



# GUVERNUL REPUBLICII MOLDOVA

**HOTĂRÂRE nr. \_\_\_\_**

**din \_\_\_\_\_ 2022**

**Chișinău**

**Cu privire la aprobarea Conceptului Sistemului informațional  
„Registrul de stat al incidentelor de securitate cibernetică”**

-----

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, 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 Conceptul Sistemului informațional „Registrul de stat al incidentelor de securitate cibernetică” (se anexează).

**2.** Se instituie Registrul de stat al incidentelor de securitate cibernetică, proprietate a statului.

**3.** Crearea, implementarea, funcționarea și dezvoltarea Sistemului informațional „Registrul de stat al incidentelor de securitate cibernetică” va fi asigurată de către Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică”.

**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.

**Prim-ministru**

**NATALIA GAVRILIȚA**

Contrasemnează:

**Viceprim-ministru  
pentru digitalizare**

**Iurie ȚURCANU**

Aprobat  
prin Hotărârea Guvernului nr.     /2022

**CONCEPT**  
**al Sistemului Informațional**  
**„Registrul de stat al incidentelor de securitate cibernetică”**

**I. INTRODUCERE**

În conformitate cu prevederile art. 10 alin (1) al Legii nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat, cu modificările ulterioare, Hotărârii Guvernului nr. 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetică 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, Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică” (în continuare - STISC), în calitate sa de Centru guvernamental de reacție la incidente de securitate cibernetică (în continuare - CERT Gov), ce constituie punctul unic de contact și de raportare a incidentelor de securitate cibernetică a Guvernului, asigură securitatea cibernetică a sistemelor și resurselor informaționale de stat.

Una din atribuțiile STISC în calitate de CERT Gov este de a crea și pune în aplicare Registrul de stat al incidentelor de securitate cibernetică. De asemenea, conform pct.5 sbp. 7) și sbp.8) ale Măsurilor necesare pentru asigurarea securității cibernetică la nivel guvernamental, aprobate prin Hotărârea Guvernului nr. 482/2020, CERT Gov are atribuția de a oferi o platformă informațională de comunicare strategică cu entitățile publice precum și de a asigura evidența amenințărilor, vulnerabilităților în spațiul cibernetic și incidentelor de securitate cibernetică identificate sau raportate.

În prezent, pentru raportarea incidentelor de securitate cibernetică și alte date 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 de securitate cibernetică) și sunt remise prin poșta electronică, fiind înregistrate manual într-o bază de date în format .xls Metoda actuală nu asigură realizarea unei analize comprehensive, care ar permite identificarea cauzelor și a ariilor expuse riscului de securitate. Înregistrarea și monitorizarea tuturor tipurilor de incidente de securitate cibernetică, ar îmbunătăți aspecte ce țin de: definiția, clasificarea, învățarea din incidente.

Astfel, apare necesitatea creării și implementării unui Sistem informațional „Registrul de stat al incidentelor de securitate cibernetică” (în continuare - SI

RSISC). Prin aceasta se urmărește îmbunătățirea proceselor existente în cadrul CERT Gov, a modului de gestiune a incidentelor de securitate cibernetică, precum și facilitarea raportării acestora pentru structurile de tip CERT departamentale ale Guvernului.

Prezentul Concept stabilește scopurile, sarcinile și funcțiile SI RSISC, 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. SI RSISC va respecta Reglementarea tehnică „Procese ciclului de viață ale software-ului RT 38370656-002:2006, aprobată prin ordinul ministrului dezvoltării informaționale nr. 78/2006 (în continuare-Reglementarea tehnică).

Beneficiile implementării SI RSISC sunt:

- 1) optimizarea proceselor de lucru și reducerea costurilor operaționale;
- 2) regăsirea rapidă a datelor și documentelor relevante pentru procesele de lucru ale CERT Gov;
- 3) consolidarea unei baze de date electronice aferentă incidentelor de securitate cibernetică;
- 4) consolidarea unei baze de cunoștințe ce ar contribui la îmbunătățirea calității funcționării CERT Gov;
- 5) înregistrarea și evidența totalității documentelor aferente incidentelor de securitate cibernetică;
- 6) standardizarea datelor și acuratețea informațiilor gestionate în sistem;
- 7) reducerea birocrăției prin eliminarea treptată a evidențelor manuale;
- 8) simplificarea procesului de introducere, modificare, actualizare a informațiilor aferente incidentelor de securitate cibernetică;
- 9) centralizarea în format electronic a informațiilor cu privire la incidentele raportate de entitățile publice;
- 10) asigurarea interoperabilității cu sisteme informatice ale entităților publice pentru schimbul bidirecțional de date.
- 11) asigurarea schimbului de date cu privire la incidentele de securitate cibernetică, în format electronic, între CERT Gov și CERT departamentale, conform legislației;
- 12) reducerea timpului mediu de raportare și răspuns la incidente de securitate cibernetică;
- 13) asigurarea unui mediu operațional partajat, precum și a unei securități crescute a datelor electronice și informațiilor în cadrul și între entitățile publice.

## **II. DISPOZIȚII GENERALE**

**1.** SI RSISC reprezintă totalitatea sistematizată de date privind incidentele cibernetică raportate prin punctul unic de contact CERT Gov, deținătorii resurselor informaționale afectate, precum și documentele și mijloacele de identificare a incidentelor de securitate cibernetică raportate.

**2.** SI RSISC este parte componentă a Resurselor informaționale de stat ale Republicii Moldova.

**3.** SI RSISC creează un spațiu informațional unitar, care reprezintă sursa oficială de informație cu privire la amenințările, vulnerabilitățile în spațiul cibernetic și incidentele de securitate cibernetică identificate sau raportate la nivel guvernamental.

**4.** SI RSISC reprezintă un ansamblu de resurse și tehnologii informaționale, de mijloace de program și metodologii, aflate în interconexiune și destinate evidenței și gestionării incidentelor de securitate cibernetică în conformitate cu atribuțiile STISC în calitate de CERT Gov prevăzute în Măsurile necesare pentru asigurarea securității ciberetice la nivel guvernamental, aprobate prin Hotărârea Guvernului nr. 482/2020.

**5.** Destinația SI RSISC constă în formarea Registrului de stat al incidentelor de securitate cibernetică, automatizarea procesului de înregistrare a incidente de securitate cibernetică, precum și documentarea și gestionarea incidentelor de securitate cibernetică, în conformitate cu actele normative.

**6.** Crearea SI RSISC 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 de securitate cibernetică, monitorizarea și evidența alertelor, vulnerabilităților în spațiul cibernetic și incidentelor de securitate cibernetică identificate sau raportate, pe de altă parte se constituie interacțiunea CERT-urilor departamentale cu CERT Gov privind incidentele de securitate cibernetică și alte informații aferente securității ciberetice.

**7.** SI RSISC reprezintă un sistem oficial de identificare și gestionare a incidentelor ciberetice la nivel guvernamental din Republica Moldova. Acesta va servi drept instrument de susținere a activităților CERT Gov, prin oferirea mijloacelor tehnice de schimb informațional, colaborare și transparentizare a activității desfășurate. În aceste condiții, SI RSISC va crea un sistem informațional accesibil, modern și securizat.

