare critice, conform cadrului normativ în vigoare;

12) reducerea timpului de raportare și răspuns la incidentele cibernetice;

13) asigurarea unui mediu operațional sigur.

II. DISPOZIȚII GENERALE

1. RSIC reprezintă totalitatea sistematizată de date privind incidentele cibernetice, alertele și vulnerabilitățile cibernetice raportate către ASC, I.P. STISC, CERT sectoriale, precum și privind documentele și mijloacele de identificare a acestora.

2. RSIC este parte componentă a resurselor informaționale de stat ale Republicii Moldova.

3. SI RSIC creează un spațiu informațional unitar, care reprezintă sursa oficială de informație cu privire la alertele, vulnerabilitățile din spațiul cibernetic național și incidentele cibernetice identificate sau raportate.

4. SI RSIC reprezintă totalitatea de resurse şi tehnologii informaţionale interdependente, de metode şi de personal, destinată păstrării, prelucrării şi furnizării de informaţii privind incidentele cibernetice identificate sau raportate, alertele și vulnerabilitățile din spațiul cibernetic național, precum și gestionării incidentelor cibernetice.

5. Destinația SI RSIC constă în formarea Registrului de stat al incidentelor cibernetice, automatizarea procesului de înregistrare a incidentelor cibernetice, alertelor și vulnerabilităților, precum documentarea și gestionarea acestora conform actelor normative.

6. Crearea SI RSIC contribuie la soluționarea unei probleme polivalente: pe de o parte, se elaborează mecanismul care asigură automatizarea proceselor de identificare, înregistrare, clasificare și analiză a incidentelor cibernetice, monitorizarea și evidența alertelor, vulnerabilităților în spațiul cibernetic identificate sau raportate, iar pe de altă parte, se constituie interacțiunea ASC cu I.P. STISC și CERT sectoriale, furnizori de servicii din sectoare critice privind incidentele cibernetice și alte informații aferente securității cibernetice.

7. SI RSIC reprezintă totalitatea de resurse şi tehnologii informaţionale interdependente, de metode şi de personal, destinată păstrării, prelucrării şi furnizării de informaţie privind apariția, evoluția și soluționarea incidentelor cibernetice, automatizării proceselor de identificare, înregistrare, documentare, clasificare, analizare și gestionare a unor astfel de incidente, al monitorizării și evidenței alertelor, amenințărilor cibernetice și vulnerabilităților . Acesta va servi drept instrument de susținere a activităților ASC, I.P. STISC, CERT sectoriale prin oferirea mijloacelor tehnice de schimb informațional și de colaborare.

8. Grupul-țintă al sistemului îl reprezintă ASC, I.P. STISC, CERT sectoriale și furnizorii de servicii identificați în baza Hotărârii Guvernului nr. 860/2024 cu privire la identificarea furnizorilor de servicii, entitățile publice care au atribuții de asigurare a securității statului.

9. În sensul prezentului Concept se utilizează următoarele noțiuni de bază:

atac cibernetic – acțiune ostilă, desfășurată în spațiul cibernetic, de natură să afecteze securitatea cibernetică;

integritatea datelor – păstrarea informației cu toate atributele sale inițiale și modificarea ei doar de către persoanele autorizate;

metadate – date care descriu datele sistemului, modul în care sunt obținute și stocate, precum și precizează structura datelor, proveniența lor, regulile de transformare, de agregare și de calcul;

Alte noțiuni sunt utilizate în sensul definit de cadrul legislativ și normativ aferent domeniului securității cibernetice.

10.1. 10. Scopul SI RSIC rezidă înasigurarea formării resurselor informaționale de stat aferente incidentelor cibernetice, alertelor, vulnerabilităților în spațiul cibernetic;

10.2. dezvoltarea unei soluții tehnice flexibile și modulare;

10.3. formarea bazei de date a incidentelor cibernetice la nivel național;

10.4. asigurarea evidenței alertelor, vulnerabilităților în spațiul cibernetic și a incidentelor cibernetice identificate sau raportate, a tehnicilor și tehnologiilor folosite pentru atacuri, precum și a bunelor practici pentru protecția infrastructurilor cibernetice;

10.5. diseminarea informațiilor cibernetice și desfășurarea acțiunilor de sensibilizare și informare privind alertele, vulnerabilitățile în spațiul cibernetic, riscurile securității cibernetice și măsurile de protecție întreprinse.

11. Sarcinile de bază realizate la exploatarea SI RSIC sunt cele menționate în art. 10 din Legea nr.48/2023 privind securitatea cibernetică, precum și:

11.1. crearea și menținerea unei baze de date a incidentelor cibernetice, alertelor și vulnerabilităților și a măsurilor întreprinse pentru înlăturarea și contracararea acestora;

11.2. conectarea și realizarea schimbului de date între ASC, I.P. STISC și CERT sectoriale prin intermediul unei platforme dedicate;

11.3. promovarea bunelor practici între specialiștii ASC, I.P. STISC, CERT sectoriale și persoanele responsabile de răspuns la incidente cibernetice din cadrul furnizorilor de servicii.

12. Principiile de bază ale SI RSIC sunt:

12.1. principiul legalității – presupune crearea și exploatarea sistemului în conformitate cu legislația națională;

12.2. principiul responsabilității și conștientizării – constă în efortul continuu derulat de furnizorii de servicii în conștientizarea rolului și responsabilității individuale în atingerea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice;

12.3. principiul securității informaționale – presupune asigurarea nivelului integrității, confidențialității, exclusivității, accesibilității și eficienței protecției datelor împotriva pierderii, alterării, denaturării, deteriorării, modificării, accesului și utilizării neautorizate. Acest tip de securitate presupune rezistența la atacuri, protecția caracterului secret al informației, al integrității și pregătirea pentru lucru atât la nivel de sistem, cât și la nivel de date prezentate în această informație;

12.4. principiul modularității și scalabilității – cuprinde posibilitatea de a dezvolta sistemul fără modificarea componentelor create anterior.

III. SPAȚIUL JURIDICO-NORMATIV AL FUNCȚIONĂRII SI RSIC

13. Cadrul normativ aferent creării și implementării SI RSIC include următoarele acte normative:

Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat;

Legea nr. 71/2007 cu privire la registre;

Legea nr. 133/2011 privind protecția datelor cu caracter personal;

Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate;

Legea nr.48/2023 privind securitatea cibernetică;

Hotărârea Guvernului nr. 562/2006 cu privire la crearea sistemelor și resurselor informaționale automatizate de stat;

Hotărârea Guvernului nr. 1123/2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal;

Hotărârea Guvernului nr. 1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass);

Hotărârea Guvernului nr. 128/2014 privind platforma tehnologică guvernamentală comună (MCloud);

Hotărârea Guvernului nr. 405/2014 privind serviciul electronic guvernamental integrat de semnătură electronică (MSign);

Hotărârea Guvernului nr. 708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog);

Hotărârea Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat;

Hotărârea Guvernului nr. 211/2019 privind platforma de interoperabilitate (MConnect);

Hotărârea Guvernului nr. 376/2020 pentru aprobarea Conceptului serviciului guvernamental de notificare electronică (MNotify) și a Regulamentului privind modul de funcționare și utilizare a serviciului guvernamental de notificare electronică (MNotify);

Hotărârea Guvernului nr. 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental și modificarea Hotărârii Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat;

Hotărârea Guvernului nr.323/2021 pentru aprobarea Conceptului Sistemului informațional „Catalogul semantic” și a Regulamentului privind modul de ținere a Registrului format de Sistemul informațional „Catalogul semantic”;

Hotărârea Guvernului nr. 650/2023 cu privire la aprobarea Strategiei de transformare digitală a Republicii Moldova pentru anii 2023-2030;

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

Hotărârea Guvernului nr. 562/2025 cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice;

Hotărârea Guvernului nr. 677/2025 cu privire la consolidarea accesului la serviciile publice electronice în cadrul Portalului guvernamental integrat EVO utilizat la prestarea serviciilor publice electronice și aprobarea măsurilor necesare pentru implementarea modelului unitar de design.

14. La elaborarea și implementarea SI RSIC se vor respecta următoarele standarde tehnice:

14.1. Standardul Republicii Moldova SM EN ISO 9001:2015 „Sisteme de management al calității. Cerințe”;

14.2. Standardul Republicii Moldova SM ISO/CEI/IEEE 15288:2015 „Ingineria sistemelor și software-ului. Procesele ciclului de viață ale sistemului”;

14.3. Standardul Republicii Moldova SM EN ISO/IEC 27002:2017 „Tehnologia informației. Tehnici de securitate. Cod de bună practică pentru managementul securității informației”;

14.4. Standardul Republicii Moldova SM ISO/IEC 27005:2018 „Tehnologia informației. Tehnici de securitate. Managementul riscului securității informației”.

IV. SPAȚIUL FUNCȚIONAL AL SI RSIC

15. Funcțiile de bază ale SI RSIC sunt:

15.1. formarea resursei informaționale. Funcțiile de bază în procesul de formare a bazei de date a SI RSIC sunt cele de înregistrare, actualizare a datelor și scoaterea din evidență a obiectelor informaționale;

15.2. jurnalizarea evenimentelor. Orice acțiune a utilizatorilor se documentează în registre electronice speciale, arătând momentul și utilizatorul care a efectuat acțiunea. Pentru fiecare acțiune a utilizatorului se salvează în evenimentul jurnalizat datele care au fost modificate. SI RSIC jurnalizează evenimentele de business critice prin intermediul serviciului electronic guvernamental de jurnalizare (MLog). Acțiunile care sunt jurnalizate prin intermediul serviciului electronic guvernamental de jurnalizare (MLog) pot fi configurate în opțiunile de administrare. SI RSIC jurnalizează local evenimentele ce țin de buna funcționare a RSIC;

15.3. organizarea asigurării informaționale prin oferirea accesului la datele din SI RSIC utilizatorilor autentificați. Fiecare utilizator urmează să utilizeze datele din SI RSIC doar în scopuri legale și în conformitate cu drepturile atribuite;

15.4. asigurarea calității și consistenței informației.

16. Contururile funcționale principale ale SI RSIC sunt:

16.1. Conturul „Sistem de alertă timpurie” – totalitatea procedurilor și sistemelor tehnice care au rolul de a identifica premisele de apariție a incidentelor cibernetice și de a avertiza în cazul producerii acestora. Prin funcționalul său, conturul respectiv va asigura colectarea și sistematizarea datelor recepționate din partea entităților responsabile aferente anomaliilor parvenite din diferite surse, în scopul prelucrării ulterioare. Acest contur realizează următoarele funcții:

16.1.1. colectarea metadatelor aferente anomaliilor și alertelor parvenite de la entitățile responsabile, precum și prelucrarea și sistematizarea datelor;

16.1.2. corelarea alertelor din diferite surse și interfețe;

16.1.3. publicarea alertelor și atenționărilor privind apariția unor activități premergătoare atacurilor cibernetice.

16.2. conturul „Platforma de evidență și management al incidentelor cibernetice” – platforma asigură preluarea informațiilor aferente incidentelor cibernetice din documentele de intrare sau din cadrul conturului funcțional „Sistem de alertă timpurie”.

