CAIET DE SARCINI

pentru elaborarea
Sistemului Informațional
Registrul de Stat al Incidentelor Cibernetice

Chișinău, 2026

Cuprins

Introducere ... 3
Scop și obiective ... 4
Abrevieri și definiții ... 5
Cadrul normativ ... 7
Descriere generală ... 9
Obiecte informaționale ... 13
Model funcțional ... 15
Actori ... 15
Alerta timpurie ... 18
Incidente cibernetice ... 29
Schimb de informații ... 39
Administrare și control ... 43
Cerințe ... 50
Cerințe funcționale ... 50
Alerta timpurie ... 50
Incidente cibernetice ... 55
Schimb de informații ... 62
Administrare și control ... 64
Cerințe nonfuncționale ... 67
Cerințe arhitecturale ... 67
Cerințe de licențiere și drepturi ... 69
Cerințe de integrare ... 71
Cerințe de securitate ... 73
Cerințe de performanță ... 76
Mentenanța și actualizarea ... 77
Interfața utilizator ... 78
Documente și instruire ... 82
Raportare și taxonomie ... 83
Garantie si suport ... 85
Foaie de parcurs ... 86
Roluri cheie ... 87
Anexa: FNV - Formular Notificare de Vulnerabilitate ... 88

Introducere

Documentul este elaborat pentru Agenția de Securitate Cibernetică (ASC) din Republica Moldova în cadrul cooperării cu Banca Mondială, prin proiectul „Support on Anticorruption, Integrity and Asset Recovery Technical Assistance Project", finanțat de Guvernul Regatului Unit al Marii Britanii și Irlandei de Nord prin FCDO Trust Fund.

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

Prin Hotărârea Guvernului nr. 1028/2023, Agenția pentru Securitate Cibernetică (ASC) a fost desemnată în calitate de autoritate competentă la nivel național în domeniul securității cibernetice și ca echipă de răspuns la incidente cibernetice la nivel național. Exercitarea atribuțiilor stabilite prin cadrul normativ presupune instituirea unui mecanism unificat, sigur și interoperabil pentru gestionarea informațiilor aferente incidentelor cibernetice raportate la nivel național, fapt ce determină necesitatea creării Sistemului informațional „Registrul de stat al incidentelor cibernetice" (SI RSIC).

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

În prezent, procesele de raportare și evidență a incidentelor cibernetice sunt realizate prin mecanisme semiautomatizate, bazate pe formulare standardizate transmise prin poșta electronică și prelucrate manual în baze de date interne. Acest mod de operare generează limitări operaționale și riscuri asociate securității informației, integrității și trasabilității datelor, precum și dificultăți în realizarea unei analize comprehensive a incidentelor raportate. Totodată, procesele existente nu permit gestionarea eficientă a fluxurilor operaționale și a schimbului de informații între entitățile implicate în prevenirea și răspunsul la incidente cibernetice.

În acest context, se impune dezvoltarea și implementarea Sistemului informațional „Registrul de stat al incidentelor cibernetice" (SI RSIC), destinat automatizării proceselor de identificare, raportare, înregistrare, clasificare, analiză, gestionare și monitorizare a incidentelor cibernetice, precum și consolidării schimbului de date între Agenția pentru Securitate Cibernetică, echipele de răspuns la incidente cibernetice sectoriale (CERT sectoriale) și alte entități prevăzute de cadrul normativ.

Prezentul Caiet de sarcini stabilește cerințele funcționale, tehnice, organizaționale și de securitate aferente dezvoltării, implementării și exploatării SI RSIC. Documentul definește obiectivele sistemului, arhitectura generală, componentele funcționale, fluxurile informaționale, cerințele de interoperabilitate, măsurile de securitate informațională, precum și condițiile privind administrarea, mentenanța și dezvoltarea ulterioară a platformei.

Implementarea SI RSIC urmărește realizarea unei platforme informaționale centralizate, capabile să asigure:

- gestionarea unificată a incidentelor cibernetice la nivel național;

- evidența și păstrarea structurată a datelor și documentelor aferente incidentelor;
- standardizarea proceselor și a datelor gestionate;
- reducerea timpului de raportare și răspuns la incidentele cibernetice;
- facilitarea schimbului securizat de informații între autoritățile și entitățile implicate;
- interoperabilitatea cu alte sisteme informaționale de stat;
- monitorizarea alertelor, amenințărilor și vulnerabilităților cibernetice;
- asigurarea unui mediu operațional sigur și a trasabilității operațiunilor efectuate în sistem.

Scop și obiective

Documentul prezintă cerințele software ce specifică funcționalitatea și capabilitățile sistemului informațional automatizat Registrul de Stat al Incidentelor Cibernetice (RSIC) conceput prin Hotărârea de Guvern 822/2025. Obiectivul principal al documentului este de a susține procesul de achiziție și contractare a furnizorului soluției software pentru RSIC.

Abrevieri și definiții

Termen sau abreviere	Detalii
API	Application Programming Interface
ASC	Agenția pentru Securitate Cibernetică din Moldova
AWS	Amazon Web Services
BD	Bază de date
CDN	Content Delivery Network
CERT	Echipele de răspuns la incidente cibernetice (sectoriale)
CF	Cerință funcțională
CISA	Cybersecurity and Infrastructure Security Agency (https://www.cisa.gov/about)
CNF	Cerință nonfuncțională
CNMC	Centrul Național de Management al Crizelor
COTS	Commercial off-the-shelf - cu referire la produse software comerciale
CSAF	Common Security Advisory Framework
CSV	Comma Separated Value - format al fișierelor de date
CU	Caz de utilizare, elementul de bază a modelului de utilizare
DNS	Domain Name System
ENISA	Agenția Uniunii Europene pentru Cibersecuritate
EUVD	EU Vulnerability Database
HG	Hotărâre Guvern
HTTP	HyperText Transfer Protocol
HTTPS	Secure HTTP
ID	Identitate
IDNO	Identificatorul național al organizațiilor
IDNP	Identificatorul național al persoanelor
IODEF	Incident Object Description Exchange Format
IP	Internet Protocol
ISO	International Standards Organization
MCabinet	Cabinetul personal al cetățeanului pe platforma guvernamentală
MCloud	Soluția Cloud a Guvernului RM
MF	Ministerul Finanțelor
MLog	Soluția de jurnalizare și audit a platformei guvernamentale
MNotify	Serviciul de notificare a platformei guvernamentale
MPass	Serviciul de identități și autentificare a platformei guvernamentale, mpass.gov.md
MSign	Serviciul de semnătură electronică a platformei guvernamentale, msign.gov.md
OWASP	Open Web Application Security Project®, owasp.org
PDF	Portable Document Format
PWA	Progressive web application
RBAC	Role Based Access Control
RFC	Request for Comment
RM	Republica Moldova

RO	România
RSIC	Registrul de Stat al Incidentelor Cibernetice
RTO/RPO	Recovery Time Objective, Recovery Point Objective
SDD	Software Design Document - document de proiect al sistemului
SGBD	Sistem de gestiune a bazelor de date
SI (SIA)	Sistem Informatic (sau sistem informațional automatizat)
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SRD	Document de cerințe software (Abrevierea EN Software requirements document)
SSI	Subsistem Informatic
STISC	Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică”
TCO	Costul total de deținere (Total Cost of Ownership)
TIC	Tehnologii Informaționale și de Comunicare
TLS	Transport Layer Security protocol
UDP	User Datagram Protocol
UI	User Interface, de obicei bazat pe tehnologii Web
UML	Unified Modeling Language
WSDL	Web Services Description Language
XML	Extensible Markup Language
XSS	Cross Site Scripting

Cadrul normativ

Cadrul normativ pentru sistem este format în primul rând de următoarele acte normative:

- HG 822/2025 privind aprobarea Conceptului Sistemului informațional „Registrul de stat al incidentelor cibernetice” și a Regulamentului cu privire la modul de ţinere a Registrului de stat al incidentelor cibernetice
- Lege 48/2024 privind securitatea cibernetică
- HG 824/2025 pentru aprobarea Regulamentului privind divulgarea coordonată a vulnerabilităților în domeniul securității cibernetice
- HG 860/2024 cu privire la identificarea furnizorilor de servicii

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

- Legea 467/2003 cu privire la informatizare și la resursele informaționale de stat;
- Legea 71/2007 cu privire la registre;
- Legea 133/2011 privind protecția datelor cu caracter personal;
- Legea 142/2018 cu privire la schimbul de date și interoperabilitate;
- Legea 48/2023 privind securitatea cibernetică;
- HG 562/2006 cu privire la crearea sistemelor și resurselor informaționale automatizate de stat;
- HG 1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass);
- HG 128/2014 privind platforma tehnologică guvernamentală comună (MCloud);
- HG 405/2014 privind serviciul electronic guvernamental integrat de semnătură electronică (MSign);
- HG 708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog);
- HG 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat;
- HG 211/2019 privind platforma de interoperabilitate (MConnect);
- HG 376/2020 pentru aprobarea Conceptului serviciului guvernamental de notificare electronică (MNotify) și a Regulamentului privind modul de funcționare și utilizare a serviciului guvernamental de notificare electronică (MNotify);
- HG 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental și modificarea Hotărârii Guvernului 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat;
- HG 323/2021 pentru aprobarea Conceptului Sistemului informațional „Catalogul semantic” și a Regulamentului privind modul de ținere a Registrului format de Sistemul informațional „Catalogul semantic”;
- HG 650/2023 cu privire la aprobarea Strategiei de transformare digitală a Republicii Moldova pentru anii 2023-2030;
- HG 562/2025 cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice;
- HG 677/2025 cu privire la consolidarea accesului la serviciile publice electronice în cadrul Portalului guvernamental integrat EVO utilizat la prestarea serviciilor publice electronice și aprobarea măsurilor necesare pentru implementarea modelului unitar de design.

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

- Ordinul ministrului dezvoltării informaționale 78/2006 cu privire la aprobarea reglementării tehnice „Procesele ciclului de viață al software-ului” RT 38370656 - 002:2006.
- Standardul Republicii Moldova SM EN ISO 9001:2015 „Sisteme de management al calității. Cerințe”;
- Standardul Republicii Moldova SM ISO/CEI/IEEE 15288:2015 „Ingineria sistemelor și software-ului. Procesele ciclului de viață ale sistemului”;
- Standardul Republicii Moldova SM EN ISO/IEC 27002:2017 „Tehnologia informației. Tehnici de securitate. Cod de bună practică pentru managementul securității informației”;
- Standardul Republicii Moldova SM ISO/IEC 27005:2018 „Tehnologia informației. Tehnici de securitate. Managementul riscului securității informației”.

Descriere generală

RSIC face parte din spațiul informațional al ASC care la rândul său interoperează cu platforma tehnologică comună. Arhitectural RSIC utilizează o abordare SOA care prestează și consumă servicii.

Diagrama de componente UML evidențiază:

- perimetrul ASC care scoate în evidență RSIC dar și sisteme ASC relevante,
- perimetrul platformei tehnologice comune a guvernării formată din servicii reutilizate de RSIC,
- natura SOA a sistemelor și prezența interfețelor prestate și consumate de serviciile digitizate.

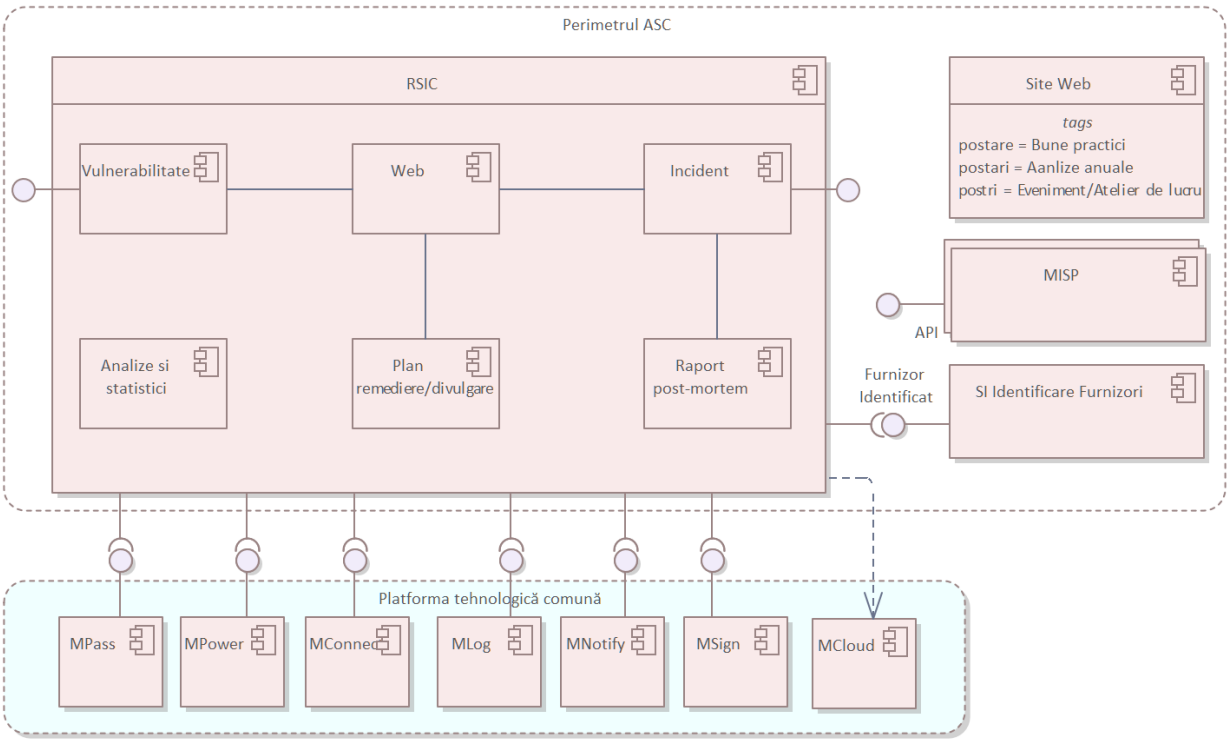

Fig. 1: Arhitectura RSIC

Diagrama scoate în evidență următoarele aspecte:

- Funcționalitatea cheie a RSIC concentrată pe Vulnerabilități (amenințări) și Incidente cibernetice.
- RSIC este o soluție SOA prestând și consumând Web Servicii mai ales pentru reutilizarea serviciilor de platformă guvernamentală comună dar și de la sisteme/organizații specializate în ramură.
- Pentru funcționalitatea cheie a RSIC sunt prestate și consumate serviciile corespunzătoare Vulnerabilitate și Incident. Modelul de date al acestora și serviciile prestate sunt conforme cu standardele din ramură pentru Incidente (IODEF) și Vulnerabilități (CSAF). Acestea asigură interoperabilitatea cu organizațiile internaționale specializate în domeniu dar și cu instrumentariul adiacent acestora.
- ASC utilizează o aplicație/subsistem separat pentru Identificarea Furnizorilor de servicii critice și unde este necesar aceste servicii sunt oferite RSIC.

- MISP este o aplicație utilizată atât intern de ASC dar și de alte organizații din ramură cu care colaborăm. API MISP informează Web Serviciile prestate de RSIC în acest mod fiind facilitată sincronizarea informațiilor dar și vocabularelor standard pentru schimb de informații între RSIC și instrumentariul de specialitate.
- serviciile prestate de platforma tehnologică comună sunt integrate în RSIC pentru funcții de identificare, acces, interoperabilitate, jurnalizare sau notificare. Lista de servicii de platformă este incompletă dar ilustrativă.
- RSIC este un sistem Cloud Ready și proiectat pentru a fi ținut în MCloud.
- RSIC include o componentă de interfață utilizator bazată pe tehnologii Web.
- RSIC include un subsistem flexibil de operare cu planurile calendaristice atât pentru remedierea cazurilor cât și divulgarea coordonată. Același subsistem asigură respectare constrângerilor de timp agreate și coordonate între părți dar și pentru conformarea cu cadrul normativ în vigoare.
- Site Web (asc.gov.md) e utilizate de ASC pentru comunicare cu publicul și publicare articole, postări, evenimente, rapoarte analitice care nu sunt conectate direct cu obiectele informaționale cheie a RSIC - Vulnerabilități, Alerte și Incidente cibernetice.

RSIC asigură înregistrarea, investigarea, soluționarea și informarea privind riscurile, amenințările, atacurile, vulnerabilitățile, incidentele cibernetice dar și a recomandărilor, bunelor practici în domeniu. Un proces cheie pentru care RSIC este implementat este procesul de divulgare coordonată este reglementat prin HG 824/2025. La nivel înalt procesul dat este prezentat mai jos.

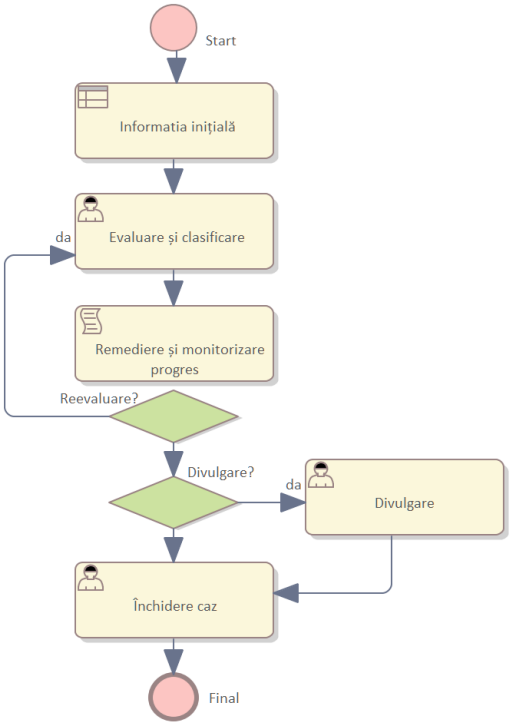

Fig. 2: Procesul de investigare cazuri cibernetice (nivel înalt)

Diagrama detaliata utilizând BPMN 2.0 este întâi clarificată în legenda de mai jos.

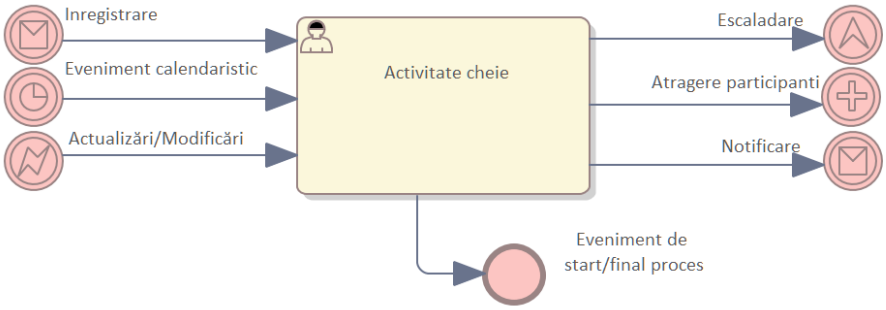

Fig. 3: Legendă

Activitățile cheie scot în evidență fluxul de lucru dar și comunicarea, informarea, escaladarea și atragerea părților în proces în bază de severitate dar și conform interesului public. Procesul anticipează, acceptă și produce o serie de evenimente, notificări, escaladări, coordonări, sincronizări periodice etc care facilitează înțelegerea cazului, soluționarea acestuia și după caz necesității de divulgare coordonată. În diferite culori sunt identificate fazele procesului:

- (rosu) faza inițială de recepționare a informației atât despre vulnerabilități dar și despre incidente și trierea/corelarea acestora
- (galben) ciclul de evaluare/clasificare și remediere/monitorizare în care participanții colectează detalii, analizează situația și decid asupra severității și impactului și consecvent stabilesc calendar standard sau accelerat de remediere, coordonatorul, escaladarea și atragerea altor participanți și planul de divulgare coordonată.
- (alb) activitățile de pregătire pentru divulgarea coordonată dar și publicarea/consultarea informațiilor despre cazul analizat
- (verde) închiderea cazului când remedierea finală este validată

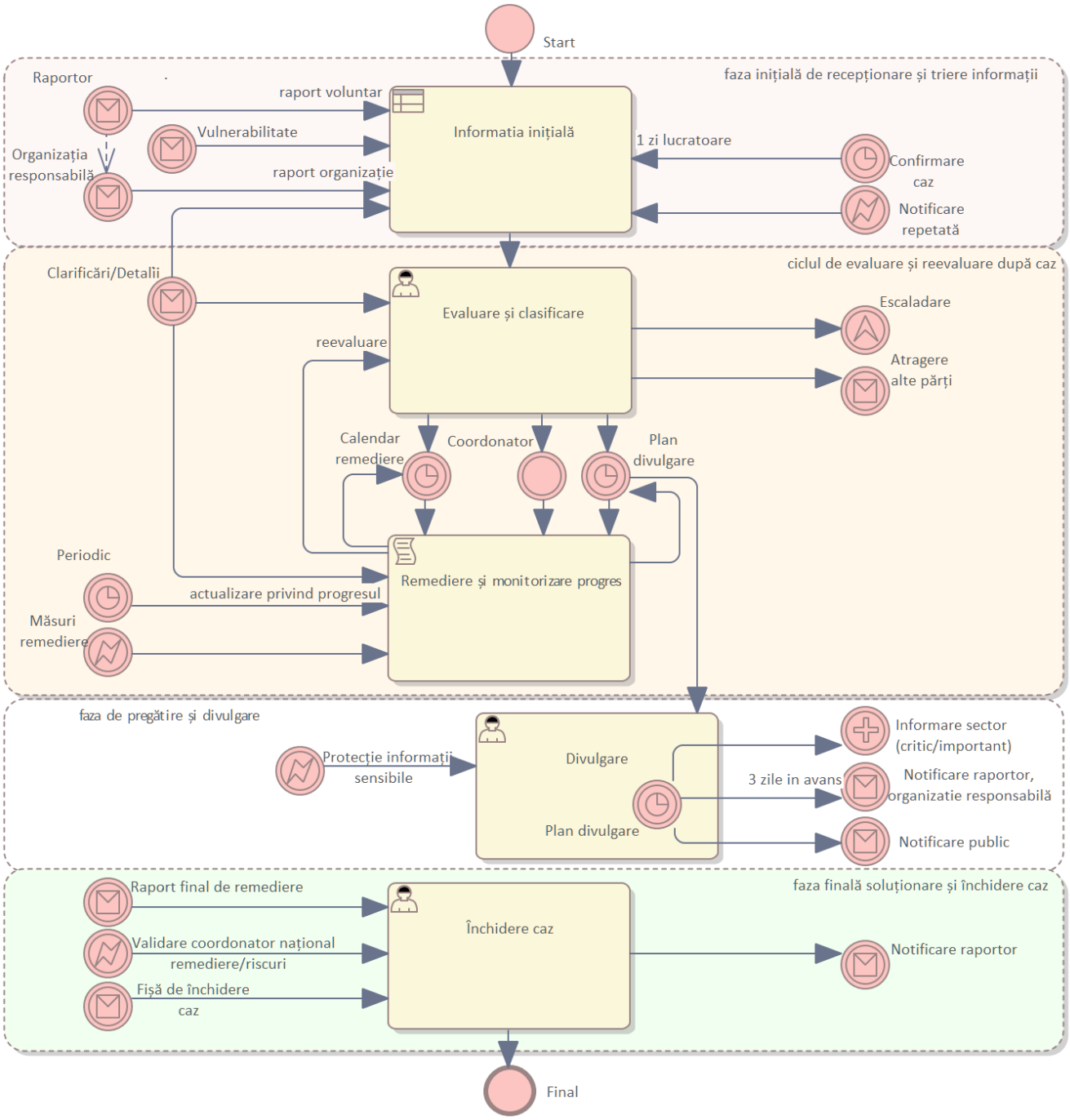

Fig. 4: Investigare cazuri cibernetice si divulgarea coordonată

Adițional la procesul ilustrat în diagramă notăm următoarele:

- Raportorul - un cercetător în ramură - când descoperă o informație de interes alege s-o raporteze către ASC (voluntar) sau către organizația responsabilă. Abia apoi organizația responsabilă raportează către RSIC informația inițială pe care o deține. De notat că unele alerte, amenințări sau vulnerabilități cibernetice înregistrate în sistem pe alte căi și ele la rândul lor pot servi ca informație inițială pentru investigarea și soluționarea unui caz.