**8.** Grupul țintă al sistemului îl reprezintă entitățile publice menționate în pct.5 al Hotărârii Guvernului nr.482/2020, entitățile publice care au atribuții de asigurare a securității statului, precum și partenerii naționali cu care sunt stabilite relații de cooperare.

**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;

*audit de securitate cibernetică* - evaluare sistemică, detaliată, măsurabilă și tehnică a modului în care politicile de securitate cibernetică sunt aplicate la nivelul infrastructurilor cibernetică, cu emiterea de recomandări pentru minimizarea riscurilor identificate;

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

*metadata* - date, care descriu datele sistemului, modul în care sunt obținute și stocate, precizează structura datelor, proveniența lor, regulile de transformare, de agregare și de calcul; joacă un rol esențial în alimentarea sistemului cu date, sunt consultate și actualizate pe întreg ciclul de viață al sistemului;

*risc de securitate în spațiul cibernetic* - probabilitate ca o amenințare să se materializeze, exploatând o anumită vulnerabilitate specifică infrastructurilor cibernetică;

*vulnerabilitate în spațiul cibernetic* - ineficacitate în proiectarea și implementarea infrastructurilor cibernetică sau a măsurilor de securitate aferente, care poate fi exploatată de către o amenințare.

Alte noțiuni, sunt utilizate în sensul definit de Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat, Hotărârea Guvernului nr. 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetică 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 și Hotărârea Guvernului nr. 128/2014 privind platforma tehnologică guvernamentală comună (MCloud).

## **10. Scopul SI RSISC:**

1) asigurarea formării resurselor informaționale de stat aferent incidentelor de securitate cibernetică;

2) dezvoltarea unei soluții tehnice flexibile și modulare care ar permite îmbunătățirea activității STISC, în rolul său de CERT Gov;

3) formarea bazei de date a incidentelor de securitate cibernetică la nivel guvernamental;

4) asigurarea evidenței amenințărilor, vulnerabilităților în spațiul cibernetic și incidentelor de securitate cibernetică identificate sau raportate, tehnicilor și tehnologiilor folosite pentru atacuri, precum și bunelor practici pentru protecția infrastructurilor cibernetică;

5) diseminarea informațiilor de securitate cibernetică și desfășurarea acțiunilor de sensibilizare și informare privind amenințările, vulnerabilitățile în spațiul cibernetic, riscurile securității cibernetică și măsurile de protecție întreprinse.

**11.** Sarcinile de bază realizate la exploatarea SI RSISC sunt cele menționate în pct. 5 sbp. 1), 2), 4), 6) și 8) din Măsurile necesare pentru asigurarea securității cibernetice la nivel guvernamental aprobate prin Hotărârea Guvernului nr. 482/2020, precum și:

- 1) crearea și menținerea unei baze de date a incidentelor de securitate cibernetică și a măsurilor întreprinse pentru înlăturarea și contracararea acestora;
- 2) conectarea și realizarea schimbului de date între CERT-uri departamentale și CERT Gov prin intermediul unei platforme dedicate;
- 3) promovarea bunelor practici între specialiștii CERT Gov și persoanele responsabile de răspuns la incidente de securitate cibernetică din cadrul entităților publice.

**12.** Principiile de bază ale SI RSISC sunt:

- 1) *principiul legalității*, care presupune crearea și exploatarea sistemului în conformitate cu legislația națională;
- 2) *principiul responsabilității și conștientizării* - constă în efortul continuu derulat de entitățile de drept public și privat în conștientizarea rolului și responsabilității individuale pentru atingerea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice;
- 3) *principiul securității informaționale* - asigurarea nivelului integrității, confidențialității, exclusivității, accesibilității și eficienței protecției datelor împotriva pierderii, alterării, denaturării, deteriorării, modificării, accesului și utilizării neautorizate. Securitatea dată 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;
- 4) *principiul modularității și scalabilității* - posibilitatea de a dezvolta sistemul fără modificarea componentelor create anterior.

### **III. SPAȚIUL JURIDICO-NORMATIV AL FUNCȚIONĂRII SI RSISC**

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

- 1) Legea nr. 982/2000 privind accesul la informație;
- 2) Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat;
- 3) Legea nr. 71/2007 cu privire la registre;
- 4) Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice;
- 5) Legea nr. 133/2011 privind protecția datelor cu caracter personal;
- 6) Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate;
- 7) Hotărârea Guvernului nr. 562/2006 cu privire la crearea sistemelor și resurselor informaționale automatizate de stat;

8) 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;

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

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

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

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

13) Hotărârea Guvernului nr. 201/2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică;

14) 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;

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

16) 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);

17) 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.

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

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

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

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

4) Standardul Republicii Moldova SM ISO/IEC 27005:2018 Tehnologia informației, Tehnici de securitate. Managementul riscului securității informației.

#### IV. SPAȚIUL FUNCȚIONAL AL SI RSISC

**15.** Contururile funcționale principale ale SI RSISC sunt prezentate în figura 1, acestea fiind:

1) *Conturul Sistemul de alertă timpurie și reacție în timp real privind incidentele cibernetice* - 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. Sistemul include conexiuni de date ce vor transporta informații referitoare la incidentele cibernetice raportate, către conturul funcțional platforma de management a incidentelor și schimbului de informații. Prin funcționalul său, conturul dat va asigura colectarea și sistematizarea datelor recepționate din partea entităților responsabile, aferent anomaliilor parvenite din diferite surse, cu scopul prelucrării ulterioare. Conturul respectiv realizează următoarele funcții:

- a) colectarea metadatelor aferent anomaliilor și alertelor parvenite de la entitățile responsabile, precum și prelucrarea și sistematizarea datelor;
- b) corelarea alertelor din diferite surse și interfețe și transferarea datelor către platforma de management a incidentelor .

2) *Conturul Platformă de management a incidentelor și schimbului de informații* – platforma preia informațiile aferente incidentelor de securitate cibernetică din documentele de intrare sau din cadrul conturului funcțional sistemului de alertă timpurie și reacție în timp real privind incidentele cibernetice. Informațiile respective sunt prelucrate ulterior prin intermediul instrumentelor automatizate de analiză, incorporate în platforma de management. Conturul realizează următoarele funcții:

- a) formarea bazei de date a SI RSISC. Evidență primară a incidentelor de securitate cibernetică și actualizarea sistematică a bazei de date a incidentelor de securitate cibernetică, la modificarea sau completarea datelor obiectelor de evidență;

b) asigurarea informațională. Informația se pune la dispoziția autorităților competente. Nivelul de acces al beneficiarilor SI RSISC va fi stabilit în Regulamentul privind modul de ținere a RSISC, format de SI RSISC;

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

d) asigurarea răspunsului la incidente de securitate cibernetică. Conturul respectiv recepționează raportări privind incidentele de securitate cibernetică, care afectează sistemele informaționale și rețelele entităților publice și ulterior furnizează entităților care au făcut raportarea informații relevante în ceea ce privește acțiunile ulterioare raportării;



e) întocmirea datelor statistice și elaborarea rapoartelor aferent incidentelor de securitate cibernetică;

f) publicarea alertelor și atenționărilor privind apariția unor activități premergătoare atacurilor cibernetice;

g) asigurarea securității informației. Securitatea informației se asigură la toate etapele de colectare, păstrare și utilizare a resurselor informaționale de stat;

