SPECIFICAŢII TEHNICE

Anexa nr. 22 la Documentația standard
aprobată prin Ordinul Ministrului Finanţelor nr. 115 din 15.09.2021

Numărul procedurii de achiziție: ***Licitație deschisă 21532341/ ocds-b3wdp1-MD-1766753786343***
Denumirea licitaţiei: ***Servicii de dezvoltare reingineria și automatizare a SIA „Registrul Informaților Criminalistice și Criminologice" (etapa II)***

Denumirea serviciilor	Denumirea modelului serviciului	Ţara de origine	Produ-cătorul	Specificarea tehnică deplină solicitată de către autoritatea contractantă	Specificarea tehnică deplină propusă de către ofertant	Standarde de referinţă
1	2	3	4	5	6	7
Lotul 1 Servicii de dezvoltare reingineria și automatizare a SIA „Registrul Informaților Criminalistice și Criminologice"						
Reingineria și automatizare a SIA „Registrul Informaților Criminalistice și Criminologice"	----	MD	DSS	Conform Caietului de sarcini și Termenilor de Referinţă (anexa la Caietul de sarcini)	Ăn strictă conformitate cu cerințe din Caietul de sarcini, Termenii de Referinţă și Descrierea tehnică anexată.	**ISO**

Semnat:_____
Numele, Prenumele: Sirbu Ion
În calitate de: Director
Ofertantul: DAAC Software Systems S.R.L.
Adresa: mun.Chisinau str.Calea Iesilor 10

Digitally signed by Sîrbu Ion
Date: 2026.01.19 12:33:49 EET
Reason: MoldSign Signature
Location: Moldova

MOLDOVA EUROPEANĂ

DAAC digital

Serviciul Tehnologii Informaționale al MAI

Codul CPV: 48200000-0

Oferta tehnică

privind reinginerie și automatizare a proceselor de lucru aferente gestiunii Registrului Informațiilor Criminalistice și Criminologice în cadrul Ministerului Afacerilor Interne

Aprobat: Sîrbu Ion
Director
DAAC Software Systems S.R.L.
Data: 20.01.2026
Semnătura: _____

CUPRINS

1 LISTA DE CONFORMITATE CU CERINȚELE

Tabel de navigație privind cerințele documentației de atribuire (Etapa 2)

Categoria informațiilor solicitate	**Descrierea cerinței (conform documentației de atribuire)**	**Referință secțiune ofertă / Număr pagină**
1. Date administrative și calificare		
Documentul Unic de Achiziții European (DUAE)	Confirmarea îndeplinirii criteriilor de selecție și absența motivelor de excludere.	A se vedea doc. DUAE DSS; DUAE DSI
Dreptul de exercitare a activității (Licențe)	Copia licenței de activitate și/sau autorizației de funcționare în domeniul dezvoltării sistemelor informaționale.	A se vedea doc. Extras DSS 28.11.2025; Extras DSI 13.11.2025
Dovada înregistrării persoanei juridice	Certificat/decizie de înregistrare și extrasul din Registrul de Stat al persoanelor juridice.	A se vedea doc. Certificat de inregistrare
2. Experiența și capacitatea tehnică		
Experiența specifică în domeniu	Minim 3 ani (2022-2025) de experiență în dezvoltarea sau mentenanța Sistemelor Informaționale Automatizate.	A se vedea doc. Oferta STI MAI Reingineria Automatizarea RICC Etapa II
Lista contractelor realizate	Lista livrărilor efectuate în ultimii 3 ani (minim un contract de 50% din valoarea lotului curent).	A se vedea doc. Oferta STI MAI Reingineria Automatizarea RICC Etapa II
Scrisori de recomandare	Prezentarea a cel puțin două scrisori de recomandare de la instituții publice.	A se vedea doc. Scrisori de recomandare
Standarde de asigurare a calității și securității	Deținerea certificatelor ISO 9001 și ISO 27001.	A se vedea doc. Certificate ISO 2025-2028
Descriere metodologie de implementare		A se vedea p. «Abordarea de dezvoltare»
Descrierea generală a soluției propuse (arhitectură, tehnologie, structurare, performanțe, eventuale referințe de la implementări ale soluției);		A se vedea: p. «Principiile generale de constituire a sistemului» p. „Descrierea zonei de automatizare”

		p. ”Arhitectura” p. „Modelul-business al domeniului de automatizare”
Licențiere și proprietate intelectuală		A se vede p. Licențiere și proprietate intelectuală
3. Personalul și echipa de proiect		
Componența echipei de proiect	Lista experților cheie: Manager de proiect, analist de business, dezvoltatori (.NET/C#), administrator BD, specialist migrare și QA.	A se vedea p. 17 Echipa de proiect
Calificarea experților propuși	CV-urile specialiștilor	A se vedea CV-urile atasate
4. Metodologia și organizarea lucrărilor		
Fazele proiectului	Descrierea etapelor de analiză, proiectare (SRS/SDD), dezvoltare, testare și lansare în producție.	A se vedea p. 18 Fazele proiectului si Planul de implementare
Programul de implementare (Timeline)	Graficul de execuție cu termenul limită 24 decembrie 2026.	A se vedea p. 18 Fazele proiectului si Planul de implementare
Managementul riscurilor și schimbării	Metodologia de gestionare a riscurilor și a modificărilor pe parcursul proiectului.	A se vedea doc. "Project implementation risk management EN.pdf"
5. Garanție și suport tehnic		
Obligații de garanție	Mentenanța și suportul tehnic pentru o perioadă de 12 luni de la recepția finală.	A se vedea p. 19 Metodologia de suport și mentenanță tehnică
Nivelul serviciilor (SLA)	Timpul de răspuns (TR) și de soluționare (TS) în funcție de criticitatea incidentelor.	A se vedea p. 19 Metodologia de suport și mentenanță tehnică
Serviciul de suport (ServiceDesk)	Descrierea asistenței tehnice oferite prin intermediul unui serviciu permanent de tip ServiceDesk.	A se vedea p. 19 Metodologia de suport și mentenanță tehnică
6. Propunerea Tehnică: Specificații și Cerințe		

Conformitatea cu cerințele funcționale și nefuncționale	Descrierea detaliată a modului în care soluția satisface cerințele funcționale (UC01–UC25) și specificațiile nefuncționale privind performanța, securitatea și stiva tehnologică.	A se vedea p. «Check-list»
Metodologia de migrare a datelor	Metodologia și instrumentele pentru transferul datelor istorice din "RICC Old" în noul sistem.	A se vedea p. 15 Transformarea și migrarea datelor

2 INFORMAȚII GENERALE

Sistemul informațional automatizat ”Registrului Informaților Criminalistice și Criminologice” (în continuare SIA «RICC»), este resursă informațională de stat, care reprezintă totalitatea informației sistematizate despre infracțiuni, cauze penale, precum și despre persoanele care au săvârșit infracțiuni și alte obiecte supuse evidenței. SIA RICC este parte componentă a resursei informaționale integrate a organelor de drept, care, la rândul său, intră în componența Resurselor informaționale de stat ale Republicii Moldova. Până în prezent SIA «RICC» se asigură suportul informațional al activității organelor de drept și altor autorități administrative centrale cu atribuții în domeniul asigurării ordinii publice și combaterii infracționalității.

3 TERMENI ȘI ABREVIERI

Pentru înțelegerea corectă a ofertei respective, se utilizează termeni și abrevieri determinate în caietul de sarcini destinat achiziționării serviciilor de programare, dezvoltare și implementare a SIA ”e-Dosar”, de asemenea în Regulamentul Tehnic al Republicii Moldova RT 38370656 - 002:2006

Suplimentar, s-au determinat următorii termeni:

Nr.	Abreviere/ Acronim	Descriere
1.	MAI	Ministerul Afacerilor Interne al Republicii Moldova
2.	IDNO	Numărul de identificare al persoanei juridice, numărul unic din 13 cifre
3.	IDNP	Numărul de identificare al persoanei fizice, numărul unic din 13 cifre
4.	IGP	Inspectoratul General de Poliție al MAI
5.	RICC	Registrul informației criminalistice și criminologice
6.	ToR	Termeni de Referință
7.	BD	Bază de Date
8.	SIA	Sistemul informațional automatizat
9.	CPIA	Centrul principal de informare și analiză
10.	BDDP	Bază de date cu documente primare
11.	FSU	Format de schimb unificat

12.	BDI	Bancă de date integrată
13.	SII	Sistem informatic integrat
14.	RI	Resurse de informații
15.	CII	Cartea infracțiunilor și incidentelor
16.	MAI	Ministerul Afacerilor Interne
17.	BII	Banca interstatală de informații
18.	SO	Sistem operațional
19.	FOI	Fişierul operativ-informaţional al persoanelor care au săvârşit infracţiuni
20.	CSI	Comunitatea Statelor Independente
21.	ISC	Interfață specială de căutare
22.	SGBD	Sistem de gestionare a bazei de date
23.	ST	Sarcina tehnică
24.	BDC	Baza de date centrală
25.	RSP	Registrul de stat al populației
26.	RSUD	Registrul de stat al unităților de drept
27.	Responsabil (înregistrarea sesizărilor)	Specialistul autorizat să înregistreze sesizările în sistemul RICC
28.	Responsabil (introducerea altor date)	Specialistul autorizat să introducă alte date în sistemul RICC

4 ABORDAREA DE DEZVOLTARE

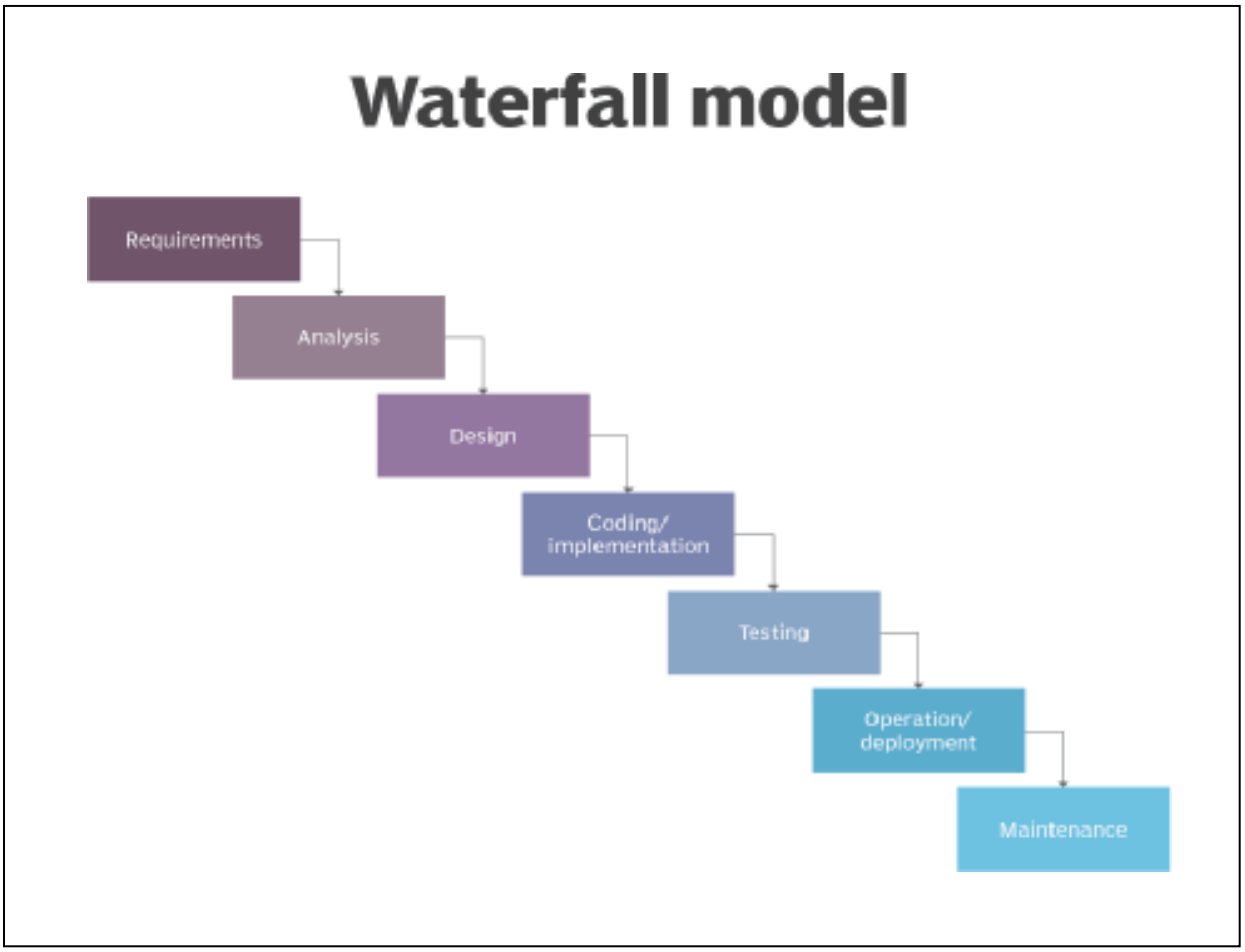
4.1 INFORMAȚII GENERALE

Modelul în cascadă (Waterfall) este un model de dezvoltare software în care procesul de realizare a aplicației urmează un flux secvențial, trecând consecutiv prin fazele de analiză a cerințelor, proiectare, implementare, testare, livrare și suport.

În conformitate cu modelul Waterfall, dezvoltatorul de sistem parcurge etapele într-o succesiune strictă, fără revenire la fazele anterioare:

- În prima etapă se finalizează complet definirea cerințelor, rezultând o listă detaliată de cerințe funcționale și nefuncționale ale sistemului software.
- Odată ce cerințele au fost clar definite și aprobate, se trece la etapa de proiectare, în cadrul căreia sunt elaborate documente tehnice care descriu modul în care cerințele vor fi implementate din punct de vedere arhitectural și logic.
- După finalizarea completă a proiectării, programatorii implementează soluția tehnică conform specificațiilor.
- Etapa următoare presupune dezvoltarea componentelor individuale de către diferite echipe de programatori, în conformitate cu planul stabilit.
- Ulterior, după finalizarea implementării și livrării interne, are loc testarea și depanarea produsului software. În această fază sunt identificate și corectate defectele apărute în etapele anterioare.
- În final, produsul software este implementat în mediul de producție, se realizează instruirea utilizatorilor, derularea exploatării pilot și ulterior se asigură suportul continuu, inclusiv corectarea erorilor și adăugarea de funcționalități noi.

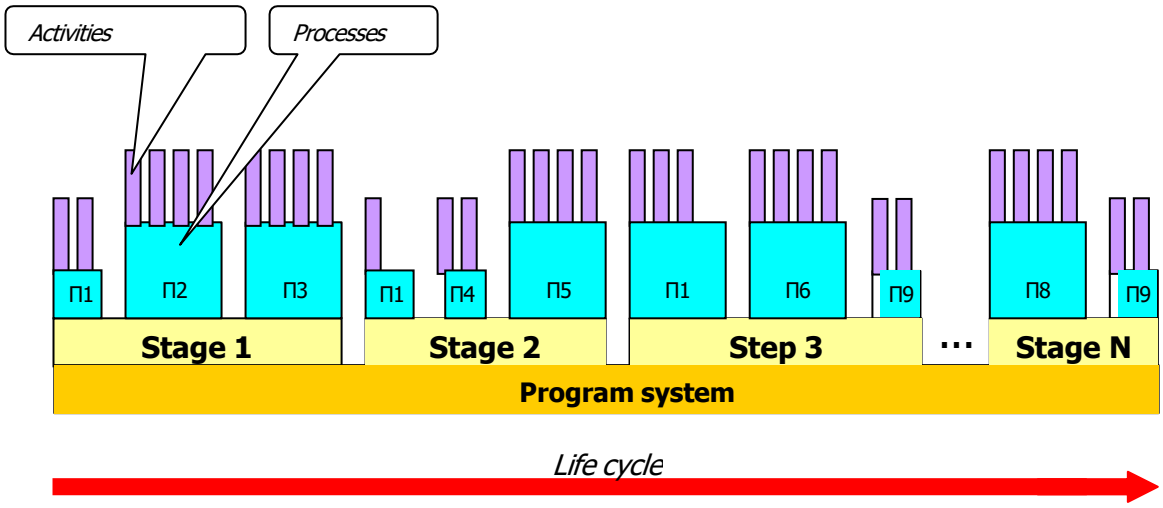
4.2 ALGORITMUL DE ACȚIUNE



Algoritmul acțiunilor în metodologia "Waterfall"

Pentru implementarea proiectului, alegem o modificare a modelului Waterfall — modelul "Sashimi" sau modelul Waterfall cu faze suprapuse. În acest model, la fel ca în metodologia originală, fazele se succed, dar se suprapun în timp.

Ciclul de viață al unui sistem software conform metodologiei Waterfall-Sashimi constă într-o serie de etape în care sistemul software este planificat, creat, implementat, operat, întreținut și dezafectat. Acest lucru este ilustrat printr-un model tipic al ciclului de viață al sistemului software prezentat în figura de mai jos.



Modelul ciclului de viață al sistemului software conform metodologiei Waterfall

4.3 ETAPELE CICLULUI DE VIAȚĂ

Etapele ciclului de viață sunt organizate în secvențe care pot să se suprapună și/sau să se repete, în funcție de limitele, dimensiunea, complexitatea, nevoile în schimbare și capacitățile de implementare ale sistemului software. Acestea sunt iterative și se realizează prin acțiuni pas cu pas.

Modelul ciclului de viață al metodologiei Waterfall pentru un sistem software constă în șase etape:

1. Analiza cerințelor proiectului. Se definesc cerințele programului pentru domeniul informațional al sistemului.

2. Proiectare. Se dezvoltă și se formulează o specificație tehnică logică și coerentă a sistemului software. Detalierea sistemului.

3. Dezvoltare. Realizarea unui proiect complet funcțional.

4. Testarea produsului. Exploatarea de test a produsului.

5. Implementare. Include instalarea produsului, instruirea personalului și acceptarea oficială a produsului.

6. Suport. Furnizarea de asistență tehnică pentru produs după lansarea comercială.

ANALIZA CERINȚELOR PROIECTULUI

Aceasta este, probabil, cea mai responsabilă și importantă etapă în crearea unui sistem software de succes. Toate informațiile colectate sunt utilizate pentru a planifica abordarea de bază a proiectului.

În plus, în această fază se planifică cerințele de asigurare a calității și se identifică diverse riscuri asociate proiectului. Rezultatul analizei constă în identificarea diferitelor abordări tehnice care pot fi utilizate pentru implementarea cu succes a proiectului, cu riscuri minime.

În această etapă, echipa de specialiști și părțile interesate convin asupra tuturor detaliilor viitorului produs, răspunzând la întrebări esențiale:

- Care este scopul viitorului produs?
- Ce probleme ar trebui să rezolve?
- Pentru ce este creat produsul?

După clarificarea acestor aspecte, toți participanții au o viziune comună și corectă asupra viitorului produs. Acest lucru facilitează dezvoltarea și minimizează riscurile în crearea software-ului.

PROIECTAREA ȘI DOCUMENTAREA CERINȚELOR

După finalizarea analizei inițiale a cerințelor, următorul pas este definirea clară și documentarea completă a cerințelor pentru produs, urmată de aprobarea acestora de către Client. Dacă scopul primei etape a fost înțelegerea și analiza cerințelor, atunci în această etapă toate obiectivele trebuie formalizate și documentate — acest lucru oferă protecție ambelor părți implicate.

În această fază, echipa de specialiști colaborează cu reprezentanții Clientului și, în unele cazuri, chiar și cu potențiali utilizatori finali, pentru a colecta toate detaliile relevante privind dezvoltarea proiectului. Procesul pornește de la cercetarea pieței și continuă până la definirea stack-ului tehnologic și a funcționalităților viitorului produs.

Toate aceste informații sunt ulterior înregistrate în documentația proiectului, care stă la baza planificării etapelor de dezvoltare, a cronogramului și a termenelor de execuție pentru livrabilele succesive.

După ce cerințele funcționale și stack-ul tehnologic au fost clarificate, se poate trece la proiectarea tehnică și arhitecturală. În această etapă, echipa de dezvoltare elaborează arhitectura viitorului sistem, utilizând tehnologia selectată. Se creează un design adaptiv și orientat pe experiența utilizatorului, se planifică legătura dintre partea de interfață (frontend) și server (backend), se definesc modulele și se proiectează sistemul de securitate al aplicației.

DEZVOLTARE

Etapa de dezvoltare reprezintă faza în care codul sursă este efectiv scris. Specialiștii tehnici utilizează documentația proiectului, prototipurile, designul și arhitectura pentru a crea aplicația sau site-ul web viitor.

Sarcinile sunt distribuite între membrii echipei conform specializării fiecăruia:

- Dezvoltatorii back-end sunt responsabili pentru crearea logicii serverului și asigurarea comunicării eficiente între interfața utilizatorului și server.
- Administratorii de baze de date gestionează structura și integritatea

datelor, asigurând stocarea și accesul optim la informații.

- Dezvoltatorii front-end creează interfața responsivă a aplicației web, garantând o experiență utilizator fluidă și intuitivă.

Rezultatul acestei etape este un produs software funcțional, pregătit pentru testare și implementare ulterioară.

TESTARE

Crearea unui produs funcțional nu reprezintă finalul ciclului de dezvoltare. După faza de dezvoltare urmează etapa de testare. În această etapă, echipa compară aplicația concepută în faza de analiză a cerințelor cu cea realizată după implementare. Se răspunde la întrebări esențiale precum:

- Toate funcționalitățile planificate și integrările funcționează corect?
- Toate butoanele/interfețele reacționează corespunzător?
- S-a obținut rezultatul final specificat în cerințele inițiale?

Înainte de trecerea la exploatarea comercială a sistemului, este esențială verificarea performanței în toate modurile prevăzute în specificație, inclusiv în „condiții extreme”. De exemplu, dacă este planificată introducerea distribuită a datelor de către 100 de utilizatori simultan, trebuie verificat dacă sistemul poate procesa corect activitatea simultană a acestora. Aceasta este ideea de bază a testării de încărcare (load testing).

Testarea de încărcare

Are scopul de a prezice comportamentul sistemului în condiții reale și extreme, de a detecta erori, de a monitoriza performanța și disponibilitatea în condiții variate. Obiectivele includ:

- Evaluarea performanței aplicației în următoarele faze:
  - Dezvoltare;
  - Exploatare pilot;
  - Mentenanță și lansări (patch-uri, actualizări).
- Optimizarea aplicației.
- Selectarea platformei hardware/software optime și a configurației serverului:

Categorii esențiale de testare:

Testare de performanță (load testing)

Simularea unui volum mare de utilizatori care accesează simultan diferite module:

- Determinarea timpului de execuție pentru diverse operațiuni la diferite nivele de încărcare;
- Stabilirea performanței maxime posibile a sistemului

Testare de stres (stress testing)

Testarea comportamentului sistemului la sarcini peste limita planificată:

- Evaluarea capacității sistemului de a reveni la parametri normali după suprasarcină;
- Esențială pentru sisteme critice unde eșecul ar avea costuri ridicate.

Testare de fiabilitate (reliability testing)

- Determinarea duratei de funcționare fără erori;
- Stabilitatea sistemului în condiții de încărcare medie pe perioade extinse;
- Identificarea:
  - Scăpărilor de memorie;
  - Configurațiilor incorecte;
  - Rebooturi neplanificate ale serverului.

Testare de configurație (configuration testing)

- Evaluarea impactului modificărilor de configurare asupra performanței
- Compatibilitate cross-platform / cross-browser
- Identificarea „bottleneck”-urilor în modulele sistemului
- Determinarea configurației hardware optime
- Verificarea compatibilității cu OS-uri și

aplicații terțe Pașii implicați:

1. Crearea unei matrice de acoperire pentru toate configurațiile posibile
2. Prioritizarea acestora
3. Planificarea ciclului de viață al testelor
4. Organizarea efectivă a testării conform priorităților

Testare de volum (volume testing)

Această etapă evaluează stabilitatea și performanța aplicației în condițiile procesării unor volume mari de date și a unui număr crescut de utilizatori. Se urmărește determinarea limitei maxime de utilizatori activi simultan fără degradarea performanței.

Absenta unei astfel de testări poate crește semnificativ riscurile operaționale și poate conduce la eșecul soluției într-un interval scurt după implementare. Pentru a preveni aceste riscuri, este esențial ca testarea să fie organizată corespunzător încă din faza de implementare, fiind aplicabilă și sistemelor deja în producție.

Dacă aplicația nu funcționează conform așteptărilor, problemele identificate în această etapă sunt comunicate echipei de dezvoltare pentru remediere. După efectuarea corecțiilor necesare, produsul este pregătit pentru următoarea fază a ciclului de viață.

Secvența activităților necesare pentru efectuarea acestui tip de testare:

1. Se creează o matrice de acoperire care descrie toate configurațiile posibile ale sistemului.
2. Se efectuează prioritizarea configurațiilor.
3. Se planifică ciclul de viață al testării (IP lifecycle).
4. În final, se organizează testarea tuturor configurațiilor majore, conform priorităților stabilite.

IMPLEMENTARE

Etapa de implementare a sistemului reprezintă una dintre cele mai importante faze din perspectiva distribuției responsabilităților între Client și Furnizor. Rolul principal al Furnizorului constă în instalarea modulelor pe serverul de producție, prin migrarea configurației finale din mediul de test.

Totuși, prin formarea corespunzătoare și implicarea activă a specialiștilor Clientului în procesul de creare și implementare a sistemului, o serie de activități pot fi preluate de aceștia, inclusiv:

- Asigurarea funcționalității rețelei locale (LAN) pentru toate stațiile de lucru
  automatizate ale utilizatorilor.
- Configurarea serverului de producție.
- Stabilirea listei și a numărului de stații de lucru care urmează să fie utilizate în
  etapa OP (operare pilot).
- Instalarea și configurarea posturilor de lucru, inclusiv alocarea drepturilor de
  acces.
- Pregătirea informațiilor actualizate pentru fiecare modul al sistemului, inclusiv gestionarea nomenclatoarelor care ar putea să-și fi pierdut

relevanța între faza de testare și cea de implementare.

- Organizarea mecanismelor de actualizare a datelor din sistem, inclusiv integrarea cu sisteme externe.

