CAIET DE SARCINI

destinat elaborării Sistemului Informațional Automatizat „Registrul de stat al incidentelor de securitate cibernetică”

CUPRINS

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 și 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 MS Excel. 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 Sistemului 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 furnizarea următoarelor beneficii:

- optimizarea proceselor de lucru și reducerea costurilor operaționale;
- regăsirea rapidă a datelor și documentelor relevante pentru procesele de lucru ale CERT Gov;
- consolidarea unei baze de date electronice aferentă incidentelor de securitate cibernetice;
- consolidarea unei baze de cunoștințe ce ar contribui la îmbunătățirea calității funcționării CERT Gov;
- înregistrarea și evidența totalității documentelor aferente incidentelor de securitate cibernetică;
- standardizarea datelor și acuratețea informațiilor gestionate în sistem;
- reducerea birocrației prin eliminarea treptată a evidențelor manuale;
- simplificarea procesului de introducere, modificare, actualizare a informațiilor aferente incidentelor de securitate cibernetică;

- centralizarea în format electronic a informațiilor cu privire la incidentele raportate de entitățile publice;
- asigurarea interoperabilității cu sisteme informatice ale entităților publice pentru schimbul bidirecțional de date.
- asigurarea schimbului de date cu privire la incidentele de securitate cibernetică, în format electronic, între CERT Gov și CERT departamentale, conform legislației;
- reducerea timpului mediu de raportare și răspuns la incidente de securitate cibernetică;
- asigurarea unui mediu operațional partajat, precum și a unei securități crescute a datelor electronice și informațiilor în cadrul și între entitățile publice.

Prezentul document prezintă o viziune conceptuală asupra dezvoltării, implementării și Exploatării Sistemului Informațional Automatizat „Registrul de stat al incidentelor de securitate cibernetică” incluzând aspecte privind scopul și obiectivele, principiile, caracteristicile de bază, funcționalitatea și arhitectura conceptuală, cerințele funcționale și nefuncționale ale sistemului informatic.

În acest sens este prezentată o descriere succintă a componentelor de bază ale viitoarei soluții accentuând principiile și particularitățile de implementare a funcționalităților și fluxurilor de lucru de care trebuie să se țină cont la elaborarea Sistemului Informațional Automatizat „Registrul de stat al incidentelor de securitate cibernetică”.

1. Informație generală

1.1. Noțiuni utilizate

Acronimele și abrevierile principale utilizate în prezentul document sunt delimitate în tabelul 1.1.

Tabelul 1.1. Abrevierile și acronimele utilizate în document

Nr.	Abreviere/Acronim	Descriere
1.	AP	Autoritate publică
2.	BD	Bază de Date
3.	STISC	Serviciul Tehnologia Informației și securitate Cibernetică
4.	COTS	Commercial off-the-shelf
5.	KPI	Key Performance Indicators (Indicatori cheie de performanță)
6.	PDGD	Portalul Datelor Guvernamentale Deschise
7.	QBE	Query by Example
8.	SDD	Software design document.
9.	SGBD	Sistem de gestiune a bazelor de date
10.	SI	Sistem Informatic
11.	SLA	Service Levele Agreement
12.	SPOF	Single Point of Failure
13.	SRS	Software Requirements Specification
14.	TI	Tehnologie informatică
15.	TIC	Tehnologie Informatică și de Comunicație
16.	TLS/SSL	Protocolul TLS sau predecesorul său, Protocolul SSL, sunt protocoale criptografice care asigură comunicarea sigură între 2 noduri ale rețelei de calculatoare pentru acțiuni cum ar fi vizitarea paginilor Web, e-mail, internet-fax, schimb de mesaje instantanee și alte transferuri de date.

Definițiilor noțiunilor frecvent utilizate în prezentul document sunt explicate în tabelul 1.2.

Tabelul 1.2. Definiții și noțiuni utilizate în document

Nr.	Abreviere/Acronim	Descriere
1.	Atac cibernetic	Acțiune ostilă, desfășurată în spațiul cibernetic, de natură să afecteze securitatea cibernetică.
2.	Audit de securitate cibernetică	Evaluare sistemică, detaliată, măsurabilă și tehnică a modului în care politicile de securitate cibernetică sunt aplicate la nivelul infrastructurilor cibernetice, cu emiterea de recomandări pentru minimizarea riscurilor identificate.

Nr.	Abreviere/Acronim	Descriere
3.	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.
4.	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.
5.	Credențiale	Set de atribute ce stabilesc identitatea și autenticitatea utilizatorilor și sistemelor în cadrul sistemelor informaționale.
6.	Date	Unități informaționale elementare despre persoane, subiecte, fapte, evenimente, fenomene, procese, obiecte, situații etc. prezentate într-o formă care permite notificarea, comentarea și procesarea lor.
7.	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.
8.	Incident de securitate cibernetică	Eveniment survenit în spațiul cibernetic ale cărui consecințe afectează securitatea cibernetică.
9.	Integritatea datelor	Stare a datelor, când acestea își păstrează conținutul și sunt interpretate univoc în cazuri de acțiuni aleatorii. Integritatea se consideră păstrată dacă datele sunt corecte și este asigurată încrederea în ele.
10.	Jurnalizare	Funcție de înregistrare a informației despre evenimente. În cadrul sistemelor informaționale înregistrările despre evenimente includ detalii despre data și ora, utilizatorul, datele personale identificate, acțiunea întreprinsă.
11.	Metadate	Modalitate de atribuire de valoare semantică datelor stocate în baza de date (date despre date).
12.	Obiect informațional	Reprezentare virtuală al entităților materiale și nemateriale existente.
13.	Platforma MCloud	Infrastructură informațională guvernamentală comună care funcționează în baza tehnologiei de „cloud computing” găzduită în infrastructura consolidată de centre de date.
14.	Risc de securitate în spațiul cibernetic	Probabilitate ca o amenințare să se materializeze, exploatând o anumită vulnerabilitate specifică infrastructurilor cibernetice.

Nr.	Abreviere/Acronim	Descriere
15.	Securitate cibernetică	Stare de normalitate rezultată în urma aplicării unui ansamblu complex de măsuri pro active și reactive prin care în spațiul cibernetic se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și non repudierea informațiilor în format electronic, a sistemelor și resurselor informaționale, a serviciilor electronice publice și private. Măsurile pro active și reactive includ politici, concepte, standarde și ghiduri de securitate, managementul riscului, activități de instruire și conștientizare, implementarea de soluții tehnice de protecție a infrastructurilor cibernetice, managementul identității, managementul consecințelor
16.	SIA RSISC	Sistem informatic destinată colectării, sistematizării și gestiunii datelor 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.
17.	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.
18.	Sistem informatic	Ansamblu de programe și echipamente care asigură prelucrarea automată a datelor (componenta automatizată a sistemului informațional).
19.	Sistem Informațional	Sistem de prelucrare a informației, împreună cu resursele organizaționale asociate, cum ar fi resursele umane și tehnice, care furnizează și distribuie informația.
20.	Software Design Document	Document director al sistemului informatic care cuprinde descrierea detaliată a următoarelor viziuni: structurile de date și constrângerile acestora, arhitectura sistemului informatic care oferă totalitatea secțiunilor conceptuale ale sistemului informatic, interfața sistemului informatic care cuprinde conceptualizarea totalității componentelor interfeței utilizator sistemului informatic, funcționalitățile sistemului informatic care cuprinde descrierea detaliată a totalității scenariilor de implementare a sistemului informatic.
21.	Software Requirements Specification	Document care conține descrierea detaliată a totalității scenariilor de interacțiune între utilizatori și aplicația informatică.
22.	Tehnologie informatică și de comunicație	Termen comun care include toate tehnologiile utilizate pentru schimbul și manipularea informației.

Nr.	Abreviere/Acronim	Descriere
23.	Veridicitatea datelor	Nivel de corespundere a datelor, păstrate în memoria calculatorului sau în documente, stării reale a obiectelor din domeniul respectiv al sistemului, reflectate de aceste date.
24.	Vulnerabilitate în spațiul cibernetic	Ineficacitate în proiectarea și implementarea infrastructurilor cibernetice sau a măsurilor de securitate aferente, care poate fi exploatată de către o amenințare

1.2. Referințe și aspecte legale pentru elaborarea sistemului informatic

Analizând cadrul normativ-legislativ în vigoare al Republicii Moldova și practica internațională pot fi evidențiate un șir de acte, standarde și bune practici, prevederile cărora trebuie luate în considerație la proiectarea, dezvoltarea și implementarea SIA RSISC.

În acest sens, pentru dezvoltarea, implementarea și funcționarea SIA RSISC a fost identificat un set de 47 acte juridice și normative grupate în funcție de gradul de aplicabilitate după cum urmează:

- cadrul normativ național aferent proceselor de business ale SIA RSISC;
- cadrul normativ național în domeniul informatizării și tehnologiei informației;
- standarde și bune practici în domeniul TIC.

II. Cadrul normativ național aferent proceselor de business ale SIA RSISC:

1. Hotărârea Guvernului nr. 811 din 29.11.2015 cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, Monitorul Oficial nr. 306-310 din 13.11.2015.
2. Hotărârea Guvernului nr. 201 din 28.03.2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică, Monitorul Oficial nr. 109-118 din 07.04.2017.
3. Hotărârea Guvernului nr. 414 din 08.05.2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat, Monitorul Oficial nr. 157-166 din 18.05.2018.
4. Hotărârea Guvernului nr. 482 din 08.07.2020 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, Monitorul Oficial nr. 180-187 din 17.07.2020.
5. Hotărârea Guvernului nr. 822 din 11.01.2020 cu privire la aprobarea acțiunilor necesare a fi întreprinse ca urmare a inventarierii resurselor și sistemelor informaționale de stat existente și a modificărilor ce se operează în unele hotărâri ale Guvernului, Monitorul Oficial nr. 304-312 din 20.11.2020.

II. Cadrul normativ național în domeniul informatizării și tehnologiei informației:

6. Legea nr. 982 din 11.05.2000 privind accesul la informație, Monitorul Oficial nr. 88-90 din 28.07.2000;
7. Legea nr. 1069 din 22.06.2000 cu privire la informatică, Monitorul Oficial nr. 73-74 din 05.07.2001.

8. Legea nr. 467 din 21.11.2003 cu privire la informatizare și la resursele informaționale de stat, Monitorul Oficial nr. 6-12 din 01.01.2004;
9. Legea Nr. 71 din 22.03.2007 cu privire la registre, Monitorul Oficial nr. 70-73 din 25.05.2007.
10. Legea nr. 241 din 15.11.2007 a comunicațiilor electronice, Monitorul Oficial nr. 51-54 din 14-03-2008.
11. Legea Nr. 91 din 29.05.2014 cu privire la semnătura electronică și documentul electronic, Monitorul Oficial nr. 174-177 din 04.07.2014.
12. Legea nr. 142 din 19.07.2018 cu privire la schimbul de date și interoperabilitate, Monitorul Oficial nr. 295-308 din 10.08.2018.
13. Hotărârea Guvernului nr. 546 din 20.07.2011 privind aprobarea Regulamentului cu privire la acordarea serviciilor Sistemului de telecomunicații al autorităților administrației publice și operarea modificărilor în unele hotărâri ale Guvernului, Monitorul Oficial nr. 118-121 din 22.07.2011.
14. Hotărârea Guvernului nr. 7104 din 20.09.2011 cu privire la aprobarea Programului strategic de modernizare tehnologică a guvernării (e-Transformare), Monitorul Oficial nr. 156-159 din 23.09.2011
15. Hotărârea Guvernului nr. 656 din 05.09.2012 cu privire la aprobarea Programului privind Cadrul de Interoperabilitate, Monitorul Oficial nr. 186-189 din 07.09.2012.
16. Hotărârea Guvernului nr. 857 din 31.10.2013 cu privire la Strategia națională de dezvoltare a societății informaționale „Moldova Digitală 2020”, Monitorul Oficial nr. 252-257 din 08.11.2013.
17. Hotărârea Guvernului nr. 1090 din 31.12.2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass), Monitorul Oficial nr. 4-8 din 10.01.2014.
18. Hotărârea Guvernului nr.128 din 20.02.2014 privind platforma tehnologică guvernamentală comună (MCloud), Monitorul Oficial nr. 47-48 din 25.02.2014.
19. Hotărârea Guvernului nr. 405 din 02.06.2014 privind serviciul electronic guvernamental integrat de semnătură digitală (MSign), Monitorul Oficial nr. 147-151 din 06.06.2014.
20. Hotărârea Guvernului nr. 700 din 25.08.2014 cu privire la datele guvernamentale deschise, Monitorul Oficial nr. 256-260, 29.08.2014.
21. Hotărârea Guvernului nr. 701 din 25.08.2014 cu privire la aprobarea Metodologiei publicării datelor guvernamentale deschise, Monitorul Oficial nr. 256-260 din 29.08.2014.
22. Hotărârea Guvernului nr. 708 din 28.08.2014 privind serviciul electronic guvernamental de jurnalizare (MLog), Monitorul Oficial nr. 261-267 05.09.2014.
23. Hotărârea Guvernului nr. 211 din 03.04.2019 privind platforma de interoperabilitate (MConnect), Monitorul Oficial nr. 132-138 din 12.04.2019
24. Hotărârea Guvernului nr. 375 din 10.06.2020 pentru aprobarea Conceptului Sistemului informațional automatizat „Registrul împuternicirilor de reprezentare în baza semnăturii electronice” (MPower) și a Regulamentului privind modul de ținere a Registrului împuternicirilor de reprezentare în baza semnăturii electronice, Monitorul Oficial nr. 153-158 din 26.06.2020.

25. Hotărârea Guvernului nr. 376 din 10.06.2020 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), Monitorul Oficial nr. 149-151 din 19.06.2020.

III. Standarde și bune practici în domeniul TIC:

26. Reglementarea tehnică RT 38370656-002:2006 „Procesele ciclului de viață al software-ului”, aprobată prin ordinul Ministerului Tehnologiei Informației și Comunicațiilor nr.78/2006.
27. Standardul Republicii Moldova SMV ISO CEI 15288: 2009, „Ingineria sistemelor și software-ului. Procesele ciclului de viață al sistemului”.
28. SM ISO/CEI 12207 „Ingineria sistemelor și software-ului. Procesele ciclului de viață al software-ului”.
29. SM ISO/CEI 27002 „Tehnologia informației. Tehnici de securitate. Cod de bună practică pentru managementul securității informației”.
30. SM ISO/CEI 15408-1 „Tehnologia informației. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informației. Partea 1: Introducere și model general”.
31. SM ISO/CEI 15408-2 „Tehnologia informației. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informației. Partea 2: Cerințe funcționale de securitate”.
32. SM ISO/CEI 15408-3 „Tehnologia informației. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informației. Partea 3: Cerințe de asigurare a securității”.
33. Michael O. Leavitt, Ben Shneiderman, Research-Based Web Design & Usability Guidelines, https://www.usability.gov/sites/default/files/documents/guidelines_book.pdf
34. Recomandările World Wide Web Consortium (W3C) (http://www.w3c.org) privind calitatea conținutului paginilor Web, posibilitățile vizualizării corecte a informației, folosind exploratoare Internet larg utilizate, și compatibilitatea cu diferite platforme informatice.
35. Recomandările WAI (Web Accessibility Initiative) (http://www.w3c.org/WAI) privind asigurarea posibilității utilizării resurselor site-urilor de către persoanele cu dizabilități.
36. Recomandările WCAG (Web Content Accessibility Guidelines) http://www.w3.org/TR/WCAG21/
37. Recomandările W3C (http://validator.w3.org) privind testarea paginilor WEB. Toate paginile WEB generate de SIA RSISC se vor testa în conformitate cu aceste recomandări.

1.3. Principiile de elaborare ale sistemului informatic

Întru asigurarea obiectivelor înaintate sistemului informatic SIA RSISC, la proiectarea, realizarea și implementarea acestuia trebuie să se țină cont de următoarele principii generale:

- **Principiul legalității**: care presupune crearea și exploatarea sistemului informatic, în conformitate cu legislația națională în vigoare, a normelor și standardelor internaționale recunoscute în domeniu;
- **Principiul responsabilității și conștientizării** care 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 divizării arhitecturii pe nivele** care constă în proiectarea și implementarea componentelor funcționale ale SIA RSISC în conformitate cu standardele de interfață dintre nivele;
- **Principiul arhitecturii bazate pe servicii (SOA)** care constă în distribuirea componentelor funcționale ale sistemului informatic în componente mai mici, distincte - numite servicii - care pot fi distribuite într-o rețea și pot fi utilizate împreună pentru a crea aplicații destinate implementării funcțiilor de business ale sistemului informatic. Aceste componente vor putea fi implementate fără dependențe reciproce rigide și vor interacționa prin interfețe externe implementate în bază de standarde deschise și independente de tehnologie. Acest fapt conferă flexibilitatea alegerii tehnologiilor și cicluri de viață independente pentru componentele SIA RSISC De asemenea, va permite părților interesate să selecteze opțiuni tehnologice alternative pentru capabilitățile de introducere și accesare date.
- **Principiul reutilizării capabilităților existente** care presupune că SIA RSISC va fi implementat prin reutilizarea la nivelul componentelor sale a capabilităților TIC curente la care are acces STISC. Dezvoltarea de noi capabilități specifice SIA RSISC se va face doar în cazul lipsei acestora în arhitectura TIC curentă a STISC (cu păstrarea arhitecturii SOA și asigurarea posibilității reutilizării acestor capabilități de alte sisteme informatice, unde e posibil). Acest fapt presupune utilizarea serviciilor de platformă guvernamentală, sau a soluțiilor de platformă implementate în cadrul STISC, pentru dezvoltarea componentelor ce formează SIA RSISC.
- **Principiul alinierii la arhitectura TIC de scară largă a STISC** care presupune că locul SIA RSISC în arhitectura TIC de scară largă este explicit delimitat în raport cu alte sisteme informatice ale STISC. SIA RSISC trebuie implementat cu aplicarea principiilor de arhitectură TIC stabilite de STISC și trebuie să fie capabil să interacționeze cu alte componente ale arhitecturii TIC. Principiile de arhitectură TIC sunt la rândul lor aliniate la principiile de arhitectură guvernamentală.
- **Principiului modelului de date deschis și interoperabil** care presupune că modelul de date susținut de SIA RSISC este documentat și comunicat către toți actorii interesați. SIA RSISC urmează a fi dezvoltat în baza standardelor acceptate în domeniu și aliniat la modelul de date guvernamental și departamental (adoptarea taxonomiei și semanticii deja existente la nivel național și departamental și îmbogățirea acesteia pentru a satisface necesitățile specifice domeniului asigurării securității informației).
- **Principiul securității prin design** care presupune proiectarea SIA RSISC în cunoștință de cauză cu privire la riscurile de securitate a informației ce pot afecta buna funcționare a sistemului informatic. Cerințele legale aplicabile pentru protecția datelor personale trebuie considerate la etapa de proiectare a SIA RSISC și implementate la etapa de dezvoltare. SIA RSISC va asigura accesarea controlată, transparentă și responsabilă a datelor.
- **Principiul integrității, plenitudinii și veridicității datelor** care presupune implementarea mecanismelor care permit păstrarea conținutului și interpretării univoce a datelor în condițiile unor influențe accidentale și eliminării fenomenelor de denaturare sau lichidare accidentală a acestora, furnizarea unui volum de date suficient executării funcțiilor de business al sistemului informatic și asigurarea unui grad înalt de corespundere a datelor cu starea reală a obiectelor pe care le reprezintă și care fac parte din SIA RSISC.
- **Principiul accesibilității informației cu caracter public** care presupune implementarea procedurilor de asigurare a accesului solicitanților la informația cu caracter public furnizată de soluția informatică.

- **Principiul expansibilității** care stipulează posibilitatea extinderii și completării sistemului informatic cu noi funcții sau îmbunătățirea celor existente;
- **Principiul de prioritate a primei persoane/a centrului unic** care presupune existența unei persoane responsabile de rang înalt, cu drepturi suficiente pentru luarea deciziilor și coordonarea activităților în vederea creării și exploatării sistemului informatic;
- **Principiul scalabilității** care presupune asigurarea unei performanțe constante a soluției informatice la creșterea volumului de date și a solicitării sistemului informatic;
- **Principiul simplității și comodității utilizării** care presupune proiectarea și realizarea tuturor aplicațiilor, mijloacelor tehnice și de program accesibile utilizatorilor SIA RSISC, bazate pe principii exclusiv vizuale, ergonomice și logice de concepție.

1.4. Destinația, obiectivele și sarcinile sistemului informatic

SIA RSISC este o componentă a Resurselor informaționale de stat ale Republicii Moldova reprezentând sursa oficială de date cu privire la incidentele de securitate cibernetică raportate la nivel guvernamental.

În acest sens 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”.

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.

Implementarea SIA RSISC va contribui 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.

SIA RSISC reprezintă un sistem informatic oficial de identificare și gestionare a incidentelor cibernetice la nivel guvernamental al Republicii 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.

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.

În acest sens următoarele obiective sunt urmărite a fi a tinse odată cu implementarea SIA RSISC:

- asigurarea formării resurselor informaționale de stat aferent incidentelor de securitate cibernetică;
- dezvoltarea unei soluții tehnice flexibile și modulare care ar permite îmbunătățirea activității STISC, în rolul său de CERT Gov ;
- formarea bazei de date a incidentelor de securitate cibernetică la nivel guvernamental;

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

Întru implementarea obiectivelor propuse, SIA RSISC trebuie să realizeze următoarele sarcini în procesul de exploatare:

- identificarea, înregistrarea, clasificarea și analiza incidentele de securitate cibernetică și coordonarea, cooperarea și sesizarea organelor de drept, după caz;
- asigurarea cadrului organizatoric și suportul tehnic necesar schimbului de informații dintre diverse echipe de tip CERT, utilizatori, entități publice;
- crearea și menținerea unei baze de date a incidentelor de securitate cibernetică și a măsurilor întreprinse pentru înlăturarea și/sau contracararea acestora;
- conectarea și realizarea schimbului de date între CERT-uri departamentale și CERT Gov prin intermediul unei platforme dedicate;
- promovarea bunelor practici între specialiștii CERT Gov și persoanele responsabile de răspuns la incidente de securitate cibernetică din cadrul entităților publice;
- întocmirea datelor statistice și elaborarea rapoartelor cu privire la incidente de securitate cibernetică înregistrate, precum și dinamica acestor incidente;
- asigurarea implementării politicilor de prevenire și contracarare a incidentelor cibernetice potrivit competenței;
- oferirea unei platforme informaționale de comunicare strategică.

2. Arhitectura sistemului informatic

SIA RSISC trebuie să furnizeze o interfață WEB, accesibilă prin intermediul unui explorator Internet de largă utilizare (MS Internet Exlorer/MS Edge, Mozila FireFox, Opera, Google Chrome sau Safari). Din punct de vedere funcțional se va dezvolta o soluție fiabilă și scalabilă atât în cazul creșterii numărului de utilizatori concurenți sau, cât și în cazul creșterii volumului de informație gestionată de acesta.

La baza SIA RSISC va sta o arhitectură orientată la servicii de minim 3 nivele (care exclude interacțiunea directă a aplicației cu baza de date) bazată pe tehnologiile WEB adecvate timpului. Întru asigurarea unui nivel adecvat al securității informaționale, sistemul informatic livrat trebuie să permită realizarea de conexiuni securizate între stațiile client și serverul de aplicație pentru asigurarea siguranței informației expediate (utilizându-se conexiuni VPN și sesiunilor TLS/SSL).

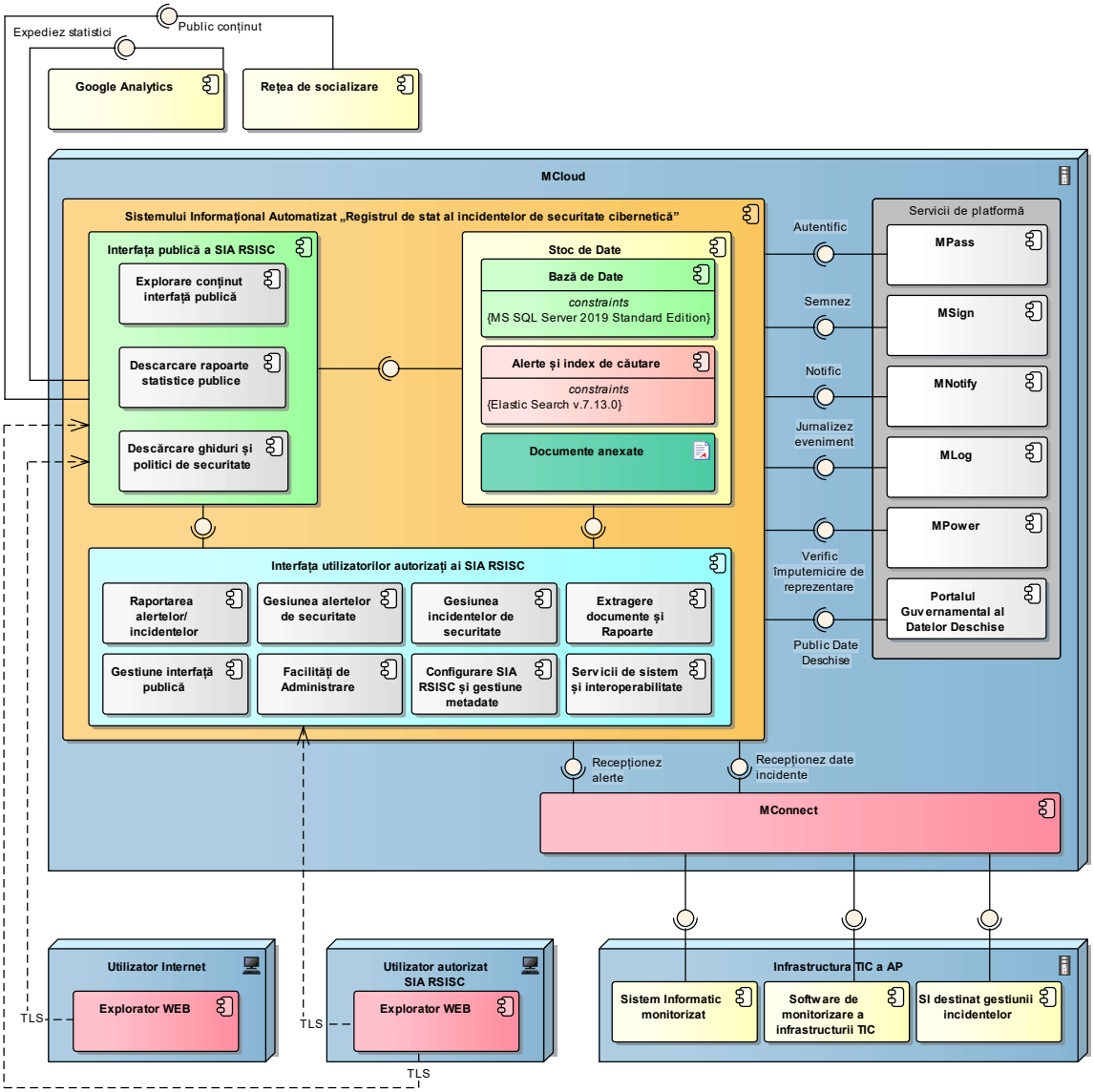

Figura 2.1. Arhitectura SIA RSISC.

SIA RSISC va fi desfășurat și va funcționa în cadrul platformei guvernamentale MCloud. Întru asigurarea obiectivelor înaintate soluției informatice, la proiectarea, dezvoltarea și implementarea SIA RSISC trebuie să se țină cont de arhitectura descrisă în figura 2.1.

După cum se vede în figura 2.1, soluția de cooperare a resurselor pentru asigurarea funcționalității SIA RSISC constă din 5 categorii de noduri distincte:

- **MCloud** – infrastructura TIC a platformei tehnologice guvernamentale comune care formează cloud-ul guvernamental (MCloud) unde sunt găzduite, de regulă, toate sistemele informatice ale AP din Republica Moldova și unde urmează a fi găzduit SIA RSISC. Trebuie de menționat faptul că SIA RSISC va consuma serviciile de platformă MCloud. Toate conexiunile cu sistemele informatice externe se va realiza preponderent prin intermediul platformei de interoperabilitate guvernamentale MConnect.
- **Infrastructura Tic a autorităților publice ale Republicii Moldova** – infrastructura TIC a autorităților publice ale Republicii Moldova (configurată în cadrul platformei guvernamentale comune MCloud sau în cadrul centrelor de date deținute de autoritățile publice) care găzduiesc sistemele informatice monitorizate din punct de vedere al asigurării securității informației, soluției software de monitorizare a funcționării infrastructurii TIC a autorității publice și sistemelor informatice utilizate de autoritățile publice ale Republicii Moldova în scopul documentării proceselor de gestiune a incidentelor de securitate.
- **Infrastructura Google Analytics** – infrastructura TIC a serviciului Google destinat colectării datelor comportamentului Internauților și generării rapoartelor statistice aferente utilizării interfețe publice a SIA RSISC.
- **Infrastructura rețelelor de socializare** – infrastructura TIC a serviciilor expuse de rețelele de socializare (LinkedIn, Facebook, Twitter) în scopul publicării conținutului interfeței publice a SIA RSISC.
- **Calculatoarele client** – calculatoarele, de la care se va accesa de către utilizatorii autorizați și anonimi (în funcție de drepturi și roluri) funcționalitățile SIA RSISC.