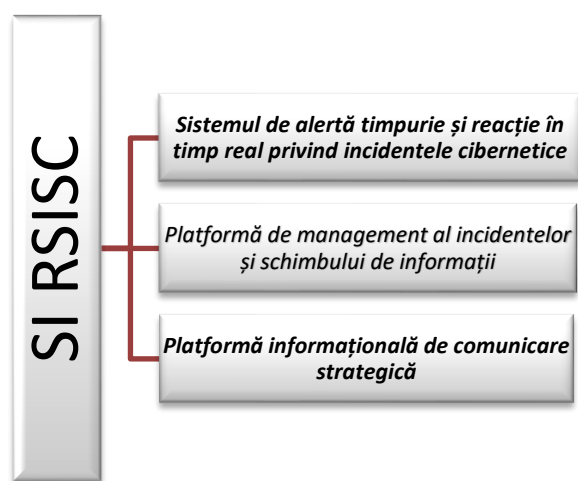
3) *Conturul Platformă informațională de comunicare strategică* – acest contur asigură comunicarea măsurilor necesare în prevenirea și răspunsul la incidente de securitate cibernetică pentru entitățile publice. Materialele furnizate de platforma informațională de comunicare strategică precum: ghidurile de securitate, bune practici și recomandările sunt publicate în scopul diseminării informațiilor privind riscurile de securitate cibernetică, care pot afecta sistemele informaționale și rețelele. În baza informațiilor furnizate de conturile funcționale: sistemul de alertă timpurie și reacție în timp real privind incidentele cibernetice și platforma de management al incidentelor și schimbului de informații, specialiștii CERT Gov vor identifica și promova informații relevante în scopul consolidării capacității de reacție la atacuri cibernetice. Conturul realizează următoarele funcții:

a) promovarea acțiunilor de sensibilizare și informare privind amenințări, vulnerabilități în spațiul cibernetic, riscuri de securitate cibernetică și măsuri de protecție necesare;

b) diseminarea informațiilor de securitate cibernetică, inclusiv a rezultatelor analizei incidentelor de securitate cibernetică, cu respectarea prevederilor acordurilor de cooperare ;

c) informarea aferent desfășurării exercițiilor și atelierelor de lucru în domeniul securității cibernetice;

d) publicarea ghidurilor de securitate cibernetică și a recomandărilor de soluționare a incidentelor de securitate cibernetică.



**Figura 1.** Contururile funcționale de bază ale SI RSISC

**16.** SI RSISC stabilește interconexiunea modulelor de lucru și urmează să îndeplinească în primul rând funcțiile specifice determinate de obiectivele,

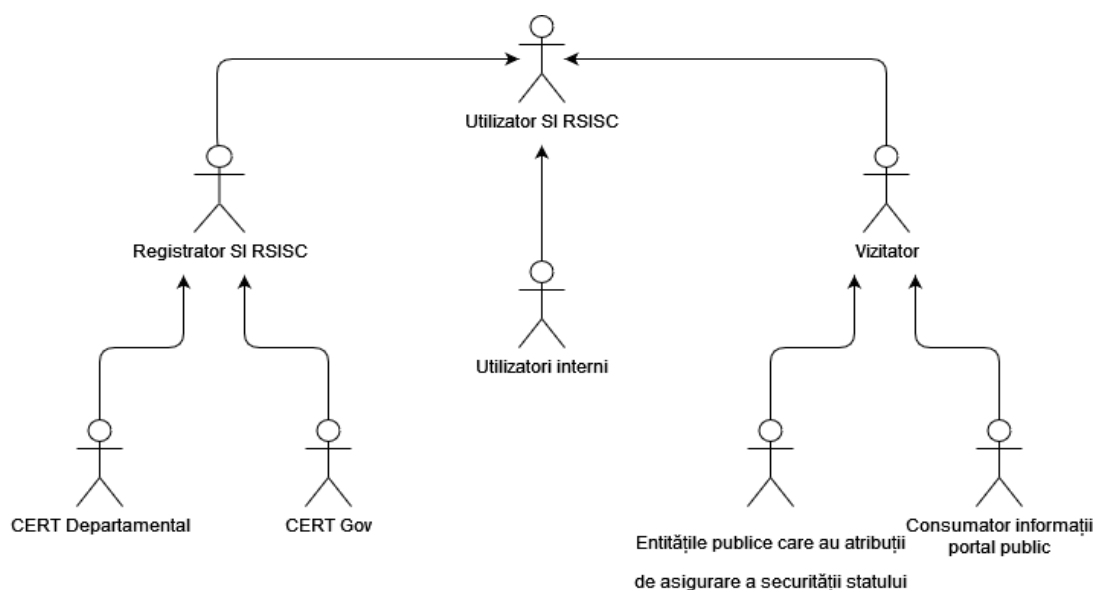
scopurile și destinația prezentului Concept. Pe lângă funcțiile de bază, SI RSISC va asigura realizarea unor funcții auxiliare necesare bunei funcționări ai acestuia.

**17. Funcții de audit și control:**

- 1) auditarea și inspecția activităților din cadrul SI;
- 2) păstrarea istoriei modificărilor și activităților SI;
- 3) colectarea statisticii și raportarea.

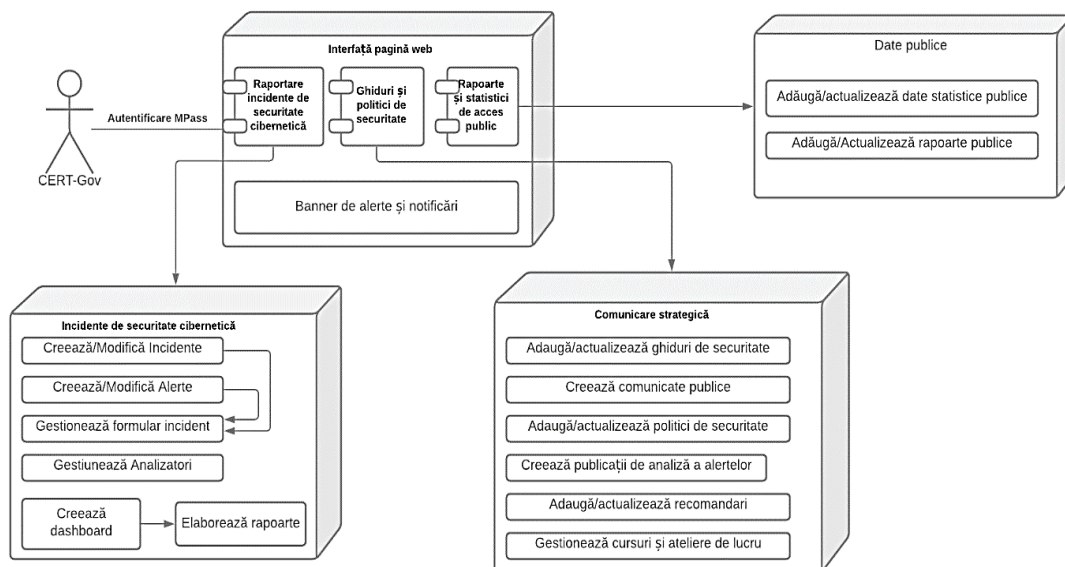
**18. SI RSISC va recunoaște cel puțin 3 tipuri de utilizatori, redați în figura 2:**

- 1) utilizatori interni – utilizatori cu drepturi depline asupra datelor și funcționalităților disponibile ale SI RSISC;
- 2) registrator – utilizator care operează, introduce sau modifică datele din cadrul SI RSISC, dar nu configurează însuși funcționalitățile SI;
- 3) vizitator – utilizator care are acces la vizualizarea informații, fără drepturi de a introduce/modifica/șterge date din cadrul sistemului.