Scopul principal al acestei etape este pregătirea sistemului pentru exploatarea pilot, prin instruirea utilizatorilor finali, introducerea datelor inițiale și emiterea documentației necesare privind trecerea în regim pilot.

Activități majore ale etapei de implementare:

- Asigurarea îndeplinirii necondiționate a tuturor cerințelor de pregătire a modulelor pentru lansarea în regim de operare pilot (conform unui document dedicat).
- Introducerea și validarea datelor inițiale (de exemplu: solduri de început) în fiecare
  modul.
- Simularea acțiunilor reale ale utilizatorilor în paralel cu aplicațiile deja existente,
  direct la posturile de lucru.
- Elaborarea, coordonarea și aprobarea regulamentelor interne de interacțiune între departamentele clientului implicate în utilizarea sistemului în regim OP.
- Integrarea modulului cu alte module sau sisteme externe implementate anterior.

Condiții necesare pentru lansarea etapei OP:

- Modulele sistemului au fost migrate cu succes și funcționează pe serverul de producție și pe posturile de lucru ale utilizatorilor, cu drepturi de acces configurate corespunzător.
- Toate nomenclatoarele lipsă au fost completate și introduse în sistem, fiind reconciliate corespunzător.
- Documentația finală a fost aprobată de către Client.

Instruirea utilizatorilor

Instruirea se realizează pe baza principiilor fundamentale de utilizare a sistemului, prin exemple de control, individual pentru fiecare modul. Utilizatorii sunt familiarizați cu interfața aplicației, regulile de lucru și funcționalitățile de bază. În cazul existenței ghidurilor metodologice, acestea vor fi puse la dispoziția utilizatorilor pentru studiu suplimentar.

Etapele principale de instruire:

1. Instruirea utilizatorilor-cheie în etapa de implementare, înainte de organizarea
   testelor.

2. Instruirea utilizatorilor-cheie înainte de instalarea pe serverul de test (banc).

3. Instruirea utilizatorilor finali înainte de lansarea în regim de exploatare pilot.

Așa cum se poate observa, această divizare a etapelor este determinată de trei repere

principale:

În primul rând, este necesar să fie explicate principiile de funcționare ale sistemului deja configurat înaintea primei testări cu utilizatorii-cheie.

Următorul reper — instalarea pe serverul de testare (banc de lucru) — este important ca etapă intermediară, în cadrul căreia utilizatorii-cheie vor fi implicați din nou, de această dată pentru a descrie funcționarea sistemului și interfețele într-un mod mult mai detaliat, astfel încât să fie identificate și eliminate toate observațiile critice rămase înainte de trecerea la operarea pilot (OP).

Desigur, până la acest moment, toți specialiștii IT care vor fi implicați în suportul sistemului trebuie să cunoască în detaliu arhitectura internă a soluției și să fie capabili să efectueze revizii sau să genereze cerințe de modificare, dacă este necesar.

În cele din urmă, este organizată cea mai amplă instruire pentru restul angajaților care vor lucra efectiv cu sistemul. În acest caz, sistemul este prezentat nu din perspectiva arhitecturii tehnice, ci din punctul de vedere al utilizatorului final — axat pe principiile de introducere, procesare și regăsire a datelor.

Indiferent de specificul sistemului, al domeniului de aplicare sau al etapei de instruire, următoarele activități sunt necesare pentru organizarea eficientă a procesului de formare::

Pasul 1: Identificarea utilizatorilor-cheie

În primul rând, sunt identificați „utilizatorii-cheie” – unul sau doi specialiști din fiecare unitate funcțională (împărțirea poate fi logică, nu neapărat organizațională).

Sprijinul acestor persoane este esențial în etapa următoare, în cadrul instruirii utilizatorilor finali, deoarece, pe lângă faptul că pot oferi observații privind utilizarea sistemului și necesitatea unor îmbunătățiri, experiența lor practică ajută ceilalți utilizatori să înțeleagă modul de lucru în sistem și să nu apeleze la echipa de suport a Furnizorului pentru orice întrebare.

Este important de menționat că, în funcție de amploarea și specificul sistemului, acești specialiști pot lucra nu doar cu partea de utilizare a sistemului, ci și cu deplasarea și configurarea independentă a modulelor funcționale, în funcție de cerințele utilizatorilor.

Din acest motiv, formarea, certificarea și implicarea lor activă trebuie să aibă loc mult înainte de etapa OP, deoarece majoritatea angajaților vor interacționa cu sistemul pentru prima dată abia în faza de operare pilot sau industrială, atunci când acești utilizatori-cheie vor deveni formatori și puncte de sprijin.

Cursurile de instruire pentru utilizatorii-cheie (pe domenii funcționale) sunt organizate de echipa Furnizorului și pot include certificare.

Forma de organizare poate fi:

- în format fizic (cu trainer din partea Furnizorului, la sediul Clientului sau Furnizorului);
- la distanță – în cazul în care prezența fizică nu este posibilă sau oportună.

Webinariile și teleconferințele devin din ce în ce mai populare, oferind eficiență în timp și costuri reduse..

Pasul 2: Instruirea utilizatorilor finali

Până la acest punct, este necesar ca un număr suficient de specialiști din echipa de implementare a Clientului să fie capabili să:

- instaleze și configureze componentele funcționale ale sistemului la stațiile de lucru;
- instruiască utilizatorii finali;
- ofere suport legat de configurarea standard;
- mențină sistemul în regim operațional.

Metodologia instruirii poate varia în funcție de dimensiunea companiei, proiectului sau preferințele Clientului. În practică, instruirile se desfășoară:

- în mai multe sesiuni;
- în grupuri mici (10–15 persoane);
- formate în funcție de rolul fiecărui tip de utilizator.

Temele abordate includ:

- Prezentare generală a obiectivelor sistemului;
- Navigarea și utilizarea interfeței;
- Funcționalități de bază;
- Funcționalități specifice rolului;
- Sesiuni de întrebări și răspunsuri.

Uneori, instruirea este urmată de configurarea parametrilor necesari direct la stațiile de lucru (ex. integrare cu conturi Outlook, setări de sincronizare), în funcție de caracteristicile aplicației.

Pasul 3: Perfecționare profesională / recalificare

Este important să fie luată în considerare necesitatea unor sesiuni de instruire periodice, organizate pentru dezvoltarea continuă a competențelor angajaților. Acestea pot fi împărțite, în mod condiționat, în trei categorii principale:

Instruire planificată după modificări ale sistemului – organizată atunci când sunt adăugate funcționalități noi, implementate module suplimentare sau introduse modificări majore în arhitectura existentă.

Reinstruire periodică – destinată perfecționării cunoștințelor angajaților care dețin deja competențe profesionale în utilizarea sistemului și au nevoie de actualizare în funcție de noile cerințe sau standarde interne.

Instruire la cerere – parte a activităților de suport pentru utilizatori în etapa de exploatare. Se desfășoară în situațiile în care un utilizator întâmpină o problemă specifică sau are nevoie de o sesiune metodologică aplicată.

Trebuie menționat că, în cazul anumitor tipuri de sisteme — în special cele asociate cu managementul unor obiective care, în caz de control deficitar, pot pune în pericol viața sau sănătatea oamenilor — simpla instruire nu este suficientă. În aceste situații, se organizează testări suplimentare de cunoștințe, iar accesul la sistem este permis doar pe baza promovării acestor evaluări, prin obținerea unui certificat personal de competență.

Exemple relevante includ sisteme informatice utilizate pentru:

- managementul siguranței traficului feroviar și aerian;
- lansarea de obiecte spațiale;
- controlul proceselor din industria chimică;
- alte activități cu risc ridicat.

În mod evident, la planificarea oricărui program de instruire trebuie avute în vedere și următoarele aspecte:

- experiența angajaților;
- nivelul de cunoștințe perceput și demonstrat;
- abilitățile de leadership, de management și de organizare.

Versiunea finalizată și testată a software-ului este lansată în producție. Serviciul de suport sau clientul colectează feedback de la utilizatori. Dacă în această etapă sunt identificate erori care nu au fost detectate în timpul testării, dar care corespund cerințelor produsului, acestea sunt transmise dezvoltatorilor pentru a fi remediate în următoarea etapă a ciclului de viață.

SUPORT ȘI MENTENANȚĂ

După lansare, proiectul intră în faza de mentenanță. În această etapă are loc o monitorizare continuă a funcționării corecte a produsului, a performanței sistemului, a securității și a riscurilor de învechire tehnologică.

Specialiștii tehnici remediază problemele apărute în utilizarea resursei software. Aceasta poate include tratarea erorilor reziduale care nu au putut fi corectate înainte de lansare, precum și rezolvarea noilor incidente semnalate de utilizatori. În cazul proiectelor de amploare, perioada de mentenanță este adesea mai extinsă decât în cazul proiectelor de dimensiuni mai reduse.

În cadrul procesului de suport, sunt evidențiate următoarele tipuri principale de activități:

- Suport de garanție
- Mentenanță corectivă
- Mentenanță evolutivă (de îmbunătățire)
- Mentenanță adaptivă

Suport de garanție

Reprezintă activitățile de suport și servicii garantate de dezvoltatorul sistemului în cazul apariției unor defecțiuni sau erori în perioada de garanție. Aceste intervenții sunt reglementate contractual, fiind realizate pe cheltuiala furnizorului și incluzând toate obligațiile asumate privind produsele livrate.

Mentenanță corectivă

Vizează corectarea erorilor identificate în timpul testării sau în utilizarea curentă. Utilizatorii se așteaptă ca problemele apărute („bug-uri”) să fie remediate prompt, iar pierderea feedbackului lor poate genera nemulțumiri. De aceea, acest tip de mentenanță este tratat cu o atenție deosebită.

Mentenanță evolutivă (de îmbunătățire)

Constă în adăugarea de funcționalități noi sistemului. Solicitările provin de regulă de la utilizatori, însă și analiștii de business pot genera cerințe de îmbunătățire pe baza observațiilor din operare.

Mentenanță adaptivă

Implică modificări ale sistemului pentru a-l adapta la noi condiții hardware sau software. Schimbările de infrastructură, de interfață sau de structură a datelor pot impune refactorizarea unor componente pentru a le menține funcționale. Nu se extinde neapărat funcționalitatea, ci se asigură continuitatea acesteia într-un nou mediu operațional.

Aplicarea modificărilor presupune, în cele mai multe cazuri, intervenții directe în codul sursă și declanșează un lanț complet de activități de modernizare software – de la analiză, la testare și livrare către utilizatori. Pentru eficientizarea acestor procese sunt dezvoltate metodologii care reduc efortul de muncă, cum ar fi abordarea orientată pe obiect, larg utilizată în dezvoltarea modernă.

4.4 PROCESE

În cadrul metodologiei Waterfall, fiecare proces aplicat în ciclul de viață al unui sistem software necesită un timp considerabil. Structura acestuia poate fi împărțită în trei faze, conform reprezentării din figura de mai jos.

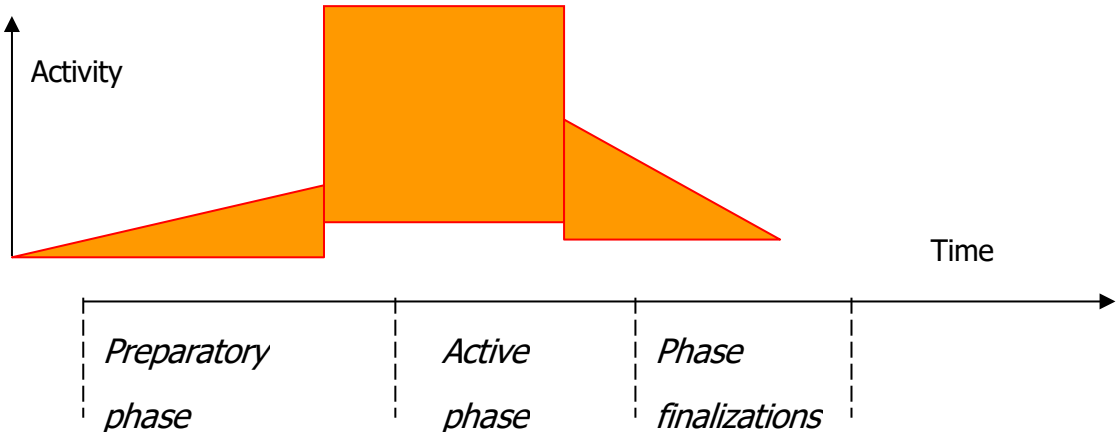


Figura - Structura de Execuție a Procesului

Faza de pregătire poate include familiarizarea cu domeniul de activitate, examinarea rezultatelor proceselor realizate anterior, precum și planificarea și calculele preliminare.

În timpul fazei active, procesul este executat propriu-zis. În descrierea proceselor din prezentul regulament tehnic, sunt acoperite exclusiv activitățile specifice fazei active.

În cadrul fazei de finalizare, pot fi desfășurate activități de analiză a rezultatelor, pot fi încheiate activități inițiate în faza activă, iar lucrările care nu sunt limitate de termenul final pot continua.

Pe baza acestor etape și procese, Furnizorul împreună cu Clientul elaborează un model de ciclu de viață al unui anumit sistem software.

Fiecare fază are un obiectiv distinct și contribuie la parcursul integral al ciclului de viață al sistemului software. Toate fazele sunt luate în considerare în procesul de planificare și execuție a acestui ciclu de viață.

Pentru implementarea fiecărei faze, organizația trebuie să dispună de:

- infrastructură adecvată,
- buget,
- componente software și hardware,
- instrumente tehnice,
- proceduri aprobate,
- resurse umane competente.

Toate aceste componente sunt planificate înainte de începerea fiecărei faze și sunt stabilite și/sau achiziționate, după caz.

Începutul și sfârșitul fiecărui pas și proces trebuie documentate în conformitate cu procedurile instituționale ale organizației.

Acest model presupune execuția strict secvențială și unică a fiecărei faze a proiectului. Tranziția de la o fază la alta este permisă doar după finalizarea cu succes a fazei precedente. Fiecare fază implică o planificare detaliată și asigurarea unei acurateți complete a rezultatului.

Această constrângere de secvențialitate strictă permite construirea unui proces de

dezvoltare transparent și previzibil pentru Client.

4.5 PROIECTARE ȘI DOCUMENTARE

O particularitate esențială a acestei metodologii este necesitatea menținerii și actualizării constante a documentației de dezvoltare a produsului. Orice modificare trebuie coordonată cu Clientul. În absența acestui pas, un nivel insuficient de detaliere a cerințelor poate conduce la creșterea bugetului și extinderea termenelor proiectului — aspecte dificil de estimat corect în avans.

Reprezentantul autorizat al Clientului trebuie să fie activ implicat în procesul de dezvoltare. Acesta va avea trei responsabilități principale:

- Gestionarea portofoliului de produs. Product Owner-ul, împreună cu Business Analyst-ul, va actualiza regulat backlog-ul pentru a reflecta lista prioritizată a funcționalităților ce urmează a fi implementate.
- Răspuns la întrebările echipei de dezvoltare. Reprezentantul Clientului trebuie să fie disponibil pentru a oferi clarificări și a evita comunicarea excesiv formală care poate încetini proiectul. Pentru a livra un produs funcțional la finalul fiecărui sprint, este esențial ca echipa să aibă acces la informațiile necesare la momentul potrivit.
- Acceptarea livrabilelor. La finalul fiecărui sprint, pachetele de lucru finalizate sunt prezentate Reprezentantului Clientului pentru acceptare. Acesta va valida

rezultatele sau va transmite Furnizorului observații privind eventualele neconformități identificate, care trebuie rezolvate înainte de următorul sprint.

Deși nu este obligatoriu, Reprezentantul Clientului poate participa la ședințele echipei de dezvoltare pentru a urmări progresul și a reacționa prompt la eventuale blocaje.

Tot Reprezentantul Clientului va decide dacă produsul este gata pentru lansare

conform planului de release.

Conform principiilor metodologiei de management de proiect, Clientul elaborează un concept de dezvoltare a produsului, precum și un roadmap pentru a urmări progresul și a asigura o evoluție coerentă a livrabilelor.

Utilizăm această metodologie de dezvoltare datorită transparenței ridicate oferite în proces. Nivelul înalt de formalizare face ca gestionarea proiectului să fie mai facilă și predictibilă. Modelul în cascadă reduce riscurile și aduce claritate în derularea proiectelor complexe, mai ales în situațiile în care lucrează zeci de specialiști.

Adoptăm acest model în mod special în proiectele guvernamentale de mari dimensiuni, unde cerințele sunt clar definite și fixate de la început. Nu recomandăm utilizarea acestei metodologii pentru dezvoltarea de aplicații comerciale flexibile, orientate spre business.

4.6 ASPECTE POZITIVE ȘI NEGATIVE ALE METODOLOGIEI

Avantaje:

- Transparență ridicată a etapelor de dezvoltare și a fazelor proiectului
- Succesiune clară a activităților
- Stabilitate a cerințelor de-a lungul proiectului
- Control strict asupra managementului de proiect
- Facilitează elaborarea planului de proiect și formarea echipei de lucru
- Definirea clară a procedurii de control al calității

Dezavantaje:

- Proiectul trebuie să fie însoțit permanent de documentație actualizată.
  Actualizarea documentației este obligatorie și adesea redundantă
- Metodologia nu este suficient de flexibilă
- Clientul nu are posibilitatea de a interacționa din timp cu sistemul, de exemplu

printr-o versiune pilot

- Utilizatorul final nu are ocazia să se acomodeze treptat cu produsul
- Toate cerințele trebuie cunoscute de la începutul ciclului de viață al proiectului
- Este necesar un management riguros și o monitorizare constantă; în caz contrar, proiectul riscă să iasă rapid din grafic
- Poate crea o impresie eronată asupra progresului proiectului (ex. formularea
  „45% complet” nu oferă valoare reală, fiind doar un indicator de stare pentru

  managerul de proiect)
- Nu permite remodelări pe parcurs – întregul proiect este dezvoltat într-o singură iterație

Dezavantajele de mai sus nu împiedică aplicarea cu succes a metodologiei Waterfall, în următoarele condiții:

- Clientul știe exact ce dorește să obțină. A analizat în prealabil conceptul, are o viziune clară asupra rezultatului final și nu intenționează să modifice cerințele în timpul dezvoltării.
- Clientul este de acord ca întregul proces de management al proiectului să fie asumat de către Furnizor. Nu își propune să participe activ în procesul de dezvoltare, control sau feedback, ci dorește doar să primească rezultatul final.
- Clientul este conștient de calendarul proiectului și de livrabilele așteptate la fiecare etapă.
- Echipa de dezvoltare cunoaște din timp tehnologiile și metodele de lucru ce urmează a fi utilizate și deține soluții standard pe baza cărora va livra produsul.

Modelul Waterfall este, de asemenea, o alegere potrivită în cazul în care echipa dezvoltă un produs complex, iar procesul de creare necesită respectarea unei secvențe stricte de pași și un buget substanțial.

4.7 UTILIZAREA METODOLOGIEI

Aplicăm această metodologie:

- Pentru proiecte de dimensiune medie și mare, care implică zeci de programatori și mai multe echipe de proiect distincte;

- În proiecte în care cerințele și limitele sunt clare, transparente și bine definite încă de la începutul ciclului de viață al proiectului.

Astfel, modelul în cascadă (Waterfall) presupune că tranziția de la o fază de dezvoltare la alta are loc doar după finalizarea completă și cu succes a fazei anterioare.

Modelul permite suprapunerea etapelor de implementare, dar nu presupune revenirea (backtracking) sau săritul etapelor – ordinea este secvențială, cu faze care se pot suprapune, dar nu inversa.

4.8 ROLUL FURNIZORULUI

Furnizorul este responsabil de gestionarea proiectului în conformitate cu planul de proiect și cu practicile agreate împreună cu Clientul.

Responsabilitățile Furnizorului includ:

- Identificarea și mobilizarea resurselor necesare pentru desfășurarea activităților din aria sa de responsabilitate, conform planului de management al proiectului și nivelului de calitate convenit;

- Elaborarea documentației de arhitectură la nivel înalt pentru soluția IT propusă, care va include principalele aspecte de implementare: obiectivele de livrare, arhitectura sistemului, stack-ul tehnologic, infrastructura de implementare, componentele funcționale, machetele (mock-up-urile) principalelor interfețe etc.

Cu acordul beneficiarului, în proiect poate fi utilizată o metodologie hibridă de dezvoltare, care va permite livrarea parțială a funcționalităților sistemului în etapele timpurii ale proiectului, pentru testare din partea beneficiarului.

O descriere detaliată a metodologiei hibride de dezvoltare este prezentată în documentul anexat: „Metodologia de dezvoltare hibridă RO.pdf”

5 PRINCIPIILE GENERALE DE CONSTITUIRE A SISTEMULUI

Platforma WEB centralizată

Dezvoltarea modernă a comunicațiilor permite automatizarea structurilor distribuite geografic prin stocarea și procesarea centralizată a informațiilor. Acest model îmbunătățește semnificativ viteza și fiabilitatea procesării datelor, reducând în același timp costurile de instalare, implementare și întreținere a sistemului.

Utilizarea internetului asigură accesibilitate extinsă, atât la nivel național, cât și internațional.

Utilizarea platformelor și instrumentelor de dezvoltare moderne

Soluția va fi dezvoltată pe baza Microsoft .NET Framework, care reprezintă standardul de facto în industrie pentru construirea sistemelor informatice multi-nivel. Acesta este susținut de

cei mai importanți furnizori de software la nivel global și permite dezvoltarea de aplicații scalabile, flexibile și securizate.

Arhitectura platformei va permite, dacă va fi necesar, extinderea funcționalităților sistemului, adăugarea de module suplimentare sau integrarea cu alte componente software.

Interfața web utilizator

Implementarea unei interfețe web pentru utilizatori va minimiza cerințele hardware și software la nivelul stațiilor de lucru. Soluția va fi cross-platform, eliminând dependența de un anumit sistem de operare.

Accesul la funcționalitățile Ministerului Muncii și Protecției Sociale va fi compatibil cu cele mai utilizate browsere web, inclusiv:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome

Compatibilitatea va fi asigurată pentru ultimele trei versiuni ale fiecărui browser.

Utilizarea componentelor open source

În dezvoltarea sistemului vor fi utilizate componente Open Source și standarde deschise, asigurând flexibilitate și interoperabilitate. Soluția va fi construită folosind biblioteci open source recunoscute, precum și instrumente de dezvoltare larg răspândite.

Dacă utilizarea unor componente proprietare va fi necesară, acestea vor respecta principiile standardelor deschise și nu vor implica costuri suplimentare pentru beneficiari.

Astfel, Beneficiarul nu va suporta taxe suplimentare de licențiere pentru dezvoltarea și utilizarea soluției.

6 PLATFORMA TEHNOLOGICĂ

Arhitectura sistemului va fi ierarhică, de tip client-server, și va conține următoarele componente:

Platforma hardware

Platforma hardware va fi formată dintr-un complex tehnic de procesare și transport al datelor, integrat în infrastructura sistemului M-Cloud. Aceasta va asigura:

- Servere protejate redundant, destinate găzduirii bazelor de date, software-ului de sistem și aplicațiilor funcționale;
- Echipamente de comunicații, necesare pentru formarea rețelelor locale LAN și organizarea comunicațiilor teritoriale WAN;
- Performanță optimă, pentru atingerea obiectivelor sistemului și asigurarea scalabilității acestuia;
- Nivel adecvat de securitate, privind transportul și protecția datelor.

Platforma software

Platforma software va avea următoarele caracteristici:

- Sistemele de operare ale serverelor de baze de date și ale serverului de aplicații vor fi Microsoft Windows (Enterprise Edition), fiind asigurate de Platforma M-Cloud;
- Sistemul de gestiune a bazelor de date (SGBD) va fi Microsoft SQL Server, cu licențele furnizate de Beneficiar;
- Stațiile utilizatorilor vor dispune implicit de un browser web, acesta fiind asigurat de Beneficiar.

Arhitectura Sistemului SIA "RICC New" este proiectată ținând cont de principiile flexibilității maxime și independenței tehnologice, ceea ce asigură scalabilitatea, ușurința în mentenanță și conformitatea cu standardele arhitecturii IT ale Ministerului Afacerilor Interne (MAI).

6.1 Independența de Platforma Tehnologică

Componentele SIA "RICC New" sunt dezvoltate astfel încât să fie independente de platforma tehnologică pe care funcționează. Acest principiu asigură posibilitatea ca aplicațiile să ruleze pe orice platformă tehnologică.

- Sistemul este bazat pe tehnologii și standarde deschise (open source), larg cunoscute și implementate în Republica Moldova, excluzând dependența de soluțiile proprietare ale furnizorului.
- Pentru dezvoltare sunt utilizate limbaje de programare și framework-uri moderne (de exemplu, C#, ASP.NET Core), care sunt acceptate pe scară largă în industrie și sunt accesibile specialiștilor IT locali.
- Este asigurată omogenitatea tehnologiilor utilizate (un număr minim de tehnologii diferite) pentru simplificarea administrării și creșterea stabilității.

6.2 Optimizarea pentru Mediile Cloud (Cloud computing / MCloud)

Arhitectura SIA "RICC New" este optimizată pentru funcționarea eficientă în medii virtualizate de tip Cloud computing (MCloud), fiind în concordanță cu inițiativele Guvernului.

- Sistemul este dezvoltat ținând cont de caracteristicile cheie ale soluțiilor cloud: este conștient de latență, rezistent la căderi de componente, paralelizabil și ține cont de utilizarea eficientă a resurselor.
- Pentru asigurarea flexibilității și scalabilității, sunt aplicate tehnologii de containerizare și orchestrare, precum Kubernetes și Docker. Kubernetes este utilizat ca tehnologie de orchestrare și balansare a încărcării sarcinilor.
- Arhitectura susține implementarea și funcționarea în mediul MCloud. La necesitate, sistemul susține implementarea pe echipamente standard care sunt disponibile pentru achiziționare liberă pe piață.

6.3 Suport pentru Formatul Unicode (UTF-8)

Sistemul SIA "RICC New" asigură crearea, modificarea, procesarea, stocarea și accesarea textului în format Unicode (CNFG.40), garantând compatibilitatea și standardizarea datelor în cadrul sistemului (CNFG.13, CNFG.40).