Conturul realizează următoarele funcții:

16.2.1. formarea bazei de date a SI RSIC. Se asigură evidența primară a incidentelor cibernetice și actualizarea sistematică a bazei de date a incidentelor cibernetice, la modificarea sau completarea datelor obiectelor de evidență;

16.2.2. asigurarea informațională. Informația se pune la dispoziția autorităților competente;

16.2.3. gestionarea incidentelor cibernetice. Se asigură înregistrarea, clasificarea, analiza incidentelor cibernetice. De asemenea, are loc evidența amenințărilor și vulnerabilităților în spațiul cibernetic și a incidentelor cibernetice identificate sau raportate, a tehnicilor și tehnologiilor folosite pentru atacuri cibernetice;

16.2.4. asigurarea răspunsului la incidente cibernetice;

16.2.5. recepționarea raportărilor privind incidentele cibernetice care afectează sistemele informatice și rețelele furnizorilor se servicii;

16.2.6. furnizarea entităților care au făcut raportarea informațiilor relevante în ceea ce privește acțiunile ulterioare raportării;

16.2.7. întocmirea datelor statistice și elaborarea rapoartelor aferente incidentelor cibernetice;

16.3. Conturul „Platforma schimb de informații” – asigură comunicarea interinstituțională între ASC, I.P. STISC și CERT sectoriale, precum și cu furnizorii de servicii din sectoarele critice. Platforma asigură funcționalitatea comunicării măsurilor necesare pentru prevenirea și răspunsul la incidente cibernetice. Totodată, platforma asigură accesul la materiale precum ghidurile de securitate, bunele practici și recomandările, informații privind riscurile cibernetice care pot afecta sistemele informatice și rețelele.

Conturul realizează următoarele funcții:

16.3.1. comunicarea informațiilor privind amenințările, vulnerabilitățile în spațiul cibernetic, riscurile cibernetice și măsurile de protecție necesare;

16.3.2. comunicarea informațiilor privind rezultatele analizei incidentelor cibernetice, cu respectarea prevederilor acordurilor de cooperare;

16.3.3. informarea privind desfășurarea exercițiilor și a atelierelor de lucru în domeniul securității cibernetice;

16.3.4. accesarea ghidurilor de securitate cibernetică și a recomandărilor de soluționare a incidentelor cibernetice.

16.4. conturul „Administrare și Control”, care asigură următoarele funcții:

16.4.1. administrarea bazei de date;
16.4.2. asigurarea integrității logice a SI RSIC;
16.4.3. auditarea și inspecția activităților din cadrul SI RSIC;
16.4.4. păstrarea istoriei modificărilor și activităților SI RSIC;
16.4.5. colectarea statisticii și raportarea;
16.4.6. determinarea nivelului de acces al utilizatorilor;
16.4.7. asigurarea securității și protecției informației;
16.4.8. jurnalizarea evenimentelor de sistem;
16.4.9. monitorizarea performanței SI RSIC;
16.4.10. suport tehnic și mentenanță.

17. SI RSIC stabilește interconexiunea modulelor de lucru și urmează să îndeplinească, în primul rând, funcțiile specifice determinate de obiectivele, scopurile și destinația prezentului Concept.

V. STRUCTURA ORGANIZAȚIONALĂ A SI RSIC

18. Funcțiile de bază privind formarea și exploatarea SI RSIC sunt repartizate între posesor, deținător, utilizator, registratori, furnizor al datelor resursei informaționale.

19. Proprietarul SI RSIC este statul.

20. Posesorul SI RSIC este ASC, care are drept de gestionare și de utilizare a datelor și a resurselor informaționale și exercită atribuțiile deținătorului și administratorului tehnic al sistemului.

21. Registratorii SI RSIC sunt:

ASC, care înregistrează incidentele, alertele și vulnerabilitățile cibernetice din sectorul public și privat la nivel național.

I.P „STISC”, care înregistrează incidentele și alertele cibernetice din sectorul guvernamental;

CERT sectoriale, care înregistrează incidentele și alertele cibernetice din sectorul gestionat.

22. Dacă legea nu prevede altfel, în baza acordului exprimat în scris al posesorului registrului, atribuțiile registratorului pot fi exercitate, pe baze contractuale, de către o altă persoană, denumită subregistrator.

23. Furnizorii datelor RSIC sunt furnizorii de servicii din sectoarele critice identificați în baza prevederilor Legii nr. 48/2023 privind securitatea cibernetică și Hotărârii Guvernului nr. 860/2024 cu privire la identificarea furnizorilor de servicii.

24. Destinatari ai datelor RSIC sunt ASC, I.P. „STISC”, CERT sectoriale, furnizorii de servicii din sectoarele critice identificați în baza prevederilor Legii nr. 48/2023 privind securitatea cibernetică și Hotărârii Guvernului nr. 860/2024 cu privire la identificarea furnizorilor de servicii, autoritățile publice cu atribuții de asigurare a securității statului, precum și alte entități publice care dețin drept de acces conform prevederilor cadrului normativ în vigoare.

25. Utilizatorii SI RSIC sunt:

25.1. utilizatori interni din cadrul ASC, I.P. „STISC” și CERT sectoriale desemnați de posesor – utilizatori cu drepturi depline asupra datelor și funcționalităților disponibile ale SI RSIC;

25.2. registrator – utilizator care operează, introduce sau modifică datele din cadrul SI RSIC, dar nu configurează însuși funcționalitățile sistemului;

25.3. vizitator – utilizator care are acces la vizualizarea informației, fără drepturi de a introduce/modifica/șterge date din cadrul sistemului.

VI. CLASIFICAREA DOCUMENTELOR SI RSIC

26. În cadrul SI RSIC sunt folosite următoarele categorii de documente:

26.1. documente de intrare – în baza cărora sunt înregistrate incidentele cibernetice, alertele și vulnerabilitățile raportate;

26.2. documente interne – informațiile și rapoartele generate de instrumentele de lucru, rezultatele preventive ale procesării datelor de intrare, ce urmează a fi prelucrate de sistem pentru generarea documentelor de ieșire;

26.3. documente de ieșire – documente obținute în urma funcționării sistemului, precum rapoarte, statistici, diagrame aferente incidentelor cibernetice, alertelor și vulnerabilităților înregistrate;

26.4. documente tehnologice – care conțin informații ce descriu procesele tehnologice, precum instrucțiunile de lucru.

27. Din categoria documentelor de intrare fac parte: notificările incidentelor, alertelor și vulnerabilităților cibernetice, rapoartele preliminare și finale privind incidentele, alertele și vulnerabilitățile cibernetice, informațiile furnizate de la conturul funcțional

„Sistem de alertă timpurie”, precum și informațiile furnizate prin canalele de comunicare ale conturului funcțional „Platforma schimb de informații”.

28. Conținutul formularelor de notificare a incidentelor, alertelor și vulnerabilităților cibernetice, precum și conținutul rapoartelor preliminare și finale privind incidentele, alertele și vulnerabilitățile cibernetice se aprobă prin ordinul Directorului ASC.

29. Fiecare obiect informațional înregistrat va stoca istoria modificărilor, documentele interne aferente prelucrării informațiilor de intrare, precum și documentele de ieșire generate în final de SI RSIC.

30. Din categoria documentelor interne fac parte rapoartele de analiză generate de instrumentele de lucru ale conturului funcțional „Platforma de evidență și management al incidentelor cibernetice”.

31. Sistemul include o serie de documente și mijloace tehnologice, precum: lista utilizatorilor și drepturilor acestora, versiunile documentelor și modificările acestora; rapoartele și statisticile agregate.

32. Documentele de ieșire ale SI RSIC sunt: informațiile aferente statutului incidentelor cibernetice, alertelor și vulnerabilităților și recomandările emise de către specialiștii ASC, I.P. „STISC” și CERT sectoriale (ex.: bune practici, anexe aferente incidentelor notificate).

VII. SPAȚIUL INFORMAȚIONAL AL SI RSIC

33. Obiectele informaționale de bază ale SI RSIC sunt:

33.1. incident cibernetic;
33.2. alertă cibernetică;
33.3. vulnerabilitate cibernetică.

34. Identificatorii obiectelor informaționale sunt constituiți din numărul de ordine atribuit de SI RSIC.

35. Scenariul de bază reprezintă lista evenimentelor aferente obiectelor informaționale.

36. Scenariile referitoare la obiectul informațional „ Incident cibernetic” sunt:

36.1. punerea inițială în evidență, realizată de către registrator, la recepționarea notificării privind incidentul cibernetic;

36.2. analiza datelor din documentele de intrare, inclusiv cu suportul instrumentelor de analiză disponibile în cadrul SI RSIC, în scopul oferirii suportului și remedierii incidentului cibernetic în caz de necesitate, conform procedurilor operaționale aprobate prin ordinul Directorului ASC.

36.3. analiza complexității incidentului cibernetic și necesității escaladării către entitățile publice care au atribuții de asigurare a securității statului.

În scenariul escaladării, registratorul incidentului cibernetic consemnează prin comentariu motivul escaladării și inițiază remiterea cazului către Centrul Național de Management al Crizelor. Cazul incidentului cibernetic poate fi închis ulterior de către registrator în baza solicitării Centrului Național de Management al Crizelor.

36.4. actualizarea datelor, realizată de către registrator, la recepționarea raportului preliminar și final privind incidentul cibernetic, precum și în cazul necesității modificării sau completării informației despre incidentul cibernetic;

36.5. transmiterea în arhiva electronică, realizată de către registrator, în cazul soluționării incidentului cibernetic.

37. Scenariile referitoare la obiectul informațional „Alertă cibernetică" va conține 3 scenarii de bază:

37.1. alertă pozitivă – se referă la activități anomalice recepționate sau raportate prin căile de comunicare aprobate, care au potențial de a degenera în vulnerabilitate cibernetică sau incident cibernetice. În scenariul respectiv, utilizatorii desemnați responsabili de această alertă în cadrul SI RSIC vor emite notificări în cadrul Platformei de evidență și management al incidentelor cibernetice și vor analiza activitatea anomalică în scopul identificării potențialelor riscuri cibernetice asociate alertei respective;

37.2. alertă fals-pozitivă – se referă la cazul în care alertele recepționate prezintă activități anomalice, dar care nu reprezintă risc de securitate sau care nu au potențial de a deveni vulnerabilitate în spațiul cibernetic sau incident cibernetic. În acest scenariu, actorii desemnați responsabili de alerta respectivă în cadrul SI RSIC vor închide alerta de securitate în cadrul SI RSIC, cu mențiunile de rigoare în comentariu;

37.3. alertă degenerată în incident cibernetic – se referă la cazul în care activitatea anomalică raportată este rezultatul desfășurării unui atac cibernetic în timp real, ce devine incident cibernetic. În acest scenariu, responsabilii de incidentul cibernetic identificat vor gestiona alertele, asociind, în cadrul SI RSIC, datele stocate despre alertă către cazul incidentului cibernetic deschis. Ca urmare, alerta respectivă va obține statutul de alertă închisă, cu menționarea în comentarii a identificatorului cazului incidentului cibernetice asociat.

38. Scenariile referitoare la obiectul informațional „Vulnerabilitate cibernetică" sunt:

38.1. punerea inițială în evidență, realizată de către registrator, la recepționarea notificării privind vulnerabilitatea cibernetică;

38.2. analiza datelor din documentele de intrare, identificarea entităților relevante implicate în procesul de divulgare, inclusiv organizațiile responsabile pentru produsele sau serviciile TIC afectate;

38.3. evaluarea și prioritizarea vulnerabilităților raportate, în funcție de nivelul de risc, potențialul de exploatare și impactul asupra infrastructurii critice sau serviciilor esențiale;

38.4. actualizarea datelor, realizată de către registrator, în cazul modificării sau completării informației despre vulnerabilitatea cibernetică;

38.5. transmiterea în arhiva electronică, realizată de către registrator, în cazul remedierii vulnerabilității cibernetice.