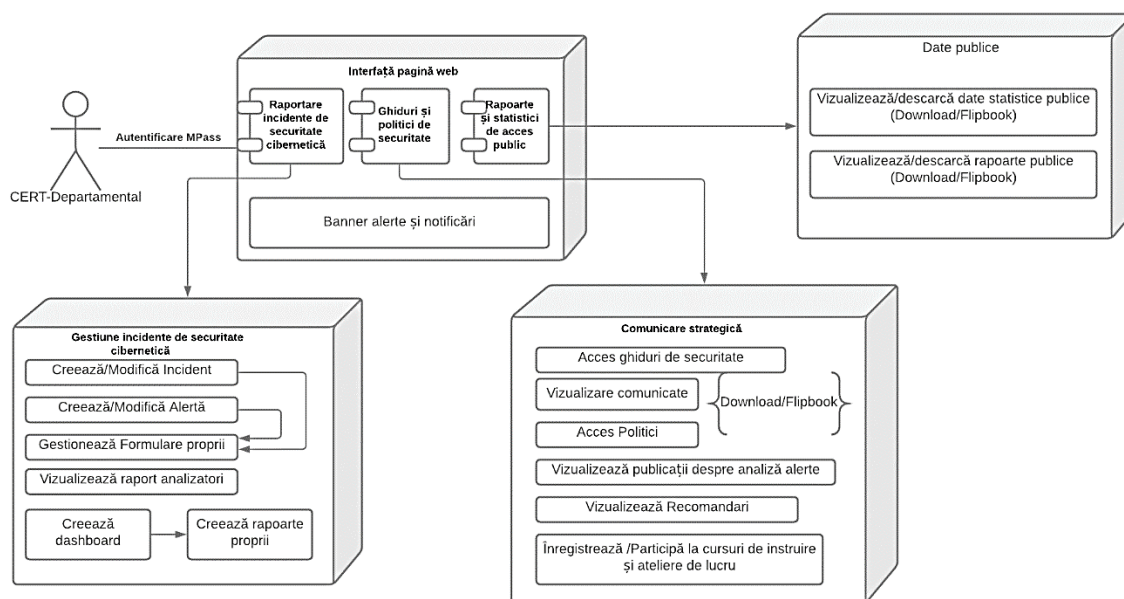


**Figura 2.** *Utilizatorii sistemului SI RSISC*

**19. Registratorul sistemului va avea acces la principalele funcționalități ale SI RSISC, conform atribuțiilor oferite de către posesor, conform figurii 3.**



**Figura 3. Registraturul CERT-Gov.**



**Figura 4. Registraturul CERT-departamental**

## V. STRUCTURA ORGANIZAȚIONALĂ A SI RSISC

**20.** Funcțiile de bază privind formarea și exploatarea SI RSISC sunt repartizate între posesor, deținător, utilizator, registratori, furnizor a datelor resursei informaționale.

**21.** Proprietarul SI RSISC este Statul.

**22.** Posesorul SI RSISC este STISC în calitate de CERT Gov, care are drept de gestionare și de utilizare a datelor și a resurselor informaționale și exercită atribuțiile deținătorului și administratorului tehnic al sistemului.

**23.** Registratorii SI RSISC sunt entitățile publice declarate conform Hotărârii Guvernului nr. 482/2020, precum și specialiștii CERT Gov.

1) Atribuțiile se transmit în temeiul actelor normative sau acordurilor încheiate între posesorul registrului și registrator.

2) 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. Înregistrarea prin sistem de subregistratură poate fi organizată pe criterii teritoriale sau pe alte criterii stabilite de posesorul registrului.

3) Registratorul sau participantul la schimbul de date este în drept, în temeiul acordului sau al legii, să delege funcții de introducere nemijlocită a datelor în registrul persoanei responsabile de aceasta, cu condiția capacității ei depline de exercițiu și calificării adecvate, în conformitate cu Legea nr.133/2011 privind protecția datelor cu caracter personal.

4) În cazul în care registratorul sau subregistratorul se schimbă, avizul respectiv urmează a fi publicat în mijloacele de informare în masă sau pe pagina web a deținătorului registrului, cu cel mult 10 zile calendaristice înainte de încetarea mandatului acestuia.

**24.** Furnizorii datelor în SI RSISC sunt STISC în calitate de CERT Gov, entitățile publice declarate conform Hotărârii Guvernului nr. 482/2020 și entitățile publice care au atribuții de asigurare a securității statului, cu următoarele funcții:

1) să asigure corectitudinea și autenticitatea datelor prezentate pentru a fi introduse în registru și actualizarea acestora în modul stabilit de lege sau acord.

2) în cazul modificării datelor obiectului registrului, furnizorul datelor registrului este obligat să informeze despre aceasta deținătorul registrului în modul stabilit de deținător.

3) în cazul solicitării de către deținătorul registrului sau registrator (subregistrator) a unor informații suplimentare despre obiectul supus înregistrării, furnizorul datelor registrului este obligat să răspundă la solicitare în termen de 10 zile lucrătoare.

4) să primească de la deținătorul registrului toate datele despre obiect care se conțin în registru și sînt prezentate de furnizor, inclusiv să adreseze registratorului (subregistratorului) interpelări despre existența atribuțiilor și volumul acestora.

**25.** Destinatari și utilizatori ai datelor din SI RSISC sunt angajații CERT Gov, entitățile publice, precum și cele care au atribuții de asigurare a securității statului. Drepturile și obligațiile destinatarului datelor registrului se stabilesc de legislația privind accesul la informație și de legislația cu privire la schimbul de date și interoperabilitate.

## **VI. CLASIFICAREA DOCUMENTELOR SISTEMULUI**

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

- 1) documente de intrare, în baza cărora sunt înregistrate incidentele de securitate cibernetică raportate;
- 2) documente interne precum 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;
- 3) documente de ieșire, documente obținute în rezultatul funcționării sistemului, precum rapoarte, statistici, diagrame aferent incidentelor de securitate cibernetică înregistrate;
- 4) documente tehnologice, care conțin informații ce descriu procesele tehnologice precum instrucțiuni de lucru.

