Proiect

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÎRE nr._____
din _____2021
mun. Chișinău

cu privire la aprobarea Conceptului tehnic al Sistemului Informațional Automatizat „Registrul de stat al incidentelor de securitate cibernetică”

În temeiul art. 10, art. 16, art. 22 și art.23, alin. (3) din Legea nr.467/2003 cu privire la informatizare şi la resursele informaționale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr.6-12, art.44), cu modificările ulterioare, şi 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

HOTĂRĂŞTE:

1. Se aprobă Conceptul Sistemului informaţional automatizat „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, funcţionarea şi dezvoltarea Sistemului informaţional automatizat „Registrul de stat al incidentelor de securitate cibernetică” va fi asigurată de către Instituția publică „Serviciul Tehnologia Informaţiei și Securitate Cibernetică”.

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

PRIM-MINISTRU

Contrasemnează:

Ministrul economiei și infrastructurii

Anexă

CONCEPT TEHNIC
al Sistemului Informațional Automatizat
„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, Hotărârii 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, Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică” (în continuare - STISC), în calitatea sa de Centru guvernamental de reacție la incidente de securitate cibernetică (în continuare - CERT Gov) și punct unic de contact și de raportare a incidentelor de securitate cibernetică pentru structurile de tip CERT departamentale ale Guvernului, asigură securitatea, inclusiv securitatea cibernetică, a resurselor şi sistemelor 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 subpunctul 7) și 8) ale Măsurilor necesare pentru asigurarea securității cibernetice 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 și incidentelor de securitate cibernetice 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 automatizat „Registrul de stat al incidentelor de securitate cibernetică” (în continuare - SIA 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 tehnic stabilește scopurile, sarcinile și funcțiile SIA 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. SIA RSISC va respecta reglementarea tehnică RT38370656-002:2006 „Procesele ciclului de viață al software-ului” aprobată prin ordinul Ministerului Tehnologiei Informației și Comunicațiilor nr.78/2006.

Beneficiile 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 ale CERT Gov;

3) consolidarea unei baze de date electronice aferentă incidentelor de securitate cibernetice;

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 birocrației 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. SIA RSISC reprezintă totalitatea sistematizată de date privind incidentele cibernetice 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. SIA RSISC este o componentă a Resurselor informaționale de stat ale Republicii Moldova.

3. SIA RSISC este sursa oficială de informație cu privire la incidentele de securitate cibernetică raportate la nivel guvernamental.

4. SIA 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 prevăzute prin Hotărârea Guvernului nr.482/2020 „Măsurile necesare pentru asigurarea securității cibernetice la nivel guvernamental”.

5. Destinația SIA 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 legislația în vigoare.

6. Crearea 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, pe de altă parte se constituie interacțiunea CERT-urilor departamentale cu CERT Gov privind incidentele de securitate cibernetică și alte informații aferente securității cibernetice.

7. SIA RSISC reprezintă un sistem oficial de identificare și gestionare a incidentelor cibernetice 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, SIA 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, organele de drept, 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 şi tehnică a modului în care politicile de securitate cibernetică sunt aplicate la nivelul infrastructurilor cibernetice, cu emiterea de recomandări pentru minimizarea riscurilor identificate;

bază de date - totalitate de date, organizate conform unei structuri conceptuale, ce descriu caracteristicile principale și raporturile dintre esențe, destinată unui domeniu sau mai multor domenii de aplicare;

CERT departamental - subdiviziune sau persoană responsabilă desemnată în cadrul entităților publice care dețin infrastructuri/sisteme de tehnologia informației și comunicații și care dispun de capacitatea necesară pentru a ține evidența operativă obligatorie și a raporta incidentele de securitate cibernetică;

entități publice - ministerele, alte autorități administrative centrale subordonate Guvernului, Cancelaria de Stat și structurile organizaționale din sfera lor de competență (autoritățile administrative din subordine, serviciile publice desconcentrate și cele aflate în subordine, precum și instituțiile publice și întreprinderile de stat în care ministerul, Cancelaria de Stat sau altă autoritate administrativă centrală are calitatea de fondator) și organizațiile de stat autonome înființate de Guvern;

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

incident de securitate cibernetică - eveniment survenit în spațiul cibernetic ale cărui consecințe afectează securitatea cibernetică.