6.4 Interoperabilitate (Standarde deschise și integrare cu MConnect)

Sistemul va fi construit ținând cont de principiile deschiderii și extensibilității:

- Standarde deschise. Utilizarea protocoalelor de integrare general acceptate (REST/JSON, SOAP, XML Schema, Swagger/OpenAPI 3.0), care asigură independența față de tehnologiile specifice ale furnizorului.
- Interacțiune în timp real printr-o arhitectură care suportă schimbul asincron de evenimente (webhooks, publish–subscribe, AMQP/Kafka sau soluții echivalente).
- Set complet de interfețe API, care include operațiuni de citire și scriere, precum și mecanisme de autorizare bazate pe OAuth2 / JWT.
- Integrarea cu platforma MConnect este asigurată prin canale standardizate de schimb de date, formate de mesaje aliniate și mecanisme automatizate de rutare a informațiilor.
- Este prevăzută jurnalizarea interacțiunilor, monitorizarea fluxurilor de integrare și gestionarea erorilor cu mecanisme de retry.

6.5 Performanța sistemului

Arhitectura și soluțiile tehnologice utilizate în SIA „RICC New” asigură respectarea integrală a cerințelor de performanță, scalabilitate și funcționare în timp real. Toți indicatorii sunt atinși în cadrul platformei tehnologice propuse.

1. Timp de răspuns ≤ 3 secunde pentru tranzacțiile utilizatorilor (CNFG.71)

Executarea operațiunilor tranzacționale este realizată cu un timp de răspuns de maximum 3 secunde datorită următoarelor măsuri:

- utilizarea mecanismelor de caching de înaltă performanță (Redis/Memcached);
- optimizarea interogărilor SQL și indexarea adecvată a bazei de date;
- aplicarea procesării asincrone pentru reducerea timpului de așteptare;
- distribuirea încărcării între mai multe instanțe ale serviciilor.

2. Suport pentru 500 sesiuni paralele cu scalare până la 1000

Sistemul suportă până la 500 sesiuni simultane și permite scalarea până la 1000 de sesiuni datorită:

- scalării orizontale a serviciilor;
- utilizării infrastructurii containerizate cu auto-scalare;
- echilibrării traficului;
- separării serviciilor pe profiluri de încărcare, eliminând astfel punctele critice.

3. Gestionarea proceselor cu impact ridicat asupra performanței

Documentația operațională include:

- lista proceselor care generează încărcare ridicată (backup, operațiuni în masă, rapoarte complexe);
- recomandări privind executarea acestora în intervale cu activitate redusă;
- mecanisme de limitare a execuțiilor paralele pentru operațiuni consumatoare de resurse;
- reguli privind interacțiunea proceselor de fundal cu cele tranzacționale.

4. Izolarea sarcinilor de raportare față de sarcinile tranzacționale

Separarea sarcinilor este asigurată prin:

- executarea rapoartelor în fluxuri separate, neafectând logica tranzacțională;
- utilizarea proceselor ETL și a vitrinelor locale de date;
- evitarea operațiunilor analitice grele în baza de date tranzacțională;
- prevenirea blocării tranzacțiilor în timpul generării rapoartelor.

5. Identificarea rapoartelor cu impact semnificativ asupra performanței și recomandări

Documentația sistemului include:

- lista rapoartelor cu impact major asupra performanței;
- recomandări privind frecvența și intervalele optime de execuție;
- parametri de filtrare care reduc volumul de date procesat;
- recomandări privind executarea în condiții de siguranță fără a afecta performanța.

6. Funcționarea în regim de timp real

Funcționarea în timp real este posibilă datorită:

- interacțiunii optimizate dintre servicii;
- minimizării latenței la nivel de API și bază de date;
- distribuției dinamice a încărcării între componentele sistemului;
- unei arhitecturi orientate către procesarea imediată a datelor pentru utilizatori.

6.6 Scalabilitate

Arhitectura SIA „RICC New” este proiectată pentru a asigura scalabilitate orizontală, adaptarea resurselor la nivelul încărcării curente și capacitatea sistemului de a deservi un număr ridicat de sesiuni simultane. Scalabilitatea reprezintă un principiu fundamental al sistemului, care permite extinderea și optimizarea continuă fără modificări majore ale infrastructurii.

1. Mecanisme tehnice pentru scalabilitatea orizontală

Arhitectura SIA „RICC New” prevede posibilitatea utilizării următoarelor abordări pentru extinderea capacității sistemului:

- Posibilitatea implementării componentelor în regim stateless, ceea ce facilitează adăugarea de instanțe suplimentare ale serviciilor și distribuirea uniformă a sarcinii. Acest model poate fi aplicat acolo unde este justificat funcțional.
- Suport pentru utilizarea mecanismelor externe de gestionare a stării, inclusiv depozite centralizate pentru stocarea sesiunilor, metadatelor sau conținutului, atunci când este necesară sincronizarea între mai multe noduri.
- Posibilitatea de a distribui servicii identice pe mai multe noduri, permițând extinderea capacității de procesare fără modificarea logicii aplicațiilor.
- Suport pentru distribuirea sarcinii între nodurile sistemului, ceea ce asigură extinderea flexibilă a resurselor de procesare în funcție de necesități.

Aceste opțiuni arhitecturale oferă o bază solidă pentru scalabilitatea orizontală și permit extinderea sistemului în condiții de creștere a cererii.

2. Scalabilitatea bazei de date

Arhitectura sistemului oferă posibilitatea aplicării mai multor mecanisme pentru extinderea și optimizarea subsistemului de stocare a datelor:

- Separarea fluxurilor de citire și scriere (read/write splitting) pentru distribuirea sarcinii și îmbunătățirea capacității de procesare.
- Utilizarea replicilor bazei de date, care pot fi folosite pentru operațiuni de citire, analize sau procese de fundal.
- Partiționarea (partitioning) tabelelor, permițând gestionarea eficientă a unor volume mari de date prin distribuirea lor logică.
- Scalarea orizontală a stocării (de exemplu, sharding) atunci când volumul datelor crește semnificativ.
- Gestionarea flexibilă a indexurilor și a structurii datelor, asigurând menținerea performanței pe măsură ce volumul tranzacțiilor crește.
- Posibilitatea de a reloca procesele analitice intensive în depozite separate sau vitrine de date, reducând sarcina asupra bazei tranzacționale.

Aceste capacități oferă o evoluție controlată și scalabilă a sistemului de stocare fără restructurări majore.

3. Adaptarea resurselor în funcție de încărcare

Arhitectura permite ajustarea resurselor în funcție de volumul activității:

- creșterea numărului de instanțe ale serviciilor în perioade de suprasolicitare;
- reducerea automată a resurselor atunci când volumul scade;
- utilizarea metricilor de încărcare și latență pentru declanșarea ajustărilor;
- reacție rapidă la variații bruște în numărul de utilizatori sau tranzacții.

Acest mecanism contribuie la menținerea stabilității și la optimizarea costurilor de operare.

4. Capacitatea de a deservi un număr ridicat de sesiuni simultane

SIA „RICC New” poate susține numărul declarat de sesiuni simultane datorită:

- utilizării scalării orizontale ca metodă principală de extindere;
- distribuirii sarcinii între servicii care funcționează în paralel;
- mecanismelor optimizate de gestionare a accesului concurent;
- posibilității de extindere până la niveluri superioare prin alocarea resurselor necesare.

Acest model permite adaptarea sistemului la creșteri semnificative ale volumului de activitate.

5. Flexibilitate în extinderea funcționalităților

Arhitectura permite:

- extinderea rapidă a funcționalităților existente;
- integrarea de servicii și module noi fără modificări complicate;
- adaptarea la noi cerințe operaționale fără costuri semnificative;
- modernizarea graduală în cadrul proceselor de reinginerie.

6. Optimizare pentru medii cloud

Sistemul este proiectat pentru funcționare eficientă în infrastructuri cloud, oferind:

- suport pentru procesare paralelă;
- reziliență la defectarea componentelor individuale;
- optimizarea comunicației între servicii cu reducerea latenței;
- utilizarea eficientă a resurselor de procesare și stocare.

6.7 Flexibilitate

Realizarea SIA „RICC New” prevede mecanisme de adaptare a sistemului la noi cerințe cu modificarea minim necesară a codului sursă, prin utilizarea unei arhitecturi extensibile și a instrumentelor de configurare.

1. Configurarea rapoartelor

Pentru asigurarea flexibilității în configurarea rapoartelor se implementează următoarea funcționalitate:

- Mecanismele de configurare a rapoartelor sunt bazate pe capabilitățile descrise în secțiunea „Modul Z-spravka”.

2. Gestiunea informației normative și de referință

Pentru gestionarea clasificatoarelor și a informațiilor de referință se implementează următoarele funcționalități:

- Se asigură crearea, editarea și modificarea structurilor clasificatoarelor, inclusiv modele multi-nivel.
- Se implementează posibilitatea încărcării datelor de referință din surse interne sau externe (BD, servicii web, fișiere) înainte de lansarea sistemului în exploatare.
- Se asigură posibilitatea modificării valorilor, stărilor și parametrilor elementelor de referință în timpul funcționării sistemului.

3. Instrumente administrative de configurare

Pentru adaptarea parametrilor sistemului fără modificarea codului sursă se implementează următoarele mecanisme:

- Toate configurările sistemului sunt accesibile administratorului prin instrumente specializate.
- Instrumentele de administrare permit modificarea parametrilor de automatizare.
- Sunt implementate instrumente pentru crearea formularelor de căutare și interogare.

4. Mecanisme de gestionare a stărilor obiectelor

Pentru administrarea flexibilă a ciclului de viață al obiectelor sunt implementate următoarele capacități:

- Sunt configurabile drepturile de acces în funcție de starea obiectului informațional.
- Este implementat un mecanism de detectare a conflictelor la modificarea stărilor sau a operațiunilor permise.

6.8 Reziliență și continuitate

Soluția se bazează pe capabilitățile infrastructurale ale platformei M-Cloud, care oferă mecanismele necesare pentru continuitatea operațională.

1. Copii de rezervă și gestionarea acestora

Pentru asigurarea protecției datelor, sistemul include măsuri și instrumente dedicate proceselor de backup.

- Instrumente de creare a copiilor de rezervă.

  Sistemul permite generarea automată a copiilor de rezervă pentru componente critice, cum ar fi baza de date și fișierele de conținut. Realizarea acestor funcții este responsabilitatea infrastructurii M-Cloud.

- Gestionarea versiunilor istorice ale copiilor de rezervă.

  Arhitectura prevede păstrarea și administrarea versiunilor istorice ale backup-urilor, funcționalități oferite de serviciile infrastructurale ale M-Cloud.

- Restabilirea funcționalității pe baza copiilor de rezervă.
- Sistemul poate fi restaurat utilizând o copie de rezervă selectată de administrator, iar operațiunile de restaurare sunt susținute de infrastructura M-Cloud.
- Funcții administrative. Platforma M-Cloud trebuie să pună la dispoziția administratorului mijloacele necesare pentru crearea, gestionarea și restaurarea copiilor de rezervă.

2. Integritatea datelor și protecția în cazul incidentelor

Pentru menținerea corectitudinii și consistenței datelor, sistemul include măsuri orientate spre reducerea impactului incidentelor.

- Restabilirea rapidă a funcționalității.

  În cazul unui incident, sistemul poate fi readus într-o stare operațională prin aplicarea procedurilor de restaurare, conform regulilor interne. Asigurarea acestor proceduri depinde de infrastructura M-Cloud.

3. Arhitectură rezilientă și evitarea punctelor singulare de cădere

Arhitectura sistemului este gândită pentru a funcționa chiar și atunci când anumite componente nu sunt disponibile.

- Funcționare în condiții de defectare a unor componente.

  Continuitatea serviciilor este asigurată de infrastructura M-Cloud, care utilizează mecanisme precum Kubernetes pentru repornirea automată sau relocarea serviciilor în cazul unor căderi.

4. Mecanisme de restabilire a disponibilității

Pentru a readuce rapid sistemul în stare funcțională, arhitectura include procese și mecanisme orientate spre recuperare.

- Aceste funcții trebuie să fie asigurate de infrastructura platformei M-Cloud, inclusiv prin instrumente automate de restabilire a componentelor și de gestionare a continuității serviciilor.

5. Monitorizare și semnalizare a disponibilității

Pentru a permite detectarea rapidă a problemelor și menținerea controlului operațional, sistemul poate dispune de mecanisme de semnalizare.

- Semnale de tip „heart-beat”.

  Sistemul poate avea posibilitatea de a transmite periodic informații privind starea sa.

- Monitorizarea disponibilității.

  Sistemul poate oferi posibilitatea furnizării către servicii externe a datelor necesare monitorizării.

Ambele categorii de funcționalități trebuie să fie asigurate de infrastructura M-Cloud.

7 STIVA TEHNOLOGICĂ

Pentru dezvoltarea sistemului „RICC”, vom utiliza cele mai recente versiuni ale următoarelor tehnologii:

- Limbaj de programare: C#
- Soluție ORM: Entity Framework Core v9
- Framework web: ASP.NET MVC Core
- Cadrul web: React v18
- SGBD: Microsoft SQL Server 2022 Standard (asigurat de Beneficiar)
- Server de poștă: asigurat de Beneficiar
- Server de memorie cache și session store: Redis v8
- Sistem de deploiment in baza platformei Kubernetes RKE2 - v1.33.3+rke2r1 (asigurat de Beneficiar)
- Server de memorie cache și session store: Redis
- Soluție ETL: Apache NiFi v2
- Sistem de deploiment in baza platformei Kubernetes, Docker
- Jenkins, Nexus 3.84.1-01
- Server de cache și spațiu de stocare pentru sesiuni: Microsoft SQL Server 2022 Standard.
- Soluție de monitorizare a logurilor: Elastic Search + Kibana v9.2

Deși în cerințele din solicitare este indicată platforma .NET 8.0, noi propunem migrarea la o platformă mai nouă și mai sigură, .NET 10.0. Această tranziție va spori nivelul de securitate și va permite utilizarea noilor capabilități necesare pentru realizarea funcționalităților din Etapa 2, precum și pentru dezvoltarea ulterioară a sistemului.

Totodată, vom asigura suportul tehnologiilor utilizate la Etapa 1, pentru a menține compatibilitatea și integrarea corectă a componentelor existente.

În procesul de dezvoltare a SIA „RICC” pot fi propuse componente adiționale necesare pentru dezvoltarea și funcționarea adecvată a soluției în mediul de producție.

8 INFRASTRUCTURA HARDWARE ȘI TELECOMUNICAȚII

Toate cerințele privind infrastructura, resursele de calcul, disponibilitatea rețelei și comunicațiile trebuie să fie asigurate de platforma guvernamentală MCloud și de furnizorul acesteia, în conformitate cu politicile de exploatare și arhitectura platformei Cloud. Implementarea SIA „RICC New” prevede găzduirea integrală și operarea sistemului în mediul

MCloud, utilizând mecanismele de virtualizare, orchestrare și infrastructura de rețea oferite de aceasta.

1. Operarea în mediul MCloud

Pentru funcționarea sistemului se asigură:

- găzduirea tuturor componentelor aplicației în infrastructura platformei guvernamentale MCloud;
- utilizarea resurselor hardware standard puse la dispoziție de MCloud (CPU, memorie RAM, stocare, interfețe de rețea);
- compatibilitatea completă cu mecanismele de alocare automată a resurselor, monitorizare, scalare și management al componentelor implementate în MCloud

2. Arhitectură optimizată pentru medii virtualizate și Cloud

Arhitectura SIA „RICC New” este proiectată pentru operarea în medii virtualizate și Cloud:

- componentele aplicației sunt proiectate ca portabile, capabile să funcționeze stabil în medii virtualizate și distribuții Cloud;
- arhitectura este optimizată pentru scenarii Cloud, inclusiv variații de latență și redistribuirea dinamică a resurselor;
- sistemul este proiectat să fie tolerant la căderi ale componentelor individuale, cu posibilitatea executării paralele a proceselor;
- structurile de stocare și procesare a datelor sunt adaptate pentru utilizarea resurselor distribuite ale MCloud.

3. Tehnologii și infrastructură software

Implementarea SIA „RICC New” utilizează tehnologii moderne compatibile cu arhitectura Cloud:

- Kubernetes este utilizat pentru orchestrarea containerelor, gestionarea stării serviciilor, scalarea și relansarea automată a componentelor;
- Docker este utilizat pentru containerizarea serviciilor aplicației;
- sistemul suportă instalarea și rularea în mediile virtualizate puse la dispoziție de MCloud;
- sunt definite și operate următoarele medii:
    - mediul de dezvoltare,
    - mediul de testare,
    - mediul de producție,
    - mediul de instruire (după necesitate).

4. Telecomunicații și infrastructură de rețea

Comunicarea între componentele sistemului se realizează folosind canale securizate:

- toate comunicațiile utilizează arhitectura de rețea TCP/IP, cu obligativitatea utilizării protocolului HTTPS;
- accesul la sistem este disponibil utilizatorilor conectați la rețeaua internă a Beneficiarului, conform politicilor acestuia;
- interacțiunea dintre componentele aplicației se realizează prin interfețe interne și canale securizate;
- arhitectura permite segmentarea nivelului de rețea în conformitate cu regulile de operare în MCloud.

5. Parametrii informaționali și cerințe pentru infrastructură

- Furnizorul va primi de la Beneficiar informații privind caracteristicile resurselor disponibile în MCloud, necesare pentru determinarea configurației sistemului.
- Ofertantul va transmite Beneficiarului lista completă a cerințelor de infrastructură necesare pentru funcționarea SIA „RICC New”, incluzând parametrii privind resursele de calcul, memoria, spațiul de stocare, conexiunile de rețea și mediile software suportate.

9 LICENȚIERE ȘI PROPRIETATE INTELECTUALĂ

Ofertantul garantează conformitatea deplină a soluției propuse cu cerințele Achizitorului (MAI) referitoare la drepturile de proprietate intelectuală și licențierea software-ului SIA "RICC New".

1. Asigurarea Drepturilor de Utilizare și Licențiere (CNF.3, CNF.6)

Noi oferim un model de licențiere care asigură Achizitorului drepturile necesare pentru utilizarea și exploatarea Sistemului.

- Accesul utilizatorilor.

  Cantitatea licențelor oferite trebuie să permită accesarea și utilizarea SIA RICC (în orice mediu în care funcționează) de cel puțin 500 de utilizatori concurenți.

- Lipsa restricțiilor.

  Nu vor exista restricții cu privire la numărul tranzacțiilor sau modul de accesare a SIA RICC (de exemplu, limitări la accesare concurentă).

- Dreptul de utilizare nelimitată (pe termen nelimitat).

  Achizitorul obține dreptul de utilizare neexclusivă pe termen nelimitat a softului aplicativ, fără drept de multiplicare și distribuire.

2. Transferul Proprietății Intelectuale (CNF.5)

Ofertantul transferă Achizitorului toate drepturile asupra componentelor dezvoltate și adaptate în conformitate cu cerințele din Termenii de Referință.

- Proprietatea exclusivă.

  Toate drepturile pe rezultatele, inclusiv drepturile de autor sau alte drepturi de proprietate intelectuală sau industrială, dobândite în cadrul contractului vor fi proprietatea exclusivă a Achizitorului.

- Rezultatele transmise.

  Noi transmitem MAI toate drepturile asupra dezvoltărilor, ajustărilor, configurărilor și personalizărilor efectuate pentru implementarea SIA "RICC New". Acestea includ codurile sursă complete, fișierele executabile, soluțiile tehnice, documentația, procedurile și orice alte rezultate obținute în cadrul contractului.

- Dreptul de utilizare și cesionare.

  Achizitorul va avea dreptul de a utiliza, publica, cesiona sau transfera aceste drepturi fără restricții, cu excepția cazurilor în care există drepturi de proprietate intelectuală preexistente.

10 ARHITECTURA

Sistemul „RICC” va fi implementat ca o soluție software independentă, capabilă să interacționeze cu alte sisteme informatice prin intermediul serviciilor web și să asigure interacțiunea cu utilizatorii printr-o interfață web intuitivă.

Arhitectura sistemului „RICC” va fi concepută astfel încât să permită extinderea funcționalităților în timp și să asigure compatibilitatea cu diferite tipuri de documente.

- Arhitectura va utiliza soluții integrate, bazate pe cele mai bune practici din industria IT;
- Arhitectura sistemului va fi multistrat, cu delimitări foarte clare între nivele;
- Componentele sistemului vor fi relativ independente și vor interacționa între ele prin intermediul interfețelor selectate;
- Sistemul va fi capabil să fie găzduit pe platforma guvernamentală MCloud;
- Modificările și parametrii sistemului, acolo unde este posibil, nu vor afecta activitatea curentă a sistemului, sesiunile active, solicitările sau alte procese;
- Arhitectura soluției software va asigura un nivel înalt de accesibilitate pentru implementarea noilor versiuni și va permite lansarea concomitentă a mai multor instanțe;
- Modelul de date va fi descris și furnizat beneficiarului în formatul convenit.

Arhitectura Sistemului Informațional Automatizat (SIA) "RICC New" este concepută ca un sistem deschis, modular și bazat pe componente inter-operabile, în conformitate cu principiile MAI privind flexibilitatea și mentenanța sistemului informatic.

1. Arhitectura Multistrat (Pe Mai Multe Niveluri)

Arhitectura SIA "RICC New" este implementată ca un model standard pe trei niveluri (client-server), asigurând o delimitare foarte clară între straturi.

- Nivelul Bazei de Date (BD).

Asigură stocarea și gestionarea datelor într-un mediu securizat și optimizat. Structura bazei de date garantează acces rapid la date pentru executarea tranzacțiilor. Generarea rapoartelor statistice nu afectează performanța operațiunilor tranzacționale.

- Serverul de Aplicații (Nivelul Logicii de Afaceri).

  Este componenta principală care gestionează procesarea datelor și execută toată logica de afaceri a sistemului.

- Web Client (Nivelul de Prezentare).

  Oferă interfața utilizator cu acces la funcționalitățile sistemului printr-un browser web. Acest nivel este compatibil cu medii de operare standard și necesită configurări minime.

Arhitectura este structurată astfel încât fiecare nivel superior să depindă doar de nivelul său inferior.

2. Arhitectura Orientată pe Servicii (SOA)

Sistemul SIA "RICC New" utilizează o arhitectură orientată pe servicii (SOA), asigurând un nivel înalt de granularitate și modularitate.

- Servicii Autonome.

  Arhitectura este orientată spre servicii TI autonome (funcțional și instituțional), care pot fi combinate pentru a forma servicii aplicative compuse.

- Modularitate și Independență.

  Nivelul logicii de business este complet modular, bazat pe componente reutilizabile și interfețe abstracte. Acesta este complet independent în raport cu nivelul de prezentare.

- Cuplare Slabă (Loose Coupling).

  Componentele sistemului sunt slab legate și interacționează prin interfețe bine definite. Interacțiunea internă între subsisteme, precum și schimbul de date cu sisteme externe, este realizată prin intermediul unui API, utilizând microservicii.

- Încapsulare.

  Entitățile de business sunt clar identificate și încapsulate în componente de tip "business entities". Accesarea acestor componente se realizează prin intermediul componentelor de tip "business workflow".

3. Bazarea pe Standarde Deschise

Arhitectura SIA "RICC New" este integral bazată pe standarde deschise, principiu fundamental care asigură interoperabilitatea cu alte sisteme.

- Tehnologii.

  Sunt utilizate tehnologii deschise (fără soluții proprietare ale furnizorului), larg cunoscute și implementate în Republica Moldova.

- Protocoale și Formate.

  Sistemul utilizează standarde deschise pentru protocoalele de comunicație și formatele de date. Toate interfețele destinate interacțiunii folosesc standarde deschise.

- Independența de Platformă.

  Componentele SIA "RICC New" sunt independente de platforma tehnologică pe care rulează. Arhitectura este optimizată pentru rularea în medii Cloud computing (MCloud).

4. Extensibilitatea și Scalabilitatea Funcționalităților

Arhitectura SIA "RICC New" asigură extinderea funcționalităților și capacitatea de ajustare rapidă, conform principiilor flexibilității/scalabilității și extensibilității.

- Reziliență și Disponibilitate.

  Arhitectura este rezistentă la căderi de componente și nu deține puncte singulare de cădere (SPOF).

- Scalare.