**27.** Din categoria documente de intrare fac parte: informațiile furnizate de la conturul funcțional sistemului de alertă timpurie și reacție în timp real privind incidentele cibernetică, precum și informațiile furnizate prin canalele de comunicare menționate în pct.9 din Măsurile necesare pentru asigurarea securității cibernetică la nivel guvernamental, aprobate prin Hotărârea Guvernului nr. 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetică 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.

**28.** Fiecare incident de securitate cibernetică înregistrat, va stoca istoria modificărilor, documentele interne ale CERT Gov aferent prelucrării informațiilor de intrare precum și documentele de ieșire generate final de SI RSISC.

**29.** Din categoria documentelor interne fac parte rapoartele de analiză a incidentelor de securitate cibernetică generate de instrumentele de lucru ale conturului funcțional platforma de management a incidentelor de securitate informațională și schimb de informații, a cărui informații sunt ulterior folosite ca bază în gestionarea incidentului de securitate raportat.

**30.** Sistemul include o serie de documente și mijloace tehnologice precum: imagini scanate a documentelor, cuvinte-cheie ce facilitează căutarea incidentelor, lista utilizatorilor și drepturilor acestora, versiunile documentelor și modificările acestora; rapoarte și statistici agregate privind utilizarea SI RSISC.

**31.** Documentele de ieșire ale SI RSISC sunt: informații privind statutul incidentelor cibernetică, scrisorile de notificare aferent statutului incidentelor de

securitate cibernetică către raportorii incidentului de securitate cibernetică, precum și recomandări emise de către specialiștii CERT Gov (ex: bune practici, anexe aferent incidentelor notificate).

## **VII. SPAȚIUL INFORMAȚIONAL AL SI RSISC**

**32.** Obiectele informaționale vor fi create în baza datelor generate de sistemul de alertă timpurie și informare în timp real privind incidentele cibernetică, precum și prezentate de către parteneri și prin preluarea datelor primare din surse de date veridice.

**33.** Obiectele informaționale de bază ale SI RSISC sunt:

- 1) Incident de securitate cibernetică;
- 2) Alertă de securitate cibernetică.

**34.** Totalitatea identificatorilor obiectelor informaționale sunt determinate de scopul și destinația SI RSISC și includ colectarea următoarelor informații:

- 1) Metadate de trafic aferente comunicațiilor electronice;
- 2) Date aferent amenințărilor și vulnerabilităților în spațiul cibernetic;
- 3) Date aferent incidentelor de securitate cibernetică;
- 4) Date aferent tehnicilor și tehnologiilor folosite pentru atacuri;
- 5) Date aferent bunelor practici pentru protecția infrastructurilor cibernetică;
- 6) Date de identificare a utilizatorilor autorizați al SI RSISC împrumutate din alte sisteme informaționale de stat, menționate ulterior în pct.46.

**35.** Obiectul informațional Incident de securitate cibernetică va conține 2 scenarii de bază:

- 1) Incident de securitate cibernetică tipic, se referă la un caz de incident de securitate cibernetică înregistrat și gestionat în cadrul SI RSISC, care în baza datelor colectate este analizat în scopul oferirii suportului și remedierii după posibilitate. Cazul poate fi închis de către persoana desemnată responsabilă, după ce au fost luate toate măsurile prevăzute în procedurile operaționale de rigoare.
- 2) Incident de securitate escaladat, ce se referă la un caz de incident de securitate cibernetică deschis în cadrul SI RSISC, care în urma datelor colectate se constată a fi în afara atribuțiilor CERT Gov și necesită escaladarea către entitățile publice care au atribuții de asigurare a securității statului.. În scenariul respectiv persoana responsabilă de cazul dat în cadrul SI RSISC, desemnează o altă persoană responsabilă și consemnează prin comentariu motivul escaladării. Cazul incidentului de securitate poate fi închis de reprezentanții entităților publice desemnate responsabile de gestiune ulterioară a incidentului de securitate cibernetică, sau de către registratorul inițial al incidentului de securitate

cibernetică în cazul în care s-a depășit termenul limită de analiză a incidentului fără parvenirea unui raport.

**36.** Obiectul informațional Alertă de securitate cibernetică va conține 3 scenarii de bază:

1) Alertă pozitivă, ce se referă la activități anormale recepționate sau raportate prin

căile de comunicare aprobate, care au potențial de a degenera în vulnerabilitate cibernetică sau incident de securitate cibernetică. În scenariului respectiv, utilizatorii desemnați responsabili de alerta respectivă în cadrul SI RSISC, vor emite notificări în cadrul platformei de gestiune a incidentelor cibernetice și vor analiza activitatea anormală, în scopul identificării potențialelor riscuri de securitate cibernetică asociate alertei respective.

2) Alertă fals-pozitivă, ce se referă la cazul în care alertele recepționate prezintă

activități anormale, dar care nu reprezintă risc de securitate sau care nu au potențial de a deveni vulnerabilitate în spațiul cibernetic sau incident de securitate cibernetică. În scenariul respectiv, actorii desemnați responsabili de alerta respectivă în cadrul SI RSISC, vor închide alerta de securitate în cadrul SI RISC, cu mențiunile de rigoare în comentariu.

3) Alertă degenerată în incident de securitate cibernetică, se referă la cazul în care activitatea anormală raportată este rezultatul desfășurării unui atac cibernetic în timp real ce devine incident de securitate cibernetică. În scenariul dat, responsabilii de incidentul de securitate cibernetică identificat vor gestiona alertele, asociind în cadrul SI RSISC datele stocate despre alertă către cazul incidentului de securitate cibernetică deschis. Ca urmare alerta respectivă va obține statul de alertă închisă, cu menționarea în comentarii a identificatorului cazului incidentului de securitate cibernetică asociat.

**37.** Datele din cadrul formularelor de raportare a incidentelor și alertelor de securitate cibernetică sunt considerate confidențiale.

**38.** Obiectele informaționale de bază vor conține, în mod obligatoriu, următoarele atribute și date ce le caracterizează, precum:

1) elementele de identificare a resurselor și sistemelor informaționale de stat afectate;

2) descrierea succintă a incidentului sau alertei de securitate cibernetică;

3) data și ora detectării incidentului sau alertei de securitate cibernetică;

4) clasificarea incidentului sau alertei de securitate cibernetică;

5) măsuri preliminare întreprinse.

**39.** Formularele de raportare nu trebuie să conțină informații clasificate sau date care pot cauza atingere drepturilor și libertăților cetățenilor ori

intereselor legitime ale unor terțe entități implicate în incidentul de securitate raportat, în condițiile legii.

**40.** Registratorii din cadrul CERT Gov vor opera cu informațiile colectate în cadrul SI RSISC cu scopul:

- 1) corelării datelor aferent activităților anormale (alertelor) raportate spre identificarea preventivă unor incidente de securitate cibernetică potențiale;
- 2) diagnosticării specificii problemelor securității cibernetică a entităților publice și oferirii serviciilor de consultanță și elaborarea recomandărilor de soluționare și prevenire a incidentelor de securitate cibernetică;
- 3) întocmirii datelor statistice și a rapoartelor privind alertele, riscurile și incidentele de securitate cibernetică;
- 4) promovării bunelor practici aferent prevenției și minimizării impactului potențialelor incidente de securitate cibernetică.