Platforma MCloud - infrastructură informațională guvernamentală comună care funcționează în baza tehnologiei de „cloud computing” găzduită în infrastructura consolidată de centre de date;

metadate - 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 ciclu de viață al sistemului;

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

securitate cibernetică - stare de normalitate rezultată în urma aplicării unui ansamblu complex de măsuri pro active şi reactive prin care în spațiul cibernetic se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea şi non repudierea informațiilor în format electronic, a sistemelor şi resurselor informaționale, a serviciilor electronice publice și private. Măsurile pro active şi reactive includ politici, concepte, standarde şi ghiduri de securitate, managementul riscului, activități de instruire şi conştientizare, implementarea de soluții tehnice de protecție a infrastructurilor cibernetice, managementul identității, managementul consecințelor;

sistem de alertă timpurie și informare în timp real privind incidentele cibernetice - ansamblul de proceduri și sisteme tehnice care au rolul de a identifica premisele de apariție a incidentelor cibernetice și de a avertiza în cazul producerii acestora. Sistemul include și conexiuni de date ce vor transporta informații referitoare la incidentele cibernetice identificate de senzori dedicați, precum și informații statistice referitoare la valorile de trafic înregistrate în nodurile de rețea ale infrastructurilor cibernetice ce asigură funcționalități de utilitate publică ori asigură servicii ale societății informaționale;

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

10. Scopul SIA 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 și incidentelor de securitate cibernetică identificate sau raportate, tehnicilor și tehnologiilor folosite pentru atacuri, precum și bunelor practici pentru protecția infrastructurilor cibernetice;

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

11. Sarcinile de bază realizate la exploatarea SIA RSISC sunt:

1) identificarea, înregistrarea, clasificarea și analiza incidentele de securitate cibernetică și coordonarea, cooperarea și sesizarea organelor de drept, după caz;

2) asigurarea cadrului organizatoric și suportul tehnic necesar schimbului de informații dintre diverse echipe de tip CERT, utilizatori, entități publice;

3) crearea și menținerea unei baze de date a incidentelor de securitate cibernetică și a măsurilor întreprinse pentru înlăturarea și/sau contracararea acestora;

4) conectarea și realizarea schimbului de date între CERT-uri departamentale și CERT Gov prin intermediul unei platforme dedicate;

5) promovarea bunelor practici între specialiștii CERT Gov și persoanele responsabile de răspuns la incidente de securitate cibernetică din cadrul entităților publice;

6) întocmirea datelor statistice și elaborarea rapoartelor cu privire la incidente de securitate cibernetică înregistrate, precum și dinamica acestor incidente;

7) asigurarea implementării politicilor de prevenire și contracarare a incidentelor cibernetice potrivit competenței;

8) oferirea unei platforme informaționale de comunicare strategică.

12. Principiile de bază ale SIA RSISC sunt:

principiul legalității, care presupune crearea și exploatarea sistemului în conformitate cu legislația națională;

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;

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;

principiul modularității și scalabilității - posibilitatea de a dezvolta sistemul fără modificarea componentelor create anterior.

III. SPAȚIUL JURIDICO-NORMATIV AL FUNCȚIONĂRII SIA RSISC

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

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

2) Legea 71/2007 cu privire la registre;

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

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

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

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

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

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

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

10) 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;

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

12) Hotărârea Guvernului nr. 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental și modificarea HG 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 SIA RSISC se vor respecta următoarele standarde tehnice:

1) Standardul Republicii Moldova SM EN ISO/IEC 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 EN ISO/IEC 27005:2018 „Tehnologia informației. Tehnici de securitate. Managementul Riscului securității informaționale."

IV. SPAȚIUL FUNCȚIONAL AL SIA RSISC

15. Contururile funcționale principale ale SIA RSISC sunt:

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/sau 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 SIA 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 SIA RSISC este stabilit în Regulamentul privind ținerea „Registrului de stat al incidentelor de securitate cibernetică";

c) gestionarea incidentelor de securitate. Se asigură înregistrarea, clasificarea, analiza incidentelor de securitate cibernetică. De asemenea, are loc evidența amenințărilor și/sau vulnerabilităților 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/sau 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* – aceast contur asigură comunicarea măsurilor necesare în prevenirea și/sau 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 contururile 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, 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.