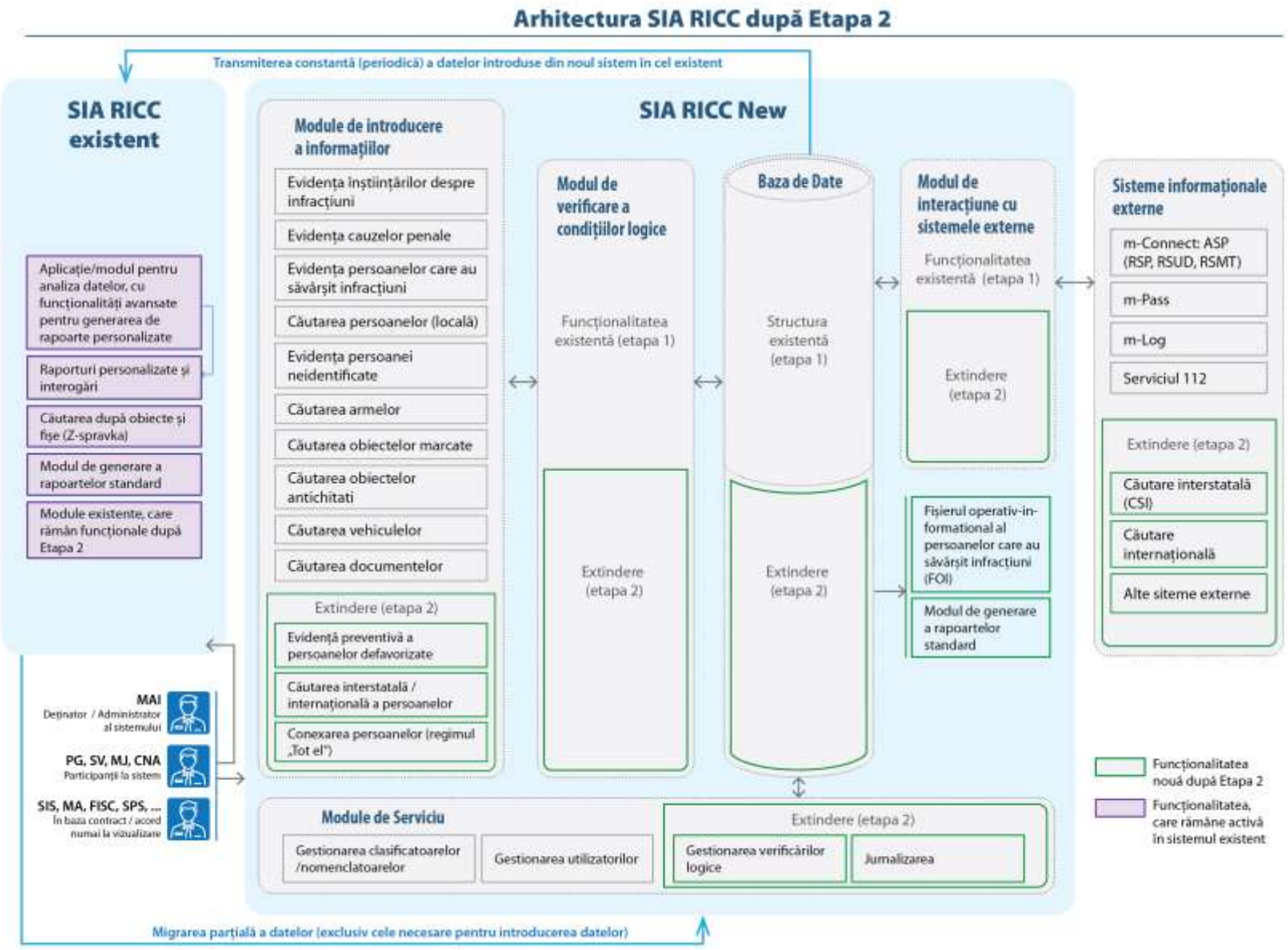
  Sistemul susține creșterea capacității de procesare prin extinderea pe orizontală (adăugarea de noi noduri server și balansare a încărcării), fără a întrerupe funcționarea serviciilor.

- Configurabilitate.

  Sistemul permite adaptarea și extinderea rapidă a funcționalităților existente prin ajustări de configurare. SIA "RICC New" oferă administratorilor posibilitatea de a Defini și configura Condițiile Logice de Validare (CLV)

11 DESCRIEREA ZONEI DE AUTOMATIZARE

Diagrama organizării obiectelor informaționale și a utilizării sistemului ”RICC” este ilustrată în figura 2.



Figură 2 - Diagrama organizării obiectelor informaționale și a utilizării sistemului ”RICC”

Arhitectura SIA RICC după finalizarea Etapei 2

Arhitectura generală a sistemului este proiectată ca un mediu hibrid, multi-modular, în care două platforme — SIA RICC existent (vechea) și SIA RICC New (noua) — funcționează în paralel și se completează reciproc, utilizând mecanisme unificate de schimb de date și de integrare cu resursele guvernamentale externe.

1. Conturul unitar SIA RICC New (nucleul de introducere și prelucrare operativă)

Sistemul nou are rolul instrumentului principal de înregistrare și procesare a informațiilor curente. Structura acestuia include:

- Module de introducere a informației

  Asigură evidența sesizărilor privind infracțiunile, a cauzelor penale și a persoanelor. În Etapa 2 acest bloc se extinde cu funcții de evidență preventivă a *persoanelor defavorizate*, căutare interstatală și modul „Tot el” pentru unificarea dublurilor identităților.

- Fișierul operativ-informațional (FOI).

  Modul specializat pentru evidența persoanelor care au comis infracțiuni, cu propriul sistem de administrare și generare a rapoartelor standard.

- Stratul de logică de business

  Include un modul extensibil de verificare a condițiilor logice (LUS), care garantează corectitudinea datelor la introducere.

- Module de serviciu

  Componente comune sistemului pentru administrarea utilizatorilor, clasificatoarelor, verificărilor logice și jurnalizare centralizată (Jurnalizarea).

2. Conturul SIA RICC existent (centru analitic și arhivă)

Sistemul existent își păstrează relevanța ca hub analitic și arhivă a datelor istorice:

- Analitică și căutare.

  Module pentru analiză aprofundată, generarea rapoartelor personalizate și executarea interogărilor complexe prin aplicația „Z-spravka”.

- Raportare standard.

  Module de generare a formularelor statistice aprobate, care continuă să funcționeze pe baza datelor acumulate.

- Continuitate funcțională.

  Toate modulele sistemului vechi rămân active, asigurând utilizatorilor acces la instrumentele uzuale până la transferul complet al funcțiilor în noul mediu.

3. Mecanisme de integrare și sincronizare a datelor

Elementul de legătură al arhitecturii îl reprezintă două fluxuri bidirecționale de informații:

- Sincronizare permanentă.
- Se asigură prin transmiterea periodică a tuturor datelor noi înregistrate în SIA RICC New către baza de date existentă (SIA RICC existent). Aceasta permite utilizarea instrumentelor analitice vechi pentru lucrul cu cele mai recente date.

- Migrare țintită.

  Transfer unic, parțial, al datelor istorice din sistemul vechi către cel nou, necesar pentru funcționarea corectă a noilor formulare de introducere și căutare (principiul suficienței datelor).

4. Interacțiune externă și servicii guvernamentale

Arhitectura este integrată profund în infrastructura IT guvernamentală:

- mConnect.

  Magistrală unică pentru schimbul de date cu registre externe (RSP, RSUD, registrul armelor, al mijloacelor de transport etc.).

- mPass și mLog.

  Servicii centralizate de autentificare și jurnalizare securizată a evenimentelor.

- Interacțiune internațională

  Module pentru căutare interstatală (CSI/CIS) și internațională a persoanelor și obiectelor.

Avantajele arhitecturii propuse

1. Continuitatea activității (Business Continuity).

   Funcționarea în paralel a celor două sisteme elimină riscurile de întrerupere a înregistrării infracțiunilor sau de pierdere a raportării în perioada de tranziție.

2. Integritatea datelor.

   Vitrina de date și sistemul de referințe încrucișate asigură coerența informațiilor între obiectele de evidență vechi și cele noi.

3. Flexibilitate în administrare.

   Modulele extinse de administrare permit MAI să configureze independent logica de business și drepturile de acces în ambele contururi.

12 ASIGURAREA SECURITĂȚII

1. Principii și cadrul normativ

În arhitectura SIA „RICC New” sunt integrate principii fundamentale de securitate a informațiilor, orientate spre confidențialitate, integritate și disponibilitate. La proiectare se vor lua în considerare actele normative ale Republicii Moldova privind protecția informațiilor și a datelor cu caracter personal.

- **Securitate prin proiectare (Secure by Design).**

  Măsurile de securitate sunt luate în considerare la proiectarea tuturor nivelurilor sistemului.

- **Confidențialitate.**

  Accesul la informație este permis doar în limitele drepturilor utilizatorului.

- **Protecția datelor cu caracter personal.**

Prelucrarea datelor va respecta legislația relevantă și tratatele internaționale aplicabile.

- **Eliminarea limitărilor versiunii vechi a sistemului.**

  Arhitectura SIA „RICC New” prevede mecanisme moderne de securitate și posibilitatea extinderii funcționalităților de protecție.

2. Arhitectura de securitate

Arhitectura sistemului include măsuri multilayer de prevenire și control al riscurilor de securitate.

- **Protecție împotriva atacurilor de rețea (inclusiv DDoS).**

  Infrastructura care va găzdui sistemul trebuie să prevadă protecție împotriva atacurilor distribuite, precum și a amenințărilor din categoria OWASP Top 10.

- **Principiul privilegiilor minime.**

  Procesele și serviciile funcționează doar cu drepturile strict necesare.

- **Segmentarea rețelei și controlul traficului.**

  Furnizorul va oferi recomandări privind configurarea regulilor de acces necesare pentru interacțiunea securizată dintre componente.

- **Protecția interfețelor publice.**

  Este prevăzută posibilitatea implementării unor mecanisme de limitare a accesului anonim și de prevenire a supraîncărcărilor, atunci când este necesar.

- **Gestionarea centralizată a secretelor și credențialelor.**

  Parametrii de acces sunt administrați prin interfețe dedicate, fiind exclusă includerea acestora în cod.

- **Metode sigure de integrare.**

  Comunicarea cu sistemele externe poate utiliza certificate și canale securizate.

3. Autentificare

SIA „RICC New” include un model modern de autentificare.

- **Autentificare prin serviciul MPASS.**

  Este prevăzută utilizarea serviciului guvernamental centralizat, precum și autentificarea cu ID și parolă.

- **Politică de complexitate a parolelor.**

  Sistemul include posibilitatea definirii regulilor privind complexitatea parolelor.

- **Limitarea timpului de inactivitate.**

  Sistemul permite stabilirea perioadei maxime de inactivitate a sesiunii.

- **Protecție împotriva interceptării și atacurilor asupra parolelor.**

  Este prevăzută posibilitatea extinderii funcționalității de protecție.

4. Autorizare

Controlul accesului la resursele sistemului se bazează pe reguli clare și configurabile.

- **Gestionare granulară a drepturilor.**

  Drepturile de acces pot fi definite pentru obiecte precum documente, entități, operațiuni, rapoarte și interfețe.

- **Utilizarea rolurilor utilizatorilor.**

  Sistemul permite atribuirea de drepturi și combinarea acestora, în funcție de responsabilități.

- **Reguli predefinite pentru configurarea drepturilor.**

  Sistemul permite stabilirea drepturilor pe baza logicii de business.

5. Validarea datelor și protecția informațiilor

Mecanismele de validare asigură integritatea datelor și reduc riscurile de manipulare.

- **Validare pe toate nivelurile sistemului.**

  Sistemul efectuează controale la nivelul interfeței, logicii de business și nivelului de stocare.

- **Executarea operațiunilor în cadrul fluxurilor definite.**

  Modificarea datelor critice se realizează doar în cadrul proceselor stabilite.

- **Protecție împotriva manipulării datelor.**

  Sistemul include mecanisme pentru verificarea datelor de intrare și a celor stocate.

- **Măsuri suplimentare pentru date confidențiale.**

  Sistemul poate fi extins pentru funcționalități precum mascarea datelor, criptare și reautentificare.

6. Audit și monitorizare de securitate

Sistemul prevede instrumente dedicate pentru monitorizarea acțiunilor utilizatorilor și evenimentelor de securitate.

- **Audit centralizat.**

  Sistemul colectează și stochează înregistrările de audit într-un mod unificat.

- **Structura înregistrărilor de audit.**

  Fiecare eveniment conține cel puțin: momentul, utilizatorul, obiectul, acțiunea și adresa IP.

- **Compatibilitate cu MLog.**

  Sistemul va putea transmite evenimente critice către platforma guvernamentală MLog.

- **Integritatea datelor de audit.**

  Sunt prevăzute mecanisme pentru protejarea și menținerea consistenței jurnalelor.

- **Păstrarea pe termen lung a jurnalelor.**

Durata se stabilește conform politicilor instituției.

7. Gestionarea erorilor și excepțiilor

SIA „RICC New” include un mecanism centralizat de înregistrare și analiză a erorilor.

- **Înregistrare centralizată a excepțiilor.**

  Toate erorile generate de componente sunt documentate într-o structură unificată.

- **Mesaj standard pentru utilizatori.**

  La producerea unei erori, utilizatorului i se afișează un mesaj generic, fără detalii tehnice.

- **Instrumente de analiză.**

  Sistemul include posibilitatea examinării evenimentelor pentru identificarea cauzelor și remedierea acestora.

13 UTILIZABILITATEA

1. Principii generale de implementare a interfeței

- Interfața este dezvoltată aplicând principiul minimizării schimbărilor pentru utilizatorii versiunii existente a sistemului. Amplasarea elementelor, succesiunea operațiunilor și logica de navigare sunt reproduse în măsura maxim posibilă.
- Interfața este organizată astfel încât operațiunile principale ale utilizatorului să fie realizate cu un număr minim de acțiuni.
- În toate formularele sistemului sunt oferite instrucțiuni privind utilizarea elementelor interfeței și a operațiunilor efectuate.
- Elementele interfeței sunt construite pe baza unor șabloane vizuale și structurale unificate, care asigură predictibilitatea comportamentului.

2. Implementarea interfețelor pentru utilizatori

- Funcționalitățile utilizatorilor sistemului sunt oferite prin interfețe grafice.
- Formularele interfeței sunt dezvoltate cu segmentare pe zone de introducere, vizualizare și executare a operațiunilor, cu o amplasare ordonată a elementelor.
- Interfața este realizată cu localizare completă în limba română.
- În procesele funcționale care necesită păstrarea stării se implementează salvarea intermediară a datelor (automată sau manuală, în funcție de scenariu).
- În interfață sunt incluse mecanisme de filtrare a datelor prin utilizarea măștilor de căutare (de exemplu, „323*”, „*Core”).
- Se utilizează un dicționar centralizat de termeni, care asigură uniformitatea textelor afișate.
- Se implementează posibilitatea de atașare a fișierelor la obiectele sistemului, cu păstrarea fișierelor în conformitate cu regulile de lucru cu obiectele de date.

- Se implementează mecanisme de căutare a datelor.

3. Parametri tehnici și condiții de compatibilitate

- Accesul la sistem se realizează printr-un browser web modern.
- Interfața suportă funcționarea în limbile română și rusă.
- Machetele grafice și componentele interfeței sunt optimizate pentru o rezoluție de cel puțin 1316×1080.
- Schimbul de date între partea client și partea server este organizat cu minimizarea traficului de rețea.
- Interfața este compatibilă cu sistemele de operare Windows 10/11.
- Browsere suportate: Google Chrome, Microsoft Edge.

14 MENTENABILITATE ȘI UȘURINȚĂ ÎN ADMINISTRARE

Arhitectura și mecanismele operaționale ale SIA „RICC New” asigură un nivel ridicat de mentenabilitate, ușurință în administrare, transparență în gestionarea modificărilor, precum și jurnalizarea centralizată a erorilor. Sistemul este proiectat astfel încât impactul modificărilor asupra componentelor existente să fie minim, iar procesele de exploatare să fie eficiente și bine controlate.

1. Implementarea simplificată a modificărilor și minimizarea ariei de impact

Modelul arhitectural al SIA „RICC New” permite:

- structură modulară, care permite modificarea componentelor individuale fără a afecta întregul sistem;
- identificarea clară a modulelor afectate de modificări și a dependențelor acestora;
- localizarea automată a ariilor care necesită testare după modificări;
- cuplare redusă între componente și interfețe bine documentate.

Această abordare reduce costurile de mentenanță și crește predictibilitatea modificărilor.

2. Monitorizarea componentelor critice ale sistemului

Sistemul include mecanisme integrate de monitorizare care asigură:

- observarea nivelului de încărcare asupra serviciilor și asupra bazei de date;
- colectarea telemetriei în timp real (metrici de performanță, utilizarea resurselor, disponibilitatea serviciilor) **după necesitate**.

Aceste funcționalități permit identificarea rapidă a deviațiilor în funcționarea sistemului.

3. Jurnalizarea centralizată a erorilor și excepțiilor

SIA „RICC New” înregistrează:

- toate erorile și excepțiile generate la nivelul aplicației, serviciilor, API-urilor și bazei de date;
- informații tehnice detaliate necesare analizei (stack trace, context de execuție, marcaje temporale);
- date care permit echipei de suport să identifice rapid înregistrarea relevantă din jurnal.

Jurnalele sunt centralizate și pot fi analizate prin instrumentele puse la dispoziție în sistem.

4. Proceduri de tratare și analiză a erorilor

Sistemul oferă capabilități pentru:

- analizarea erorilor înregistrate;
- vizualizarea datelor structurate privind incidentele;
- formularea de recomandări de îmbunătățire pe baza informațiilor colectate.

5. Mesaje de eroare afișate utilizatorului

La apariția unei erori, utilizatorului i se afișează:

- un mesaj neutru, fără detalii tehnice sensibile;
- date care permit echipei de suport să identifice corespunzător incidentul în jurnale.

6. Jurnalizarea acțiunilor utilizatorilor

Sistemul înregistrează:

- autentificarea și deconectarea utilizatorilor;
- operațiunile de modificare a datelor;
- acțiunile administrative;
- evenimentele cu impact asupra securității sau integrității datelor.

Aceasta asigură trasabilitate completă și conformitate cu cerințele de audit.

7. Instrumente de administrare și exploatare a sistemului

SIA „RICC New” pune la dispoziția administratorilor:

- funcționalități de gestionare a componentelor sistemului (pornire, oprire, repornire);
- proceduri automatizate de creare a copiilor de siguranță (baza de date și fișiere de conținut);
- procese de restabilire pe baza copiilor de siguranță;
- mecanisme de verificare a consistenței datelor după restaurare.

Aceste instrumente permit MAI să efectueze operațiunile de administrare fără intervenția dezvoltatorilor.

8. Portabilitatea între medii

SIA „RICC New” poate fi transferată cu ușurință între:

- mediul de producție;
- mediul de testare;
- mediul de dezvoltare.

15 TRANSFORMAREA ȘI MIGRAREA DATELOR

Oferim o metodologie completă și un set de instrumente pentru asigurarea migrării complete, corecte și controlate a datelor istorice din sistemele existente SIA „RICC Old” către Baza de Date Integrată (BDI) a SIA „RICC New”.

15.1 Responsabilități și Metodologie de migrare

Ofertantul își asumă responsabilitatea pentru:

- definirea metodologiei de migrare;
- elaborarea planurilor de migrare;
- pregătirea instrumentelor și procedurilor necesare pentru transferul datelor.

Beneficiarul (MAI) pregătește și furnizează seturile de date necesare. Formatul și structura dataset-urilor sunt stabilite de Executor.

Metodologia de migrare include următoarele elemente:

1. Pregătirea datelor
   Se stabilesc reguli de calitate, standarde de curățare și proceduri de pregătire a seturilor de date.
2. Maparea (Mapping)
   Se dezvoltă metoda de mapare a modelelor de date din SIA „RICC Old” la structura BDI a SIA „RICC New”.

3. Transferul datelor
   Se definesc procesele de transmitere, regulile de verificare a corectitudinii și mecanismele de confirmare a conformității datelor importate.
4. Planul de punere în exploatare
   Include succesiunea acțiunilor, termenele, procedurile de testare și mecanismele de control al succesului migrării.

15.2 Procesul de transformare și asigurare a calității datelor

Ofertantul pune la dispoziție instrumentele software necesare și asigură realizarea următoarelor etape:

1. Validarea și transformarea datelor

- Verificarea calității datelor înainte de integrare.
- Maparea câmpurilor și conversia tipurilor de date.
- Asigurarea compatibilității datelor cu structura BDI.

2. Controlul integrității

- Menținerea tuturor relațiilor logice și legăturilor dintre obiecte după migrare.
- Identificarea și corectarea eventualelor neconcordanțe.

3. Verificarea (Verificarea calității)

- Verificarea și validarea seturilor de date înainte de import.
- Verificarea integrității datelor după migrare.
- În cazul în care datele furnizate conțin erori sau sunt incomplete, Beneficiarul furnizează informațiile suplimentare necesare.

4. Suport pentru diverse scenarii de migrare

- Migrare completă (full).
- Migrare incrementală.
- Migrare în loturi (batch).
- Monitorizarea progresului și controlul volumului de date procesat.

15.3 Recepție și securitate

Transferul datelor

Seturile de date din SIA „RICC Old” sunt transmise către SIA „RICC New” conform metodelor, formatelor și procedurilor stabilite împreună cu Executorul.

Securitate

Pe întreaga durată a procesului de migrare sunt respectate politica de securitate a MAI, standardele de protecție a datelor și cerințele de confidențialitate aplicabile.

Criterii de succes

Etapa de migrare se consideră finalizată atunci când:

- toate datele sunt migrate complet și corect;
- verificările de calitate sunt îndeplinite;
- este semnat Procesul-verbal de recepție a lucrărilor.

16 MODELUL-BUSINESS AL DOMENIULUI DE AUTOMATIZARE

16.1 UC01 „Evidența înștiințărilor despre infracțiuni”

Soluția propusă asigură automatizarea completă a procesului de primire, înregistrare și prelucrare primară a informațiilor despre incidente și infracțiuni în cadrul Etapei 2 de dezvoltare a SIA „RICC New”. Modulul este proiectat ca o verigă centralizată, care conectează sursele externe de informații cu registrele interne ale sistemului.

1. Funcționalități și integrare (CF.1.1)
Sarcina de bază a modulului la această etapă este implementarea cerinței CF.1.1 privind recepționarea automatizată a datelor din sisteme externe.
• **Integrare cu SIA „e-Dosar”**: Sistemul asigură importul automat al datelor și completarea formularului electronic al Registrului nr. 1 (R1) pe baza informațiilor recepționate din SIA „e-Dosar”. Aceasta exclude dublarea introducerii datelor și minimizează riscul apariției erorilor.
• **Interacțiune prin MConnect**: Metoda de schimb de date cu SIA „e-Dosar” va fi determinată la etapa de implementare și, dacă este necesar, integrarea poate fi realizată prin M-Connect

2. Gestionarea registrelor (R1)
Soluția suportă o logică separată de evidență în funcție de natura informației:
• **Registrul nr. 1 (R1)**: Este destinat înregistrării plângerilor oficiale, denunțurilor și materialelor organelor de constatare, în baza cărora se adoptă decizia de inițiere a urmăririi penale.

3. Stack tehnologic și arhitectură
Implementarea modulului se bazează pe un stack modern de tehnologii, aprobat în Caietul de sarcini:
• **Backend**: Dezvoltare pe platforma .NET utilizând limbajul C#, ceea ce asigură performanță înaltă la procesarea tranzacțiilor.
• **Frontend**: Interfață web intuitivă pe baza React, optimizată pentru utilizare prin browsere standard (Chrome, Edge).
• **Securitate**: Accesul la funcțiile de înregistrare este oferit doar după autentificarea cu succes prin serviciul MPass. Fiecare acțiune a utilizatorului, inclusiv crearea și modificarea înregistrărilor, este supusă logării obligatorii în sistemul MLog.

4. Integritatea datelor și identificare
• **Unicitate**: Fiecărui obiect înregistrat în sistem i se atribuie un identificator unic, care rămâne neschimbat pe întreg ciclul de viață al înregistrării.
• **Validare logică (CLV)**: La salvarea formularului R1, sistemul efectuează verificarea automată a respectării condițiilor logice (CLV) furnizate de Beneficiar, ceea ce garantează „curățenia” și

corectitudinea datelor în Baza de date centrală (BDC).
• **Cronologie**: Toate modificările se păstrează în ordine cronologică, cu păstrarea metadatelor despre documentele-bază pentru corectare.

5. Condiții de integrare
Integrarea va fi realizată dacă sistemele externe vor fi pregătite pentru integrare nu mai târziu decât cu 2 luni înainte de expirarea perioadei de dezvoltare a planului contractual agreat. Beneficiarul asigură pregătirea interfețelor de migrare din partea sistemelor externe.

Rezultatul implementării: Implementarea UC01 va asigura crearea unui câmp informațional unic pentru toate organele de urmărire penală ale Republicii Moldova, garantând transparența adoptării deciziilor și completitudinea statisticii primare.

16.2 UC02: Evidența cauzelor penale

Modulul propus asigură colectarea automatizată, înregistrarea și gestionarea ciclului de viață al dosarelor penale în cadrul unui spațiu informațional unic al organelor de urmărire penală.

1. Integrare și import automatizat al datelor (CF.2.2)
În conformitate cu cerințele, implementarea modulului UC02 se bazează pe integrarea strânsă cu sisteme externe:
• **SIA „e-Dosar”**: Sistemul asigură importul automat al datelor despre infracțiunile comise, persoanele suspecte, victime și martori. Informația recepționată este repartizată automat în formularele electronice corespunzătoare (fișe) F1.0–F6.0.
• **SIA „e-Dosar al Procuraturii Generale”**: Modulul recepționează informații actuale despre desfășurarea urmăririi penale și deciziile procesuale ale procurorilor.
• **Sincronizare**: Orice actualizare transmisă din sistemele externe se reflectă în „RICC New”. Sistemul garantează excluderea dublării datelor și păstrarea istoricului complet al modificărilor pentru asigurarea trasabilității.

2. Validare logică și controlul calității (CLV)
Pentru asigurarea „curățeniei” Bazei de date centrale (BDC), toate informațiile recepționate din e-Dosar și e-Dosar al Procuraturii Generale trec prin verificare automată de conformitate cu Condițiile logice de validare (CLV) furnizate de Beneficiar. Sistemul blochează salvarea datelor incorecte și notifică angajatul responsabil despre neconformitățile depistate sau returnează eroarea de validare către sistemul extern.

3. Implementare tehnologică
• **Arhitectură**: Soluția este construită pe baza unei arhitecturi de microservicii utilizând .NET și C#.
• **Stratul de date**: Toate tranzacțiile și legăturile dintre obiecte (dosar – persoană – obiect) sunt fixate în MS SQL Server.
• **Securitate**: Accesul la informațiile dosarelor penale este delimitat pe baza rolurilor (grupul „Evidența”, „Utilizator STI” etc.). Fiecare accesare a materialelor dosarului este fixată în jurnalul de audit MLog.

6. Condiții de integrare
Integrarea va fi realizată dacă sistemele externe vor fi pregătite pentru integrare nu mai târziu

decât cu 2 luni înainte de expirarea perioadei de dezvoltare a planului contractual agreat. Beneficiarul asigură pregătirea interfețelor de migrare din partea sistemelor externe.

Rezultatul implementării: Modulul UC02 elimină necesitatea introducerii manuale a datelor, asigurând transparența completă a circulației dosarelor penale din momentul inițierii până la adoptarea deciziei finale

---

16.3 UC05 “Căutarea interstatală/ internațională a persoanelor”UC02: Evidența cauzelor penale

În conformitate cu solicitarea dvs., soluția se concentrează pe crearea mecanismelor de interfață pentru prelucrarea datelor recepționate prin canalele de comunicare nesistemice existente, asigurând continuitatea proceselor operaționale curente până la momentul automatizării complete a schimbului de date.