**41.** După înregistrarea incidentului sau alertei de securitate cibernetică în cadrul SI RSISC, angajații CERT Gov:

- 1) analizează preliminar detaliile alertei sau incidentului de securitate cibernetică și sesizează ori notifică, după caz, alte entități afectate precum și autoritățile cu responsabilități în prevenirea, limitarea și combaterea efectelor incidentului de securitate cibernetică parvenit;
- 2) solicită, după caz, furnizorului de date informații suplimentare privind incidentul sau alerta de securitate cibernetică raportată, în vederea îndeplinirii obligațiilor ce îi revin, menționând termenul de furnizare a acestora;
- 3) oferă registratorilor, atunci când circumstanțele o permit, informații care ar putea sprijini gestionarea incidentului de securitate cibernetică;
- 4) coordonează la nivel guvernamental reacția la incidente de securitate cibernetică în colaborare cu celelalte entități publice, conform domeniului de activitate și responsabilitate.

**42.** Impactul unui incident de securitate cibernetică se determină ținând-se cont de numărul de utilizatori afectați de perturbarea serviciului și durata incidentului de securitate cibernetică.

**43.** CERT-Gov poate înștiința public despre o alertă sau un incident de securitate cibernetică, atunci când este necesară prevenirea unor potențiale incidente asemănătoare ca formă și conținut.

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



**45.** Arhitectura SI RSISC este concepută după schema-tip a infrastructurii informaționale a sistemului informațional și este găzduit pe platforma tehnologică guvernamentală comună (MCloud).

**46.** SI RSISC va conține și obiectele informaționale împrumutate din alte sisteme informaționale de stat precum:

1) *Registrul de stat al unităților de drept (RSUD)* – pentru recepționarea datelor de identificare a persoanelor juridice, utilizatori autorizați ai sistemului informațional SI RSISC.

2) *Registrul de stat al populației (RSP)* - pentru recepționarea datelor de identificare a persoanelor fizice, utilizatori autorizați ai sistemului informațional SI RSISC.

**47.** SI RSISC va fi integrat cu următoarele sisteme informaționale partajate relevante:

1) *platforma de interoperabilitate (MConnect)* – pentru recepționarea datelor aferente alertelor și incidentelor de securitate;

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

3) *serviciul electronic guvernamental de jurnalizare (MLog)* – pentru jurnalizarea evenimentelor de business critice;

4) *serviciul electronic guvernamental integrat de semnătură electronică (MSign)* – pentru aplicarea semnăturii electronice în cadrul proceselor de business ale SI RSISC;

5) *serviciul guvernamental de notificare electronică (MNotify)* – pentru notificarea utilizatorilor autorizați;

6) *Sistemul informațional automatizat registrul împuternicirilor de reprezentare în baza semnăturii electronice (MPower)* – pentru verificarea împuternicirilor de reprezentare a utilizatorilor necesare autorizării acțiunilor acestora;

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

**48.** Pentru asigurarea funcționalității eficiente și neîntrerupte a SI RSISC, schimbul informațional de date din cadrul sistemului informațional este asigurat în regim non-stop.

## **VIII. SPAȚIUL TEHNOLOGIC AL SI RSISC**

**49.** Spațiul tehnologic al SI RSISC reprezintă un complex informațional. Toate datele sistemului dat se depozitează într-o bază de date centralizată. Prezența componentelor software și a mijloacelor tehnologice în complexul

informațional respectiv este stabilită la etapa elaborării sarcinii tehnice și proiectului tehnic a sistemului.

**50.** Arhitectura complexului software-hardware se determină la etapa elaborării caietului de sarcini a SI RSISC. Aceasta reprezintă soluția constructivă a sistemului și reprezintă viziunea strategică managerială asupra proceselor de activitate în domeniu. Pentru arhitectura SI RSISC se insistă asupra respectării următoarelor principii:

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;

2) acceptarea soluțiilor care vor furniza o interfață web pentru utilizatorii sistemului;

3) minimizarea numărului diferitor tehnologii și produse care oferă aceleași funcționalități sau sunt similare după destinație;

4) recunoașterea informației ca patrimoniu și gestionarea ei adecvată;

5) implementarea funcționalităților de notificare prin e-mail a gestionării incidentelor înregistrate, către persoana ce a detectat și raportat incidentul cibernetic.

6) asigurarea confidențialității și integrității datelor prezentului sistem prin limitarea accesului în 2 etape: acces doar prin autentificare precum și stabilirea individuală a drepturilor de acces a utilizatorului la atributele sistemului de către administratorul SI RSISC.

**51.** Tipurile principale de standarde utilizate:

1) standardele datelor;

2) standardele metadatelor;

3) standardele schimbului de informații;

4) standardele de calitate;

5) standardele de securitate;

6) standardele de multilingvism;

**52.** Conformitatea cu aceste standarde va consta în:

1) susținerea interfeței browser-ului public pentru accesare;

2) XML ca mijloc principal pentru integrarea datelor;

3) utilizarea standardelor Internet și WWW-HTML, TCP/IP, SMTP;

4) utilizarea standardelor naționale și internaționale ISO.

**53.** În scenariul de bază privind gestiunea unui incident de securitate cibernetică în cadrul SI RSISC se vor parcurge câteva etape principale, redată în figura 5, și anume:

1) identificarea și raportarea evenimentelor/incidentelor de securitate cibernetică conform modului de interacțiune stabilite în Măsuri necesare pentru asigurarea securității cibernetică la nivel guvernamental aprobate prin Hotărârea Guvernului nr. 482/2020;

2) înregistrarea evenimentului/incidentului de securitate cibernetică și asignarea subdiviziunii/persoanei responsabile. Prioritizarea procesării incidentului conform evaluării impactului incidentului de securitate cibernetică ;

3) investigarea incidentelor de securitate cibernetică și identificarea cauzei producerii acestora, inclusiv a măsurilor de prevenire care vor asigura depistarea la timp a unor incidente similare;

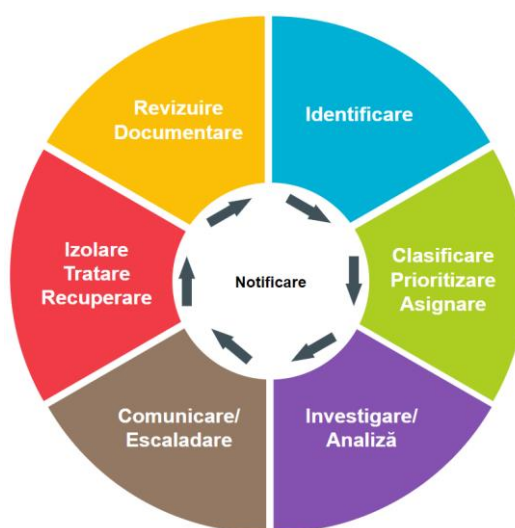
4) cooperarea eficientă și comunicarea permanentă, ce presupune schimbul de informații dintre diverse echipe de tip CERT, utilizatori, entități publice, după caz, sesizarea entităților publice care au atribuții de asigurare a securității statului.