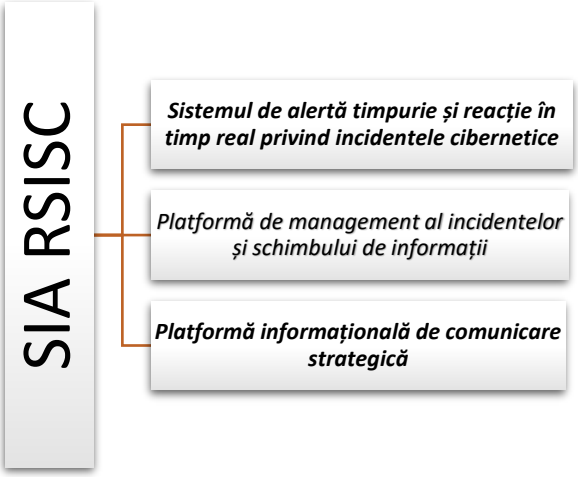


Figura 1 – Contururile funcționale de bază ale SIA RSISC

16. SIA 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, SIA 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 SIA;
2) păstrarea istoriei modificărilor și activităților SIA;
3) colectarea statisticii și raportarea.

18. SIA RSISC va recunoaște cel puțin 3 tipuri de utilizatori:

1) administrator – utilizator cu drepturi depline asupra datelor și funcționalităților disponibile ale SIA RSISC;

2) registrator – utilizator care operează, introduce și/sau modifică datele din cadrul SIA RSISC, dar nu configurează însuși funcționalitățile SIA;

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

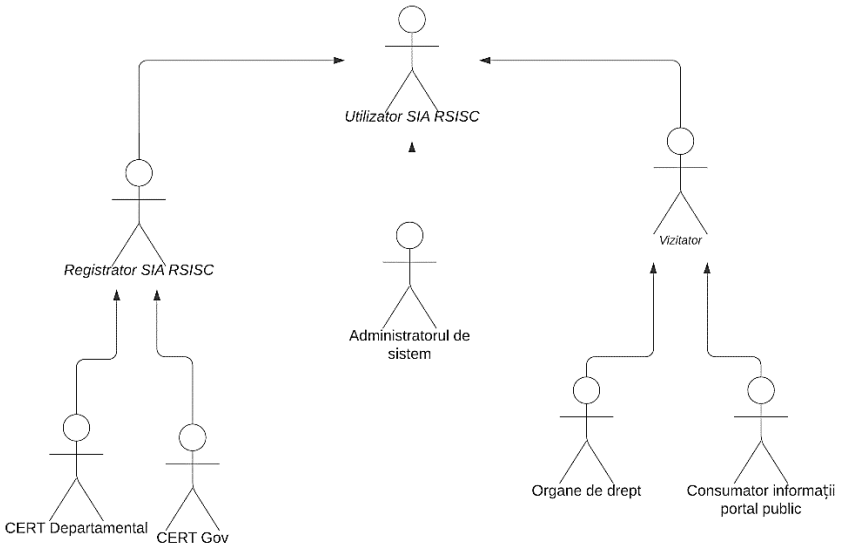


Figura 2 – Actorii sistemului SIA RSISC

19. Registratorul sistemului va avea acces la principalele funcționalități ale SIA RSISC, conform atribuțiilor oferite de către Administrator.