Conform diagramei de desfășurare și componente din figura 2.1, SIA RSISC constă din 3 componente de bază:

- **Interfața publică** – componentă funcțională accesibilă utilizatorilor anonimi care furnizează acces la informația cu caracter public (*exemplu: rapoarte statistice, indicatori de performanță, ghiduri, recomandări etc.*).
- **Interfața utilizatorilor autorizați** – componentă importantă a SIA RSISC destinată activității actorilor implicați în procesul de raportare a alertelor și/sau incidentelor de securitate cibernetică și actorii implicați în procesele de gestiune a incidentelor de securitate și supervizare/monitorizare a acestora.
- **Stocul de date** – componenta SIA RSISC care răspunde de stocarea datelor aferente SIA RSISC. Trebuie de menționat că datele SIA RSISC urmează a fi stocate în cadrul a 2 baze de date: baza de date principală implementată în baza Microsoft SQL Server 2019 Standard Edition care va conține datele interfeței publice SIA RSISC și datele aferente cazurilor de gestiune a incidentelor de securitate cibernetică și baza de date implementată în baza Elastic Search, care va conține datele aferente alertelor de securitate cibernetică și indexul de căutare a SIA RSISC.

Pentru implementarea unui șir de funcționalități, SIA RSISC va consuma un șir de servicii de platformă și API-uri furnizate de sisteme informatice guvernamentale și externe după cum urmează:

1. **Autentific** furnizat de serviciul de platformă MPass în scopul autentificării utilizatorilor prin intermediul semnăturii electronice sau mobile.
2. **Semnez** furnizat de serviciul de platformă MSign în scopul aplicării semnăturii electronice sau mobile pe documentele și formularele perfectate în cadrul proceselor de business ale SIA RSISC.
3. **Notific** furnizat de serviciul de platformă MNotify în scopul implementării unui mecanism universal și centralizat de notificare a utilizatorilor SIA RSISC.
4. **Jurnalizez eveniment** furnizat de serviciul de platformă MLog în scopul jurnalizării evenimentelor de business sensibile produse în urma exploatării SIA RSISC.
5. **Verific împuternicire de reprezentare** furnizat de serviciul de platformă MPower în scopul verificării împuternicirilor de reprezentare a utilizatorilor autorizați și autorizare a accesului în baza acestor împuterniciri.
6. **Public date deschise** care interacționează cu Portalul Datelor Guvernamentale Deschise (https://date.gov.md) în scopul publicării seturilor de date publice produse în cadrul proceselor de business ale SIA RSISC.
7. **Expediez statistici** furnizat de Google Analytics în scopul furnizării datelor de comportament a Internauților în cadrul interfeței publice a SIA RSISC.
8. **Public conținut** furnizate de rețelele de socializate (exemplu: LinkedIn, Facebook, Twitter) în scopul partajării documentelor publicate prin intermediul interfeței publice a SIA RSISC.

SIA RSISC va expune un șir de interfețe prin intermediul platformei de interoperabilitate MConnect destinate interacțiunii cu sisteme informatice externe după cum urmează:

1. **Recepționez alerte de securitate cibernetică** prin intermediul căreia vor fi recepționate automat alertele de securitate cibernetică expediate de sistemele informatice monitorizate sau software-ul de monitorizare a infrastructurii TIC a autorităților publice ale Republicii Moldova.
2. **Recepționez date incidente de securitate cibernetică** prin intermediul căreia vor fi recepționate automat datele aferente cazurilor de gestiune a incidentelor de securitate cibernetică documentate de autoritățile publice ale Republicii Moldova prin intermediul soluțiilor software dedicate.

3. Părțile implicate și roluri ale sistemului informatic

3.1. Roluri de business ale sistemului informatic

În conformitate cu legislația în vigoare, următoarele entități ale Republicii Moldova sunt interesate sau trebuie implicate în procesele de elaborare și asigurare a bunei funcționări a SIA RSISC:

- **Serviciul Tehnologia Informației și Securitate Cibernetică** – în calitate de Centru Guvernamental de reacție la incidente de securitate cibernetică, entitate responsabilă de implementarea și asigurarea bunei funcționări a SIA RSISC, precum și acordarea suportului entităților publice din Republica Moldova în utilizarea soluțiilor TIC și implementarea măsurilor proactive și reactive, în vederea reducerii riscurilor de incidente cibernetice și acordarea asistenței în reacția la incidente de securitate cibernetică.
- **Autoritățile Publice ale Republicii Moldova** în calitate de posesoare a soluțiilor TIC pentru care trebuie furnizate servicii de asigurare a securității infrastructurii TIC deținute sau soluțiilor software exploatate.
- **Agenția de Guvernare Electronică** – în calitate de organism abilitat cu elaborarea și implementarea politicii de e-Transformare în Republica Moldova, platformei tehnologice guvernamentale unice MCloud și posesoare a serviciilor de platformă cu care trebuie să se integreze Pagina WEB oficială tip.
- **Utilizatori Internet** în calitate de beneficiari direcți ai interfeței publice a SIA RSISC în vederea accesării datelor, documentelor și statisticilor de interes public produse în cadrul proceselor de business ale SIA RSISC.

3.2. Achizitorul sistemului informatic

SIA RSISC va fi achiziționat de către Serviciul Tehnologia Informației și Securitate Cibernetică. În calitate de achizitor, Serviciul Tehnologia Informației și Securitate Cibernetică va superviza totalitatea activităților de proiectare, implementare a Paginii WEB oficiale tip.

3.3. Posesorul sistemului informatic

Posesorul SIA RSISC este Serviciul Tehnologia Informației și Securitate Cibernetică, în calitate de Centru guvernamental de reacție la incidente de securitate cibernetică, care conform HG. Nr. 482/2020 are drept de gestionare și de utilizare a datelor și a resurselor și exercită atribuțiile deținătorului și administratorului tehnic al sistemului informatic de gestiune a incidentelor de securitate cibernetică.

3.4. Deținătorul sistemului informatic

Deținătorul SIA RSISC este Serviciul Tehnologia Informației și Securitate Cibernetică ca urmare a faptului că SIA RSISC urmează a fi găzduit în cadrul platformei guvernamentale comune MCloud. În calitate de deținător al SIA RSISC Serviciul Tehnologia Informației și Securitate Cibernetică va soluționa totalitatea problemelor tehnice depistate pe parcursul exploatării SIA RSISC.

3.5. Registratorul sistemului informatic

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

3.6. Administratorul sistemului informatic

Administratorul de sistem al SIA RSISC este una sau mai multe persoane desemnate de Serviciul Tehnologie a Informației și Securitate Cibernetică. Administrarea conținutului interfeței publice a SIA RSISC va fi efectuată de specialiștii din cadrul STISC. La nivelul infrastructurii MCloud a SIA RSISC funcțiile de administrare vor fi exercitate de STISC (administrator de infrastructură tehnică).

Administratorul de Sistem are acces deplin la toate funcționalitățile SIA RSISC, fișiere și baze de date aferente SIA RSISC, aplicațiile software care asigură securitatea datelor SIA RSISC. Responsabilitățile Administratorului de Sistem al SIA RSISC sunt următoarele:

- asigurarea funcționării normale a sistemului informatic garantând accesibilitatea, securitatea și integritatea datelor;
- monitorizarea activitatea utilizatorilor în sistem;
- diagnosticarea și soluționarea problemelor tehnice;
- configurarea sistemului informatic;
- gestiunea metadatelor;
- administrarea infrastructurii tehnice a SIA RSISC.

3.7. Utilizatorii și rolul acestora în cadrul sistemului informatic

Rolurile umane și sistemele informatice ce interacționează cu SIA RSISC sunt prezentate în figura 3.1. După cum se vede în această figură, în cadrul aplicației vor interacționa 8 categorii de actori umani și 4 categorii de sisteme informatice.

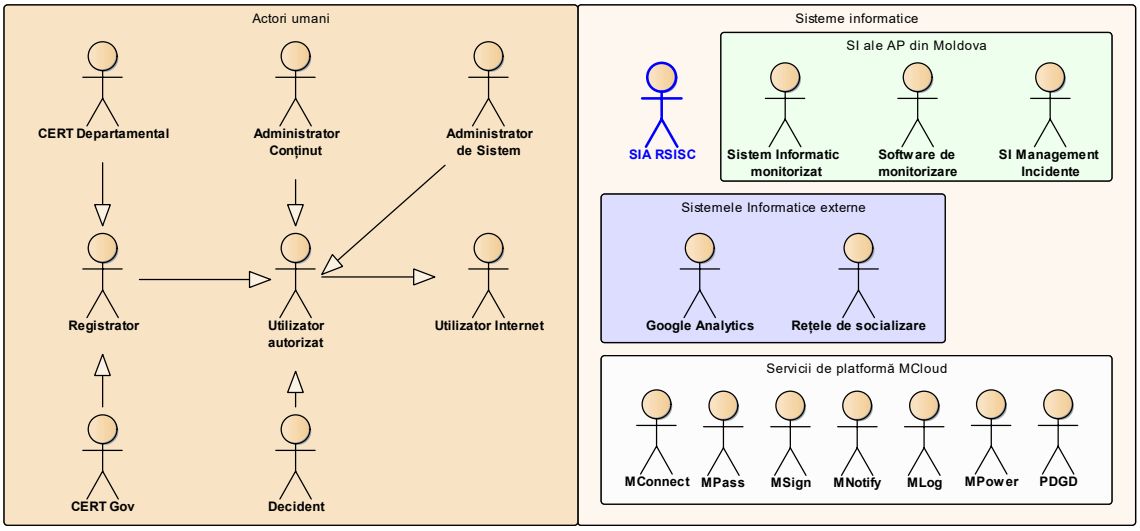

Figura 3.1. Actorii SIA RSISC.

Utilizator Internet - actor uman care accesează din extern interfața publică a SIA RSISC în scopul accesării datelor, documentelor și rapoartelor cu caracter public produse în cadrul proceselor de business ale SIA RSISC. Categoria dată de actori are acces la următoarele funcționalități:

- explorarea conținutului interfeței publice a SIA RSISC;

- descărcarea rapoartelor cu caracter public;
- explorarea knowledge base în domeniul securității informației;
- contactarea STISC.

Utilizator autorizat – rol generic care furnizează funcționalitățile comune tuturor categoriilor de utilizatori autorizați, indiferent de rolul deținut în cadrul SIA RSISC (CERT Departamental, CERT Gov, Decident, Administrator de conținut sau Administrator de Sistem). Actorii în cauză vor dispune de acces la următoarele funcționalități:

- acces la toate funcționalitățile disponibile Utilizatorilor Internet;
- utilizarea Dashboard-ului pentru accesarea notificărilor și accesarea rapidă a formularelor electronice specifice evenimentelor de business aferente atribuțiilor de serviciu;
- raportarea alertelor de securitate cibernetică;
- raportare incidentelor de securitate cibernetică;
- generarea documentelor și rapoartelor statistice;
- recepționarea notificărilor.

Administrator de Conținut – actor uman responsabil de administrarea conținutului interfeței publice a SIA RSISC (adăugare/modificarea/suprimarea conținutului, configurarea aspectului interfeței publice etc.). Actorii în cauză vor dispune de acces la următoarele funcționalități:

- acces la toate funcționalitățile disponibile Utilizatorilor Internet;
- acces la toate funcționalitățile disponibile Utilizatorilor autorizați;
- configurarea aspectului de prezentare a interfeței publice a SIA RSISC;
- gestiunea conținutului interfeței publice a SIA RSISC.

Registrator – rol generic specific utilizatorilor care operează, introduce și/sau modifică datele din cadrul SIA RSISC, dar nu configurează însuși funcționalitățile SIA RSISC. Actorii în cauză vor dispune de acces la următoarele funcționalități:

- acces la toate funcționalitățile disponibile Utilizatorilor Internet;
- acces la toate funcționalitățile disponibile Utilizatorilor autorizați;
- gestiunea alertelor de securitate cibernetică;
- gestiunea incidentelor de securitate cibernetică.

CERT Departamental – rol specific Registratorilor care gestionează alertele și incidentele de securitate la nivelul instituției unde sunt atestate acestea. Actorii în cauză vor dispune de acces la următoarele funcționalități:

- acces la toate funcționalitățile disponibile Utilizatorilor Internet;
- acces la toate funcționalitățile disponibile Utilizatorilor autorizați;
- acces la toate funcționalitățile disponibile Registratorilor.

CERT Gov– rol specific Registratorilor care gestionează alertele și incidentele de securitate la nivelul Centrului pentru Securitatea Cibernetică (în cazul în care alertele și incidentele de securitate nu pot fi

gestionate de către CERT Departamental). Actorii în cauză vor dispune de acces la următoarele funcționalități:

- acces la toate funcționalitățile disponibile Utilizatorilor Internet;
- acces la toate funcționalitățile disponibile Utilizatorilor autorizați;
- acces la toate funcționalitățile disponibile Registratorilor.

Decident- actor uman, care reprezintă totalitatea utilizatorilor autorizați cu rol de decizie în activitatea Centrului pentru Securitatea Cibernetică. Actorii în cauză dispun de acces la următoarele funcționalități:

- acces la toate funcționalitățile disponibile Utilizatorilor Internet;
- acces la toate funcționalitățile disponibile Utilizatorilor autorizați;
- aprobă/respinge proiectele de documente aferente proceselor de gestiune a alertelor și incidentelor de securitate cibernetică.

Administrator de Sistem - actor uman, abilitat cu administrarea utilizatorilor sistemului, configurarea sistemului informatic precum și cu startarea/stoparea/restartarea componentelor sistemului informatic. Dacă mediul tehnologic include capabilități suficiente pentru îndeplinirea lucrărilor de administrare apoi implementarea acestora în sistem este opțională. Categoria dată de actori are acces la următoarele funcționalități:

- acces la funcționalitățile accesibile tuturor categoriilor de utilizatori ale SIA RSISC;
- administrarea profilurilor utilizatorilor autorizați, rolurilor și drepturilor de acces a acestora;
- gestiunea sistemului de clasificatoare, nomenclatoare și metadate;
- configurarea parametrilor de funcționare a SIA RSISC;
- configurarea fluxurilor, formularelor și șabloanelor de rapoarte;
- monitorizarea operațională, diagnosticul și soluționarea problemelor de funcționare a SIA RSISC;
- administrarea serverului de aplicații;
- administrarea bazei de date tehnologice și în producție;
- generarea rapoartelor aferente auditului sistemului informatic și conținutului informațional a Bazei de Date a sistemului informatic;
- efectuarea copiilor de rezervă și restabilire a funcționalităților SIA RSISC în caz de dezastru.

Sistemele informatice ale autorităților publice ale Republicii Moldova:

- **Sisteme informatice monitorizate** – sistemele informatice ale autorităților publice din Republica Moldova care vor expedia în mod automat alerte de securitate către SIA RSISC în cazul producerii unor evenimente de business specifice pasibile a genera incidente de securitate.
- **Software de monitorizare** – soluții software care monitorizează starea curentă a infrastructurii TIC care vor expedia în mod automat alerte de securitate cibernetică către SIA RSISC în cazul producerii unor evenimente pasibile de a genera incidente de securitate cibernetică;

- **Sisteme informatice de management a incidentelor de securitate cibernetică** – soluții software specializate exploatate de entitățile publice din Republica Moldova, prin intermediul cărora sunt administrate și documentate procesele de gestiune a incidentelor de securitate cibernetică . Aceste sisteme informatice vor expedia către SIA RSISC datele aferente alertelor și/sau incidentelor de securitate cibernetică documentate.

Sisteme informatice externe:

- **Google Analytics** - sistem informatic extern utilizat pentru colectarea statisticilor și generarea rapoartelor și KPI de utilizare a interfeței publice a SIA RSISC;
- **Rețele de socializare** - integrarea cu care va permite publicarea în cadrul rețelelor de socializare a documentelor de conținut a interfeței publice a SIA RSISC.

Serviciile guvernamentale MCloud:

- **MConnect** - platforma guvernamentală de interoperabilitate și schimb de date. SIA RSISC va utiliza platforma dată pentru schimbul de date cu sisteme informatice ale altor autorități publice.
- **MPass** – serviciul de platformă utilizat pentru controlul accesului la sistemele informatice și asigurarea procedurilor de autentificare prin intermediul semnăturii electronice sau mobile.
- **MSign** – serviciul de platformă utilizat la aplicarea și validarea semnăturii electronice, inclusiv semnăturii mobile.
- **MNotify** – serviciul de platformă utilizat pentru notificarea utilizatorilor autorizați ai SIA RSISC;
- **MLog** - serviciul de platformă utilizat pentru jurnalizarea tuturor evenimentelor de business critice aferente sistemelor informatice ale AP din Republica Moldova.
- **MPower** - Registrul Împuternicirilor de Reprezentare care furnizează date privind împuternicirea deținută de utilizatorii autorizați de a efectua acțiuni specifice în cadrul SIA RSISC.
- **PDGD** (*Portalul Datelor Guvernamentale Deschise* https://date.gov.md) - portalul datelor guvernamentale deschise prin intermediul căruia SIA RSISC va publica indicatori de performanță, statistici și rapoarte cu caracter public produse în cadrul proceselor sale de business implementate.

4. Modelul funcțional al sistemului informatic

4.1. Modelul de date al sistemului informatic

Analizând domeniul modelat pot fi delimitate totalitatea obiectelor informaționale de care trebuie să se țină cont la elaborarea SIA RSISC. În figura 4.1 sunt expuse obiectele informaționale cheie care vor sta la baza proiectării și dezvoltării SIA RSISC (direct utilizate în implementarea proceselor de business aferente gestiunii incidentelor de securitate cibernetică). Astfel, elementul central al arhitecturii de date al SIA RSISC îl constituie fișa incidentului de securitate cibernetică.

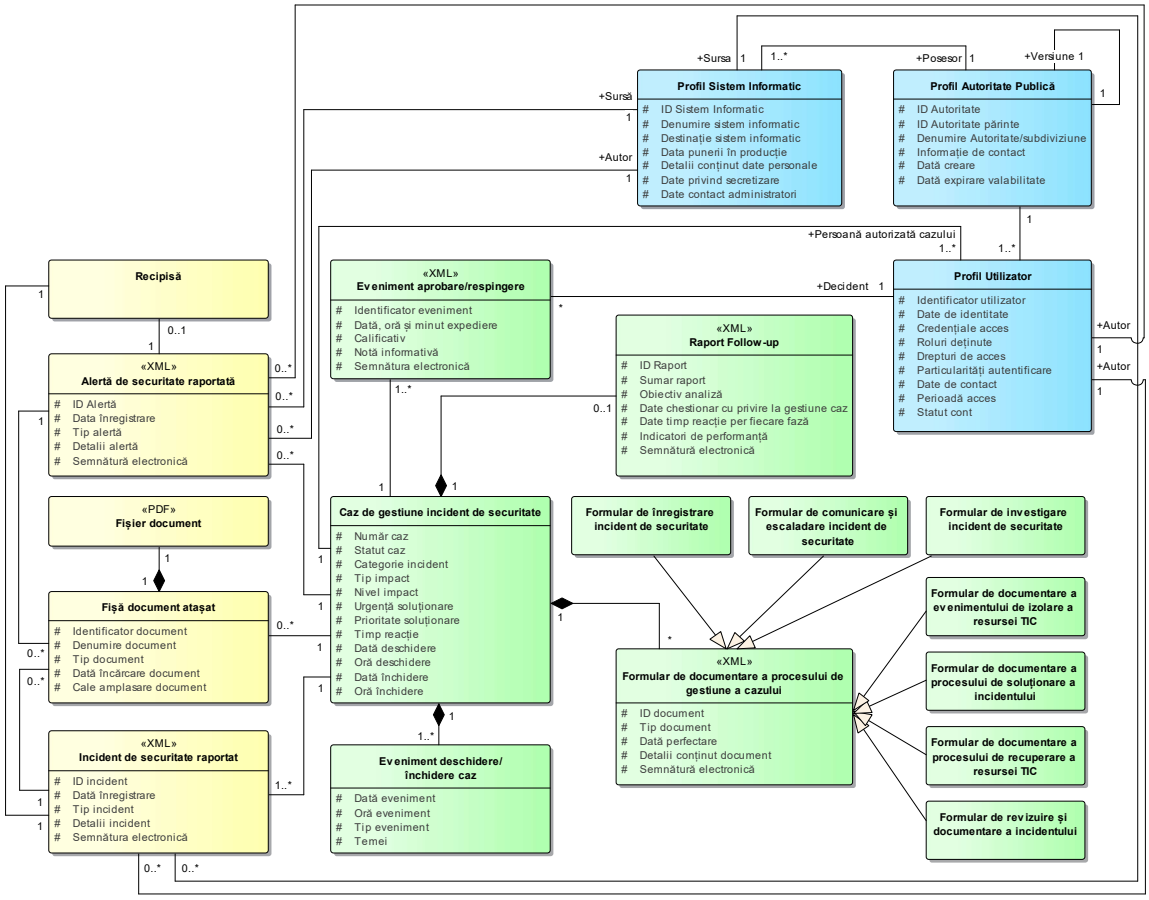

Figura 4.1. Modelul de date al SIA RSISC.

Întru asigurarea funcționalității în bune condiții a SIA RSISC este necesară implementarea funcționalităților necesare gestiunii următoarelor grupuri de obiecte informaționale:

- caz de gestiune a incidentului de securitate cibernetică;
- alertă de securitate cibernetică raportată;
- incident de securitate cibernetică raportat;
- fișier atașat;
- recipisă;

- profil.

1. Caz de gestiune a incidentului de securitate

Este obiectul informațional complex cheie care conține toate datele necesare proceselor de documentare și gestiune a incidentelor de securitate cibernetică. Un caz de gestiune a incidentului de securitate este definit prin intermediul următoarelor obiecte informaționale:

A. ***Fișa incidentului de securitate***. Este un element de grupare a datelor, nu modalitate de perfectare a evenimentelor de business aferente documentării și gestiunii incidentului de securitate cibernetică, care sunt perfectate prin intermediul unor formulare specializate care urmează a fi atașate dosarului cazului de gestiune a incidentului de securitate cibernetică. Un dosar al cazului de gestiune a incidentului de securitate gestionează și grupează următoarele categorii de date:

   a) Număr caz (identificatorul fișei);
   b) Statut curent al incidentului de securitate cibernetică înregistrat;
   c) Categorie incident de securitate cibernetică;
   d) Tipul impactului generat de incidentul de securitate cibernetică;
   e) Nivelul impactului;
   f) Urgența de soluționare a incidentului de securitate cibernetică;
   g) Timpul de reacție;
   h) Dată deschidere caz;
   i) Oră, minut deschidere caz;
   j) Dată închidere caz;
   k) Oră, minut închidere caz;
   l) Utilizatorii autorizați cazului;
   m) Sistemul informatic aferent cazului.

B. ***Eveniment Deschidere/Închidere caz de gestiune incident de securitate cibernetică***. Un caz de gestiune a incidentului de securitate cibernetică poate fi deschis/închis, în funcție de circumstanțele aferente cazului. Acest obiect informațional înregistrează evenimentul de deschidere și închidere a cazului gestionând următoarele categorii de date:

   a) Dată producere eveniment;
   b) Oră și minut producere eveniment;
   c) Tip eveniment (deschidere/închidere);
   d) Temei înregistrare eveniment.

C. ***Formular electronic de documentare a procesului de gestiune a cazului de gestiune a incidentului de securitate***. Reprezintă un obiect informațional prin intermediul căruia sunt stocate datele aferente formularelor electronice prin intermediul cărora sunt analizate incidentele de securitate cibernetică și documentate procesele de gestiune a acestora. Următoarele categorii de date caracterizează acest obiect informațional:

   a) Identificator document;

b) Caz aferent document;

c) Autor document;

d) Tip document;

e) Dată perfectare;

f) Detaliile de conținut a documentului;

g) Semnătură electronică a autorului (dacă e cazul).

În funcție de categoria documentelor perfectate în procesul de gestiune a incidentului de securitate cibernetică SIA RSISC trebuie să implementeze următoarele formulare electronice:

- *Formular de înregistrare incident de securitate cibernetică* – formularul prin intermediul căruia se documentează detaliat incidentul de securitate cibernetică. Formularul dat prevede completarea atât a câmpurilor descriptive, cât și alegerea valorilor clasificatoarelor relevante (exemplu: categorie incident, tip impact incident, nivelul impactului incidentului, urgența de soluționare a incidentului, prioritate de soluționare a incidentului, timpul de reacție la incident etc.).
- *Formular de comunicare și escaladare incident de securitate cibernetică* – formularul prin intermediul căruia este identificată echipa responsabilă de soluționarea incidentului și implementate mecanismele de comunicare între actorii relevanți cazului.
- *Formular de investigare incident de securitate cibernetică* – formularul prin intermediul căruia sunt colectate toate tipurile de date cu referire la categoria și clasificarea incidentului, corelarea informațiilor extrase precum și planificarea măsurilor de reacție pentru a limita impactul (severitatea) și implementa acțiunile necesare pentru tratarea incidentului de securitate cibernetică.
- *Formular de documentare a evenimentului de izolare a resursei TIC* – formular prin intermediul căruia sunt documentate acțiunile de izolare a resursei TIC întru limitarea impactului negativ al incidentului de securitate cibernetică.
- *Formular de documentare a procesului de soluționare a incidentului* – formular electronic prin intermediul căruia este documentat procesul de tratare a incidentului de securitate cibernetică (acțiunile efectuate, procedurile utilizate, rezultatele obținute).
- *Formular de documentare a procesului de recuperare a resursei TIC* – formular electronic prin intermediul căruia este documentat procesul de recuperare a disponibilității resursei TIC afectate de incidentul de securitate cibernetică.
- *Formular de revizuire și documentare a incidentului* – formular electronic destinat evaluării eficacității procesului de management al incidentului de securitate cibernetică, documentare a sugestiilor de îmbunătățire precum și notificarea autorităților vizate.

D. ***Formularul Raportului follow-up***. Reprezintă un obiect informațional prin intermediul căruia sunt stocate datele aferente analizei follow-up al incidentului de securitate. Raportul post incident are scopul de a evidenția/dezvălui punctele lipsă în procedurile operaționale sau inexactitățile în procesul de gestiune a incidentelor, oferind o argumentare cu un set obiectiv de date în vederea implementării acțiunilor corective. Următoarele categorii de date caracterizează acest obiect informațional:

a) Identificator raport;

b) Identificator caz de gestiune incident de securitate cibernetică;

c) Descriere sumară raport;

d) Descrierea obiectivelor analizei;

e) Date aferente chestionarului cu privire la aprecierea cum a fost gestionat cazul;

f) Date privind timpul de reacție per fiecare fază de gestiune a incidentului;

g) Indicatorii de performanță aferenți procesului de gestiune a incidentului;

h) Semnătura electronică a autorului (dacă e cazul).

E. ***Eveniment de aprobare/respingere***. Reprezintă un obiect informațional prin intermediul căruia sunt înregistrate evenimentele de aprobare/respingere de către rolurile decidente a diferitor proiecte de formulare perfectate în cadrul proceselor de gestiune a incidentului de securitate cibernetică. Următoarele categorii de date caracterizează acest obiect informațional:

a) Identificator eveniment aprobare/respingere;

b) Identificator caz de gestiune a incidentului de securitate cibernetică;

c) Identificator decident;

d) Dată, oră, minut expediere;

e) Calificativ (aprobare/respingere);

f) Nota informativă;

g) Semnătura electronică (dacă e cazul).

2. Alertă de securitate raportată

Obiect informațional care descrie alertele de securitate cibernetică raportate de posesorii de sisteme informatice sau de sistemele informatice în mod automat. Acest obiect informațional este caracterizat de următoarele categorii de date:

- Identificator alertă de securitate cibernetică;
- Data înregistrării alertei;
- Tipul alertei;
- Detaliile descriptive a alertei;
- Identificatorul raportorului alertei;
- Identificatorul sistemului informatic aferent alertei;
- Identificatorul autorității publice aferente alertei;
- Identificatorul cazului de gestiune a incidentului de securitate cibernetică (dacă e cazul);
- Semnătura electronică a raportorului (dacă e cazul).

3. Incident de securitate cibernetică raportat

Obiect informațional care descrie incidentele de securitate cibernetică raportate de posesorii de sisteme informatice sau de sistemele informatice specializate în gestiunea incidentelor de securitate cibernetică. Acest obiect informațional este caracterizat de următoarele categorii de date:

- Identificator incident de securitate cibernetică;
- Data înregistrării incidentului;
- Tipul incidentului;
- Detaliile descriptive ale incidentului;
- Identificatorul raportorului incidentului;
- Identificatorul sistemului informatic aferent incidentului;
- Identificatorul autorității publice aferente incidentului;
- Identificatorul cazului de gestiune a incidentului de securitate cibernetică;
- Semnătura electronică a raportorului (dacă e cazul).

4. Fișier atașat

Obiect informațional care reprezintă fișierele atașate formularelor perfectate în cadrul proceselor de business ale SIA RSISC. Acest obiect informațional este caracterizat de următoarele categorii de date:

- Identificator fișier;
- Denumire document aferent fișierului;
- Tip document;
- Identificator formular/caz unde este atașat fișierul;
- Dată încărcare document;
- Cale amplasare fișier;
- Conținut fișier PDF atașat.

5. Recipisă

Obiect informațional care reprezintă recipisa expediată în mod automat de SIA RSISC în adresa utilizatorului autoriza pentru confirmarea recepționării alertei și/sau incidentului de securitate cibernetică raportat de acesta. Acest obiect informațional este caracterizat de următoarele categorii de date:

- Identificator recipisă;
- Data, ora, minut recepționare alertă/incident de securitate cibernetică;
- Identificator alertă/incident de securitate cibernetică;
- Identificator sistem informatic afectat;
- Identificator utilizator care a raportat alerta/incidentul de securitate cibernetică;
- Identificator autoritate publică posesoare a sistemului informatic;
- Conținut textual recipisă;
- Semnătură electronică (dacă e cazul).