39. Obiectele informaționale vor conține, în mod obligatoriu, următoarele atribute și date ce le caracterizează:

39.1. Atributele obiectului informațional „incident cibernetic":

39.1.1. datele de identificare a furnizorului de servicii vizat de atacul cibernetic;

39.1.2. elementele de identificare a rețelelor și/sau sistemelor informatice afectate;

39.1.3. descrierea incidentului;

39.1.4. data și ora detectării incidentului;

39.1.5. clasificarea incidentului;

39.1.6. măsurile preliminare și finale întreprinse pentru soluționarea incidentului cibernetic;

39.1.7. metadate de trafic aferente comunicațiilor electronice;

39.1.8. date aferente tehnicilor și tehnologiilor folosite în cadrul atacului cibernetic;

39.1.9. alte date aferente incidentului cibernetic, preluate din documentele de intrare specificate la Capitolul VI;

39.2. Atributele obiectului informațional „alertă cibernetică”:

39.2.1. elementele de identificare a rețelelor și/sau sistemelor monitorizate;

39.2.2. descrierea alertei;

39.2.3. data și ora emiterii;

39.2.4. clasificarea alertei;

39.2.5. măsurile preliminare și finale întreprinse pentru preîntâmpinarea incidentelor cibernetice;

39.2.6. recomandările privind reducerea riscurilor de apariție a incidentelor cibernetice;

39.2.7. metadate de trafic aferente comunicațiilor electronice;

39.2.8. alte date aferente alertei cibernetice, preluate din documentele de intrare specificate la Capitolul VI;

39.3. Atributele obiectului informațional „vulnerabilitate cibernetică”:

39.3.1. date de identificare a organizației responsabile – producător, furnizor, dezvoltator sau administrator al unui produs sau serviciu TIC afectat de vulnerabilitate;

39.3.2. date de identificare a produsului al tehnologiei informației și comunicațiilor (produs TIC) afectat de vulnerabilitate;

39.3.3. date de identificare a raportorului – orice persoană fizică sau juridică, inclusiv cercetători, specialiști ori alți participanți în domeniul securității cibernetice, care notifică, în mod voluntar și cu bună credință, o vulnerabilitate identificată într-un produs sau serviciu TIC;

39.3.4. date de identificare a cercetătorului sau participantului în domeniul securității – persoană fizică sau juridică care deține experiența, competențele și/sau certificările necesare și care, acționând cu bună-credință și în conformitate cu cadrul normativ, identifică, evaluează și raportează vulnerabilități în produsele și serviciile TIC, în scopul îmbunătățirii securității acestora, fiind înregistrată de către coordonatorul procesului de divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice;

39.3.5. date privind divulgarea coordonată a vulnerabilităților – proces structurat prin care informațiile privind vulnerabilitățile sunt transmise producătorului sau furnizorului de produse TIC ori de servicii TIC, potențial vulnerabile, într-un mod care să le permită acestora să diagnosticheze și să remedieze vulnerabilitățile respective înainte ca informațiile detaliate privind vulnerabilitatea să fie dezvăluite unor părți terțe sau publicului;

39.3.6. date privind divulgarea publică – comunicarea înainte de remediere a informațiilor despre vulnerabilitate către publicul larg sau către o audiență extinsă, inclusiv prin publicarea în baze de date publice, forumuri, platforme de social media sau mass-media;

39.3.7. informații de remediere - procesul de eliminare sau atenuare a vulnerabilității prin implementarea de corecții, versiuni noi, actualizări de securitate sau alte măsuri tehnice și organizatorice;

39.3.8. alte date aferente vulnerabilității cibernetice, preluate din documentele de intrare specificate la Capitolul VI;

40. În vederea asigurării veridicităţii şi reducerii volumului informaţiei păstrate în SI RSIC, precum şi pentru o clasificare corectă a obiectelor în acesta, se utilizează sistemul de clasificatoare elaborate în baza clasificatoarelor naţionale ale Republicii Moldova şi a actelor UE:

40.1. clasificatoarele internaţionale;

40.2. clasificatoarele naţionale ale Republicii Moldova;

40.3. clasificatoarele intrasistemice, elaborate în baza clasificatoarelor internaţionale, a clasificatoarelor naţionale ale Republicii Moldova şi a actelor UE.

Clasificatoarele intrasistemice se elaborează şi se utilizează în cadrul SI RSIC doar în cazurile absenţei clasificatoarelor naţionale şi internaţionale aprobate.

41. SI RSIC va prelua date aferente obiectelor informaționale din alte sisteme informaționale de stat, precum:

41.1. Registrul de stat al unităților de drept – pentru recepționarea datelor de identificare a persoanelor juridice;

41.2. Registrul de stat al populației – pentru recepționarea datelor de identificare a persoanelor fizice.

42. SI RSIC va fi integrat cu următoarele sisteme informaționale partajate relevante:

42.1. platforma de interoperabilitate (MConnect) – pentru recepționarea datelor din alte sisteme și resurse informaționale de stat;

42.2. serviciul electronic guvernamental de autentificare și control al accesului (MPass) – pentru autentificarea și controlul accesului utilizatorilor;

42.3. serviciul electronic guvernamental de jurnalizare (MLog) – pentru jurnalizarea evenimentelor de business critice;

42.4. serviciul electronic guvernamental integrat de semnătură electronică (MSign) – pentru aplicarea semnăturii electronice în cadrul proceselor de business ale SI RSIC;

42.5. serviciul guvernamental de notificare electronică (MNotify) – pentru notificarea utilizatorilor autorizați;

42.6. Sistemul informațional automatizat „Registrul împuternicirilor de reprezentare în baza semnăturii electronice” (MPower) – pentru verificarea împuternicirilor de reprezentare a utilizatorilor necesare pentru autorizarea acțiunilor acestora;

42.7. portalul guvernamental unic de date deschise (PDGD) – pentru publicarea seturilor publice de date produse în cadrul fluxurilor de lucru ale SI RSIC.

43. Pentru asigurarea funcționalității eficiente și neîntrerupte a SI RSIC, schimbul informațional de date din cadrul sistemului informațional este asigurat în regim nonstop.

44. În scopul asigurării interoperabilității și a schimbului de date cu alte sisteme și resurse informaționale de stat, ASC înregistrează activele semantice utilizate în Sistemul informațional „Catalogul semantic.

VIII. SPAȚIUL TEHNOLOGIC AL SI RSIC

45. SI RSIC este proiectat ca sistem modular compatibil cu tehnologii de „cloud computing” (nor informațional), care asigură posibilitatea dezvoltării sale fără perturbarea continuității funcționării.

46. SI RSIC este găzduit pe platforma tehnologică deținută de ASC. Toate datele sistemului se depozitează într-o bază de date centralizată.

47. Arhitectura complexului software-hardware trebuie să corespundă următoarelor principii:

47.1. implementarea unei soluții SOA (service oriented architecture –arhitectură software bazată pe servicii), care oferă posibilitatea realizării unor funcții ale sistemului în cadrul altor procese sau permite extinderea sistemului cu noi funcționalități fără a perturba funcționarea sistemului;

47.2. acceptarea soluțiilor care vor furniza o interfață web pentru utilizatorii sistemului;

47.3. minimizarea numărului diferitelor tehnologii și produse care oferă aceleași funcționalități sau sunt similare după destinație;

47.4. implementarea funcționalităților de notificare prin e-mail;

47.5. asigurarea confidențialității și integrității datelor sistemului prin limitarea accesului în 2 etape: asigurarea accesului doar prin autentificare, precum și stabilirea individuală a drepturilor de acces a utilizatorilor.

48. Principale tipuri de standarde utilizate:

48.1. standardele datelor;
48.2. standardele metadatelor;
48.3. standardele schimbului de informații;
48.4. standardele de calitate;
48.5. standardele de securitate;
48.6. standardele de multilingvism.

49. Conformitatea cu aceste standarde va consta în:

49.1. susținerea interfeței browserului pentru accesare;
49.2. XML ca mijloc principal pentru integrarea datelor;
49.3. utilizarea standardelor Internet și WWW-HTML, TCP/IP, SMTP;
49.4. utilizarea standardelor naționale și internaționale ISO.

50. Lista produselor hardware şi software utilizate la crearea infrastructurii informaţionale și de comunicații electronice a SI RSIC este determinată de către ASC, de comun acord cu furnizorul soluției de implementare a sistemului informaţional.

Prezența componentelor software și a mijloacelor tehnologice în complexul informațional respectiv este stabilită la etapa elaborării sarcinii tehnice a sistemului.

IX. ASIGURAREA SECURITĂȚII INFORMAȚIONALE A SI RSIC

51. Securitatea SI RSIC presupune starea de protecţie a resurselor şi infrastructurii informaţionale, prin care se asigură veridicitatea, integritatea, confidenţialitatea,

disponibilitatea şi autenticitatea resurselor informaționale. Sistemul securităţii informaţionale reprezintă totalitatea acțiunilor juridice, organizatorice, economice şi tehnologice orientate spre prevenirea pericolelor asociate resurselor şi infrastructurii informaţionale.

52. Securitatea informațională a SI RSIC include o serie de măsuri de prevenție, măsuri de reacție și măsuri de contracarare, politici interne, tehnologii, structuri responsabile abilitate cu atribuții și funcții în sistem.

53. Pericol asociat securităţii informaţionale reprezintă un eveniment sau o acţiune potenţial posibilă, orientată spre cauzarea unui prejudiciu resurselor sau infrastructurii informaţionale.

Principalele pericole pentru securitatea informaţională a SI RSIC sînt:

53.1. colectarea şi/sau utilizarea ilegală a informaţiei;
53.2. încălcarea tehnologiei de prelucrare a informaţiei;
53.3. încălcarea confidenţialităţii informaţiei;
53.4. încălcarea integrităţii logice şi a integrităţii fizice a informaţiei;
53.5. încălcarea funcţionării infrastructurii informaţionale;
53.6. acţiunea fizică asupra componentelor infrastructurii informaţionale;
53.7. inserarea în produsele software şi hardware a componentelor care realizează funcţii neprevăzute în documentaţia cu privire la aceste produse;
53.8. elaborarea şi răspîndirea programelor care afectează funcţionarea normală a sistemelor informaţionale şi de telecomunicaţii, precum şi a sistemelor securităţii informaţionale;
53.9. nimicirea, deteriorarea şi suprimarea radioelectronică sau distrugerea mijloacelor şi sistemelor de prelucrare a informaţiei, de telecomunicaţii şi comunicaţii;
53.10. influenţa asupra sistemelor cu parolă-cheie de protecţie a sistemelor automatizate de prelucrare şi transmitere a informaţiei;
53.11. compromiterea cheilor şi mijloacelor de protecţie criptografică a informaţiei;
53.12. scurgerea informaţiei prin canale tehnice;
53.13. implementarea dispozitivelor electronice pentru interceptarea informaţiei în mijloacele tehnice de prelucrare, păstrare şi transmitere a informaţiei prin canalele de comunicaţii, precum şi în încăperile de serviciu ale autorităţilor;
53.14. nimicirea, deteriorarea, distrugerea sau sustragerea suporturilor de informaţie mecanice sau a altor suporturi;
53.15. interceptarea informaţiei în reţelele de transmitere a datelor şi în liniile de comunicaţii, decodificarea acestei informaţii şi/sau răspîndirea informaţiei false;
53.16. utilizarea tehnologiilor informaţionale necertificate, a mijloacelor de protecţie a informaţiei, a mijloacelor de informatizare, de telecomunicaţii şi comunicaţii necertificate în procesul creării şi dezvoltării infrastructurii informaţionale;
53.17. accesul neautorizat la resursele informaţionale;
53.18. încălcarea restricţiilor legale privind accesul şi divulgarea informaţiei.