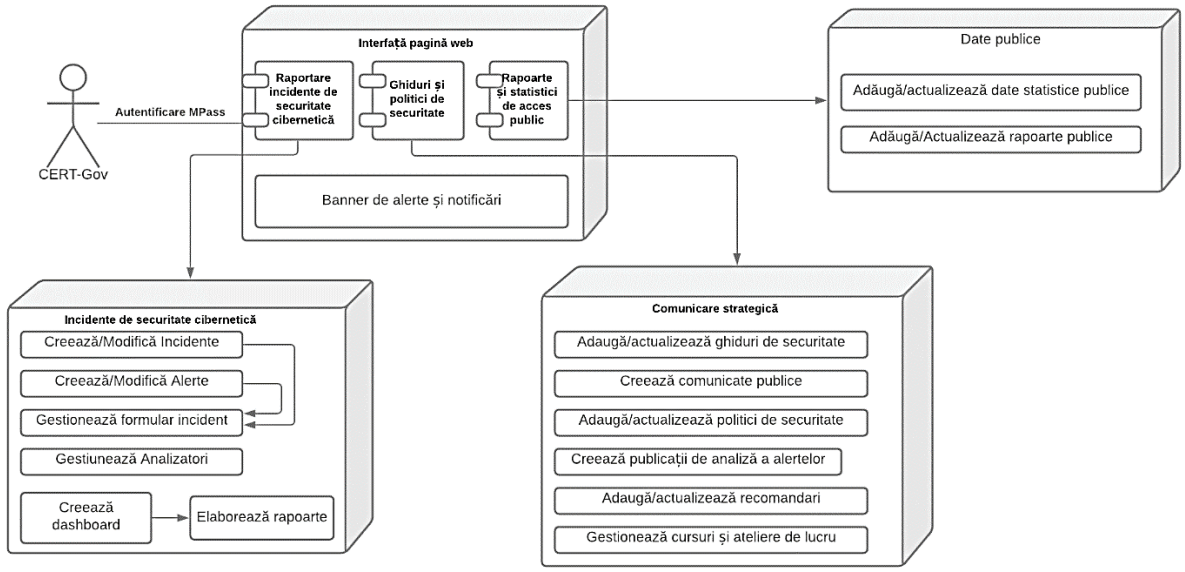


Figura 3 – Registratorul CERT-Gov

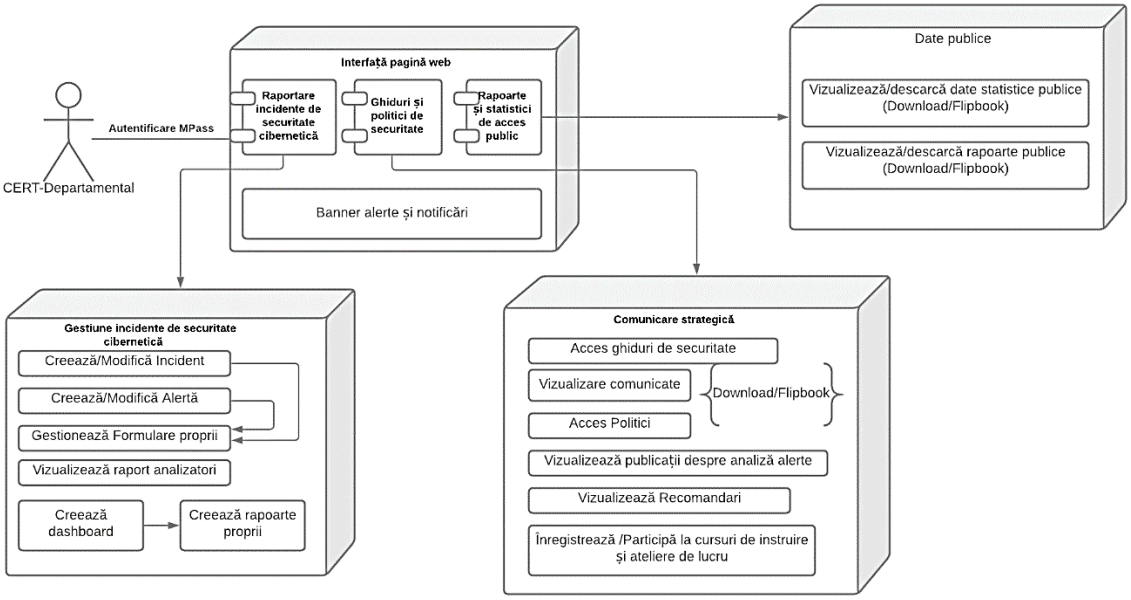


Figura 4 – Registratorul CERT-departamental

V. SPAȚIUL ORGANIZATORIC AL SIA RSISC

20. Funcțiile de bază privind formarea și exploatarea SIA RSISC sunt repartizate între posesor, administrator, utilizator și furnizor a datelor resursei informaționale.

21. Proprietarul SIA RSISC este Statul.

22. Posesorul SIA RSISC este STISC, care are drept de gestionare și de utilizare a datelor și a resurselor și exercită atribuțiile deținătorului și administratorului tehnic al sistemului.

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

24. Furnizorii datelor în SIA RSISC sunt STISC, entitățile publice și organele de drept declarate conform Hotărârii Guvernului nr. 482/2020.

25. Destinatari ai datelor din SIA RSISC sunt angajații CERT Gov, entitățile publice și organele de drept, conform prevederilor Hotărârea Guvernului nr.482/2020.

VI. CLASIFICAREA DOCUMENTELOR SISTEMULUI

26. În cadrul SIA 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/sau 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 cibernetice, precum și informațiile furnizate prin canalele de comunicare menționate în pct.9 cap. III al Hotărârii Guvernului nr. 482/2020.

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 SIA 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 SIA RSISC.

31. Documentele de ieșire ale SIA RSISC sunt: informații privind statutul incidentelor cibernetice, 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 SIA RSISC

32. Resursele informaționale vor fi create în baza datelor prezentate de către furnizori și prin preluarea datelor primare din alte surse de date administrative.