5) escaladarea incidentelor de securitate cibernetică ce nu vizează domeniul de competență al CERT Gov și furnizarea entităților publice care au făcut raportarea informații relevante în ceea ce privește acțiunile ulterioare escaladării;

6) tratarea incidentelor de securitate cibernetică și oferirea recomandărilor de soluționare a acestora;

7) evidența și stocarea informațiilor aferent incidentelor de securitate cibernetică;

8) notificarea permanentă despre modificarea statutul incidentului de securitate cibernetică, precum și informarea registratorilor despre măsurile întreprinse.



**Figura 5.** Etapele de gestiune a unui incident de securitate cibernetică

**54.** Fluxurile informaționale ale sistemului SI RSISC sunt redată în figura 6.



4) elaborarea și răspândirea programelor ce afectează funcționarea normală a sistemelor informaționale și de comunicații electronice, precum și a sistemelor securității informaționale;

5) nimicirea, deteriorarea, suprimarea radioelectronică sau distrugerea mijloacelor și sistemelor de prelucrare a datelor, de comunicații electronice;

6) influențarea sistemelor cu parolă-cheie de protecție a sistemelor automatizate de prelucrare și transmitere a datelor;

7) compromiterea cheilor și mijloacelor de protecție criptografică a informației;

8) scurgerea informației prin canale tehnice;

9) implementarea dispozitivelor electronice pentru interceptarea informației în mijloacele tehnice de prelucrare, păstrare și transmitere a datelor utilizând sistemele de comunicații;

10) accesul nesanționat la resursele informaționale din băncile și bazele de date;

11) încălcarea restricțiilor legale privind răspândirea informației;

12) încălcarea prevederilor Legii nr. 133/2011 privind protecția datelor cu caracter personal.

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

1) accesul la date doar prin interfața unică de obiect;

2) delimitarea accesului utilizatorilor la date în conformitate cu rolurile acestora în SI RSISC;

3) dirijarea centralizată și controlul accesului la date;

4) înregistrarea jurnalelor de audit de securitate, pentru analiza integrității sistemului și pentru monitorizarea activității utilizatorilor;

5) crearea copiilor de rezervă (backup), pentru restabilirea sistemului și recuperarea datelor în caz de dezastru.

**59.** Sistemul asigură următoarele obiective de securitate:

1) *autentificarea* – garantează că sistemul va fi accesibil doar utilizatorilor cu o identitate verificată și confirmată;

2) *autorizarea* – utilizatorii autentificați pot accesa serviciile și datele care corespund drepturilor lor de acces;

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

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

**60.** 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.

**61.** Definirea utilizatorilor și grupurilor sau rolurilor, precum și atribuirea de drepturi se realizează de către utilizatori cu drepturi de administrator. Sistemul permite delegarea administrării drepturilor complet sau limitat la anumite operații.

**62.** Pentru gestiunea riscurilor de securitate vor fi implementate proceduri operaționale de răspuns la incidente cibernetice.

**63.** CERT Gov și entitățile publice prelucrează date cu caracter personal în conformitate cu prevederile Legii nr. 133/2011 privind protecția datelor cu caracter personal.

**64.** Prelucrarea de date în cadrul registrului de stat al incidentelor de securitate cibernetică trebuie să garanteze respectarea următoarelor reguli privind protecția datelor cu caracter personal:

- 1) specificarea și limitarea scopului;
- 2) adoptarea de măsuri tehnice și organizaționale în scopul asigurării unui nivel adecvat de protecție a datelor cu caracter personal, în conformitate cu prevederile legislației.

**65.** Informația comunicată reciproc între entitățile publice și CERT Gov va fi considerată drept confidențială și nu va fi divulgată în niciun mod, total sau parțial, decât în scopuri de efectuare a analizelor, investigațiilor, statisticilor sau alte cazuri prevăzute de legislație.

## **X. ÎNCHEIERE**

**66.** Prezentul Concept conține descrierea principalelor aspecte organizaționale privind crearea SI RSISC 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 de securitate cibernetică, monitorizarea și evidența alertelor, vulnerabilităților și incidentelor de securitate cibernetică identificate sau raportate, iar pe de altă parte se constituie interacțiunea CERT-urilor departamentale cu CERT Gov privind incidentele de securitate cibernetică și alte informații aferente.

**67.** Beneficiile Statului urmare a creării și implementării sistemului informațional sunt următoarele:

- 1) consolidarea capacității de răspuns la incidente de securitate cibernetică;

- 2) ameliorarea imaginii Republicii Moldova pe plan extern;
- 3) monitorizarea incidentelor de securitate cibernetică la nivel guvernamental.

**NOTA INFORMATIVĂ**  
**la proiectul hotărârii Guvernului**  
**cu privire la aprobarea Conceptului tehnic al Sistemului informațional automatizat**  
**„Registrul de stat al incidentelor de securitate cibernetică”**

**1. Denumirea autorului proiectului**

Proiectul hotărârii Guvernului cu privire la aprobarea Conceptului tehnic al Sistemului informațional automatizat „Registrul de stat al incidentelor de securitate cibernetică” este elaborat de către Viceprim-ministrul pentru digitalizare, cu suportul Cancelariei de Stat și al Instituției publice „Serviciul Tehnologia Informației și Securitate Cibernetică”.

**2. Condițiile ce au impus elaborarea proiectului și finalitățile urmărite**

Proiectul este elaborat în temeiul prevederilor art. 22 lit. d) din Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat, conform căruia „*Securitatea, inclusiv securitatea cibernetică, a sistemelor și resurselor informaționale de stat este asigurată de către autoritățile publice, instituțiile publice și alte entități de stat, în limita competențelor acestora și în conformitate cu reglementările stabilite de către Guvern*”, precum și în temeiul art.16 din Legea nr.71/2007 cu privire la registre, potrivit căruia Registrele de stat de bază și cele departamentale se instituie de Guvern sau de o altă autoritate publică abilitată prin lege, cu adoptarea deciziei de instituire a registrului

Necesitatea elaborării proiectului este dictată de prevederile pct. 4 al Hotărârii Guvernului nr.482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetică 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, conform căreia, *Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică”, va crea și va pune în aplicare Registrul de stat al incidentelor de securitate cibernetică, fiind totodată desemnată în calitate de Centru guvernamental de reacție la incidente de securitate cibernetică și punct unic de contact și de raportare a incidentelor de securitate cibernetică pentru structurile de tip CERT departamentale ale Guvernului.*

În prezent, pentru raportarea incidentelor de securitate cibernetică și alte date aferente acestora se utilizează procese semi-automatizate, ceea ce presupune numeroase riscuri privind: securitatea informației, integritatea datelor, istoricul modificărilor etc. Această metodă însă, nu asigură realizarea unei analize comprehensive, care ar permite identificarea cauzelor și a ariilor expuse riscului de securitate. Astfel, înregistrarea și monitorizarea tuturor tipurilor de incidente de securitate cibernetică, ar îmbunătăți aspecte ce țin de: definiția, clasificarea, învățarea din incidente.

Crearea Sistemul informațional automatizat „Registrul de stat al incidentelor de securitate cibernetică” (în continuare - SIA RSISC) 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 de securitate cibernetică, monitorizarea și evidența alertelor, vulnerabilităților și incidentelor de securitate cibernetică identificate sau raportate, iar pe de altă parte, se instituie și reglementează interacțiunea CERT-urilor departamentale cu CERT Gov privind incidentele de securitate cibernetică și alte informații aferente.