6. Profil

Obiect informațional complex care definește totalitatea informației de profil necesară exploatării SIA RSISC. Profilurile sistemului informatic sunt definite de următoarele categorii de obiecte informaționale:

A. ***Profilul utilizatorului autorizat***. Reprezintă datele utilizatorilor autorizați ai sistemului informatic care vor fi implicați în procesele de business ale SIA RSISC sau vor necesita acces la detaliile dosarului cazului de gestiune a incidentului de securitate cibernetică (reprezintă persoane autorizate cazului). Pentru utilizatorului autorizat trebuie să poată fi gestionate următoarele date

   a) Identificatorul utilizatorului;
   b) Date de identitate (nume, prenume, IDNP etc.);
   c) Credențiale de acces;
   d) Roluri deținute;
   e) Drepturi specifice de acces;
   f) Particularități de autentificare;
   g) Date de contact;
   h) Perioadă de acces
   i) Statut cont.

B. ***Profil autoritate publică.*** Reprezintă profilurile autorităților publice implicate în procesele de business ale SIA RSISC sau posesoare de sisteme informatice care fac obiectul alertelor/incidentelor de securitate cibernetică. Pentru profilul autorității publice trebuie să poată fi gestionate următoarele date:

   a) Identificator autoritate publică/subdiviziune;
   b) Referință la autoritatea publică/subdiviziune ierarhic superioară (dacă există);
   c) Denumire autoritate publică/subdiviziune;
   d) Date de contact autoritate publică/subdiviziune;
   e) Dată creare înregistrare;
   f) Date expirare valabilitate înregistrare.

C. ***Profil sistem informatic.*** Reprezintă profilurile sistemelor informatice care fac obiectul alertelor/incidentelor de securitate cibernetică. Pentru profilul sistemului informatic trebuie să poată fi gestionate următoarele date:

   a) Identificator sistem informatic;
   b) Denumire sistem informatic;
   c) Destinație sistem informatic;
   d) Data punerii în producție sistem informatic;
   e) Date privind categoriile de date cu caracter personal procesate (dacă există);
   f) Date privind secretizarea sistemului informatic;
   g) Date de contact a administratorilor sistemului informatic.

4.2. *Funcționalitățile sistemului informatic*

Funcționalitățile furnizate de SIA RSISC sunt prezentate în diagrama din figura 4.2. După cum se vede în figura 4.2, SIA RSISC va furniza funcționalitățile sale actorilor relevanți prin intermediul a 20 cazuri de utilizare.

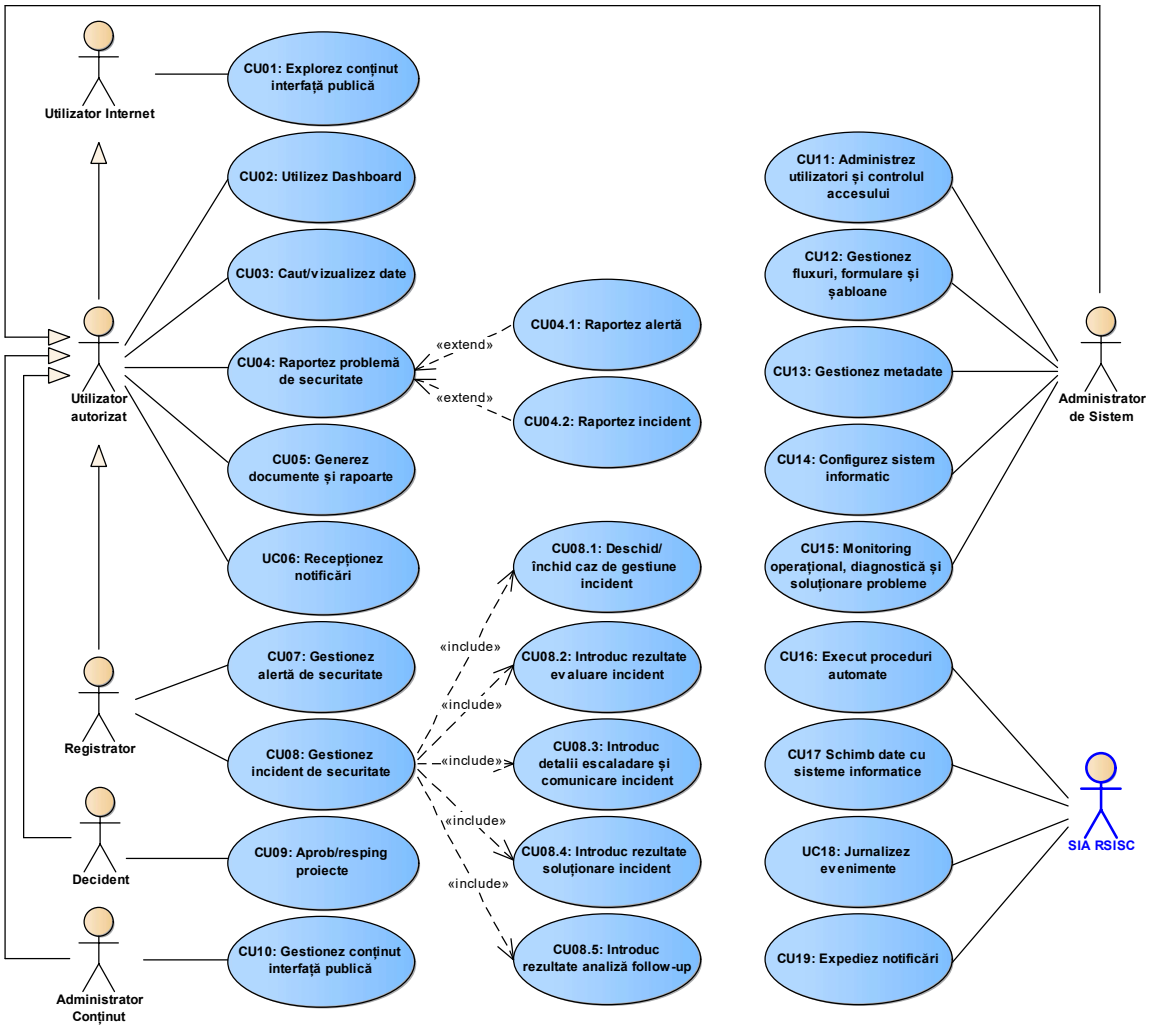

Figura 4.2. Funcționalitățile SIA RSISC.

CU01: Explorez conținut interfață unică

Caz de utilizare, prin intermediul căruia Interfața Publică a SIA RSISC furnizează utilizatorilor anonimi totalitatea funcționalităților de navigare în conținutul Interfeței Publice a SIA RSISC, contactare responsabili din cadrul Centrului pentru Securitatea Cibernetică precum și accesarea și descărcarea informației relevante necesităților Internauților cum ar fi:

- Noutăți/comunicate de presă;
- Răspunsul la întrebări frecvente (F.A.Q.);
- Ghiduri de securitate;

- Publicații aferente activității CERT-GOV, precum și domeniului securității cibernetice;
- Recomandări cu privire la securitatea cibernetică;
- Alte categorii de informație.

CU02: Utilizez Dashboard

Reprezintă o funcționalitate prin intermediul căreia utilizatorul autorizat al SIA RSISC va fi atenționat, va putea vizualiza și accesa rapid totalitatea evenimentelor de business specifice atribuțiilor de serviciu sau interacțiunii sale cu SIA RSISC (notificări de sistem, evenimente ale fluxurilor de lucru, etc.).

De asemenea, prin intermediul Dashboard-ului personal utilizatorul autorizat va avea acces direct la funcționalitățile aferente evenimentelor de business notificate (exemplu: deschiderea formularului electronic necesar procesării cazului de gestiune a incidentului de securitate, deschidere formularului electronic al alertei raportate, deschiderea formularului electronic al incidentului raportat etc.).

În calitate de Dashboard va servi pagina principală a interfeței utilizatorului autorizat al SIA RSISC unde vor fi amplasate toate elementele și notificările aferente utilizatorului.

Dashboard-ul va conține, de asemenea, o zonă (Favorite) dedicată configurării și afișării listei formularelor electronice aferente activității curente a utilizatorului autorizat.

CU03: Caut/vizualizez date

Caz de utilizare furnizat de SIA RSISC prin intermediul căruia utilizatorii autorizați vor putea explora stocul de date la care dispun de acces în virtutea rolului deținut în cadrul sistemului informatic și atribuțiilor de serviciu.

În acest sens SIA RSISC va oferi mecanism de căutare a datelor folosindu-se diverse criterii cum ar fi:

- date de identificare a sistemului informatic;
- date de identificare a autorităților publice posesoare de sisteme informatice;
- date aferente sistemului de metadate specific alertelor/incidentelor de securitate cibernetică;
- date aferente utilizatorilor autorizați care au procesat înregistrările bazei de date;
- date de detaliu a cazurilor de gestiune a incidentelor de securitate cibernetică;
- date de detaliu ale alertelor raportate;
- date de detaliu ale incidentelor raportate;
- statutul înregistrărilor;
- alte categorii de date specifice.

SIA RSISC va afișa în calitate de rezultate găsite:

- autorități publice posesoare de sisteme informatice;
- utilizatori autorități;
- alerte raportate;
- incidente raportate;
- cazuri de gestiune a incidentelor;

- formulare ale cazurilor de gestiune a incidentelor de securitate cibernetică;
- alte ținte specifice.

Pentru fiecare categorii de rezultate SIA RSISC va permite efectuarea următoarelor manipulări:

- pentru utilizatorii găsiți: vizualizarea profilului utilizatorului, vizualizarea cazurilor de gestiune a incidentelor de securitate aferente utilizatorului, vizualizarea formularelor aferente cazului de gestiune a incidentului de securitate cibernetică, vizualizarea alertelor de securitate cibernetică raportate/ procesate, vizualizarea incidentelor de securitate cibernetică raportate/procesate, generarea raportului generalizator al cazului de gestiune a incidentului de securitate cibernetică etc.;
- pentru dosarele cazurilor de gestiune a incidentelor de securitate cibernetică: accesare conținut dosar caz de gestiune incident de securitate cibernetică, generarea fișei cazului de gestiune a incidentului de securitate cibernetică etc.;
- pentru evenimentele de business ale cazurilor de gestiune a incidentelor de securitate cibernetică: vizualizarea documentului aferent evenimentului, accesarea formularului electronic de perfectare a evenimentului de business, aprobarea/respingerea formularului, generarea documentului aferent evenimentului de business;
- pentru alertele/incidentele de securitate cibernetică raportate: deschiderea cazului de gestiune a incidentului de securitate cibernetică, schimbare statut al formularului alertei/incidentului raportat etc.

Este binevenit ca SIA RSISC să livreze mecanism de căutare indexată a datelor și prezentarea rezultatelor în funcție de relevanța rezultatelor interogării formulate.

CU04: Raportez alertă și/sau incident de securitate cibernetică

Caz de utilizare complex care furnizează totalitatea funcționalităților destinate raportării problemelor de securitate cibernetică. Acestea vor fi perfectate prin intermediul unor formulare electronice specializate cu facilități de aplicare a semnăturii electronice a raportorilor. Raportarea alertelor și/sau incidentelor de securitate cibernetică va păutea fi realizată prin intermediul a 2 opțiuni:

- **CU04.1: Raportez alertă**. Destinat raportării alertelor de securitate cibernetică (evenimente care reprezintă indicii privind riscul înalt de producere a unui eveniment de securitate).
- **CU04.2: Raportez incident**. Destinat raportării unui eveniment de securitate cibernetică pentru a fi escaladat și soluționat de către specialiștii în domeniu din cadrul entității raportoare sau STISC.

CU05: Generez documente și rapoarte

Funcționalitate accesibilă utilizatorilor autorizați ai SIA RSISC care permite generarea documentelor specifice proceselor de business implementate și a rapoartelor statistice destinate utilizatorilor autorizați pentru analiza conținutului informațional și asistarea procesului de luare a deciziei.

Rapoartele în cauză sunt utile pentru producerea documentelor și rapoartelor specifice activității STISC, analiza bazei informaționale a sistemului informatic, performanței activității utilizatorilor autorizați în, permițând extragerea unor indicatori de performanță destinați analizei proceselor de business ale cazurilor de gestiune a incidentelor de securitate cibernetică.

Este binevenit ca sistemul informatic să integreze o soluție dedicată configurării și generării rapoartelor statistice (generator de rapoarte) care să fie reutilizată, de asemenea, pentru configurarea și extragerea

documentelor tipizate specifice proceselor de business ale SIA RSISC. Documentele pot fi generate, de asemenea, în baza unor șabloane configurabile.

CU06: Recepționez notificări

Caz de utilizare prin intermediul căruia utilizatorii autorizați, indiferent de rolul lor vor recepționa notificările expediate de SIA RSISC referitoare la evenimentele de business unde sunt implicați.

SIA RSISC va asigura generarea notificării în formatul solicitat și expedierea acesteia. Utilizatori autorizați cu roluri specifice vor putea configura individual preferințele de recepționare a notificărilor prin intermediul Dashboard-ului personal.

CU07: Gestionez alertă de securitate cibernetică

Caz de utilizare complex care furnizează rolurilor relevante funcționalitățile necesare examinării și procesării alertelor de securitate recepționate prin intermediul CU04 și CU17. Procesarea alertelor de securitate cibernetică presupune examinarea alertelor, schimbarea statutului și efectuarea unor acțiuni, în funcție de caz (exemplu: închiderea alertei, inițierea unui caz de gestiune a incidentului de securitate etc.).

CU08: Gestionez incident de securitate cibernetică

Unul din cele mai complexe cazuri de utilizare care furnizează funcționalitățile cheie ale SIA RSISC: gestiunea incidentelor de securitate cibernetică. Acest caz de utilizare furnizează totalitatea formularelor electronice necesare documentării procesului de gestiune a incidentului de securitate cibernetică. Acest proces este digitizat prin intermediul următoarelor funcționalități:

- **CU08.1: Deschid/ închid caz de gestiune incident**. Funcționalitate utilizată pentru deschiderea și închiderea cazurilor de gestiune a incidentelor de securitate cibernetică. Un caz de gestiune a unui incident de securitate cibernetică poate fi deschis doar în baza unui incident de securitate raportat și poate fi închis doar în cazul când toate etapele de gestiune a incidentului de securitate cibernetică au fost efectuate (toate formularele electronice aferente au fost perfectate și aprobate).
- **CU08.2: Introduc rezultate evaluare incident**. Funcționalitate utilizată pentru evaluarea, documentarea și clasificarea incidentelor de securitate cibernetică (descrierea incidentului de securitate, stabilirea categoriei incidentului de securitate cibernetică, determinarea impactului incidentului de securitate cibernetică, evaluarea impactului incidentului de securitate cibernetică, estimarea urgenței soluționării incidentului de securitate cibernetică, prioritizarea incidentului de securitate cibernetică, stabilirea timpului minim de reacție a specialiștilor în securitatea informației cibernetică.
- **CU08.3: Introduc detalii escaladare și comunicare incident**. Funcționalitate prin intermediul căreia este configurată strategia de escaladare a incidentului de securitate cibernetică și implementat mecanismul de comunicare între utilizatorii desemnați să soluționeze incidentul de securitate cibernetică.
- **CU08.4: Introduc rezultate soluționare incident**. Funcționalitate care furnizează totalitatea formularelor electronice destinate documentării etapelor de soluționare a incidentului de securitate cibernetică: investigarea incidentului de securitate cibernetică, izolarea resursei TIC afectate de incidentul de securitate cibernetică, tratarea incidentului de securitate cibernetică, recuperarea resursei TIC afectate de incidentul de securitate cibernetică, determinarea cauzei incidentului de securitate cibernetică și formularea recomandărilor destinate tratării pe viitor a unor incidente de securitate cibernetică similare.

- **CU08.5: Introduc rezultate analiză follow-up**. Funcționalitate care furnizează formularul electronic destinat perfectării raportului follow-up al incidentului de securitate cibernetică în baza căruia se va face analiza performanței specialiștilor implicați în soluționarea incidentului de securitate cibernetică.

CU09: Aprob/resping proiecte

Caz de utilizare disponibil utilizatorilor cu rol decident în cadrul SIA RSISC prin intermediul căruia va putea aproba sau respinge proiectele formularelor electronice și documentelor specifice evenimentelor de business aferente cazurilor de gestiune a incidentelor de securitate cibernetică.

Aprobarea sau respingerea formularului electronic constă din perfectarea unui aviz/comentariu, selectarea opțiunii de aprobare/respingere și aplicarea semnăturii electronice a utilizatorului cu rol decident.

CU10: Gestionez conținut interfață publică

Caz de utilizare care urmează să furnizeze mijloacele funcționale destinate administrării aspectului și conținutul interfeței publice a SIA RSISC. Prin intermediul funcționalităților furnizate de acest caz de utilizare Administratorului de Conținut va putea:

- configura structura și aspectul interfeței publice (meniu de navigare, compartimente informaționale, aspect pagină principală etc.);
- plasa documente de conținu de diferită natură aferente proceselor de gestiune a incidentelor de securitate cibernetică;
- gestiona materiale instructiv-metodice aferente proceselor de asigurare a securității informației și soluționare a incidentelor de securitate cibernetică destinate specialiștilor și publicului larg;
- configura aspectul și conținutul interfeței publice a SIA RSISC.

CU11: Administrez utilizatori și controlul accesului

Caz de utilizare care implementează funcționalitățile destinate gestiunii profilurilor utilizatorilor și drepturilor de acces la resursele și datele SIA RSISC. SIA RSISC va utiliza 3 alternative de autentificare a utilizatorilor: login+parolă, semnătură electronică și soluția LDAP a STISC.

Sistemul informatic va furniza funcționalitățile necesare gestiunii grupurilor/rolurilor și drepturilor asociate acestora care urmează să fie ulterior atribuite utilizatorilor autorizați. Drepturile de acces la interfața utilizator și înregistrările bazei de date vor fi definite de grupul/rolul aferent utilizatorului sau explicit pentru fiecare utilizator în parte.

Pentru roluri specifice, drepturile de acces a utilizatorilor la datele și funcționalitățile SIA RSISC vor fi atribuite explicit de către utilizatori cu rol administrator.

CU12: Gestionez fluxuri, formulare și șabloane

Reprezintă un caz de utilizare destinat Administratorilor de Sistem care furnizează totalitatea funcționalităților disponibile acestora pentru actualizarea fluxurilor de lucru, formularelor electronice și modelelor de documente tipizate necesare imprimării documentelor de intrare sau ieșire (rapoartelor statistice): configurarea zonelor de antet, subsol, conținut static și dinamic, formatare, aspect grafic etc..

Un șablon de document/raport va conține, în cazul în care nu va fi utilizată o platformă de generare a rapoartelor, balize prin intermediul cărora va fi posibilă popularea acestuia cu informația de conținut

extrasă din conținutul fișei incidentului de securitate cibernetică. Astfel, va fi posibilă uniformizarea și standardizarea setului de documente emise și procesate în cadrul proceselor de raportare și gestiune a alertelor și incidentelor de securitate cibernetică.

CU13: Gestionez metadate

Caz de utilizare a SIA RSISC prin intermediul căruia vor fi gestionate următoarele categorii de metadate:

- **Clasificatoare Internaționale**, valorile cărora sunt standardizate și acceptate la nivel internațional (exemplu: Clasificatorul Internațional al Unităților de Măsură – SI, clasificatorul țărilor etc.);
- **Clasificatoare oficiale naționale**, exemplu: Clasificatorului Unităților Administrativ-Teritoriale al Republicii Moldova, alte metadate oficiale necesare documentării proceselor de soluționare a incidentelor de securitate cibernetică;
- **Clasificatoare/nomenclatoare de interoperabilitate** valorile cărora sunt utilizate pentru implementarea schimbului de date cu sisteme informatice externe;
- **Clasificatoare/nomenclatoare interne** exemplu: variabile de sistem, parametri ai interfeței utilizator, parametri de configurare a sistemului informatic și proceselor implementate în cadrul sistemului informatic, roluri, metadate de trafic telecomunicațional, categorii de incidente, tipuri de impact, nivelul impactului, urgența soluționării incidentului, prioritățile de soluționare a incidentelor, nivele ierarhice de escaladare a incidentelor, surse de date etc.).

Clasificatoarele și nomenclatoarele interne se vor elabora și utiliza în cadrul SIA RSISC numai în absența clasificatoarelor/nomenclatoarelor internaționale și naționale oficiale.

CU14: Configurez sistem informatic

Reprezintă un caz de utilizare care furnizează totalitatea funcționalităților necesare configurării parametrilor de funcționare a SIA RSISC. Trebuie de menționat faptul că SIA RSISC trebuie să fie un sistem configurabil și adaptarea lui la necesitățile curente ale utilizatorilor trebuie să se facă prin intermediul mecanismelor de configurare fără a fi necesară intervenția în codul program, compilarea acestuia și activități de desfășurare repetată a sistemului informatic.

CU15: Monitoring operațional, diagnostică și soluționare probleme

Caz de utilizare complex prin intermediul căruia rolurile administrative ale SIA RSISC vor avea acces la funcționalitățile de monitorizare a parametrilor de funcționare a SIA RSISC, diagnostic și depanare a problemelor tehnice apărute în procesul exploatării SIA RSISC.

Cazul dat de utilizare va furniza funcționalități destinate generării rapoartelor statistice predefinite și ad-hoc privind evenimentele de exploatare a SIA RSISC. Rapoartele în cauză sunt utile pentru analiza proceselor desfășurate, bazei informaționale a sistemului informatic, performanței activității utilizatorilor autorizați, permițând anticiparea problemelor de securitate informațională. Spre deosebire de CU05 cazul de utilizare CU15 este destinat proceselor de audit informatic pentru asistența mecanismelor de asigurare a securității informației.

CU16: Execut proceduri automate

Caz de utilizare complex care furnizează funcționalitățile de declanșare și funcționare în regim automat a unui șir de funcționalități ale SIA RSISC în vederea utilizării raționale a resurselor server și furnizării la momentul oportun a datelor pentru utilizatorii autorizați.

La categoria astfel de proceduri pot fi menționate:

- Interogarea periodică a sistemelor informatice externe întru recepționarea datelor aferente alertelor și incidentelor de securitate cibernetică;
- Generarea automată a copiilor de rezervă;
- Arhivarea datelor vechi și inutile proceselor de business curente ale STISC și eliminare a acestora de pe platforma de producție;
- Ștergerea automată a formularele electronice aflate în statut „Proiect” care au depășit termenul limită de aflare în acest statut;
- Calcularea agregatelor aferente indicatorilor statistici și a rapoartelor complexe furnizate de SIA RSISC;
- Notificarea utilizatorilor autorizați ca urmarea întârzierilor, inacțiunilor în cadrul fluxurilor de lucru unde sunt implicați.

CU17: Schimb de date cu sisteme informatice

Caz de utilizare care va furniza funcționalitățile necesare SIA RSISC pentru realizarea schimbului de date cu sisteme informatice externe sau implementarea funcționalităților furnizate de serviciile guvernamentale de platformă.

Acest schimb de date se referă la expunerea sau consumarea interfețelor destinate schimbului reciproc de date (recepționarea datelor din surse externe, expedierea datelor către sisteme informatice externe și schimbul bidirecțional al datelor).

O parte din integrările cu sisteme informatice externe (cazul sistemelor informatice ale AP raportoare de alerte de securitate cibernetică sau furnizoare a datelor aferente soluționării incidentelor de securitate cibernetică) urmează a fi implementate prin intermediul platformei de interoperabilitate MConnect. Serviciile de platformă (MPass, MSign, MLog, MNotify, MPower, PDGD) urmează a fi integrate direct prin intermediul API-urilor expuse de acestea. Aceiași strategie urmează a fi utilizată pentru integrarea cu Google Analytics și rețelele de socializare.

Integrarea SIA RSISC cu sistemele informatice interne ale STISC (dacă există) urmează a fi efectuată în mare parte prin intermediul unei infrastructuri de microservicii.

CU18: Jurnalizez evenimente

Caz de utilizare prin intermediul căruia va fi efectuată jurnalizarea evenimentelor de business generate de componentele funcționale ale SIA RSISC. Orice eveniment generat în cadrul proceselor de business implementate în SIA RSISC vor fi jurnalizate și salvate în tabelele corespunzătoare ale Bazei de Date.

Mecanismul de jurnalizare va fi dezvoltat în baza standardelor și bunelor practici implementate în industrie. Sistemul informatic va livra funcționalități de configurare a strategiei de jurnalizare a evenimentelor de business, inclusiv: categoriile de evenimente de business supuse jurnalizării, perioada calendaristică de jurnalizare (determinată sau nedeterminată) etc.

Pentru evenimentele de business critice sau sensibile, jurnalizarea se va efectua în paralel utilizându-se serviciul de platformă MLog.

CU19: Expediez notificări

Caz de utilizare care furnizează funcționalitățile de notificare a utilizatorilor autorizați ai SIA RSISC. Notificările vor fi stocate în Dashboard-ul utilizatorilor autorizați asigurând-se acces direct la formularul electronic, evenimentul de business al căruia a generat notificarea.

SIA RSISC va genera și expedia automat notificări aferent oricărui eveniment de business generat de procesele de recepționare date din surse externe, procesare date recepționate din surse externe și derularea evenimentelor de business specifice raportării alertelor și incidentelor de securitate cibernetică sau specifice cazurilor de gestiune a incidentelor de securitate cibernetică. De asemenea, SIA RSISC va genera și expedia automat utilizatorilor autorizați notificări aferente oricărui eveniment de business care necesită implicarea acestora.

Sistemul informatic va notifica utilizatorii atât prin intermediul mecanismelor de notificare internă (integrate în cadrul SIA RSISC), cât și prin intermediul serviciului de platformă MNotify.

4.3. Fluxurile de lucru cheie ale sistemului informatic

SIA RSISC urmează a fi implementat în baza principiului tranzacțional, când orice adăugare, actualizare sau radiere a datelor se efectuează prin intermediul unor formulare electronice specifice ce urmează a fi procesate în baza unor fluxuri de lucru specializate.

Pentru asigurarea funcționalității în bune condiții a SIA RSISC e necesară implementarea următoarelor categorii de fluxuri:

1. **Raportarea alertei și/sau incidentului de securitate cibernetică**. Reprezintă fluxul de lucru prin care vor fi implementate mecanismele de raportare a alertelor și/sau incidentelor de securitate cibernetică (descris prin intermediul cerințelor funcționale ale cazului de utilizare CU04).
2. **Gestiunea incidentului de securitate cibernetică**. Reprezintă fluxul de lucru care furnizează totalitatea funcționalităților necesare gestiunii unui caz de soluționare a unui incident raportat (deschidere caz, evaluare caz, escaladare caz, soluționare caz, analiză follow-up) descris prin intermediul cerințelor funcționale ale cazului de utilizare CU08.

4.4. Interfața utilizator a sistemului informatic

SIA RSISC trebuie să ofere o interfață utilizator ergonomică, intuitivă și accesibilă tuturor tipurilor de utilizatori. Interfața utilizator a sistemului informatic va fi accesată prin intermediul unui navigator Internet și va poseda un design grafic intuitiv, agreabil, echilibrat și distinct optimizat pentru rezoluția minimă 1360x468 de lucru la calculatoarele de tip PC.

Interfața publică a SIA RSISC trebuie să fie responsivă pentru rezoluțiile dispozitivelor de tip smartphone și tabletă și optimizată pentru ecranele tactile.

Pentru ușurința utilizatorilor, soluția informatică va dispune un sistem de ajutor contextual on-line, la nivelul fiecărei interfețe utilizator.

În dependență de categoriile utilizatorilor (drepturile și rolurile acestora) sistemul informatic va furniza o interfață personalizată fiecărei categorii de utilizator.

SIA RSISC va furniza o interfață utilizator în limba română și rusă. Procedurile de regăsire a datelor vor fi implementate prin intermediul unor căutări simple (specificarea unor șiruri de căutare) sau a unor căutări de complexitate mai ridicată, prin intermediul cărora se poate realiza o filtrare mai exacta a informației (formulare QBE). Indiferent de natura informației căutate, utilizatorul va folosi aceeași metodă de interogare și regăsire a informației pentru orișicare compartiment al sistemului informatic.

Adițional la modulul de căutare realizat pe baza principiului QBE care va da posibilitatea de a defini interogări sofisticate în mod vizual, interfața utilizator trebuie să ofere posibilitatea de a afina rezultatele căutării prin asigurarea posibilității filtrării datelor în lista cu rezultatele căutării.

Interfața utilizator a SIA RSISC trebuie să asigure filtrarea înregistrărilor ce corespund criteriului de căutare prezentate utilizatorilor în funcție de drepturile lor de acces.

Mărimile indexate (valori din clasificatoare, nomenclatoare) trebuie să poată fi filtrate prin alegerea valorii din liste predefinite. Pentru câmpurile de tip numeric sau dată caracterial trebuie să existe posibilitatea filtrării după valoarea exactă a caracteristicii căutate sau după mască de căutare. Pentru câmpurile de tip dată calendaristică se va putea indica data exactă sau interval.

Conținutul oricărui tabel cu rezultate sau formă electronică, în funcție de natura informației conținute, trebuie să poată fi exportat fie în format CSV, XLS/XSLX și PDF. Exportul datelor va fi strict delimitat prin roluri. Toate acțiunile de export a datelor vor fi jurnalizate.

4.5. Mecanismul de raportare, audit și statistică al sistemului informatic

SIA RSISC va avea implementate funcționalități destinate auditului/jurnalizării pe larg utilizat în industrie. Acesta trebuie să fie configurabil pentru a jurnaliza evenimentele tehnice și business.

Sistemul informatic va furniza mecanism de generare a rapoartelor predefinite și ad-hoc capabile să asigure o analiză sau evaluare pertinentă a proceselor de business aferente funcționării SIA RSISC.