• **Descrierea soluției**

Soluția propusă asigură evidența centralizată a persoanelor date în căutare în afara Republicii Moldova, prin implementarea unor instrumente specializate de introducere a datelor, adaptate formatelor curente de schimb de informații cu partenerii internaționali.

1. Dezvoltarea formularelor specializate de introducere a datelor

Pentru a asigura completitudinea bazei de date „RICC New” în cadrul Etapei 2, se dezvoltă două formulare electronice unificate, care permit înregistrarea informațiilor recepționate pe cale nesistemică (de exemplu, prin canale securizate de e-mail, corespondență oficială sau fișiere de schimb):

• **Formularul nr. 1**: Evidența căutării interstatale (spațiul CSI). Formularul este proiectat pentru introducere manuală sau semi-automatizată a datelor corespunzătoare formatului unificat de schimb acceptat între țările CSI. Include un set extins de atribute pentru identificarea persoanei, descrierea infracțiunii comise și temeiul declarării în căutare.

• **Formularul nr. 2**: Evidența căutării internaționale (liniile Interpol). Formular consolidat pentru înregistrarea solicitărilor din partea organizațiilor internaționale. Formularul suportă introducerea datelor, ceea ce pune baza pentru integrarea viitoare cu sistemele europene.

2. Funcționalitățile modulelor de introducere

• **Validare logică (CLV)**: Sistemul verifică automat datele introduse pentru conformitatea cu condițiile logice furnizate de Beneficiar. Aceasta garantează completarea corectă a câmpurilor obligatorii (IDNP, nume de familie, număr dosar de căutare) înainte de salvare în Baza de date centrală.

• **Regimul „Tot el” (UC06)**: Datele introduse prin formulare sunt verificate automat pentru coincidență cu înregistrările deja existente în sistem, pentru a preveni dublarea persoanelor cu identificatori diferiți.

3. Baza tehnologică și securitate

• **Interfață**: Formularele sunt implementate pe baza React și integrate în structura generală de navigare a sistemului „RICC New”, asigurând tranziție „fără cusur” între modulele de evidență și căutare.

• **Audit și logare (UC18)**: Fiecare acțiune de introducere, modificare sau ștergere a informațiilor despre căutare este înregistrată în sistemul MLog, ceea ce asigură transparență totală și

responsabilitate a acțiunilor operatorilor.
• **Drepturi de acces**: Accesul la formularele de introducere este strict limitat rolurilor grupurilor „Evidența” și „Utilizator STI”, conform principiului „este interzis tot ceea ce nu este permis explicit”.

4. Metodologia de implementare
Implementarea prin formulare de introducere în locul integrării directe API la această etapă permite Beneficiarului să înceapă utilizarea sistemului imediat, fără a aștepta pregătirea tehnică a sistemelor informaționale externe ale partenerilor pentru schimb direct de date.

Rezultatul implementării: Crearea unui mecanism fiabil de acumulare a datelor privind căutarea internațională, care asigură actualitatea statisticii și pregătirea sistemului pentru trecerea ulterioară la schimb complet automatizat prin MConnect.

16.4 UC06 „Conexarea persoanelor (regimul „Tot el”)”

Această soluție este orientată spre asigurarea calității și „curățeniei” datelor în sistem prin eliminarea dublării informațiilor despre persoanele fizice în cadrul Etapei 2 de dezvoltare a SIA „RICC New”.

• **Descrierea soluției**
Modulul propus asigură management inteligent al obiectelor de evidență de tip „Persoană fizică”, permițând identificarea și unificarea înregistrărilor duplicat apărute ca urmare a problemelor de înregistrare sau a identificării unor date noi despre persoanele fizice, care permit identificarea mai exactă a persoanei.

1. Destinație funcțională și logica de unificare (CF.6.1)
Sarcina principală a modulului este oferirea utilizatorului a instrumentelor pentru consolidarea mai multor înregistrări despre o persoană fizică într-un singur obiect de sistem.
• **Identificarea dublurilor**: Sistemul permite analizarea înregistrărilor în care coincid parametri-cheie: nume, prenume, patronimic, data nașterii sau IDNP.
• **Eliminarea anomaliilor**: Regimul „Tot el” este destinat corectării erorilor istorice, precum și prelucrării situațiilor în care unei persoane i-au fost atribuite mai multe IDNP sau când cetățeni străini (sau cetățeni cu dublă cetățenie) au fost înregistrați după documente diferite.
• **Unificarea datelor**: La stabilirea conexiunii „Tot el”, datele cu caracter personal ale obiectelor se unifică, creând un profil actual și complet al persoanei în sistem.

2. Păstrarea integrității și a legăturilor (CF.6.2)
Arhitectura soluției garantează că procesul de unificare a înregistrărilor nu va duce la pierderea informațiilor sau la încălcarea structurii logice a bazei de date:
• **Păstrarea legăturilor cu dosarele**: Toate legăturile cu cauzele penale (UC02), care erau atribuite unor „dubluri” separate, sunt transferate automat către înregistrarea unificată.
• **Trasabilitate**: Sistemul păstrează informația despre care anume înregistrări au fost unificate, asigurând posibilitatea auditării istoricului modificărilor obiectului.

3. Domeniu de aplicare și modularitate (CF.6.3)
Regimul „Tot el” este implementat ca funcționalitate transversală și este disponibil în următoarele segmente ale sistemului:

• **Baza de date centrală (**BDC**)**: Pentru asigurarea „curățeniei” statisticii și evidențelor oficiale.
• **Fișierul operativ-informațional (FOI)**: Pentru menținerea corectă a fișierului de evidență a persoanelor care au comis infracțiuni.

4. Implementare tehnologică și securitate
• **Backend și logică**: Implementarea în C# (.NET) asigură viteză înaltă de procesare a procedurilor de fuziune a datelor în MS SQL Server.
• **Validare**: Orice operațiune de unificare a înregistrărilor trece prin modulul de verificare a condițiilor logice (CLV), ceea ce exclude fuziunea eronată a datelor unor persoane diferite.
• **Audit și control (UC18)**: Operațiunea de unificare a identităților este critică, de aceea fiecare astfel de acțiune este supusă logării obligatorii în jurnalul de evenimente, cu fixarea datelor operatorului și a timpului efectuării procedurii.

5. Interfața utilizatorului
Utilizatorului i se oferă o interfață grafică specializată (pe baza React), care permite compararea vizuală a atributelor a două sau mai multe înregistrări înainte de confirmarea fuziunii.

Rezultatul implementării: Modulul UC06 va permite atingerea unui nivel înalt de veridicitate a informațiilor în SIA „RICC New”, excluzând supraestimarea artificială a indicatorilor statistici din cauza dublării persoanelor și asigurând crearea unui dosar digital unic pentru fiecare subiect de evidență.

16.5 UC07 „Registrul de evidență preventivă (evidența persoanelor defavorizate)”

Soluția este orientată spre crearea instrumentelor de avertizare timpurie a infracțiunilor și monitorizare a persoanelor care prezintă o potențială amenințare la adresa securității publice.
• **Descrierea soluției**
În cadrul Etapei 2 de dezvoltare a SIA „RICC New” se implementează un modul specializat de evidență preventivă. Acest instrument este destinat identificării și înregistrării categoriilor de persoane care, la moment, nu sunt implicate în activitate infracțională activă, dar necesită atenție din partea organelor de drept în virtutea modului lor de viață sau a legăturilor asociative.

1. Destinație funcțională și categorii de evidență
Sarcina principală a modulului (cerința CF.7.1) este crearea și menținerea dosarelor digitale pentru persoane al căror comportament sau statut poate indica riscul comiterii infracțiunilor în viitor. Sistemul permite clasificarea obiectelor de evidență în următoarele categorii:
• contravenienți în domeniul protecției ordinii publice;
• persoane care au legături cu locuri de prestare a serviciilor dubioase (pritoane etc.);
• persoane implicate în practicarea prostituției;
• alte categorii de cetățeni a căror activitate necesită monitorizare preventivă conform instrucțiunilor interne.

2. Instrumente de înregistrare și administrare a datelor
Modulul oferă utilizatorilor o interfață completă pentru gestionarea înregistrărilor:
• **Fișa electronică de evidență preventivă**: Conține un set extins de atribute pentru identificarea persoanei, inclusiv descrierea comportamentului, factorilor de risc și temeiurilor

de includere în evidență.
• **Validare logică (CLV)**: La introducerea datelor, sistemul verifică automat corectitudinea completării câmpurilor și respectarea algoritmilor de validare stabiliți. Aceasta previne crearea dublurilor și asigură „curățenia” datelor în Baza de date centrală (BDC).
• **Conectarea obiectelor**: Arhitectura modulului permite stabilirea legăturilor logice interne între persoane, obiecte și adrese în cadrul „Vitrinei de date” (UC22), ceea ce este necesar pentru analiza aprofundată a mediului criminogen.

3. Implementare tehnologică și securitate
• **Stack tehnologic**: Dezvoltarea se realizează pe platforma .NET (C#) cu utilizarea MS SQL Server pentru stocarea datelor, ceea ce garantează viteză înaltă la procesarea interogărilor de căutare și fiabilitate la păstrarea informației.
• **Delimitarea accesului**: Accesul la informațiile evidenței preventive este strict limitat. Drepturile de vizualizare, creare și editare sunt distribuite de administratorul sistemului în conformitate cu modelul de roluri („Utilizator STI”, „Grup Evidența”).
• **Auditul acțiunilor (MLog)**: Fiecare accesare a registrului, introducerea unei informații noi sau modificarea celei existente este supusă protocoalizării obligatorii, ceea ce asigură responsabilitate completă a angajaților.

Rezultatul implementării: Crearea unei baze informaționale eficiente pentru prevenirea criminalității, care permite organelor de drept să acționeze proactiv și să minimizeze riscurile de încălcare a securității publice.

16.6 UC08: Căutarea armelor (identificate) pierdute / Evidența și controlul armelor și muniției

Această soluție este axată pe crearea unei evidențe centralizate a armelor de foc și muniților în cadrul Etapei 2 de dezvoltare a SIA „RICC New”, utilizând date din registrul de stat.
• **Descrierea soluției**
Modulul propus asigură automatizarea proceselor de înregistrare și urmărire a statutului armelor asociate dosarelor penale sau incidentelor. Particularitatea-cheie a implementării este integrarea strânsă cu sistemul de stat de profil pentru asigurarea veridicității datelor.

1. Integrare cu SI „Registrul de stat al armelor” (CF.8.1)
Implementarea modulului se bazează pe interacțiune automatizată cu Registrul de stat al armelor (RSA) prin platforma MConnect:
• **Recepționarea datelor**: Sistemul asigură importul informațiilor actuale despre caracteristicile armei (tip, model, calibru, număr de serie) și proprietarii săi legali direct din RSA.
• **Înregistrarea incidentelor**: La recepționarea informațiilor despre furtul sau pierderea armei, datele se sincronizează cu RSA, ceea ce permite actualizarea statutului obiectelor în ambele sisteme în regim de timp real.
• **Excluderea dublării**: Utilizarea datelor RSA ca sursă etalon garantează lipsa erorilor la introducerea caracteristicilor tehnice ale armei în SIA „RICC New”.

2. Funcționalități de evidență
• **Fișa electronică a obiectului**: Conține istoricul „ciclului de viață” al armei în cadrul sistemului — din momentul introducerii în bază în legătură cu infracțiunea până la depistare, ridicare sau

confiscare.
• **Conectarea cu obiectele de evidență**: Fiecare unitate de armă este legată logic de un dosar penal concret (UC02) și de persoanele corespunzătoare (proprietari, suspecți) în cadrul funcționalității „Vitrina de date” (UC22).

3. Integrare cu Registrul de Stat al Armelor
Datele despre arme, recepționate din RSA și completate în SIA „RICC New”, devin disponibile:
• **Căutare după atribute**: Posibilitatea căutării instantanee după numărul de serie (complet sau parțial), marcă sau model.

4. Implementare tehnologică și securitate
• **Stack tehnologic**: Modulul este dezvoltat pe platforma .NET utilizând C# și stocare în MS SQL Server.
• **Validare**: Toate datele recepționate ca rezultat al integrării cu RSA trec prin verificare automată de conformitate cu condițiile logice (CLV) furnizate de Beneficiar.
• **Audit (UC18)**: Orice acces la informațiile despre armă, precum și operațiunile de schimbare a statutului acesteia, sunt supuse logării obligatorii în jurnalul de evenimente, cu fixarea datelor utilizatorului și a timpului tranzacției.

5. Condiții de integrare
• Integrarea va fi realizată dacă sistemele externe vor fi pregătite pentru integrare nu mai târziu decât cu 2 luni înainte de expirarea perioadei de dezvoltare a planului contractual agreat. Beneficiarul asigură pregătirea interfețelor de migrare din partea sistemelor externe.
•

Rezultatul implementării: Crearea integrării cu Registrul de stat al armelor, care exclude introducerea manuală a datelor și asigură identificarea operativă a obiectelor aflate în căutare sau care figurează ca probe materiale în dosare penale.

16.7 UC14 „Fișierul operativ-informațional al persoanelor care au săvârșit infracțiuni (FOI)”

• **Descrierea soluției**

Soluția propusă este destinată ținerii evidenței operative automatizate a persoanelor care au comis infracțiuni și formării unui dosar digital unic pe baza datelor organelor de urmărire penală, procuraturii și instanțelor de judecată. Modulul FOI este proiectat ca un segment al sistemului cu nivel înalt de protecție pentru activitate operativă și analitică.

1. Integrare cu sisteme externe (MConnect)

Pentru asigurarea completitudinii și veridicității datelor, modulul FOI realizează interacțiune automatizată prin platforma MConnect cu următoarele sisteme:

• **SIA „Urmărire penală: E-Dosar” al Procuraturii Generale**: recepționarea datelor statistice actuale despre infracțiunile comise, mersul dosarelor penale și persoanele cu statut de suspect sau învinuit.

• **SIA „Registrul persoanelor reținute, arestate și condamnate”**: importul informațiilor despre persoanele aflate în detenție (reținute, arestate) sau care își execută pedeapsa, pentru urmărirea operativă a statutului lor curent.
• **Programul Integrat de Gestionare a Dosarelor (PIGD)**: recepționarea informațiilor despre hotărâri judecătorești, sentințe și mișcarea dosarelor în instanțe pentru actualizarea înregistrărilor din fișierul FOI.
• **SIA „Registrul procedurilor de executare”**: acces la date despre acțiunile de executare întreprinse de executorii judecătorești în privința persoanelor din evidențele operative.
• **SIA „Registrul dactiloscopic”**: recepționarea și corelarea datelor despre fișele dactiloscopice (desene papilare) pentru identificarea exactă a persoanei și conectarea obiectelor de evidență cu datele biometrice.

2. Funcționalități ale modulului (CF.14.2)
Implementarea UC14 asigură îndeplinirea următoarelor funcții-cheie:

• **Introducere automatizată și manuală**: posibilitatea înregistrării datelor din surse electronice (prin integrări) și introducerea manuală a informațiilor de pe suport de hârtie de către operator.
• **Căutare complexă**: prelucrarea cererilor operatorilor după date complete (nume complet, data nașterii, IDNP) și efectuarea căutării extinse după atribute incomplete sau intersectate.
• **Actualizare date**: mecanisme de actualizare automată a bazei de date la recepționarea informațiilor noi din sistemele integrate (de exemplu, schimbarea măsurii preventive sau pronunțarea sentinței).

3. Implementare tehnologică și securitate

• **Stack tehnologic**: Modulul este construit pe baza .NET și MS SQL Server, ceea ce garantează performanță înaltă la prelucrarea volumelor mari de date și a interogărilor complexe de căutare.
• **Audit și control (UC18)**: Toate acțiunile operatorilor în modulul FOI (vizualizare date, introducere, modificare, interogări către sisteme externe) sunt supuse logării obligatorii. Evenimentele critic importante sunt duplicate în serviciul de stat MLog pentru a asigura transparență totală și imposibilitatea modificării neautorizate a istoricului.
• **Delimitarea accesului**: Accesul la FOI se acordă conform modelului de roluri („Administrator FOI”, „Operator FOI”) doar după autentificare reușită prin serviciul MPass.

4. Integritate și validare (UC21)
Toate datele recepționate din sistemele E-Dosar, PIGD și alte registre, completând formularele, trec prin verificare de conformitate cu Condițiile logice de validare (CLV). Sistemul asigură corelarea automată a numelor (inclusiv particularități lingvistice) și verificarea câmpurilor obligatorii, ceea ce exclude apariția dublurilor și a înregistrărilor incorecte.

5. Condiții de integrare
Integrarea va fi realizată dacă sistemele externe vor fi pregătite pentru integrare nu mai târziu decât cu 2 luni înainte de expirarea perioadei de dezvoltare a planului contractual agreat. Beneficiarul asigură pregătirea interfețelor de migrare din partea sistemelor externe.

Rezultatul implementării: Implementarea UC14 va crea un instrument centralizat de control operativ, care unește informația de investigație, judiciară, penitenciară și biometrică într-o bază de date unică, actualizată permanent.

16.8 UC15 „Căutarea după obiecte și fișe (Zspravka)”. Dezvoltarea funcționalității de căutare a datelor (Z-spravca)

• **Descrierea soluției**
Pregătirea arhitecturală a stratului analitic (Conceptul Z-spravka)

În cadrul acestei Etape 2 se realizează proiectarea arhitecturii sistemului, asigurând pregătirea tehnologică pentru implementarea ulterioară, la etapele următoare, a instrumentelor de analiză profundă și raportare. Atenția principală este acordată creării unei baze scalabile, care în viitor va permite implementarea următoarelor posibilități

1. Proiectarea modelului de date dinamice: Stabilirea bazelor pentru generarea viitoare a rapoartelor tabelare și de tip listă (ad-hoc) pe baza SQL Server, cu suport pentru rânduri și coloane dinamice.
2. Suport arhitectural pentru structuri modulare: Dezvoltarea unei scheme logice care, în perspectivă, va permite separarea rapoartelor în blocuri (interogare principală, antete, panouri laterale) și aplicarea transformărilor complexe asupra acestora.
3. Determinarea mecanismelor de prelucrare logică: Formarea stack-ului tehnic pentru asigurarea calculelor viitoare (sume, procente, creștere) și a regulilor de corelare a datelor cu perioadele anterioare.
4. Pregătirea standardelor de vizualizare: Crearea structurii pentru suportul șabloanelor configurabile de formatare, inclusiv posibilitatea evidențierii datelor în funcție de condiții și integrarea atributicii corporative (logo-uri, semnături).
5. Proiectarea conceptului interfețelor de interacțiune: Determinarea protocoalelor pentru export/import viitor de date și integrarea cu șabloane externe Excel, cu păstrarea structurii stilurilor.
6. Planificarea drepturilor de acces și a securității: Dezvoltarea conceptului de delimitare a drepturilor de acces la nivel de grupuri de utilizatori pentru gestionarea șabloanelor viitoare de rapoarte.

7. Vizualizare și lucru cu date șterse (CF.15.8)
Una dintre particularitățile-cheie ale Etapei 2 este implementarea mecanismelor de transparență a datelor:
• **Afișarea înregistrărilor șterse**: în interfața FOI va fi implementată posibilitatea de vizualizare a datelor marcate ca șterse. Acest lucru este critic pentru asigurarea auditului și restabilirea cronologiei evenimentelor.
• **Limitarea domeniului de aplicare**: această funcționalitate (vizualizarea datelor șterse) se implementează pentru toate formularele și obiectele dezvoltate în cadrul Etapelor 1 și 2, ceea ce garantează performanță înaltă și afișarea corectă a metadatelor în noul strat arhitectural.

5. Implementare tehnologică și arhitectură
• **Backend**: prelucrarea interogărilor se realizează pe platforma .NET, ceea ce asigură viteză mare de executare a operațiunilor JOIN complexe în baza de date MS SQL Server.

• **Frontend**: vizualizarea „arborelui de conexiuni” dintre obiecte (persoană — dosar — etc.) se realizează cu ajutorul bibliotecilor grafice moderne pe React.
• **Securitate**: accesul la căutare și vizualizarea datelor șterse este strict reglementat de modelul de roluri. Toate interogările de căutare sunt protocoalizate automat în jurnalul de evenimente pentru a preveni accesul neautorizat la informații confidențiale.

16.9 UC16 „Gestionarea clasificatoarelor /nomenclatoarelor” (pentru modulul FOI)

Soluția este dezvoltată pentru a asigura administrarea centralizată a datelor de referință ale sistemului SIA „RICC New” în cadrul Etapei 2.

• **Descrierea soluției**
Soluția propusă oferă administratorilor sistemului SIA „RICC New” un set complet de instrumente pentru gestionarea informației normativ-referențiale, a clasificatoarelor și a metadatelor acestora. Modulul este proiectat ca un component administrativ izolat, care asigură integritatea datelor în toate blocurile funcționale ale sistemului, inclusiv modulul FOI.

1. Funcționalități de gestionare (CF.16.3)
Sistemul asigură executarea ciclului complet de operațiuni pentru mentenanța nomenclatoarelor:
• **Creare și editare**: posibilitatea inițierii clasificatoarelor noi și modificarea structurii celor existente.
• **Gestionarea valorilor**: adăugarea înregistrărilor noi și corectarea valorilor curente din nomenclatoare.
• **Structuri multilevel**: suport pentru gestionarea clasificatoarelor ierarhice (multinivel) pentru reflectarea legăturilor logice complexe.
• **Export de date**: exportul conținutului nomenclatoarelor în diverse formate pentru analiză externă sau backup.

2. Instrumente pentru utilizator și interfață
Pentru sporirea eficienței administratorilor sunt implementate următoarele funcții:
• **Interfață dedicată**: modulul are o interfață grafică separată pentru optimizarea proceselor de administrare.
• **Căutare inteligentă (CF.16.2)**: suport pentru căutare rapidă după primele caractere ale valorii și utilizarea măștilor de căutare pentru găsirea operativă a înregistrărilor.
• **Gestionarea statuturilor (CF.16.4)**: suport pentru versiuni prin mecanisme de atribuire a statuturilor: „activ”, „arhivat” sau „șters”.

3. Aplicabilitate pentru modulul FOI
Funcționalitatea UC16 se aplică pe deplin nomenclatoarelor specializate ale Fișierului operativ-informațional (FOI). Sistemul garantează că clasificatoarele specifice FOI pot fi configurate de angajați dedicați care au drepturile de acces corespunzătoare.

4. Securitate și control (CF.16.1)
• **Delimitarea drepturilor**: accesul la modificarea clasificatoarelor este oferit doar utilizatorilor autorizați conform modelului de roluri, aprobat de administratorul principal.
• **Trasabilitate**: orice modificare a datelor de referință este supusă urmăririi obligatorii (history

tracking). Sistemul fixează cine și când a introdus corectări, ceea ce este critic pentru menținerea „curățeniei” datelor în Baza de date centrală (BDC).

5. Implementare tehnologică
• **Backend**: logica de prelucrare a nomenclatoarelor este implementată pe .NET utilizând C#, ceea ce garantează viteză înaltă a tranzacțiilor la actualizări masive.
• **Stocare**: datele clasificatoarelor sunt plasate în MS SQL Server, ceea ce asigură suport fiabil al legăturilor relaționale și integritatea metadatelor.

Rezultatul implementării: Implementarea UC16 va asigura sistemului „RICC New” flexibilitate și autonomie în gestionarea datelor de referință, permițând adaptarea operativă a clasificatoarelor la modificări legislative sau regulamente interne fără implicarea dezvoltatorilor.

16.10 UC17 „Gestionarea utilizatorilor” (pentru modulul FOI)

• **Descrierea soluției**
Soluția propusă prevede extinderea modulului centralizat de administrare, care asigură ciclul complet de viață al gestionării conturilor, rolurilor și drepturilor de acces în cadrul întregului sistem SIA „RICC New” pentru modulul FOI.

1. Funcționalități de gestionare (CF.17.1 – CF.17.4)
Modulul oferă administratorilor sistemului instrumente pentru configurarea flexibilă a accesului pe baza modelului de roluri (RBAC). Funcțiile principale includ:
• **Gestionarea conturilor**: creare, căutare și editare a profilurilor utilizatorilor (login, parolă, date personale).
• **Delimitare granulară a drepturilor**: atribuirea permisiunilor la nivelul documentelor individuale pentru grupuri de utilizatori și operații (creare, citire, modificare, ștergere).
• **Gestionarea grupurilor**: formarea grupurilor de utilizatori cu definirea cumulativă a drepturilor de acces.
• **Ciclul de viață al contului**: posibilitatea blocării temporare, dezactivării sau ștergerii logice a conturilor fără posibilitatea restabilirii, în scopuri de securitate.

2. Politica de securitate și autorizare
Sistemul implementează o politică strictă de acces, bazată pe principiul „este interzis tot ceea ce nu este permis explicit”.
• **Profilare**: fiecare utilizator autorizat are un profil unic, structurat pe categorii specializate, ceea ce garantează acces doar la informația relevantă atribuțiilor sale de serviciu.
• **Securitatea parolelor**: sunt implementate mecanisme de protecție a parolelor împotriva interceptării și recuperării, precum și politici de complexitate și periodicitate a schimbării credențialelor.

3. Modelul de roluri al sistemului
Soluția suportă separarea rolurilor pentru diferite blocuri funcționale:
• **Blocul Bazei de date centrale (**BDC**)**: include rolurile „Grup de evidență” (vizualizare a tuturor datelor, editare doar a propriilor), „POISK” (doar vizualizare), „Administrator rapoarte” și „Utilizator STI” (acces complet la operații).

• **Fișierul operativ-informațional (FOI)**: include rolurile „Administrator FOI” (acces complet la modul și nomenclatoare) și „Operator FOI” (introducere și editare fără funcții administrative).
• **Administratori specializați**: se alocă roluri de administrator utilizatori, administrator nomenclatoare și administrator de sistem (gestionare backup și restaurare).

4. Implementare tehnologică
• **Interfață**: administrarea se realizează printr-o interfață web grafică intuitivă, dezvoltată pe React.
• **Backend**: toată logica de gestionare a utilizatorilor și verificare a permisiunilor este implementată pe platforma .NET.
• **Trasabilitate**: orice acțiune a administratorului privind modificarea drepturilor sau crearea utilizatorilor este supusă logării interne obligatorii pentru asigurarea auditului de securitate.