- Odată informația inițială prezentă în sistem aceasta este examinată de reprezentanți ai ASC și se iau decizii privind clasificarea, corelarea, confirmarea sau infirmarea cazului. Dacă raportorii cazului sunt cunoscuți - aceștia sunt notificați despre această decizie.
- Cazurile confirmate sunt luate în lucru și în primul rând are loc evaluarea severității, impactului și clasificarea mai exactă a cazului. La această etapă cazul este suplimentat cu clarificării și detalii dar și cu referințe și înregistrări adiționale. Pentru cazurile critice se aplică escaladările necesare, se identifică un calendar accelerat de remediere și se colaborează cu organizația responsabilă în vederea obținerii măsurilor de remediere temporare și finale.
- Cazurile cu un calendar de remediere accelerat includ obligativitatea raportării progresului și eventualelor dificultăți apărute. Clarificările și detaliile adiționale dar și prezența măsurilor de remediere pot face necesară o re-evaluare a cazului.
- Divulgarea coordonată a cazului se face prin includerea unui plan de divulgare coordonată care include atât elemente calendaristice precum și aspecte de distribuire și limitare a accesului la informații sensibile.
- Participanții la caz pot face propuneri de modificare a planului de divulgare de care va ține cont echipa ASC.
- Divulgarea coordonată include o serie de acțiuni de protecție a informațiilor sensibile din caz dar și de formulare a unui mesaj clar privind informațiile divulgate. De asemenea, în baza riscului se decide informarea sectorului afectat pentru a lua măsurile de remediere și protecție necesare. Cu 3 zile înaintea divulgării publice a informației despre caz raportorul și organizația responsabilă sunt notificate.
- Închiderea cazului are loc când sunt întrunite condițiile necesare și acestea includ prezența măsurilor de remediere definitive, confirmarea acestora de către ASC, aplicarea acestor măsuri de părțile afectate dar și înregistrarea unei fișe privind închiderea cazului.

Obiecte informaționale

Din perspectiva informațională RSIC asigură crearea unei baze de date electronice naționale pentru

- incidente cibernetice,
- vulnerabilități și amenințări cibernetice

Diagrama de mai jos scoate în evidență aceste două obiecte informaționale cheie și suplimentează aceste obiecte cu:

- Document CSAF asigură interoperabilitatea în ramură privind amenințările și vulnerabilitățile,
- Document IODEF asigură interoperabilitatea în ramură privind incidentele cibernetice,
- Înregistrările sub forma de documente structurate sau ne-structurate imutabile stau la baza întregului sistem, inclusiv formulare, rapoarte dar și recomandări.
- Deși sistemul recepționează înregistrări din diferite surse, unele vulnerabilități, atenționări și toate incidentele de asemenea sunt înglobate în formă de caz asupra căruia reprezentanții ASC și a altor organizații relevante colaborează în vederea analizei, clarificării și soluționării acestora.
- Istoria tuturor modificărilor cazului dar și suplimentarea acestuia cu înregistrări adiționale sau corectate oferă context și trasabilitate pentru progresul în soluționarea cazului dar și pentru actualizarea înregistrărilor când pentru acestea avem detalii adiționale.
- Utilizatorii și echipele acestora formează lista părților autorizate să participe în lucrul sistemului.

- O serie explicită de tipuri de înregistrări ținute în sistem sub formă de document structurat este prezentată pentru a scoate în evidență multitudinea acestora.
- Colecții de articole/postări sunt ținute în sistem pentru informare bunelor practici, măsurilor de remediere, statisticilor și trendurilor în ramură dar și evoluția (coronologică) a anumitor crize/incidente.

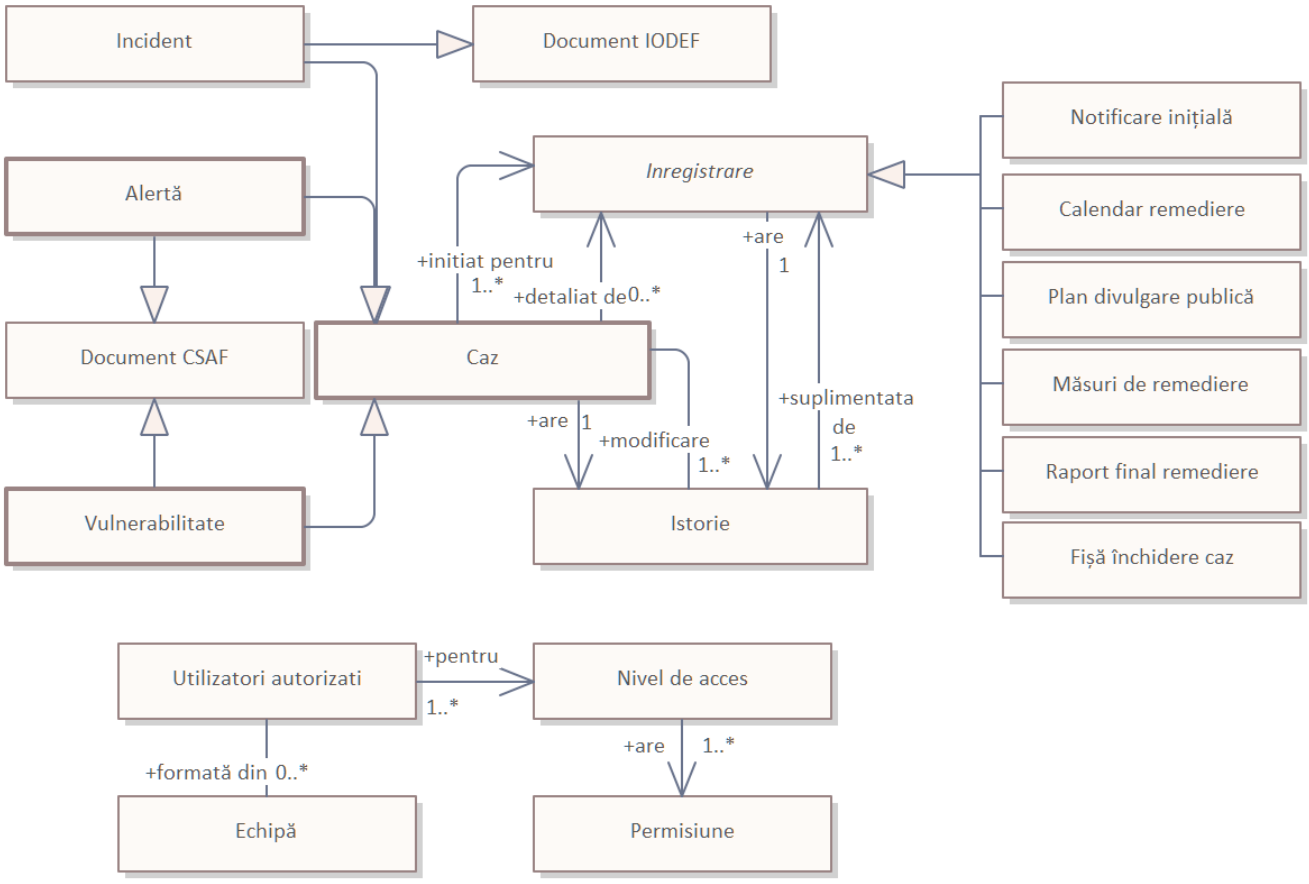

Fig. 5: Obiecte informaționale cheie

Model funcțional

Modelul funcțional descrie utilizarea sistemului printr-un ansamblu de interacțiuni și facilități care ating un obiectiv comun. Aici sunt identificați actorii și cazurile de utilizare (Use Case) ce stau la baza automatizării.

Compartimentul descrie funcțiile din perimetrul sistemului informatic inclusiv actorii interni și externi implicați. Diagrama ce urmează identifică grupurile de cazuri de utilizare cheie conform perimetrului RSIC. Acestea sunt detaliate în capitolele următoare.

Notă: Cazurile de utilizare din afara perimetrului sunt marcate cu stereotipul <<info>> și sunt incluse în text pentru context.

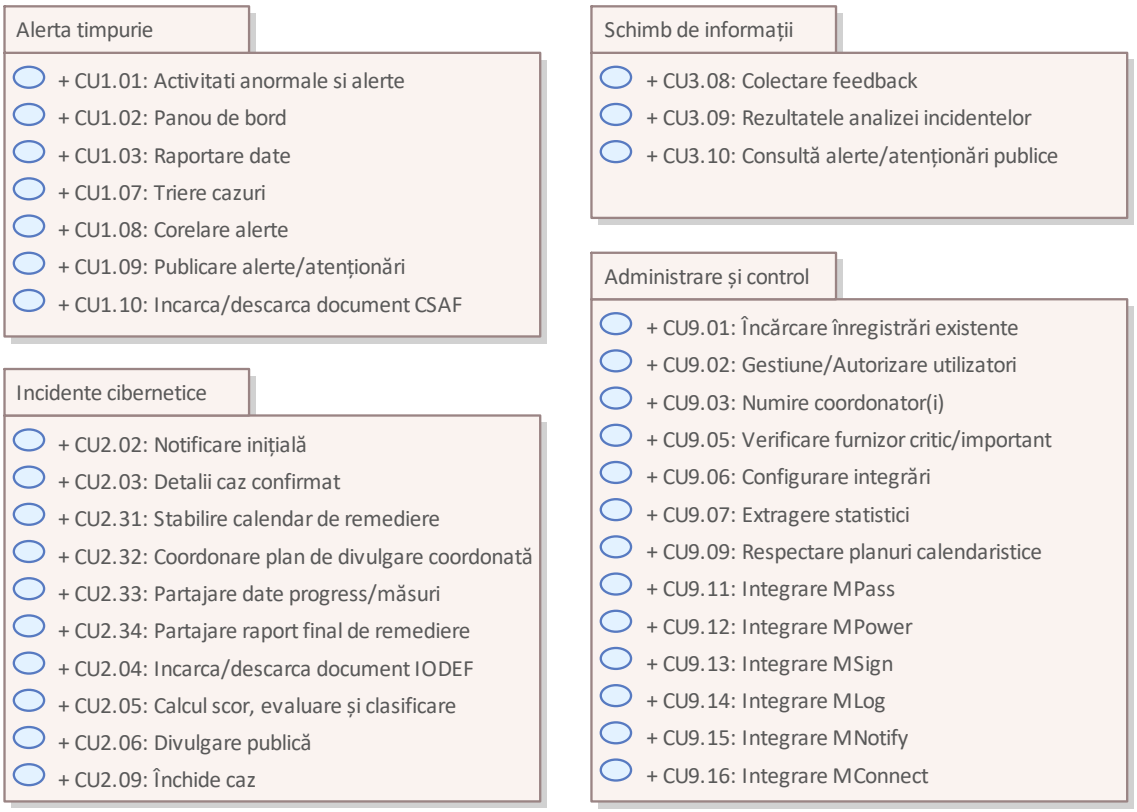

Fig. 6: Perimetrul RSIC

Actori

Capitolul dat identifică participanții la sistem - utilizatori umani, servicii de platformă și subsistemele informaționale cheie parte a sistemului.

Notă: Pentru ilustrare este utilizată diagrama actorilor în UML.

Diagrama scoate în evidență relația ierarhică dintre utilizatorii umani ai sistemului și anume:

- utilizatorii interni reprezentanți ai ASC (și STISC) au cele mai multe permisiuni
- Registratorii care reprezintă organizațiile responsabile și furnizorii identificați au un nivel de acces limitat informațiile și cazurile organizațiilor pe care le reprezintă
- Furnizori ai datelor au acces și mai redus constrâns doar la acele cazuri în care participă direct
- Destinatarii datelor reprezintă mediul de afaceri și publicul larg care consultă informațiile făcute publice de utilizatorii interni ai sistemului.

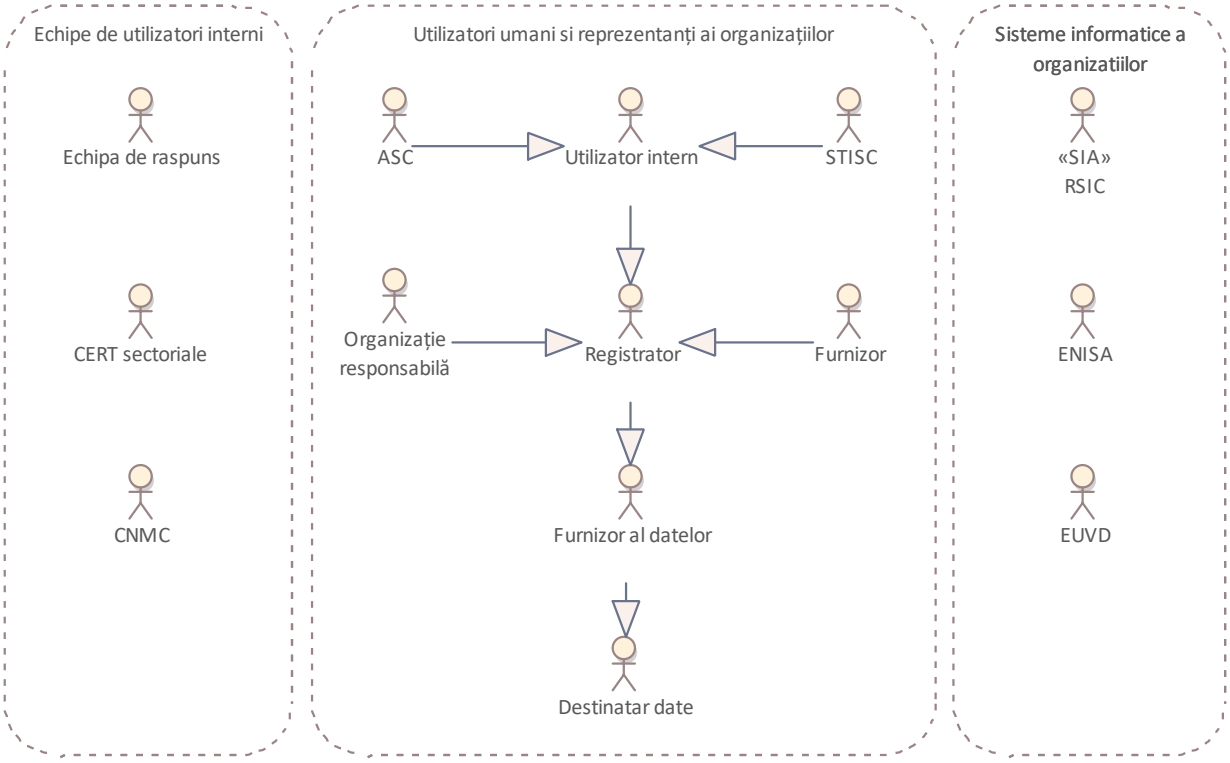

Fig. 7: Actori

ASC

Agenția de Securitate Cibernetică (prin intermediul reprezentanților acesteia)

STISC

Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică” (prin intermediul reprezentanților acesteia)

CNMC

Centrul Național de Management al Crizelor

RSIC *«SIA»*

Registrului de stat al incidentelor cibernetice ofera:

- o platformă de management al incidentelor cibernetice și de schimb de informații, în scopul cooperării cu echipele de răspuns la incidente cibernetice, precum și o platformă destinată intermedierii schimbului de informații între furnizorii de servicii și alte persoane juridice
- monitorizarea amenințărilor cibernetice, a vulnerabilităților și a incidentelor cibernetice la nivel național.

ENISA
Agenția Uniunii Europene pentru Cibersecuritate, ENISA, este agenția Uniunii dedicată atingerii unui nivel comun ridicat de securitate cibernetică în întreaga Europă.

https://www.enisa.europa.eu/about-enisa/what-we-do

EUVD
EU Vulnerability Database

https://euvd.enisa.europa.eu/homepage

Furnizor
Furnizorii de servicii din sectoare critice

Echipa de raspuns
Echipă de răspuns la incidente cibernetice la nivel național din ASC

Organizație responsabilă
Organizația care produce echipament sau software afectat de vulnerabilități și incidente cibernetice

CERT sectoriale
Echipele de răspuns la incidente cibernetice sectoriale

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

Registrator
Utilizator care operează, introduce sau modifică datele din cadrul SI RSIC, dar nu configurează funcționalitățile sistemului

Furnizor al datelor
Utilizator care asigură furnizarea informației, fără drepturi de a înregistra/modifica/șterge date din cadrul sistemului spre exemplu cercetător în securitatea cibernetică (organizație sau persoană individuală) care a descoperit vulnerabilități, riscuri sau comportamente malițioase și le raportează

Destinatar date
Utilizator care are acces la vizualizarea informației, fără drepturi de a introduce/modifica/șterge date din cadrul sistemului.

Alerta timpurie

Conturul „Sistem de alertă timpurie” include totalitatea procedurilor și sistemelor tehnice care au rolul de a identifica premisele de apariție a incidentelor cibernetice și de a avertiza în cazul producerii acestora. Prin funcționalul său se va asigura colectarea și sistematizarea datelor recepționate din partea entităților responsabile aferente activităților anormale parvenite din diferite surse, în scopul prelucrării ulterioare.

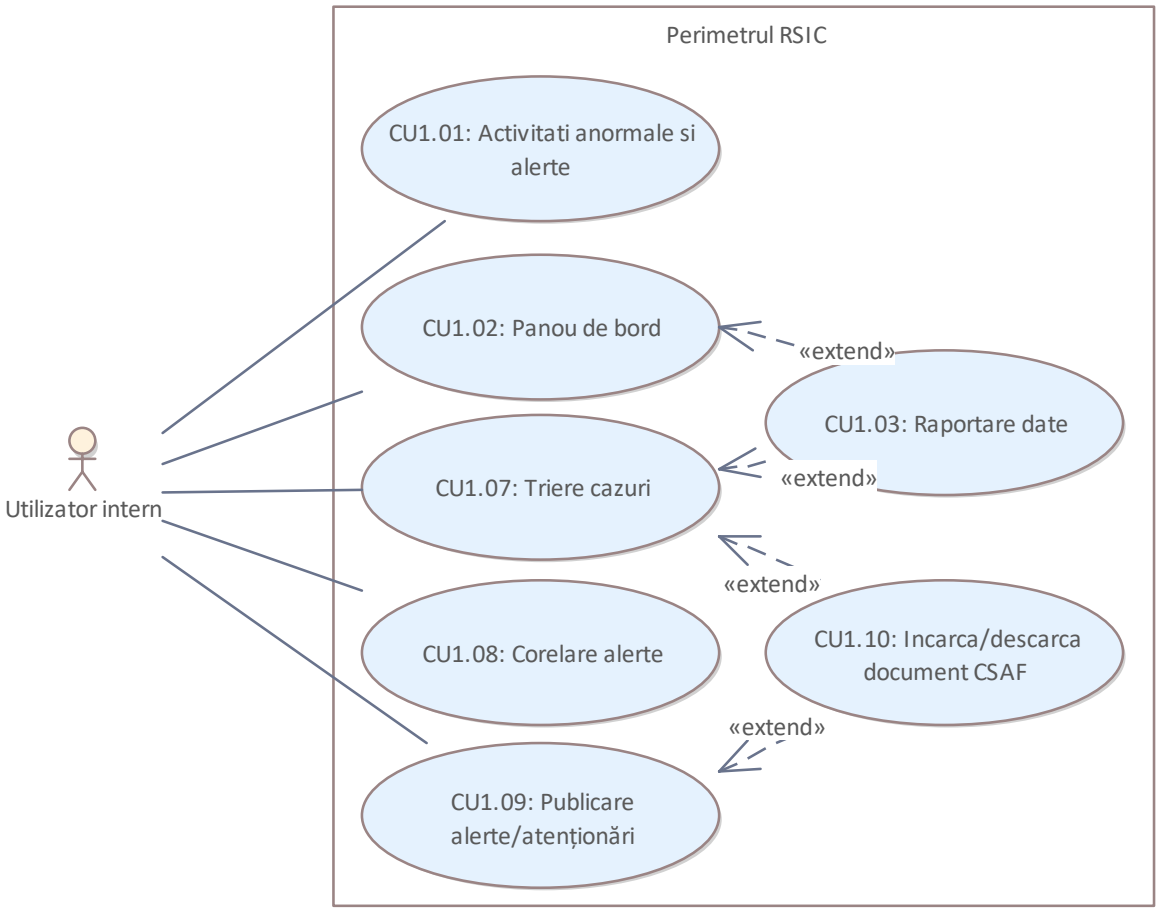

Fig. 8: Alerta timpurie

CU1.01: Activitati anormale si alerte

Sistemul înregistrează alertele și activitățile anormale. Aici este descrisă funcționalitatea oferită utilizatorilor ce permite examinarea înregistrărilor noi și existente inclusiv adăugarea de înregistrări noi conform formularului.