Sistemul de raportare a SIA RSISC va delimita 4 categorii de rapoarte:

- **Documentele generate în baza șablonului predefinit** – pentru fiecare tip se va crea câte un șablon care va fi populat cu informație relevantă documentului (exemplu: Raport de analiză follow-up etc.);
- **Rapoarte statistice** – reprezintă rapoarte de analiză a proceselor de business specifice raportării și soluționării incidentelor de securitate cibernetică;
- **Rapoarte de monitorizare** – reprezintă o categorie de rapoarte destinate administratorilor de sistem utilizate pentru aprecierea modalității de interacțiune a utilizatorilor autorizați cu SIA RSISC. Această categorie de rapoarte va permite anticiparea problemelor de performanță în activitatea STISC sau a problemelor de securitate cibernetică și vulnerabilitate a sistemului informatic;
- **Rapoarte de performanță** – reprezintă o categorie de rapoarte statice destinate auditului și analizei conținutului informațional al SIA RSISC în vederea aprecierii eficienței activității angajaților STISC (exemplu: raportul de performanță a utilizatorului autorizat, raportul de performanță subdiviziunilor teritoriale, raportul de performanță al STISC per ansamblu etc.).

Particularitățile mecanismului de raportare sunt descrise într-un șir de compartimente ale prezentului document cum ar fi:

- compartimentul 5.2 (cerințele funcționale pentru cazul de utilizare CU01: Explorez conținut interfață publică);
- compartimentul 5.6 (cerințele funcționale pentru cazul de utilizare CU05: Generez documente și rapoarte);
- compartimentul 5.16 (cerințele funcționale pentru cazul de utilizare CU13: Monitoring operațional, diagnostică și soluționare probleme).

5. Cerințele funcționale ale sistemului informatic

5.1. Convenții la formularea cerințelor funcționale

Cerințele stabilite în acest document sunt marcate utilizând următoarea convenție:

- toate cerințele sunt indexate cu 3 valori **C.X.Y**, unde **C** reprezintă categoria cerinței (**CF** – cerință funcțională) **X** reprezintă cazul de utilizare pentru care este formulată cerința funcțională iar **Y** este identificatorul unic al cerinței în cazul de utilizare din care face parte.
- pentru fiecare cerință funcțională este menționată obligativitate: **M** – cerință obligatorie a fi implementată (de la noțiunea **Mandatoriu**), **D** – cerință dorită a fi implementată, opțională (de la noțiunea **Dorit**), **I** – cerință informativă.

Oferta tehnică trebuie să fie conformă în mod obligatoriu tuturor cerințelor indicate ca fiind obligatorii. Oferta tehnică va obține un avantaj competitiv pentru fiecare cerință opțională asumată a fi implementată.

Cerințele informative sunt destinate să ofere mai multă informație de suport, pentru o înțelegere mai bună a contextului altor cerințe.

5.2. CU01: Explorez conținut interfață publică

Cerințele funcționale ale facilităților de explorare a interfeței publice a SIA RSISC sunt expuse în tabelul 5.1.

Tabelul 5.1. Cerințele funcționale ale cazului de utilizare CU01

ID	Obligativitate	Descrierea cerinței funcționale
CF 01.01.	M	Interfața Publică a SIA RSISC va furniza mecanism de navigare în categoriile de structură în scopul găsirii rapide a informației relevante.
CF 01.02.	M	Navigarea se va efectua prin intermediul meniului principal de navigare și interfața utilizator a Paginii Principale.
CF 01.03.	M	La accesarea mecanismului de navigare în categoriilor de structură, Interfața Publică a SIA RSISC tip va furniza un mecanism de navigare similar după principiile de utilizare unui director de căutare (unde arborele de structură corespunde structurii Paginii WEB).
CF 01.04.	M	Documentele de conținut vor fi amplasate în categoriile frunză ale arborelui de structură a Interfeței Publice a SIA RSISC.
CF 01.05.	M	Interfața Publică a SIA RSISC va afișa referințe de nivel pentru a arăta nivelul ierarhic compartimentului curent al Interfeței Publice.
CF 01.06.	M	Referințele de structură vor avea referințe hipertext care vor permite navigarea spre nivelele ierarhice superioare categoriei curente.
CF 01.07.	M	Interfața Publică a SIA RSISC trebuie să furnizeze mecanism de generare a conținutului textual în format A4 (optimizat pentru imprimare) și descărcare a documentelor plasate în conținut.

ID	Obligativitate	Descrierea cerinței funcționale
CF 01.08.	M	Interfața publică a SIA RSISC va asigura acces la o bază de cunoștințe prin intermediul căreia se vor accesa următoarele categorii de date și facilități funcționale: • documente în format HTML (redactate cu ajutorul editoarelor WYSIWYG); • ghiduri/instrucțiuni încărcate în format PDF, DOC/DOCX, PPT/PPTX etc.; • documente de politici cu privire la securitatea informației; • recomandări cu privire la securitatea informației; • răspuns la întrebările frecvente (F.A.Q.); • referințe la cadrul legal în vigoare conținut în Registrul de Stat al Actelor Juridice (https://www.legis.md); • informație multimedia încărcată nemijlocit în SIA RSISC sau publicată prin intermediul resurselor externe (exemplu: Youtube, Rețele de socializare etc.).
CF 01.09.	M	Interfața publică a SIA RSISC va asigura acces la KPI și rapoarte statistice cu caracter public generate în baza datelor produse în cadrul fluxurilor de lucru aferente SIA RSISC.
CF 01.10.	M	Interfața Publică a SIA RSISC va furniza facilități de partajare a conținutului pe cele mai populare rețele de socializare (Facebook, Twitter, LinkedIn etc.).
CF 01.11.	M	Interfața public va furniza mecanism de feedback și contact prin intermediul cărora Internauții vor putea interacționa cu responsabilii din cadrul Centrului pentru Securitatea Cibernetică.
CF 01.11.	M	Toată informația statistică de interacțiune a Utilizatorilor Internet cu interfața publică a SIA RSISC va fi colectată prin intermediul API-ului expus de Google Analytics (Furnizorul va efectua toate activitățile de integrare a SIA RSISC cu Google Analytics).

5.3. CU02: Utilizez Dashboard

Cerințele funcționale destinate funcționării Dashboard-ului utilizatorilor autorizați ai SIA RSISC sunt expuse în tabelul 5.2.

Tabelul 5.2. Cerințele funcționale ale cazului de utilizare CU02

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 02.01.	M	SIA RSISC va livra utilizatorilor autorizați o soluție Dashboard prin intermediul căreia vor fi notificați asupra evenimentelor de business importante și accesa rapid detaliile acestora.
CF 02.02.	M	Pot fi enumerate următoarele categorii de evenimentele de business afișate în cadrul Dashboard-ului:

Identificator	Obligativitate	Descrierea cerinței funcționale
		• notificări de sistem; • notificări privind alertele de securitate cibernetică ce urmează a fi examinate; • notificări privind incidentele de securitate cibernetică ce urmează a fi gestionate; • notificări privind necesitatea implicării utilizatorului în activitățile fluxurilor de lucru ale SIA RSISC (inclusiv alerte de întârziere); • notificări privind formulare sau documente care așteaptă aprobare de la rolurile decidente (inclusiv alerte de întârziere); • notificări privind completarea fișei incidentului de securitate cibernetică cu noi documente sau formulare electronice; • notificări privind evenimentele de trasabilitate a alertelor și incidentelor de securitate cibernetică; • alte evenimente relevante.
CF 02.03.	M	Dashboard-ul utilizatorului SIA RSISC va afișa doar evenimente de business relevante rolurilor și drepturilor asignate utilizatorului autorizat.
CF 02.04.	M	Dashboard-ul utilizatorului cu rol Administrator de Sistem va afișa toate evenimente de business aferente funcționalității SIA RSISC (totalitatea notificărilor afișate în Dashboard-ul tuturor utilizatorilor SIA RSISC și notificările dedicate exclusiv utilizator cu rol de Administrator de Sistem).
CF 02.05.	M	Dashboard-ul va grupa evenimentele de business afișându-le sub formă de indicatori cu valori agregate (exemplu: Notificări de sistem necitite -14; Alerte de securitate noi - 45, Incidente de securitate noi – 6, Cazuri curente de gestiune a incidentelor - 8, Formulare expediate spre aprobare - 8 etc.) care vor conține referință hipertext de accesare a detaliilor.
CF 02.06.	M	SIA RSISC va afișa înregistrări detaliate ale Dashboard-ului în ferestre sau zone specializate pe pagina principală a interfeței utilizatorului autorizat care la rândul lor vor dispune de referință hipertext de accesare directă a detaliilor (*exemplu: lista alertelor ce urmează a fi procesate*).
CF 02.07.	M	La accesarea referinței hipertext aferentă valorii agregate sau înregistrării detaliate a Dashboard-ului SIA RSISC va asigura accesul la informația de detaliu aferentă acestora sau funcționalitatea solicitată (*exemplu: formularul de evaluare a incidentului, formularul de escaladare a incidentului, formularul de introducere a rezultatelor soluționare incident etc.*).

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 02.08.	M	Dashboard-ul SIA RSISC va conține o zonă specializată (favorite) în care utilizatorul și va plasa referințe la informația de conținut la care lucrează. Acestea pot fi de 3 tipuri: • cazuri de gestiune a incidentelor de securitate cibernetică deschise/închise; • formulare electronice perfectate (evenimente de business aferente cazurilor de gestiune a alertelor sau incidentelor de securitate cibernetică perfectate curent); • formulare electronice examinate spre aprobare.
CF 02.09.	D	SIA RSISC va oferi fiecărui utilizator autorizat funcționalitate de configurare individuală a aspectului și conținutului Dashboard-ului.

5.4. CU03: Caut/vizualizez date

Cerințele funcționale aferente mecanismului de căutare a datelor stocate în baza de date a SIA RSISC sunt expuse în tabelul 5.3.

Tabelul 5.3. Cerințele funcționale ale cazului de utilizare CU05

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 03.01.	M	SIA RSISC va furniza mecanism complex de căutare a datelor în întreg conținutul bazei de date.
CF 03.02.	M	SIA RSISC va furniza mecanism de căutare indexată a datelor utilizând Elastic Search.
CF 03.03.	M	SIA RSISC va permite definirea următoarelor ținte de căutare (rezultatul căutării va afișa lista de): • autorități publice posesoare de sisteme informatice; • utilizatori autorități; • alerte raportate; • incidente raportate; • cazuri de gestiune a incidentelor; • formulare ale cazurilor de gestiune a incidentelor de securitate cibernetică • alte ținte specifice.
CF 03.04.	M	SIA RSISC va furniza un mecanism flexibil și performant de definire a criteriilor de căutare.
CF 03.05.	M	În calitate de criterii de căutare vor putea fi folosite: • date aferente sistemului informatic sursă a alertei sau a incidentului de securitate cibernetică;

Identificator	Obligativitate	Descrierea cerinței funcționale
		• date de identificare a autorităților publice posesoare de sisteme informatice; • date aferente utilizatorilor autorizați care au procesat înregistrările bazei de date; • date aferente sistemului de metadate specific alertelor sau incidentelor de securitate cibernetică; • date de detaliu a cazurilor de gestiune a incidentelor de securitate cibernetică; • date de detaliu ale alertelor raportate; • date de detaliu ale incidentelor raportate; • statutul înregistrărilor; • alte categorii de date specifice.
CF 03.06.	M	În cazul formulări unor criterii de căutare prea largi, sau care necesită prea mult timp și resurse pentru execuție SIA RSISC nu va executa aceste interogări ci va solicita utilizatorului îngustarea domeniului de valori căutate.
CF 03.07.	M	Rezultatele căutării vor fi ordonate în funcție de relevanța rezultatului interogării de căutare, alfabetic sau dată creare/ultimă actualizare.
CF 03.08.	M	Utilizatorul va putea defini criterii de ordonare și grupare a conținutului listei cu rezultatele procesului de căutare.
CF 03.09.	M	SIA RSISC va oferi mecanism de paginare a rezultatelor căutării destinat evitării supraîncărcării exploratorului WEB și canalelor de transport date.
CF 03.10.	D	Înregistrările rezultatelor căutării vor fi marcate (culoare sau iconiță specifică) în funcție de natura sau statutul obiectului informațional găsit.
CF 03.11.	M	SIA RSISC va furniza funcționalitate de afinare a căutării în rezultatele găsite.
CF 03.12.	M	SIA RSISC va permite declanșarea unor procese asupra rezultatelor găsite sau a unui grup de rezultate găsite și marcate cum ar fi: • selectare înregistrări ale rezultatului căutării; • vizualizare detalii înregistrări găsite; • semnare electronică multiplă; • suprimare multiplă; • pentru utilizatorii găsiți: vizualizarea profilului utilizatorului, vizualizarea cazurilor de gestiune a incidentelor de securitate aferente utilizatorului, vizualizarea formularelor aferente cazului de gestiune a incidentului de securitate, vizualizarea alertelor de securitate raportate/ procesate, vizualizarea incidentelor de securitate raportate/procesate etc.;

Identificator	Obligativitate	Descrierea cerinței funcționale
		• pentru dosarele cazurilor de gestiune a incidentelor de securitate: accesare conținut dosar caz de gestiune incident de securitate, generarea fișei cazului de gestiune a incidentului de securitate etc.; • pentru evenimentele de business ale cazurilor de gestiune a incidentelor de securitate: vizualizarea documentului aferent evenimentului, accesarea formularului electronic de perfectare a evenimentului de business, aprobarea/respingerea formularului, generarea documentului aferent evenimentului de business; • pentru alertele/incidentele de securitate raportate: deschiderea cazului de gestiune a incidentului de securitate, schimbare statut al formularului alertei/incidentului raportat etc. • alte acțiuni relevante.
CF 03.13.	M	SIA RSISC va afișa în rezultatele căutării doar datele ce corespund domeniul de competență a utilizatorului autorizat, rolurilor și drepturile definite în profilul de utilizator autorizat al SIA RSISC.
CF 03.14.	M	SIA RSISC va restricționa accesul la detaliile rezultatelor găsite în cazul când utilizatorul care a declanșat procesul de căutare nu dispune de drepturi de acces la obiectele informaționale solicitate a fi accesate.
CF 03.15.	M	SIA RSISC va permite exportarea tabelului cu rezultatele căutării în format CSV sau PDF.

5.5. CU04: Raportez alertă sau incident de securitate cibernetică

Cerințele funcționale necesare implementării funcționalităților destinate raportării alertelor și/sau incidentelor de securitate sunt expuse în tabelul 5.4.

Tabelul 5.4. Cerințele funcționale ale cazului de utilizare CU04

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 04.01.	M	SIA RSISC va furniza utilizatorilor autorizați funcționalitate destinată Raportării alertelor și/sau incidentelor de securitate cibernetică.
CF 04.02.	M	Utilizatorii autorizați vor putea raporta prin intermediul CU04: • alerte de securitate cibernetică; • incidente de securitate cibernetică.
CF 04.03.	M	Alertele de securitate cibernetică vor putea fi perfectate fie de utilizatorii autorizați (prin intermediul CU04), fie expediate automat de sisteme informatice externe (prin intermediul CU18).
CF 04.04.	M	Alerta și/sau incidentul se raportează conform formularului prezentat în Anexa 2.1.

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 04.05.	D	Formularele de raportare a alertelor și/ sau incidentelor de securitate cibernetică perfectate prin intermediul CU04 vor fi afișate în baza configurațiilor definite prin intermediul CU13.
CF 04.06.	M	Stările și tranzițiile prin care poate formularele de raportare a - alertelor și/ sau incidentelor de securitate cibernetică perfectate prin intermediul CU04 sunt configurate prin intermediul cazului de utilizare CU13.
CF 04.07.	M	SIA RSISC va asigura acces utilizatorilor autorizați la lista de formulare de raportare a problemelor de securitate în funcție de rolurile deținute de aceștia și împuternicirilor furnizate de MPower.
CF 04.06.	M	Perfectarea formularului electronic destinat raportării - alertelor și/ sau incidentelor de securitate cibernetică se efectuează doar prin intermediul unor mecanisme exclusiv vizuale.
CF 04.07.	M	Formularul electronic destinat raportării - alertelor și/ sau incidentelor de securitate cibernetică va conține constrângeri și restricții de conținut în vederea limitării erorilor mecanice.
CF 04.08.	M	SIA RSISC va permite atașarea de fișiere la formularul electronic de raportare a - alertei și/ sau incidentului de securitate cibernetică (documente PDF, CSV, capturi ecran sau fișiere video etc.).
CF 04.09.	M	SIA RSISC va furniza mecanism de verificare a plenitudinii sau corectitudinii perfectării formularului electronic de raportare a - alertelor și/ sau incidentelor de securitate cibernetică (obligativitate conținut date, corectitudine tip date inserate, integritate date introduse etc.).
CF 04.10.	M	Doar un formular electronic de raportare a alertei și/sau incidentului de securitate cibernetică care a trecut cu succes procedura de verificare a corectitudinii perfectării va putea fi expediat spre examinare.
CF 04.11.	M	SIA RSISC va asigura un mecanism de trasabilitate (păstrarea istoricului) de examinare a alertei și/sau incidentului de securitate cibernetică raportate.
CF 04.12.	M	SIA RSISC nu va permite suprimarea niciunui formular de raportare a alertei și/sau incidentului de securitate cibernetică expediat spre examinare, în examinare sau procesat ci doar anularea acestuia.
CF 04.13.	M	Un formular de raportare a alertei și/sau incidentului de securitate cibernetică expediat prin intermediul CU04 trebuie semnat electronic de expeditor anterior expedierii spre examinare.
CF 04.14.	M	În calitate de mecanism de semnare electronică a formularului de raportare a alertei și/sau incidentului de securitate cibernetică va fi utilizat serviciul guvernamental MSign.

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 04.1.01	M	SIA RSISC va furniza funcționalitate de raportare a alertelor de securitate cibernetică.
CF 04.1.02	I	O alertă de securitate reprezintă o notificare a unei activități anomalice, ce poate servi ca un indiciu de vulnerabilitate cu risc înalt de exploatare în scopul producerii unui incident de securitate cibernetică
CF 04.1.03	M	O alertă de securitate cibernetică poate fi expediată, de asemenea, în mod automat de către sistemele informatice unde este atestată. Aceste alerte sunt recepționate prin intermediul CU18.
CF 04.1.04	M	Formularul alertei de securitate cibernetică poate avea mai multe stări (statute) și tranziții, în funcție de configurările definite prin intermediul CU13.
CF 04.1.04	M	Conținutul unui formular al alertei de securitate cibernetică poate fi modificat doar în statutul de proiect (până la semnarea electronică a acestuia).
CF 04.1.06	M	SI RISC va păstra proiectul de alertă de securitate cibernetică o perioadă determinată de timp (definită prin intermediul CU15), după care proiectul de alertă va fi suprimat, autorul fiind notificat în prealabil.
CF 04.1.07	M	În momentul în care, alerta va fi expediată spre examinare SIA RSISC va notifica expeditorul și utilizatorul responsabil de procesare a alertei privind recepționarea acesteia..
CF 04.1.08	M	În calitate de mecanism de notificare externă va fi utilizat serviciul guvernamental MNotify.
CF 04.2.01	M	SIA RSISC va furniza funcționalitate de raportare a incidentelor de securitate cibernetică.
CF 04.2.02	I	Un incident de securitate este un eveniment (acțiune ce perturbă activitatea normală) , care poate indica faptul că sistemele sau datele unei entități au fost compromise sau că măsurile de securitate cibernetică adoptate pentru a le proteja au eșuat.
CF 04.2.03	M	Formularul incidentului de securitate cibernetică poate avea mai multe stări (statute) și tranziții, în funcție de configurările definite prin intermediul CU13.
CF 04.2.04	M	Conținutul unui formular al incidentului de securitate cibernetică poate fi modificat doar în statutul de proiect (până la semnarea electronică a acestuia).
CF 04.2.04	M	SI RISC va păstra proiectul de incident de securitate cibernetică o perioadă determinată de timp (definită prin intermediul CU15), după care formularul incidentului de securitate cibernetică în statut proiect va fi suprimat, autorul fiind notificat în prealabil.

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 04.2.06	M	În momentul în care cazul incidentului de securitate cibernetică va fi expediat spre examinare, SIA RSISC va notifica expeditorul și utilizatorul responsabil de procesare a incidentului privind recepționarea acestuia.
CF 04.2.07	M	În calitate de mecanism de notificare externă va fi utilizat serviciul guvernamental MNotify.
CF 04.2.08	M	Un formular de raportare a incidentului de securitate cibernetică va avea asociat un caz gestiune a incidentului de securitate cibernetică care va conține istoricul și evenimentele de trasabilitate a acestuia.

5.6. CU05: Generez documente și rapoarte

Cerințele funcționale ale componentei de extragere a documentele specifice proceselor de business și a rapoartelor statistice a SIA RSISC sunt expuse în tabelul 5.5.

Tabelul 5.5. Cerințele funcționale ale cazului de utilizare CU05

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 05.01.	M	SIA RSISC trebuie să fie în măsură să ofere un număr de documente, rapoarte statistice și ad-hoc, astfel încât să acopere toate necesitățile proceselor de business destinate asigurării securității informației și escaladare a incidentelor de securitate cibernetică (după caz).
CF 05.02.	D	Este binevenit ca la baza generării rapoartelor să stea o platformă dedicată destinată configurării generării dinamice a rapoartelor (*exemplu: JasperReport*).
CF 05.03.	M	SIA RSISC trebuie să pună la dispoziția utilizatorilor un număr predefinit de documente/rapoarte configurabile și la necesitate să asigure producerea la necesitate a rapoartelor ad-hoc.
CF 05.04.	M	SIA RSISC va oferi un set de documente ce urmează a fi generate în baza datelor stocate în baza de date a sistemului informatic după cum urmează: • Raportare alertă de securitate cibernetică; • Raportare incident de securitate cibernetică; • Raport de evaluare a alertei de securitate cibernetică raportate; • Raport de analiză a incidentului de securitate cibernetică raportat; • Raport de evaluare a incidentului de securitate cibernetică; • Raport privind escaladarea și comunicarea incidentului de securitate cibernetică;

Identificator	Obligativitate	Descrierea cerinței funcționale
		• Raport privind rezultatul soluționării incidentului de securitate cibernetică; • Raport privind cauzele incidentului de securitate cibernetică; • Raport de analiză follow-up; • Recipisă de recepționare a formularului de raportare a alertei și/sau incidentului de securitate cibernetică; • Notificare de sistem; • Alte documente relevante.
CF 05.05.	M	SIA RSISC va dispune de șabloane predefinite (redactabile) pentru fiecare tip de document generat necesar actualizării eventuale a regulilor de generare.
CF 05.06.	M	Furnizorul va implementa până la 20 documente ce urmează a fi generate de SIA RSISC, inclusiv cele expuse în CF 05.04. Lista completă a documentelor urmează a fi identificată pe parcursul analizei de business.
CF 05.07.	M	SIA RSISC va oferi un set de rapoarte ce urmează a fi generate în baza datelor stocate în baza de date a sistemului informatic după cum urmează: • Raportul de performanță al SIA RSISC (date statistice privind conținutul curent al SIA RSISC) cu diferite principii de agregare (conform AP, conform sistemelor informatice, conform tipurilor de alerte/incidente, conform priorității, conform impactului, conform statutului curent al alertelor și/sau incidentelor, etc.); • Raport de performanță a utilizatorului autorizat, care conține date statistice și detalii privind cazurile de gestiune a incidentelor nou deschise, cazuri în curs de operare, cazuri închise pe perioadă determinată de timp cu un grad diferit de agregare; • Fișa dosarului cazului de gestiune a incidentelor (o sinteză a datelor din toate formularele cazului de gestiune a incidentului); • Raport privind cazurile de gestiune a incidentelor (conform subdiviziunilor, conform perioadei de timp, conform clasificatoarelor incidentelor, conform rezultatului escaladării, conform sursei etc.); • Liste de incidente (conform tuturor modalităților de filtrare posibile); • Liste de alerte conform tuturor modalităților de filtrare posibile); • Indicatori de performanță;

Identificator	Obligativitate	Descrierea cerinței funcționale
		• Alte rapoarte relevante.
CF 05.08.	M	SIA RSISC va dispune de mecanism de definire a setului de rapoarte și date disponibile fiecărei categorii de utilizator, în funcție de rolurile și drepturile deținute.
CF 05.09.	M	Un utilizator care vizualizează un document sau raport în cadrul sistemului, trebuie să-l poată exporta într-un fișier extern redactabil (XLS/XLSX și DOCX).
CF 05.10.	M	Implicit, documentele și rapoartele vor fi extrase în format PDF.
CF 05.11.	M	Furnizorul va implementa până la 20 categorii de rapoarte predefinite solicitate de beneficiar inclusiv cele specificate în CF 05.07.
CF 05.12.	M	SIA RSISC va jurnaliza toate evenimentele de generare și imprimare a documentelor și rapoartelor statistice.

5.7. CU06: Recepționez notificări

Cerințele funcționale ale mecanismului destinat recepționării notificărilor expediate de SIA RSISC în adresa utilizatorilor autorizați sunt expuse în tabelul 5.6.

Tabelul 5.6. Cerințele funcționale ale cazului de utilizare CU06

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 06.01.	M	SIA RSISC va notifica automat orice utilizator autorizat în cazul înregistrării unui eveniment de business ce implică acțiunea utilizatorului sau care modifică statutul proceselor gestionate, monitorizate de acesta sau care-l vizează.
CF 06.02.	M	Utilizatorii autorizați vor recepționa notificări în Dashboard-ul personal.
CF 06.03.	M	O copie a notificării va fi expediată la adresa E-mail indicată în profilul utilizatorului autorizat din SIA RSISC.
CF 06.04.	M	Utilizatorul autorizat SIA RSISC va dispune de funcționalitate de configurare a preferințelor de recepționare a notificărilor (la adresa E-mail sau Dashboard).
CF 06.05.	M	SIA RSISC va expedia tot spectrul de notificări destinate utilizatorilor autorizați: • notificare cu privire la recepționarea unei alerte de securitate cibernetică raportate; • notificare cu privire la recepționarea unui incident de securitate cibernetică raportat; • notificare cu privire la deschiderea/actualizarea/închiderea cazurilor de gestiune a incidentelor de securitate cibernetică;

Identificator	Obligativitate	Descrierea cerinței funcționale
		• notificare cu privire la necesitatea implicării pe fluxurile de lucru a SIA RSISC; • notificare cu privire la întârzierea acțiunii utilizatorului (depășirea termenului limită de aprobare/respingere proiect de formular, perfectare formular aferent gestiunii incidentului de securitate cibernetică etc.); • notificare cu privire la aprobarea/respingerea proiectelor de formulare electronice de către rolurile decidente; • notificare cu privire la problemele de funcționare a SIA RSISC; • alte notificări relevante.
CF 06.06.	M	O notificare expediată stocată în Dashboard-ul utilizatorului autorizat va conține referință hipertext pentru a deschide formularul electronic relevat notificării.
CF 06.08.	M	Utilizatorii SIA RSISC vor recepționa notificărilor prin E-mail în format HTML sau Format Text îmbogățit.
CF 06.09.	M	Notificările externe (citite prin intermediul mijloacelor externe, în afara interfeței utilizator a SIA RSISC) vor fi expediate prin intermediul serviciului de platformă MNotify.

5.8. CU07: Gestionez alertă de securitate cibernetică

Cerințele funcționale ale mecanismului destinat gestiunii alertelor de securitate cibernetică sunt expuse în tabelul 5.7.

Tabelul 5.7. Cerințele funcționale ale cazului de utilizare CU07

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 07.01.	M	SIA RSISC va furniza mecanism de procesare a alertelor de securitate cibernetică recepționate și înregistrate.
CF 07.02.	M	Alertele de securitate cibernetică vor parveni prin intermediul a 2 canale: • expediate automat de către sistemele informatice; • raportate de utilizatorii autorizați.
CF 07.03.	M	Procesarea alertei de securitate cibernetică presupune efectuarea următoarelor acțiuni puse la dispoziție de SIA RSISC: • analiza problemei; • perfectarea unui raport de analiză a alertei de securitate cibernetică; • schimbare statut alertă de securitate cibernetică (închiderea alertei în cazul în care se consideră ignorabilă);

Identificator	Obligativitate	Descrierea cerinței funcționale
		• asocierea alertei de securitate cibernetică unui incident de securitate cibernetică raportat.
CF 07.04.	M	Pentru alertele raportate de utilizatori autorizați (perfectate prin intermediul CU04.1) trebuie să fie completat un raport de analiză și răspuns la alertă (chiar dacă specialistul în securitatea informației nu depistează un careva pericol generat de alertă de securitate raportată).
CF 07.05.	M	Pentru alertele raportate de sistemele informatice nu este obligatorie completarea unui raport de analiză și răspuns la alertă. Pentru acestea este suficientă doar schimbarea statutului în cazul când specialistul de securitate nu atestă un pericol.
CF 07.06.	M	SIA RSISC va furniza funcționalitate de schimbare simultană a statutelor mai multor alerte de securitate raportate (valabil pentru alertele raportate automat de sistemele informatice).
CF 07.07.	M	SIA RSISC va notifica raportatorii de alerte de securitate cibernetică privind orice evenimente de trasabilitate aacestora. În calitate de mecanism de notificare va fi utilizat serviciul guvernamental MNotify.
CF 07.08.	M	SIA RSISC va jurnaliza toate evenimentele de procesare a alertelor de securitate cibernetică raportate (inclusiv alternativ prin intermediul serviciului guvernamental MLog).