Rezultatul implementării: Implementarea UC17 va asigura un control de acces fiabil și flexibil la informațiile confidențiale ale modulului FOI din SIA „RICC New”, permițând serviciilor IT ale Beneficiarului să gestioneze independent drepturile a mii de utilizatori fără implicarea dezvoltatorului.

16.11 UC18: Logarea/ Jurnalizarea activităților utilizatorilor (pentru modulul FOI)

• **Descrierea soluției**
Modulul propus reprezintă un sistem intern de audit care fixează automat evenimentele generate de utilizatori în cadrul proceselor de business digitale. Sistemul este dezvoltat în conformitate cu standardele IT moderne și bunele practici avansate de securitate a datelor.

1. Categorii de evenimente înregistrate
Sistemul asigură înregistrarea obligatorie a următoarelor tipuri de evenimente:
• **Evenimente de sistem**: evenimente critice pentru funcționarea platformei.
• **Evenimente de business**: operațiuni legate de prelucrarea datelor (creare, modificare, ștergere obiecte de evidență), unde înregistrarea este obligatorie pentru asigurarea semnificației juridice a acțiunilor.
• **Evenimente de securitate**: încercări de autentificare (autentificare) și de ieșire din sistem (deautorizare).

2. Componența datelor jurnalului (Componența atributivă)
Fiecare înregistrare din jurnalul de audit conține un set exhaustiv de date pentru reconstruirea contextului evenimentului:
• **Marcaj temporal**: momentul exact al acțiunii (sincronizat cu ceasul sistem al serverului).
• **Subiect (User ID)**: identificatorul unic al utilizatorului care a efectuat acțiunea.
• **Obiect**: entitatea concretă sau elementul de date (de exemplu, dosar penal, fișa armei sau profilul persoanei) asupra căruia a fost direcționată acțiunea.
• **Tipul acțiunii**: descrierea operațiunii efectuate (citire, modificare, ștergere etc.).
• **Sursa (IP-adresă)**: adresa de rețea a dispozitivului de pe care a fost inițiată cererea, precum și numele dispozitivului (dacă este posibil).

3. Securitatea și integritatea jurnalului
• **Protecția confidențialității**: înregistrările de audit nu conțin parole sau alte informații

sensibile (de exemplu, caractere introduse la încercări nereușite de autentificare).
• **Toleranță la erori**: posibilele erori la scrierea datelor în jurnalul de audit nu blochează funcționarea funcțiilor principale ale sistemului, asigurând continuitatea proceselor de business.
• **Mecanism de arhivare**: modulul include funcționalitate de arhivare a înregistrărilor istorice de audit după parametri stabiliți (termen de păstrare, volum de date) – la necesitate.

4. Interfață administrativă și analiză
Administratorilor și ofițerilor de securitate li se oferă instrumente pentru lucrul cu log-urile:
• **Filtrare și căutare**: posibilitatea căutării înregistrărilor după orice câmp (utilizator, perioadă, tip obiect).
• **Trasabilitatea modificărilor**: sistemul permite determinarea ușoară a naturii datelor modificate și găsirea înregistrărilor afectate de evenimente concrete de creare sau modificare.

5. Implementare tehnologică
Modulul este implementat pe partea serverului de aplicații (ASP.NET / C#) utilizând stocare securizată în MS SQL Server. Aceasta garantează viteză înaltă de înregistrare a evenimentelor chiar și la încărcări de vârf (până la 500–1000 sesiuni simultane).

Rezultatul implementării: Crearea unui mediu transparent de responsabilitate, unde fiecare acțiune a utilizatorului este documentată și nu poate fi ascunsă sau modificată, ceea ce este critic pentru sistemele din domeniul aplicării legii.

16.12 UC19 «Generarea rapoartelor standard parametrizate». Dezvoltarea rapoartelor standardizate (statistice și analitice);

• **Descrierea soluției**
Soluția propusă asigură utilizatorilor SIA „RICC New” instrumente pentru formarea rapoartelor statistice în formate optimizate pentru tipărire și analiză ulterioară. În cadrul implementării acestui punct de cerințe, în sistem se introduc 5 rapoarte parametrice predefinite, bazate pe datele acumulate în cadrul Etapei 2.

1. Componența funcțională a raportării
Pentru asigurarea necesităților Beneficiarului, se dezvoltă următoarele rapoarte cel mai frecvent generate:

• **Lista dosarelor de căutare** RPT_902: raport de tip listă pe baza datelor din formularele Dosar de căutare.
• **Lista infracțiunilor** RPT_903: raport de tip listă pe baza datelor din formularele Cauza penală: 1.0, 1.1.
• **Înștiințare despre infracțiune/incident** RPT_920: raport de tip listă pe baza datelor din formularele R1/R2
• CNA lista infracţiunilor RPT_934: raport de tip listă pentru CNA pe baza datelor din formularele Cauza penală.
• **Registru 1,2 pentru CAI al INI** RPT_926: raport pentru subdiviziunea analitică a MAI pe baza datelor din formularele R1/R2

Rapoartele propuse vor fi generate doar pe baza datelor din baza curentă – funcția de obținere a datelor din „ sectiuni” nu este inclusă în Etapa 2.

2. Parametrizare și filtrare
Fiecare dintre cele cinci rapoarte este dotat cu o formă fixă de filtrare, care permite utilizatorului să stabilească valori doar pentru atribute predefinite, de exemplu:
• **Interval temporal**: posibilitatea selectării perioadei (lună, trimestru, an, zi).
• **Structura organizațională**: selectarea subdiviziunii sau organului teritorial concret – depinde de raport.
• **Valori tipice de referință**: filtrare după valori din clasificatoarele de sistem fără posibilitatea modificării logicii filtrului – depinde de raport.

3. Structură și formatare
Designul rapoartelor este strict reglementat pentru a asigura uniformitatea raportării în întregul sistem:
• **Sortare fixă**: ordinea de afișare a datelor (de exemplu, cronologică sau alfabetică) este setată la nivel de cod și nu poate fi modificată de utilizator.
• **Antet unificat**: în antetul fiecărui raport se afișează automat filtrele aplicate, data și ora exactă a generării documentului – la necesitate.
• **Numerotare**: se asigură numerotarea automată continuă a paginilor, rândurilor și coloanelor.

4. Formate de export și tipărire
Sistemul suportă generarea rapoartelor pe baza șabloanelor HTML predefinite. Pentru comoditatea utilizatorilor este implementată posibilitatea exportului documentelor în următoarele formate:
• **MS Excel (.xlsx)**: format implicit pentru lucrul cu date tabelare.
• **PDF**: pentru circuit documentar oficial și tipărire.
• **MS Word (.docx)**: pentru utilizarea datelor în rapoarte text.

5. Securitate și audit
Accesul la generarea rapoartelor este strict limitat de roluri (de exemplu, „Administrator rapoarte”). Fiecare acțiune de formare sau export a raportului este fixată automat în jurnalul de evenimente, ceea ce garantează controlul asupra utilizării informațiilor confidențiale.

Rezultatul implementării: Crearea unei baze fiabile de raportare standard, care permite obținerea indicatorilor statistici-cheie „într-un click”, minimizând influența factorului uman asupra corectitudinii datelor și excluzând necesitatea integrărilor directe cu registre externe la această etapă.

16.13 UC20 «Crearea unor interogări aleatorii în baza de date»» (pentru modulul FOI)

În cadrul Etapei 2 curente de dezvoltare a SIA „RICC New”, această cerință este considerată ca un fundament conceptual-arhitectural. Focusul principal este orientat spre proiectarea mecanismelor analitice, care vor permite la etapele ulterioare implementarea unui instrument complet de generare a rapoartelor în regim ad-hoc.
• **Descrierea soluției**
Soluția propusă este orientată spre crearea condițiilor pentru extragerea operativă a

informației consolidate din SIA „RICC New” și analiza activității utilizatorilor. La această etapă, lucrările de proiect se concentrează pe stabilirea fundamentului pentru implementarea mecanismului de generare a rapoartelor, care în viitor va permite utilizatorilor să formeze „sectiuni” analitice.

1. Formarea bazei arhitecturale
În Etapa 2 se realizează o pregătire critic importantă a sistemului, care asigură funcționalitatea viitoare a modulului UC20:
• **Proiectarea modelului de date**: În cadrul fazei de analiză se proiectează structura bazei de date, optimizată pentru executarea rapidă a tranzacțiilor analitice complexe.
• **Dezvoltarea „Vitrinei de date” (UC22)**: Implementarea acestui modul la etapa curentă este o condiție-cheie pentru UC20, deoarece anume „Vitrina” asigură integrarea obiectelor de evidență și construirea legăturilor între ele, care vor deveni baza pentru interogările viitoare.
• **Unificarea componenței atributive**: Se asigură structurarea datelor într-un format care va permite ulterior selectarea câmpurilor din formularele de introducere pentru includerea în rapoarte dinamice.

2. Conceptul funcționalității viitoare (la etapele următoare)
Bazele puse acum vor permite ulterior implementarea unui generator vizual complet, cu următoarele posibilități:
• **Construirea dinamică a rapoartelor**: Crearea documentelor de tip tabel și listă cu formarea rândurilor și coloanelor în funcție de starea datelor în bază.
• **Analiză multidimensională**: Posibilitatea efectuării studiilor analitice pe baza unuia sau mai multor atribute, cu aplicarea filtrelor.

3. Premise administrative și tehnice
Soluția Etapei 2 prevede elaborarea prototipului unei interfețe administrative pentru lucrul viitor cu baza de date:
• **Instrumente de validare**: Se creează premise pentru executarea de către administrator a interogărilor către tabele, în scopul verificării integrității datelor și corectării masive a informațiilor.
• **Scalabilitate și export**: Arhitectura sistemului este proiectată cu suport pentru exportul volumelor mari de date în formatele PDF, XML, XLS și DOCX, precum și utilizarea șabloanelor HTML.

4. Asigurarea securității și auditului (UC18)
Bazele logării puse la etapa curentă garantează că orice operațiuni viitoare de creare a interogărilor arbitrare vor fi transparente. Sistemul de jurnalizare este proiectat astfel încât să fixeze subiectul, timpul și natura interogării, prevenind accesul neautorizat la informații sensibile.

Rezultatul etapei curente: Este formată o arhitectură analitică stabilă și un model de date, ceea ce garantează implementarea „fără cusur” a generatorului universal de interogări ad-hoc la etapele ulterioare de dezvoltare a sistemului, fără necesitatea reproiectării nucleului SIA „RICC New”.

16.14 UC21 «Gestionarea condițiile logice de validare» (pentru modulul FOI)

Acest modul este destinat asigurării calității, integrității și consistenței datelor în Fișierul operativ-informațional (FOI) prin configurarea regulilor flexibile de verificare a informațiilor la etapa introducerii acestora.

• **Descrierea soluției**
Soluția propusă reprezintă un instrument de administrare vizuală, care permite angajaților cu rolul „Administrator FOI” să configureze independent logica de business de verificare a datelor fără implicarea dezvoltatorilor și fără modificări în codul sursă al sistemului.

1. Funcționalități ale modulului (CF.21.1)
Implementarea modulului UC21 asigură îndeplinirea următoarelor sarcini-cheie:
• **Definirea condițiilor logice**: Crearea regulilor de verificare pentru câmpurile documentelor primare. Sistemul blochează salvarea înregistrării dacă datele introduse nu corespund criteriilor stabilite (de exemplu, data nașterii nu poate fi mai târziu decât data comiterii infracțiunii).

2. Mecanismul multilingv al CLV (Condiții Logice)
Una dintre particularitățile-cheie ale Etapei 2 este dezvoltarea mecanismului de multilingvism pentru sistemul de validare. În conformitate cu cerințele generale pentru interfața SIA „RICC New”:
• **Localizarea notificărilor**: Pentru fiecare condiție logică, administratorul configurează textele mesajelor de eroare și avertisment în mai multe limbi (română, rusă).
• **Adaptivitate**: La declanșarea verificării, sistemul afișează automat utilizatorului explicația în limba selectată în profilul său curent.
• **Nomenclatoare multilingve**: Condițiile logice prelucrează corect datele din clasificatoarele multilingve, asigurând uniformitatea verificărilor indiferent de limba introducerii.

3. Implementare tehnologică și securitate
• **Stack tehnologic**: Modulul este dezvoltat pe platforma .NET (C#) utilizând un mecanism performant de prelucrare a regulilor pe partea serverului de aplicații și a bazei de date MS SQL Server.
• **Interfață de administrare**: Se realizează o interfață grafică comodă pe React, care permite construirea vizuală a regulilor de validare.
• **Auditul modificărilor (UC18)**: Orice modificare, adăugare sau ștergere a unei condiții logice este fixată în jurnalul de audit cu indicarea autorului și a timpului modificării, ceea ce garantează trasabilitatea setărilor sistemului.

4. Excluderea dependențelor externe
În cadrul acestui punct de cerințe, soluția se implementează ca un component intern autonom al sistemului SIA „RICC New”. Toate verificările se efectuează pe baza structurilor interne de date și a clasificatoarelor, fără utilizarea serviciilor externe de integrare la etapa executării validării.

Rezultatul implementării: Modulul UC21 va permite Beneficiarului să adapteze flexibil sistemul la cerințe legislative și instrucțiuni interne în schimbare, asigurând „curățenia” bazei de date FOI și minimizând riscul apariției erorilor tehnice la înregistrarea infracțiunilor și persoanelor.

16.15 UC22 „Vitrina de date”

Soluția este elaborată ca un component arhitectural-cheie al sistemului SIA „RICC New”, asigurând consolidarea datelor și construirea legăturilor între obiectele de evidență în cadrul Etapei 2.

• **Descrierea soluției**
Soluția propusă este destinată gestionării și integrării datelor despre obiectele de evidență în Baza de date integrată (BDI). Modulul „Vitrina de date” asigură corectitudinea, actualitatea și conectivitatea informațiilor, creând „scheletul” informațional pentru funcționarea instrumentelor analitice precum „Z-spravka”.

1. Funcționalități principale (CF.22.1 – CF.22.6)
Implementarea UC22 la această etapă asigură îndeplinirea următoarelor sarcini:

• **Integrarea datelor**: transfer automat al informației din baza documentelor primare (BPD) în baza integrată (BDI).
• **Construirea legăturilor**: formarea și actualizarea lanțurilor logice între diferite obiecte de evidență (de exemplu, legătura „persoană – dosar penal – armă ridicată – mijloc de transport”).
• **Gestionarea atributelor**: prelucrarea și stocarea caracteristicilor suplimentare ale obiectelor, inclusiv indicatori specializați (de exemplu, statut de căutare).
• **Prelucrare automatizată**: analiză periodică a documentelor recepționate pentru actualizarea automată a profilurilor obiectelor de evidență.

2. Particularități de implementare în Etapa 2
În cadrul etapei curente, dezvoltarea modulului „Vitrina de date” se realizează cu următoarele priorități:

• **Focus pe formulare noi**: Toate mecanismele de construire a legăturilor, structurile „vitrinelor” și logica de unificare a atributelor se dezvoltă exclusiv conform cerințelor și logicii noilor formulare electronice create în Etapa 2.
• **Implementare directă în cod (fără configuratoare)**: În conformitate cu planul arhitectural al etapei, soluția implementează logica de business necesară la nivel de cod și structuri BD.
• **Izolare**: Modulul funcționează ca un component intern autonom. Toate procesele de integrare și validare a datelor au loc în interiorul conturului SIA „RICC New” fără utilizarea serviciilor externe de integrare la această etapă.

3. Stack tehnologic și performanță

• **Backend**: Logica de prelucrare și transformare a datelor se implementează pe platforma .NET (C#) utilizând Entity Framework Core, ceea ce asigură viteză înaltă a tranzacțiilor la construirea arborilor complecși de legături.
• **Stocare**: Structurile BDI se desfășoară în MS SQL Server, asigurând integritatea legăturilor relaționale și acces rapid la informația agregată.
• **Scalabilitate**: Arhitectura „vitrinelor” este proiectată cu suport viitor pentru până la 1000 sesiuni simultane și posibilitatea scalării orizontale.

Rezultatul implementării: Implementarea UC22 va forma un strat informațional unic al sistemului, unde datele disparate din diverse fișe statistice sunt unite în profiluri coerente ale obiectelor. Aceasta va asigura fundamentul pentru analiza profundă a informației criminalistice și funcționarea corectă a mecanismelor de căutare ale Etapei 2.

16.16 UC23 „Secțiuni BD «Statistica penală»”

• **Descrierea soluției**

Soluția propusă este orientată spre automatizarea proceselor de reorganizare anuală a bazei de date „Statistica penală”, asigurând transferul obiectelor de evidență din masivul de lucru în fonduri arhivistice sau de tranziție. Accentul principal în implementarea acestui punct de cerințe este pus pe universalitatea mecanismelor de schimbare a statuturilor și izolarea arhitecturală a proceselor.

1. Mecanism universal de transfer al statuturilor și stărilor (CF.23.4)

Spre deosebire de sistemul RICC Old, unde transferul automat al stărilor și curățarea bazei erau limitate doar la un set specific de formulare (1.0, 1.1, 2.1, dosare de căutare și identificare), noua soluție este scalabilă și universală:

• **Acoperirea tuturor tipurilor de date**: Logica de clasificare și rutare a înregistrărilor se aplică tuturor formularelor electronice dezvoltate la etapa curentă și vor fi prescrise în caietul de sarcini pentru dezvoltarea sistemului.

• **Automatizarea tranzițiilor**: Sistemul determină automat apartenența înregistrării la „soldul de tranziție” (soldul de tranziție) în baza stării acesteia la data închiderii anului de raportare.

• **Marcaj inteligent**:

o Obiectele nefinalizate primesc automat indicatorul „anilor trecuți” (PPL) și rămân în masivul de lucru pentru prelucrare ulterioară.

o Dosarele finalizate și soluționate definitiv sunt transferate în fondul arhivistic (FOND) cu marcajul corespunzător, eliberând resursele bazei principale.

2. Izolare arhitecturală și păstrarea integrității

Condiția esențială a implementării este păstrarea stabilității mecanismelor existente de raportare:

• **Independență față de mecanismele de creare a „**sectiuni**”**: Dezvoltarea în cadrul UC23 este limitată exclusiv la logica de schimbare a statuturilor și transferul datelor între straturile logice (PREST — PPL — FOND). Soluția propusă nu atinge și nu influențează algoritmii de creare a „sectiuni” propriu-zise — copiile imuabile ale tabelelor la sfârșitul perioadei. Aceasta garantează că datele istorice „înghețate” vor rămâne intacte, iar raportarea statistică pentru anii trecuți — veridică.

• **Integritatea legăturilor**: La schimbarea statutului formularului și transferul acestuia în PPL sau FOND, se păstrează integral toate referințele încrucișate către obiectele din „Vitrina de date” (UC22), inclusiv legăturile cu persoane, arme sau mijloace de transport.

3. Funcționalități și control (CF.23.5 – CF.23.6)

• **Registrul de control**: Sistemul suportă starea actuală a registrului de control, permițând administratorilor să determine instantaneu locația oricărui dosar penal (baza curentă, PPL sau arhivă).

• **Auditul operațiunilor**: Fiecare acțiune de transfer masiv al datelor sau schimbare a statutului înregistrărilor în timpul reorganizării anuale este fixată în jurnalul de audit (UC18), asigurând trasabilitate completă a procesului.
• **Autonomie**: Soluția se implementează ca un component intern al sistemului SIA „RICC New” la nivel de proceduri ale bazei de date. Integrări externe pentru aceste funcții nu sunt necesare.

4. Implementare tehnologică
• **Platformă**: Logica de prelucrare a masivelor mari de date se implementează pe .NET și C# utilizând tranzacții performante în MS SQL Server.
• **Performanță**: Mecanismul este optimizat pentru prelucrarea datelor în condiții de încărcare înaltă (până la 500–1000 sesiuni simultane), minimizând timpul de indisponibilitate a sistemului în perioada închiderii anului.

Rezultatul implementării: MAI al Republicii Moldova va primi un instrument modern de gestionare a ciclului de viață al datelor, care permite evidență transversală pe toate direcțiile de activitate fără acumularea „zgomotului digital” în bazele curente și fără risc pentru integritatea datelor statistice istorice.

16.17 UC24 „Migrarea datelor”

• **Descrierea soluției**
Soluția propusă descrie procesul de transfer al datelor din sistemul „RICC Old” în baza de date integrată (BDI) a noului sistem. În conformitate cu cerințele etapei curente, migrarea are caracter țintit: se transferă doar seturile de date necesare pentru asigurarea funcționalității componentelor dezvoltate la această etapă.

1. Scopuri și volum de migrare (CF.24.1)
Sarcina principală este transferul obiectelor informației primare și a atributelor acestora pentru asigurarea completitudinii și corectitudinii funcționării noilor module.
• **Limitarea volumului**: Migrarea include doar datele critic importante pentru funcționarea componentelor de sistem ale Etapei 2 (precum FOI, „Vitrina de date”).
• **Autonomia procesului**: Transferul datelor se realizează în interiorul conturului protejat al sistemului. Integrările externe cu registre de stat în cadrul acestui proces nu sunt utilizate.

2. Etapele implementării procesului (CF.24.2 – CF.24.5)
Procesul de migrare se implementează în câteva etape consecutive pentru minimizarea riscurilor de pierdere a datelor:
• **Validare și mapping**: Verificarea datelor sursă înainte de integrare, maparea câmpurilor (mapping) și transformarea tipurilor de date pentru compatibilitate completă cu structura BDI.
• **Asigurarea conectivității**: În timpul transferului, sistemul păstrează și restabilește automat legăturile logice dintre obiectele de evidență, ceea ce este o condiție critică pentru funcționarea ulterioară a „Vitrinei de date” (UC22).
• **Transformare**: Conversia datelor în formatul suportat de noua arhitectură a sistemului.
• **Testare**: Efectuarea migrației în mediul de testare pentru verificarea corectitudinii algoritmilor înainte de transferul final în mediul productiv.

3. Gestionarea erorilor și securitate
Pentru asigurarea transparenței și fiabilității procesului, se implementează următoarele mecanisme:
• **Jurnalizare (Logging)**: Fiecare operațiune de migrare este fixată în jurnalul de sistem. În cazul depistării documentelor problematice, sistemul formează un raport detaliat de erori pentru analiza ulterioară și corectarea manuală.
• **Controlul integrității**: Verificarea finală a datelor în BDI pentru confirmarea că transferul a fost realizat complet și fără distorsiuni.

4. Implementare tehnologică și responsabilități
• **Metodologie**: Migrarea poate fi realizată atât complet, cât și incremental (în porții), ceea ce permite controlul încărcării asupra sistemului și urmărirea progresului în timp real.
• **Distribuirea rolurilor**: Compania noastră (Executantul) asigură dezvoltarea metodologiei, planurilor și instrumentelor software de migrare, în timp ce Beneficiarul pregătește seturile de date inițiale în formatul agreat.

Rezultatul implementării: Implementarea UC24 va asigura SIA „RICC New” cu o bază informațională de calitate, suficientă pentru lansarea completă a funcționalității noi, păstrând în același timp valoarea și conectivitatea datelor acumulate.

16.18 UC25 „Urmărirea motivului ștergerii înregistrărilor în CDB”

Această funcționalitate asigură control strict asupra ciclului de viață al datelor și auditul operațiunilor de excludere a informațiilor din masivul activ al sistemului SIA „RICC New”.
• **Descrierea soluției**
Soluția propusă este orientată spre asigurarea transparenței și trasabilității juridice a procesului de ștergere a informațiilor din Baza de Date Centrala (BDC). Sistemul implementează mecanismul de ștergere logică, care permite excluderea documentelor din circulația curentă și din raportare, păstrând în același timp posibilitatea auditării acțiunilor de ștergere.

1. Delimitarea drepturilor și executanți
Operațiunea de ștergere este o funcție de securitate critică. În cadrul implementării acestei cerințe:
• **Împuterniciri exclusive**: Dreptul de a șterge documente de orice tip se atribuie exclusiv angajaților STI MAI.
• **Model de roluri**: Funcționalitatea este disponibilă doar utilizatorilor cu rolul „Utilizator STI” sau administratorilor de sistem cu privilegii corespunzătoare. Operatorii obișnuiți și inspectoratele teritoriale nu au acces la funcția de ștergere.

2. Justificarea obligatorie a ștergerii (CF.25.1)
Pentru prevenirea ștergerii nejustificate, sistemul blochează executarea operațiunii fără introducerea metadatelor:
• **Introducerea obligatorie a motivului**: La inițierea comenzii de ștergere, sistemul deschide un formular de ecran obligatoriu, în care angajatul STI trebuie să introducă justificarea textuală (motivul) acțiunii efectuate.
• **Componența atributivă**: În baza de date se păstrează o înregistrare care conține

identificatorul documentului șters, ID-ul executantului, marcajul temporal și textul motivului ștergerii.

3. Domeniu de aplicare și tipuri de documente
Mecanismul este universal și nu are limitări după tipul obiectelor:
• **Orice tipuri de documente**: Pot fi șterse orice formulare electronice, fișe statistice (de exemplu, formularele 1.0, 2.1, 6.0) și înregistrări în registre acumulate în sistem.

4. Vizibilitatea datelor și raportare
Se implementează principiul separării vizibilității operative și arhivistice a datelor:
• **Excluderea din rapoarte**: Ștergerea înregistrărilor va permite la etapele următoare excluderea acestor date din toate tipurile de rapoarte statistice, analitice și standard (UC19). Aceasta garantează veridicitatea statisticii oficiale.
• **Acces prin căutare**: Datele șterse nu mai apar în listele generale, dar rămân disponibile pentru vizualizare ulterioară cu condiția activării filtrului special „Afișează șterse”. Aceasta permite angajaților STI să desfășoare investigații interne și să verifice justificarea ștergerilor efectuate anterior.

5. Izolare arhitecturală
• **Legătura cu vitrinele de date**: Implementarea acestui mecanism este autonomă și nu afectează logica „Vitrinei de date” (UC22). Modulul „Vitrina de date” continuă să lucreze cu legături actuale ale obiectelor, în timp ce documentele șterse trec într-un statut special, fără a încălca integritatea structurilor analitice existente.
• **Integrări**: Soluția se implementează ca un component intern al sistemului. Integrări externe pentru această funcție nu sunt necesare.