Condiții

- Utilizator autentificat prin MPass
- Utilizator reprezentant al ASC

Scenariu

Pas	Acțiune

1	Utilizator navighează la alerte și vulnerabilități
2	Sistem validează accesul utilizatorului și setează restricțiile aplicate
3	Sistem listează înregistrările din sistem conform preferințelor sau criteriilor de filtrare/sortare a utilizatorului
4	Utilizator crează înregistrare nouă manual *alternativa 4a:* ***Utilizator modifică criterii de filtrare/sortare*** *continuare la Final* *alternativa 4b:* ***Utilizator selectează înregistrare existentă*** *continuare la 5*
5	Sistem crează o înregistrare cu statut Nou, cu valori implicite a elementelor acesteia și prezintă formularul înregistrării inclusiv compartimentele și atributele colectate
6	Utilizator completează atributele compartimentului ales și trece la alte compartimente după caz *alternativa 6a:* ***Utilizator trece la alt compartiment a înregistrării*** *continuare la 6* *alternativa 6b:* ***Utilizator invită alți participanți*** *continuare la 6*
7	Sistem pastreaza modificările sub forma de înregistrare incompletă/temporară. Sistem evidențiază elementele obligatorii lipsă sau eronate
8	Utilizator confirmă completitudinea înregistrării
9	Sistem salvează datele
10	Sistem jurnalizează acțiune utilizator cu MLog
11	Utilizator închide/părăsește funcționalitatea *alternativa 11a:* ***Utilizator continuă lucrul cu lista*** *continuare la 2*

Utilizator trece la alt compartiment a înregistrării

Pas	Acțiune
1	Sistem afișează compartimentul selectat

Utilizator continuă lucrul cu lista

Pas	Acțiune
1	Sistem întoarce utilizator la început scenariu

Utilizator modifică criterii de filtrare/sortare

Pas	Acțiune
1	Sistem actualizează criteriile de filtrare și inversează criteriile de sortare după caz

Utilizator selectează înregistrare existentă

Pas	Acțiune
1	Sistem afișează datele din înregistrarea selectată inclusiv compartimentele existente a acesteia

Utilizator invită alți participanți

Pas	Acțiune
1	Sistem oferă posibilitatea de a invita utilizatori cunoscuți în sistem cu Nume sau Prenume, dar și alte persoane fizice și juridice indicând IDNP sau IDNO
2	Utilizator adaugă sau exclude din lista de participanți la caz și confirmă modificările
3	Sistem salvează lista de participanți actualizată (sub forma de listă de IDNx) și afișează nume/prenume acolo unde datele există în sistem
4	Sistem jurnalizează acțiune utilizator cu MLog

ID	De văzut și:	Statut
CF101	ENISA Threat Taxonomy se utilizează pentru clasificare cazuri	Obligatoriu
CF102	Detalii alerte/vulnerabilități conform CSAF	Obligatoriu
CF104	Datele obiectului informațional „alertă cibernetică”	Obligatoriu
CF105	Datele obiectului informațional „vulnerabilitate cibernetică”	Obligatoriu
CF115	Corelarea alertelor din diferite surse	Obligatoriu
CF116	Recepționare informații din diferite surse	Obligatoriu
CF121	Restrictionare/distribuire date conform TLP	Obligatoriu
CF126	Data ultimei sincronizări	Obligatoriu
CF127	Distribuire restricționată implicit	Obligatoriu
CF128	Încărcare date noi din CSAF	Obligatoriu
CF135	Atribute caz	Obligatoriu
CF139	Istorie caz	Obligatoriu
CF140	Notificări	Obligatoriu
CF231	Evaluare/clasificare caz conform CVSS	Obligatoriu

CU1.02: Panou de bord

Se oferă un panou de bord ce sumarizează 10-12 aspecte privind datele din sistem, spre exemplu:

- total inregistrări conform filtrelor
- total inregistrări distribuite calendaristic/după tip
- înregistrări noi ce n-au fost examinate/triate
- cazuri critice în progress (ne-soluționate)
- cazuri personale în derulare (unde utilizatorul e responsabil sau participant la caz) și statutul nu este închis
- cazuri cu cel mai putin timp rămas conform calendarului de remediere/divulgare
- formular de creare rapidă a unei înregistrări noi
- utilizatori cu cele mai multe cazuri în derulare

Fiecare din elementele tin panoul de bord este coordonat cu beneficiarul dar cel puțin oferă următoarele:

- top 10-15 elemente afișate
- set redus de coloane/atribute afișate
- posibilitatea de navigare la CU1.07/CU1.08 filtrate conform elementului din panou
- limitează conținutul afișat la înregistrări la care utilizatorul are acces

ID	De văzut și:	Statut
CNF186	Elemente panou de bord	Obligatoriu
CNF187	Panou de bord configurabil	Obligatoriu
CNF188	Panou de bord interactiv	Obligatoriu

CU1.03: Raportare date

Se oferă opțiunea de a afișa/salva elementele din panoul de bord și datele afișate sub formă de raport.

Adițional la elementele din panoul de bord se propun și se coordonează cu beneficiar alte 5 rapoarte (vizualizări).

Notă: Datele afișate sub formă de raport exclud din vizualizare elementele de interfață utilizator - butoane, câmpuri de date, elemente de navigare, fundaluri/ferestre etc.

ID	De văzut și:	Statut
CNF188	Panou de bord interactiv	Obligatoriu
CF249	Prezentarea datelor	Obligatoriu

CU1.07: Triere cazuri

Sistemul oferă facilități de listare, filtrare, sortare, regăsire, grupare a cazurilor conform solicitării utilizatorului.

Scenariu

Pas	Acțiune
1	Utilizator navighează la funcționalitatea de triere a cazurilor
2	Sistem prezintă lista cazurilor pentru criteriile specificate de utilizator
3	Utilizator examinează lista și ajustează criteriile de filtrare, sortare, grupare, paginare etc după caz *alternativa 3a:* ***Extrage datele*** *continuare la 2* *alternativa 3b:* ***Navigare la unul din cazuri*** *continuare la Final* *alternativa 3c:* ***Criterii de filtrare*** *continuare la 2* *alternativa 3d:* ***Paginare*** *continuare la 2* *alternativa 3e:* ***Coloane afișate*** *continuare la 2*
4	Sistem jurnalizează actiune utilizator și revine la pas 2

Extrage datele

Pas	Acțiune
1	Utilizator alege să extragă datele sub formă de tabel electronic, CSV sau HTML
2	Sistem extrage datele conform criteriilor utilizator și le oferă pentru a fi descărcate/salvate în formatul indicat de utilizator
3	Sistem jurnalizează acțiune utilizator

Navigare la unul din cazuri

Pas	Acțiune
1	Utilizator inițiază funcționaltate de vizualizare a detaliilor pentru un caz anume
2	Sistem afișează detalii și oferă utilizator opțiuni pentru pașii următori
3	[Invokes: CU1.08: Corelare alerte]
4	[Invokes: CU1.09: Publicare alerte/atenționări]
5	Utilizator modifică starea pozitivă, fals-pozitivă, incident sau radierea informației
6	Sistem jurnalizează acțiune utilizator cu MLog
7	Sistem notifică părțile implicate privind modificarea prin MNotify

Criterii de filtrare

Pas	Acțiune
1	Utilizator seteaza criterii de filtrare în baza datelor calendaristice, statut, evaluare și clasificare caz, persoanele responsabile etc

Paginare

Pas	Acțiune
1	Utilizatorul navighează prin paginile listei rezultative și indică numărul de cazuri afișate pe pagină

Coloane afișate

Pas	Acțiune
1	Utilizator selectează care din coloanele de date sunt afișate/ascunse la prezentarea rezultatelor

ID	De văzut și:	Statut
CF101	ENISA Threat Taxonomy se utilizează pentru clasificare cazuri	Obligatoriu
CF104	Datele obiectului informațional „alertă cibernetică”	Obligatoriu
CF105	Datele obiectului informațional „vulnerabilitate cibernetică”	Obligatoriu
CF107	Alertă pozitivă	Obligatoriu
CF108	Alertă fals-pozitivă	Obligatoriu
CF109	Alerta fals-pozitivă inchisă imediat	Obligatoriu
CF110	Alertă degenerată în incident cibernetic	Obligatoriu

ID	De văzut și:	Statut
CF113	Prezentare integrată a cazurilor corelate	Obligatoriu
CF123	Radiere caz	Obligatoriu
CF124	Notificarea permanentă privind modificarea	Obligatoriu
CF129	Actualizare date existente din fisier CSAF	Obligatoriu
CF132	Identificator AALLDD-XXXX	Obligatoriu
CF133	Cazuri personale	Obligatoriu
CF137	Responsabilii/participantii la caz	Obligatoriu
CF138	Comentarii și colaborare	Obligatoriu
CF139	Istorie caz	Obligatoriu
CF140	Notificări	Obligatoriu
CF231	Evaluare/clasificare caz conform CVSS	Obligatoriu
CNF181	Afișare paginată	Obligatoriu
CNF182	Coloane afișate în pagini	Obligatoriu
CNF183	Sortarea elementelor din pagini	Obligatoriu
CNF184	Evidențiere elemente	Obligatoriu
CNF185	Filtrare liste	Obligatoriu

CU1.08: Corelare alerte

Pentru alerte și amenințări provenite din diferite surse sistemul oferă facilități de corelare manuală a acestora cu scopul de a evidenția informația ce poate fi relevantă în analiza și soluționarea cazului.
Sistemul consideră următoarele situații:

- pentru o înregistrare nouă și una existentă (luată deja în evidență) în cazul corelării datele noi sunt comasate în înregistrarea deja existentă
- pentru înregistrări noi ce au identificator extern alocat, spre exemplu CVE - ambele înregistrări sunt comasate și luate la evidență împreună
- pentru înregistrări confirmate și identificate în sistem separat se formează o corelare permanentă unde datele din înregistrarea corelată sunt prezentate sumar pentru vizualizare
- pentru înregistrări noi sau existente ne-corelate dar care au atribute similare sistemul listează utilizatorului înregistrările date sub forma de candidați de corelare și oferă opțiunea de confirmare a corelării către utilizatori.
- utilizatorului î-i este oferită posibilitatea de a corela înregistrarea cu oricare alta deja luată în evidență în baza identificatorului public a acesteia, spre exemplu CVE sau identificatorului RSIC stabilit

Furnizor coordonează cu beneficiar criterile de similaritate a diferitor atribute dar acestea pot include spre exemplu:

- adresa IP sursa/destinație
- sub-rețeaua sursă/desitnație identificată prin CIDR
- data/ora înregistrării/raportării/desfășurării evenimentului înregistrat

Condiții

- Utilizator autentificat prin MPass
- Utilizator reprezentant al ASC
- Corelarea permisă doar dacă e permis accesul asupra tuturor elementelor corelate (alerte/incidente)

Scenariu

Pas	Acțiune
1	Utilizator navigează la o înregistrare
2	Sistem afișează detaliile despre înregistrare și oferă facilități de corelare *alternativa 2a:* ***Corelări confirmate existente*** *continuare la 2* *alternativa 2b:* ***Corelări candidat existente*** *continuare la 2*
3	Utilizator vizualizează (sumar) detaliile altor înregistrări similare
4	Utilizator confirmă o corelare cu alte înregistrări din sistem *alternativa 4a:* ***Corelare cu identificator public*** *continuare la 5*
5	Sistem salvează corelarea, consolidează datele din mai multe înregistrări după caz *alternativa 5a:* ***Una din înregistrări este nouă*** *continuare la 5*
6	Sistem jurnalizează acțiunea utilizator
7	Sistem notifică participanți prin MNotify privind corelarea
8	Utilizator finalizează lucrul *alternativa 8a:* ***Utilizator continuă lucrul cu înregistrarea curentă*** *continuare la 2*

Corelări confirmate existente

Pas	Acțiune
1	Sistem combină informația corelată și evidențiază originea acestora

Una din înregistrări este nouă

Pas	Acțiune
1	Sistem include detaliile din înregistrarea nouă ca informație adițională a înregistrării corelate luate deja în evidență (fără a atribui acesteia un identificator public RSIC etc).

Corelări candidat existente

Pas	Acțiune
1	Sistem listează sumar corelările candidat identificate conform adrese IP, segmente de rețea CIDR sau interval de timp și include posibilitatea de vizualizare sumară a detaliilor acestora

Corelare cu identificator public

Pas	Acțiune

1	Utilizator inițiază o corelare cu o înregistrare luată în evidență deja în baza identificatorului acesteia
2	Sistem propune utilizator să specifice identificatorului înregistrării existente cu care se va corela înregistrarea curentă, validează corectitudine identificatorului propus și existența înregistrării date în sistem

Utilizator continuă lucrul cu înregistrarea curentă

Pas	Acțiune
1	Sistem revine la pas inițial din scenariu

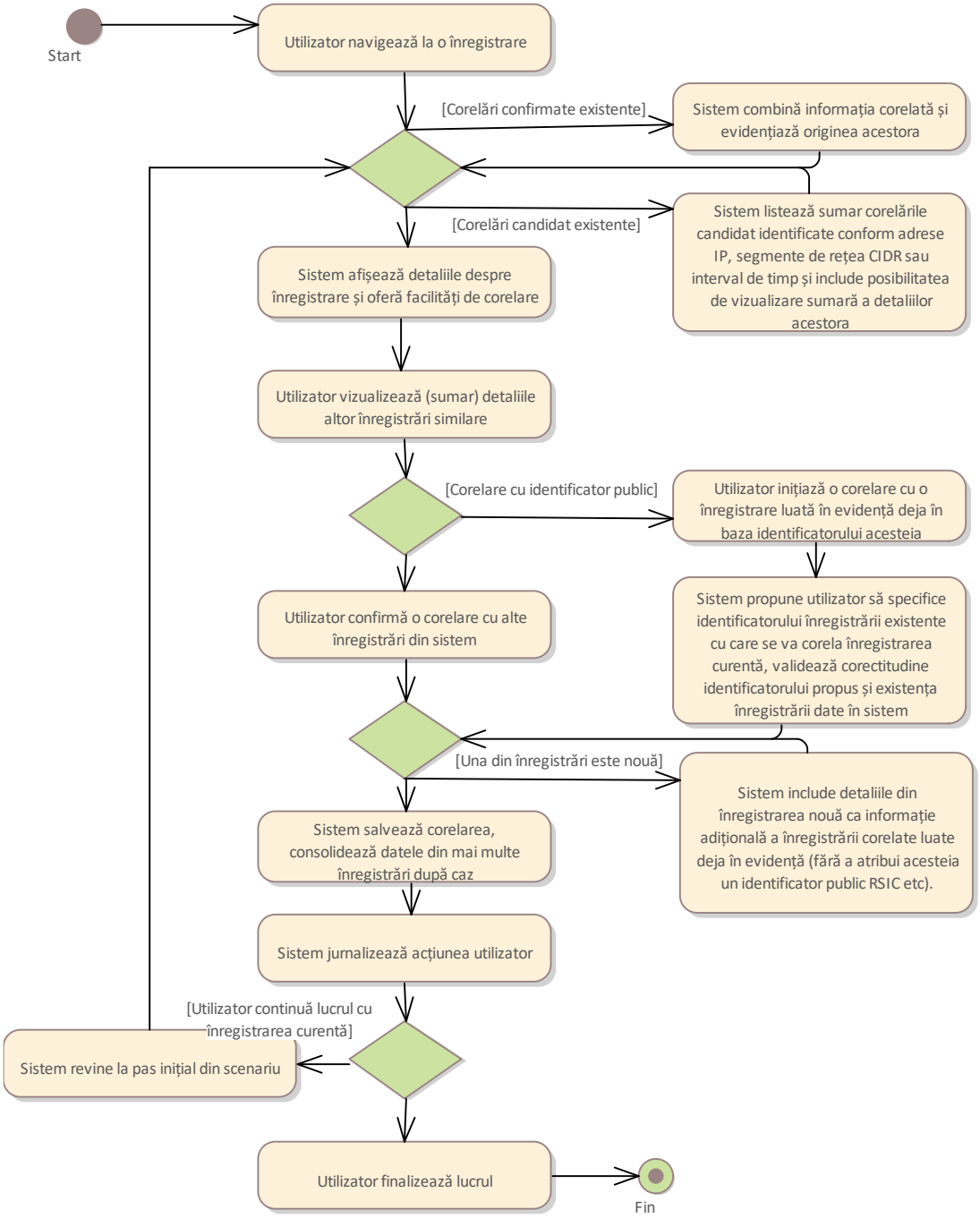

Fig. 9: CU1.08: Corelare alerte

ID	De văzut și:	Statut
CF105	Datele obiectului informațional „vulnerabilitate cibernetică”	Obligatoriu
CF110	Alertă degenerată în incident cibernetic	Obligatoriu
CF113	Prezentare integrată a cazurilor corelate	Obligatoriu
CF115	Corelarea alertelor din diferite surse	Obligatoriu
CF123	Radiere caz	Obligatoriu

ID	De văzut și:	Statut
CF124	Notificarea permanentă privind modificarea	Obligatoriu

CU1.09: Publicare alerte/atenționări

Sistemul facilitează publicarea alertelor și atenționărilor privind apariția unor activități premergătoare atacurilor cibernetice. Sistem oferă utilizatorului elementele de date ale înregistrării ce pot fi făcute publice. Pentru elementele de date restricționate sistem interzice publicarea. Elementele de date făcute publice sunt marcate cu nivelul de acces public (tlp:clear) conform protocolului TLP specificat la https://www.first.org/tlp/

Elementele publice din înregistrare devin publice doar atunci când înregistrarea propriu zisă (la nivel de rădăcină) este marcată corespunzător.

Condiții

- Utilizator autentificat prin MPass
- Marcarea cu tlp:clear este jurnalizată
- Înregistrarea este considerată publicată doar dacă este marcată corespunzător cu tlp:clear

Scenariu

Pas	Acțiune
1	Utilizator navighează la înregistrarea pentru publicare
2	Sistem afișează înregistrarea selectată și evidențiază nivelul de restricție a elementelor acesteia
3	Utilizator modifică nivelul de restricție a elementelor de date din înregistrare *alternativa 3a:* ***Utilizator finalizează lucrul*** *continuare la Final* *alternativa 3b:* ***Utilizator marchează înregistrarea publică*** *continuare la 4*
4	Sistem păstrează temporar modificările solicitate și continuă să accepte asemenea modificări de la utilizator
5	Utilizator confirmă setarea restricțiilor la nivelul ales *alternativa 5a:* ***Utilizator continuă modificări*** *continuare la 2*
6	Sistem păstrează permanent modificările indicate și jurnalizează acțiunea utilizator
7	Sistem notifică participanți prin MNotify privind modificarea

Utilizator continuă modificări

Pas	Acțiune
1	/continuare/

Utilizator finalizează lucrul

Pas	Acțiune
1	Sistem alertează utilizator că modificările temporare vor fi pierdute
2	Utilizator acceptă

Utilizator marchează înregistrarea publică

Pas	Acțiune
1	Sistem afișează valoarea tlp:clear și alertează utilizator că înregistrarea va deveni publică la salvarea modificărilor
2	Utilizator confirmă intenția

ID	De văzut și:	Statut
CF100	Aliniere model date la modelul EU	Obligatoriu
CF101	ENISA Threat Taxonomy se utilizează pentru clasificare cazuri	Obligatoriu
CF102	Detalii alerte/vulnerabilități conform CSAF	Obligatoriu
CF122	Elementele de date spre publicare	Obligatoriu
CF124	Notificarea permanentă privind modificarea	Obligatoriu
CF127	Distribuire restricționată implicit	Obligatoriu
CF127	Distribuire restricționată implicit	Obligatoriu

CU1.10: Incarca/descarca document CSAF

Sistemul oferă posibilitatea de a încărca/descărca detaliile despre alertă/vulnerabilitate în format CSAF:

- https://docs.oasis-open.org/csaf/csaf/v2.1/csaf-v2.1.html

La încărcare, pentru înregistrările deja existente în sistem detaliile acestuia sunt doar actualizate cu date noi din extras.

ID	De văzut și:	Statut
CF102	Detalii alerte/vulnerabilități conform CSAF	Obligatoriu
CF104	Datele obiectului informațional „alertă cibernetică”	Obligatoriu
CF105	Datele obiectului informațional „vulnerabilitate cibernetică”	Obligatoriu
CF128	Încărcare date noi din CSAF	Obligatoriu
CF129	Actualizare date existente din fisier CSAF	Obligatoriu
CF132	Identificator AALLDD-XXXX	Obligatoriu

Incidente cibernetice

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

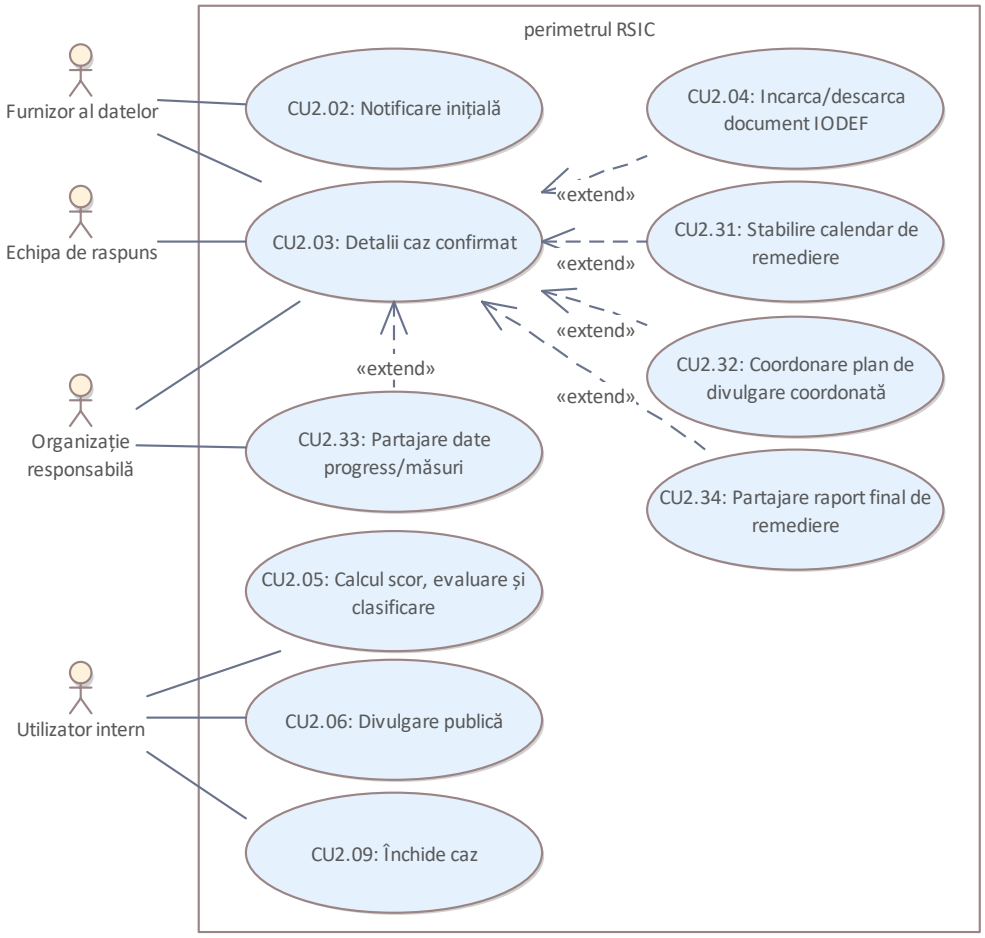

Fig. 10: Incidente cibernetice

CU2.02: Notificare inițială

Sistem oferă posibilitatea de captare și recepționare a unei notificări inițiale privind vulnerabilitatea, amenințarea sau incidentul conform formularului.