5.9. CU08: Gestionez incident de securitate cibernetică

Cerințele funcționale care specifică particularitățile de gestiune a cazurilor de gestiune a incidentelor de securitate cibernetică și perfectare a formularelor electronice aferente analizei și escaladării incidentelor de securitate cibernetică raportate sunt expuse în tabelul 5.8.

Tabelul 5.8. Cerințele funcționale ale cazului de utilizare CU08

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 08.01.	M	SIA RSISC va furniza funcționalitate destinată gestiunii cazurilor de gestiune a incidentelor de securitate cibernetică.
CF 08.02.	M	Gestiunea unui caz de gestiune a incidentului de securitate cibernetică presupune efectuarea următoarelor acțiuni: • deschidere/închidere/redeschidere caz de gestiune a incidentului de securitate cibernetică; • evaluarea incidentului de securitate cibernetică; • escaladarea incidentului de securitate cibernetică; • soluționarea incidentului de securitate cibernetică; • investigarea cauzei producerii incidentului de securitate cibernetică.

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 08.03.	M	SIA RSISC va permite, completarea electronică a conținutului fișei incidentului de securitate cibernetică de către Registrator precum și introducerea retroactivă a detaliilor incidentului de securitate cibernetică (cazul când raportatorul dispune de soft destinat documentării incidentului de securitate cibernetică și datele parvin automat prin intermediul CU18).
CF 08.04.	M	SIA RSISC va permite completarea automată a unor formulare electronice aferente cazului de gestiune a incidentului de securitate cibernetică utilizând datele altor cazuri de gestiune a incidentelor de securitate completate în prealabil (exemplu: în cazul unor incidente de securitate similare).
CF 08.05.	M	Formularele electronice de completare a fișei incidentului de securitate cibernetică vor fi afișate și validate în baza configurațiilor definite prin intermediul CU13.
CF 08.06.	M	Stările și tranzițiile prin care poate trece formularul electronic destinat documentării cazului de gestiune a incidentului de securitate cibernetică sunt configurate prin intermediul cazului de utilizare CU13.
CF 08.07.	M	Orice formular electronic destinat documentării procesului de gestiune a incidentului de securitate cibernetică va avea asociat un șablon de document care va fi configurat prin intermediul CU13 și extras prin intermediul CU05 în baza datelor conținute în formular.
CF 08.08.	M	Formularul electronic destinat documentării cazului de gestiune a incidentului de securitate cibernetică poate fi accesat explicit din opțiunile de meniu, apelat din fișa incidentului de securitate cibernetică (cu completare prealabilă automată a datelor care pot fi extrase din conținutul dosarului cazului de gestiune a incidentului) sau din lista rezultatelor furnizate de CU03 (exemplu: inițierea cazului de gestiune a incidentului de securitate cibernetică în baza unor alerte sau incidente de securitate cibernetică anterior raportate).
CF 08.09.	M	SIA RSISC va asigura acces utilizatorilor autorizați la lista de formulare electronice destinate documentării cazului de gestiune a incidentului de securitate cibernetică în funcție de rolurile deținute de aceștia și împuternicirilor furnizate de MPower.
CF 08.10.	M	Perfectarea formularului electronic destinat documentării cazului de gestiune a incidentului de securitate cibernetică se efectuează doar prin intermediul unor mecanisme exclusiv vizuale.
CF 08.11.	M	Formularul electronic destinat documentării cazului de gestiune a incidentului de securitate cibernetică va conține constrângeri și restricții de conținut în vederea limitării erorilor mecanice.
CF 08.12.	M	SIA RSISC va dispune de capacități de calculare a unor valori agregate în baza datelor primare conținute (exemplu: totaluri, subtotaluri, cuantificări, calculare a unor indicatori generalizatori etc.)

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 08.13.	M	SIA RSISC va permite atașarea de copii electronice a documentelor relevante la formularul electronic aferent cazului de gestiune a incidentului de securitate cibernetică.
CF 08.14.	M	SIA RSISC va furniza mecanism de verificare a plenitudinii sau corectitudinii perfectării formularului electronic de documentare a cazului de gestiune a incidentului de securitate cibernetică (obligativitate conținut date, corectitudine tip date inserate, integritate date introduse etc.).
CF 08.15.	M	Doar un formular electronic de documentare a cazului de gestiune a incidentului de securitate cibernetică care a trecut cu succes procedura de verificare a corectitudinii perfectării va putea trece în statutul final sau expediat spre aprobare Decidentului (în cazul când formularul necesită aprobare).
CF 08.16.	M	SIA RSISC va asigura mecanism de trasabilitate (păstrarea istoricului) la propagarea modificărilor în fișa incidentului de securitate cibernetică (toate evenimentele de adăugare, modificare, suprimare date, precum și vizualizare conținut dosar vor fi accesibile spre vizualizare).
CF 08.17.	M	SIA RSISC va furniza Registratorilor funcționalitate de semnare electronică a formularelor electronice de documentare a cazului de gestiune a incidentului de securitate cibernetică (dacă această obligativitate este inclusă configurațiile formularului definite prin intermediul CU12).
CF 08.18.	M	În calitate de mecanism de aplicare a semnăturii electronice va fi folosit serviciul guvernamental MSign.
CF 08.19.	M	SIA RSISC va jurnaliza toate evenimentele de gestiune a dosarului cazului de utilizare prin intermediul serviciului guvernamental MLog.
CF 08.1.01.	M	SIA RSISC va furniza funcționalitate de deschidere a unui caz de gestiune a incidentului de securitate cibernetică în baza: • alertelor de securitate cibernetică raportate prin intermediul CU04.1 • alertelor de securitate cibernetică recepționate prin intermediul CU18; • incidentelor de securitate cibernetică raportate prin intermediul CU04.2; • Incidentelor de securitate cibernetică recepționate prin intermediul CU17.
CF 08.1.02.	M	Pentru deschiderea cazului de gestiune a evenimentului de securitate cibernetică este necesară: • Identificarea alertei sau incidentului de securitate cibernetică relevant;

Identificator	Obligativitate	Descrierea cerinței funcționale
		• completarea metadatelor aferente fișei de securitate cibernetică; • definirea persoanelor responsabile în documentarea și soluționarea incidentului de securitate cibernetică; • atașarea copiilor electronice și metadatelor asociate ale documentelor specifice deschiderii cazului de gestiune a incidentului de securitate cibernetică.
CF 08.1.03.	M	Unui dosar ai cazului de gestiune a incidentului de securitate cibernetică îi pot fi atașate mai multe alerte de securitate cibernetică sau incidente de securitate cibernetică raportate.
CF 08.1.04.	M	SIA RSISC va efectua o verificare a completitudinii dosarului și corectitudinii datelor introduse anterior deschiderii cazului de gestiune a incidentului de securitate cibernetică.
CF 08.1.05.	M	Registratorul va activa un buton specializat pentru deschiderea cazului în cazul când validarea CF 08.1.04 a trecut cu succes.
CF 08.1.06.	M	Odată deschis cazul, SIA RSISC va notifica toți utilizatorii autorizați cazului și raportatorul/sursa alertei sau incidentului de securitate cibernetică (în cazul existenței adresei E-mail în profilul acestuia) asupra deschiderii unui nou caz de gestiune a incidentului de securitate cibernetică.
CF 08.1.07.	M	Un caz de gestiune a incidentului de securitate cibernetică poate trece în statut „Închis” în cazul în care toate procesele de evaluare, documentare și soluționare a incidentului de securitate cibernetică au fost finisate.
CF 08.1.08.	M	Registratorul va dispune de funcționalitate de închidere a cazului de gestiune a incidentului de securitate cibernetică (buton specializat pentru schimbarea statutului).
CF 08.1.09.	M	SIA RSISC va efectua o verificare a plenitudinii dosarului cazului de gestiune a incidentului de securitate cibernetică și doar în cazul lipsei problemelor cazul de gestiune a incidentului de securitate cibernetică va putea fi închis.
CF 08.1.08.	M	Cazurile de gestiune a incidentelor de securitate cibernetică incomplete sau care au depășit termenul limită de soluționare vor fi închise cu un statut special cu mențiunea cauzei închiderii cazului.
CF 08.1.08.	M	Odată închis cazul de gestiune a incidentului de securitate cibernetică, SIA RSISC va notifica toți utilizatorii autorizați cazului și raportatorul incidentului de securitate cibernetică (dacă există E-mail de contact în profilul acestuia).
CF 08.1.08.	M	Toate evenimentele de business aferente fișei incidentului de securitate cibernetică trebuie jurnalizate exhaustiv prin intermediul

Identificator	Obligativitate	Descrierea cerinței funcționale
		mijloacelor proprii ale SIA RSISC și în paralel prin intermediul serviciului de platformă MLog.
CF 08.2.01.	M	SIA RSISC va furniza formular de documentare a incidentului de securitate cibernetică.
CF 08.2.02.	M	Conținutul formularului de documentare a incidentului de securitate cibernetică și fluxul de lucru aferent vor fi configurate prin intermediul CU12.
CF 08.2.03.	M	Documentarea unui incident de securitate cibernetică presupune colectarea și introducerea următoarelor categorii de date: • rezultatele analizei preliminare a incidentului de securitate cibernetică; • detaliile evenimentelor adverse (dacă există); • categoria incidentului; • tipul de impact al incidentului; • rezultatul evaluării primare a impactului și a rezultatelor produse de incidentul de securitate cibernetică; • rezultatul evaluării preliminare a urgenței soluționării incidentului de securitate cibernetică; • prioritatea de soluționare a incidentului de securitate cibernetică; • alte categorii de date relevante.
CF 08.2.04.	M	Formularul de documentare primară a incidentului de securitate cibernetică va dispune de posibilitate de atașare a copiilor electronice ale documentelor (exemplu: fișiere log, capturi de ecran, seturi de date specifice etc.).
CF 08.2.05.	M	Un formular de documentare a incidentului de securitate cibernetică se consideră finisat în cazul în care este semnat de Registratorul care l-a completat.
CF 08.3.01.	M	SIA RSISC va furniza formular de comunicare și escaladare a incidentului de securitate cibernetică.
CF 08.3.02.	M	Conținutul formularului de comunicare și escaladare a incidentului de securitate cibernetică și fluxul de lucru aferent vor fi configurate prin intermediul CU12.
CF 08.3.03.	M	Escaladarea și comunicarea unui incident de securitate cibernetică presupune identificarea și introducerea următoarelor categorii de date: • echipa responsabilă de soluționarea incidentului de securitate cibernetică; • personalul responsabil de soluționare a incidentului de securitate cibernetică;

Identificator	Obligativitate	Descrierea cerinței funcționale
		• nivelele ierarhice implicate în escaladarea incidentului de securitate cibernetică; • instituțiile externe implicate în escaladarea incidentului de securitate cibernetică.
CF 08.3.04.	M	Formularul de escaladare și documentare a incidentului de securitate cibernetică va dispune de posibilitate de atașare a copiilor electronice ale documentelor (exemplu: contracte prestări servicii, acorduri SLA, planuri de continuitate etc.).
CF 08.3.05.	M	Un formular de escaladare și comunicare a incidentului de securitate cibernetică se consideră finisat în cazul în care este semnat de Registratorul care l-a completat.
CF 08.3.06.	M	Odată finisat și semnat formularul electronic destinat escaladării și comunicării incidentului de securitate cibernetică, SIA RSISC va notifica toți actorii care urmează a fi implicați în procesul de soluționare a incidentului (introduși prin intermediul CF 08.3.03) și va asigura acces la fișa incidentului de securitate cibernetică.
CF 08.4.01.	M	SIA RSISC va furniza toate formularele electronice necesare documentării procesului de soluționare a incidentului de securitate cibernetică.
CF 08.4.02.	M	Conținutul formularelor electronice destinate documentării măsurilor de soluționare a incidentului de securitate cibernetică și fluxurile de lucru aferente vor fi configurate prin intermediul CU12.
CF 08.4.03.	M	Documentarea procesului de soluționare a incidentului informatic presupune perfectarea formularelor electronice destinate documentării următoarelor etape de soluționare a incidentului de securitate cibernetică: • investigarea incidentului de securitate cibernetică; • izolarea resursei informatice afectate de incidentul de securitate cibernetică; • tratarea incidentului de securitate cibernetică; • recuperarea resursei informatice afectate de incidentul de securitate cibernetică; • revizuirea și documentarea (inclusiv îmbunătățirea procedurilor existente, formularea recomandărilor, evaluarea eficacității măsurilor întreprinse etc.).
CF 08.4.04.	M	Formularele electronice destinate documentării procesului de soluționare a incidentului de securitate cibernetică va dispune de posibilitate de atașare a copiilor electronice ale documentelor (utilizate în calitate de dovezi pentru acțiunile întreprinse).

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 08.4.05.	M	Un formular de documentare a procesului de soluționare a incidentului de securitate cibernetică se consideră finisat în cazul în care este semnat de Registratorul care l-a completat.
CF 08.4.06.	M	Odată finisat și semnat formularul electronic destinat escaladării și comunicării incidentului de securitate cibernetică, SIA RSISC va notifica toți actorii care urmează a fi implicați în procesul de soluționare a incidentului (introduși prin intermediul CF 08.3.03) și va asigura acces la fișa incidentului de securitate cibernetică.
CF 08.5.01.	M	SIA RSISC va furniza formularele electronic destinat introducerii rezultatelor analizei follow-up a incidentului de securitate cibernetică destinat investigării eficienței tratării incidentului de securitate cibernetică și documentării lecțiilor învățate.
CF 08.5.02.	M	Conținutul formularului electronic destinat analizei follow-up a incidentului de securitate cibernetică și fluxul de lucru aferent vor fi configurate prin intermediul CU12.
CF 08.5.03.	M	Analiza follow-up a unui incident de securitate cibernetică presupune identificarea și introducerea următoarelor categorii de date (o parte vor fi preluate din formularele deja perfectate a cazului de gestiune a incidentului de securitate cibernetică): • datele de identificare a incidentului de securitate cibernetică; • datele de clasificare a incidentului de securitate cibernetică; • obiectivele analizei follow-up; • date privind timpul de reacție per fiecare fază de gestiune a incidentului de securitate cibernetică; • date privind indicatorii de performanță a proceselor de soluționare a incidentului de securitate cibernetică.
CF 08.5.04.	M	Raportul de analiză follow-up a incidentului de securitate cibernetică se perfectează conform șablonului inclus în anexa A1.3.
CF 08.5.05.	M	Formularul raportului de analiză follow-up a incidentului de securitate cibernetică va dispune de posibilitate de atașare a copiilor electronice ale documentelor.
CF 08.5.06.	M	Un formular de perfectare a raportului de analiză follow-up a incidentului de securitate cibernetică se consideră finisat în cazul în care este semnat de Registratorul care l-a completat.
CF 08.5.07.	M	Un formular de analiză follow-up nu poate fi perfectat dacă fișa incidentului de securitate cibernetică nu este complet (nu au fost finisate etapele definite de CU08.1-CU08.4) și reprezintă constrângerea de bază pentru închiderea unui caz de gestiune a incidentului de securitate cibernetică.

5.10. CU09: Aprob/resping proiecte

Cerințele funcționale ale componentei destinate rolurilor decidente destinate aprobării sau respingerii formularelor electronice perfectate prin intermediul SIA RSISC sunt expuse în tabelul 5.9.

Tabelul 5.9. Cerințele funcționale ale cazului de utilizare CU09

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 09.01.	M	SIA RSISC va furniza actorilor autorizați (cu rol decident) mecanism de aprobare sau respingere a proiectelor de formulare perfectate de utilizatori autorizați (cu rol de Registrator) care necesită aprobare înainte de a fi salvate sau procesate.
CF 09.02.	M	Obligativitatea aprobării formularului electronic este configurată prin intermediul CU12 și va cuprinde setul de formulare perfectate prin intermediul CU08.
CF 09.03.	M	Lista completă a formularelor electronice care vor necesita aprobări din partea rolurilor decidente vor fi identificate în procesul analizei de business.
CF 09.04.	M	Aprobarea sau respingerea constă în perfectarea unei note, alegerea statutului (Aprobat sau Respins), confirmarea acestuia și aplicarea semnăturii electronice a utilizatorului cu rol decident.
CF 09.05.	M	Accesul la funcționalitatea de aprobare/respingere a proiectului va fi posibilă numai în cazul în care utilizatorul cu rol Decident dispune de asemenea împuternicire (verificarea se va face prin intermediul MPower).
CF 09.06.	M	SIA RSISC va utiliza serviciul de platformă MSign pentru aplicarea semnăturii electronice la Aprobarea/Respingerea formularului electronic.
CF 09.07.	M	În cazul aprobării formularului electronic, SIA RSISC va notifica toți utilizatorii relevanți acestuia privind evenimentul de aprobare/respingere.
CF 09.08.	M	În cazul respingerii formularului electronic, fluxul de lucru va trece automat la etapa precedentă (va întoarce spre reperfectare formularul utilizatorului care l-a expediat spre aprobare) și va notifica toți utilizatorii relevanți.
CF 09.09.	M	În momentul în care un formular este expediat spre aprobare acesta nu poate fi modificat decât de decidentul care trebuie să-l aprobe cu aplicarea repetată a semnăturii electronice.
CF 09.10.	M	SIA RSISC va jurnaliza toate evenimentelor de aprobare/respingere a proiectelor de formulare electronice.

5.11. CU10: Gestionez conținut interfață publică

Cerințele funcționale necesare gestiunii conținutul interfeței publice a SIA RSISC sunt incluse în tabelul 5.10.

Tabelul 5.10. Cerințele funcționale ale cazului de utilizare CU10

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 10.01.	M	SIA RSISC va furniza un mecanism de gestiune a interfeței publice destinate accesării de către utilizatori anonimi.
CF 10.02.	M	Mecanismul de gestiune a interfeței publice destinate accesării de către utilizatori anonimi și candidați trebuie să furnizeze următoarele funcționalități: • gestiunea meniului de navigare; • configurarea paginii principale; • gestiunea informației de conținut (noutăți, F.A.Q., publicații, informație multimedia); • gestiunea materialelor instructiv metodice; • gestiunea studiilor de caz.
CF 10.03.	M	SIA RSISC va furniza un mecanism de gestiune a structurii conținutului interfeței publice în baza căreia va fi afișat meniul de navigare.
CF 10.04.	I	Structura interfeței publice a SIA RSISC reprezintă un arbore cu nelimitat în nivele ierarhice frunzele căruia conțin informația de conținut.
CF 10.05.	M	SIA RSISC va furniza funcționalitate de reorganizare a arborelui de structură a interfeței publice (mutare subcategorie dintr-o categorie în alta, ascundere/ștergere categorii ale arborelui de structură, redenumire a categoriilor arborelui de structură etc.).
CF 10.06.	M	Pentru categoriile de structură a arborelui de structură se va putea defini: • informație de conținut (adăugare/modificare/ștergere informație de conținut); • URL de acces la modulele interfeței publice sau accesare a resurselor externe; • Subcategorii subordonate.
CF 10.07.	M	SIA RSISC nu va permite suprimarea unei categorii de structură dacă conține cel puțin un document de conținut sau categorie subordonată.
CF 10.08.	M	SIA RSISC va furniza un mecanism de gestiune a paginii principale a interfeței publice.
CF 10.09.	I	Pagina principală reprezintă un mecanism de acces rapid la serviciile și facilitățile interfeței publice.

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 10.10.	M	Pentru pagina principală a interfeței publice a SIA RSISC trebuie să existe următoarele facilități de configurare: • definire aspect de prezentare a informației (număr de culoare afișate, compartimente și ordinea lor de afișare pe Pagina Principale); • configurarea blocurilor cu informații extrase din conținutul informațional al interfeței publice; • configurarea zonelor cu bannere de acces la serviciile SIA RSISC, resurse STISC sau externe; • configurarea accesului la serviciile electronice accesibile prin intermediul SIA RSISC; • gestiunea informației plasate în subsolul Paginii Principale și a interfeței publice.
CF 10.11.	M	SIA RSISC va dispune de funcționalitate de configurare a accesului la serviciile electronice oferite prin intermediul interfeței publice.
CF 10.12.	M	Serviciile electronice furnizate de SIA RSISC (exemplu: raportare alertă/incident) vor fi implementate prin intermediul unor module dedicate interfața cărora va fi posibilă a fi integrată în paginile interfeței publice a SIA RSISC.
CF 10.13.	M	Serviciile electronice integrate în interfața publică a SIA RSISC vor putea fie accesate la URL-uri permanente.
CF 10.14.	M	SIA RSISC va dispune de funcționalitate de gestiune a conținutului informațional prin intermediul unor facilități specifice Sistemelor de Gestiune a Conținutului care va furniza următoarele funcționalități: • redactarea și publicarea documentelor prin intermediul editoarelor WYSIWYG; • încărcarea de fișiere și imagini în conținutul documentelor publicate sau atașarea lor acestor documente; • încărcarea și publicarea informației multimedia (video); • publicarea informației multimedia din surse externe (exemplu: Youtube).
CF 10.15.	M	Toate documentele de conținut și metadatele atașate acestora publicate prin intermediul interfeței publice a SIA RSISC trebuie să corespundă rigorilor Hotărârii Guvernului nr. 188 din 03.04.2012 privind paginile oficiale ale autorităților administrației publice în rețeaua Internet.
CF 10.16.	M	SIA RSISC va furniza funcționalități pentru gestiunea unei baze de cunoștințe care să conțină informații instructiv metodice în domeniul gestiunii incidentelor de securitate.

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 10.17.	M	SIA RSISC va furniza funcționalități de definire și gestiune a structurii bazei de cunoștințe.
CF 10.18.	M	SIA RSISC trebuie să fie capabil să plaseze (și afișeze ulterior în interfața publică) următoarele tipuri de conținut în baza de cunoștințe: (materiale instructiv-metodice) • documente în format HTML (redactate cu ajutorul editoarelor WYSIWYG); • ghiduri/instrucțiuni încărcate în format PDF, DOC/DOCX, PPT/PPTX etc. • referințe la cadrul legal în vigoare conținut în Registrul de Stat al Actelor Juridice (https://www.legis.md); • informație multimedia încărcată nemijlocit în cadrul SIA RSISC sau publicată prin intermediul resurselor externe (exemplu: Youtube, Rețele de socializare etc.); • studii de caz, extrase în baza dosarelor cazurilor de gestiune a incidentelor de securitate.

5.12. CU11: Administrez utilizatori și controlul accesului

Cerințele funcționale ale componentei de administrare a utilizatorilor și configurarea accesului la interfața utilizator și conținutul bazei de date a SIA RSISC sunt reflectate în tabelul 5.11.

Tabelul 5.11. Cerințele funcționale ale cazului de utilizare CU11

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 11.01.	M	SIA RSISC va furniza funcționalitate de definire și gestiune dinamică a utilizatorilor, rolurilor și drepturilor de acces a acestora.
CF 11.02.	M	Fiecare utilizator autorizat va dispune de un profil cu următoarele categorii de date: • nume utilizator; • prenume utilizator; • adresă E-mail de contact; • număr telefon de contact; • login de acces; • parolă de acces; • strategie de autentificare (utilizator+parolă, MPass etc.); • cont activ/dezactivat; • perioadă de valabilitate a accesului; • rolurile utilizatorului; • drepturi particulare de acces la interfața utilizator și date;

Identificator	Obligativitate	Descrierea cerinței funcționale
		• alte date relevante.
CF 11.03.	M	SIA RSISC va conține o categorie implicită de utilizatori creată de Furnizor și credențialele pentru acesta sunt remise la livrare pentru categoria de **superadministrator**.
CF 11.04.	M	SIA RSISC trebuie să asigure accesul la unele funcționalități specifice doar după autentificarea și autorizarea utilizatorului. SIA RSISC va asigura suport pentru următoarele alternative de autentificare a utilizatorilor: • semnătură electronică (prin intermediul serviciului MPass); • login și parolă;
CF 11.05.	M	Gestionarea utilizatorilor precum si a rolurilor atribuite in sistem se va efectua prin intermediul MPass.
CF 11.06.	M	SIA RSISC va furniza mecanism de definire pentru utilizatori a drepturilor de acces la date în funcție categoriile sau tipurile de alerte/incidente, arealul geografic, categorii specific de date etc. ținându-se cont de atribuțiile de serviciu a utilizatorul autorizat.
CF 11.07.	M	SIA RSISC va furniza utilizatorilor autorizați funcționalități de modificare și restabilire a parolei de acces.
CF 11.08.	M	SAI SPM va asigura protecție parolelor utilizatorilor autorizați. Metoda de protecție utilizată trebuie să asigure imposibilitatea interceptării, deducerii și recuperare a parolei de acces.
CF 11.09.	M	SIA RSISC va permite blocarea/deblocarea accesului utilizatorului.
CF 11.10.	M	Comunicarea între dispozitivul utilizatorului și serverul aplicație a SIA RSISC trebuie să fie criptată (utilizând protocolul SSL/TLS).
CF 11.11.	M	SIA RSISC trebuie să fie capabil să configureze numărul de sesiuni paralele posibile de a fi inițiate de același utilizator.
CF 11.12.	M	SIA RSISC trebuie să fie capabil să configureze perioada de inactivitate a utilizatorului după care sesiunea urmează a fi închisă în mod automat.
CF 11.13.	M	SIA RSISC trebuie să prevină orice posibilitate de preluare neautorizată a sesiunilor active inițiate de utilizatorii autorizați
CF 11.14.	M	SIA RSISC va permite blocarea sesiunii la cererea utilizatorului sau automat la expirarea sesiunii utilizatorului.
CF 11.15.	M	Un Profil de utilizator autorizat poate fi eliminat fizic doar în cazul când nu există evenimente jurnalizate sau înregistrări aferente acestuia.
CF 11.16.	M	SIA RSISC trebuie să furnizeze un mecanism de gestiune granulară a drepturilor de acces la obiectele sale și a acțiunilor posibile asupra acestora (alerte de securitate cibernetică raportate, incidente de

Identificator	Obligativitate	Descrierea cerinței funcționale
		securitate cibernetică raportate, cazuri de gestiune a incidentelor de securitate cibernetică , formulare electronice, meniuri, funcționalități, rapoarte, acțiuni de adăugare/vizualizare/actualizare/ștergere date etc.).
CF 11.17.	M	Metoda de autorizare a utilizatorilor SIA RSISC trebuie să se bazeze pe principiul „*tot ce nu este permis este interzis*”.
CF 11.18.	M	SIA RSISC va furniza funcționalitate de definire a grupurilor și rolurilor utilizatorilor și facilități de asociere a utilizatorilor la grupuri și roluri.
CF 11.19.	M	Un rol este definit prin denumire generică, descriere succintă și statutul de activ/dezactivat. Rolurile dezactivate nu vor fi afișate la configurarea drepturilor de acces la resursele aplicației sau a drepturile utilizatorilor.
CF 11.20.	M	Odată introdus și activat, rolul va fi disponibil de a fi utilizat în modulele de gestiune a utilizatorilor (atașarea de roluri utilizatorilor) și gestiune a componentelor SIA RSISC (atașarea rolurilor care au acces la componentele interfeței utilizator și configurarea modalității de acces a acestora).
CF 11.21.	M	SIA RSISC trebuie să permită acordarea drepturilor de acces a la nivel de utilizator explicit, grup sau rol. Un grup de utilizatori poate cuprinde mai multe subgrupuri/roluri. Un utilizator poate fi asociat cu unul sau mai multe grupuri și roluri, iar drepturile de acces ale utilizatorului sunt determinate cumulativ.
CF 11.22.	M	SIA RSISC trebuie să permită acordarea drepturilor de acces în baza regulilor de afaceri (*exemplu: o înregistrare poate fi modificată doar atunci când utilizatorul este autorul acestuia sau când acțiunea de modificare este efectuată într-o anumită perioadă de timp, stare sau context*).
CF 11.23.	M	Un rol nu va putea fi suprimat dacă acesta este atașat măcar unui utilizator sau unei componente ale interfeței utilizator a SIA RSISC.
CF 11.24.	M	SIA RSISC va furniza mecanism de înregistrare a componentelor interfeței utilizator (resurselor) în scopul asigurării unui mecanism de definire a drepturilor de acces a utilizatorilor la interfața utilizator. Prin componentă se înțelege orice entitate modulară a aplicației (formular, meniu, opțiune de meniu, câmp etc.) gradul de detaliere a căreia este suficientă pentru configurarea drepturilor de acces, tranzițiilor fluxurilor de lucru și acțiunilor accesibile utilizatorilor.
CF 11.25.	M	SIA RSISC va permite configurarea ierarhiei componentelor interfeței utilizator, la nivelul rădăcină fiind modulele de bază ale aplicației iar nivelele subordonate nu vor fi limitate în adâncime, ierarhia fiind determinată de arhitectura acestora.

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 11.26.	M	Orice componentă a interfeței utilizator SIA RSISC va conține date privind denumire generică, descriere succintă, acțiunile disponibile utilizatorilor (evenimentele de business pe care le pot genera) rolurile care au acces la componenta interfeței utilizator sau acțiunile ce pot fi întreprinse.
CF 11.27.	M	Orice componentă a interfeței utilizator SIA RSISC va conține date privind, statutele prin care pot trece datele gestionate prin intermediul componentei, tranzițiile de parcurgere a statutelor componentei (configurare fluxuri de lucru).
CF 11.28.	M	SIA RSISC va permite definirea permisiunilor aferente acțiunilor (evenimentelor de business) disponibile utilizatorilor cu acces la componentele interfeței utilizator. Vor fi configurate următoarele categorii de acțiuni disponibile utilizatorilor: • vizualizare înregistrări; • adăugare înregistrări; • modificare înregistrări; • eliminarea înregistrări; • tranziție flux de lucru; • alte acțiuni relevante.
CF 11.29.	M	SIA RSISC trebui să permită atribuirea temporară a drepturilor deținute de un utilizator către alt utilizator. Această atribuire trebuie făcută prin păstrarea sau suspendarea drepturilor deținute de utilizatorul căruia i se atribuie temporar drepturile. Aceste împuterniciri urmează a fi definite/verificate prin intermediul serviciului de platformă MPower.
CF 11.30.	D	SIA RSISC trebuie să permită separarea activităților administrative (*exemplu: Administratorul 1 face modificările și Administratorul 2 le confirmă*).
CF 11.31.	M	SIA RSISC trebuie să furnizeze facilități pentru vizualizare și generarea de rapoarte cu privire la drepturile de acces configurate. Generarea unor asemenea rapoarte trebuie efectuată în funcție de cel puțin următoarele criterii: grup de utilizatori/rol, login, proprietăți, acțiuni permise.