54. Pentru asigurarea implementării sistemului eficient de asigurare a securităţii informaționale ale obiectelor SI RSIC sînt necesare:

54.1. identificarea cerinţelor securităţii informaţiei specifice pentru fiecare obiect al protecţiei în cauză;
54.2. respectarea cerinţelor actelor normative naţionale şi internaţionale;

54.3. utilizarea celor mai bune practici (standarde, metodologii) pentru asigurarea securităţii informaţionale;

54.4. determinarea subdiviziunilor responsabile pentru asigurarea securităţii informaţionale;

54.5. distribuirea între subdiviziuni a sferelor de responsabilitate în asigurarea securităţii informaţionale;

54.6. în baza gestionării riscurilor de securitate a informaţiei, determinarea cerinţelor tehnice și organizatorice, care constituie politica de securitate informaţională a obiectului protecţiei;

54.7. realizarea cerinţelor politicii de securitate informaţională prin implementarea metodelor software şi hardware şi a mijloacelor de protecţie a informaţiei corespunzătoare;

54.8. realizarea sistemului de management al securităţii informaţionale.

55. Sarcinile de bază ale asigurării securităţii informaţionale sînt:

55.1. asigurarea confidenţialităţii informaţiei, prevenirea accesului la informaţie fără drepturi şi împuterniciri corespunzătoare;

55.2. asigurarea integrităţii logice a informaţiei, prevenirea introducerii, actualizării şi nimicirii neautorizate a informaţiei;

55.3. asigurarea integrităţii fizice a informaţiei;

55.4. asigurarea protecţiei infrastructurii informaţionale împotriva deteriorării şi tentativelor de modificare a funcţionării.

56. Sistemul asigură următoarele obiective de securitate:

56.1. *autentificarea, exclusiv prin intermediul serviciului MPass* – garantează că sistemul va fi accesibil doar utilizatorilor cu o identitate verificată și confirmată;

56.2. *autorizarea* – garantează că utilizatorii autentificați pot accesa serviciile și datele care corespund drepturilor lor de acces;

56.3. *confidențialitatea* – garantează că datele înregistrate nu pot fi accesate de o terță parte neautorizată;

56.4. *integritatea* – garantează că datele nu au fost modificate sau alterate de o terță parte neautorizată.

57. Mecanismele tehnologice de bază pentru asigurarea protecției și securității datelor sunt:

57.1. autentificarea şi autorizarea;
57.2. controlul accesului;
57.3. dirijarea centralizată și controlul accesului la date;
57.4. înregistrarea acţiunilor şi auditul;
57.5. accesul la date doar prin interfața unică de obiect;
57.6. criptarea informaţiei;
57.7. analizarea și modelarea fluxurilor informaționale (sistemele CASE);
57.8. monitorizarea reţelelor;
57.9. detectarea şi prevenirea intruziunilor (IDS/IPS);
57.10. prevenirea scurgerii informaţiei confidenţiale (sistemului DLP);
57.11. analizatori de protocoale;
57.12. mijloacele de programare antivirus;
57.13. ecrane între reţele (firewall);
57.14. sistemele copierii de rezervă;

57.15. sistemele de alimentare fără întrerupere cu energie electrică;
57.16. organizarea pazei, securității;
57.17. mijloacele de prevenire a accesului neautorizat în clădiri și încăperi;
57.18. mijloacele de analiză a sistemelor de protecţie;
57.19. alte mecanisme.

58. Utilizarea mecanismelor de asigurare a securităţii informaţionale se planifică la etapa de proiectare a sistemelor şi infrastructurii informaţionale.

59. Securitatea informațională presupune protejarea informației prin aplicarea unor măsuri la nivel logic, prin utilizarea tehnologiilor informaționale. Aceasta include: programele antivirus, delimitarea logică a rețelei, paravanul de protecție (*firewall*), controlul asupra licențelor produselor software.

60. Organizarea sistemului de protecție a datelor cu caracter personal constituie o parte componentă a mecanismului de asigurare a securităţii informaționale a SI RSIC.

61. Sistemul de protecţie a datelor cu caracter personal se constituie în baza:

61.1. raportului privind rezultatele efectuării auditului intern;
61.2. listei datelor cu caracter personal care trebuie să fie protejate;
61.3. actului de clasificare a sistemului informaţional care prelucrează date cu caracter personal;
61.4. modelelor de pericole pentru securitatea datelor cu caracter personal;
61.5. prevederilor privind delimitarea drepturilor de acces la datele cu caracter personal prelucrate;

X. ÎNCHEIERE

62. Prezentul Concept conține descrierea principalelor aspecte organizaționale ce țin de crearea SI RSIC și vine să contribuie la soluționarea unei probleme polivalente: pe de o parte, se elaborează mecanismul care asigură automatizarea proceselor de identificare, înregistrare, clasificare și analiză a incidentelor cibernetice, monitorizarea și evidența alertelor, vulnerabilităților și incidentelor cibernetice identificate sau raportate, iar pe de altă parte, se instituie interacțiunea ASC cu I.P. STISC, CERT sectoriale, precum și furnizorii de servicii din sectoarele critice.

Anexa nr. 2

REGULAMENTUL

Registrului de stat al incidentelor cibernetice

CAPITOLUL I
DISPOZIȚII GENERALE

1. Prezentul Regulament stabilește drepturile și obligațiile subiecților raporturilor juridice aferente creării și ținerii Registrului de stat al incidentelor cibernetică (în continuare – RSIC), modalitatea de ținere a resursei informaționale; procedura de înregistrare, modificare, completare și radiere a datelor; procedura de interacțiune cu furnizorii de date; măsuri privind asigurarea securității RSIC.

2. Registrul de stat al incidentelor cibernetice este un registru departamental de stat și este parte componentă a resurselor informaționale de stat ale Republicii Moldova.

3. Registrul de stat al incidentelor cibernetice constituie unica sursă oficială de date despre incidentele cibernetice, alertele și vulnerabilitățile cibernetice raportate către Agenția pentru Securitate Cibernetică (în continuare - ASC), Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică” (în continuare I.P. STISC) și echipele de răspuns la incidente cibernetice sectoriale (în continuare - CERT sectoriale). Datele registrului se consideră corecte și veridice până la proba contrarie, în modul prevăzut de lege.

4. Accesul la Registrul de stat al incidentelor cibernetice este limitat, iar datele din registru sunt destinate utilizării interne, cu excepția cazului în care cadrul normativ prevede altfel.

5. Noțiunile utilizate în prezentul Regulament sunt cele definite în. Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat, Legea nr. 71/2007 cu privire la registre și Legea nr. 48 din 2023 privind securitatea cibernetică și Conceptul SI RSIC.

CAPITOLUL II
SUBIECȚILOR RAPORTURILOR JURIDICE AFERENTE CREĂRII ȘI ȚINERII RSIC

6. Subiecții raporturilor juridice aferente creării și ținerii RSIC sunt:

6.1. proprietarul;
6.2. posesorul;
6.3. deținătorul;
6.4. registratorul;
6.5. furnizorul datelor;
6.6. destinatarul datelor.

7. Proprietarul RSIC este statul.

8. Posesorul și deținătorul RSIC este Agenția pentru Securitatea Cibernetică (în continuare - ASC), care asigură condițiile juridice, financiare și organizatorice pentru crearea și ținerea RSIC.

9. Registratorii RSIC sunt:

9.1. ASC, care înregistrează incidentele, alertele și vulnerabilitățile cibernetice din sectorul public și privat la nivel național.

9.2. I.P „STISC”, care înregistrează incidentele și alertele cibernetice din sectorul guvernamental;

9.3. CERT departamentale, care înregistrează incidentele și alertele cibernetice din sectorul gestionat.

10. Furnizorii datelor RSIC sunt furnizorii de servicii identificați în baza prevederilor Legii nr. 48/2023 privind securitatea cibernetică și Hotărârii Guvernului nr. 860/2024 cu privire la identificarea furnizorilor de servicii.:

11. Destinatarii datelor sunt ASC, I.P. „STISC”, CERT departamentale, autoritățile publice cu atribuții de asigurare a securității statului, precum și alte entități publice care dețin drept de acces conform prevederilor cadrului normativ în vigoare.

Capitolul III
DREPTURILE, ATRIBUȚIILE ȘI OBLIGAȚIILE SUBIECȚILOR RSIC

12. Subiecții RSIC beneficiază de drepturi de acces în conformitate cu atribuțiile și funcțiile exercitate, nivelul de acces la informație fiind determinat în raport cu responsabilitățile fiecărui participant și cu criteriile de acces stabilite.

13. Accesul la RSIC este structurat pe unități de conținut și reglementat prin atribuirea drepturilor specifice fiecărei categorii de utilizatori.

Secțiunea 1
Drepturile și obligațiile posesorului RSIC

14. Posesorul RSIC are dreptul:

14.1. să elaboreze și să aprobe, în limita competențelor sale, cadrul normativ privind ținerea și utilizarea RSIC;

14.2. să prezinte propuneri privind dezvoltarea RSIC autorității administrației publice centrale de specialitate responsabile de realizarea politicii statului în domeniul securității cibernetice;

14.3. să propună și să implementeze soluții destinate îmbunătățirii și eficientizării procesului de ținere a RSIC.

15. Posesorul RSIC are următoarele obligații:

15.1. să asigure condițiile juridice, organizatorice, tehnice și financiare necesare pentru crearea, funcționarea și ținerea RSIC;

15.2. să organizeze procesul de creare și dezvoltare a Sistemului informațional „Registrul de stat al incidentelor de securitate cibernetică” (SI RSIC);

15.3. să asigure înregistrarea obiectelor supuse evidenței, în conformitate cu cadrul normativ aplicabil;

15.4. să garanteze autenticitatea, plenitudinea, integritatea și actualitatea datelor înscrise în RSIC, prevenind modificările sau accesările neautorizate;

15.5. să adopte și să implementeze măsuri organizatorice și tehnice pentru protejarea și securitatea datelor conținute în RSIC, prevenind accesul neautorizat, pierderea, distrugerea sau modificarea neautorizată a informațiilor;

15.6. să monitorizeze și să reglementeze accesul la datele din RSIC, asigurând respectarea drepturilor de acces pentru destinatarii autorizați, conform prevederilor legale și regulilor aplicabile;

15.7. să asigure corectarea datelor în cazul constatării erorilor sau omisiunilor;

15.8. să utilizeze datele din RSIC exclusiv în scopurile prevăzute de cadrul normativ în vigoare;

15.9. să asigure accesul destinatarilor autorizați la datele din RSIC, în conformitate cu legislația și prezentul Regulament;

15.10.să exercite orice alte atribuții necesare pentru ținerea RSIC, potrivit cadrului normativ aplicabil.

Secțiunea a 2-a

Drepturile și obligațiile deținătorului RSIC

16. Deținătorul RSIC are dreptul:

16.1. să restricționeze temporar accesul la RSIC în cazul unei situații excepționale stabilite conform actelor normative aplicabile, în cazul unor incidente majore sau al existenței unor riscuri semnificative de securitate;

16.2. să supravegheze respectarea regulilor și cerințelor privind ținerea și utilizarea RSIC;

16.3. să solicite de la persoanele responsabile (registratori, furnizori de date) actualizarea sau corectarea informațiilor în RSIC, în cazul identificării unor omisiuni sau erori;

16.4. să suspende dreptul de acces al unui utilizator al RSIC în cazul în care acesta încalcă regulile de acces, cerințele de securitate ori normele legale privind protecția informațiilor.