Informațiile remise includ

- date de contact raportor (opțional)
- organizația afectată
- descriere
- impactul asupra sistemului
- anomaliile observate

La notificarea inițială a incidentului informațiile raportate sunt păstrate cu posibilitatea acestora de a fi integrate ca informații adiționale al unui incident deja în lucru.

Scenariu

Pas	Acțiune
1	Utilizator autentificat sau anonim solicită depunerea unei notificări inițiale
2	Sistem prezintă compartimentele formularului și oferă utilizator completarea datelor obligatorii și opționale
3	Utilizator completează datele din compartimentele formularului și remite notificarea inițială
4	Sistem validează corectitudinea datelor prezentate, respectare formatului datelor și domeniului de valori, prezența datelor obligatorii și salveaza notificare inițială *alternativa 4a:* ***Erori în date*** *continuare la 2* *alternativa 4b:* ***Suspiciune de abuz*** *continuare la 4*
5	Sistem jurnalizează acțiune utilizator cu MLog
6	Sistem remite o notificare prin MNotify la persoana responsabilă de notificările inițiale și către organizația declarată afectată

Erori în date

Pas	Acțiune
1	Sistem evidențiază cîmpurile eronate și oferă utilizator posibilitatea de corectare a acestora

Suspiciune de abuz

Pas	Acțiune
1	Pentru încercarea de notificare repetată de același utilizator sau din rețele dubioase sistemul informează utilizator despre suspiciune și ilegalitatea abuzului
2	Sistem jurnalizează acțiunea abuzivă suspectată
3	Sistem propune utilizator un test de confirmare a validității informației remise
4	Utilizator rezolvă testul cu succes și continuă sau la abandonare notificare inițială nu este preluată în sistem

ID	De văzut și:	Statut
CF113	Prezentare integrată a cazurilor corelate	Obligatoriu
CF204	Punerea inițială în evidență	Obligatoriu
CF212	Formular de notificare	Obligatoriu
CF213	Conținut formular de notificare inițială	Obligatoriu
CF214	Notificare inițială	Obligatoriu
CF215	Protejare identitate raportor	Obligatoriu
CF216	Consimțământ privind identitate raportor	Obligatoriu
CF218	Primirea notificărilor securizat	Obligatoriu
CF219	Asistență raportorilor	Obligatoriu
CF220	Notificarea acceptată de la oricine	Obligatoriu
CF221	Confirmare recepționare notificare inițială	Obligatoriu

CU2.03: Detalii caz confirmat

Sistem afișează detalii caz, inclusiv istoria modificărilor și oferă posibilitatea utilizatorilor implicați în caz să contribuie detalii adiționale, să suplimenteze cazul cu înregistrări, să clasifice și să evalueze cazul conform diferitor seturi de caracteristici, inclusiv ENISA threat taxonomy sau TLP.

Utilizator navighează la această funcționalitate prin mijloacele de triere caz (UC1.07) sau direct conform identificatorului.

Condiții

- Utilizator autentificat prin MPass
- Utilizator administrativ al ASC
- Utilizator invitat să participe la caz

Scenariu

Pas	Acțiune
1	Utilizator navighează la informațiile despre caz *alternativa 1a:* ***Lista cazurilor*** *continuare la 1*
2	Sistem validează autorizația utilizator de a vizualiza cazul
3	Sistem ascunde datele ce nu corespund cu nivelul de distribuire aplicabil pentru utilizator
4	Utilizator examinează detalii caz și aplică modificări *alternativa 4a:* ***Adaugă/modifică înregistrări caz*** *continuare la 5* *alternativa 4b:* ***Adaugă/exclude participant*** *continuare la 5* *alternativa 4c:* ***Caz critic*** *continuare la 5* *alternativa 4d:* ***Inchide caz*** *continuare la 5* *alternativa 4e:* ***Caz radiat*** *continuare la 5*
5	Sistem actualizează istorie caz cu modificările aplicate
6	Sistem jurnalizează acțiune utilizator
7	Sistem informează participanți prin MNotify despre modificări
8	Utilizator continuă lucrul la caz (pas 4)

Adaugă/modifică înregistrări caz

Pas	Acțiune
1	Utilizator adaugă/modifică înregistrări (structurate) referitoare la caz ca spre exemplu măsuri de remediere, evenimente în calendar de remediere și plan de divulgare, raport final etc
2	Sistem notifică prin MNotify participanți la caz despre înregistrările făcute

Adaugă/exclude participant

Pas	Acțiune
1	Utilizator adaugă/exclude participant la caz sub forma de IDNP sau IDNO
2	Sistem notifică participanții noi despre caz prin MNotify

Caz critic

Pas	Acțiune
1	Utilizator apreciază cazul ca fiind Critic
2	Sistem propune escaladare caz către persoane și echipe responsabile de tratarea cazurilor critice
3	Utilizator identifică părțile către care este escaladat cazul
4	Sistem notifică părțile identificate prin MNotify

Inchide caz

Pas	Acțiune
1	[Invokes: CU2.06: Închide caz]

Caz radiat

Pas	Acțiune
1	Sistem solicită partajarea document confirmativ privind radiere
2	Utilizator partajează document confirmativ pentru radiere caz și confirmă radierea
3	Sistem setează starea Radiat a cazului și salvează documentul confirmativ partajat

Lista cazurilor

Pas	Acțiune
1	Sistem afișează lista paginată a cazurilor similar cu CU1.07
2	[Invokes: CU1.07: Triere cazuri]

ID	De văzut și:	Statut
CF100	Aliniere model date la modelul EU	Obligatoriu
CF101	ENISA Threat Taxonomy se utilizează pentru clasificare cazuri	Obligatoriu
CF102	Detalii alerte/vulnerabilități conform CSAF	Obligatoriu
CF110	Alertă degenerată în incident cibernetic	Obligatoriu
CF113	Prezentare integrată a cazurilor corelate	Obligatoriu
CF124	Notificarea permanentă privind modificarea	Obligatoriu
CF127	Distribuire restricționată implicit	Obligatoriu

ID	De văzut și:	Statut
CF135	Atribute caz	Obligatoriu
CF137	Responsabilii/participantii la caz	Obligatoriu
CF138	Comentarii și colaborare	Obligatoriu
CF139	Istorie caz	Obligatoriu
CF140	Notificări	Obligatoriu
CF201	Model de date aliniat la cerințele HG 822 și standardelor UE	Obligatoriu
CF202	Model de date conform IODEF	Obligatoriu
CF203	Motiv escaladare	Obligatoriu
CF204	Punerea inițială în evidență	Obligatoriu
CF205	Identificatorii obiectelor informaționale	Obligatoriu
CF206	Transmiterea în arhiva	Obligatoriu
CF211	Cazurile critice pot fi escaladate către CNMC	Obligatoriu
CF215	Protejare identitate raportor	Obligatoriu
CF216	Consimțământ privind identitate raportor	Obligatoriu
CF217	Confirmare plan de divulgare	Obligatoriu
CF222	Implicare CERT-Gov la necesitate	Obligatoriu
CF223	Notificarea recepționată de la organizația responsabilă	Obligatoriu
CF224	Notificări critice incomplete	Obligatoriu
CF225	Condiții de situație critică	Obligatoriu
CF226	Suplimentare notificări incomplete în maximum 2 zile	Obligatoriu
CF227	Completare notificare din oficiu	Obligatoriu
CF228	Informare sector în maximum 2 ore pentru cazuri critice	Obligatoriu
CF229	Calendar accelerat de remediere și divulgare pentru cazuri critice	Obligatoriu
CF230	Grupare cazuri identice/repetate	Obligatoriu
CF232	Nivelul cazurilor/vulnerabilităților	Obligatoriu
CF249	Prezentarea datelor	Obligatoriu
CNF181	Afișare paginată	Obligatoriu
CNF182	Coloane afișate în pagini	Obligatoriu
CNF183	Sortarea elementelor din pagini	Obligatoriu
CNF184	Evidențiere elemente	Obligatoriu
CNF185	Filtrare liste	Obligatoriu

CU2.31: Stabilire calendar de remediere

Sistemul oferă posibilitatea de a crea și ține un calendar de remediere în conformitate cu severitatea cazului. Șabloane de calendar accelerat și normal sunt oferite pentru cazuri critice și non-critice ca punct de start pentru crearea calendarului. Calendarul creat este utilizat pentru monitorizare progres și informare/notificare părți privind detaliile, clarificările, măsurile de remediere propuse etc.

ID	De văzut și:	Statut
CF224	Notificări critice incomplete	Obligatoriu
CF225	Condiții de situație critică	Obligatoriu

ID	De văzut și:	Statut
CF229	Calendar accelerat de remediere și divulgare pentru cazuri critice	Obligatoriu
CF234	Conținut plan/calendar de remediere	Obligatoriu
CF235	Informare periodică privind progresul	Obligatoriu

CU2.32: Coordonare plan de divulgare coordonată

Sistemul oferă posibilitatea de a iniția și ține un plan (calendaristic) de divulgare coordonată, inclusiv demarcarea datelor sensibile ce sunt partajate doar limitat către alte părți afectate din ramură/sector. Demarcarea datelor cu distribuire limitată utilizează TLP.

Dacă un plan de divulgare coordonată a fost creat pentru caz atunci sistemul notifică reprezentantul ASC despre diferitele măsuri ce urmează a fi întreprinse în baza acestui plan dar și organizația responsabilă si raportorul despre calendarul agreat. Propuneri de ajustare a planului de divulgare coordonată pot fi remise de participanți. Ajustări la plan se fac conform situației reale de către reprezentanții ASC.

Condiții

- Planul este creat de reprezentanții ASC
- Planul este actualizat/sters de reprezentanții ASC

ID	De văzut și:	Statut
CF217	Confirmare plan de divulgare	Obligatoriu
CF224	Notificări critice incomplete	Obligatoriu
CF225	Condiții de situație critică	Obligatoriu
CF228	Informare sector în maximum 2 ore pentru cazuri critice	Obligatoriu
CF229	Calendar accelerat de remediere și divulgare pentru cazuri critice	Obligatoriu
CF237	Momentul și forma divulgării	Obligatoriu
CF241	Notificare în avans privind divulgarea publică	Obligatoriu
CF243	Consultarea prealabilă a autorității sectoriale	Obligatoriu
CF247	Propuneri de ajustare plan remediere/divulgare	Obligatoriu

CU2.33: Partajare date progress/măsuri

Sistemul oferă posibilitatea de a suplimenta cazul de către persoana responsabilă privind progresul și măsurile intermediare/finale de remediere. Progresul și măsurile de remediere sunt actualizate cu periodicitatea stabilită în calendarul de remediere. De exemplu, pentru cazurile critice periodicitatea de actualizare este la fiecare 2 ore (inclusiv în afara orelor de lucru).

Condiții

- Utilizator autentificat prin MPass
- Utilizator reprezintă organizația responsabilă

ID	De văzut și:	Statut
CF234	Conținut plan/calendar de remediere	Obligatoriu

ID	De văzut și:	Statut
CF235	Informare periodică privind progresul	Obligatoriu

CU2.34: Partajare raport final de remediere

Sistemul oferă posibilitatea de a suplimenta cazul de către persoana responsabilă privind raportul final de remediere, inclusiv modul de validare/testare a acestora. Partajarea raportului final de remediere este notificată de sistem prin MNotify către toți participanții numiți la caz.

ID	De văzut și:	Statut
CF236	Conținut raport final de remediere	Obligatoriu
CF236	Raport final de remediere	Obligatoriu
CF249	Prezentarea datelor	Obligatoriu

CU2.04: Incarca/descarca document IODEF

Sistemul oferă posibilitatea de a încărca/descărca detaliile despre incident în format IODEF versiunea 2 dar și extensia acestuia IODEF-SCI. Acestea sunt specificate ca RFC 7970 și RFC 7203:

- https://www.rfc-editor.org/rfc/rfc7970
- https://www.rfc-editor.org/rfc/rfc7203.html

Pentru incidentele deja existente în sistem detaliile acestuia sunt doar actualizate cu date din fisierul încărcat.

CU2.05: Calcul scor, evaluare și clasificare

Severitatea și impactul unei vulnerabilități sau al unui incident este determinată utilizând practici standard în ramură ca spre exemplu CVSS 4.0 specificat la:

https://www.first.org/cvss/v4.0/specification-document

Sistem include funcționalitate de validare a severității și impactului cazului în corespundere cu scorul indicat și evidențiază discrepanțele după caz. Spre exemplu un caz de severitate joasă sau normală contrazice un scor ce depășește 7 din 10. Totuși sistemul nu automatizează calculul scorului, evaluarea și clasificarea cazului. Aceste aspecte rămân în responsabilitatea utilizatorului uman.

ID	De văzut și:	Statut
CF101	ENISA Threat Taxonomy se utilizează pentru clasificare cazuri	Obligatoriu
CF102	Detalii alerte/vulnerabilități conform CSAF	Obligatoriu
CF113	Prezentare integrată a cazurilor corelate	Obligatoriu
CF231	Evaluare/clasificare caz conform CVSS	Obligatoriu
CF232	Informare raportor și organizație responsabilă despre evaluare	Obligatoriu
CF233	Termenul de evaluare și clasificare	Obligatoriu

CU2.06: Divulgare publică

Sistem include un plan de divulgare publică pentru cazurile evaluate că necesită asemenea acțiune. Totuși, divulgarea publică se face doar pentru informațiile marcate cu tlp:clear conform TLP.

Similar cu CU1.09, sistemul facilitează specificarea distribuției informațiilor din cazul spre divulgare. La data indicată în planul de divulgare coordonată cazul dat (informațiile publice) devine accesibil public prin intermediul CU3.11.

Condiții

- Utilizator reprezentant al ASC
- Utilizator autentificat prin MPass

Scenariu

Pas	Acțiune
1	[Invokes: CU1.09: Publicare alerte/atenționări]

ID	De văzut și:	Statut
CF237	Momentul și forma divulgării	Obligatoriu
CF238	Divulgare doar descriere generală a vulnerabilității	Obligatoriu
CF239	Decizie de divulgare fără remediere	Obligatoriu
CF240	Decizia de divulgare se adoptă pe baza unei evaluări documentate	Obligatoriu
CF241	Notificare în avans privind divulgarea publică	Obligatoriu
CF242	Divulgare fără notificare în avans a părților	Obligatoriu
CF243	Consultarea prealabilă a autorității sectoriale	Obligatoriu

CU2.09: Închide caz

Sistem urmărește stabilirea măsurilor finale de remediere dar și remiterea de către partea responsabilă a unui raport final de remediere și a concluziilor/recomandărilor. Reprezentanții ASC validează informațiile raportate și coordonează închidere caz cu raportorul și alte părți implicate.

Condiții

- Utilizator reprezintă ASC
- Utilizator autentificat prin MPass

Scenariu

Pas	Acțiune
1	Utilizator navighează la caz și completează înregistrări necesare pentru închidere caz, inclusiv validare raport final de remediere și fișa de închidere caz *alternativa 1a: **Abandonare acțiune** continuare la Final*
2	Sistem validează corectitudinea înregistrărilor și salvează

3	Sistem jurnalizează acțiune utilizator
4	Sistem permite închidere caz *alternativa 4a:* ***Alte modificări*** *continuare la Final*
5	Utilizator solicită închidere caz
6	Sistem primește confirmare închidere caz de la utilizator, validează corectitudine înregistrări pentru soluționare caz și persistă cazul închis *alternativa 6a:* ***Erori de validare*** *continuare la 1* *alternativa 6b:* ***Utilizator refuză confirmare*** *continuare la 4*
7	Sistem jurnalizează acțiune utilizator cu MLog
8	Sistem notifică raportor despre inchidere caz prin MNotify

Erori de validare

Pas	Acțiune
1	Sistem informează utilizator despre prezența erorilor în date, evidențiază erorile în date, compartimentele cazului și înregistrările asociate

Utilizator refuză confirmare

Pas	Acțiune
1	/retur/

Alte modificări

Pas	Acțiune
1	[Invokes: CU2.03: Detalii caz confirmat]

Abandonare acțiune

Pas	Acțiune
1	Utilizator abandonează acțiunea inițiată prin navigare altundeva în sistem sau prin închidere pagină
2	Sistem abandonează orice modificări incomplete

ID	De văzut și:	Statut
CF109	Alerta fals-pozitivă inchisă imediat	Obligatoriu
CF113	Prezentare integrată a cazurilor corelate	Obligatoriu
CF206	Transmiterea în arhiva	Obligatoriu
CF209	Caz închis prin solicitare CNMC	Obligatoriu
CF210	Arhivare cazuri închise	Obligatoriu

ID	De văzut și:	Statut
CF236	Raport final de remediere	Obligatoriu
CF244	Condiții pentru a închide caz	Obligatoriu
CF245	Fișa de închidere caz înregistrată la închidere	Obligatoriu
CF246	Conținut fișa de închidere caz	Obligatoriu

Schimb de informații

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

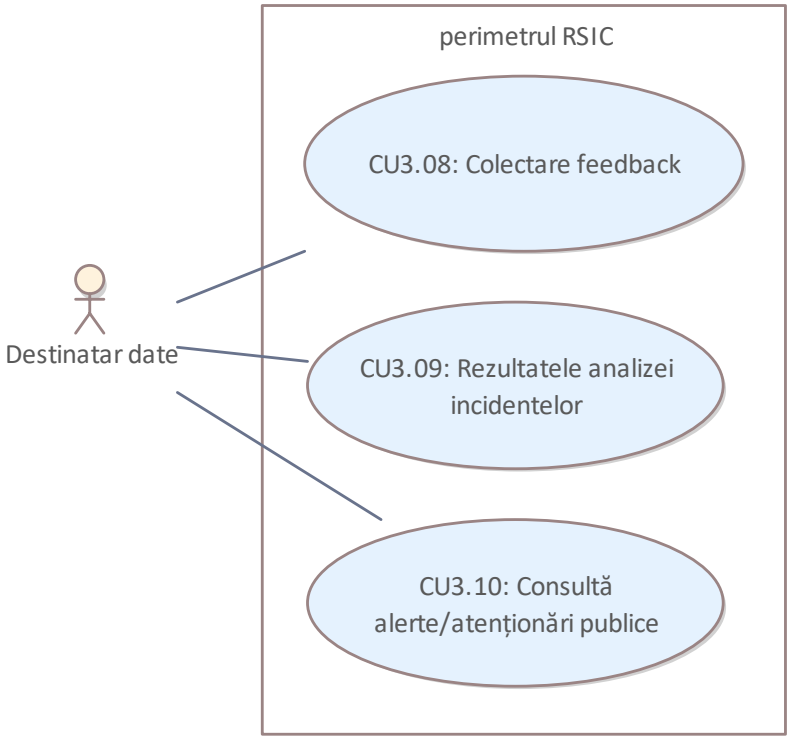

Fig. 11: Schimb de informații

CU3.08: Colectare feedback

Stabilirea unui responsabil de colectare feedback despre eveniment în vederea informării raportului despre incident dar și privind lecțiile învățate și recomandărilor privind incidentele și altor evenimente (ca spre exemplu teste, instruiri sau bune practici).

Adițional sistemul oferă opțiunea de a partaja opinii și recomandări, inclusiv anonime, privind procesul de divulgare coordonată, interacțiunea părților și propunerilor de îmbunătățire.

Condiții

- Solicitare feedback permisă coordonatorului pentru cazuri închise
- Completare formular de feedback permisă participanților la caz

Scenariu

Pas	Acțiune

1	Coordonator caz inițiază colectarea părerilor și propunerilor (feedback) privind cazul indicând un subset din persoanele implicate în caz
2	Sistem salvează datele și jurnalizează acțiune utilizator
3	Sistem remite notificări individuale prin MNotify privind solicitarea de feedback, adresa formularului și cazul vizat pentru persoanele indicate
4	Utilizator navighează la formularul de feedback și-l completează asigurându-se că se face referire la caz
5	Sistem validează permisiuni utilizator și corectitudine date din formular și salvează feedbackul remis cu referire la caz
6	Sistem jurnalizeaza acțiune utilizator

ID	De văzut și:	Statut
CF307	Colectare opinii și recomandări	Obligatoriu
CF313	Destinatar date	Obligatoriu
CF314	Coordonator caz poate iniția colectarea feedbackului de la participanți	Obligatoriu
CF315	Feedback anonim	Obligatoriu
CF316	Formular feedback	Obligatoriu
CF317	Reflectarea în istorie caz	Obligatoriu
CF318	Reflectare în statistici	Obligatoriu

CU3.09: Rezultatele analizei incidentelor

Se ține o colecție de rapoarte și se asigură comunicarea informațiilor privind rezultatele analizei incidentelor cibernetice, cu respectarea prevederilor acordurilor de cooperare. Rezultatele analizei pot face referire la unul sau mai multe cazuri/incidente/vulnerabilități din RSIC sau pot fi de totalizare.