5.13. CU12: Gestionez fluxuri, formulare și șabloane

Cerințele funcționale ale componentei de configurare a fluxurilor de lucru, formularelor electronice destinate inserării datelor și șabloanelor documentelor care vor fi populate cu date și generate de SIA RSISC sunt expuse în tabelul 5.12.

Tabelul 5.12. Cerințele funcționale ale cazului de utilizare CU12

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 12.01.	M	SIA RSISC va dispune de mecanism de gestiune a resurselor program (module, formulare electronice, opțiuni de meniu, butoane etc.) pentru configurarea fluxurilor de lucru și definirea regulilor de procesare a acestora pentru toate scenariile aferente proceselor de raportare a alertelor sau incidentelor de securitate cibernetică și a cazurilor de gestiune a incidentelor de securitate cibernetică.
CF 12.02.	M	Gestiunea fluxurilor de lucru trebuie să se poată realiza folosind interfața grafică a sistemului informatic în care utilizatorul lucrează în mod obișnuit.
CF 12.03.	M	Fluxurile de lucru vor fi definite prin specificarea stărilor în care poate trece un formular electronic și pașii de procesare (etapele sau tranzițiile de evoluție a fluxului de lucru și acțiunile ce pot fi făcute în starea concretă a formularului) realizați de utilizatori cu roluri specifice.
CF 12.04.	M	Un flux de lucru va fi implementat ca o colecție de activități prin care trece un formular electronic perfectat în cadrul proceselor de business ce se desfășoară secvențial.
CF 12.05.	M	Numărul de pași ce pot fi incluși într-un flux nu trebuie să fie limitat. În așa fel soluția informatică va fi adaptabilă modificărilor metodologiei de lucru cu documentele procesate în cadrul procedurilor de gestiune a cazurilor de gestiune a incidentelor de securitate cibernetică.
CF 12.06.	D	Un flux de lucru trebuie să poată avea asociat un coordonator (supervizor). Coordonatorul trebuie să poată primi mesajele de avertizare (notificări) generate de rularea fluxului respectiv. Utilizatorul care lansează un formular spre procesare pe un flux de lucru trebuie să poată specifica cine este supervizorul fluxului.
CF 12.07.	M	Furnizorul va configura fluxurile de procesare a formularelor electronice destinate perfectării tuturor evenimentelor de business aferente proceselor de raportare a alertelor de securitate cibernetică și cazurilor de gestiune a incidentelor de securitate cibernetică.
CF 12.08.	M	SIA RSISC va oferi un mecanism de configurare a formularelor electronice utilizate în interfața utilizator destinată raportării alertelor de securitate cibernetică și cazurile e gestiune a incidentelor de securitate.
CF 12.09.	M	SIA RSISC va oferi mecanisme de configurare a șabloanelor de documente (și rapoartelor) aferente proceselor de business implementate (șabloanele vor avea o structură bine definită care va permite modificarea aspectului și conținutului documentului extras).
CF 12.10.	D	Este binevenit ca șabloanele de documente și rapoarte să fie configurate prin intermediul unei platforme de configurare și generare a rapoartelor (*Exemplu: JasperReports,*

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 12.11.	M	Toate șabloanele de documente și rapoarte configurate prin intermediul CF 12.09 – CF 12.10 vor fi utilizate la generarea rapoartelor/documentelor prin intermediul CU05 și CU15.
CF 12.12.	M	Dezvoltatorul va configura la cererea Beneficiarului până la 20 șabloane de documente și 20 șabloane de rapoarte ce urmează a fi generate de SIA RSISC.

5.14. CU13: Gestionez metadate

Cerințele funcționale necesare gestiunii metadatelor SIA RSISC sunt incluse în tabelul 5.13.

Tabelul 5.13. Cerințele funcționale ale cazului de utilizare CU13

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 13.01.	M	SIA RSISC va furniza mecanism de gestiune a nomenclatoarelor, clasificatoarelor ce conțin totalitatea metadatelor destinate configurării sistemului informatic și gestiunii proceselor de raportare a alertelor de securitate cibernetică și a gestiunii incidentelor de securitate cibernetică.
CF 13.02.	M	Următoarele categorii de metadate urmează a fi utilizate în cadrul SIA RSISC: • **Clasificatoare Internaționale**, valorile cărora sunt standardizate și acceptate la nivel internațional (exemplu: Clasificatorul Internațional al Unităților de Măsură – SI, clasificatorul țărilor etc.); • **Clasificatoare oficiale naționale** (exemplu: Clasificatorului Unităților Administrativ-Teritoriale al Republicii Moldova etc.); • **Clasificatoare/nomenclatoare de interoperabilitate** (valorile cărora sunt utilizate pentru implementarea schimbului de date cu sisteme informatice terțe); • **Clasificatoare/nomenclatoare interne** (exemplu: variabile de sistem, parametri ai interfeței utilizator, parametri de configurare a sistemului informatic și proceselor implementate în cadrul sistemului informatic, roluri, metadate de trafic telecomunicațional, categorii de incidente, tipuri de impact, nivelul impactului, urgența soluționării incidentului, prioritățile de soluționare a incidentelor, nivele ierarhice de escaladare a incidentelor, surse de date etc.).
CF 13.03.	M	Furnizorul trebuie să implementeze mecanism destinat actualizării automate a metadatelor (dacă acestea există) necesare implementării schimbului de date cu sisteme informatice externe.
CF 13.04.	M	SIA RSISC va furniza mecanism de export și import a clasificatoarelor din interfața utilizator în format XML sau CSV. Drepturile de import și

Identificator	Obligativitate	Descrierea cerinței funcționale
		export vor fi atribuite utilizatorilor cu rolul de Administrator de Sistem.
CF 13.05.	M	Pentru clasificatoarele oficiale, internaționale și cele furnizate de sistemele informatice externe cu care efectuează schimbul reciproc de date vor fi limitate drepturile de modificare a valorilor prin intermediul facilităților SIA RSISC.
CF 13.06.	M	Pentru sistemul de clasificatoare/nomenclatoare și metadate interne, SIA RSISC va livra mecanism de definire și administrare dinamică a acestora (trebuie să fie posibilă adăugarea dinamică a categoriilor de nomenclatoare/clasificatoare și a conținutului acestora).
CF 13.07.	M	SIA RSISC va furniza funcționalitate de gestiune a valorilor textuale a clasificatoarelor/nomenclatoarelor altor categorii de metadate în 3 versiuni lingvistice: Română, Engleză și Rusă.
CF 13.08.	M	SIA RSISC va furniza funcționalitate de gestiune a etichetelor și mesajelor interfeței utilizator în 3 versiuni lingvistice: Română, Engleză și Rusă.
CF 13.09.	M	SIA RSISC nu va permite eliminare unei categorii de metadate dacă aceasta este utilizată cel puțin într-o înregistrare a bazei de date.
CF 13.10.	M	SIA RSISC va oferi mecanism de versionare a valorilor metadatelor și stabilite a intervalului de timp aferent validității valorilor metadator.

5.15. CU14: Configurez sistem informatic

Cerințele funcționale necesare implementării facilităților de configurare a SIA RSISC sunt incluse în tabelul 5.15.

Tabelul 5.14. Cerințele funcționale ale cazului de utilizare CU14

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 14.01.	M	SIA RSISC va dispune de facilități de configurare a strategiilor de jurnalizare a evenimentelor de business.
CF 14.02.	M	SIA RSISC va dispune de facilități de configurare a rapoartelor existente (*exemplu: ajustarea seturilor de date, reformatarea rapoartelor etc.*) modificând fișierele șabloanelor implementate sau platforme specializate (*exemplu: utilizarea generatoarelor de rapoarte*).
CF 14.03.	D	SIA RSISC trebuie să permită adăugarea și configurarea unor noi rapoarte.
CF 14.04.	M	SIA RSISC trebuie să dispună de facilități pentru a configura rapoartelor ce urmează a fi generate periodic automat. Generarea

Identificator	Obligativitate	Descrierea cerinței funcționale
		automată este specifică pentru rapoartele complexe care necesită un timp îndelungat de procesare a datelor. Rapoartele generate automat vor fi stocate în sistem (pentru a fi accesate de utilizatorii autorizați) sau trimise la adrese e-mail sau utilizatori concreți.
CF 14.05.	M	SIA RSISC va dispune de funcționalitate de definire a termenului de valabilitate a formularelor electronice aflate în statut „Proiect” după care pot fi suprimate automat.
CF 14.06.	M	SIA RSISC trebuie dispună de funcționalități destinate configurării job-urilor care trebuie să ruleze automat în funcție de parametrii de timp sau producerea anumitor evenimente de business. SIA RSISC trebuie să permită adăugarea și configurarea de job-uri noi precum și modificarea parametrilor de funcționare a job-urilor existente.
CF 14.07.	M	SIA RSISC va furniza funcționalitate de import manual a datelor primare în baza unor fișiere tipizate cu structură predefinită. Această funcționalitate urmează a fi utilizate pentru sincronizarea în regim manual cu sursele de date oficiale (în cazul inaccesibilității facilităților de interoperabilitate).
CF 14.08.	M	Datele potențial variabile ale SIA RSISC (parametrii de funcționare, valorile constantelor, căile de acces la fișiere/date, parametrii de integrare cu sisteme informatice externe, metadatele specifice etc.) trebuie să poată fi configurabile prin intermediul facilităților oferite de interfața utilizator fără a fi necesară compilarea și/sau desfășurarea repetată a codului sursă sau intervenții directe în conținutul bazei de date.

5.16. CU15: Monitoring operațional, diagnostică și soluționare probleme

Cerințele funcționale necesare implementării facilităților monitorizare, diagnostic și soluționare a problemelor tehnice apărute pe parcursul exploatării SIA RSISC sunt incluse în tabelul 5.15.

Tabelul 5.15. Cerințele funcționale ale cazului de utilizare CU15

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 15.01.	M	SIA RSISC va avea încorporat un serviciu Heartbeat care va comunica periodic statutul curent de funcționare a sistemului informatic.
CF 15.02.	M	SIA RSISC trebuie să conțină mecanisme de monitorizare a gradului de încărcare și statutul curent al tuturor componentelor cheie (Furnizorul trebuie să furnizeze soluție software de monitorizare a performanței SIA RSISC).
CF 15.03.	M	SIA RSISC trebuie să expedieze notificări rolurilor relevante în cazul când performanța componentelor sale este în degradare (*exemplu:*

Identificator	Obligativitate	Descrierea cerinței funcționale
		timpul de răspuns la unele interogări este mai mare decât cel așteptat).
CF 15.04.	M	Furnizorul trebuie să asigure facilități de administrare a SIA RSISC după cum urmează: • startarea componentelor SIA RSISC; • oprirea componentelor SIA RSISC; • restartarea componentelor SIA RSISC; • generarea copiilor de rezervă; • restabilirea datelor în baza copiilor de rezervă; • împrospătarea memoriei operaționale.
CF 15.05.	M	Mijloacele care implementează funcțiile de administrare a SIA RSISC pot fi implementate folosind comenzile și facilitățile software-ului de platformă, fără a fi nevoie de implementarea unei interfețe grafice dedicate.
CF 15.06.	M	Furnizorul trebuie să enumere mijloacele care trebuie utilizate pentru depanarea problemelor tehnice de funcționare a SIA RSISC.
CF 15.07.	M	SIA RSISC trebuie să fie în măsură să ofere un număr de rapoarte de management, de statistică și ad-hoc, astfel încât rolurile administrative să poată monitoriza activitatea și statutul sistemului.
CF 15.08.	I	Rapoartele gestionate prin intermediul CU15 sunt destinate funcțiilor de audit informatic și nu include rapoarte aferente evenimentelor de business specifice CU05.
CF 15.09.	M	Această raportare este necesară în cadrul întregului sistem, incluzând: • nomenclatoarele și clasificatoarele; • înregistrările bazei de date; • activitatea utilizatorului; • permisiunile de acces și securitate.
CF 15.10.	M	Rapoartele vor fi generate în baza următoarelor categorii de evenimente jurnalizate: • autentificare cu succes a utilizatorilor; • autentificare nereușită a utilizatorilor; • notificări expediate; • acțiuni asupra datelor (accesare, adăugare, modificare, eliminare).
CF 15.11.	M	SIA RSISC va permite extragerea agregată a rapoartelor sau detalierea acestora per utilizator concret, subdiviziune centrală sau teritorială a STISC sau a unor grupuri de utilizatori.

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 15.12.	M	Un utilizator care vizualizează un raport în cadrul sistemului, trebuie să-l poată exporta în format PDF sau într-un fișier extern redactabil (XLS/XLSX, CSV, DOC/DOCX).
CF 15.13.	M	Furnizorul va implementa până la 10 rapoarte predefinite ale auditului informatic solicitate de STISC. Rapoartele de audit care pot fi generate prin intermediul mijloacelor de sistem nu vor fi implementate în interfața utilizator a SIA RSISC.
CF 15.14.	D	Pentru extragerea rapoartelor și statisticilor de sistem relevante CU15 este binevenită utilizarea unei platforme dedicate configurării și generării rapoartelor.

5.17. CU16: Execut proceduri automate

Cerințele funcționale ale componentei funcționale destinate executării procedurilor automate sunt expuse în tabelul 5.16.

Tabelul 5.16. Cerințele funcționale ale cazului de utilizare CU16

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 16.01.	M	SIA RSISC va furniza funcționalitate de lansare a procedurilor automate destinate funcționării în bune condiții a sistemului informatic.
CF 16.02.	M	Momentul de timp și periodicitatea lansării spre execuție a procedurilor automate este configurat prin intermediul CF 14.05.
CF 16.03.	M	SIA RSISC va livra mecanism de generare automată a copiilor de rezervă (conform unor reguli prestabilite) în baza cărora să fie posibilă restabilirea funcționalității sistemului informatic în cazul producerii unor incidente de securitate.
CF 16.04.	M	SIA RSISC va livra mecanism de arhivare a datelor vechi și inutile proceselor de business curente ale STISC și eliminare a acestora de pe platforma de producție.
CF 16.05.	M	SIA RSISC va declanșa în mod automat procedurile de schimb reciproc de date cu sisteme informatice externe definite prin intermediul CU17.
CF 16.06.	M	SIA RSISC va șterge automat formularele electronice aflate în statut „Proiect” care au depășit termenul limită de aflare în acest statut configurat prin intermediul CU14.
CF 16.07.	M	SIA RSISC va fi capabil să efectueze periodic și planificat (în orele de solicitare minimă a SIA RSISC) calculele preliminare ale indicatorilor necesari generării în timp util a rapoartelor statistice complexe.

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 16.08.	M	SIA RSISC identifica automat și expedia notificările ce trebuie expediate utilizatorilor autorizați ca urmare a unor evenimente de business (*exemplu: întârzieri în executarea sarcinilor*).
CF 16.09.	M	SIA RSISC trebuie să furnizeze interfață de vizualizare a statutului curent al procedurile executate automat în curs de procesare.
CF 16.10.	M	SIA RSISC trebuie să furnizeze facilități de gestiune a procedurilor automate planificate: • startarea manuală a procedurii automate; • oprirea din execuție a procedurii automate; • redemararea procedurii automate oprite anterior; • anularea executării procedurii automate.
CF 16.11.	M	SIA RSISC va publica periodic în cadrul interfeței publice și Partalului Datelor Deschise rapoarte și KPI cu caracter public produse în cadrul proceselor de business implementate.
CF 16.12.	M	Toate evenimente aferente funcționării procedurilor automate definite prin intermediul cerințelor funcționale CF 16.03 - CF 16.11 trebuie jurnalizate.
CF 16.13.	M	SIA RSISC trebuie să furnizeze facilități de corelare, in baza datelor acumulate, precum si cele disponibile public (ipReputation,DomainReputation,BotNets,etc) precum si stabilirea gradului de risc in baza mai multor criterii.
CF 16.14.	M	SIA RSISC trebuie să furnizeze facilități de identificare si ridicarea gradului de risc in baza clasificatoarelor precum si corelarea acestora cu MITRE ATT&CK®.

5.18. CU17: Schimb de date cu sisteme externe

Cerințele funcționale ale procedurilor de schimb de date între SIA RSISC și sistemele informatice externe sunt expuse în tabelul 5.17.

Tabelul 5.17. Cerințele funcționale ale cazului de utilizare CU17

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 17.01.	M	SIA RSISC trebuie să fie dezvoltat în baza unei arhitecturi capabile să implementeze facilități de interoperabilitate cu sisteme informatice externe.
CF 17.02.	M	SIA RSISC va efectua schimb de date cu sistemele informatice externe prin intermediul API-urilor expuse de acestea (cazul sistemelor informatice neguvernamentale) și platforma de interoperabilitate a MConnect (pentru cazul sistemelor informatice ale AP).

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 17.03.	M	Interacțiunea SIA RSISC cu sistemele informatice interne ale STISC în cazul în care serviciile de furnizate/recepționate a datelor nu sunt solicitate de sisteme informatice ale altor AP din Republica Moldova vor fi implementate prin intermediul microserviciilor.
CF 17.04.	M	SIA RSISC trebuie să fie capabil a se integra cu următoarele servicii de guvernamentale: • MPass - pentru autentificare și controlul accesului utilizatorilor; • MSign - pentru aplicarea semnăturii electronice în cadrul proceselor de business ale SIA RSISC; • MLog - pentru jurnalizarea evenimentelor de business critice; • MNotify - pentru notificarea utilizatorilor autorizați; • MPower - pentru verificarea împuternicirilor de reprezentare a utilizatorilor necesare autorizării acțiunilor acestora; • PDGD - pentru publicarea seturilor publice de date produse în cadrul fluxurilor de lucru ale SIA RSISC.
CF 17.05.	M	SIA RSISC se va integra prin intermediul platformei guvernamentale MConnect cu următoarele sisteme informatice pentru recepționarea datelor aferente alertelor și incidentelor de securitate: • Sisteme informatice ale AP - care vor expedia în mod automat alerte de securitate cibernetică în cazul producerii unor evenimente considerate cu risc major asupra securității informației; • Soluțiilor software de monitorizare a infrastructurii TIC a AP - care vor expedia în mod automat alerte de securitate cibernetică în cazul producerii unor evenimente considerate cu risc major asupra securității informației;; • Soluții informatice destinate gestiunii incidentelor de securitate cibernetică - pentru preluarea automatizată a datelor aferente alertelor și e a incidentelor de securitate cibernetică.
CF 17.06.	M	La recepționarea datelor de la soluții informatice ale AP utilizate pentru gestiunea incidentelor de securitate cibernetică SIA RSISC va crea automat evenimentele de raportare a alertelor și incidentelor de securitate cibernetică și va crea în mod automat cazurile de gestiune a incidentelor cu completarea formularelor relevante în baza datelor recepționate.
CF 17.07.	M	SIA RSISC se va integra cu Google Analytics în scopul expedierii datelor statistice privind exploatarea Interfeței Publice.

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 17.08.	M	SIA RSISC se va integra cu rețele de socializare (LinkedIn, Facebook și Twitter) în scopul publicării informației de conținut a interfeței publice SIA RSISC.
CF 17.09.	M	Toate evenimentele de schimb de date cu sisteme informatice externe prin intermediul procedurilor descrise de cerințele funcționale CF 17.04 - CF 17.06 vor fi jurnalizate prin intermediul mecanismului de jurnalizare intern a SIA RSISC și serviciului de platformă MLog.
CF 17.10.	M	Sistemul va permite importarea automatizata(prin intermediul adaptoarelor), din diferite surse de date(csv,xls,sql), prin diferite protocoale(soap,rest,syslog) cu posibilitatea ajustarii parametrilor pentru fiecare sursa de date intr-un mod dinamic si individual.
CF 17.11.	M	Sistemul va include adaptoare la cheie pentru urmatoarele surse de date(Fortinet,ShadaowServer,Barracuda Spam, si WAF, Nginx, WangGuard)
CF 17.12.	M	Sistemul va permite importarea, periodica, din diferite surse publice, IpReputation, botnet, etc.

5.19. CU18: Jurnalizez evenimente

Cerințele funcționale ale componentei de jurnalizare a evenimentelor de business produse pe parcursul exploatării SIA RSISC sunt expuse în tabelul 5.18.

Tabelul 5.18. Cerințele funcționale ale cazului de utilizare CU18

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 18.01.	M	SIA RSISC va conține mecanism de jurnalizare a tuturor evenimentelor de business aferente utilizării sale.
CF 18.02.	M	Administratorul de Sistem va putea configura strategiile de jurnalizare aferente evenimentelor de business produse de SIA RSISC prin intermediul cazului de utilizare CU12 și CU15 (inclusiv care evenimente vor fi jurnalizate doar prin intermediul mecanismelor interne și care suplimentar prin intermediul serviciului guvernamental MLog).
CF 18.03.	M	SIA RSISC va furniza Administratorilor de Sistem mecanism de căutare, filtrare și vizualizare a detaliilor evenimentelor jurnalizate.
CF 18.04.	M	Vor fi jurnalizate următoarele categorii de evenimente: • autentificare utilizator; • deconectare utilizator; • adăugare/modificare/eliminare/accesare înregistrare; • evenimente de business specifice fluxurilor de lucru ale SIA RSISC;

Identificator	Obligativitate	Descrierea cerinței funcționale
		• schimbul de date cu sisteme informatice externe; • generare/accesare raport; • interogări la baza de date; • alte evenimente de business specifice.
CF 18.05.	M	Evenimentele jurnalizate vor salva următoarele categorii de date (în funcție de natura evenimentului jurnalizat: • identificatorul utilizatorului care a generat evenimentul; • categoria evenimentului jurnalizat; • momentul jurnalizării evenimentului; • modulul SIA RSISC care a generat evenimentul de business; • înregistrarea afectată de evenimentul de business; • acțiunea efectuată de utilizator (exemplu: detaliile modificării, datele adăugate etc.).
CF 18.06.	M	SIA RSISC va jurnaliza exhaustiv toate evenimentele de business produse.
CF 18.07.	M	SIA RSISC va jurnaliza în paralel evenimentele de business critice prin intermediul serviciul guvernamental de jurnalizare MLog.
CF 18.08.	M	SIA RSISC va furniza funcționalitate de definire a evenimentelor de business critice care urmează a fi jurnalizate în paralel prin intermediul serviciului de platformă MLog.

5.20. CU19: Expediez notificări

Cerințele funcționale a componentei de notificare a actorilor SIA RSISC sunt expuse în tabelul 5.19.

Tabelul 5.19. Cerințele funcționale ale cazului de utilizare CU19

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 19.01.	M	În funcție de utilizator (datele de configurare a profilului acestuia), funcționalitatea de notificare a utilizatorilor va aplica una din 3 strategii de notificare: • notificare prin E-mail; • notificare în Dashboard-ul utilizatorului autorizat; • ambele categorii de mai sus.
CF 19.02.	M	SIA RSISC va notifica utilizatorii relevanți la producerea unui eveniment de business specific activității lor.
CF 19.03.	M	Notificarea va conține referință de accesare a înregistrării/formularului electronic relevant evenimentului de business care a generat notificarea (valabil pentru notificările stocate în Dashboard-ul utilizatorului).

Identificator	Obligativitate	Descrierea cerinței funcționale
CF 19.04.	M	Utilizatorii autorizați (indiferent de rolurile de care dispun) vor putea să-și configureze preferințele mijloacelor de notificare.
CF 19.05.	M	Toate categoriile de utilizatori autorizați vor primi notificări privind evenimentele de business aferente obligațiilor sale de serviciu (*exemplu: necesitate procesare alertă sau incident de securitate* cibernetică *raportate, necesitatea escaladării incidentului de securitate* cibernetică*, necesitate aprobare proiecte de formulare electronice, întârziere în executarea atribuțiilor de serviciu etc.*).
CF 19.06.	M	Administratorul de Sistem va dispune de funcționalitate de perfectare și expediere notificări utilizatorilor expliciți sau grupurilor de utilizatori.
CF 19.07.	M	SIA RSISC va notifica Administratorul de Sistem asupra oricăror probleme ce afectează performanța și disponibilitatea sistemului informatic.
CF 19.08.	M	SIA RSISC va notifica utilizatorii care recepționează notificările prin mijloace externe prin intermediul serviciului guvernamental de notificare MNotify.

6. Cerințele nefuncționale ale sistemului informatic

6.1. Convenții la formularea cerințelor non-funcționale

Cerințele non-funcționale stabilite în acest document sunt marcate utilizând următoarea convenție:

- toate cerințele sunt indexate cu două valori X.Y, unde X reprezintă categoria cerinței descrise în tabelul 6.1 iar Y este identificatorul unic al cerinței în categoria din care face parte.
- pentru fiecare cerință este menționată obligativitate: M – cerință obligatorie a fi implementată (de la noțiunea engleză Mandatory), D – cerință dorită a fi implementată, opțională (de la noțiunea engleză Desirable) și I – cerință cu caracter informativ.

Tabelul 6.1. Categoriile de cerințe ale caietului de sarcini

Valoare	Semnificație	Interpretare
DEL	Cerință față de livrabil	Cerința se referă la livrabilele ce urmează a fi prezentate de dezvoltatorul SIA RSISC.
DOC	Cerință de documentare	Cerința se referă la documentația aferentă SIA RSISC ce urmează a fi livrată de Furnizor.
GEN	Cerință generală	Cerințe generale de implementare a SIA RSISC.
GMS	Cerință de garanție, mentenanță și suport post-implementare	Cerința se referă la caracteristicile serviciilor de menținere operațională și dezvoltare post-implementare ale SIA RSISC, solicitate în cadrul achiziției.
INT	Cerință de interoperabilitate	Cerința se referă la cadrul de interoperabilitate al SIA RSISC.
LIPR	Cerințe licențiere și proprietate intelectuală	Cerințele se referă drepturile de proprietate intelectuală aferente SIA RSISC și componentelor soft necesare funcționării SIA RSISC.
PER	Cerință de performanță	Cerința se referă la performanța de funcționare a SIA RSISC.
SEC	Cerință de securitate	Cerința se referă la aspectele de asigurare a securității informației cărora trebuie să corespundă SIA RSISC.
SHC	Cerință de platformă	Cerințe aferente platformei software, hardware și canalelor de comunicație necesare funcționării SIA RSISC.
SR	Cerință de scalabilitate	Cerința se referă la proprietățile de scalabilitate a SIA RSISC la sporirea numărului utilizatorilor, tranzacțiilor sau volumului de date procesat.

Propunerea prezentată de Furnizor trebuie să corespundă în mod obligatoriu tuturor cerințelor indicate ca fiind obligatorii. Furnizorii vor obține un avantaj competitiv pentru fiecare cerință opțională asumată de Furnizor.

Cerințele informative sunt destinate să ofere mai multă informație, pentru o înțelegere mai bună a contextului altor cerințe.

6.2. Cerințe generale ale sistemului informatic

Cerințele generale de sistem sunt definite de politicile și strategiile elaborate și adoptate în Republica Moldova. E important de menționat că aceste acte sunt bazate pe bunele practici din industrie și cuprind multe măsuri organizatorice dar și o serie de măsuri tehnice. Cerințele generale de sistem specifice pentru SIA RSISC sunt expuse în tabelul 6.2.

Tabelul 6.2. Cerințele generale înaintate sistemului informatic

ID	Obligativitate	Descrierea cerinței
GEN 001	M	SIA RSISC trebuie să fie dezvoltat în baza metodologiei Agile.
GEN 002	M	Toate interfețele utilizator și conținutul bazei de date vor fi perfectate în limba română cu utilizarea diacriticelor românești.
GEN 003	M	Interfața utilizator al interfeței publice a SIA RSISC și valorile metadatelor textuale (clasificatoare, nomenclatoare etc.) trebuie să fie accesibile în limbile română, engleză și rusă.
GEN 004	M	Datele bazei de date a SIA RSISC urmează a fi stocate în format unicode (*exemplu: utilizând UTF-8*).
GEN 005	M	Elementele interfeței utilizator trebuie să se conformeze la Nivel A cu cerințele *Web Content Accessibility Guidelines (WCAG) 2.0.*
GEN 006	M	Interfața utilizatori pentru utilizatorii autorizați ai SIA RSISC va fi optimizată rezoluției 1360x768 cu evitarea apariției barelor de defilare pentru interfețele utilizator prezentate de soluția informatică.
GEN 007	M	SIA RSISC va furniza interfață publică adaptabilă (va livra interfață responsivă) în funcție de dispozitivul utilizat de acesta (*notebook, netbook, calculator desktop, smartphone, tabletă etc.*)
GEN 008	M	Interfața Publică va genera paginile de conținut ținând cont de cele mai bune practici de optimizare SEO.
GEN 009	M	Procedurile de căutare a datelor vor fi implementate prin intermediul unor căutări simple (specificarea unor șiruri de căutare) sau a unor căutări de complexitate mai ridicată, prin intermediul cărora se poate realiza o filtrare mai exact a informației (formulare QBE). Indiferent de natura informației căutate utilizatorul va utiliza aceeași metodă de interogare și regăsire a datelor pentru orișicare compartiment al interfeței utilizator a produsului informatic.
GEN 010	M	Interfața utilizator a sistemului informatic trebuie să asigure căutarea, filtrarea și vizualizarea înregistrărilor ce corespund criteriului de căutare prezentate utilizatorilor în funcție de drepturile lor de acces.
GEN 011	M	Conținutul oricărui tabel cu rezultate ale căutării trebuie să poată fi exportat fie în format XLS, CSV și PDF.
GEN 012	M	Arhitectura SIA RSISC va fi concepută integrat, dezvoltată cu aplicarea celor mai bune practici în domeniu (exemplu: principii de arhitectură și arhitecturi de referință aliniate TOGAF 9.1).