16.5. să desfășoare alte activități necesare pentru menținerea integrității, securității și utilizării eficiente a RSIC.

17. Deținătorul SI RSIC este obligat:

17.1. să stabilească planuri de dezvoltare ale RSIC în conformitate cu cerințele cadrului normativ aplicabil;

17.2. să gestioneze drepturile de acces ale utilizatorilor, să autorizeze accesul acestora și, după caz, să dispună suspendarea drepturilor de acces în cazul în care acesta încalcă regulile de acces, cerințele de securitate ori normele legale privind protecția informațiilor;

17.3. să asigure păstrarea și protecția datelor din RSIC, prevenind orice acces, modificare sau ștergere neautorizată;

17.4. să acorde suport metodologic și tehnic registratorilor în procesul de introducere a datelor în RSIC, asigurând respectarea cerințelor privind acuratețea, completitudinea și structura informațiilor;

17.5. să asigure veridicitatea și integritatea datelor conținute în RSIC, prevenind omisiunile și erorile în procesul de actualizare;

17.6. să asigure păstrarea și protecția metadatelor din RSIC, prevenind orice pierdere sau modificare neautorizată;

17.7. să acorde suport metodologic și tehnic registratorilor în procesul de înregistrare și actualizare a datelor, respectând standardele tehnice și metodologice aplicabile;

17.8. să elaboreze ți să aprobe ghidul utilizatorului RSIC, oferind instrucțiuni clare privind accesul, utilizarea și administrarea datelor;

17.9. să monitorizeze și să supravegheze activitățile de accesare și utilizare a RSIC pentru a preveni accesările neautorizate, identificând eventualele incidente de securitate;

17.10.să implementeze măsuri organizatorice și tehnice pentru protecția și confidențialitatea informațiilor stocate în RSIC, prevenind distrugerea, modificarea, blocarea, copierea, diseminarea sau alte acțiuni neautorizate, asigurând un nivel corespunzător de securitate în raport cu riscurile asociate prelucrării datelor;

17.11. să exercite și alte atribuții necesare pentru menținerea integrității, securității și funcționării eficiente a RSIC, în conformitate cu actele normative în vigoare.

Secțiunea a 3-a
Drepturile și obligațiile registratorului RSIC

18. Registratorul are dreptul:

18.1. să acceseze RSIC în conformitate cu drepturile de acces stabilite;

18.2. să vizualizeze și să editeze informațiile din RSIC în limitele rolului atribuit și conform competențelor delegate;

18.3. să înainteze posesorului propuneri privind modificarea actelor normative care reglementează ținerea acestuia;

18.4. să solicite și să primească de la posesor și deținător suport metodologic și tehnic privind utilizarea RSIC;

18.5. să înainteze posesorului și deținătorului propuneri privind îmbunătățirea și sporirea eficacității ținerii RSIC;

18.6. să solicite și să primească de la deținător suport metodologic și tehnic privind utilizarea RSIC pentru crearea sau actualizarea metadatelor.

19. Registratorul RSIC este obligat:

19.1. să înregistreze datele în RSIC în conformitate cu prevederile cadrului normativ în vigoare;

19.2. să asigure corectitudinea, autenticitatea și veridicitatea datelor introduse, prevenind erorile și informațiile inexacte;

19.3. să asigure actualizarea în timp real a datelor introduse în RSIC exclusiv în baza informațiilor documentate, recepționate de la deținătorii sau furnizorii de date, utilizând mecanismele de interoperabilitate prevăzute de cadrul normativ în vigoare;

19.4. să întreprindă măsuri pentru prevenirea accesului neautorizat al persoanelor terțe la datele din RSIC;

19.5. să utilizeze informațiile RSIC în exclusivitate conform destinației acestora și în strictă conformitate cu legislația.

Secțiunea a 4-a
Drepturile și obligațiile furnizorului de date

20. Furnizorul de date are dreptul:

20.1. să înainteze posesorului propuneri privind modificarea actelor normative care reglementează ținerea și utilizarea RSIC;

20.2. să înainteze posesorului propuneri privind îmbunătățirea și sporirea eficacității procesului de ținere și utilizare a RSIC.

21. Furnizorul de date este obligat:

21.1. să asigure corectitudinea, autenticitatea, veridicitatea și integritatea datelor furnizate;

21.2. să asigure actualitatea datelor furnizate, conform cerințelor stabilite de cadrul normativ în vigoare;

21.3. să implementeze măsuri organizatorice necesare pentru asigurarea furnizării corecte și sigure a datelor către registratorii RSIC;

21.4. să asigure măsurile necesare pentru protecția și securitatea informațiilor furnizate către RSIC, să documenteze orice încercare de acces neautorizat și să adopte măsurile necesare pentru prevenirea și remedierea incidentelor de securitate.

Secțiunea a 5-a
Drepturile și obligațiile destinatarului datelor din RSIC

22. Destinatarul datelor are dreptul:

22.1. să acceseze și să utilizeze date din RSIC, în conformitate cu drepturile de acces stabilite prin cadrul normativ în vigoare;

22.2. să înainteze posesorului RSIC propuneri privind modificarea actelor normative care reglementează ținerea și utilizarea acestuia;

22.3. să solicite și să primească de la posesorul și de la deținătorul RSIC ajutor metodologic și practic privind utilizarea acestuia;

22.4. să solicite și să primească de la posesorul RSIC informații referitoare la nivelul agreat al serviciilor conform cadrului normativ;

22.5. să solicite și să primească de la posesor accesul la datele/informațiile RSIC în conformitate cu scopul prelucrării și cu rolul atribuit;

22.6. să vizualizeze datele/informațiile/documentele din RSIC în conformitate cu drepturile de acces stabilite în baza atribuțiilor și funcțiilor deținute, fără dreptul de a modifica aceste date/informații/documente;

22.7. să prezinte posesorului RSIC propuneri privind îmbunătățirea și eficientizarea procesului de ținere și utilizare a acestuia.

23. În funcție de rolurile atribuite, destinatarul este obligat:

23.1. să asigure confidențialitatea datelor obținute din RSIC în conformitate cu normele legale privind protecția informației și a datelor cu caracter personal;

23.2. să asigure accesarea și utilizarea datelor din RSIC în conformitate cu rolul atribuit și cu scopul legitim de utilizare a acestora;

23.3. să implementeze măsuri pentru protecția și securitatea informațiilor din RSIC, să documenteze incidentele de securitate și să întreprindă măsurile necesare pentru prevenirea și remedierea acestora;

23.4. să respecte regulile de acces și exploatare a RSIC, asigurând utilizarea corectă și protejată a informațiilor;

23.5. să utilizeze informația obținută doar în scopurile stabilite de legislație;

23.6. să informeze posesorul RSIC, în termen de o zi lucrătoare, despre orice incident care ar putea afecta negativ exercitarea funcțiilor sale sau utilizarea RSIC.

24. Utilizarea RSIC fără autorizare nominală este interzisă și urmează a fi considerată ca acces neautorizat. Introducerea și/sau modificarea informațiilor în RSIC de pe un nume sau profil de utilizator străin este interzisă, urmând a fi considerată ca acces neautorizat. Utilizatorii urmează să se asigure de faptul că profilul de utilizator, precum și semnătura electronică sunt confidențiale.

25. Dreptul de acces la RSIC poate fi limitat, suspendat sau retras de către deținător, în condițiile prezentului Regulament. Suspendarea ori revocarea dreptului de acces al salariatului utilizatorului se dispune de către deținător în următoarele situații:

25.1. la încetarea raporturilor de serviciu sau de muncă ale salariatului, ori la suspendarea temporară a acestora (de exemplu, concediu neplătit, detașare), caz în care accesul se retrage corespunzător duratei/necesității;

25.2. la modificarea atribuțiilor de serviciu/de muncă ale salariatului, când noile responsabilități nu mai necesită acces la datele din RSIC;

25.3. dacă posesorul sau deținătorul constată că salariatul a accesat RSIC fără autorizare ori a permis accesul nesancționat al altor persoane;

25.4. dacă posesorul sau deținătorul constată încălcarea măsurilor de securitate de către salariat, punând în pericol integritatea sau confidențialitatea datelor.

26. Lucrările de mentenanță planificate în complexul de mijloace software a SI RSIC se efectuează după notificarea registratorilor de către deținător cu cel puțin două zile lucrătoare înainte de începerea lucrărilor, cu indicarea termenului de finalizare a acestora. Lucrările de mentenanță neplanificate se efectuează la solicitarea utilizatorilor și coordonarea prealabilă cu posesorul în situația nefuncționării sau funcționării necorespunzătoare a complexului de mijloace software.

Capitolul IV

ȚINEREA ȘI ASIGURAREA OPERĂRII RSIC

Secțiunea 1

Modalitatrea de ținere a RSIC

27. Datele din RSIC nu sunt publice și pot fi accesate doar în condițiile prevăzute de cadrul normativ în vigoare.

28. RSIC se ține în limba română.

29. Principalele procese implicate în ținerea RSIC sunt: înregistrarea inițială a datelor, actualizarea periodică pentru menținerea corectitudinii și relevanței informațiilor, precum și arhivarea acestora.

30. Înregistrarea datelor în RSIC se efectuează de către registrator prin intermediul SI RSIC, în baza informației parvenite de la furnizor.

31. Înainte de înregistrare, registratorul verifică datele și aprobă sau respinge înregistrarea, asigurându-se că acestea respectă cerințele aprobate pentru colectare și/sau instrucțiunile stabilite la momentul înregistrării. Aceste cerințe includ componența, exhaustivitatea, calitatea, formatul, conformitatea cu reglementările legale și tehnice, precum și corectitudinea atributelor datelor.

32. În cazul depistării unor erori sau inexactități, registratorul este obligat să informeze furnizorul datelor și deținătorul.

33. Dacă furnizorul de date constată necesitatea rectificării unor informații eronate sau inexacte, acesta notifică registratorul din cadrul RSIC, care va efectua corectările necesare și va informa furnizorul despre modificările realizate.

34. Toate înregistrările și modificările operate în RSIC sunt păstrate în ordine cronologică, asigurând posibilitatea obținerii istoricului datelor pentru o perioadă determinată.

35. SI RSIC dispune de mecanisme de gestionare a versiunilor informațiilor stocate în RSIC, care asigură păstrarea unui istoric al fiecărei modificări efectuate.

36. Radierea datelor incorecte și neveridice din RSIC se efectuează de către registratorul care gestionează datele respective, în baza documentelor confirmative, cu respectarea strictă a cerințelor privind protecția datelor.

37. RSIC permite realizarea unor analize complexe ale informațiilor, precum și generarea rapoartelor și a indicatorilor de performanță. Accesul la rapoarte și la indicatorii de performanță este disponibil pentru utilizatorii RSIC, în funcție de rolurile atribuite și drepturile de acces stabilite.

38. Păstrarea și administrarea datelor din RSIC este asigurată de către deținător până la adoptarea deciziei de lichidare a acestuia. În cazul lichidării acestuia, datele și documentele conținute în RSIC se transmit în arhivă conform legislației.