Condiții

- Acces deplin pentru reprezentanți ASC
- Acces de citire pentru utilizatori anonimi/ne-autorizați

Scenariu

Pas	Acțiune
1	Utilizator intern crează o analiză a incidentelor cibernetice, atașează materiale (imagini, fișiere externe (pdf etc)), referire la cazuri din RSIC și salvează datele
2	Sistem validează datele, stochează materialele atașate și salvează materialul
3	Sistem jurnalizează acțiune utilizator
4	Utilizator solicită publicare material ca Rezultate a analizei incidentelor și confirmă solicitare
5	Sistem marchează materialul ca fiind publicat și deschide accesul pentru destinatarii datelor
6	Sistem jurnalizează acțiune utilizator
7	Sistem adaugă în istoria cazurilor din referințe înregistrări către materialul publicat

8	Destinatar date navighează la material din colecție și-l vizualizează
9	Sistem jurnalizează acțiune utilizator
10	Sistem include date despre vizualizare în statistici

ID	De văzut și:	Statut
CF302	Se asigură comunicarea rezultatelor analizei incidentelor cibernetice	Obligatoriu
CF307	Colectare opinii și recomandări	Obligatoriu
CF311	ASC crează și publică rezultate a analizei incidentelor	Obligatoriu
CF312	Rezultate analiză incidente informat de feedback-ul partajat	Obligatoriu
CF318	Reflectare în statistici	Obligatoriu
CF319	Rezultatele analizei incidentelor în istoria caz	Obligatoriu
CF320	Rezultatele analizei incidentelor accesibile pentru destinatari date	Obligatoriu
CF320	Rezultatele analizei incidentelor accesibile pentru destinatari date	Obligatoriu
CF321	Rezultatele analizei incidentelor pot fi publicate sau retrase de utilizatori interni	Obligatoriu
CNF181	Afișare paginată	Obligatoriu
CNF183	Sortarea elementelor din pagini	Obligatoriu
CNF185	Filtrare liste	Obligatoriu

CU3.10: Consultă alerte/atenționări publice

Sistemul facilitează accesul public la informații publice, inclusiv alerte, atenționări, amenințări, riscuri, vulnerabilități, rapoarte privind incidentele etc.

Restricționarea la elementele de date din structura ierarhică a înregistrării conform TLP sunt următoarele:

- tlp:red - utilizatori identificați personal ca participanți la caz
- tlp:amber sau tlp:amber+strict - utilizatori ce reprezintă organizații numite personal ca participanți la caz
- tlp:green - utilizatori cunoscuți de sistemul RSIC
- tlp:clear - oricare utilizator inclusiv vizitatori anonimi ai RSC

Condiții

- Utilizator autentificat prin MPass

Scenariu

Pas	Acțiune
1	Utilizator navighează la înregistrare
2	Sistem decide nivelul de acces pe care îl are utilizator conform protocol TLP
3	Sistem afișează doar acele elemente de date conform nivelului de acces determinat în ordine top-down
4	Sistem jurnalizează acțiune utilizator
5	Sistem contorizează accesul în statistici

ID	De văzut și:	Statut
CF100	Aliniere model date la modelul EU	Obligatoriu
CF101	ENISA Threat Taxonomy se utilizează pentru clasificare cazuri	Obligatoriu
CF102	Detalii alerte/vulnerabilități conform CSAF	Obligatoriu
CF121	Restrictionare/distribuire date conform TLP	Obligatoriu
CF122	Elementele de date spre publicare	Obligatoriu
CF249	Prezentarea datelor	Obligatoriu
CF301	Informare privind riscurile cibernetice	Opțional
CF313	Destinatar date	Obligatoriu
CNF181	Afișare paginată	Obligatoriu
CNF183	Sortarea elementelor din pagini	Obligatoriu
CNF185	Filtrare liste	Obligatoriu

Administrare și control

Conturul „Administrare și control” asigură administrarea și integritatea bazei de date, păstrarea istoriei acțiunilor în sistem, monitorizarea performanței, configurarea accesului, integrarea și sincronizarea cu alte surse de date etc.

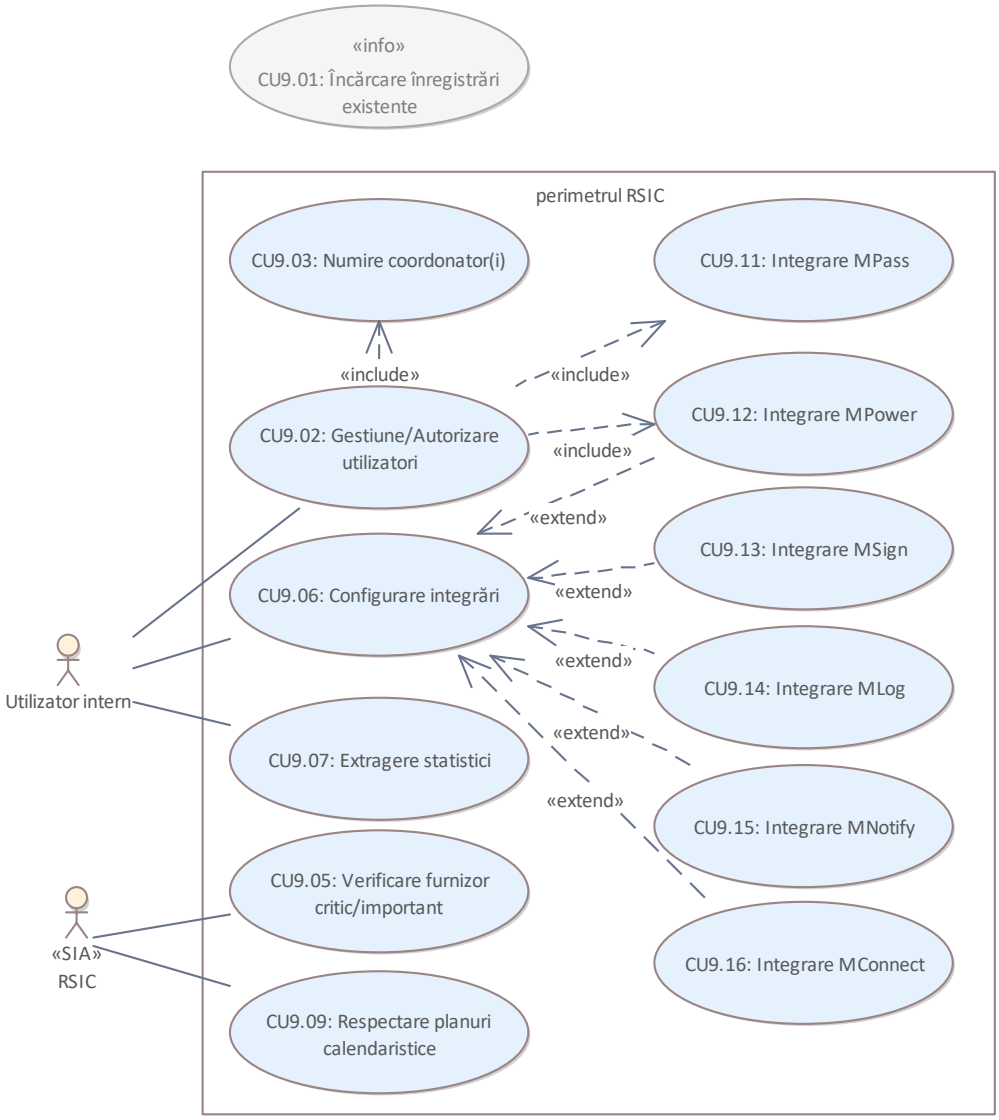

Fig. 12: Administrare și control

CU9.01: Încărcare înregistrări existente *«info»*

Datele și înregistrările existente NU sunt încărcate în RSIC la momentul implementării. La necesitate, utilizatorii vor încărca manual minimul necesar de date despre cazuri existente în vederea stabilirii legăturilor cu cazuri noi.

CU9.02: Gestiune/Autorizare utilizatori

Sistem ține liste de utilizatori autorizați în principal componenți a echipelor de intervenție din partea ASC și STISC. Alte roluri privind responsabilii și punctele de contact pentru escaladare pot fi incluse în aceste

liste. Listele propriu zise includ IDNP și IDNO. Detalii despre aceste persoane pot fi captate si actualizate la întrarea în sistem a acestor persoane.

Echipe de utilizatori pot fi formate pentru a facilita atragerea și implicarea acestora în soluționarea cazurilor fără a fi necesară indicarea nominală a acestora (mai ales în situații de crize).

Roluri/Nivele de acces sunt definite în sistem pentru a facilita acordarea unor seturi de permisiuni în acest mod facilitând acordarea de permisiuni multiple. Permisiunile sunt alocate individual sau în baza de roluri.

Notă: Funcționalitatea dată se recomandă a fi realizată în baza unor librării/soluții existente de RBAC suplimentate de identități în bază de IDNP/IDNO.

Important! MPass asigură autentificarea identității, MPower asigură verificarea dreptului de reprezentare atunci când utilizatorul acționează în numele unei persoane juridice, iar SI RSIC gestionează doar rolurile funcționale, permisiunile de business și regulile de acces la obiectele informaționale. Se va exclude instituirea unor conturi locale sau mecanisme paralele de acces.

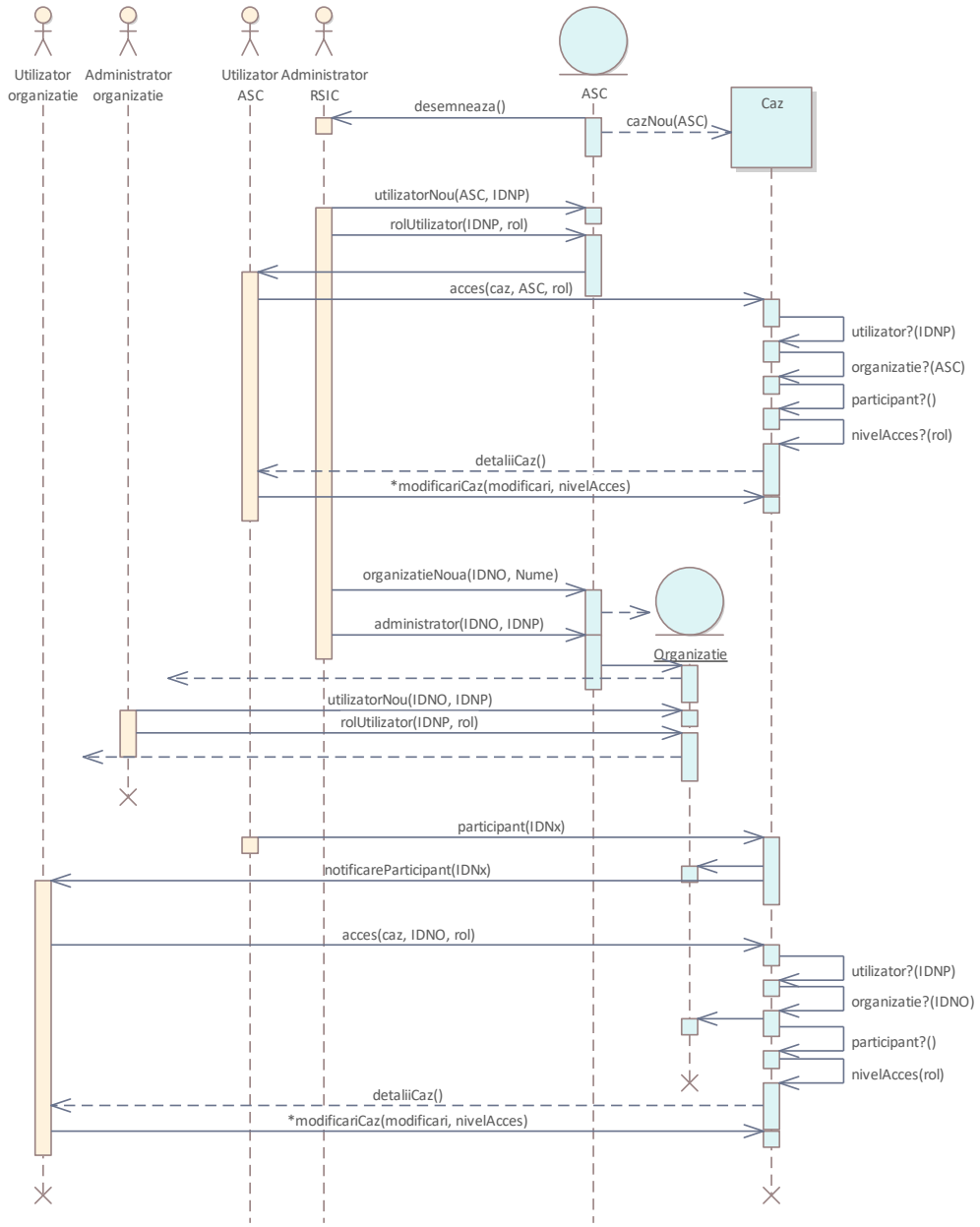

Fig. 13: CU9.02: Gestiune/Autorizare utilizatori

Diagrama de secvență ilustrează la nivel înalt următoarele aspecte:

- ASC ca organizație stă la baza sistemului
- Funcțiile administrative dar și cazurile noi luate la evidență în sistem sunt create în contextul organizațional al ASC
- Utilizatorii ASC sunt gestionați de administratorul RSIC în contextul organizațional ASC
- Autorizarea utilizatorilor ASC și accesul la cazuri este disponibilă în contextul organizațional
- Alte organizații pot fi adăugate explicit de Administratorul RSIC și chiar permisiunea de administrare a utilizatorilor acestei organizații poate fi delegată unei persoane din această organizație
- Utilizatorii organizației date sunt autorizați doar în limita implicării organizației date
- Implicarea organizațiilor și utilizatorilor acestor organizații se face explicit de utilizatori ce reprezintă ASC prin includerea acestora ca participanți la caz
- Verificarea accesului urmează aceiași procedură de validare a utilizatorului în baza IDNP, stabilire a organizației pe care utilizatorul o reprezintă, verificarea includerii utilizatorului și/sau organizației în lista de participanți și stabilirea nivelului de acces acordat în baza rolului utilizator

ID	De văzut și:	Statut
CF901	Autentificare utilizatori	Obligatoriu
CF902	Utilizatori autorizați	Obligatoriu
CF903	Echipe dedicate	Obligatoriu
CF908	Limitare acces	Obligatoriu
CF909	Dreptul de acces poate fi limitat, suspendat sau retras	Obligatoriu
CF911	Delimitare acces	Obligatoriu
CF920	Roluri pentru gestiune acces	Obligatoriu
CF921	Control acces	Obligatoriu
CF922	Limitare acces	Obligatoriu
CNF181	Afișare paginată	Obligatoriu
CNF183	Sortarea elementelor din pagini	Obligatoriu
CNF185	Filtrare liste	Obligatoriu

CU9.03: Numire coordonator(i)

Sistem păstrează o listă de coordonatori care sunt implicați în regim automat în soluționarea cazurilor. Lista include o persoană desemnată coordonator implicit. Adițional lista poate include coordonatori pentru:

- cazuri critice
- cazuri noi
- incidente, alerte și vulnerabilități
- cazuri clasificate conform ENISA threat taxonomy

Furnizor coordonează cu beneficiar aceste și alte desemnări de coordonatori după caz.

CU9.05: Verificare furnizor critic/important

Acest proces este susținut de un subsistem informațional automatizat al ASC extern acestui sistem.

La conectarea unui reprezentant al organizațiilor din MD sau la remiterea unor documente din partea acestor organizații sistemul verifică dacă organizația dată este un furnizor de servicii critice/importante din Lista furnizorilor de servicii.

Verificarea se face prin consumarea unui serviciu prestat de aplicația dată. Detaliile de integrare sunt coordonate cu beneficiarul.

CU9.06: Configurare integrări

Sistem oferă facilități de configurare/actualizare a setărilor necesare pentru funcționarea integrărilor. Spre exemplu se poate indica URL pentru serviciul producție sau test, coduri de acces, credențiale utilizate etc.

CU9.07: Extragere statistici

Sistemul include un tabel virtual (view) în baza de date și documentează modalitatea de conectare la aceasta cu instrumente de tip tabel electronic.

ID	De văzut și:	Statut
CF318	Reflectare în statistici	Obligatoriu
CF914	Statistici	Obligatoriu

CU9.09: Respectare planuri calendaristice

Sistemul include facilități automate de control a respectării planurilor calendaristice atasate cazurilor și anume:

- notificare coordonator și responsabil caz privind iminența limitei de timp agreate
- înregistrare în caz, istorie și jurnal faptul depășirii limitelor de timp agreate

De notat că iminența limitei de timp este (configurabil) de 10-15 min pentru actualizările periodice privind progresul de soluționare cazuri critice și de 4-24 ore pentru data/ora agreată de remediere a cazurilor non-critice.

ID	De văzut și:	Statut
CF131	Procesele repetate periodic în format cron	Obligatoriu
CF915	Iminența limitei de timp pentru planuri calendaristice	Obligatoriu
CF916	Notificare privind iminența limitei de timp	Obligatoriu
CF917	Depășirea limitei de timp agreate	Obligatoriu
CF918	Evidența respectării limitelor de timp	Obligatoriu
CF919	Jurnalizare depășire limite de timp	Obligatoriu

CU9.11: Integrare MPass

Autentificarea utilizatorilor se face prin integrarea serviciilor MPass. Detalii sunt disponibile la:

- procedura de integrare administrativă https://mpass.gov.md/info/procedure
- procedura de integrare tehnică https://egov-moldova.github.io/egov4dev/guides/mpass/integration-development/

Integrarea acoperă cel puțin:

- autentificare din RSIC
- autentificare existentă
- expirare sesiune
- ieșire din sistem

Important! MPass asigură autentificarea identității, MPower asigură verificarea dreptului de reprezentare atunci când utilizatorul acționează în numele unei persoane juridice, iar SI RSIC gestionează doar rolurile funcționale, permisiunile de business și regulile de acces la obiectele informaționale. Se va exclude instituirea unor conturi locale sau mecanisme paralele de acces.

ID	De văzut și:	Statut
CF901	Autentificare utilizatori	Obligatoriu
CF902	Utilizatori autorizați	Obligatoriu
CF908	Limitare acces	Obligatoriu

CU9.12: Integrare MPower

Autorizări și împuterniciri pot fi acordate utilizatorilor prin integrarea serviciilor MPower. Detalii sunt disponibile la:

- procedura de integrare administrativă https://egov-moldova.github.io/egov4dev/guides/mpower/process/
- procedura de integrare tehnică https://egov-moldova.github.io/egov4dev/guides/mpower/integration-development/
- tipuri de împuterniciri https://mpower.gov.md/#/ro/public-authorization-types

Lista de împuterniciri relevante pentru RSIC este coordonată cu beneficiar dar poate include cel puțin:

- Reprezentarea intereselor față de ASC
- Reprezentarea intereselor în RSIC

Deținătorii de cel puțin una din împuterniciri pot reprezenta entitatea care a remis împuternicirea în limita accesului acesteia la sistem.

Important! MPass asigură autentificarea identității, MPower asigură verificarea dreptului de reprezentare atunci când utilizatorul acționează în numele unei persoane juridice, iar SI RSIC gestionează doar rolurile funcționale, permisiunile de business și regulile de acces la obiectele informaționale. Se va exclude instituirea unor conturi locale sau mecanisme paralele de acces.

ID	De văzut și:	Statut
CNF127	Reprezentanti ai organizațiilor	Obligatoriu

CU9.13: Integrare MSign

Semnătura electronică a documentelor și înregistrărilor se face prin MSign. Detalii sunt disponibile la:

- procedura de integrare administrativă https://egov-moldova.github.io/egov4dev/guides/msign/process/
- procedura de integrare tehnică https://egov-moldova.github.io/egov4dev/guides/msign/integration-development/

Integrarea permite semnarea a cel puțin:

- Calendar remediere

Toate înregistrările atașate la caz permit semnarea (opțională) a acestora.

CU9.14: Integrare MLog

Jurnalizarea evenimentelor cu forță juridică se face în MLog. Detalii sunt disponibile la:

- procedura de integrare administrativă https://egov-moldova.github.io/egov4dev/guides/mlog/process/
- procedura de integrare tehnică https://egov-moldova.github.io/egov4dev/guides/mlog/integration-development/

Se jurnalizează cel puțin acțiuni (business) a utilizatorilor ca:

- Login/Logout
- Creare/Modificare Incident/Vulnerabilitate/Alertă
- Adăugare/Ștergere participanț la caz

Lista de evenimente jurnalizate se va suplimenta prin coordonare cu beneficiar.

ID	De văzut și:	Statut
CF904	Jurnalizare acțiuni utilizator	Obligatoriu
CF905	Jurnalizare modificare	Obligatoriu
CF906	Jurnalizare evenimente de business cu MLog	Obligatoriu
CF907	Actiuni jurnalizate MLog configurabile	Obligatoriu
CF910	Jurnalizare locală	Obligatoriu

CU9.15: Integrare MNotify

Notificări către persoane fizice și juridice în baza IDNP și IDNO sunt transmise prin MNotify. Detalii sunt disponibile la:

- procedura de integrare administrativă https://egov-moldova.github.io/egov4dev/guides/mnotify/process/
- procedura de integrare tehnică https://egov-moldova.github.io/egov4dev/guides/mnotify/integration-development/

Se va asigura cel puțin:

- transmitere notificare către IDNx
- setare șablon notificare

Notificări sunt transmise participanților la caz cel puțin pentru:

- modificare obiect informațional
- includere ca participant la caz
- conform calendarului pentru responsabil și coordonator caz

ID	De văzut și:	Statut
CNF126	Notificare părți cu MNotify	Obligatoriu

CU9.16: Integrare MConnect

Platforma de interoperabilitate MConnect oferă acces la resurse informaționale deținute de toate serviciile publice din țară. Aceste resurse figurează în catalogul semantic. Detalii privind interconectarea sunt disponibile la:

- procedura de integrare https://semantic.gov.md/ro/mconnect

Integrarea consumă cel puțin următoarele resurse:

- clasificatoare relevante
- informații succinte despre organizație din RSUD
- infomații succinte despre persoane din RSP
- validare persoana este angajat a organizației

ID	De văzut și:	Statut
CF912	Clasificatoare RM	Obligatoriu
CF912	Reutilizare clasificatoare	Obligatoriu
CF913	Clasificatoare noi descurajate	Obligatoriu

Cerințe

Compartimentul documentului privind cerințele funcționale și non-funcționale.