ID	Obligativitate	Descrierea cerinței
GEN 013	M	Arhitectura completă SIA RSISC va fi coordonată în prealabil cu STISC.
GEN 014	M	Arhitectura SIA RSISC trebuie să asigure utilizarea rațională și balansată a resurselor de procesare.
GEN 015	M	SIA RSISC va fi dezvoltat în baza unei arhitecturi SOA multi-nivel (cel puțin 3 nivele arhitecturale (*exemplu: nivelul de prezentare, nivelul logicii de business și nivelul de date*).
GEN 016	M	SIA RSISC trebuie să ofere interfețe web de interacțiune cu sisteme informatice ale STISC și ale altor autorități publice ale Republicii Moldova prin intermediul microserviciilor și MCloud.
GEN 017	M	SIA RSISC va fi optimizat în transferul minim de date între calculatorul client și server, punându-se accent pe evitarea la maximum a cererilor inutile, implementarea AJAX cu JSON, solicitării la minim a resurselor server necesare procedurilor de autentificare, autorizare și jurnalizare.
GEN 018	M	Informația potențial variabilă (*exemplu: diferiți parametri, căi de stocare a datelor, cai de conexiune cu servicii externe, clasificatoare etc.*) va fi configurabilă și NU va necesita recompilarea soluției sau intervenții directe în baza de date.

6.3. Cerințele de performanță a sistemului informatic

Cerințele de performanță specifice SIA RSISC care corespund necesităților și așteptărilor STISC sunt expuse în tabelul 6.3.

Tabelul 6.3. Cerințele de performanță înaintate sistemului informatic

ID	Obligativitate	Descrierea cerinței
PER 001	M	Timpul mediu de răspuns al serverului nu va depăși 3 secunde la încărcătura nominală a sistemului.
PER 002	M	SIA RSISC trebuie sa fie capabil să permită activitatea a cel puțin 200 utilizatori autorizați.
PER 003	M	SIA RSISC va permite activitatea concurentă a cel puțin 150 utilizatori autorizați și deservirea concomitentă a cel puțin 100 interogări fără a afecta performanța de funcționare.
PER 004	M	Interfața publică a SIA RSISC trebuie sa fie capabilă sa deservească accesul anual a peste 500000 utilizatori anonimi.
PER 005	M	Interfața publică a SIA RSISC trebuie să fie capabilă să deservească cel puțin 500 utilizatori anonimi concurenți și 300 interogări paralele.
PER 006	M	SIA RSISC trebuie să fie capabil să recepționeze, proceseze și stocheze anual datele a peste 100 000 000 alerte și peste și peste 10 000 incidente de securitate.

ID	Obligativitate	Descrierea cerinței
PER 007	M	Anterior livrării SIA RSISC vor fi efectuate totalitatea testelor de performanță și securitate.
PER 008	M	Testarea performanței va include minim doua componente: testarea încărcăturii sistemului (*load testing*) și testarea comportamentului sistemului la solicitări mari (*stress testing*).

Pe parcursul utilizării SIA RSISC, este posibil ca numărul de tranzacții procesate și utilizatorilor concurenți să crească sau să scadă simțitor de la o perioadă la alta. Pentru a avea o utilizare rațională a resurselor de procesare, sistemul informatic trebuie să fie ușor scalabil (în sus și în jos). Tabelul 6.4 conține cerințe privind caracteristicile de scalabilitate aferente SIA RSISC.

Tabelul 6.4. Cerințele de scalabilitate a sistemului informatic

ID	Obligativitate	Descrierea cerinței
SR 001	M	SIA RSISC va permite creșterea capacității de procesare fără a întrerupe funcționarea sa. În acest scop, sistemul va suporta extinderea pe orizontală a capacității de procesare (exemplu: adăugarea de noi noduri server și efectuare balansare a încărcării).
SR 002	D	SIA RSISC va putea fi configurat pentru scalare automată la nivelul componentelor cheie (lag sensitive). Scalarea sistemului se va face atât în sus, cât și în jos.
SR 003	M	SIA RSISC trebuie să dețină posibilitatea de a deservi un număr nelimitat de tranzacții, cu condiția alocării corespunzătoare a resurselor de procesare și stocare date. Resursele vor fi alocate pe orizontală (alocare noi servere, fără creșterea performanței pe serverele existente).

6.4. Cerințe software, hardware și canale de comunicație

Tabelul 6.5 conține cerințele de asigurare software, hardware și tehnologie de comunicație destinate implementării SIA RSISC.

Tabelul 6.5. Cerințele de asigurare software, hardware și comunicație

ID	Obligativitate	Descrierea cerinței
SHC 001	M	SIA RSISC trebuie să poată fi instalat atât pe servere dedicate, cât și pe soluții de virtualizare (SIA RSISC trebuie să fie conform cerințelor de desfășurare a sistemelor informatice pe platforma guvernamentală tehnologică comună MCloud).
SHC 002	M	Este necesară demonstrarea capacității de virtualizare prin livrarea către STISC a unei imagini a sistemului ce poate fi încărcată și devine funcțională cu configurări minime pe una din soluțiile de virtualizare existente pe piață.

ID	Obligativitate	Descrierea cerinței
SHC 003	M	Furnizorul va demonstra posibilitatea instalării și operării SIA RSISC în infrastructura MCloud.
SHC 004	M	SIA RSISC trebuie să poată fi accesat pe canale de comunicații de cel puțin 512Kbps.
SHC 005	M	SIA RSISC trebuie să fie dezvoltat în baza următoarelor tehnologii: • Microsoft Windows Server 2019 (în calitate de sistem de operare); • IIS 10 (în calitate de server WEB); • Microsoft SQL Server 2019 Standard Edition (în calitate de SGBD); • Elastic Search (în calitate de motor de căutare indexată a datelor și soluție de stocare/gestiune a alertelor); • ASP.NET Core (în calitate de framework de dezvoltare); • Entity Framework (în calitate de soluție ORM); • Microsoft SQL Server Report Services (în calitate de generator de rapoarte); • Angular JS, React JS sau Knockout JS (în calitate de framework destinat implementării interfeței utilizator); • Nginx (în calitate de soluție pentru balansor)
SHC 006	M	Furnizorul va indica explicit în ofertă platforma software în baza căreia urmează a fi dezvoltat SIA RSISC și platforma software necesară exploatării acestuia.
SHC 007	M	Tehnologiile propuse de Furnizor trebuie să fie accesibile pentru cel puțin 3 companii specializate în dezvoltarea soluțiilor software care activează pe piața locală a Republicii Moldova
SHC 008	M	SIA RSISC va utiliza standarde deschise pentru formate și protocoale de comunicare.
SHC 009	M	Serviciile expuse către public de SIA RSISC vor fi tehnologic neutre (Sistem de Operare, explorator Internet etc.).
SHC 010	M	Produsul program generic recomandat pentru operarea și interacțiunea cu SIA RSISC reprezintă exploratorul WEB.
SHC 011	M	Sistemul va fi compatibil cu cel puțin 2 cele mai recente versiuni ale următoarelor exploratoare Web: *MS Internet Explorer/MS Edge, Mozilla Firefox, Google Chrome*, *Safari* și *Opera*.
SHC 012	M	Compatibilitatea cu exploratorul WEB *MS Internet Explorer/MS Edge* este obligatorie.
SHC 013	D	SIA RSISC va încorpora un serviciu Heart-beat care va comunica periodic starea normală de lucru a sistemului.

ID	Obligativitate	Descrierea cerinței
SHC 014	M	Sistemul va include mijloace configurabile de jurnalizare tehnică (logging).
SHC 015	M	Sistemul trebuie să fie capabil să producă cel puțin următoarele nivele de jurnalizare tehnică: *info*; *warning*; *critic*; *error*.
SHC 016	M	Dezvoltatorul va enumera mijloacele ce vor fi utilizate la depanarea tehnică a sistemului.
SHC 017	M	Furnizorul va pregăti mijloace ce facilitează funcțiile de administrare a sistemului: • startarea componentelor sistemului; • stoparea componentelor sistemului; • restartarea componentelor sistemului, • crearea copiei de rezervă a bazei de date, • restaurarea datelor de pe copia de rezervă indicată, • împrospătarea memoriei operaționale a sistemului.
SHC 018	M	SIA RSISC va opera în rețele TCP/IP și în special HTTPS.
SHC 019	M	SIA RSISC va utiliza XML în calitate de mijloc principal pentru integrarea datelor.
SHC 020	M	Furnizorul va sugera alte servicii de rețea și utilitare necesare pentru operarea sistemului.

6.5. Cerințe de licențiere și proprietate intelectuală

STISC va deține toate drepturile necesare pentru utilizarea pe termen nelimitat a SIA RSISC și a tuturor componentelor soft necesare bunei funcționări a SIA RSISC. Tabelul 6.6 conține specificarea cerințelor aferente licențierii și drepturilor de proprietate intelectuală aferente SIA RSISC și componentelor soft necesare funcționării sistemului informatic.

Tabelul 6.6. Cerințele de licențiere și proprietate intelectuală

ID	Obligativitate	Cerință
LIC 001	I	STISC va asigură următoarele medii de operare pentru SIA RSISC: • Mediul de producție; • Mediul de testare/instruire; • Mediul de dezvoltare.
LIC 002	M	Furnizorul va include în oferta sa financiară licențele pentru toate produsele soft de tip COTS (diferite de cele menționate în SHC 005), necesare implementării și exploatării SIA RSISC în cele trei medii puse la dispoziție de STISC. Aici sunt incluse următoarele: sisteme de operare, sisteme de gestiune baze de date, biblioteci software, utilitare și alt soft de sistem.

LIC 003	M	Cantitatea licențelor oferite trebuie să permită accesarea și utilizarea SIA RSISC (în orice mediu în care funcționează) de cel puțin 200 de utilizatori autorizați nominali, precum și nelimitat de utilizatori anonimi și sisteme externe. Nu vor exista restricții cu privire la numărul de documente, tranzacții sau mod de accesare a SIA RSISC (*exemplu: limitări la accesare concurentă*).
LIC 004	M	Cantitatea licențelor oferite trebuie să permită accesarea API-urilor expuse de SIA RSISC de orice aplicație și sistem extern.
LIC 005	M	Furnizorul va transmite către STISC toate drepturile asupra dezvoltărilor, ajustărilor, configurărilor și personalizărilor efectuate pentru implementarea SIA RSISC conform cerințelor. Acestea pot fi aferente produselor soft terțe licențiate sau pot fi componente elaborate în cadrul proiectului.
LIC 006	M	Orice date stocate în cadrul bazelor de date aferente SIA RSISC sunt proprietatea STISC. Accesul la aceste date pe întreaga perioada de contractare a furnizorului, cât și după, este subiect al cerințelor și clauzelor de confidențialitate a informației.
LIC 007	M	Furnizorul va prezenta modelul său de licențiere propus pentru SIA RSISC care trebuie să corespundă cerințelor LIPR 001 – LIPR 006. Furnizorul va descrie modelul de licențiere propus, argumentând de ce acesta este cel optim pentru STISC. Va prezenta o analiză comparativă cu alte modele de licențiere oferite de obicei pentru soluția ofertată.

6.6. Cerințe de interoperabilitate

Interoperabilitatea SIA RSISC reprezintă caracteristica sistemului informatic de a comunica cu alte aplicații informatice. Arhitectura de sistem stabilește interfețele ce trebuie să existe intre SIA RSISC și alte sisteme informatice ale STISC sau ale altor autorități publice ale Republica Moldova. În tabelul 6.7 sunt definite cerințele privind caracteristicile de interoperabilitate ale SIA RSISC solicitate de STISC.

Tabelul 6.7. Cerințele cadrului de interoperabilitate a sistemului informatic

ID	Obligativitate	Cerință
INT 001	I	Toate interfețele expuse de SIA RSISC trebuie să fie bazate pe standarde deschise. Toate fluxurile de mesaje între SIA RSISC și entități externe se vor realiza cu utilizarea standardelor deschise.
INT 002	M	SIA RSISC va deține capabilități de implementare a interfețelor prin intermediul MConnect.
INT 003	M	SIA RSISC va deține capabilități de integrare cu sistemele informatice ale AP din Republica Moldova în vederea recepționării automate a datelor referitoare la alertele înregistrate pe parcursul exploatării lor.
INT 004	M	SIA RSISC va deține capabilități de integrare cu sistemele informatice ale AP din Republica Moldova destinate gestiunii incidentelor de securitate

		în vederea recepționării datelor referitoare la incidentele de securitate gestionate în cadrul AP.
INT 005	M	SIA RSISC se va integra cu platforma de interoperabilitate MConnect pentru a consuma date din sisteme informatice externe (exemplu: extragerea datelor din registre de stat).
INT 006	M	SIA RSISC se va integra cu serviciul guvernamental MPass pentru implementarea mecanismului de autentificare a utilizatorilor prin intermediul semnăturii electronice sau mobile.
INT 007	M	SIA RSISC se va integra cu serviciul guvernamental MSign pentru implementarea infrastructurii de utilizare a semnăturii electronice.
INT 008	M	SIA RSISC se va integra cu serviciul guvernamental MLog pentru jurnalizarea evenimentelor de business critice.
INT 009	M	SIA RSISC se va integra cu serviciul guvernamental MNotify pentru implementarea mecanismului de notificare a utilizatorilor.
INT 010	M	SIA RSISC se va integra cu serviciul guvernamental MPower pentru verificarea împuternicirilor utilizatorilor autoriza de a efectua acțiuni specifice în cadrul interfeței utilizator.
INT 011	M	SIA RSISC se va integra cu serviciul guvernamental Portalul Datelor Deschise (https://date.gov.md) pentru publicarea datelor deschise produse în cadrul fluxurilor de lucru implementate.
INT 012	M	Toate interfețele furnizate de SIA RSISC vor interacționa cu aplicațiile externe instantaneu sau programat prin intermediul unor job-uri specializate.
INT 013	M	Interfața publică a SIA RSISC se va integra cu Google Analytics și cele mai importante rețele de socializare (LinkedIn, Facebook și Twitter) în vederea expedierii statisticilor de vizitare a conținutului public și publicării conținutului public pe rețelele de socializare.
INT 014	D	SIA RSISC va deține capabilități de definire a noilor interfețe standard pentru accesarea tuturor funcțiilor de business cheie ale sistemului (*exemplu: generare documente, generare tranzacții, accesare informații despre entitățile de business stocate în cadrul SIA RSISC*).
INT 015	D	Interfețele respective trebuie să permită gestiunea entităților de business cu aplicarea tuturor regulilor de business relevante și cu utilizarea tuturor proprietăților aferente entităților de business.
INT 016	D	SIA RSISC va deține capabilități de definire a noilor interfețe pentru accesarea sistemelor externe cu utilizarea standardelor deschise. Aceste interfețe vor fi accesibile pentru apelare în cadrul funcțiilor sistemului, la implementarea funcționalităților SIA RSISC.
INT 017	M	SIA RSISC va deține interfețe standard pentru exportul datelor în cadrul instrumentelor de tipul Data Warehouse.

6.7. Cerințe de migrare și populare a datelor

Tabelul 6.6 conține cerințele de migrare și populare a datelor în SIA RSISC. Trebuie menționat faptul că acceptanța sistemului informatic va fi realizată după popularea bazei de date cu seturile de date furnizate de STISC.

Tabelul 6.8. Cerințele de migrare și populare a datelor

ID	Obligativitate	Descrierea cerinței de migrare
MIG 001.	M	STISC va pregăti și livra seturile de date și metadate necesare populării cu date primare a SIA RSISC. Formatul datelor migrate va fi convenit de comun acord cu Dezvoltatorul.
MIG 002.	M	Dezvoltatorul va trebuie să convertească valori specifice ale metadatelor aferente seturilor de date externe conform sistemului de metadate statistice al STISC.
MIG 003.	M	Dezvoltatorul va include în oferta tehnică abordarea sa privind procedura de implementare a procedurii de migrare și populare inițială a bazei de date.
MIG 004.	M	Dezvoltatorul trebuie să furnizeze mecanism care va asigura popularea automatizată a bazei de date a SIA RSISC cu metadatele relevante (nomenclatoare, clasificatoare, variabile de diferită natură etc.) și seturile de date primare furnizate de STISC în vederea consolidării stocului de date inițial al SIA RSISC.
MIG 005.	M	Pe parcursul implementării procedurii de migrare și populare a datelor Furnizorul este responsabil pentru: • definirea metodologiei utilizate în procesul de migrare și populare a datelor; • elaborarea planurilor detaliate de migrare și populare a datelor; • furnizarea mecanismelor software destinate migrării și populării datelor; • definirea cerințelor de calitate către seturile de date destinate migrării/populării și procesarea lor prin intermediul mecanismelor de migrare și populare elaborate; • maparea valorii metadatelor recepționate din surse externe (în cazul divergențelor); • definirea criteriilor de reconciliere a datelor migrate și populate; • participarea în procesul de curățare și îmbogățire a datelor; • verificarea și validarea calității seturilor de date ce urmează a fi migrate și populare; • popularea bazei de date a SIA RSISC în baza seturilor de date furnizate de STISC; • identificarea și soluționarea excepțiilor/erorilor pe parcursul procesului de migrare și populare a datelor.

ID	Obligativitate	Descrierea cerinței de migrare
MIG 006.	M	Furnizorul trebuie să propună către STISC metodologia de migrare și populare a datelor. Metodologia de migrare și populare a datelor trebuie să conțină următoarele elemente: • metodologia de pregătire a datelor ce urmează a fi migrate și populate; • metodologia de mapare a datelor migrate și populate; • metodologie de curățare și îmbogățire a datelor migrate/populate și asigurare a calității lor; • metodologia completării valorii datelor solicitate obligatoriu de SIA RSISC dar care lipsesc în seturile de date furnizate; • procedura automatizată de migrare și populare a datelor; • principiile de reconciliere a datelor migrate și populate; • planul de recuperare în caz de eșec (pentru fiecare etapă a procesului de migrare și populare a datelor); • planul de livrare a mecanismului de migrare și populare a datelor.
MIG 007.	M	Furnizorul trebuie să pregătească și livreze planul detailat al migrării și populării inițiale cu date a SIA RSISC (strategia de migrare și conversie a datelor). Acest plan trebuie să fie aliniat planului de implementare a SIA RSISC.
MIG 008.	M	Furnizorul trebuie să livreze către STISC soluție software destinată automatizării proceselor de migrare și populare inițială cu date a SIA RSISC.
MIG 009.	M	Toate activitățile de migrare și populare inițială a SIA RSISC cu date trebuie să fie efectuate în mediul de operare controlat de STISC. Datele nu vor părăsi niciodată infrastructura TIC a STISC.
MIG 010.	M	În procesul migrării Furnizorul se va confirma politicii de securitate a STISC.
MIG 011.	M	Furnizorul va demonstra corectitudinea instrumentarului de migrare și populare inițială cu date a SIA RSISC specialiștilor STISC (un act de acceptanță a migrării și populării inițiale cu date a SIA RSISC urmează a fi semnat între Furnizor și STISC).

6.8. Cerințe de asigurare a securității informaționale

SIA RSISC trebuie să permită un control adecvat asupra riscurilor de securitate a informației aferente utilizării. Măsurile de securitate implementate trebuie să fie aliniate la politicile de securitate aprobate în cadrul STISC și să asigure prevenirea, detectarea și reacționarea adecvată la incidentele de securitate cibernetică.

SIA RSISC trebuie să implementeze o abordare de tipul „Multi-layered security” (securitate de mai multe nivele) la nivelul sistemului și să dețină capacitatea de a se integra în modelul instituțional al STISC pentru managementul securității informației (bazat pe familia de standarde ISO 27000).

În acest compartiment sunt stabilite cerințele privind caracteristicile de securitate aferente SIA RSISC solicitate de STISC.

Tabelul 6.9. Cerințele pentru arhitectura de securitate

ID	Obligativitate	Cerință
SEC 001	M	Arhitectura SIA RSISC trebuie să fie concepută prin aplicarea unei abordări de tipul *„Security by design”* (securitate prin design).
SEC 002	M	Arhitectura de securitate a SIA RSISC trebuie să fie documentată la nivel tehnic. Documentația va conține: • descrierea modelului de securitate implementat; • componentele prezente; • rolul fiecărei componente din punct de vedere al securității
SEC 003	M	Documentația va conține, de asemenea, specificațiile privind plasarea la nivel de rețea a componentelor SIA RSISC și recomandările Furnizorului privind regulile de acces la nivel de rețea necesar a fi setate de STISC în vederea accesului securizat la toate componentele sistemului (*exemplu: matrice de comunicare între servicii*).
SEC 004	M	Toate procesele de sistem aferente componentelor SIA RSISC vor rula cu privilegii minime necesare executării sarcinilor atribuite.
SEC 005	M	Toate credențialele de acces utilizate de SIA RSISC trebuie să fie configurabile în interfețele administrative. SIA RSISC nu va conține credențiale de acces hard-coded.
SEC 006	M	SIA RSISC nu va conține credențiale de acces stocate la nivelul componentelor sale (în baza de date, fișiere de configurație) în formă deschisă.
SEC 007	M	Toate interfețele expuse ale SIA RSISC vor fi accesate cu aplicarea metodelor sigure de autentificare (*exemplu: certificate X.509*).
SEC 008	M	Accesul la funcțiile oferite utilizatorilor neautentificați (interfața publică furnizată de SIA RSISC) trebuie să fie controlat cu mijloace de protecție contra suprasolicitării (*exemplu: CAPTCHA, RECAPTCA etc.)*.
SEC 009	M	Conținutul câmpurilor din formularele completate de către utilizatori trebuie să fie validat în mod obligatoriu atât pe calculatorul client cât și pe server până la stocarea în baza de date.
SEC 010	M	SIA RSISC va fi securizat pentru OWASP Top 10 vulnerabilities (2017).
SEC 011	M	SIA RSISC va asigura confidențialitatea datelor transmise-recepționate pe canalele de comunicație.
SEC 012	M	Acțiunile utilizatorilor trebuie să fie înregistrate în jurnale electronice.
SEC 013	D	SIA RSISC va emite un semnal periodic care indică starea sa funcțională.

Tabelul 6.10. Cerințele pentru mecanismul de autentificare

ID	Obligativitate	Cerință
SEC 014	M	SIA RSISC va permite accesarea funcțiilor sale doar după autentificarea cu succes a utilizatorului, oferind suport pentru cel puțin următoarele metode de autentificare: • în bază de login și parolă; • în bază de soluție LDAP; • autentificarea prin intermediul semnăturii electronice sau mobile (MPass).
SEC 015	M	SIA RSISC va permite utilizatorilor mecanism de schimbare și restabilire a parolelor individuale.
SEC 016	M	SIA RSISC va permite înregistrarea utilizatorilor și a informației de profil aferentă acestora (*exemplu: login, parolă, nume, prenume, IDNP, Email etc.*).
SEC 017	M	Parolele utilizatorilor trebuie să fie protejate. Metoda de protejare a parolelor trebuie să asigure imposibilitatea interceptării, deducerii sau recuperării acestora (algoritm de criptare unidirecțională).
SEC 018	D	SIA RSISC va permite aplicarea diferențiată a politicilor de utilizare a parolelor pentru diferite grupuri de utilizatori.
SEC 019	M	SIA RSISC va permite blocarea, dezactivarea sau suspendarea conturilor utilizatorilor la nivel de aplicație.
SEC 020	D	SIA RSISC va permite aplicarea diferențiată a metodelor de autentificare, în funcție de rolurile deținute de utilizatori și componentele funcționale accesate
SEC 021	M	SIA RSISC va permite setarea numărului de conexiuni simultane ce pot fi inițiate de un utilizator.
SEC 022	M	SIA RSISC va permite setarea timpului de expirare a sesiunilor utilizatorilor autorizați în caz de inactivitate (valoarea implicită este de 15 minute).
SEC 023	M	SIA RSISC va deține mecanisme eficiente de prevenire a preluării neautorizate a sesiunilor active inițiate de utilizatorii autorizați.
SEC 024	M	Sesiunea de lucru în SIA RSISC va fi blocată la solicitarea utilizatorului sau automat, la expirarea timpului rezervat sesiunii.

Tabelul 6.11. Cerințele pentru mecanismul de autorizare

ID	Obligativitate	Cerință
SEC 025	M	SIA RSISC va permite gestiunea granulară a drepturilor de acces la toate obiectele sale și acțiunile posibile asupra acestora (*exemplu: formulare*

ID	Obligativitate	Cerință
		electronice, meniuri, rapoarte, acțiuni de creare/vizualizare/actualizare/ eliminare etc.).
SEC 026	M	Metoda de autorizare în cadrul sistemului se va baza pe principiul „*este interzis tot ce nu este explicit permis*”.
SEC 027	M	SIA RSISC va permite definirea de grupuri de utilizatori și roluri și asocierea utilizatorilor la aceste grupe și roluri.
SEC 028	M	SIA RSISC va permite acordarea drepturilor de acces la nivel de utilizator explicit, grup și rol. Un grup de utilizatori va putea conține mai multe subgrupuri/roluri. Un utilizator poate fi asociat unuia sau mai multor grupuri și roluri, drepturile sale de acces fiind determinate cumulativ.
SEC 029	M	SIA RSISC va permite acordarea drepturilor de acces bazate pe reguli de business (exemplu: modificarea înregistrării doar dacă utilizatorul este autor sau dacă operațiunea se face într-un anumit interval de timp, stare sau context).
SEC 030	M	SIA RSISC va permite atribuirea temporară a drepturilor deținute de un utilizator către un alt utilizator. Atribuirea va putea fi efectuată cu păstrarea sau suspendarea drepturilor deținute de utilizatorul către care se deleagă drepturile.
SEC 031	D	SIA RSISC va permite segregarea activităților administrative (exemplu: Administratorul 1 modifică, Administratorul 2 confirmă).
SEC 032	M	SIA RSISC va furniza vizualizări și rapoarte privind drepturile de acces configurate. Acestea vor putea fi parametrizate în funcție de cel puțin următoarele criterii: grup de utilizatori/roluri, login utilizator, acțiuni admise etc.
SEC 033	M	SIA RSISC va deține capabilități de autentificare și autorizare a utilizatorilor prin intermediul atât a mecanismelor interne, cât și prin intermediul serviciului de platformă MPass.
SEC 034	M	SIA RSISC va autoriza accesul utilizatorilor la compartimentele interfeței utilizator și date după verificarea împuternicirilor acestora prin intermediul MPower.

Tabelul 6.12. Cerințele pentru mecanismul de validare a datelor de intrare/ieșire

ID	Obligativitate	Cerință
SEC 035	M	SIA RSISC va deține mecanisme adecvate pentru a preveni manipularea datelor de intrare (date de intrare parvenite de la utilizatorii autorizați, date de intrare parvenite de la aplicații externe).
SEC 036	M	Toate acțiunile de modificare date critice și sensibile în cadrul SIA RSISC vor fi efectuate prin intermediul formularelor și documentelor specializate, conform fluxului de lucru stabilit pentru aceste categorii de documente (*exemplu: corectarea datelor incidentelor documentate*).

ID	Obligativitate	Cerință
SEC 037	M	SIA RSISC va efectua validarea completă și independentă a datelor pe partea de nivelul de prezentare, nivelul logicii de business, nivelul de date, în scopul asigurării integrității, completitudinii și corectitudinii datelor.
SEC 038	M	Toate afișările de date în cadrul SIA RSISC trebuie să fie însoțite de un marcaj de securitate, conform unui clasificator stabilit în acest sens în cadrul SIA RSISC.
SEC 039	M	Datele confidențiale nu vor fi stocate și accesate nesecurizat în cadrul SIA RSISC (*exemplu: fișiere log, caching etc.*).
SEC 040	M	SIA RSISC va deține mecanisme de protejare adițională a datelor deosebit de confidențiale (exemplu: afișarea mascată a datelor, stocarea datelor în formă criptată, autentificarea repetată sau utilizând mijloace suplimentare a utilizatorului etc.).
SEC 041	M	SIA RSISC va deține proceduri de rutină pentru verificarea și detectarea posibilelor coruperi a relațiilor de integritate a datelor.
SEC 042	M	SIA RSISC va deține mecanisme adecvate pentru a preveni manipularea datelor stocate în cadrul aplicației.