Secțiunea 2

Proceduri operaționale privind gestionarea alertelor și incidentelor cibernetice

39. În scenariul de bază privind gestiunea alertelor și incidentelor cibernetice se vor parcurge următoarele etape principale:

39.1. identificarea și notificarea alertelor/incidentelor cibernetice;

39.2. înregistrarea alertei/incidentului cibernetic și asignarea subdiviziunii/persoanei responsabile;

39.3. prioritizarea procesării alertei/incidentului cibernetic conform evaluării impactului real sau posibil;

39.4. investigarea alertei/incidentului cibernetic și identificarea cauzei producerii acestuia, inclusiv a măsurilor de prevenire care să asigure depistarea la timp a unor incidente similare;

39.5. solicitarea, după caz, de la furnizorul de date a informațiilor suplimentare privind incidentul sau alerta cibernetică raportată, cu specificarea termenului de furnizare al acestora;

39.6. notificarea permanentă despre modificarea statutului alertei/incidentului cibernetic, precum și informarea registratorilor despre măsurile întreprinse;

39.7. cooperarea eficientă și comunicarea permanentă, ce presupune schimbul de informații dintre diverse echipe de tip CERT, utilizatori, entități publice, după caz; sesizarea entităților publice care au atribuții de asigurare a securității statului;

39.8. escaladarea incidentelor cibernetice care necesită implicarea Centrului Național de Management al Crizelor și furnizarea de către entitățile care au făcut notificarea a informației relevante în ceea ce privește acțiunile ulterioare escaladării;

39.9. tratarea incidentelor cibernetice și oferirea recomandărilor de soluționare a acestora;

39.10. înștiințarea publică despre o alertă sau un incident cibernetic atunci când este necesară prevenirea unor potențiale incidente asemănătoare ca formă și conținut;

39.11. evidența și stocarea informațiilor aferente alertelor/incidentelor cibernetice;

39.12. întocmirea datelor statistice și a rapoartelor privind alertele, riscurile și incidentele cibernetice;

39.13. promovarea bunelor practici aferente prevenției și minimizării impactului potențialelor incidente cibernetice.

Capitolul V

INTERACȚIUNEA CU FURNIZORII DE DATE

40. În vederea asigurării operativității și continuității funcționării RSIC, schimbul de date între participanți se efectuează continuu.

41. Schimbul informațional cu furnizorii de date se realizează prin intermediul „Platformei schimb de informații" a SI RSIC, precum și prin intermediul platformei de interoperabilitate (MConnect) sau a Sistemului de comunicații al autorităților publice.

42. Datele sunt prezentate de furnizori conform conținutului formularelor de notificare a incidentelor, alertelor și vulnerabilităților cibernetice, precum și conținutului rapoartelor preliminare și finale privind incidentele, alertele și vulnerabilitățile cibernetice, care se aprobă prin ordinul Directorului ASC.

Capitolul VI
INTEROPERABILITATEA CU ALTE SISTEME ȘI RESURSE INFORMAȚIONALE DE STAT

43. Pentru asigurarea actualizării operative și automate a conținutului informațional al RSIC cu informație veridică, se asigură interacțiunea și sincronizarea cu alte registre și resurse informaționale de stat.

44. Pentru preluarea datelor cu conținut informațional relevant, SI RSIC realizează schimbul de date prin intermediul platformei de interoperabilitate (MConnect), cu următoarele sisteme și resurse informaționale de stat:

44.1. Registrul de stat al unităților de drept – pentru recepționarea datelor de identificare a persoanelor juridice;

44.2. Registrul de stat al populației – pentru recepționarea datelor de identificare a persoanelor fizice.

45. Pentru asigurarea autenticității, integrității și securității accesului la date, SI RSIC utilizează următoarele servicii informaționale partajate:

45.1. platforma de interoperabilitate (MConnect) – pentru recepționarea datelor din alte sisteme și resurse informaționale de stat;

45.2. serviciul electronic guvernamental de autentificare și control al accesului (MPass) – pentru autentificarea și controlul accesului utilizatorilor;

45.3. serviciul electronic guvernamental de jurnalizare (MLog) – pentru jurnalizarea evenimentelor de business critice;

45.4. serviciul electronic guvernamental integrat de semnătură electronică (MSign) – pentru aplicarea semnăturii electronice în cadrul proceselor de business ale SI RSIC;

45.5. serviciul guvernamental de notificare electronică (MNotify) – pentru notificarea utilizatorilor autorizați;

45.6. Sistemul informațional automatizat „Registrul împuternicirilor de reprezentare în baza semnăturii electronice" (MPower) – pentru verificarea împuternicirilor de reprezentare a utilizatorilor necesare pentru autorizarea acțiunilor acestora;

45.7. portalul guvernamental unic de date deschise (PDGD) – pentru publicarea seturilor publice de date produse în cadrul fluxurilor de lucru ale SI RSIC.

Capitolul VII
ASIGURAREA PROTECȚIEI ȘI SECURITĂȚII INFORMAȚIEI RSIC

46. Datele conținute în RSIC fac parte din categoria datelor cu acces limitat. Asigurarea securității, confidențialității și integrității acestor date este responsabilitatea

subiecților cu drepturi de acces la RSIC, care trebuie să respecte cerințele legale privind protecția datelor cu caracter personal în procesul de prelucrare a acestora.

47. Obiectele asigurării protecției și securității datelor din RSIC sunt considerate toate mijloacele software și infrastructurile tehnologice utilizate pentru realizarea proceselor informaționale, în conformitate cu cerințele legale aplicabile privind securitatea sistemelor informaționale.

48. Securitatea informațională a RSIC se efectuează prin aplicarea metodelor și prin efectuarea acțiunilor prevăzute pentru SI RSIC descrise în Conceptul SI RSIC.

49. Protecția datelor cu caracter personal sunt asigurate prin următoarele acțiuni:

49.1. posesorul, deținătorul, registratorii și furnizorii de date vor prelucra doar acele date cu caracter personal care sunt strict necesare, neexcesive scopului prestabilit, conform competențelor atribuite și respectând principiile stabilite de cadrul normativ privind protecția datelor cu caracter personal;

49.2. în procesul de prelucrare a datelor cu caracter personal, posesorul, deținătorul, registratorii și furnizorii vor asigura măsuri organizatorice și tehnice necesare pentru a proteja datele cu caracter personal împotriva distrugerii, modificării, blocării, copierii, răspândirii sau a altor acțiuni ilegale. Aceste măsuri asigură un nivel adecvat de securitate, corespunzător riscurilor asociate prelucrării și caracterului datelor prelucrate.

50. Respectarea drepturilor subiectului de date cu caracter personal se realizează în conformitate cu prevederile cadrului legislativ.

51. Persoana responsabilă de protecția datelor cu caracter personal notifică Centrului Național pentru Protecția Datelor cu Caracter Personal orice indicii sau incidente care ar putea indica încălcări ale legislației privind protecția datelor cu caracter personal.

52. Protecția datelor SI RSIC se efectuează prin următoarele metode:

52.1. prevenirea acțiunilor intenționate și/sau neintenționate ale utilizatorilor, care pot duce la distrugerea sau denaturarea datelor;

52.2. utilizarea obligatorie a produselor de program licențiate și aprobate;

52.3. monitorizarea procesului de utilizare a RSIC prin intermediul mecanismului de jurnalizare, gestionat de deținătorul acestuia.

53. Subiecții RSIC asigură implementarea normelor de securitate, acestea urmând să conțină acte ce confirmă:

53.1. identitatea persoanei responsabile de implementarea normelor de securitate și împuternicirile acesteia;

53.2. implementarea principalelor măsuri tehnico-organizatorice necesare pentru protecția RSIC;

53.3. implementarea procedurilor interne pentru prevenirea modificărilor neautorizate asupra conținutului informațional;

53.4. informarea utilizatorilor interni și instruirea acestora cu privire la modalitățile și mecanismele de asigurare a securității informaționale;

53.5. procedurile de control intern ale subiecților care accesează RSIC privind respectarea condițiilor de securitate informațională.

54. Schimbul informațional se efectuează cu utilizarea mijloacelor software și a infrastructurilor tehnologice autorizate, prin canale securizate, asigurând integritatea și securitatea datelor, în conformitate cu cerințele legale aplicabile.

55. Normele de securitate se aduc la cunoștința fiecărui utilizator al SI RSIC.

56. Utilizatorii asigură instruirea angajaților privind metodele și procedeele de contracarare a pericolelor informaționale.

Capitolul VIII

ASIGURAREA CONTROLULUI ȘI RĂSPUNDEREA

57. Ținerea RSIC este supusă controlului intern și extern. Controlul intern se efectuează de către posesor. Controlul extern se efectuează de către autoritățile abilitate de cadrul normativ în vigoare.

58. Controlul legalității operațiilor de prelucrare a datelor cu caracter personal realizate în RSIC se efectuează de către Centrul Național pentru Protecția Datelor cu Caracter Personal.

59. În cazul apariției unor circumstanțe excepționale și dificultăți tehnice care afectează infrastructura de suport a RSIC, funcționalitatea acestuia poate fi suspendată temporar. În astfel de cazuri, subiecții RSIC vor fi informați prin intermediul mijloacelor tehnice disponibile.

60. Toți subiecții RSIC poartă răspundere, conform legislației, pentru prelucrarea, divulgarea și transmiterea informației din RSIC persoanelor terțe, contrar prevederilor legislației.

NOTA DE FUNDAMENTARE
la proiectul hotărârii Guvernului
privind aprobarea Conceptului Sistemului informațional "Registrul de stat al incidentelor cibernetice" și a Regulamentului Registrului de stat al incidentelor cibernetice"

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

Proiectul hotărârii Guvernului privind aprobarea Conceptului Sistemului informațional "Registrul de stat al incidentelor cibernetice" și a Regulamentului Registrului de stat al incidentelor cibernetice" este elaborat de către Ministerul Dezvoltării Economice și Digitalizării.

2. Condițiile ce au impus elaborarea proiectului actului normativ

2.1. Temeiul legal sau, după caz, sursa proiectului actului normativ

Proiectul de hotărâre a fost elaborat în temeiul art. 22 lit. d) din Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat, art. 10 din Legea nr.48/2023 privind securitatea cibernetică și al art. 16 din Legea nr. 71/2007 cu privire la registre.

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

În scopul evidenței datelor privind apariția, evoluția și soluționarea incidentelor cibernetice, al automatizării proceselor de identificare, înregistrare, documentare, clasificare, analizare și gestionare a unor astfel de incidente, al monitorizării și evidenței alertelor cibernetice și vulnerabilităților, în conformitate cu prevederile art. 10 alin. (1) din Legea nr.48/2023 privind securitatea cibernetică, Guvernul a fost abilitat cu competențe privind crearea Registrului de stat al incidentelor cibernetice și sistemului informațional destinat ținerii registrului respectiv.

Totodată, conform Legii nr. 48/2023 privind securitatea cibernetică și Hotărârii Guvernului nr. 1028/2023 cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică, Agenția pentru Securitate Cibernetică (în continuare – ASC) este desemnată în calitate de autoritate competentă la nivel național în domeniul securității cibernetice și exercită inclusiv funcția de echipă de răspuns la incidentele cibernetice la nivel național și cea de punct național unic de contact și de raportare a incidentelor de securitate cibernetică la nivel național. Totodată, ASC asigură monitorizarea amenințărilor cibernetice, vulnerabilităților și incidentelor cibernetice la nivel național.