6. Securitate și audit (UC18)
Fiecare eveniment de ștergere este un obiect al jurnalizării obligatorii. Datele despre motivul ștergerii sunt stocate protejat și sunt disponibile doar pentru audit administratorilor sistemului.

Rezultatul implementării: Crearea unui mecanism de control strict asupra integrității datelor, care exclude dispariția fără urme a informației din sistem și asigură responsabilitatea personală a angajaților STI pentru fiecare operațiune de ștergere a documentelor.

16.19 Extinderea modulului de administrare

Acest component este critic important pentru asigurarea flexibilității și autonomiei funcționării SIA „RICC New”, permițând Beneficiarului să gestioneze logica de business a sistemului.
• **Descrierea soluției**
În cadrul implementării funcționalității Etapei 2, inclusiv introducerea modulului FOI (Fișierul operativ-informațional), „Vitrinei de date” și a noilor formulare, se propune extinderea modulului existent de administrare. Aceasta va asigura management centralizat al parametrilor și nomenclatoarelor specifice, necesare pentru exploatarea stabilă a tuturor subsistemelor noi.

1. Gestionarea parametrilor modulului FOI
Pentru asigurarea funcționării fișierului operativ-informațional (FOI), modulul de administrare se extinde cu următoarele funcții:
• **Nomenclatoare specifice**: Crearea și menținerea clasificatoarelor și nomenclatoarelor

separate destinate exclusiv modulului FOI (de exemplu, categorii de evidență operativă, tipuri de solicitări).
• **Gestionarea drepturilor de acces FOI**: Configurarea drepturilor granulare de acces pentru rolurile „Administrator FOI” și „Operator FOI”, asigurând delimitarea funcțiilor de vizualizare, introducere și corectare a datelor fișierului operativ.

2. Configurare extinsă a parametrilor de sistem
Pentru suportul noilor funcționalități ale sistemului în Etapa 2 se extind instrumentele de configurare generală, care vor fi determinate la etapa de elaborare a caietului de sarcini.

4. Multilingvism și localizare (CLV/ЛУС)
Va fi extins mecanismul de gestionare a traducerilor pentru mesajele de sistem:
• **Notificări multilingve**: Administratorul va putea edita centralizat textele avertismentelor și erorilor verificărilor logice în limbile română și rusă, asigurând interacțiunea corectă a sistemului cu utilizatori din grupuri lingvistice diferite.

5. Securitate și audit al setărilor
Toate modificările parametrilor de sistem și ale clasificatoarelor, efectuate prin modulul de administrare extins, sunt supuse jurnalizării obligatorii în sistem. Aceasta garantează trasabilitate completă a acțiunilor administratorilor și previne modificarea neautorizată a logicii de business.

Rezultatul extinderii: Crearea unui panou universal de administrare, care permite specialiștilor IT ai MAI să adapteze flexibil SIA „RICC New” la sarcinile curente fără implicarea dezvoltatorilor, asigurând pregătirea completă a sistemului pentru lucrul cu informație operativă și analiză complexă.

16.20 Extinderea integrarii cu sisteme externe

Această extindere este necesară pentru susținerea continuității proceselor de lucru și asigurarea raportării statistice corecte în perioada de tranziție.
• **Descrierea soluției**
În cadrul implementării Etapei 2 de dezvoltare a sistemului SIA „RICC New”, cerința-cheie este asigurarea conectivității complete cu versiunea existentă RICC. Aceasta este necesară pentru ca datele înregistrate prin noile module funcționale să fie disponibile în sistemul vechi pentru generarea raportării curente, analiză și executarea sarcinilor specifice, care la această etapă sunt încă atribuite platformei istorice.

1. Mecanismul de transmitere și sincronizare a datelor
Pentru a asigura interacțiunea „fără cusur” a celor două sisteme, va fi utilizat mecanismul de transfer periodic al datelor, bazele căruia au fost puse la etapele anterioare de dezvoltare. Soluția include:
• **Schimb bidirecțional de informații**: Configurarea procedurilor de transfer al datelor introduse în SIA „RICC New” către baza de date a sistemului vechi.
• **Automatizarea procesului**: Transferul datelor va fi realizat în regim de fundal conform unui program prestabilit (Job-scripturi), ceea ce exclude necesitatea dublării manuale a informației de către operatori.

• **Transformare și mapping**: Deoarece sistemul vechi se bazează pe tehnologii Oracle, iar cel nou — pe .NET și MS SQL Server, va fi implementat un strat de mapare a câmpurilor (mapping), care asigură conversia corectă a noilor formulare electronice în structurile de date ale sistemului vechi.

2. Volumul informației transmise
Integrarea acoperă toate obiectele de evidență dezvoltate și implementate în Etapa 2:
• **Documente primare**: Toate fișele statistice și formularele noi, înregistrate în sistemul nou, vor fi replicate automat în baza veche.
• **Datele modulului FOI**: Informația din Fișierul operativ-informațional va fi sincronizată pentru a asigura accesul angajaților MAI la date operative prin interfețele obișnuite ale sistemului vechi.
• **Legăturile obiectelor**: La transmiterea datelor se păstrează integritatea lanțurilor logice dintre obiecte (persoană – infracțiune – decizie), ceea ce este critic pentru funcționarea „Vitrinei de date” și a instrumentelor analitice.

3. Asigurarea integrității și continuității (Business Continuity)
• **Suport pentru raportare**: Implementarea transferului de date va permite utilizarea instrumentelor existente de generare a rapoartelor ale sistemului vechi până la migrarea completă și transferul lor în SIA „RICC New”.
• **Controlul versiunilor**: Sistemul de sincronizare va urmări modificările în înregistrări. La corectarea documentului în sistemul nou, înregistrarea corespunzătoare din sistemul vechi va fi actualizată, ceea ce garantează identitatea informației în ambele contururi.
• **Minimizarea riscurilor**: Abordarea etapizată a integrării permite evitarea întreruperilor în activitatea organelor de drept și garantează stabilitatea proceselor de business ale Beneficiarului în perioada migrației la tehnologii noi.

4. Securitate și audit (UC18)
Toate operațiunile de transfer de date între contururile sistemelor vor fi fixate strict în jurnalul de audit. Sistemul va loga timpul fiecărei sincronizări, volumul înregistrărilor transmise și statutul executării operațiunii (succes/eroare), asigurând transparență completă a procesului pentru administratorii de sistem.

Rezultatul implementării: Integrarea va asigura coexistența temporară a celor două sisteme ca un singur spațiu informațional. Aceasta va permite transferul treptat al înregistrării datelor către noua platformă a Etapei 2, fără a întrerupe funcționarea mecanismelor existente de analiză și raportare ale MAI până la scoaterea completă din exploatare a sistemului vechi.

17 ECHIPA DE PROIECT

Experți cheie:

1) Project manager/ Scrum master
2) Business analist / System arhitect
3) Dezvoltator software
4) Dezvoltator/ Administrator bază de date
5) Dezvoltator /Specialist integrare

6) Dezvoltator /Specialist în migrarea datelor
7) DevOps Expert
8) Specialist Quality Assurance/Formator

Funcție/Rol	Cerințe minime
Manager de Proiect	**Ion Sirbu**
Calificări şi abilităţi solicitate conform caietului de sarcini	• studii superioare în domeniul TIC sau alt domeniu relevant; • cel puțin 7 ani de experiență în dezvoltarea software; • experiența în gestionarea riscurilor proiectului și elaborarea strategiilor de reducere a riscurilor; • cunoașterea instrumentelor de management al proiectelor; • cel puțin 5 ani de experiență demonstrată în managementul echipei/proiectului cu aplicarea metodologiei Agile sau Waterfall, cu cel puțin 2 proiecte implementate în ultimii 3 ani; • cel puțin 2 proiecte finalizate cu succes cu autoritățile publice, experiența în implementarea proiectelor în cadrul autorităților publice din Republica Moldova va fi considerat un avantaj. • cunoașterea ciclului de viață al software-lui; • certificatele recunoscute în domeniul managementului proiectelor vor constitui un avantaj (de ex. Prince, PMI, PMP, etc.). • abilitate de comunicare în limba română.
Confirmarea experienței profesionale	Conform CV-lui anexat
Experienta Profesională specifică	Informația specificată în cv-ul anexat, în partea proiectelor realizate
System Architect/Business Analyst	**Paprotskiy Igor**
Calificări şi abilităţi solicitate conform caietului de sarcini	• studii superioare în domeniul TIC sau alt domeniu relevant; • cel puțin 5 ani de experiență în dezvoltarea/proiectarea software; • cunoașterea ciclului de viață al software-lui; • cel puțin 5 ani de experiență demonstrată în analiză de business cu aplicarea metodologiei Agile sau Waterfall, cu cel puțin 2 proiecte implementate în ultimii 3 ani; • experiența în utilizarea instrumentelor de modelare și a cunoștințelor despre arhitecturi microservicii și cloud, având în vedere scalabilitatea sistemului; • cel puțin 5 ani de experiență în calitate de Business Analist/System arhitect, demonstrată prin implicarea în proiecte în roluri similare pentru proiectarea, dezvoltarea și implementarea de sisteme informatice cu utilizare sau complexitate comparabile; • participarea demonstrată în calitate de Business Analist/System arhitect la cel puțin 2 proiecte de complexitate similară în ultimii 3 ani; • deținerea certificărilor se va considera un avantaj; • abilitate de comunicare în limba română și rusă.
Confirmarea experienței fesionale	Conform CV-lui anexat
Experienta Profesională specifică	Informația specificată în cv-ul anexat, în partea proiectelor realizate
Dezvoltator software	**Croitor Alexandru**
Calificări şi abilităţi solicitate	• studii superioare în domeniul TIC sau alt domeniu relevant;

Funcție/Rol	Cerințe minime
conform caietului de sarcini	• cel puțin 3 ani de experiență în dezvoltarea software; • participarea în cel puțin 2 proiecte de dezvoltare software în ultimii 3 ani cu aplicarea metodologiei Agile sau Waterfall; • experiența în utilizarea stivei tehnologice solicitate; • experiență în utilizarea metodologiilor moderne; • cunoștințe despre securitatea aplicațiilor software; • experiență demonstrată de testare unitară, integrare continuă, DevOps; • deținerea certificărilor în tehnologie propusă se va considera un avantaj; • abilitate de comunicare în limba română și rusă.
Confirmarea experienței fesionale	Conform CV-lui anexat
Experienta Profesională specifică	Informația specificată în cv-ul anexat, în partea proiectelor realizate
Dezvoltator/Administrator Bază de date	**Andrei Cojocaru**
Calificări şi abilităţi solicitate conform caietului de sarcini	• studii superioare în domeniul TIC sau alt domeniu relevant; • cel puțin 5 ani de experiență în dezvoltarea software; • cel puțin 3 ani de experiență în dezvoltarea de software, cu un rol de dezvoltator/administrator de baze de date; • participarea în cel puțin 2 proiecte implementate în ultimii 3 ani cu aplicarea metodologiei Agile sau Waterfall; • experiență în lucrul cu baze de date specifice (Microsoft SQL Server sau PostgreSQL etc); • experiență în implementarea procedurilor de securitate a datelor (ex.:criptare, monitorizare, audit); • experiența cu instrumente de backup/restaurare și replicare a bazei de date; • experiență în proiectarea, dezvoltarea și optimizarea bazelor de date; • deținerea certificării va fi un avantaj; • abilitate de comunicare în limba română și rusă
Confirmarea experienței profesionale	Conform CV-lui anexat
Experienta Profesională specifică	Informația specificată în cv-ul anexat, în partea proiectelor realizate
Dezvoltator /Specialist în integrare	**Vladimir Surcov**
Calificări şi abilităţi solicitate conform caietului de sarcini	• studii superioare în domeniul TIC sau alt domeniu relevant; • cel puțin 5 ani de experiență în dezvoltarea software; • implicare demonstrată într-un rol similar în cel puțin 2 proiecte de complexitate similară sau comparabilă în ultimii 3 ani; • experiență dovedită în integrarea sistemelor informatice, proiectarea și implementarea interfețelor de schimb de date (API-uri) utilizând SOAP/REST; • experiență și abilități în testarea modulară (testarea unitară); • deținerea certificărilor se va considera un avantaj; • abilitate de comunicare în limba română și rusă
Confirmarea experienței profesionale	Conform CV-lui anexat

Funcție/Rol	Cerințe minime
Experienta Profesională specifică	Informația specificată în cv-ul anexat, în partea proiectelor realizate
Dezvoltator /Specialist în migrarea datelor	**Maxim Savencov**
Calificări şi abilităţi solicitate conform caietului de sarcini	• Studii superioare în domeniul tehnologiilor informației și comunicațiilor (TIC) sau în alte domenii relevante; • Cel puțin 5 ani de experiență în dezvoltarea software; • Participarea în cel puțin 2 proiecte de dezvoltare software în ultimii 3 ani, utilizând metodologia Agile sau Waterfall; • Experienței în utilizarea instrumentelor ETL; • Experiență în migrarea și transformarea datelor mari (Big Data); • Experiența în asigurarea conformității cu reglementările privind protecția datelor; • Experiență dovedită cu Oracle Database, testare unitară, integrare continuă și DevOps; • Principii de administrare a soluțiilor cloud; • Cunoașterea principalelor tipuri de amenințări la adresa securității informațiilor și a principiilor de organizare a protecției datelor; • Principii de organizare a procesului de migrare a datelor; • Cunoștințe despre platforme de virtualizare; • Deținerea certificărilor în orice tehnologie din stiva solicitată reprezintă un avantaj; • Abilități de comunicare în limbile română și rusă.
Confirmarea experienței profesionale	Conform CV-lui anexat
Experienta Profesională specifică	Informația specificată în cv-ul anexat, în partea proiectelor realizate
DevOps Expert	**Evgenii Ivanov, Iurie Morari**
Calificări şi abilităţi solicitate conform caietului de sarcini	• licențiat/certificat în tehnologii informaționale sau alte domenii relevante; • experiență în implementarea a cel puțin 2 proiecte similare pe parcursul ultimilor 3 ani; • experiență în testarea modulară, integrarea continuă, DevOps; • experiență cu instrumente precum Kubernetes, Docker etc.; • experiență în securitatea infrastructurii și protecția împotriva atacurilor; • cunoștințe despre arhitecturi scalabile și implementarea în medii cloud; • abilitate de comunicare în limba română sau rusă.
Confirmarea experienței profesionale	Conform CV-lui anexat
Experienta Profesională specifică	Informația specificată în cv-ul anexat, în partea proiectelor realizate
Specialist Quality Assurance/Software Tester/Formator	**Angela Ciobanu**
	• studii superioare în domeniul TIC sau alt domeniu relevant; • cel puțin 3 ani de experiență în testarea software în proiecte de complexitate similară;

Funcție/Rol	Cerințe minime
	• experiență demonstrată în analiza testării și testarea de securitate; • experienței cu instrumente de testare automată; • cunoștințe despre metodologiile de testare de performanță și securitate; • experiență în realizarea sesiunilor de instruire pentru utilizatori finali și specialiști IT; • experiență de scriere a documentației tehnice, documentației destinate pentru utilizatorul final (ghidurilor de utilizare) și livrarea sesiunilor de formare practice; • deținerea certificării va fi un avantaj; • abilitate de comunicare în limba română și rusă
Confirmarea experienței profesionale	Conform CV-lui anexat
Experienta Profesională specifică	Informația specificată în cv-ul anexat, în partea proiectelor realizate

Experți non-cheie

Funcție/Rol	Cerințe minime
UI Designer	**Anna Oleinic**
Confirmarea experienței profesionale	• Conform CV-lui anexat
Experienta Profesională specifică	• Informația specificată în cv-ul anexat, în partea proiectelor realizate

18 FAZELE PROIECTULUI SI PLANUL DE IMPLEMENTARE

Tabelul 1. Termeni și Livrabile

Fază	Sarcină	Livrabile	Durată
Etapa 2. Dezvoltarea ulterioară (etapa II) a reingineriei și automatizării proceselor de lucru aferente gestiunii Registrului Informațiilor Criminalistice și Criminologice în cadrul Ministerului Afacerilor Interne.			
Faza 1	Inițierea proiectului	Livrabile 1.1. Contract semnat	1 lună, după semnarea contractului
		Livrabile 1.2. Planul de management al proiectului (Plan calendaristic de desfăşurare a activităţilor)	
		Livrabile 1.3. Planul de Management al Schimbării și Planul de Management al Riscurilor	
Faza 2	Analiza și proiectarea a sistemului SIA ”RICC New”	Livrabile 2.1. Sarcina tehnică pentru funcționalitățile SIA ”RICC New” care vor fi dezvoltate în etapa 2, conform specificațiilor funcționale și non-funcționale descrise în TOR	4 luni, după faza 1
		Livrabile 2.2. Actualizarea mediului de dezvoltare in infrastructura Prestatorului	
		Livrabile 2.3. Actul de acceptanță a livrabilelor semnat de Furnizor, Beneficiar și Achizitorul produsului.	

Fază	Sarcină	Livrabile	Durată
Faza 3	Dezvoltarea/configurarea sistemului SIA ”RICC New”	Livrabile 3.1. Dezvoltarea și configurare componentele SIA „RICC New” conform specificațiilor funcționale și non-funcționale în: • mediul de producție; • mediul de testare; • mediul de dezvoltare	7 luni, după faza 1
		Livrabile 3.2. Documentație tehnică completă aferentă componentelor implementate. Actualizare Sarcina Tehnică.	
		Livrabile 3.3. Planul și scenariile de testare și testarea componentelor SIA „RICC New” de Ofertant: • unit testing; • stress testing; • load testing.	
Faza 4	Migrare a datelor	Livrabile 4.1. Metodologia de migrare a datelor	1 luna, după faza 3
		Livrabile 4.2. Planul de migrare a datelor	
		Livrabile 4.3. Toate seturile de date relevante deținute de MAI trebuie să fie migrate complet și corect în SIA ”RICC New”.	
		Livrabile 4.4. Raportul cu privire la rezultatele testării SIA ”RICC New” acceptate de către MAI.	
		Livrabile 4.5. Actul de acceptanță a livrabilelor fazei de migrare a datelor în SIA ”RICC New” nou este semnat de către Ofertant și Beneficiar	
Faza 5	Testare de acceptanță	Livrabile 5.1. Plan de testare de acceptanță și actualizarea mediului de producție.	1 luni după faza 4
		Livrabile 5.1. Scenariile de testare pentru toate categoriile de teste (unit testing, stress testing, load testing) acceptate de către MAI	
		Livrabile 5.2. Raportul cu privire la rezultatele testării SIA ”RICC New” acceptate de către MAI	
		Livrabile 5.3. Acceptarea livrabilelor se va face dacă se vor descoperi zero nonconformități critice și mai puțin de 3 nonconformități majore	
		Livrabile 5.4. Actul de acceptanță a SIA ”RICC New” semnat de către Ofertant, MAI	
Faza 6	Instruire și documentare	Livrabile 6.1. Programa de instruire	1 lună după faza 5
		Livrabile 6.2. Planul de organizare a sesiunii de instruire.	
		Livrabile 6.3. Instruirea utilizatorilor de sistem conform planului	
		Livrabile 6.4. Instruire în administrarea și configurarea SIA ”RICC New” (utilizatorii cu rol Administrator de Sistem);	
		Livrabile 6.5. Documente însoțitoare ale SIA ”RICC New”: • ghidul de administrare a SIA ”RICC New”; • ghidul de instalare a SIA ”RICC New”; • ghiduri pentru dezvoltatori, în limita componentelor admise pentru dezvoltare interna pe partea MAI	

Fază	Sarcină	Livrabile	Durată
		Livrabile 6.6. Codul sursă și bibliotecile aferente dezvoltărilor efectuate pentru SIA ”RICC New”. Codul sursă va conține suficiente comentarii pentru a putea fi înțeles de angajații MAI și STI MAI	
		Livrabile 6.7. Materialele de suport destinate instruirii utilizatorilor și testele de evaluare a eficienței instruirii (cel puțin cele destinate administratorilor de sistem și altor utilizatori care dispun de semnătură electronică avansată calificată) să fie disponibile pe Platforma guvernamentală de instruire la distanță „MLearn” sau pe Platforma on line a Academiei de Poliție.	
		Livrabile 6.8. Actul de acceptanță a instruirilor și documentației trebuie să fie semnat de către Furnizor, MAI.	
Faza 7	Lansare în producție. Testare în producție a SIA ”RICC New”	Livrabile 7.1. Planul de lansare în producție a SIA ”RICC New”.	1 lună după faza 6
		Livrabile 7.2. Actualizare seturi de date ce au fost generate/modificate în sistemele actuale după executarea procedurii de populare cu date inițiale	
		Livrabile 7.3. Actul de acceptanță în producție a SIA ”RICC New” este semnat de Ofertant, MAI.	
Faza 8	Acceptanța finală a SIA ”RICC New”	Acceptanța finală a implementării SIA ”RICC New” se va consemna în baza Actului de acceptanță finală semnat de către Ofertant, MAI, cu condiția îndeplinirii următoarelor condiții: • perioada de testare în producție a expirat; • toate erorile, deficiențele și problemele de gravitate 1 sunt înlăturate; • sunt mai puțin de 10 erori și probleme de gravitate 2 neînlăturate; • nici un scenariu de testare nu va corupe integritatea datelor	3 zile calendaristice după faza 8
Faza 9	Mentenanță de garantie a funcționalului elaborat	Livrabile 6.1. Raport privind serviciile de mentenanță de garantie furnizata. Activitățile pot include următoarele : • Mentenanță de garantie pe perioada 12 luni ; • Corectarea defectelor de securitate (la nivel de aplicație); • Înlăturarea erorilor; • Investigarea erorilor detectate în timpul funcționării sistemului; Livrarea periodică a rapoartelor de mentenanță.	12 luni calendaristice după faza 7

19 METODOLOGIA DE SUPORT ȘI MENTENANȚĂ TEHNICĂ

19.1 INTRODUCERE

Scopul și domeniul de aplicare al metodologiei

Această metodologie descrie abordările, procesele și resursele utilizate pentru furnizarea suportului tehnic și mentenanței soluțiilor software și a sistemelor informaționale dezvoltate de compania DAAC Digital. Obiectivul principal este asigurarea unei funcționări stabile, sigure și eficiente a soluțiilor pe tot parcursul ciclului lor de viață.

Suportul este oferit pentru aplicații software specializate și sisteme informaționale complexe dezvoltate de DAAC Digital. Aceste soluții sunt utilizate în diverse sectoare — de la administrația publică până la mediul corporativ — și necesitatea mentenanței regulate, modernizării și protecției este esențială.

DAAC Digital oferă un spectru larg de servicii de suport, orientate spre asigurarea unei funcționări stabile și eficiente a soluțiilor software și a sistemelor informaționale livrate.

Elementele-cheie ale mentenanței includ:

- Menținerea funcționalității complete a aplicațiilor software;
- Asigurarea securității informațiilor;
- Optimizarea performanței;
- Monitorizarea sistematică a funcționării;
- Actualizări regulate ale componentelor;
- Corectarea promptă a erorilor și vulnerabilităților;
- Instalarea actualizărilor de securitate;
- Extinderea funcționalității conform noilor cerințe de business

Metodologia adoptată se bazează pe bune practici internaționale în managementul incidentelor, al problemelor și al schimbărilor. Aceasta garantează un nivel înalt de disponibilitate și satisfacție în rândul utilizatorilor finali.

Pentru a gestiona eficient aceste procese, compania a creat o unitate dedicată de suport tehnic, care coordonează toate activitățile de mentenanță, răspunde prompt incidentelor și optimizează în mod constant procesele operaționale.

Echipă de experți și certificare

Suportul este asigurat de circa 50 de specialiști de înaltă calificare. Mulți dintre ei au urmat cursuri certificate și seminare internaționale. Un număr semnificativ de angajați dețin certificate recunoscute la nivel internațional de la branduri tehnologice de top, precum:

- Oracle
- Dell
- Cisco
- Microsoft
- APC
- Apple
- FG Wilson și altele

19.2 METODOLOGIE ȘI STANDARDE DE MANAGEMENT AL CALITĂȚII

DAAC Digital respectă metodologii de management al calității recunoscute la nivel internațional, precum și standarde de industrie, cu scopul de a asigura un nivel ridicat de servicii, fiabilitate operațională și îmbunătățirea continuă a proceselor de suport tehnic.

Abordarea noastră se bazează pe un cadru structurat și adaptabil, fundamentat pe bune practici validate, ce acoperă întreaga paletă a serviciilor IT – de la gestionarea incidentelor și

schimbărilor, până la monitorizarea calității și analiza performanței - asigurând conformitatea cu cerințele industriei și angajamentele contractuale stabilite prin SLA.

Am adoptat frameworkul ITIL (Information Technology Infrastructure Library), care oferă un cadru metodologic clar și coerent pentru gestionarea serviciilor IT (ITSM). Acesta acoperă integral procesele de gestionare a incidentelor, rezolvare a problemelor, control al modificărilor și asigurare a continuității operaționale. Respectarea principiilor ITIL ne permite să implementăm procese de suport bine documentate, trasabile și aliniate cu obiectivele de business ale clienților noștri.

Sistemul nostru de management al calității este construit în conformitate cu standardul internațional ISO 9001:2015, oferind o abordare sistemică pentru îmbunătățirea continuă a calității serviciilor și creșterea satisfacției clienților. În paralel, respectăm cerințele ISO/IEC 27001 privind securitatea informațională, ceea ce presupune aplicarea unor protocoale stricte de protecție a datelor și de administrare a accesului în cadrul activităților de suport.

În ceea ce privește dezvoltarea și mentenanța aplicațiilor software, compania aplică metodologii internaționale moderne care permit lansarea rapidă a actualizărilor, integrarea continuă și adaptarea flexibilă la evoluția cerințelor de business. Aceste practici contribuie la identificarea și corectarea promptă a erorilor, instalarea patch-urilor de securitate și menținerea stabilității aplicațiilor.