Tabelul 6.13. Cerințele pentru mecanismul de jurnalizare și audit

ID	Obligativitate	Cerință
SEC 043	M	SIA RSISC va deține componente de audit ce vor colecta și gestiona centralizat înregistrările de audit la nivelul fiecărui modul al sistemului informatic.
SEC 044	M	Componenta de audit va permite configurarea granulară a politicilor de audit.
SEC 045	M	SIA RSISC va permite stabilirea politicilor de audit la nivel de componentă funcțională/compartiment al interfeței utilizator, categorii de date și la nivel de eveniment jurnalizat.
SEC 046	M	SIA RSISC va permite stabilirea caracteristicilor specifice evenimentelor ce trebuie să fie jurnalizate (exemplu: produse într-un anumit interval de timp, aflate într-un anumit statut sau care tranzitează un anumit statut etc.).
SEC 047	M	SIA RSISC va permite auditarea oricărui eveniment, la nivelul oricărui obiect sau entitate de business din cadrul sistemului informatic.
SEC 048	M	Fiecare înregistrare de audit va conține cel puțin: • momentul în timp al producerii evenimentului; • subiectul evenimentului (identificatorul utilizatorului); • obiectul sau entitatea afectată; • evenimentul produs;

ID	Obligativitate	Cerință
		• adresa IP de unde s-a inițiat evenimentul.
SEC 049	M	Înregistrările de audit nu vor conține date confidențiale (exemplu: parole introduse la încercările eșuate de autentificare).
SEC 050	M	Erorile ce pot apărea la jurnalizarea înregistrărilor de audit nu trebuie să afecteze funcționarea normală a sistemului informatic.
SEC 051	M	Componenta de audit va utiliza ceasul de sistem setat la nivelul sistemului de operare al serverului aplicație în care rulează funcționalitatea de jurnalizare a evenimentelor.
SEC 052	M	Componenta de audit va deține un mecanism de arhivare a înregistrărilor de audit istorice. Procesul de arhivare va putea fi parametrizat (frecvența, vechime date, format arhivare, destinație etc.).
SEC 053	M	SIA RSISC va putea genera automat notificări către persoanele responsabile la producerea anumitor evenimente de securitate, conform configurațiilor setate.
SEC 054	M	SIA RSISC va permite fixarea versiunilor istorice ale datelor, ce vor fi considerate deosebit de senzitive.
SEC 055	M	Activitățile de schimbare stări și responsabili înregistrări vor fi jurnalizate.
SEC 056	M	SIA RSISC va deține instrumente comode pentru accesarea și procesarea evenimentelor jurnalizate, inclusiv filtrarea înregistrărilor de audit după orice câmp deținut și exportul acestora în format uzual. Instrumentele de audit ale sistemului informatic vor putea fi utilizate și în scopul importului arhivelor cu fișiere de audit pentru activități de analiză ocazionale.
SEC 057	M	SIA RSISC va deține mecanisme sigure de protejare a integrității datelor de audit înregistrate.
SEC 058	M	Evenimentele de business critice trebuie jurnalizate în paralel prin intermediul serviciului guvernamental de jurnalizare MLog.
SEC 059	M	SIA RSISC va furniza mecanism de configurare a evenimentelor de business care vor fi jurnalizate în paralel prin intermediul serviciului MLog.

Tabelul 6.14. Cerințele pentru mecanismul de gestiune a excepțiilor și erorilor

ID	Obligativitate	Cerință
SEC 060	M	SIA RSISC va înregistra centralizat toate excepțiile și erorile generate de componentele sale funcționale.
SEC 061	M	La producerea unei erori, SIA RSISC va afișa utilizatorului un mesaj de eroare generic. Acesta poate conține un cod de eroare și un identificator unic al erorii, pentru a facilita implicarea serviciilor de suport.

ID	Obligativitate	Cerință
SEC 062	M	SIA RSISC va deține instrumentele necesare pentru analiza și procesarea înregistrărilor aferente excepțiilor și erorilor.
SEC 063	M	SIA RSISC va putea genera automat notificări către persoanele responsabile la producerea anumitor erori în funcționarea componentelor sale funcționale.

Tabelul 6.15. Cerințele pentru capabilitățile de reziliență

ID	Obligativitate	Cerință
SEC 064	M	SIA RSISC va avea implementate instrumente pentru executarea procedurilor de generare automată a copiilor de rezervă și gestiune a copiilor de rezervă istorice.
SEC 065	M	SIA RSISC trebuie să dețină mecanisme de asigurare a integrității datelor în cazul căderilor la nivelul oricăror componente.
SEC 066	M	SIA RSISC trebuie să dețină mecanisme de restabilire operativă a disponibilității și accesibilității în cazul unor incidente de continuitate.
SEC 067	M	Arhitectura SIA RSISC trebuie să fie rezistentă la căderi de componente și să nu dețină puncte singulare de cădere (SPOF).
SEC 068	M	SIA RSISC trebuie să dețină mecanisme de asigurare a integrității datelor în cazul unor căderi accidentale la nivelul oricăror componente ale sale.
SEC 069	M	SIA RSISC trebuie să dețină mecanisme de restabilire operativă a disponibilității și accesibilității în cazul unor incidente de continuitate.

6.9. Cerințele de desfășurare a sistemului informatic

Tabelul 6.14 conține cerințele privind mecanismele de desfășurare a SIA RSISC ce urmează a fi implementate de Furnizor. Acestea corespund cerințelor recente pentru sistemele informatice ale autorităților publice centrale ale Republicii Moldova.

Tabelul 6.16. Cerințele de desfășurare a sistemului informatic

ID	Obligativitate	Descrierea cerinței de desfășurare
DEP 001	M	SIA RSISC trebuie să capabil a fi instalat pe servere dedicate și în medii virtualizate.
DEP 002	M	SIA RSISC trebuie să capabil să fie desfășurat și să funcționeze pe o infrastructură containerizată (*exemplu: Docker Engine, Kubernetes*).
DEP 003	M	SIA RSISC trebuie să capabilă să inițieze desfășurarea pe mai multe medii simultan (*exemplu: de dezvoltare, de testare, de producție*) inițiate de la zero.
DEP 004	M	Desfășurarea SIA RSISC trebuie să fie efectuată prin intermediul unor instrumentare specializate ce asigură automatizarea

ID	Obligativitate	Descrierea cerinței de desfășurare
		procesului de creare a imaginilor docker, actualizarea acestora, versionarea, desfășurarea.
DEP 005	M	Mecanismul de desfășurare a SIA RSISC trebuie să fie capabil să definească componenta containerului ce urmează a fi actualizată (*exemplu: versiune nouă a softului de platformă, modul funcțional actualizat, etc.*).
DEP 006	M	Mecanismul de desfășurare a SIA RSISC trebuie să fie capabil să gestioneze conținutul containerului.
DEP 007	M	Mecanismul de desfășurare a SIA RSISC trebuie să fie capabil să adauge noi componente în conținutul containerului.
DEP 008	M	Pentru desfășurarea SIA RSISC este necesar ca mecanismul de desfășurare să poată specifica în ce cluster (server dedicat sau cloud) trebuie să fie efectuată desfășurarea.
DEP 009	M	Pentru desfășurarea SIA RSISC este necesar ca mecanismul de desfășurare să furnizeze flux de lucru pentru compilarea codului sau registrelor.
DEP 010	M	Mecanismul de desfășurare a SIA RSISC trebuie să furnizeze funcționalități de livrare a soluției informatice și efectuare de acțiuni terțe (*exemplu: instalarea pachetelor adiționale, configurare notificări etc.*) utilizând instrumentare existente.
DEP 011	M	Mediul de producție al SIA RSISC trebuie să poată fi actualizat automat cu posibilități de intervenție manuală (*exemplu: aprobare build manual*).
DEP 012	M	Dezvoltatorul va livra către STISC toate instrumentarele și scripturile necesare desfășurării automatizate a SIA RSISC.

6.10. Cerințe de documentare a sistemului informatic

SIA RSISC va fi acompaniat de un set complet de documentație tehnică care cuprinde compartimentele incluse în tabelul 6.15.

Tabelul 6.17. Cerințele de documentare a sistemului informatic

ID	Obligativitate	Descrierea cerinței de documentare a SIA RSISC
DOC 001	M	Furnizorul va pregăti și publica materiale de ghidare interactivă incluse în interfața utilizator a SIA RSISC.
DOC 002	M	Furnizorul va pregăti și livra manualul utilizatorului în limba Română.
DOC 003	M	Furnizorul va pregăti și livra ghidul administratorului în limba Română.
DOC 004	M	Furnizorul va pregăti și livra ghidul de instalare si configurare a sistemului (care să includă cel puțin compilarea codului, instalarea aplicației, cerințe

ID	Obligativitate	Descrierea cerinței de documentare a SIA RSISC
		hardware și software, descrierea și configurarea platformei, configurarea aplicației, proceduri de disaster recovery).
DOC 005	M	Furnizorul va pregăti și livra proiectul tehnic al sistemului informatic livrat în baza căruia vor fi efectuate totalitatea activităților de dezvoltare/acceptanță a sistemului informatic (SRS și SDD).
DOC 006	M	Furnizorul va pregăti și livra documentația de Arhitectură a sistemului cu descrierea modelelor în limbajul UML, care să includă un nivel de detaliere suficient al arhitecturii în mai multe secționări (inclusiv modelul logic și fizic al datelor).
DOC 007	M	Furnizorul va pregăti și livra documentația API-urilor consumate și expuse pentru integrare cu sistemele informatice externe.
DOC 008	M	Furnizorul va livra totalitatea instrucțiunilor necesare bunei exploatări a SIA RSISC și soluționare a unor eventuale probleme tehnice.
DOC 009	M	Furnizorul va livra codul sursă pentru aplicațiile și componentele dezvoltate în cadrul proiectului cu comentariile necesare înțelegerii codului program.
DOC 010	M	Furnizorul va livra documentația de instruire pentru toate rolurile de utilizatori ai SIA RSISC.

6.11. Cerințe de garanție, mentenanță și suport tehnic al sistemului informatic

Furnizorul va asigura garanție și suport tehnic post implementare care cuprinde compartimentele incluse în tabelul 6.18.

Tabelul 6.18. Cerințele de garanție, mentenanță și suport tehnic

ID	Obligativitate	Descrierea cerinței de garanție și suport tehnic
GMS 001	M	Dezvoltatorul va oferi garanție și suport tehnic pe parcursul a 12 luni după acceptanța finală a SIA RSISC.
GMS 002	M	Garanția și suportul tehnic va corespunde standardului național SM ISO/CEI 14764:2015 - Ingineria software. Procesele ciclului de viață al software-ului. Mentenanță.
GMS 003	M	Dezvoltatorul va pune la dispoziția STISC un serviciu Help Desk disponibil în toate zilele lucrătoare ale anului.
GMS 004	M	Utilizatorii STISC vor putea apela serviciul Help Desk la un număr de telefon național (care corespunde numerotării telefonice a Republicii Moldova).
GMS 005	M	Limba de comunicare cu serviciul Help Desk – română sau rusă.
GMS 006	M	Utilizatorii STISC vor putea semnala alternativ problemele tehnice apărute prin mecanism de ticketing, Email sau mesaje instant.

ID	Obligativitate	Descrierea cerinței de garanție și suport tehnic
GMS 007	M	Furnizorul va asigura suport de documentare a problemelor tehnice și trasabilitatea acestora pentru Beneficiar.
GMS 008	M	Termenul limită de răspuns și remediere a problemelor tehnice raportate nu va depăși 8 ore de la semnalarea acestora.
GMS 009	M	În cazul unor probleme de complexitate majoră, termenul de soluționare a acestora nu va depăși 72 ore.
GMS 010	M	Dezvoltatorul va demonstra capabilitatea de asigurare a suportului tehnic post livrare în conformitate cu cerințele GMS 001-GMS 009.
GMS 011	M	Orice eroare program depistată pe parcursul perioadei de garanție va fi remediată de Dezvoltator gratuit și în termen util.
GMS 012	M	În cazul apariției unor solicitări adăugătoare de implementare, acestea vor face obiectul unui amendament la contract și plată a contravalorii serviciilor.
GMS 013	M	Furnizorul și STISC vor semna un SLA care va specifica în detalii principiile de prestare a serviciilor de garanție, mentenanță și suport.

7. Produsul final și componentele livrate

Produsul final (SIA RSISC) e format din artefactele software și de documentare a sistemului precum și de transferul de cunoștințe către posesorul, deținătorul și administratorul soluției software. Artefactele aferente livrabilelor SIA RSISC sunt specificate în tabelul 7.1.

Tabelul 7.1. Lista livrabilelor de proiect

ID	Obligativitate	Descrierea succintă a artefactului
DEL 001	M	Codul sursă complet al modulelor și componentelor necesare compilării produsului program livrat.
DEL 002	M	Soluția software de migrare și populare primară a datelor în SIA RSISC.
DEL 003	M	Produsul final împachetat pentru instalare facilă în mediul tehnologic propus (inclusiv scripturile de deployment automatizat).
DEL 004	M	Documente și rapoarte aferente proceselor de management al proiectului de proiectare, dezvoltare și implementare a SIA RSISC.
DEL 005	M	Proiectul Tehnic (SRS+SDD).
DEL 006	M	Documentul privind desfășurarea și configurarea SIA RSISC.
DEL 007	M	Manualul Utilizatorului.
DEL 008	M	Manualul Administratorului (inclusiv planul de contingență).
DEL 009	M	Ghidul de înlăturare a defecțiunilor și activităților de mentenanță curentă a SIA RSISC.
DEL 010	M	Totalitatea materialelor aferente instruirii utilizatorilor SIA RSISC.
DEL 011	M	Specificațiile tehnice pentru interfețele consumate și publicate de SIA RSISC.
DEL 012	M	Planul de testare și rezultatele testării interne (funcționale, de integrare, de performanță, de încărcare, de securitate).
DEL 013	M	Acord SLA semnat cu STISC pentru perioada de mentenanță, garanție și suport.
DEL 014	M	Toate artefactele urmează a fi livrate pe suport electronic (DVD+-R).

Adițional la artefactele aferente livrabilelor SIA RSISC vor fi prestate un șir de servicii necesare transferului de cunoștințe către STISC conținute în tabelul 7.2.

Tabelul 7.2. Serviciile de transfer de cunoștințe aferente artefactelor livrate

ID	Obligativitate	Descrierea succintă a artefactului
DEL 015	M	Furnizorul urmează să efectueze activități de instruire destinate trainerilor STISC care vor putea instrui în continuare toate categoriile de utilizatori a SIA RSISC.

ID	Obligativitate	Descrierea succintă a artefactului
DEL 016	M	Furnizorul urmează să efectueze activități de instruire tuturor categoriilor de utilizatori autorizați și utilizatorilor cu rol administrator de sistem.
DEL 017	M	Furnizorul urmează să furnizez servicii de asistență tehnică pe perioada de pilotare a SIA RSISC.
DEL 018	M	Furnizorul va asista STISC în activitățile de testarea de acceptare a SIA RSISC.
DEL 019	M	Furnizorul urmează să furnizeze servicii de asistare a STISC în procesele de punere a SIA RSISC în producție.
DEL 020	M	Furnizorul urmează să elimine toate deficiențele și erorile ale SIA RSISC identificate pe perioada de pilotare și la testarea de acceptare.
DEL 021	M	Furnizorul urmează să asigure suport tehnic post implementare (după punerea sistemului în producție) pentru o perioadă de 12 luni, inclusiv mentenanță corectivă, adaptivă și preventivă, în conformitate cu *SM ISO/CEI 14764:2015 - Ingineria software. Procesele ciclului de viață al software-ului. Mentenanță*.

8. Etapele de implementare a sistemului informatic

Activitățile de proiectare, dezvoltare, testare și implementare a a SIA RSISC trebuie să fie realizate de către întreprinderi și instituții specializate ce posedă experiența necesară pentru îndeplinirea lucrărilor corespunzătoare și vor cuprinde următoarele etape:

1. **Etapa de elaborare a sistemului informatic** - care va fi divizată în faze coordonate cu STISC după cum urmează:
    a. Furnizorul analizează termenii de referință, efectuează analiza de business și cu aprobarea STISC propune viziunea sa de dezvoltare a sistemului informatic prin intermediul unui Proiect tehnic (SRS și SDD) elaborat în termen de 1 lună calendaristică;
    b. Furnizorul dezvoltă codul program și integrează modulele dezvoltate într-o versiune prototip a SIA RSISC (se va face o primă prezentare părților demonstrând existenta tuturor funcționalităților descrise în prezentul caiet de sarcini) care ulterior va fi perfecționată până la semnarea acceptanței finale. Etapa în cauză nu va depăși 6 luni;
    c. Furnizorul efectuează activitățile de migrare și populare inițială cu date a SIA RSISC (1 lună calendaristică).
    d. Furnizorul testează sistemului în regim de laborator (testare internă) și pregătește documentația de însoțire (se prezintă funcționalitățile sistemului cu corectările și ajustările la obiecțiile făcute în sub-etapa precedentă, se prezintă setul documentației tehnice, etc.). Etapa în cauză va dura 3 săptămâni. Testarea va cuprinde obligatoriu următoarele etape:
        - vor fi verificate în comun totalitatea scenariilor de testare privind satisfacerea tuturor cerințelor funcționale ale sistemului informatic (*functional testing, unit testing, integration testing*);
        - asupra sistemului sunt aplicate scenarii de *stress testing*, *load testing* și *security testing* în vederea verificării gradului de corespundere a acestuia așteptărilor STISC și prevederilor prezentului caiet de sarcini;
        - în baza rezultatelor testării, în caz de necesitate, vor fi operate ajustările și modificărilor solicitate, pregătindu-se o versiune ameliorată a sistemului informatic.
    e. Furnizorul efectuează activitățile de desfășurare și configurare a celor 3 medii ale a SIA RSISC (Mediul de producție, Mediul de testare/instruire, Mediul de dezvoltare). Activitatea date va dura până la 1 săptămână.
2. **Etapa de instruire** va începe odată cu finisarea testelor de acceptanță și va cuprinde instruirea a 2 utilizatori cu rol *Administrator de Sistem*, 2 traineri pentru instruirea ulterioară a utilizatorilor autorizați și până la 30 utilizator autorizați cu toate rolurile configurate.
3. **Etapa de stabilizare a SIA RSISC** va începe odată cu aprobarea procesului verbal de acceptare de către STISC în varianta prezentată și semnarea actului de punere în producție a sistemului informatic. Această etapă va dura 3 luni pe parcursul căreia Furnizorul va asista STISC în exploatarea a SIA RSISC și va efectua activități de eliminare a erorilor/deficiențelor depistate precum și optimizări în parametrii de funcționare a SIA RSISC.
4. **Darea în exploatare a sistemului** începe odată cu semnarea actului de punere în exploatare a sistemului informatic și începere a exploatării acestuia.

5. **Etapa de garanție mentenanță și suport** este perioada în care Furnizorul își asumă obligațiunea față de STISC să-l asiste în menținerea capacității sistemului informatic de a presta servicii, precum și modificarea produsului informatic (eliminarea erorilor și optimizarea parametrilor de funcționare), păstrând integritatea lui. În cazul SIA RSISC sunt necesare 12 luni calendaristice de garanție, mentenanță și suport tehnic.

9. Cerințe de perfectare a ofertelor

9.1. Cerințe privind puterea instituțională a furnizorului

La concurs pot participa companii specializate în prestarea serviciilor informatice cu o experiență în domeniu de minim 5 ani. Este preferabilă existența experienței ofertantului în elaborarea și implementarea soluțiilor complexe destinate APC și APL conforme inițiativelor e-Guvernare în Republica Moldova.

Persoanele juridice interesate trebuie să expedieze oferta tehnică care să conțină:

- Descrierea detaliată a operatorului economic (experiență, resurse umane, capacități manageriale și tehnice în domeniu, etc.);
- Portofoliul companiei cu indicarea proiectelor similare implementate;
- Referințele beneficiarilor companiei pentru ultimii 4 ani;
- Descrierea succintă a soluțiilor informatice similare;
- Oferta tehnică detaliată propusă, inclusiv restricțiile hardware de funcționare, estimarea activităților și duratelor lor.
- Metodologia de asigurare a serviciilor de garanție, mentenanță și suport (inclusiv facilitățile deținute);

9.2. Cerințe privind personalul furnizorului implicat în proiect

Toate discuțiile cu reprezentanții STISC vor fi efectuate în limba română. Toată documentația aferentă, trainingul și suportul tehnic vor fi perfectate în limba română. Toți colaboratorii implicați în proiect care interacționează nemijlocit cu reprezentanții STISC trebuie să posede la perfecție limba română.

Furnizorul va prezenta în oferta tehnică date sumare privind personalul implicat în proiect și calificarea acestuia. Este binevenită implicarea de personal calificat cu experiență în dezvoltarea și implementarea sistemelor informatice de complexitate similară în cadrul APC din Republica Moldova.

În mod explicit se vor prezenta persoanele angajate în următoarele funcții cheie:

- Manager de Proiect;
- System Architect/Business Analyst;
- Dezvoltator/Administrator Bază de date;
- Software Developer/Integration Expert;
- Software Developer/DevOps Expert;
- Software Tester;
- Trainer.

Pentru aceste posturi vor fi prezentate CV-urile persoanelor antrenate, având în vedere ca experiența membrilor echipei să includă:

1. Manager de proiect.

Master în tehnologii informaționale sau alte domenii relevante (pentru studiile conforme procesului de la Bologna) sau licențiat în tehnologii informaționale sau alte domenii relevante (pentru studiile conforme procesului pre Bologna) cu următoarea experiență:

- cel puțin 5 ani experiență în domeniul dezvoltării software;
- cel puțin 5 ani experiență demonstrată în gestiunea proiectelor de complexitate similară (preferabil pentru sectorul guvernamental) cu utilizarea metodologiei de gestiune a proiectelor propuse în cel puțin 2 proiecte similare implementate pe parcursul ultimilor 3 ani;
- cunoașterea ciclului de viață al software-lui;
- experiență relevantă în analiza proceselor de business;
- abilitate de comunicare în limbile română și engleză;
- deținerea certificării recunoscute internațional în domeniul managementului proiectului constituie un avantaj;

2. System Architect/Business Analyst.

Licențiat în tehnologii informaționale sau alte domenii cu următoarea experiență:

- cel puțin 5 ani experiență de lucru în calitate de System Architect/Business Analyst demonstrată prin implicarea în implementarea proiectelor în poziție similară pentru proiectarea/dezvoltarea/implementarea sistemelor informatice cu complexitate similară;
- experiență dezvoltată în utilizarea metodologiilor și abordărilor moderne de proiectare a sistemelor informatice și aplicarea standardelor și inițiativelor TIC specifice sectorului guvernamental al Republicii Moldova;
- în implementarea a cel puțin 2 proiecte similare pe parcursul ultimilor 3 ani;
- experiență în testarea modulară, integrarea continuă, DevOps;
- certificarea în domeniul proiectării mijloacelor software
- cunoașterea ciclului de viață al software-lui (*exemplu: TOGAF 9, CTA etc.*) va constitui un avantaj însemnat;
- abilitate de comunicare în limba română sau rusă.

3. Dezvoltator/Administrator Bază de date.

Licențiat în tehnologii informaționale sau alte domenii cu următoarea experiență:

- cel puțin 5 ani experiență de lucru în dezvoltarea software în poziție de Dezvoltator/Administrator Bază de Date în care au fost utilizate tehnologiile propuse pentru dezvoltarea și exploatarea SIA RSISC;
- în implementarea a cel puțin 2 proiecte similare pe parcursul ultimilor 3 ani;
- experiență demonstrată în proiectarea, dezvoltarea și optimizarea bazelor de date;
- experiență în testarea modulară, integrarea continuă, DevOps;
- certificare recunoscută aferentă stivei tehnologice propuse pentru SIA RSISC va constitui un avantaj esențial;
- abilitate de comunicare în limba română sau rusă.

4. Software Developer/Integration Expert.

Licențiat în tehnologii informaționale sau alte domenii cu următoarea experiență:

- cel puțin 3 ani experiență în dezvoltarea sistemelor informatice în baza tehnologiilor propuse pentru SIA RSISC;
- în implementarea a cel puțin 2 proiecte similare pe parcursul ultimilor 3 ani;
- experiență în testarea modulară;
- experiență demonstrată în integrarea software, proiectarea și dezvoltarea API, utilizând SOAP/REST;
- certificare recunoscută aferentă stivei tehnologice propuse pentru SIA RSISC va constitui un avantaj esențial;
- abilitate de comunicare în limba română sau rusă.

5. Software Developer/DevOps Expert.

Licențiat în tehnologii informaționale sau alte domenii cu următoarea experiență:

- cel puțin 3 ani experiență în dezvoltarea sistemelor informatice în baza tehnologiilor propuse pentru SIA RSISC;
- în implementarea a cel puțin 2 proiecte similare pe parcursul ultimilor 3 ani;
- experiență dezvoltată în testarea modulară, integrarea continuă, DevOps;
- certificare recunoscută aferentă stivei tehnologice propuse pentru SIA RSISC va constitui un avantaj esențial;
- abilitate de comunicare în limba română sau rusă.

6. Software Tester.

Licențiat în tehnologii informaționale sau alte domenii cu următoarea experiență:

- cel puțin 3 ani experiență în testarea produselor software de complexitate similară SIA RSISC;
- experiență demonstrată în testarea funcțională a sistemelor informatice;
- experiență demonstrată în testarea performanței și încărcării sistemelor informatice;
- experiență demonstrată în automatizarea proceselor de testare a produselor software;
- certificarea în domeniul asigurării calității (*exemplu: ISTQB*) sau aferente stivei tehnologice propuse pentru dezvoltarea și operarea SIA RSISC va constitui un avantaj esențial;
- abilitate de comunicare în limba română sau rusă.

7. Trainer.

Licențiat în tehnologii informaționale sau alte domenii cu următoarea experiență:

- experiență demonstrată în efectuarea sesiunilor de instruire a utilizatorilor cu diferit rol în cadrul sistemelor informatice în cel puțin 2 proiecte similare;
- experiență demonstrată în scrierea documentației tehnice, ghidurilor pentru utilizatorii sistemelor informatice și materialelor instructive;
- experiență în efectuarea instruirilor online;

- abilități de comunicare în limbile română sau rusă.

Ceilalți membri ai echipei de proiect (personal non-cheie) trebuie să dețină competențe în următoarele domenii:

- dezvoltare/implementarea soluțiilor informatice WEB;
- proiectarea și administrarea bazelor de date;
- proiectare/dezvoltarea/integrarea interfețelor destinate schimbului de date cu sisteme informatice externe;
- asigurare calitate inclusiv experiență în automatizarea procesului de testare;
- abilități de instruire a utilizatorilor.

Anexa 1. Șabloane de formulare

A1.1. Formularul de raportare a alertelor/incidentelor de securitate

Formular de raportare a evenimentelor/incidentelor

Nr.	Criteriu	Detaliere
Detectarea și raportarea evenimentului/incidentalului de securitate		
1.	Data/Ora depistării	Data ___/___/___ Ora ___:___
2.	Cauza incidentului	Cauză externă/parte terță: Da ☐ Nu ☐
3.	Descriere succintă a incidentului și cauza (dacă este identificată)	
4.	Resurse afectate	
5.	Localizarea (Deținătorul Resursei Informaționale)	
6.	Impact	
7.	Urgență	
8.	Măsuri întreprinse	
Raportor		
9.	Nume	
10.	Prenume	
11.	E-mailul	
Escaladare DA ☐ NU ☐		
12.	Membrul echipei de răspuns la incidente	

A1.2. Raport privind incidentul de securitate

Raport privind incidentul de securitate

Nr.	Criteriu	Detaliere
Identificarea evenimentului/incidentului		
1.	ID incident	
2.	Data/Ora procesării	Data ___/___/___ Ora ___:___
3.	Data/Ora depistării	Data ___/___/___ Ora ___:___
4.	Cauza incidentului	
5.	Descriere succintă a incidentului și cauza (dacă este identificată)	
6.	Resurse afectate	
7.	Localizarea (Deținătorul Resursei Informaționale)	
8.	Categoria incidentului	
9.	Tipul impactului	
10.	Impact	
11.	Urgență	
12.	Prioritate	
13.	Măsuri întreprinse	
Raportor DRI		
14.	Nume	
15.	Prenume	
16.	E-mailul	
Raportor MSI		
17.	Nume	
18.	Prenume	
19.	E-mail	
Escaladare DA ☐ NU ☐		
20.	Nivel	
Soluționarea incidentului		
21.	Acțiuni de soluționare	
22.	Responsabili soluționare	
23.	Timp de soluționare	___ h ___ min

Nr.	Criteriu	Detaliere
Cercetarea cauzei producerii incidentului		
24.	Concluzii	
25.	Măsuri de prevenire	
Evidență incidentelor		
26.	Statut	

A1.3. Raport de analiză post incident

Raport de analiză post incident

ID-ul incidentului	
Data și timpul identificării	
Categoria/ Clasificarea incidentului	
Severitatea incidentului (impactul tehnic)	
Subdiviziune/ Autoritatea afectată	
Sumar	
Obiective analiză: Scopul recenziei post incident urmărește majorarea nivelului de experiență a membrilor echipelor implicate, precum și îmbunătățirea procesului de gestiune a incidentelor/ serviciilor prestate de Instituție.	
Enumerați acțiunile și măsurile întreprinse în procesul de răspuns la incidentul vizat ?	
Ce acțiuni au avut un impact pozitiv și care unul negativ ?	
Ce acțiuni corective pot preveni incidentele similare în viitor ?	
Ce instrumente sau resurse suplimentare sunt necesare pentru detectarea, analizarea și atenuarea incidentelor viitoare ?	
Cum este posibil să identificăm mai rapid un potențial incident asemănător?	
Cum este posibil de îmbunătățit schimbul de informații cu alte organizații ?	
Cum este posibil să răspundem mai eficient și să remediem un incident asemănător într-un timp mai scurt?	
Ce am învățat despre rețeaua/ sistemul vizat, precum și procese/ interacțiunea între echipe în incidentul vizat?	
Cum este posibil să îmbunătățim rețeaua/ sistemul în urma experienței acumulate pe parcursul ciclului de viață a incidentului?	
Timpul de reacție per fiecare fază	
Timpul de investigare	
Timpul de izolare a resursei afectate	
Timpul de tratare	
Timpul de recuperare	
Indicatori de performanță	

Timpul de identificare (analiză preliminară)	
Timpul de recuperare	
Nr. scrisorilor de notificare expediate	
Nr. rapoartelor de investigare întocmite	