33. Totalitatea obiectelor informaționale sunt determinate de scopul și destinația SIA RSISC și includ colectarea următoarelor informații:

1) Metadate de trafic telecomunicațional;

2) Date aferent incidentelor de securitate cibernetica.

34. Datele din cadrul formularului de raportare a incidentelor de securitate cibernetică sunt considerate confidențiale.

35. Raportarea incidentelor de securitate cibernetică conține, în mod obligatoriu, următoarele informații:

1) elementele de identificare a resurselor și sistemelor informaționale de stat afectate;
2) descrierea succintă a incidentului de securitate cibernetică;
3) data și ora detectării incidentului de securitate cibernetică;
4) clasificarea incidentului de securitate cibernetică;
5) măsuri preliminare întreprinse;

36. Formularele de raportare a incidentelor de securitate cibernetică 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.

37. Registratorii din cadrul CERT Gov vor opera cu informațiile colectate în cadrul SIA RSISC cu scopul:

1) corelării datelor aferent activităților anomale raportate spre identificarea preventivă unor incidente de securitate cibernetică potențiale;

2) diagnosticării specificii problemelor securității cibernetice 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 riscurile și incidentele de securitate cibernetică;

4) promovării bunelor practici aferent prevenției și/sau minimizării impactului potențialelor incidente de securitate cibernetică;

38. După înregistrarea incidentului de securitate cibernetică în cadrul SIA RSISC, angajații CERT Gov:

1) analizează preliminar detaliile 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 de securitate cibernetică raportat, 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 administrarea incidentului de securitate cibernetică;

4) coordonează la nivel guvernamental răspunsul la incidente de securitate cibernetică în colaborare cu celelalte entități publice, conform domeniului de activitate și responsabilitate.

39. 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.

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

VIII. SPAȚIUL TEHNOLOGIC AL SIA RSISC

41. Spațiul tehnologic al SIA RSISC reprezintă un complex informațional. Toate datele sistemului dat se depozitează într-o bază de date centralizată. Prezența componentelor software şi a mijloacelor tehnologice în complexul informațional respectiv este stabilită la etapa elaborării sarcinii tehnice şi proiectului tehnic a sistemului.

42. Arhitectura complexului software-hardware se determină la etapa elaborării caietului de sarcini a SIA RSISC. Aceasta reprezintă soluția constructivă a sistemului și reprezintă viziunea strategică managerială asupra proceselor de activitate în domeniu. Pentru arhitectura SIA 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 SIA RSISC.

43. 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;

44. 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.

45. În scenariul de bază privind gestiunea unui incident de securitate cibernetică în cadrul SIA RSISC se vor parcurge câteva etape principale și anume:

1) identificarea și raportarea evenimentelor/incidentelor de securitate cibernetică conform modului de interacțiune stabilit în 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 schimbului de informații dintre diverse echipe de tip CERT, utilizatori, entități publice. După caz, sesizarea organelor de drept privind incidentele de securitate cibernetică ce nu vizează domeniul de competență al CERT Gov și furnizează entităților publice care au făcut raportarea informații relevante în ceea ce privește acțiunile ulterioare escaladării;