Notă: Cerințele cu statut opțional sunt dezirabile dar vor fi excluse din soluție dacă au impact pentru calendarul și complexitatea soluției finale.

Cerințe funcționale

Cerințele funcționale specifică detalii privind funcționalitățile oferite de sistem.

Notă: Cerințele funcționale suplimentează cazurile de utilizare descrise mai sus. O cerință funcțională poate fi realizată în cazuri de utilizare multiple. A se vedea tabelul corespunzător ce descrie cazul de utilizare pentru detalii.

Alerta timpurie

Cerințele funcționale suplimentează cazurile de utilizare privind Alerta Timpurie.

ID	Cerință	Statut
CF100	**Aliniere model date la modelul EU** Sistemul aliniază modelul de date cu modelul EU unde este posibil dar mai ales pentru datele structurate prestate ca serviciu de sistem.	Obligatoriu
CF101	**ENISA Threat Taxonomy se utilizează pentru clasificare cazuri**	Obligatoriu
CF102	**Detalii alerte/vulnerabilități conform CSAF** Modelul detaliat de date pentru alerte/vulnerabilități este aliniat la CSAF specificat la https://docs.oasis-open.org/csaf/csaf/v2.1/csaf-v2.1.html	Obligatoriu
CF104	**Datele obiectului informațional „alertă cibernetică”** Datele înregistrate includ cel puțin următoarele aspecte conform HG 822: 1. elementele de identificare a rețelelor și/sau sistemelor monitorizate; 2. descrierea alertei; 3. data și ora emiterii; 4. clasificarea alertei; 5. măsurile preliminare și finale întreprinse pentru prevenirea incidentelor cibernetice; 6. recomandările privind reducerea riscurilor de apariție a incidentelor cibernetice; 7. metadatele de trafic aferente comunicațiilor electronice; 8. alte date aferente alertei cibernetice, preluate din documentele atasate	Obligatoriu
CF105	**Datele obiectului informațional „vulnerabilitate cibernetică”** Datele înregistrate includ cel puțin următoarele aspecte conform HG 822:	Obligatoriu

ID	Cerință	Statut
	1. datele de identificare a organizației responsabile; 2. datele de identificare a produsului TIC afectat de vulnerabilitate; 3. datele de identificare a raportorului; 4. datele de identificare a cercetătorului sau a participantului în domeniul securității; 5. datele privind divulgarea coordonată a vulnerabilităților; 6. datele privind divulgarea publică; 7. informații de remediere; 8. alte date aferente vulnerabilității cibernetice, preluate din documentele atasate.	
CF107	**Alertă pozitivă** Descrie activități anormale recepționate sau raportate prin căile de comunicare aprobate, care au potențial de a degenera în vulnerabilitate cibernetică sau incident cibernetic.	Obligatoriu
CF108	**Alertă fals-pozitivă** Se referă la cazul în care alertele recepționate indică activități anormale, dar care nu reprezintă risc de securitate sau care nu au potențial de a deveni vulnerabilitate în spațiul cibernetic sau incident cibernetic	Obligatoriu
CF109	**Alerta fals-pozitivă inchisă imediat** Registratorii responsabili de alerta fals-pozitivă vor închide cazul cu mențiunile corespunzătoare în comentarii	Obligatoriu
CF110	**Alertă degenerată în incident cibernetic** Se referă la cazul în care activitatea anormală raportată este rezultatul desfășurării unui atac cibernetic în timp real, ce devine incident cibernetic.	Obligatoriu
CF113	**Prezentare integrată a cazurilor corelate** Cazurile corelate combină istoriile acestora și formează o vizualizare integrată.	Obligatoriu
CF115	**Corelarea alertelor din diferite surse** Informațiile parvenite în sistem din diferite surse potențial descriu o singură situație. În acest sens corelarea asigură cumularea acestor informații sub egida unui caz comun spre analiză și examinare/soluționare.	Obligatoriu
CF116	**Recepționare informații din diferite surse** Se asigură recepționarea raportărilor privind situațiile cibernetice care afectează sistemele informatice și rețelele furnizorilor de servicii	Obligatoriu
CF121	**Restrictionare/distribuire date conform TLP** Restricționarea la elementele de date din structura ierarhică a înregistrării conform TLP sunt următoarele: • tlp:red - utilizatori identificați personal ca participanți la caz • tlp:amber sau tlp:amber+strict - utilizatori ce reprezintă organizații numite personal ca participanți la caz • tlp:green - utilizatori cunoscuți de sistemul RSIC	Obligatoriu

ID	Cerință	Statut
	• tlp:clear - oricare utilizator inclusiv vizitatori anonimi ai RSC Protocolului TLP e specificat la https://www.first.org/tlp/	
CF122	**Elementele de date spre publicare** Elementele de date făcute publice sunt marcate cu nivelul de acces public (tlp:clear) conform protocolului TLP specificat la https://www.first.org/tlp/	Obligatoriu
CF123	**Radiere caz** Radierea datelor incorecte și neveridice se efectuează in baza documentelor confirmative Notă: Cazul este trecut în starea Radiat fiind posibilă revederea deciziei de radiere.	Obligatoriu
CF124	**Notificarea permanentă privind modificarea** Se oferă notificarea permanentă privind modificarea (statutului) alertei/incidentului cibernetic	Obligatoriu
CF126	**Data ultimei sincronizări** Data ultimei sincronizări pentru una/toate bazele de date de alerte/vulnerabilități interconectate se utilizează pentru a evita extragerea informațiilor învechite. Această dată/oră poate fi setată automat de procesele periodice care au sincronizat datele sau manual.	Obligatoriu
CF127	**Distribuire restricționată implicit** Distribuirea informațiilor noi luate la evidență este restricționată (tlp:red). Notă: Acest atribut este setat la nivel de înregistrare. Dacă alte compartimente a înregistrării includ informații privind distribuirea acestea pot fi păstrate ca la sursă.	Obligatoriu
CF128	**Încărcare date noi din CSAF** Se oferă opțiunea de a încărca o alertă/vulnerabilitate nouă din fișier CSAF.	Obligatoriu
CF129	**Actualizare date existente din fisier CSAF** Se oferă opțiunea de a actualiza datele luate în evidență încărcând un fișier CSAF a) suplimentând informația cu înregistrarea încărcată și b) actualizând atributele comune cu valori din fișier.	Obligatoriu
CF130	**Extragere manuală sau periodică din surse interconectate** Se poate configura sistemul ca sursele interconectate de date să fie operate manual la cerere utilizator sau automat cu o anumită periodicitate.	Obligatoriu
CF131	**Procesele repetate periodic în format cron** Formatul utilizat în cron este utilizat pentru păstrarea setărilor și rularea automatizată a proceselor periodice.	Obligatoriu
CF132	**Identificator AALLDD-XXXX** Un identificator în uz curent are forma AALLDD-XXXX unde • AALLDD - reprezintă Anul (doua cifre) Luna Data luării în evidență a obiectului informațional, • XXXX reprezintă un număr aleator din 4 cifre	Obligatoriu

ID	Cerință	Statut
	Furnizor coordonează cu beneficiar utilizarea acestui identificator.	
CF133	**Cazuri personale** Se oferă opțiunea de afișare doar a cazurilor personale - cazuri în care utilizatorul este implicat	Obligatoriu
CF135	**Atribute caz** Fiecare caz trebuie să conțină cel puțin: • ID unic • Titlu • Descriere • Tip (incident / vulnerabilitate) • Prioritate • Dată creare • Termen executare • Statut	Obligatoriu
CF136	**Statut caz** Statutul poate fi unul dintre: • Nou • În analiză • În remediere • În așteptare • Rezolvat • Închis	Obligatoriu
CF137	**Responsabilii/participantii la caz** Responsabilii pot fi: • Utilizatori individuali • Organizații Se admite: • Asignarea unui responsabil pentru rezolvarea tichetului. • Asignarea mai multor participanți (echipă / organizație)	Obligatoriu
CF138	**Comentarii și colaborare** Sistemul trebuie să permită adăugarea de: • Comentarii text • Atașamente (opțional) Comentariile trebuie: • Să fie asociate utilizatorului • Să fie marcate temporal (timestamp) • Să fie vizibile conform drepturilor de acces	Obligatoriu

ID	Cerință	Statut
CF139	**Istorie caz** Sistemul trebuie să păstreze un istoric complet și nemodificabil al cazului inclusiv: • Modificări de status • Schimbări de responsabil • Comentarii • Acțiuni utilizatori	Obligatoriu
CF140	**Notificări** Sistemul trebuie să transmită notificări cel putin la: • Crearea tichetului • Schimbarea statutului • Asignare / reasignare • Adăugare comentarii	Obligatoriu

Incidente cibernetice

Cerințele funcționale suplimentează cazurile de utilizare privind Incidentele Cibernetice.

ID	Cerință	Statut
CF201	**Model de date aliniat la cerințele HG 822 și standardelor UE** Conceptual modelul de date și atributele despre incident se conformează cu HG 822 și standardelor UE.	Obligatoriu
CF202	**Model de date conform IODEF** Structura de date și atributele despre incident includ definițiile standard IODEF versiunea 2 dar și extensia acestuia IODEF-SCI. Acestea sunt specificate ca RFC 7970 și RFC 7203: • https://www.rfc-editor.org/rfc/rfc7970 • https://www.rfc-editor.org/rfc/rfc7203.html	Obligatoriu
CF203	**Motiv escaladare** Registratorul incidentului cibernetic consemnează prin comentariu motivul escaladării	Obligatoriu
CF204	**Punerea inițială în evidență** Punerea inițială în evidență e realizată de către registrator la confirmarea cazului	Obligatoriu
CF205	**Identificatorii obiectelor informaționale** Identificatorii obiectelor informaționale sunt constituiți din numărul de ordine atribuit de SI RSIC	Obligatoriu
CF206	**Transmiterea în arhiva** Transmiterea în arhiva electronică e realizată de către registrator la închidere în cazul soluționării cazului	Obligatoriu
CF208	**Datele obiectului informațional „incident cibernetic”** Datele înregistrate includ cel puțin următoarele aspecte conform HG 822: 1. datele de identificare a furnizorului de servicii vizat de atacul cibernetic; 2. elementele de identificare a rețelelor și/sau sistemelor informatice afectate; 3. descrierea incidentului; 4. data și ora detectării incidentului; 5. clasificarea incidentului; 6. măsurile preliminare și finale întreprinse pentru soluționarea incidentului cibernetic; 7. metadatele de trafic aferente comunicațiilor electronice; 8. datele aferente tehnicilor și tehnologiilor folosite în cadrul atacului cibernetic; 9. alte date aferente incidentului cibernetic, preluate din documentele atasate;	Obligatoriu
CF209	**Caz închis prin solicitare CNMC**	Obligatoriu

ID	Cerință	Statut
	Cazul incidentului cibernetic poate fi închis de către registrator în baza solicitării CNMC	
CF210	**Arhivare cazuri închise** RSIC asigură transmiterea în arhiva electronică, realizată de către registrator, la soluționarea cazului cibernetic. Cazurile arhivate nu mai pot fi modificate.	Obligatoriu
CF211	**Cazurile critice pot fi escaladate către CNMC** Sistemul oferă posibilitatea de escaladare a incidentelor cibernetice care necesită implicarea Centrului Național de Management al Crizelor	Obligatoriu
CF212	**Formular de notificare** Datele sunt prezentate de furnizori conform conținutului formularelor de notificare a incidentelor	Obligatoriu
CF213	**Conținut formular de notificare inițială** Formularul și compartimentele acestuia sunt coordonate cu furnizor dar ele includ: [1/3] Date de contact: • Numele Organizației: • IDNO: • Persoană de Contact: • Funcția: • E-mail: • Numărul de Telefon: [2/3] Descrierea Incidentului: • Data și Ora la care Incidentul a fost Constatat: • Data și Ora estimată a Începutului Incidentului (Opțional): • Data și Ora estimată a Sfârșitului Incidentului: • Descrierea Incidentului: • Impact constatat sau presupus asupra activităților organizației: • Impact constatat sau presupus asupra altor entități, inclusiv din străinătate: [3/3] Detalii: • Detalii despre Acțiunile Întreprinse (Opțional): • Solicitare de Asistență: • Detalii despre Asistența Necesară (Opțional): • Comentarii Libere (Opțional): • Fișier Atașat (Opțional):	Obligatoriu
CF214	**Notificare inițială** Raportul remis de furnizorul de informație este luat în evidență sub formă de înregistrare Notificare inițială	Obligatoriu
CF215	**Protejare identitate raportor**	Obligatoriu

ID	Cerință	Statut
	Sunt incluse facilități ce garantează protejarea informației privind identitatea raportorilor	
CF216	**Consimțământ privind identitate raportor** Se permite ca raportor să exprime în mod expres consimțământul scris pentru dezvăluirea identității sale. Accesul la informațiile de identificare a raportorului este permis exclusiv persoanelor din cadrul ASC desemnate pentru a se implica direct în procesul de analiză și gestionare a vulnerabilității	Obligatoriu
CF217	**Confirmare plan de divulgare** Sunt oferite mijloace ce confirmă că divulgarea este acceptată în mod expres, în scris, de către părțile implicate	Obligatoriu
CF218	**Primirea notificărilor securizat** Se oferă un mecanism securizat pentru primirea notificărilor privind vulnerabilitățile, care asigură integritatea, confidențialitatea și disponibilitatea datelor transmise	Obligatoriu
CF219	**Asistență raportorilor** Se oferă asistență tehnică și procedurală raportorilor, sprijinindu-i în întocmirea notificării și în înțelegerea cadrului legal și metodologic aplicabil	Obligatoriu
CF220	**Notificarea acceptată de la oricine** Orice persoană fizică sau juridică, inclusiv cercetătorii și participanții în domeniul securității cibernetice, poate notifica, în mod voluntar, o vulnerabilitate identificată într-un produs sau serviciu TIC, utilizând platforma digitală pusă la dispoziție de RSIC	Obligatoriu
CF221	**Confirmare recepționare notificare inițială** Se confirmă primirea notificării în termen de o zi lucrătoare de la recepționare	Obligatoriu
CF222	**Implicare CERT-Gov la necesitate** În cazul în care vulnerabilitatea raportată poate afecta rețele sau sisteme informatice proprietate a statului la nivel guvernamental, organizația responsabilă transmite notificarea Centrului guvernamental de răspuns la incidente cibernetice (CERT-Gov) în termen de o zi lucrătoare de la primirea acesteia	Obligatoriu
CF223	**Notificarea recepționată de la organizația responsabilă** Organizația responsabilă care primește o notificare directă și o înregistrează în RSIC trebuie să furnizeze în termen de 14 zile lucrătoare, următoarele: • confirmarea că raportorul a fost informat despre transferul notificării in RSIC • evaluarea preliminară a validității vulnerabilității raportate • planul inițial de analiză și remediere • persoanele de contact desemnate	Obligatoriu
CF224	**Notificări critice incomplete** În situații excepționale sau în cazul în care vulnerabilitatea raportată prezintă un risc iminent și critic pentru securitatea națională, infrastructura critică sau siguranța	Obligatoriu

ID	Cerință	Statut
	publică, se pot accepta notificări care nu conțin toate elementele esențiale, solicitând completarea ulterioară a informațiilor esențiale	
CF225	**Condiții de situație critică** Situația este calificată ca fiind excepțională dacă survine oricare dintre următoarele condiții: • afectează servicii esențiale; • exploatarea activă a vulnerabilității este efectuată de către entități neautorizate; • există posibilitatea de compromitere a infrastructurii critice sau a sistemelor guvernamentale; • există posibilitatea producerii unui prejudiciu patrimonial și/sau moral major asupra persoanelor fizice sau juridice; • există impact asupra securității datelor cu caracter personal.	Obligatoriu
CF226	**Suplimentare notificări incomplete în maximum 2 zile** Pentru notificări incomplete și raportor identificabil, se solicită completarea informațiilor lipsă în termen de două zile lucrătoare	Obligatoriu
CF227	**Completare notificare din oficiu** Dacă notificarea primită nu conține toate elementele esențiale necesare pentru evaluare, iar raportorul nu are posibilitatea de a completa informațiile lipsă în termenul prevăzut • se inițiază procedura de verificare din oficiu, utilizând surse și instrumente proprii, precum și informațiile disponibile din alte registre sau sisteme relevante, în scopul confirmării și completării datelor necesare pentru continuarea procesului	Obligatoriu
CF228	**Informare sector în maximum 2 ore pentru cazuri critice** Pentru situațiile critice se informează autoritățile competente sectoriale în termen de maximum două ore lucrătoare de la confirmarea riscului	Obligatoriu
CF229	**Calendar accelerat de remediere și divulgare pentru cazuri critice**	Obligatoriu
CF230	**Grupare cazuri identice/repetate** În cazul notificărilor în masă (multiple vulnerabilități în același produs sau vulnerabilități similare în produse diferite), cazurile pot fi grupate (corelate)	Obligatoriu
CF231	**Evaluare/clasificare caz conform CVSS** Vulnerabilitățile sunt clasificate în funcție de nivelul de risc estimat, utilizând o metodologie standardizată, cum ar fi sistemul CVSS (Common Vulnerability Scoring System), sau alte metodologii recunoscute la nivel internațional. CVSS 4.0 e specificat la https://www.first.org/cvss/v4.0/specification-document	Obligatoriu
CF232	**Informare raportor și organizație responsabilă despre evaluare** Se comunică raportorului și organizației responsabile concluziile	Obligatoriu

ID	Cerință	Statut
	evaluării, incluzând: • rezultatele analizei tehnice și argumentele aferente; • nivelul de risc atribuit vulnerabilității; • termenele recomandate pentru implementarea măsurilor corective; • următoarele etape planificate, inclusiv cerințele de cooperare între părți	
CF232	**Nivelul cazurilor/vulnerabilităților** Cazurile sunt încadrate în una dintre următoarele nivele: • nivel critic – vulnerabilitate cu impact major asupra infrastructurii critice, ce permite compromiterea totală a sistemului fără a necesita interacțiunea utilizatorului; • nivel ridicat – vulnerabilitate care compromite date sensibile, integritatea sistemului sau funcționalități esențiale; • nivel mediu – vulnerabilitate cu impact localizat sau care necesită condiții specifice pentru a fi exploatată; • nivel scăzut – vulnerabilitate cu impact redus, dificultate mare de exploatare și risc minim.	Obligatoriu
CF233	**Termenul de evaluare și clasificare** Evaluarea și clasificarea se realizează în termen de cinci zile lucrătoare de la primirea notificării complete	Obligatoriu
CF234	**Conținut plan/calendar de remediere** Plan de remediere include: • confirmarea vulnerabilității și a nivelului de risc; • măsurile tehnice și organizatorice planificate pentru remediere; • termenele estimate pentru implementarea remediilor; • persoanele responsabile de implementare și comunicare; • eventualele constrângeri sau dependențe care pot afecta procesul de remediere	Obligatoriu
CF235	**Informare periodică privind progresul** Pe toată durata procesului de remediere, organizația responsabilă comunică periodic stadiul implementării măsurilor și notifică fără întârziere orice modificare a planului inițial sau apariția unor obstacole semnificative, prin mijloacele și în termenele stabilite	Obligatoriu
CF236	**Conținut raport final de remediere** Raport final de remediere include: • acțiunile realizate și termenele respectate; • testele de validare a eficienței remediilor; • eventualele măsuri preventive suplimentare implementate; • concluziile formulate și modificările aduse proceselor interne	Obligatoriu
CF236	**Raport final de remediere**	Obligatoriu

ID	Cerință	Statut
	După finalizarea implementării măsurilor, organizația responsabilă transmite un raport final de remediere	
CF237	**Momentul și forma divulgării** Momentul optim și forma divulgării publice se stabilește împreună cu raportorul și organizația responsabilă	Obligatoriu
CF238	**Divulgare doar descriere generală a vulnerabilității** Divulgarea publică a unei vulnerabilități, efectuată după finalizarea procesului de remediere, va include o descriere generală a vulnerabilității, fără a menționa explicit furnizorul, serviciul sau sistemul afectat	Obligatoriu
CF239	**Decizie de divulgare fără remediere** În cazul în care vulnerabilitatea identificată prezintă un risc major pentru securitatea publică și organizația responsabilă nu a remediat-o în termenul stabilit se poate adopta decizia de divulgare publică	Obligatoriu
CF240	**Decizia de divulgare se adoptă pe baza unei evaluări documentate**	Obligatoriu
CF241	**Notificare în avans privind divulgarea publică** Se notifică în scris organizații responsabile, raportorul și alte părți direct afectate decizia de divulgare publică cu cel puțin trei zile lucrătoare înainte de publicare	Obligatoriu
CF242	**Divulgare fără notificare în avans a părților** Se admite o divulgare fără respectarea termenului de notificare, cu condiția documentării motivelor care justifică urgența și a comunicării acestora părților implicate	Obligatoriu
CF243	**Consultarea prealabilă a autorității sectoriale** Divulgarea publică a unei vulnerabilități care afectează entități din domeniile financiar-bancar, energetic sau al comunicațiilor electronice se efectuează după consultarea prealabilă a autorității competente sectoriale	Obligatoriu
CF244	**Condiții pentru a închide caz** Pentru închiderea formală a cazului sunt necesare următoarele condiții cumulative: • transmiterea, de către organizația responsabilă, a raportului final de remediere; • validarea eficienței măsurilor de remediere; • lipsa unor riscuri reziduale semnificative; • informarea raportorului, cu respectarea cerințelor de confidențialitate, privind închiderea cazului.	Obligatoriu
CF245	**Fișa de închidere caz înregistrată la închidere**	Obligatoriu
CF246	**Conținut fișa de închidere caz** Fișă de închidere a cazului include cel puțin: • data închiderii și identificatorul unic al cazului;	Obligatoriu

ID	Cerință	Statut
	• sinteza etapelor parcurse: notificare, evaluare, remediere, divulgare; • măsurile implementate și eficiența acestora; • concluzii și recomandări pentru îmbunătățirea procesului; • orice aspecte juridice, instituționale sau tehnice relevante constatate pe parcurs.	
CF247	**Propuneri de ajustare plan remediere/divulgare** Propuneri de ajustare planuri de remediere sau divulgare coordonată sunt oferite de participanții la caz sub formă de comentariu (text liber) marcat corespunzător (ca propunere de modificare plan)	Obligatoriu
CF249	**Prezentarea datelor** Raportul se afișează în formă electronică similar cu formularul în uz curent. Detalii oferite în Anexa: FNV - Formular Notificare de Vulnerabilitate De asemenea se oferă posibilitatea de extragere ca PDF pentru a fi atașat sau imprimat după necesitate.	Obligatoriu

Schimb de informații

Cerințele funcționale suplimentează cazurile de utilizare privind Schimbul de informații cu participanții.