Beneficiile Instituției Publice „Serviciul Tehnologia Informației și Securitate Cibernetică” în urma implementării SIA RSISC sunt:

- 1) Optimizarea proceselor de lucru și reducerea costurilor operaționale;
- 2) Regăsirea rapidă a datelor și documentelor relevante pentru procesele de lucru;
- 3) Consolidarea unei baze de date electronice aferentă incidentelor de securitate cibernetică;
- 4) Consolidarea unei baze de cunoștințe ce ar contribui la îmbunătățirea calității funcționării CERT-ului;
- 5) Înregistrarea și evidența totalității documentelor aferente incidentelor de securitate cibernetică;
- 6) Standardizarea datelor și acuratețea informațiilor gestionate în sistem;
- 7) Reducerea birocrăției prin eliminarea treptată a evidențelor manuale;
- 8) Simplificarea procesului de introducere, modificare, actualizare a informațiilor aferente incidentelor de securitate cibernetică;



9) Centralizarea în format electronic a informațiilor cu privire la incidentele raportate de entitățile publice;

10) Posibilitate interoperabilității cu sisteme informatice ale instituțiilor partenere pentru schimbul bidirecțional de date.

Beneficiile funcționării SIA RSISC pentru entitățile publice sunt:

1) Asigurarea schimbului de date cu privire la incidentele de securitate cibernetică, în format electronic, între CERT Gov și CERT-urile departamentale, conform legislației;

2) Reducerea timpului mediu de raportare și răspuns la incidente de securitate cibernetică;

3) Creșterea acurateței și disponibilității datelor înregistrate în sistem;

4) Acces rapid și permanent la platformă informațională pentru gestiunea incidentelor de securitate cibernetică și obținerea consultațiilor și suportului necesar;

5) Asigurarea unui mediu operațional partajat, precum și a unei securități crescute a datelor electronice și informațiilor în cadrul și între autoritățile publice.

Beneficiile Statului ca urmare a creării și implementării SIA RSISC sunt:

1) Crearea sistemului automatizat privind evidența incidentelor de securitate cibernetică;

2) Consolidarea capacității de răspuns la incidente de securitate cibernetică;

3) Ameliorarea imaginii Republicii Moldova pe plan extern;

4) Monitorizarea incidentelor de securitate cibernetică la nivel guvernamental.

### ***3. Descrierea gradului de compatibilitate pentru proiectele care au ca scop armonizarea legislației naționale cu legislația Uniunii Europene***

Proiectul nu conține norme de armonizare a legislației naționale cu legislația Uniunii Europene.

### ***4. Principalele prevederi ale proiectului și evidențierea elementelor noi***

Proiectul cuprinde reglementări care au ca obiectiv instituirea SIA RSISC, stabilește scopurile, sarcinile și funcțiile sistemului, 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.

SIA RSISC va respecta Reglementarea tehnică „Procesele ciclului de viață al software-ului” RT38370656-002:2006, aprobată prin ordinul Ministerului Tehnologiei Informației și Comunicațiilor nr.78/2006.

SIA RSISC urmărește îmbunătățirea proceselor existente în cadrul CERT Gov, a modului de gestiune și răspuns la incidentele de securitate cibernetică, comunicarea strategică, precum și facilitarea raportării incidentelor de securitate cibernetică pentru structurile de tip CERT departamentale ale Guvernului.

Acesta va oferi funcționalități noi precum:

1) asigurarea formării resurselor informaționale de stat aferent incidentelor de securitate cibernetică;

2) dezvoltarea unei soluții tehnice flexibile și modulare care ar permite îmbunătățirea activității I.P „Serviciul Tehnologie Informației și Securitate Cibernetică” în rolul său de Centru guvernamental de răspuns la incidente de securitate cibernetică;

3) formarea bazei de date a incidentelor de securitate cibernetică la nivel guvernamental;

4) asigurarea evidenței amenințărilor, vulnerabilităților și incidentelor de securitate cibernetică identificate sau raportate, tehnicilor și tehnologiilor folosite pentru atacuri, precum și bunelor practici pentru protecția infrastructurilor cibernetice prin procese automatizate.

### ***5. Fundamentarea economico-financiară***

Asigurarea creării, implementării, funcționării și dezvoltării SIA RSISC se va efectua din contul și în limita mijloacelor financiare alocate din bugetul de stat și altor mijloace, conform legii.

### ***6. Modul de încorporare a actului în cadrul normativ în vigoare***

Proiectul nu impune modificarea sau abrogarea unor acte normative. Totodată, implementarea prevederilor prezentului proiect va condiționa elaborarea și aprobarea Regulamentului cu privire la

modalitatea de ținere a Registrului de stat al incidentelor de securitate cibernetică.

#### ***7. Avizarea și consultarea publică a proiectului***

În scopul respectării prevederilor Legii nr.100/2017 cu privire la actele normative și Legii nr.239/2008 privind transparența în procesul decizional, pe pagina web a Cancelariei de Stat ([www.cancelaria.gov.md](http://www.cancelaria.gov.md)), secțiunea – Transparența decizională, este asigurată plasarea:

- anunțului privind inițiativa de elaborare a proiectului, precum și
- proiectului, împreună cu Nota informativă.

Proiectul este înregistrat de către Cancelaria de Stat cu **numărul unic 161/CS/STISC/2021** și este supus avizării, inclusiv avizării/expertizării repetate, de către toate autoritățile și instituțiile a căror avizare/expertizare este necesară.

#### ***8. Constatările expertizei anticorupție***

Potrivit prevederilor art.28 alin.(2) lit.a) din Legea integrității nr. 82/2017, în coroborare cu art.24 și 35 din Legea cu privire la actele normative nr.100/2017, proiectul nu se supune expertizei anticorupție.

#### ***9. Constatările expertizei de compatibilitate***

Proiectul nu este elaborat în scopul armonizării legislației naționale cu legislația UE, exceptându-se astfel de la efectuarea expertizei de compatibilitate.

#### ***10. Constatările expertizei juridice***

Proiectul este supus expertizei juridice (*nr. 04/3123 din 04.04.2022 și nr. 04/4175 din 11.05.2022*), obiecțiile și propunerile fiind luate în considerare la definitivarea acestuia.

#### ***11. Constatările altor expertize***

Proiectul nu cade sub incidența altor expertize necesare de a fi efectuate în condițiile Legii nr.100/2017 cu privire la actele normative, dat fiind faptul că nu reglementează activitatea de întreprinzător, nu conține reglementări cu impact asupra bugetului public național sau a unor componente din cadrul acestuia și nu prevede reorganizări și reforme structurale sau instituționale ale autorităților ori ale instituțiilor publice. Prin urmare, proiectul nu cade sub incidența Metodologiei de analiză a impactului în procesul de fundamentare a proiectelor de acte normative, aprobată prin Hotărârea Guvernului nr.23/2019.

**Viceprim-ministru pentru Digitalizare**

**Iurie Țurcanu**