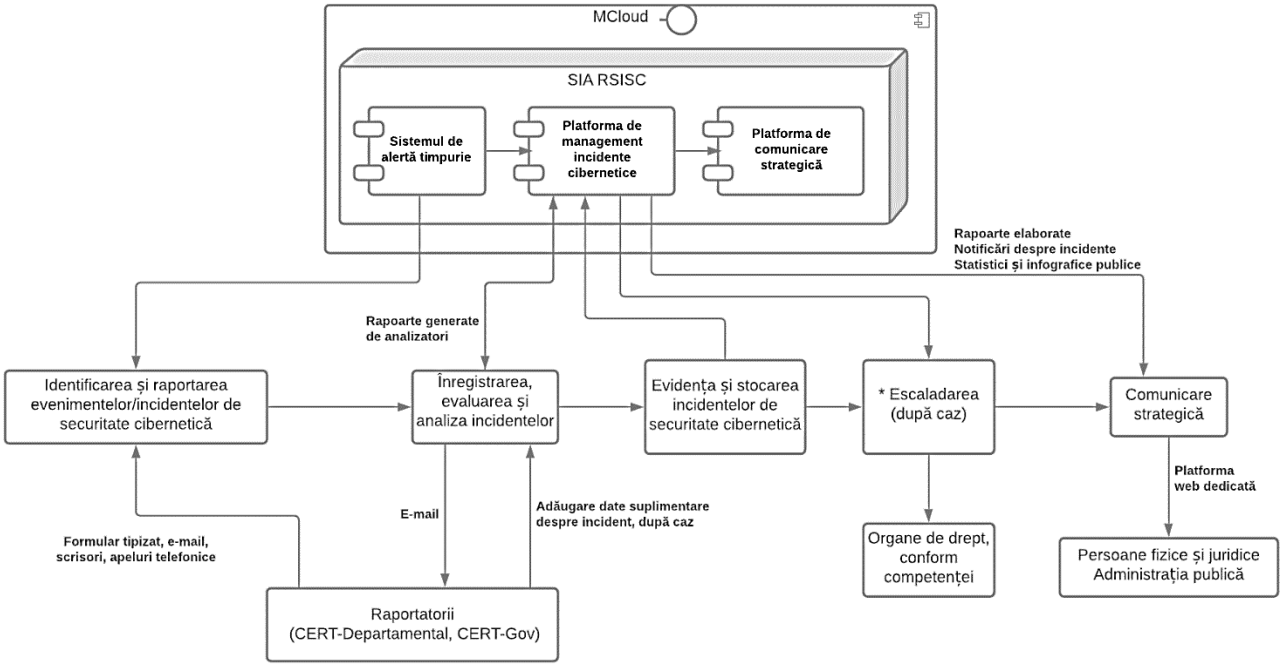
5) tratarea incidentelor de securitate cibernetică și oferirea recomandărilor de soluționare a acestora;

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

7) 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

46. Fluxurile informaționale ale sistemului SIA RSISC sunt redate în figura următoare.



IX. SECURITATEA INFORMAȚIEI ȘI PROTECȚIA DATELOR CU CARACTER PERSONAL

47. Prin securitatea informației se înțelege protecția resurselor și a infrastructurii informaționale a SIA RSISC împotriva acțiunilor premeditate sau accidentale cu caracter natural sau artificial, care au ca rezultat cauzarea prejudiciului participanților la procesul de schimb informațional.

48. Noțiunea de securitate informațională a SIA RSISC include o serie de termeni cum ar fi: măsuri de prevenție, măsuri de reacție și măsuri de contracarare, politici, tehnologii, structură organizațională, atribuții și funcții în sistem. Este necesară identificarea acestor mijloace de control pentru a asigura și implementa securitatea informațională în SIA RSISC;

49. Pericolele securității informaționale sunt:

1) colectarea și utilizarea ilegală a datelor;

2) încălcarea tehnologiei de prelucrare a datelor;

3) implementarea în produsele software și hardware a componentelor care îndeplinesc funcții neprevăzute în documentația aferentă acestor produse;

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

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

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 nesancționat 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.

50. 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 SIA RSISC;

3) dirijarea centralizată și controlul accesului la date.

51. Sistemul asigură următoarele obiective de securitate:

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

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

confidențialitatea – garantează că datele înregistrate nu pot fi accesate de o terță neautorizată;

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

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

53. 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.

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

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

56. 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.

57. 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. INTERACȚIUNEA CU ALTE SISTEME INFORMAȚIONALE

58. SIA RSISC este un sistem modular compatibil cu tehnologii de cloud computing (nor informațional), care asigură posibilitatea dezvoltării sale fără perturbarea continuității funcționării.

59. Arhitectura SIA RSISC este concepută după schema-tip a infrastructurii informaționale a sistemului informațional automatizat.

60. SIA RSISC utilizează serviciile guvernamentale de platformă MPass, MLog și este găzduit pe platforma tehnologică guvernamentală comună MCloud.

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

XI. IMPACTUL GENERAL

62. Prezentul concept este viziunea privind componentele și posibilitățile viitoare ale SIA RSISC. Recomandările principale, expuse în cadrul documentului, oferă beneficii care depășesc potențialele implicații negative.

63. Neimplementarea SIA RSISC poate avea un impact negativ substanțial asupra activității CERT Gov şi asupra aspectului de securitate, integritate şi veridicitate a datelor aferent incidentelor de securitate cibernetică colectate de către CERT Gov. Odată cu creșterea volumului de date, în lipsa unui sistem informațional automatizat, administrarea lor devine mai complicată şi ineficientă, implicând şi riscul pierderii complete al acestora.