ID	Cerință	Statut
CF301	**Informare privind riscurile cibernetice** Se asigură comunicarea informațiilor privind amenințările, vulnerabilitățile, riscurile cibernetice și măsurile de protecție necesare	Opțional
CF302	**Se asigură comunicarea rezultatelor analizei incidentelor cibernetice**	Obligatoriu
CF303	**Se oferă accesarea ghidurilor de securitate cibernetică**	Opțional
CF304	**ASC crează și publică ghiduri de securitate cibernetică**	Opțional
CF305	**Se oferă accesarea recomandărilor de soluționare a incidentelor cibernetice**	Opțional
CF306	**ASC crează și publică recomandări de soluționare incidente cibernetice**	Opțional
CF307	**Colectare opinii și recomandări** Se colectează și analizează periodic opinii privind participarea în procesul de divulgare coordonată pentru îmbunătățirea practicilor și a relațiilor de încredere	Obligatoriu
CF310	**Responsabil de comunicare** ASC poate desemna o persoană responsabilă de comunicare pentru a oferi asistență victimelor unui incident cibernetic	Opțional
CF311	**ASC crează și publică rezultate a analizei incidentelor**	Obligatoriu
CF312	**Rezultate analiză incidente informat de feedback-ul partajat**	Obligatoriu
CF313	**Destinatar date** Destinatar date din perspectiva unui caz este un utilizator autentificat sau nu prin MPass cu acces la cazurile publice.	Obligatoriu
CF314	**Coordonator caz poate iniția colectarea feedbackului de la participanți**	Obligatoriu
CF315	**Feedback anonim** Se permite solicitarea de prezentare anonimă a feedbackului. Notă: Sistem oricum validează identitatea și permisiunea persoanei ce remite feedbackul - dar salvează datele fără referire la acestea.	Obligatoriu
CF316	**Formular feedback**	Obligatoriu

ID	Cerință	Statut
	Formularul de feedback se coordonează cu beneficiar dar cel puțin include: • componente text liber ce permit formularea sugestiilor, părerilor și recomandărilor • componente de notă (1-10) ce permit evaluări a aspectelor procesului • componente de selecție unde sunt oferite 2 sau mai multe opțiuni de selectat	
CF317	**Reflectarea în istorie caz** Istoria cazului reflectă dacă s-a solicitat feedback de la participanți. Feedbackul individual de la participanți NU apare în istorie caz.	Obligatoriu
CF318	**Reflectare în statistici** Statisticile RSIC includ și informații privind feedbackul recepționat și anume datele structurate - notele și opțiunile indicate.	Obligatoriu
CF319	**Rezultatele analizei incidentelor în istoria caz** Istoria cazului este suplimentată cu referire la rezultatele analizei dacă aceasta include referințe la caz. Notă: Rezultatele analizei incidentelor pot fi publicate în RSIC ca material public (și nu generate în baza informațiilor din caz care sunt poate mult mai sensibile). În așa caz aceste materiale sunt suplimentate cu referințe la identificatorii cazurilor și în baza acestora este actualizată istoria cazurilor menționate.	Obligatoriu
CF320	**Rezultatele analizei incidentelor accesibile pentru destinatari date**	Obligatoriu
CF321	**Rezultatele analizei incidentelor pot fi publicate sau retrase de utilizatori interni**	Obligatoriu

Administrare și control

Cerințele funcționale suplimentează cazurile de utilizare privind Administrare și control a sistemului.

ID	Cerință	Statut
CF901	**Autentificare utilizatori** Oferirea accesului la datele din SI RSIC utilizatorilor autentificați prin MPass	Obligatoriu
CF902	**Utilizatori autorizați** RSIC asigură schimbul de date cu privire la situații cibernetice, în format electronic, între ASC, I.P. STISC și CERT sectoriale, precum și cu furnizorii de servicii din sectoare critice, conform cadrului normativ	Obligatoriu
CF903	**Echipe dedicate** Echipe sunt formate în avans pentru implicare în cazuri specializate includ: • CNMC • CERT guvernamental • CERT sectoriale • Echipa de răspuns	Obligatoriu
CF904	**Jurnalizare acțiuni utilizator** Orice acțiune a utilizatorilor se jurnalizează, arătând momentul și utilizatorul care a efectuat acțiunea.	Obligatoriu
CF905	**Jurnalizare modificare** Pentru fiecare acțiune a utilizatorului se salvează în evenimentul jurnalizat datele care au fost modificate.	Obligatoriu
CF906	**Jurnalizare evenimente de business cu MLog** SI RSIC jurnalizează evenimentele de business critice prin intermediul serviciului electronic guvernamental de jurnalizare (MLog)	Obligatoriu
CF907	**Actiuni jurnalizate MLog configurabile** Acțiunile care sunt jurnalizate prin intermediul serviciului electronic guvernamental de jurnalizare (MLog) pot fi configurate în opțiunile de administrare.	Obligatoriu
CF908	**Limitare acces** Sistemul asigură limitarea accesului în două etape: asigurarea accesului doar prin autentificare și stabilirea individuală a drepturilor de acces a utilizatorilor	Obligatoriu
CF909	**Dreptul de acces poate fi limitat, suspendat sau retras**	Obligatoriu
CF910	**Jurnalizare locală** Se jurnalizează local evenimentele ce țin de buna funcționare a sistemului	Obligatoriu
CF911	**Delimitare acces**	Obligatoriu

ID	Cerință	Statut
	Accesul este structurat pe unități de conținut și reglementat prin atribuirea drepturilor specifice fiecărei categorii de utilizatori	
CF912	**Clasificatoare de securitate cibernetică din UE** Clasificatoarele privind securitatea cibernetică utilizate în UE sunt disponibile în MISP	Obligatoriu
CF912	**Clasificatoare RM** Clasificatoarele RM sunt descrise în catalogul semantic și pot fi consultate/integrate prin MConnect la https://semantic.gov.md/ro/assets?asset=classifiers	Obligatoriu
CF912	**Reutilizare clasificatoare** Pentru o clasificare corectă a obiectelor se utilizează sistemul de clasificatoare elaborate în baza clasificatoarelor naţionale ale Republicii Moldova şi a actelor UE	Obligatoriu
CF913	**Clasificatoare noi descurajate** Clasificatoarele intrasistemice se elaborează şi se utilizează în cadrul SI RSIC doar în cazurile absenţei clasificatoarelor naţionale şi internaţionale aprobate.	Obligatoriu
CF914	**Statistici** Sistemul oferă mijloace pentru întocmirea datelor statistice și a rapoartelor privind alertele, riscurile și incidentele cibernetice	Obligatoriu
CF915	**Iminența limitei de timp pentru planuri calendaristice** Iminența limitei de timp pentru planuri calendaristice de remediere și de divulgare coordonată este opțională și configurabilă, spre exemplu 10-15 min pentru actualizările periodice privind progresul de soluționare cazuri critice și de 4-24 ore pentru data/ora agreată de remediere a cazurilor non-critice.	Obligatoriu
CF916	**Notificare privind iminența limitei de timp** Se notifică responsabilul de caz și coordonatorul despre iminența limitei de timp agreate în planuri calendaristice de remediere și divulgare coordonată.	Obligatoriu
CF917	**Depășirea limitei de timp agreate** Se înregistrează situațiile în care limita de timp agreată în planuri calendaristice este depășită.	Obligatoriu
CF918	**Evidența respectării limitelor de timp** Se duce evidența tuturor limitelor de timp de sistem și agreate în planurile calendaristice și faptul conformării cu acestea.	Obligatoriu
CF919	**Jurnalizare depășire limite de timp**	Obligatoriu
CF920	**Roluri pentru gestiune acces** Rolurile sunt utilizate pentru a seta un set de permisiuni utilizatorilor	Obligatoriu
CF921	**Control acces** Accesul e controlat pe bază de:	Obligatoriu

ID	Cerință	Statut
	• Roluri (RBAC)/permisiuni • Organizație • Implicare/participare în tichet	
CF922	**Limitare acces** Sistemul trebuie să impună cel puțin următoarele limitări de acces la fiecare din resursele/serviciile prestate: • Vizualizare • Editare • Comentare • Administrare	Obligatoriu

Cerințe nonfuncționale

Cerințele nonfuncționale specifică atributele de calitate a sistemului cum ar fi performanța, mentenabilitatea, licențierea, securitatea ș.a.m.d.

Cerințe arhitecturale

Cerințe privind proiectarea de nivel înalt a sistemului.

ID	Cerință	Statut
CNF100	**Aliniere model date la modelul EU** Sistemul aliniază modelul de date cu modelul EU unde este posibil dar mai ales pentru datele structurate prestate ca serviciu de sistem.	Obligatoriu
CNF101	**Arhitectura orientată pe serviciu (SOA)** Sistemul e proiectat în baza unei arhitecturi orientată pe serviciu (SOA) în conformitate cu HG650/2023.	Obligatoriu
CNF102	**Platformă tehnologică stabilă și cu utilizare largă** Sistemul are la bază tehnologii stabile și utilizate pe larg în ramură. Componente și/sau dependențe proprietare sau cu utilizare redusă sunt inadmisibile acestea având impact negativ asupra viabilității, mentenabilității și continuității sistemului.	Obligatoriu
CNF103	**Soluție Cloud Ready** Sistemul e capabil să fie rulat pe soluții de virtualizare și exclude dependențe de echipament	Obligatoriu
CNF104	**Găzduire în MCloud** MCloud este soluția Cloud elaborată și utilizată de administrația publică din RM. Sistemul e proiectat să poată fi găzduit în MCloud conform HG. 128.	Obligatoriu
CNF105	**Disponibilitate înaltă** Sistemul e proiectat să asigure disponibilitatea înaltă. Obiectivele de recuperare țintă: • RTO - 4 ore • RPO - 8 ore	Obligatoriu
CNF107	**Aplicație web** Interfața utilizator a sistemului utilizează tehnologii Web.	Obligatoriu
CNF108	**Navigatoare web compatibile** Interfața web a sistemului este compatibilă cu versiunile curente pentru navigatoare web neproprietare inclusiv: • Chromium (versiunea liberă a Chrome) • Firefox	Obligatoriu

ID	Cerință	Statut
	Notă: Majoritatea utilizatorilor pot utiliza alte navigatoare web, inclusiv navigatoare web proprietare. Aplicația urmează să fie validată în navigatoarele menționate mai sus cu așteptarea că se va exclude utilizarea capabilităților prezente doar în unele navigatoarele proprietare. În consecință, aplicația va opera corect în toate versiunile curente a navigatoarelor libere dar și proprietare.	
CNF109	**Bazat pe containere** Modul principal de configurare a versiunilor aplicațiilor pe server are la bază tehnologiile cu containere cum ar fi Docker si Kubernetes. Imaginile containerelor sunt automatizate. A se face referire la https://docs.docker.com/get-started/	Obligatoriu
CNF110	**Independență pentru baza de date** Sistemul include o implementare independentă tehnologic pentru baza de date utilizată. Soluția implementată trebuie să ofere opțiunea: • să reutilizeze serverele existente pentru bazele de date sau • să găzduiască BD pe servere dedicate în MCloud care pot rula SGBD PostgreSQL sau MS SQL Server	Obligatoriu

Cerințe de licențiere și drepturi

Cerințe privind licențierea și drepturile.

ID	Cerință	Statut
CNF111	**Codul sursă** Codul sursă și instrucțiunea privind compilarea/înpachetarea tuturor componentelor sistemului este transferat beneficiarului. Important! De sub incidența acestei cerințe sunt excluse elementele de platformă și bibliotecile de bază a limbajului de programare (SDK). Alte componente excluse vor fi coordonate cu beneficiarul cu condiția acestea să fie componente cu largă utilizare în ramură cum ar fi JQuery sau Log4j.	Obligatoriu
CNF112	**Licență perpetuă** Furnizorul va transfera beneficiarului drepturile pentru codul sursă a sistemului. Celelalte componente a sistemului vor fi însoțite de licențe perpetui privind utilizarea acestora. De sub incidența acestei cerințe sunt excluse componentele Open Source pe care beneficiarul le poate obține de la alți furnizori.	Obligatoriu
CNF113	**Datele aparțin beneficiarului** Toate datele încărcate sau create/actualizate în sistem aparțin beneficiarului. Soluția propusă nu impune restricții privind datele, completitudinea sau volumul acestora.	Obligatoriu
CNF114	**Date deschise** Toate datele păstrate sau furnizate de sistem utilizează formate de date deschise.	Obligatoriu
CNF115	**Costului total de deținere (TCO) pentru 5 ani** Documentația trebuie să prezinte distinct CAPEX și OPEX, costurile de dezvoltare, implementare, licențe, găzduire MCloud, monitorizare, securitate, backup, audit, mentenanță, suport, actualizări, dezvoltări ulterioare, instruire, transfer de cunoștințe și scoatere din exploatare. Prețul licențelor este calculat pentru: • 5000 utilizatori • 200 procesoare • 100000 GByte date • 5 ani	Obligatoriu
CNF116	**Standarde deschise** Sistemul are la bază standarde deschise pentru păstrarea datelor dar și pentru prezentarea datelor și comunicare cu alte sisteme.	Obligatoriu
CNF117	**API descris** Sistemul include un API și acesta este documentat, inclusiv utilizând standarde relevante pentru automatizare cum ar fi WSDL. Lista întreagă de resurse și operații oferite prin API va fi detaliată și coordonată cu beneficiarul.	Obligatoriu

ID	Cerință	Statut
CNF118	**Plan de transfer/ieșire** Furnizor ca parte a documentației de sistem sau separat pregătește un plan de transfer/ieșire care să permită exploatarea, mentenanța și dezvoltarea ulterioară a sistemului de către ASC (cu implicarea I.P. „STISC” sau un alt furnizor) fără dependență nejustificată de furnizorul inițial.	Obligatoriu

Cerințe de integrare

Cerințe privind integrarea cu servicii și sisteme externe.

ID	Cerință	Statut
CNF120	**XML/JSON ca mijloc principal pentru integrarea datelor** XML este utilizat pentru interoperare cu serviciile de platforma guvernamentală comuna. JSON este utilizat preferențial pentru API și schimb de date datorită simplității formatului de date.	Obligatoriu
CNF121	**Registrele de stat și servicii a altor autorități** Sistemul accesează informații din registrele de stat dar și alte surse prin intermediul platformei de interoperabilitate conform cu Lege nr. 142. Detalii privind interoperabilitatea sunt disponibile la: • mconnect.gov.md - platforma de interoperabilitate • semantic.gov.md - vocabularul de date și acțiuni	Obligatoriu
CNF122	**Identități cu MPass** MPass, prin HG. 1090, este serviciul de platformă ce facilitează accesul la sistem pe bază identități utilizator atestate de MPass. Detalii privind MPass: - https://mpass.gov.md/info/procedure	Obligatoriu
CNF123	**Documente electronice semnate cu MSign** MSign, in baza HG. 405, este serviciul de platformă proiectat să faciliteze semnătura electronică a documentelor și validarea acestora. Detalii privind MSign: - https://msign.gov.md/#/info/media	Obligatoriu
CNF124	**Jurnalizare și audit cu MLog** MLog, in baza HG. 708, este serviciul de jurnalizare și audit a evenimentelor.	Obligatoriu
CNF126	**Notificare părți cu MNotify** MNotify, prin HG. 376, e serviciul de platformă privind notificarea. Detalii despre MNotify: - https://mnotify.gov.md/#/ro/integration/api	Obligatoriu
CNF127	**Reprezentanti ai organizațiilor** Datele din MConnect, MPass, MPower se utilizează pentru a stabili dacă persoana fizică (IDNP) reprezintă o anumită organizație (IDNO). Notă: O persoană poate pleca de la organizație și acest fapt are impact asupra deciziei de autorizare.	Obligatoriu
CNF128	**Modelul de deployment stabilit/coordonat de IP STISC** Mediile Dev, Test, Prod sunt utilizate in procesul de elaborare, verificare și testare a sistemului.	Obligatoriu

ID	Cerință	Statut
	Modelul de deployment, promovarea între medii, rollback, managementul configurațiilor, pipeline-ul CI/CD sunt stabilite și coordonate cu I.P. „STISC” Furnizor prevede oferirea unei soluții de ce include cel puțin mediile Dev, Test, Prod și coordonează un plan comun de acțiuni cu I.P. „STISC” pentru pregătirea mediilor în MCloud, agrearea stivei tehnologice și validarea tehnică a soluției.	

Cerințe de securitate

Cerințe privind securitatea cibernetică.

ID	Cerință	Statut
CNF130	**Autentificarea prin MPass** Autentificarea, exclusiv prin intermediul serviciului MPass garantează că sistemul va fi accesibil doar utilizatorilor cu o identitate verificată și confirmată	Obligatoriu
CNF131	**Securizată la nivel de proiect (Secure by design)** Sistemul trebuie să includă mecanismele de securitate necesare la nivel de proiect (Secure by design) și să asigure respectarea acestora de întregul sistem. Mecanismele de securitate trebuie să includă cel puțin cele definite de HG. 201.	Obligatoriu
CNF132	**Mecanisme de securitate documentate** Sistemul include compartimente sau documente dedicate care conțin detalii despre: • fiecare mecanism de securitate utilizat de sistem • modul în care acesta este proiectat și implementat de sistem • argumente despre suficiența soluției alese • modul de verificare a acestuia	Obligatoriu
CNF133	**Secrete și parametri de securitate** Secretele (parole, chei, certificate, parole private etc) și parametrii de securitate a acestora sunt explicit listate în documentația de configurare a sistemului și modul în care acestea pot fi modificate în regim automatizat sub forma de comenzi (shell) care le generează sau înlocuiește.	Obligatoriu
CNF134	**Canale de comunicare securizate** Toate canalele de comunicare cu sisteme externe utilizează mecanisme criptografice care le securizează ca spre exemplu HTTPS sau VPN. Pentru HTTPS se configurează utilizarea doar TLS 1.3 și mai nou.	Obligatoriu
CNF135	**Expirarea sesiunilor utilizator** Sistemul include mecanisme de expirare a sesiunilor utilizator după o perioadă de inactivitate. Această facilitate este configurabilă dar valoarea implicită este de 10 min.	Obligatoriu
CNF136	**Validarea datelor de intrare** Sistemul validează toate datele de intrare atât la client cât și pe server.	Obligatoriu
CNF137	**Încercări de acces eșuate** Sistemul când refuză accesul din cauza lipsei permisiunilor: - jurnalizează evenimentul cel puțin ca EROARE - produce o avertizare că încercările de acces neautorizat vor fi investigate	Obligatoriu
CNF138	**Măsuri de asigurare a integrității datelor**	Obligatoriu

ID	Cerință	Statut
	Sistemul include mijloace de protecție a integrității datelor care protejează de încercări de corupere a informației cu mijloace externe, ca spre exemplu eliminarea sau modificarea datelor direct în baza de date.	
CNF139	**API despre viabilitatea sistemului** Sistemul include mijloace de raportare sau interogare privind viabilitatea sistemului (heartbeat). Acestea vor fi monitorizate pentru a detecta incidentele de funcționare a sistemului.	Obligatoriu
CNF140	**OWASP top 10** Sistemul include mecanisme de protecție pentru cel puțin vulnerabilitățile descrise în ”OWASP Top 10 vulnerabilities”. Detalii la: https://owasp.org/www-project-top-ten/	Obligatoriu
CNF141	**Securizat din start** Sistemul utilizează doar valori implicite securizate pentru parametrii de securitate. De exemplu, nu sunt admise parole sau chei cu valori implicite. Acestea trebuiesc produse/păstrate de sistem utilizând proceduri automatizate sigure.	Obligatoriu
CNF142	**Protejat de atacuri tipice** Sistemul include mecanisme ce protejează de atacuri tipice cum sunt spre exemplu: • SQL injection, • cross-site scripting (XSS), • cross-site request forgery (CSRF), • file inclusion, • cookie poisoning etc Aceste mecanisme vor fi documentate și vor explica modul în care ating obiectivul propus și modalitatea de verificare	Obligatoriu
CNF143	**Web Application Firewall** Soluția propusă va include mecanisme active de scanare și filtrare care asigură că doar comunicarea admisă ajunge la componentele sistemului. De obicei aceasta se face printr-un Web Application Firewall care definește o listă de zone admise/restricționate (allow/deny). De notat că așa soluții permit setări "wildcard" care admit tot traficul. Asemenea setări vor fi evitate.	Obligatoriu
CNF144	**Scanare vulnerabilități** Furnizorul va scana soluția pe mediul de dezvoltare utilizând mijloace de scanare de vulnerabilități general utilizate în ramură. Rapoartele generate vor fi partajate și coordonate cu beneficiarul.	Obligatoriu
CNF145	**Teste de penetrare**	Obligatoriu

ID	Cerință	Statut
	Furnizorul va rula teste de penetrare a sistemului pe mediul de dezvoltare utilizând instrumente de testare de penetrare general utilizate în ramură. Rapoartele generate vor fi partajate și coordonate cu beneficiarul.	
CNF146	**Monitorizare incidente de securitate** Furnizorul va documenta și prezenta recomandări privind detectarea incidentelor de securitate și investigarea acestora în baza logurilor de sistem. Aceste recomandări vor include detalii despre criteriile de căutare și filtrare în loguri dar de asemenea și referire la instrumente utilizate în ramură în aceste scopuri.	Obligatoriu
CNF147	**Modernizare platformă** Securitatea informațională nu poate fi realizată utilizând tehnologii învechite. Furnizorul va oferi recomandări privind modernizarea și fixarea atât a componentelor proprii a sistemului cât și a componentelor terțe a soluției (sisteme de operare, librării și platforme, SGBD, web server, firewall etc). În același timp furnizorul va asigura lansarea sistemului utilizând componente curente a soluției. Componentele mai vechi de 12 luni vor fi evidențiate și coordonate cu beneficiarul.	Obligatoriu
CNF148	**Scanare antivirus/antimalware a atasamentelor** Se asigură scanarea atașamentelor cu antivirus/antimalware pentru a valida că nu includ date malițioase. Furnizor coordonează cu beneficiar soluția propusă.	Obligatoriu
CNF149	**Protecția datelor cu caracter personal** Organizarea sistemului de protecție a datelor cu caracter personal constituie o parte componentă a mecanismului de asigurare a securităţii informaționale. Datele cu caracter personal sunt ținute separat de celelalte date a sistemului. Sistemul asigură păstrarea unui set redus de date cu caracter personal limitat la: • IDNP/IDNO • Nume/Prenume utilizatori • Denumire organizație Setul de date personale poate fi extins doar coordonarea motivelor cu beneficiar..	Obligatoriu
CNF150	**Date cu caracter personal vechi** Datele cu caracter personal sunt păstrate în sistem pe o perioadă de trei ani, după care sunt șterse din baza de date. Sistemul facilitează • trasabilitatea duratei de păstrare a datelor cu caracter personal, • configurarea duratei de păstrare reglementate • modalitatea de a șterge aceste date	Obligatoriu