Una dintre atribuțiile ASC în calitate de echipă de răspuns la incidente cibernetice la nivel național este de a asigura înregistrarea incidentelor cibernetice care i-au fost notificate în Registrul de stat al incidentelor cibernetice.

De asemenea, conform pct. 7 subpct. 3) și 5) din Regulamentul cu privire la organizarea și funcționarea Agenției pentru Securitate Cibernetică (aprobat prin Hotărârea Guvernului nr.1028/2023) ASC are atribuția de a oferi o platformă de management al incidentelor cibernetice și pentru schimbul de informații, în scopul cooperării cu echipele de răspuns la incidente cibernetice, precum și o platformă destinată intermedierii schimbului de informații între furnizorii de servicii și alte persoane juridice.

În prezent, pentru raportarea incidentelor cibernetice și datelor aferente acestora se utilizează procese semi-automatizate, ceea ce presupune numeroase riscuri privind securitatea informației, integritatea datelor, istoricul modificărilor etc.

Incidentele raportate sunt documentate conform unui șablon predefinit (formular de raportare a incidentelor cibernetice) și remise prin poșta electronică, fiind înregistrate manual într-o bază de date. Metoda actuală nu asigură realizarea unei analize comprehensive, care ar permite identificarea cauzelor și a ariilor expuse riscului de securitate.

Astfel, apare necesitatea creării și implementării Sistemului informațional „Registrul de stat al incidentelor cibernetice" (în continuare – SI RSIC). Prin aceasta se urmărește dezvoltarea și îmbunătățirea proceselor din cadrul ASC și celorlalte instituții cu competențe în domeniul securității cibernetice, a modului de gestiune a incidentelor cibernetice și interacțiune dintre ASC, CERT-Gov și structurile de tip CERT departamentale.

Respectiv, implementarea RSIC va consolida la nivel național procedurile de raportare și evidență a incidentelor, alertelor și vulnerabilităților cibernetice, precum și va exclude soluțiile fragmentare care nu oferă un cadru de interoperabilitate necesar între structurile cu competențe în domeniul securității cibernetice.
Beneficiile implementării SI RSIC sunt:

1) optimizarea proceselor operaționale;

2) accesarea rapidă a datelor și a documentelor relevante pentru procesele de lucru ale ASC, CERT-Gov și CERT departamentale;

3) crearea unei baze de date electronice naționale aferente incidentelor cibernetice, vulnerabilităților și amenințărilor cibernetice;

5) înregistrarea și evidența totalității documentelor aferente incidentelor cibernetice;

6) standardizarea datelor și precizia informațiilor gestionate în sistem;

7) reducerea birocrației, prin eliminarea evidenței manuale;

8) simplificarea procesului de introducere, modificare și actualizare a informațiilor aferente incidentelor cibernetice;

9) centralizarea, în format electronic, a informațiilor cu privire la incidentele cibernetice raportate;

10) asigurarea interoperabilității cu alte sisteme informaționale de stat pentru schimbul de date;

11) asigurarea schimbului de date cu privire la incidentele cibernetice, în format electronic, între ASC, CERT Gov și CERT departamentale, precum și furnizori de servicii din sectoare critice, conform cadrului normativ în vigoare;

12) reducerea timpului de raportare și răspuns la incidentele cibernetice;

13) asigurarea unui mediu operațional sigur.

3. Obiectivele urmărite și soluțiile propuse

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

Obiective urmărite prin crearea sistemului informațional și a RSIC constituie:

1) asigurarea formării resurselor informaționale de stat aferente incidentelor cibernetice, alertelor, vulnerabilităților în spațiul cibernetic;

2) dezvoltarea unei soluții tehnice flexibile și modulare;

3) formarea bazei de date a incidentelor cibernetice la nivel național;

4) asigurarea evidenței alertelor, vulnerabilităților în spațiul cibernetic și a incidentelor cibernetice identificate sau raportate, a tehnicilor și tehnologiilor folosite pentru atacuri, precum și a bunelor practici pentru protecția infrastructurilor cibernetice;

5) diseminarea informațiilor cibernetice și desfășurarea acțiunilor de informare privind alertele, vulnerabilitățile în spațiul cibernetic, riscurile securității cibernetice și măsurile de protecție întreprinse.

Proiectul Conceptului Sistemului informațional „Registrul de stat al incidentelor cibernetice" stabilește scopurile, sarcinile și funcțiile SI RSIC, structura organizațională și baza normativă necesară pentru crearea și exploatarea lui, obiectele informaționale și lista datelor care se păstrează în acesta, infrastructura tehnologică și măsurile de securitate informațională.
Proiectul Regulamentului Registrului de stat al incidentelor cibernetice stabilește drepturile și obligațiile subiecților raporturilor juridice aferente creării și ținerii Registrului de stat al incidentelor cibernetică (în continuare – RSIC), modalitatea de ținere a resursei informaționale; procedura de înregistrare, modificare, completare și radiere a datelor; procedura de interacțiune cu furnizorii de date; măsuri privind asigurarea securității RSIC.

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

Nu este aplicabil

4. Analiza impactului de reglementare

4.1. Impactul asupra sectorului public

Implementarea Sistemului Informațional „Registrul de stat al incidentelor cibernetice" va avea un impact semnificativ asupra rezilienței cibernetice a autorităților și instituțiilor publice prin:

- oferirea unui mecanism de evidență centralizată a incidentelor cibernetice, alertelor și vulnerabilităților și a măsurilor întreprinse pentru înlăturarea și contracararea acestora;
- identificarea premiselor de apariție a incidentelor cibernetice și de a avertizare în cazul producerii acestora;
- asigurarea răspunsului la incidente cibernetice;
- conectarea și realizarea schimbului de date între ASC, CERT Gov și CERT sectoriale prin intermediul unei platforme dedicate, ce va eficientiza interoperabilitatea între autoritățile implicate, reducând timpul necesar pentru schimbul de informații și sporind eficiența colaborării interinstituționale;
- asigurarea informațională. Informația se pune la dispoziția autorităților competente.

4.2. Impactul financiar și argumentarea costurilor estimative

Asigurarea creării, implementării, funcționării și dezvoltării Sistemului informațional automatizat „Registrul de stat al incidentelor cibernetice" se va efectua din contul și în limita mijloacelor financiare alocate din bugetul de stat și altor mijloace, conform legii, inclusiv atragerea fondurilor externe de dezvoltare.

Costurile pentru implementarea SI RSIC vor fi evaluate în cadrul procesului de planificare bugetară reieșind din arhitectura complexului software-hardware (lista produselor hardware şi software utilizate la crearea infrastructurii informaţionale și de comunicații electronice a SI RSIC). Prezența componentelor software și a mijloacelor tehnologice în complexul informațional al SI RSIC este stabilită la etapa elaborării sarcinii tehnice a sistemului.

4.3. Impactul asupra sectorului privat

Proiectul nu prevede alte obligații suplimentare pentru furnizării de servicii decît cele prevăzute de Legea nr.48/2023 privind securitatea cibernetică.

4.4. Impactul social

4.4.1. Impactul asupra datelor cu caracter personal

Impactul asupra datelor cu caracter personal va fi minimizat prin respectarea strictă a reglementărilor privind protecția acestor date, conform cadrului normativ în vigoare.

4.4.2. Impactul asupra echității și egalității de gen

Nu este aplicabil

4.5. Impactul asupra mediului

Nu este aplicabil

4.6. Alte impacturi și informații relevante

Nu este aplicabil

5. Compatibilitatea proiectului actului normativ cu legislația UE

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

Proiectul nu are ca scop transpunerea unui act juridic al Uniunii Europene.

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

Proiectul este elaborat în contextul implementării prevederilor Legii nr. 48/2023 privind securitatea cibernetică, care a transpus parțial prevederile Directivei NIS2 (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).

6. Avizarea și consultarea publică a proiectului actului normativ

În conformitate cu prevederile art. 9 din Legea nr. 239/2008 privind transparența în procesul decizional, la data de 27.10.2025 a fost publicat anunțul referitor la inițierea procesului de elaborare a proiectului de hotărâre de Guvern pe pagina web oficială a Ministerului Dezvoltării Economice și Digitalizării mded.gov.md și pe platforma de consultare particip.gov.md (https://particip.gov.md/ro/document/stages/anunt-privind-initierea-procesului-de-elaborare-a-proiectului-hotararii-guvernului-privind-crearea-sistemului-informational-registrul-de-stat-al-incidentelor-cibernetice-si-resursei-informationale-formate-de-acesta/15368).

Proiectul urmează să fie supus avizării și consultării publice, conform prevederilor Legii nr. 100/2017 cu privire la actele normative.

7. Concluziile expertizelor

Proiectul urmează a fi remis conform procedurii legale Centrului Național Anticorupție pentru efectuarea expertizei anticorupție a acestuia.

Informația referitoare la concluziile expertizei privind compatibilitatea proiectului de hotărâre cu alte acte normative în vigoare, precum și respectarea normelor de tehnică legislativă va fi inclusă după recepționarea expertizei juridice.

Proiectul nu cade sub incidența Metodologiei de analiză a impactului în procesul de fundamentare a proiectelor de acte normative deoarece nu prevede alte obligații suplimentare pentru furnizorii de servicii decît cele prevăzute de Legea nr.48/2023 privind securitatea cibernetică.

8. Modul de încorporare a actului în cadrul normativ existent

Ca urmare a aprobării proiectului va fi abrogată Hotărîrea Guvernului nr.388/2022 cu privire la aprobarea Conceptului Sistemului informațional „Registrul de stat al incidentelor de securitate cibernetică”.

9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ

Pentru implementarea eficientă a prevederilor proiectului actului normativ, sunt necesare următoarele măsuri:

- elaborarea sarcinii tehnice a sistemului informațional;
- stabilirea compeluxului de mijloace hardware și software ale sistemului informațional;
- contractarea serviciilor de dezvoltare IT, testare și mentenanță;
- crearea și testarea platformei tehnologice;
- integrarea sistemului cu alte resurse informaționale de stat;
- instituirea măsurilor de securitate cibernetică și protecție a datelor;
- instruirea personalului;
- elaborarea și aprobarea procedurilor operaționale pentru gestionarea datelor;
- identificarea și alocarea resurselor: Asigurarea resurselor financiare, tehnice și umane necesare pentru fiecare etapă a procesului de implementare.
- planificarea cheltuielilor pentru mentenanță și actualizări sistemice etc.