Cerințe de performanță

Cerințe privind performanța sistemului

ID	Cerință	Statut
CNF151	**Utilizatori concurenți - 300** Sistemul e proiectat să funcționeze optim pentru cel puțin 300 utilizatori concurenți. Când numărul utilizatorilor depășește numărul indicat sunt admise degradări de performanță temporare ce pot fi adresate prin alocarea de noduri adiționale a sistemului în MCloud	Obligatoriu
CNF152	**Timp de răspuns sub 3 sec** Timpul de răspuns pentru perioade de încărcare nominală a sistemului este sub 3 sec. Furnizorul va identifica rapoarte sau sarcini atipice pentru sistem ce pot depăși acest timp și va coordona și agrea dacă depășirea este admisibilă.	Obligatoriu
CNF153	**Apeluri concurente API - 1000** Sistemul este proiectat și dimensionat pentru o încărcare tipică a sistemului de 1000 solicitări concurente la API.	Obligatoriu
CNF154	**Procesare asincronă** Sistemul, la efectuarea operațiilor de lungă durată, va utiliza un model asincron de interacțiune cu utilizatorul și anume: • acțiunea asincronă de lungă durată va fi luată în lucru și confirmată utilizatorului • un indicator despre progresul acțiunii de lungă durată va fi inclus ca element a interfeței utilizator • la finalizarea acțiunii o notificare simplă în interfața utilizator anunță finalizarea acțiunii • aplicația oferă utilizatorului un mod de a naviga și valida/confirma rezultatul acțiunii. Asemenea acțiuni pot apare în cazuri ca de exemplu: • utilizatorul încarcă în sistem un fișier de dimensiuni mari • sistemul urmează să producă un raport care în condiții tipice depășește limita de 3 secunde	Obligatoriu
CNF155	**Dimensiunea fișierelor încărcate** Sistemul implementează o setare despre dimensiunea maxima a fișierelor încarcate de utilizator în sistem. Setarea dată este configurabilă de către administratorii de sistem (de obicei în fișierele de configurare a soluției). Fișierele ce depășesc această dimensiune nu sunt admise în sistem.	Obligatoriu
CNF156	**Teste de performanță** Furnizorul va executa teste de performanță a sistemului pe mediul de dezvoltare și va partaja și coordona rezultatele cu furnizorul.	Obligatoriu

ID	Cerință	Statut
	În avans furnizorul va coordona conținutul testelor de performanță ca de exemplu scenariile de testare, instrumentariul utilizat, numărul de utilizatori simulați, durata testelor, modul de simulare etc.	
CNF157	**Funcționare corectă a sistemului** Furnizorul va asigura că sistemul funcționează corect. Aceasta se poate face testând întegral funcționalitatea sistemului pe mediul de dezvoltare și va partaja și coordona rezultatele cu furnizorul. În avans furnizorul va coordona cu beneficiarul abordare de verificare a corectitudinii sistemului, conținutul testelor ca de exemplu scenariile de testare, teste pozitive/negative, teste automatizate, restaurarea corectă din copiile de rezervă, acceptanța integrărilor etc.	Obligatoriu
CNF159	**Optimizare performanță** Furnizorul asigură utilizarea judicioasă a resurselor sistemului (procesor, memorie, timpi de răspuns, volum date stocate/transmise). Serviciile prestate de sistem și componentele acestuia sunt optimizate conform practicilor bune din ramură. Cele mai intensive procese/funcționalități din perspectiva utilizării resurselor sunt identificate și justificate beneficiarului și operatorului MCloud.	Obligatoriu

Mentenanța și actualizarea

Cerințe referitoare la mentenanța sistemului după lansare.

ID	Cerință	Statut
CNF161	**Loguri de sistem** Sistemul jurnalizează evenimente de sistem utilizand o librărie utilizată pe larg în ramură ca de exemplu log4j, log4net sau similară.	Obligatoriu
CNF162	**Nivelul logurilor** Sistemul distinge cel puțin nivelurile de loguri tipice: Critical, Error, Warning, Info, Debug Evenimente de nivel Critical se jurnalizează pentru evenimente care necesită intervenția imediată a administratorului de sistem.	Obligatoriu
CNF163	**Conținutul logurilor** Fiecare înregistrare jurnalizată va include detalii despre: • tipul evenimentului • marca de timp • nivelul evenimentului • componenta sistemului care a generat înregistrarea • utilizator, adresa IP ce descriu persoana care a inițiat evenimentul • identificatorul obiectului informațional afectat • detalii text despre eveniment	Obligatoriu

ID	Cerință	Statut
CNF164	**Stopare grațioasă (graceful shutdown)** Sistemul asigură stoparea grațioasă (fără pierderea sau coruperea datelor în proces de prelucrare) a componentelor sistemului.	Obligatoriu
CNF165	**Codul sursă** Furnizorul va livra codul sursă a aplicației și instrucțiuni automatizate privind compilarea/împachetarea componentelor sistemului. Excepție fac doar componentele/librăriile terțe explicit identificate de furnizor și coordonate cu furnizorul.	Obligatoriu
CNF166	**Instalarea sistemului** Furnizorul va documenta și automatiza cât de mult posibil instalarea componentelor sistemului. Excepție de la cerință sunt părțile independente a soluției cum ar fi sistemul de operare, SGBD care sunt de fapt pre-condiții pentru instalare și sunt documentate și coordonate cu beneficiarul.	Obligatoriu
CNF167	**Pregătirea de actualizări** Furnizorul documentează lista modificărilor și modul de verificare și actualizare a acestora.	Obligatoriu
CNF168	**Actualizarea automatizată a componentelor sistemului** Furnizorul documentează procedura automatizată de actualizare a componentelor sistemului și include mijloacele necesare de automatizare a actualizărilor în pachetele program.	Obligatoriu
CNF169	**Copierea de rezervă** Furnizorul documentează procedura de copiere de rezervă, verificare și restaurare a datelor sistemului și include mijloacele necesare de automatizare a acestor procese. Furnizor oferă recomandări privind politica de copiere de rezervă necesari pentru criteriile de disponibilitate din CNF105. Notă: De obicei aceste procese utilizează mijloace ale sistemului de operare sau SGBD. Alternativ, furnizorul elaborează asemenea utilitare de sistem.	Obligatoriu

Interfața utilizator

Cerințe referitoare la interfața utilizator a sistemului.

ID	Cerință	Statut
CNF170	**Aspectul vizual al aplicatiei** Furnizorul propune și coordonează aspectul vizual a aplicației cu beneficiarul printr-un proces iterativ ce va include prezentări, colectarea feedback-ului și validarea etapizată a soluțiilor propuse.	Obligatoriu
CNF171	**Accesibilitate**	Obligatoriu

ID	Cerință	Statut
	Interfața utilizator este proiecta în conformitate cu nivelul AA a Practicilor de Accesibilitate pentru materiale Web (Web Content Accessibility Guidelines 2.2) https://www.w3.org/TR/WCAG22/	
CNF172	**Interfață multilingvă** Interfața utilizator este multilingvă și include suport pentru limbile Ro (implicit) En și Ru.	Obligatoriu
CNF173	**Aplicații Web Progresive** Interfața utilizator e proiectată conform practicilor pentru Aplicații Web Progresive (progressive web application PWA) pentru a oferi suport pentru dispozitivele mobile.	Obligatoriu
CNF174	**Rezoluția minimă - 1280px** Interfața utilizator e proiectată pentru lățimea de min. 1280px. Notă: Pentru lățimea ecranului mai mică sunt admise deteriorări a aspectului vizual a aplicației.	Obligatoriu
CNF175	**Asistență de context** Interfața utilizator oferă pentru părțile/elementele acesteia asistență de context sub forma de Hint sau Tip care sunt acționate prin plasarea șoricelului pe aria dorită sau actionarea unui buton dedicat marcat spre exemplu cu ”?”.	Obligatoriu
CNF176	**Pagini preferate sub forma de bookmark** Paginile majore a aplicației permit salvarea referințelor la acestea sub forma de bookmark.	Obligatoriu
CNF177	**Referințe lizibile** Referințele (URL) la paginile principale a aplicației sunt lizibile. Sistemul va evita includerea în referințe a elementelor tehnice care îngreunează înțelegerea acestora de utilizator și va îngreuna transcrierea manuală a acestora.	Obligatoriu
CNF179	**Interfete utilizator dedicate** SI RSIC are un front-office propriu. Interfata utilizator a sistemului include module dedicate specializate pentru a evita aglomerarea acesteia și confuzia utilizatorilor. Furnizor va coordona cu beneficiar continutul și tematica acestor module. Spre exemplu se pot distinge modulele:. • portal public, • aplicatia internă • configurare/extragere rapoarte • administrative	Obligatoriu
CNF181	**Afișare paginată** Se oferă afișarea paginată a colecțiilor de obiecte informaționale. Implicit pagina listează 25 rânduri cu opțiune pentru 50, 100 și alte valori coordonate cu beneficiar.	Obligatoriu
CNF182	**Coloane afișate în pagini**	Obligatoriu

ID	Cerință	Statut
	Paginile ce listează elementele vizualizate afișează cel puțin Identificator, Denumire, Tip, Statut, Coordonator și Data de creare. Se oferă opțiuni de a afișa mai multe sau mai puține coloane conform solicitării utilizator.	
CNF183	**Sortarea elementelor din pagini** Elementele din pagină sunt sortate implicit după Identificator în ordine descrescătoare (cele mai recente primele). Se oferă opțiuni utilizator de a sorta ascendent/descendent după oricare din coloanele afișate în pagină.	Obligatoriu
CNF184	**Evidențiere elemente** Elementele din pagină sunt evidențiate • statut Nou - cu text îngroșat • severitate Critică - cu text îngroșat roșu	Obligatoriu
CNF185	**Filtrare liste** Se oferă mijloace de filtrare a elementelor afișate conform criteriilor indicate de utilizator. Criterii de filtrare se oferă cel puțin pentru: • identificatori • utilizatori implicați • data/ora creare, modificare, soluționare, închidere • statut • severitate • prioritate • tip • prezența/lipsa înregistrărilor de diferite tipuri • distribuire	Obligatoriu
CNF186	**Elemente panou de bord** Pentru vizualizare date sunt oferite elemente/componente ce sunt integrate sub forma de panou de bord. Acestea includ cel puțin: • KPI cards - pentru afișare indicatori cheie de performanță • grafice linie, cu bare, plăcintă • grile ca spre exemplu pentru calendare • tabele (sumarizate) Filtrele din sistem pentru căutarea/extragerea datelor informează conținutul datelor afișate în elementele de panou de bord. Notă: Este anticipată utilizarea librăriilor existente de componente a panoului de bord și a capabilităților oferite de acestea. Furnizor va coordona cu beneficiarul elementele prezente în librărie și utilizarea acestora în sistem.	Obligatoriu
CNF187	**Panou de bord configurabil** Se oferă posibilitatea de a configura și ulterior ajusta panoul de bord și elementele de date afișate.	Obligatoriu

ID	Cerință	Statut
	Notă: Pentru configurarea panou(ri) de bord este preferat de a utiliza o interfață interactivă/drag-and-drop. Alternativ, fișierele de configurare pot fi utilizate în acest scop cu condiția ca formatul și conținutul fișierelor de configurare este documentat.	
CNF188	**Panou de bord interactiv** Se oferă posibilitatea de a interacționa cu elementele panoului de bord cel puțin: • maximizare element panou de bord unde datele dintr-un element a panoului de bord sunt afișate pe toată aria paginii • extragere date sub formă de PDF, CSV, XLS • navigare la subsetul de date care a format partea de vizualizare (ca spre exemplu la selectare cazuri critice pe un grafic cu bare distribuit după severitate apoi se va naviga la lista de cazuri care filtrată după severitate critică).	Obligatoriu
CNF189	**Coordonare elemente interfață** Furnizor în vederea coordonării elementelor de interfață utilizator elaborează : • machete grafice (wireframes și mockups) pentru toate ecranele relevante; • prototipuri interactive care reflectă fluxurile principale de utilizare; • design system cuprinzând componente reutilizabile, stiluri (culori, tipografie), reguli de spațiere și stări ale elementelor (hover, focus, eroare). Elementele de interfață sunt realizate și puse la dispoziția Beneficiarului printr-o platforma ca spre exemplu Figma, printr-un link dedicat ce permite vizualizarea, comentarea și inspectarea elementelor de către toate părțile implicate. Notă: Furnizor asigura că designul este pregătit pentru implementare, incluzând: • specificații clare despre dimensiuni, culori, stiluri, comportamente responsive; • consistență vizuală și funcțională la nivelul întregii aplicații.	Obligatoriu

Documente și instruire

Cerințe referitoare la documentarea sistemului și instruiri

ID	Cerință	Statut
CNF191	**Limba de comunicare** Limba de comunicare de bază este Ro. Furnizorul va asigura traducerea comunicărilor, inclusiv disponibilitatea translatorilor în cazul comunicării în alte limbi. Se admite pregătirea materialelor în En cu condiția că ulterior vor fi furnizate traducerile acestora.	Obligatoriu
CNF192	**Manuale utilizator** Furnizorul include în livrabile următoarele manuale/materiale destinate utilizatorilor sistemului: • manual utilizator care acoperă funcționalitatea sistemului din perspectiva rolurilor utilizator • manualul admininistratorului care include detalii despre configurarea, depanarea și customizarea sistemului atât cu mijloacele oferite de sistem cât și cu utilitare externe cum ar fi cele oferite de sistemul de operare	Obligatoriu
CNF193	**Tutoriale video** Furnizorul oferă tutoriale video care ghidează utilizatorii în realizarea activității de zi cu zi în sistem.	Obligatoriu
CNF194	**Documente tehnice** Furnizorul livrează documente tehnice ce acoperă: • arhitectura și proiectarea de detaliu a sistemului (SDD - system design document) • ghidul de instalare și configurare • strategia, planul și rapoarte de testare	Obligatoriu
CNF195	**Codul sursă** Furnizorul livrează codul sursă pentru compilarea sistemului inclusiv instrucțiuni de compilare, scripturi de automatizare, scripturi de instalare inclusiv configurarea securizată a sistemului. Notă: Procedurile MCloud presupun utilizarea unui repozitoriu de control a versiunilor pe bază de Git în care se vor încărca modificările sistemului și din care se va realiza pregătirea spre instalare a aplicațiilor.	Obligatoriu
CNF196	**Referințe API** Furnizorul documentează API prestat de sistem sub forma de API Reference care are la bază WSDL sau Swagger	Obligatoriu
CNF197	**Instruiri** Furnizorul pregătește curicula de instruire și materialele necesare pentru: • utilizatorii sistemului	Obligatoriu

ID	Cerință	Statut
	• administratorii sistemului	
CNF198	**Instruirea formatorilor** Furnizorul va instrui un grup de 10-15 formatori desemnati de beneficiar pentru a-i pregăti să instruiască la rândul lor personalul care utilizează sistemul.	Obligatoriu

Raportare și taxonomie

Cerințe privind structurile de date formalizate a rapoartelor și serviciilor prestate de sistem sub forma de taxonomie/catalog semantic.

ID	Cerință	Statut
CNF201	**Catalogul semantic** Serviciile prestate de sistem sunt pregătite pentru a fi integrate și publicate in catalogul semantic: semantic.gov.md	Obligatoriu
CNF202	**Taxonomii MISP** O sursă primară de taxonomii (pregătită pentru consum automat) este menținută în proiectul MISP (https://github.com/MISP/) și anume MISP-taxonomies (https://github.com/MISP/misp-taxonomies)	Obligatoriu
CNF203	**Taxonomii - excluse** Se oferă posibilitatea de a ascunde anumite taxonomii din setul integral pentru a evita aglomerarea valorilor disponibile propuse utilizatorilor. Valorile exacte din taxonomie pot fi reproduse manual in asemenea cazuri.	Obligatoriu
CNF204	**Spatiul de nume/predicate taxonomie** Valorile descrise în taxonomii sunt însoțite de spațiu de nume, predicat/categorie valorilor înregistrate. Se coordonează cu beneficiar modul preferat de afișare a acestor valori spre exemplu: • integral unde toate elementele sunt afișate • scurt - unde doar valoarea este afișată dar evidențiată cu opțiunea de a vizualiza întreaga valoare într-un tooltip	Obligatoriu
CNF205	**Valorile din taxonomii tratate ca etichete (tag)** Valorile descrise în taxonomii sunt utilizate sub forma de etichete în informațiile înregistrate (#tag) și disponibile sub forma de filtre setate de utilizator	Obligatoriu
CNF206	**Evidențiere valori din taxonomii** Se aplică o modalitate de evidențiere a valorilor din taxonomii. Pe langa tratarea acestora sub formă de #etichete se oferă opțiunea de a seta culoare text/fundal a unei categorii de valori din taxonomie.	Obligatoriu
CNF207	**Valori din taxonomii admise în câmpuri textuale**	Obligatoriu
CNF208	**Valori din taxonomii reflectate în statistici**	Obligatoriu

ID	Cerință	Statut

Garantie si suport

Cerințe referitoare la perioada de garanție și suport pentru beneficiar și utilizatori

ID	Cerință	Statut
CNF211	**Mentenanța de corecție - 12 luni** Adițional la perioada de garanție de 12 luni furnizorul își va confirma disponibilitatea de a oferi suport pentru sistem pentru următorii 5 ani. Notă: Contractarea serviciilor extinse este agreată separat.	Obligatoriu
CNF212	**Servicii de suport** Furnizorul va oferi servicii de suport tehnic pentru sistem pe perioada de mentenanță care includ: • remedierea defectelor sistemului • asistență tehnică pentru beneficiar privind operarea și mentenanța sistemului	Obligatoriu
CNF213	**Remedierea defectelor** Furnizorul va soluționa (pozitiv sau negativ) toate defectele identificate pe perioada de garanție	Obligatoriu
CNF214	**Defecte critice** Defectele critice sunt luate în lucru de furnizor în max 2 ore de la momentul raportării și soluționate în max 6 ore. Dacă o soluție temporară sau permanentă nu este posibilă în timpul max acordat apoi furnizorul va raporta la fiecare 1 ore progresul înregistrat și timpul tentativ de soluționare.	Obligatoriu
CNF215	**Defecte non-critice** Defectele non-critice sunt confirmate de furnizor în max 8 ore de la raportare și sunt soluționate în max 5 zile lucrătoare.	Obligatoriu
CNF216	**Solicitări de modificare** Furnizorul oferă un mecanism prin care solicitările de modificare a sistemului vor fi adresate pe perioada de garanție ca spre exemplu forma în care acestea sunt coordonate, disponibilitatea personalului tehnic pentru efectuarea lucrărilor, modul de compensare, orizontul de timp etc.	Obligatoriu
CNF217	**Darea în exploatare** Furnizorul pregătește și coordonează planul de dare în exploatare a sistemului.	Obligatoriu

Foaie de parcurs

În tabelul ce urmează este prezentată o foaie de parcurs tentativă pentru elaborarea și implementarea sistemului. Fila dată este disponibilă și ca fișier PDF separat pentru a fi mai ușor citibilă.

Foaia de parcurs este prezentată în săptămâni de la începutul lucrărilor la proiect. Beneficiarul urmează să se încadreze într-o durată de elaborare/implementare de aproximativ 6-7 luni calendaristice (27-29 săptămâni). După aceasta începe perioada de garanție, suport tehnic și mentenanță de 12 luni (52 săptăpmâni).

În foaia de parcurs propusă sunt identificate o serie de sub-activități evidențiate în roșu. Acestea pot reprezenta un risc pentru încadrarea în durata propusă a proiectului și necesită o atenție sporită a furnizorului. Spre exemplu integrarea cu serviciile de platformă tehnologică comună a guvernării includ atât aspecte organizaționale/contractuale cât și aspecte tehnice și aceasta poate tărăgăna semnificativ lucrurile. Din acest motiv activități de analiză a integrărilor date dar și sub-activități ce țin de acorduri și ulterior de implementarea interfețeor sunt prezentate în foaia de parcurs.

Așteptările beneficiarului sunt ca furnizorul anticipând riscurile evidențiate:

- să aloce personal mai experimentat pentru cazurile unde există sub-activități riscante,
- să inițieze lucrări de clarificare și analiză în avans,
- să stabilească puncte de contact cu echipa de suport a acestor servicii,
- să utilizeze o echipă dedicată mai mare.

De notat că pentru pregătirea lucrărilor de acceptanță la finalizarea lucrărilor de elaborare beneficiar urmează să formeze un grup de lucru care deja are cunoștințele și așteptările necesare privind sistemul. Pentru aceasta grupul de lucru va fi format în avans iar furnizorul va organiza o serie de demonstrări/prezentări a aspectelor importante a soluției pentru acest grup. În așa mod întrebări și îngrijorări privind soluția finală vor fi anticipate și adresate din timp.

Roluri cheie

Echipa de proiect a furnizorului trebuie să includă cel puțin următoarele roluri cheie:

- manager de proiect
- analist de business/sistem
- arhitect software
- expert securitate cibernetică
- specialist integrare cu servicii guvernamentale partajate
- specialist DevOps/deployment MCloud
- QA/test automation
- UX/UI expert
- specialist instruire

Ofertele furnizorilor vor include profiluri a acestor specialiști și nivelul lor de experiență.

Anexa: FNV - Formular Notificare de Vulnerabilitate

ASC utilizează un formular tipizat de prezentare a datelor din Notificarea de Vulnerabilitate. Conținutul și stilizarea în vigoare a acestuia este coordonată cu beneficiar. Pentru exemplificare documentul include un exemplar în fișierul atașat:

- Formular_Notificare_Vulnerabilitate.docx