Viceprim-ministru,
Ministru al Dezvoltării Economice și Digitalizării **Eugen OSMOCHESCU**

SINTEZA

Avizare prealabilă la proiectul de hotărâre privind aprobarea Conceptului Sistemului informațional "Registrul de stat al incidentelor cibernetice" și a Regulamentului Registrului de stat al incidentelor cibernetice"

Participantul la avizare, consultare publică, expertizare	Nr. crt.	Conținutul obiecției, propunerii, recomandării, concluziei	Argumentarea autorului proiectului
Agenția de Guvernare Electronică 3007-220 din 05.11.2025	1.	La proiectul hotărârii Guvernului: Titlul hotărârii urmează a fi revizuit, prin redarea corectă a obiectului acestuia în concordanță cu pct.1 din proiectul de hotărâre, după cum urmează: „Proiectul de hotărâre a Guvernului privind aprobarea Conceptului Sistemului informațional "Registrul de stat al incidentelor cibernetice" și a Regulamentului Registrului de stat al incidentelor cibernetice".	**Se acceptă**
	2.	La proiectul Conceptului: Pct.7 se va reda în corespundere cu art.10 alin.(1) din Legea nr.48/2023 privind securitate cibernetică.	**Se acceptă**
	3.	Pct. 13 urmează să fie completat cu trimiteri adiționale la alte acte normative din domeniul e-Transformării guvernării, care reglementează utilizarea în spațiul tehnologic a unui sistem informațional nou, a unor sisteme informaționale partajate, funcționalitățile cărora, ar urma să fie reutilizate la dezvoltarea Sistemului informațional „Registrul de stat al incidentelor cibernetice" (în continuare – SI RSIC): 1) Hotărârea Guvernului nr. 677/2025 cu privire la consolidarea accesului la serviciile publice electronice în cadrul Portalului guvernamental integrat EVO utilizat la prestarea serviciilor publice electronice și aprobarea măsurilor necesare pentru implementarea modelului unitar de design; 2) Hotărârea Guvernului nr. 650/2023 cu privire la aprobarea Strategiei de transformare digitală a Republicii Moldova pentru anii 2023-2030; 3) Hotărârea Guvernului nr.323/2021 pentru aprobarea Conceptului Sistemului informațional „Catalogul semantic" și a Regulamentului privind modul de ținere a Registrului format de Sistemul informațional „Catalogul semantic"	**Se acceptă**

	4.	În pct.20 se vor exclude cuvintele „și administratorului tehnic”, deoarece administrarea tehnică a SI RSIC urmează a fi asigurată de către I.P. STISC, reieșind din calitatea instituției respective de posesor al platformei tehnologice guvernamentale comune (MCloud) în care va fi găzduit și SI RSIC.	**Nu se acceptă** Sistemul urmează a fi găzduit pe platforma tehnologică a ASC și administrat tehnic de aceasta. Menționăm că SI RSIC reprezintă un sistem informațional de o importanță critică majoră pentru asigurarea securității cibernetice la nivel național, iar găzduirea sistemului pe platforma tehnologică guvernamentală comună (MCloud) prezintă riscuri privind asigurarea stabilității și continuității funcționării și dezvoltării SI RSIC. Menționăm că conform informației prezentate de IP STISC, această instituție se confruntă cu lipsa finanțării corespunzătoare în ultimii ani, fapt ce a generat impedimente considerabile în procesul de dezvoltare și extindere a platformei guvernamentale MCloud, precum și dificultăți în alocarea resurselor TI conform necesităților autorităților publice. Totodată, găzduirea SI RSIC pe platforma tehnologică a ASC este impusă și de necesitatea integrării tuturor soluțiilor tehnologice implementate de ASC pe o platformă unică pentru

		a asigura interoperabilitatea acestora.
5.	Subsecvent, Capitolul V se va completa cu o normă prin care se va reglementa rolul I.P. STISC de administrator tehnic al SI RSIC.	**Nu se acceptă** A se vedea argumentarea de la pct.4 din Sinteză.
6.	În pct.26 sbp.2) se va comasa cu sbp.1), deoarece documentele interne descrise în subpunctul respectiv reprezintă de fapt documente de intrare sau, după caz, cu sbp.3) care se referă la documentele de ieșire. La acest subiect, menționăm că potrivit pct.2.2.6 din Anexa nr.3 la Reglementarea tehnică „Procesele ciclului de viață al software-ului" RT 38370656 002:2006, aprobată prin Ordinul ministrului dezvoltării informaționale nr.78/2006, în cadrul unui sistem informațional sunt descrise 3 tipuri de documente ale sistemului: documente de intrare, documente de ieșire și documente tehnologice.	**Nu se acceptă** Ordinul nr.78/2006 prevede cerințe minime, totodată, pentru funcționarea eficientă a sistemului sunt necesare documente interne – informațiile și rapoartele generate de instrumentele de lucru, rezultatele preventive ale procesării datelor de intrare, ce urmează a fi prelucrate de sistem pentru generarea documentelor de ieșire.
7.	În pct.41 textul „SI RSIC va conține următoarele obiectele informaționale preluate din alte sisteme informaționale de stat" se va substitui cu textul „SI RSIC va prelua date aferente obiectelor informaționale din alte sisteme informaționale de stat".	**Se acceptă**
8.	Capitolul VII se va completa cu o prevedere suplimentară cu următorul cuprins: „În scopul asigurării interoperabilității și a schimbului de date cu alte sisteme și resurse informaționale de stat, ASC înregistrează activele semantice utilizate în Sistemul informațional „Catalogul semantic."	**Se acceptă**
9.	Prevederea de la pct. 45 urmează a fi racordată la cea de la pct.4 sbp.1) din Hotărârea Guvernului nr.128/2014 privind platforma tehnologică guvernamentală comună (MCloud), conform căreia ministerele și structurile organizaționale din sfera lor de competență (inclusiv Agenția pentru Securitatea Cibernetică) urmează să găzduiască sistemele informaționale existente şi cele noi pe platforma tehnologică guvernamentală comună (MCloud). Subsecvent, pct.45 se va expune cu următorul conținut: „45. RSIC este găzduit pe platforma tehnologică guvernamentală comună (MCloud)."	**Nu se acceptă** A se vedea argumentarea de la pct.4 din Sinteză.

	10.	La pct.55 sbp.1) se va completa cu textul „exclusiv prin intermediul serviciului MPass”;	**Se acceptă**
	11.	Capitolul VIII se va completa cu prevederi aferente implementării Modelului Unitar de Design, în conformitate cu prevederile Hotărârii Guvernului nr.677/2025 cu privire la consolidarea accesului la serviciile publice electronice în cadrul Portalului guvernamental integrat EVO utilizat la prestarea serviciilor publice electronice și aprobarea măsurilor necesare pentru implementarea modelului unitar de design. Astfel, odată cu aprobarea actului normative menționat, Ministerele, Cancelaria de Stat, alte autorități administrative centrale subordonate Guvernului şi structurile organizaționale din sfera lor de competență vor aplica modelul unitar de design la crearea sau dezvoltarea altor resurse și sisteme informaționale de stat care nu sunt destinate prestării serviciilor publice electronice sau la crearea și dezvoltarea de site-uri web oficiale. La fel, prestatorii de servicii publice vor utiliza modelul unitar de design la crearea și dezvoltarea resurselor și sistemelor informaționale noi, destinate prestării serviciilor publice electronice. Totodată, aducem la cunoștință că, potrivit pct. 8 din Hotărârea Guvernului nr.667/2025, că înainte de punerea în exploatare a resurselor și sistemelor informaționale, design-ul elaborat va fi coordonat în prealabil cu Instituția Publică „Agenția de Guvernare Electronică”. În context, la proiectarea, dezvoltarea și actualizarea resurselor și sistemelor informaționale deținute de Agenția pentru Securitatea Cibernetică se va utiliza modelul unitar de design, iar designul sistemului se va coordona în conformitate cu Hotărârea Guvernului nr.677/2025.	**Se acceptă de principiu** Hotărârea Guvernului nr. 677/2025 a fost specificată la pct.13 din proiectul conceptului, care menționează cadrul normativ aferent creării și implementării SI RSIC. Totodată, dublarea prevederilor Hotărârii Guvernului nr.677/2025 în textul Conceptului o considerăm inoportună și nu aduce plus valoare juridică.

Viceprim-ministru,
Ministru al Dezvoltării Economice și Digitalizării **Eugen OSMOCHESCU**

Ministerul Dezvoltării
Economice și Digitalizării
al Republicii Moldova

nr. 13/2- 3200 din 12.11.2025

Cancelaria de Stat

În temeiul prevederilor pct. 38 și 185 din Regulamentul Guvernului, aprobat prin Hotărârea Guvernului nr. 610/2018, se transmite *proiectul hotărârii Guvernului privind aprobarea Conceptului Sistemului informațional "Registrul de stat al incidentelor cibernetice" și a Regulamentului Registrului de stat al incidentelor cibernetice* pentru a fi inclus în lista proiectelor care urmează a fi examinate în cadrul ședinței secretarilor generali.

Reieșind din faptul că proiectul menționat este inclus în documentele strategice ale Republicii Moldova, și anume *Agenda de reforme aferente Planului de creștere al Republicii Moldova pentru anii 2025–2027* (aprobat prin Hotărârea Guvernului nr. 260/2025) și *Foaia de parcurs privind „Statul de drept"*, care constituie un criteriu de referință în procesul de aderare a Republicii Moldova la Uniunea Europeană (aprobată prin Hotărârea Guvernului nr. 275/2025), având termen de realizare anul 2025, solicităm respectuos includerea acestuia, în regim de urgență, pe agenda ședinței secretarilor generali.

CERERE
privind înregistrarea de către Cancelaria de Stat
a proiectelor de acte ale Guvernului

Nr. crt.	Criterii de înregistrare	Nota autorului
1.	Categoria și denumirea proiectului	Proiectul hotărârii Guvernului privind aprobarea Conceptului Sistemului informațional "Registrul de stat al incidentelor cibernetice" și a Regulamentului Registrului de stat al incidentelor cibernetice.
2.	Autoritatea care a elaborat proiectul	Proiectul este elaborat de către Ministerul Dezvoltării Economiei și Digitalizării.
3.	Justificarea depunerii cererii	Proiectul este elaborat în temeiul prevederilor art. 10 (1) din Legea nr. 48/2023 privind securitatea cibernetică, precum și în scopul asigurării unui nivel sporit de securitate cibernetică a rețelelor și sistemelor informatice.
4.	Referința la documentul de planificare care prevede elaborarea proiectului *(PNA, PND, PNR, alte documente de planificare sectoriale)*	1) Agenda de reforme aferentă Planului de creștere al Republicii Moldova pentru 2025-2027 (Hotărârea Guvernului nr. 260/2025) – măsura 2.3.11, (v) delimitarea clară și transparentă a competențelor instituțiilor de securitate cibernetică ale MD, cu ajustarea mandatelor instituțiilor relevante în urma unei note a unui expert. 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. 4.3 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) – Clasterul 3, Anexa A, proiectul 34.
5.	Lista autorităților și instituțiilor a căror avizare este necesară	1. Cancelaria de Stat 2. Ministerul Infrastructurii și Dezvoltării Regionale 3. Ministerul Energiei 4. Ministerul Finanțelor 5. Ministerul Afacerilor Interne 6. Serviciul de Informații și Securitate 7. Serviciul Tehnologia Informației și Securitate Cibernetică 8. Agenția pentru Securitatea Cibernetică 9. Agenția de Guvernare Electronică 10. Agenția Servicii Publice 11. Banca Națională a Moldovei 12. Centrul Național pentru Protecția Datelor cu Caracter Personal 13. Centrul de Armonizare a Legislației
6.	Termenul-limită pentru depunerea avizelor/expertizelor	Termen-limită de prezentare a avizelor - 5 zile lucrătoare.
7.	Persoana responsabilă de promovarea proiectului	Sergiu Florea, șef al Secției politici în domeniul securității cibernetice, Direcția politici în domeniul tehnologiei informației și digitalizării tel.: 022 250 618, e-mail: sergiu.florea@mded.gov.md Victoria Iorga, consultant superior, Secția politici în domeniul securității cibernetice, Direcția politici în domeniul tehnologiei informației și digitalizării, tel. 022 250 556 e-mail victoria.iorga@mded.gov.md
8.	Anexe	1. Proiectul hotărârii Guvernului 2. Nota de fundamentare 3. Sinteza
9.	Data și ora depunerii cererii	
10.	Semnătura	

Viceprim-ministru,
Ministru al Dezvoltării Economice și Digitalizării **Eugen OSMOCHESCU**