Angajamentul nostru față de standarde ridicate este confirmat prin audituri interne și externe periodice, programe de dezvoltare profesională și evaluări constante ale performanței pe baza indicatorilor KPI. Acest lucru ne permite să livrăm servicii conforme cu SLA-urile asumate și cu cerințele sectoriale, oferind clienților noștri un nivel înalt de satisfacție și încredere.

Prin aplicarea acestor standarde și metodologii recunoscute la nivel global, garantăm un model operațional structurat, transparent și eficient, ce susține funcționarea optimă a sistemelor informatice și consolidează parteneriatele pe termen lung.

SUPORTUL UTILIZATORILOR ȘI SUPORTUL TEHNIC

Suportul utilizatorilor și suportul tehnic asigură funcționarea continuă și fiabilă a sistemului informațional, precum și un nivel ridicat de satisfacție în rândul utilizatorilor finali. Aceste servicii sunt furnizate în baza unor procese bine definite, care includ înregistrarea, procesarea, soluționarea și analiza solicitărilor utilizatorilor și a incidentelor tehnice

Principiile fundamentale ale suportului:

- Accesibilitate și multicanal: Suportul este disponibil prin multiple canale de comunicare: service desk, e-mail, telefon sau portal de tichete. Toate solicitările sunt înregistrate în sistemul de management al incidentelor și al modificărilor.
- Model ierarhic de suport (pe niveluri): Distribuția clară a responsabilităților între liniile de suport permite gestionarea eficientă a solicitărilor în funcție de complexitate
    - Nivelul 1 (suport primar): Primește solicitările utilizatorilor, realizează diagnosticarea inițială, oferă consultanță pentru situații uzuale și furnizează instrucțiuni de utilizare.

  - Nivelul 2 (suport avansat): Se ocupă de incidentele tehnice care necesită investigații detaliate, colaborând cu administratorii de sistem și echipele tehnice interne.
  - Nivelul 3 (expertiză specializată): Implică dezvoltatori sau experți externi care realizează analize aprofundate și intervin asupra codului, arhitecturii sau configurației aplicației.
- Clasificarea și prioritizarea solicitărilor: Fiecare solicitare este înregistrată cu un identificator unic, nivel de prioritate și categorie, în funcție de impactul asupra proceselor de business. Se stabilesc termene clare de răspuns și rezolvare în conformitate cu SLA-ul agreat.
- Monitorizare și escaladare: Timpul de soluționare al fiecărei solicitări este monitorizat constant. În cazul în care există riscul de nerespectare a SLA-ului sau întârzieri, se activează automat procedura de escaladare către nivelul superior de responsabilitate, cu notificarea părților implicate.
- Feedback și satisfacția utilizatorilor: Solicitările sunt închise doar după confirmarea rezolvării din partea utilizatorului. Acesta are posibilitatea de a oferi un scor de satisfacție și comentarii, care sunt ulterior analizate pentru îmbunătățirea continuă a calității serviciilor

TIPURI DE MENTENANȚĂ APLICABILĂ PRODUSULUI SOFTWARE

În funcție de natura modificărilor, obiectivele urmărite și gradul de urgență al intervenției, mentenanța unui produs software poate fi clasificată în mai multe tipuri principale. Această structurare permite o gestionare clară a solicitărilor, o prioritizare corectă a sarcinilor și o alocare eficientă a resurselor.

Mentenanță în perioada de garanție

Se realizează pe durata termenului de garanție stabilit contractual, începând cu data recepției produsului software. Aceasta vizează corectarea defectelor apărute fără vina

Beneficiarului și nu implică costuri suplimentare. Intervențiile au caracter corectiv și au drept scop menținerea funcționării declarate a sistemului.

Mentenanță corectivă

Are ca scop identificarea și remedierea erorilor sau defecțiunilor apărute în exploatarea sistemului. Problemele pot rezulta din erori de proiectare, implementare sau integrare. Având impact direct asupra funcționării, acest tip de mentenanță este tratat cu prioritate ridicată.

Exemple: corectarea bug-urilor, restaurarea funcționării după blocaje, eliminarea erorilor logice.

Etape:

- Testarea și compararea datelor;
- Identificarea și localizarea erorii;
- Analiza cauzei și remedierea;
- Verificarea funcționalității restaurate;
- Documentarea rezultatelor.

Mentenanță adaptivă

Se aplică în contextul modificărilor survenite în mediul tehnologic extern în care sistemul este integrat. Poate include migrarea pe echipamente noi, actualizarea sistemului de operare, schimbarea SGBD-ului sau ajustarea formatelor de integrare și raportare. Scopul este adaptarea sistemului la noile condiții, fără modificarea logicii aplicației.

Exemple: trecerea la o nouă platformă server, configurarea integrării cu un API actualizat, generarea de rapoarte grafice în locul celor tabelare.

Etape:

- Colectarea și clarificarea cerințelor;
- Analiza modificărilor necesare;
- Proiectarea soluțiilor;
- Implementarea și validarea actualizărilor.

Mentenanță evolutivă (dezvoltativă)

Are ca obiectiv îmbunătățirea continuă a sistemului prin extinderea funcționalităților, optimizarea experienței utilizatorului și creșterea performanței generale. Această categorie de mentenanță nu este determinată de defecțiuni sau de necesități de adaptare, ci este inițiată la solicitarea Beneficiarului pentru a sprijini evoluția proceselor de afaceri și pentru a răspunde cerințelor în schimbare ale organizației.

Exemple: dezvoltarea de funcționalități noi, modernizarea interfeței grafice, automatizarea fluxurilor de lucru, reducerea timpilor de procesare.

Obiective:

- Creșterea performanței sistemului;
- Îmbunătățirea experienței utilizatorului;
- Extinderea funcționalităților aplicației.

NIVELURI DE SUPORT

Nivel de suport	Descriere
Nivelul 1	Suport de bază: preluarea și înregistrarea solicitărilor, furnizarea de informații generale și consultanță, direcționarea cererilor către nivelurile corespunzătoare.
Nivelul 2	Analiză tehnică avansată: diagnosticarea incidentelor, rezolvarea problemelor standard și recurente, colaborarea cu echipele tehnice interne.
Nivelul 3	Dezvoltare și implementare de remedieri: intervenții asupra codului sursă, colaborare cu furnizori și vendori, soluționarea problemelor complexe și atipice.

PLANUL DE MENETENANȚĂ AL PRODUSULUI SOFTWARE

Planul de mentenanță reprezintă o componentă esențială a metodologiei de suport și are ca scop asigurarea funcționării continue, stabile și sigure a sistemului informațional pe tot parcursul ciclului său de viață.

Mentenanța acoperă atât activități tehnice, cât și operaționale și include toate componentele și modulele-cheie livrate împreună cu produsul software.

Elementele principale ale planului de mentenanță:

- **Suport planificat:** Executarea periodică a activităților programate, precum verificarea stării serviciilor, monitorizarea jurnalelor de erori, analiza gradului de utilizare a resurselor, curățarea datelor temporare și alte acțiuni preventive.
- **Acțiuni preventive:** Analiza regulată a stării sistemului și prevenirea potențialelor incidente prin audituri de performanță, analiză a jurnalelor de erori, gestionarea vulnerabilităților și configurarea corespunzătoare a setărilor de securitate.
- **Gestionarea incidentelor și a solicitărilor:** Răspuns prompt la solicitările utilizatorilor și la erorile tehnice, în conformitate cu termenele definite în SLA. Toate solicitările sunt gestionate printr-un sistem centralizat de tichete, cu monitorizarea termenelor, responsabililor și rezultatelor.
- **Procesarea solicitărilor și incidentelor:** Intervenție operativă în caz de disfuncționalități tehnice sau cereri din partea utilizatorilor. Toate tichetele sunt înregistrate și urmărite în funcție de nivelul de prioritate și tipul de suport aplicabil.
- **Monitorizare și backup:** Supravegherea continuă a parametrilor tehnici ai sistemului și realizarea automată a copiilor de siguranță, inclusiv verificarea capacității de restaurare.
- **Actualizări și îmbunătățiri periodice:** Implementarea noilor versiuni, patch-uri și funcționalități suplimentare, după testarea și aprobarea acestora de către Beneficiar. Propunerile de optimizare sunt puse în aplicare pe baza analizei incidentelor și a feedbackului utilizatorilor.
- **Raportare și documentare:** Generarea periodică de rapoarte privind activitățile de mentenanță, inclusiv statistici despre incidente, acțiunile întreprinse, timpii de răspuns și remediere, precum și recomandări pentru îmbunătățiri ulterioare.

19.3 SERVICIUL DE SUPORT „SERVICE DESK”

Pentru asigurarea unei livrări eficiente a serviciilor de suport, compania utilizează un sistem automatizat de gestionare a solicitărilor – Service Desk, construit conform standardelor ITIL (Information Technology Infrastructure Library) și principiilor de IT Service Management (ITSM). Metodologia ITIL, recunoscută la nivel internațional, oferă cele mai bune practici pentru organizarea activităților și cooperarea între departamentele IT în contextul asigurării suportului operațional.

Beneficiile implementării soluțiilor bazate pe ITIL/ITSM:

- Serviciile IT devin orientate către client, iar SLA-ul contribuie la îmbunătățirea relației
- furnizor–beneficiar;

- Serviciile sunt prezentate într-un limbaj accesibil clientului, cu detalii clare și
- relevante;
- Se asigură un control sporit asupra calității și costurilor serviciilor livrate;
- Se îmbunătățește colaborarea între client și echipele de suport.

Sistemul integrat Service Desk din cadrul companiei gestionează recepția și procesarea solicitărilor, incidentelor, reclamațiilor și cererilor, precum și analiza și interpretarea acestora pentru acțiuni ulterioare.

Canale de contact

Toate solicitările sunt înregistrate prin număr de telefon multi-canal sau adresă de e- mail dedicată.

Etapele de procesare a solicitărilor:

1. Recepționarea cererii și primul contact cu clientul;
2. Înregistrarea incidentului sau a solicitării de intervenție;
3. Evaluarea inițială, încercarea de remediere sau alocarea către responsabilul tehnic;
4. Atribuirea inginerului responsabil pentru remedierea problemei;
5. Identificarea cauzei problemei;
6. Soluționarea incidentului;
7. Evaluarea necesității de instruire suplimentară pentru utilizator;
8. Închiderea incidentului și notificarea clientului.

Procesul de tratare a incidentelor:

1. Utilizatorul final notifică echipa de suport IT (personal, telefonic sau prin e-mail) despre problema întâmpinată;
2. Echipa IT încearcă rezolvarea la primul nivel. Dacă problema este soluționată, incidentul se închide;
3. Dacă soluționarea nu este posibilă, iar problema ține de sistemul implementat, incidentul este transferat către echipa de suport tehnic;
4. Echipa de suport:
5. utilizează experiența și cunoștințele despre sistem pentru remedierea situației sau identificarea cauzei;
6. informează echipa IT despre progresul rezolvării și starea generală a
7. sistemului;
8. Dacă problema nu poate fi soluționată la primul nivel, ea este escaladată la
9. nivelul doi de suport tehnic;
10. Inginerii de nivel doi actualizează echipa IT privind măsurile luate și statusul;
11. Nivelul doi are acces la patch-uri, actualizări și instrumente de diagnostic;
12. Toate incidentele sunt înregistrate într-o bază de date dedicată.

Suportul pentru probleme tehnice complexe este de asemenea disponibil prin telefon și e-mail. La solicitarea Beneficiarului, poate fi implementat un sistem de monitorizare la distanță, care trimite notificări automate în caz de probleme. Această funcționalitate este esențială pentru sisteme critice (Non-Stop), unde nu este disponibilă prezență umană continuă. Disponibilitatea acestui sistem depinde de infrastructura de comunicații și platforma tehnologică utilizată.

Clasificarea și prioritizarea solicitărilor

Pentru eficiență, sistemul Service Desk clasifică cererile după următoarele criterii:

Nivel de criticitate (prioritate):

Nivel	Описание
Înalt	Incidente majore care afectează procese de business critice sau toți utilizatorii (ex. indisponibilitate completă a sistemului)
Mediu	Disfuncționalități parțiale sau care afectează un grup restrâns de utilizatori
Scăzut	Probleme minore fără impact asupra funcțiilor principale (ex. erori vizuale, sugestii de UI)

Tipuri de solicitări:

- Incident – disfuncționalitate neprevăzută a sistemului;
- Cerere de modificare – ajustare a funcționalității, configurării sau mediului de operare;
- Consultanță – cerere de informații, clarificări sau ghidare.

Timp de răspuns și rezolvare (SLA):

Prioritate	Timp de răspuns	Timp de rezolvare
Înalt	1 oră	24 ore
Mediu	4 ore	5 zile lucrătoare
Scăzut	1 zi lucrătoare	Conform planificării/specificațiilor

Serviciile de suport sunt oferite în zilele lucrătoare conform legislației Republicii Moldova, între orele 09:00–18:00. Timpul total alocat pentru suport nu va depăși 20 de ore pe săptămână.

19.4 ACORDUL PRIVIND NIVELUL SERVICIILOR (SLA)

Furnizorul se angajează să monitorizeze și să furnizeze Beneficiarului rapoarte privind următoarele cinci (5) categorii de SLA, cu posibilitatea auditării ulterioare a respectării fiecărui indicator:

1. SLA privind disponibilitatea sistemului (Uptime SLA)

Furnizorul va întreprinde toate măsurile rezonabile pentru a asigura disponibilitatea aplicației și a sistemului pentru toți utilizatorii. „Timpul de disponibilitate” este definit ca diferența dintre numărul total de ore dintr-o lună și durata perioadelor de mentenanță planificată. Uptime-ul este exprimat procentual, reprezentând timpul în care sistemul a fost complet accesibil și funcțional fără degradarea calității serviciului. Ținta de disponibilitate pentru sistemul informațional este de 99,9%.

2. SLA privind timpul de răspuns (Response Time SLA)

Furnizorul este responsabil de menținerea timpului de încărcare a paginilor și a timpului de răspuns al sistemului în limitele standardelor industriei pentru aplicațiile web.

Având în vedere arhitectura distribuită a sistemului și integrarea acestuia cu servicii externe, timpul de răspuns poate fi influențat de performanța acestor sisteme terțe.

În timpul implementării, Furnizorul colectează metrici privind timpul de răspuns al sistemelor externe și al interfeței aplicației. Pe baza acestor date, în colaborare cu Beneficiarul, se stabilesc valorile de referință acceptate pentru timpii de răspuns în funcție de scenariile de utilizare.

3. SLA privind monitorizarea sistemului

Furnizorul este obligat să implementeze proceduri de monitorizare a resurselor sistemului, inclusiv încărcarea procesorului (CPU), utilizarea memoriei RAM, spațiul pe disc și alți parametri relevanți pentru disponibilitate și performanță.

Monitorizarea trebuie să genereze alerte în cazul depășirii pragurilor critice și să permită intervenții proactive.

- Beneficiarul va fi notificat în timp util (estimativ cu 2–3 luni în avans) în cazul în care se constată în mod constant depășiri ale pragurilor ce pot afecta performanța sau stabilitatea sistemului, astfel încât să poată fi planificate modificări de configurare sau upgrade-uri de echipamente.
- În cazul abaterilor de la metricele agreate care pot afecta disponibilitatea, performanța sau stabilitatea aplicației, Furnizorul va transmite notificări către Beneficiar în cel mai scurt timp de la identificarea problemei prin intermediul sistemului de monitorizare.

4. SLA privind evaluarea cerințelor de îmbunătățire

În cazul în care, pe parcursul executării contractului, Beneficiarul sau alte părți interesate definesc cerințe funcționale noi care nu sunt prevăzute în documentația tehnică inițială, Furnizorul va colabora cu Beneficiarul pentru formularea cerințelor detaliate aferente funcționalității solicitate.

După aprobarea specificației, Furnizorul se angajează să transmită o estimare a duratei și a costurilor de implementare în termen de maximum o (1) săptămână.

19.5 MONITORIZARE ȘI RAPORTARE

Pentru a asigura transparența, controlul calității și îmbunătățirea continuă a proceselor de suport tehnic, se desfășoară o monitorizare sistematică a indicatorilor-cheie de performanță (KPI), însoțită de raportare periodică.

Indicatori-cheie de performanță (KPI):

- **Numărul total de solicitări** — permite evaluarea volumului de muncă al echipei de suport și identificarea perioadelor cu încărcare maximă;
- **Nivelul de satisfacție al utilizatorilor** — determinat pe baza feedbackului colectat prin chestionare, sondaje sau indicatorul NPS (Net Promoter Score), reflectă calitatea percepută a serviciilor din perspectiva clientului.

Raportare periodică:

La solicitarea Beneficiarului, pot fi elaborate rapoarte privind: stadiul actual al proiectului; funcționalitățile implementate; integrările realizate; stabilitatea sistemului; alte aspecte relevante în funcție de prioritățile clientului.

Formatul și frecvența acestor rapoarte se stabilesc de comun acord între părți.

1. FORMATUL RAPORTĂRII

Pentru urmărirea progresului sarcinilor în derulare, este utilizat un format standardizat de raportare. Raportul conține informații despre activitățile finalizate și cele în curs, statusul lucrărilor, timpul efectiv consumat și estimările privind finalizarea. Acesta poate fi furnizat la o frecvență prestabilită (săptămânal, lunar sau la cererea Beneficiarului).

Structura raportului:

№	ID-ul Sarcinii	Denumire sarcinii / Descriere activitate	Statut	Timpul utilizat	Timpul rămas / Termen de finalizare
1	TASK-001	Dezvoltarea modulului de autorizare	În lucru	12 h	8 h / până la dd.mm.aaaa
2	TASK-002	Testarea funcționalității rapoartelor	Finalizat	6 h	la solicitare
…	…	…	…	…	…

Explicații ale coloanelor:

- № – număr secvențial al înregistrării în tabel;
- ID-ul sarcinii – identificator unic al activității, generat în sistemul de management al

- sarcinilor;
- Denumire sarcinii / Descriere activitate – scurt rezumat al obiectului sarcinii sau al
- lucrării efectuate;
- Statut – starea actuală a sarcinii (de ex: În desfășurare, Finalizată, În așteptare, Amânată);
- Timpul utilizat – numărul de ore utilizate pentru realizarea sarcinilor;
- Timpul rămas / Termen de finalizare – estimarea resurselor de timp rămase sau data limită pentru încheierea activității.

19.6 INSTRUIREA ȘI DEZVOLTAREA PERSONALULUI

Pentru a asigura un nivel ridicat al calității serviciilor de suport, echipa beneficiază în mod regulat de activități de instruire și dezvoltare profesională, structurate pe următoarele direcții:

Programe de perfecționare profesională

Angajații din cadrul echipei de suport participă la cursuri specializate, axate pe aprofundarea cunoștințelor tehnice, dezvoltarea abilităților de comunicare cu utilizatorii și gestionarea incidentelor în conformitate cu SLA-urile stabilite.

Traininguri și seminare periodice

Sunt organizate sesiuni interne și externe privind noile produse, actualizările de sistem, procedurile de procesare a solicitărilor și cerințele de securitate informațională. Aceste activități contribuie la menținerea actualizată a competențelor și la adaptarea continuă la modificările de sistem.

Onboarding pentru angajații noi

Pentru specialiștii noi este prevăzut un program standardizat de integrare, care include familiarizarea cu normele de sprijin, instrumentele utilizate și baza de cunoștințe.

Promovarea unei culturi a învățării continue

Se încurajează schimbul de cunoștințe între specialiști, analiza colectivă a cazurilor standard și excepționale, precum și implicarea activă în revizuirea incidentelor și în sesiunile de tip retrospectivă. Acest cadru sprijină dezvoltarea competențelor colective și consolidarea expertizei operaționale în cadrul echipei.

19.7 POLITICI DE SECURITATE ȘI CONFIDENȚIALITATE

În cadrul prestării serviciilor de suport, se acordă o atenție deosebită protecției informațiilor, confidențialității datelor și respectării cerințelor de securitate. Se aplică următoarele politici esențiale:

Protecția datelor utilizatorilor

Toate datele cu caracter personal și informațiile de serviciu ale utilizatorilor sunt prelucrate în conformitate cu legislația în vigoare și reglementările interne. Accesul la aceste date este permis exclusiv persoanelor autorizate și strict în limita atribuțiilor funcționale.

Politici de stocare a informațiilor

Informațiile referitoare la solicitările utilizatorilor, jurnalele de activitate și datele tehnice sunt păstrate în sisteme securizate, pentru perioadele definite de politicile interne și cerințele legale. La expirarea termenelor, datele sunt fie șterse în siguranță, fie arhivate conform procedurilor stabilite.

Controlul accesului la sistem

Sistemul implementează mecanisme de control al accesului pe bază de roluri (RBAC), precum și auditarea activităților utilizatorilor. Accesul este acordat conform principiului privilegiului minim necesar (least privilege). Toate operațiunile care implică date confidențiale sunt înregistrate în jurnalele de securitate și pot fi analizate ulterior, la nevoie.

19.8 SUPORT ÎN PERIOADA DE GARANȚIE ȘI DE POST-GARANȚIE

După finalizarea etapei de recepție, produsul software intră în faza de suport în garanție, în cadrul căreia se asigură remedierea defecțiunilor, a erorilor tehnice și a altor abateri de la specificații apărute fără culpa Utilizatorului. Suportul în garanție acoperă toate modulele și componentele livrate ca parte a sistemului informațional.

Suportul în perioada de garanție include:

- Recepționarea și analiza solicitărilor din partea Utilizatorului;
- Remedierea promptă a disfuncționalităților generate de erori de dezvoltare;
- Asistență consultativă privind utilizarea sistemului;
- Aplicarea de ajustări minore care nu afectează arhitectura aplicației.

Serviciile de suport sunt prestate în termenele prevăzute prin contract, cu respectarea nivelurilor de serviciu stabilite (SLA).

19.9 MECANISME DE MANAGEMENT ȘI COORDONARE

Pentru a asigura implementarea eficientă a obligațiilor contractuale, precum și pentru a controla calitatea serviciilor furnizate, se implementează un sistem de management care include următoarele elemente esențiale:

Constituirea echipei de management al contractului

Furnizorul desemnează o echipă specializată, responsabilă de coordonarea tuturor etapelor de executare a lucrărilor, monitorizarea respectării SLA-urilor, interacțiunea cu Beneficiarul și soluționarea operativă a problemelor apărute.

Întâlniri periodice cu Beneficiarul

Se organizează întâlniri planificate (lunar/trimestrial sau conform unui calendar agreat) pentru analiza rezultatelor curente, evaluarea îndeplinirii indicatorilor de performanță (KPI), discutarea incidentelor și stabilirea pașilor următori.

Menținerea comunicării și ajustarea așteptărilor

Se asigură un schimb continuu de informații bilaterale privind aspectele-cheie ale suportului, precum și alinierea asupra eventualelor modificări legate de volum, termene sau priorități ale serviciilor prestate.

Transparență și responsabilitate

Toate acțiunile sunt documentate, însoțite de rapoarte și disponibile pentru audit. Echipa este responsabilă pentru livrarea serviciilor în timp util, la un nivel calitativ corespunzător și în volum complet.

Îmbunătățirea continuă a proceselor

Managementul se bazează pe principiile îmbunătățirii continue: se analizează metricile și feedbackul, se identifică punctele critice de dezvoltare și se implementează măsuri corective orientate spre creșterea eficienței și a satisfacției Beneficiarului.

19.10.1 GESTIONAREA MODIFICĂRILOR

Gestionarea modificărilor constituie un proces esențial în cadrul metodologiei de mentenanță și suport al sistemelor informatice, având ca obiectiv principal menținerea stabilității operaționale, asigurarea predictibilității rezultatelor și exercitarea unui control riguros asupra tuturor modificărilor aduse componentelor sistemului.

Orice modificare – inclusiv corectarea defectelor, actualizările de software, ajustările de performanță, modificările arhitecturale sau extinderea funcționalităților – este supusă unui proces standardizat, cu trasabilitate completă, derulat conform următoarelor etape operaționale:

- Inițierea RFC (Request for Change): Modificările sunt declanșate prin înregistrarea unei cereri de schimbare (RFC) de către utilizatori finali, personal tehnic sau analiști business. RFC-ul trebuie să conțină descrierea completă a modificării propuse, justificarea acesteia, obiectivele urmărite și o evaluare preliminară a riscurilor asociate.
- Analiza de impact: Se realizează o evaluare tehnică detaliată privind influența modificării asupra arhitecturii sistemului, proceselor de business suportate, interfețelor de integrare, bazelor de date și modulelor învecinate. Analiza include estimări privind efortul de implementare, termenele de execuție și resursele necesare.
- Avizarea și aprobarea: Propunerile de modificare sunt revizuite și validate de către toate părțile interesate relevante (beneficiari, echipe IT, management). Pentru modificările cu impact semnificativ, se poate constitui un CAB (Change Advisory Board) responsabil de decizia finală.
- Planificarea implementării: Se elaborează un plan de implementare structurat, care definește clar pașii operaționali, responsabilitățile, mediile implicate (dev/test/prod), strategia de testare, planul de rollback și, după caz, planul de comunicare a schimbării.
- Testare și validare: Modificările sunt supuse testării funcționale, de integrare și performanță în medii controlate, conform unui plan de testare aprobat.

Implementarea în mediul de producție se autorizează doar după obținerea rezultatelor conforme din faza de testare.

- Documentare și actualizarea configurațiilor: Toate modificările aprobate sunt înregistrate în sistemul de management al configurațiilor (CMS), iar documentația tehnică și operațională este actualizată corespunzător. Se asigură comunicarea modificărilor către utilizatorii afectați prin canalele formale stabilite.
- Review post-implementare (PIR – Post Implementation Review): Se efectuează o analiză retrospectivă pentru a valida dacă obiectivele inițiale au fost atinse, se documentează eventualele deviații și se formulează lecții învățate și recomandări pentru îmbunătățirea proceselor viitoare.

19.10.2 GESTIONAREA RISCURILOR

Gestionarea eficientă a riscurilor reprezintă o componentă critică a metodologiei de mentenanță și suport a proiectelor IT, având ca obiectiv menținerea funcționării stabile, sigure și previzibile a sistemului informațional. În cadrul activităților de suport sunt definite mecanisme formalizate pentru identificarea, evaluarea, controlul și reducerea riscurilor de natură atât tehnică, cât și organizațională.

Măsurile principale pentru gestionarea riscurilor includ:

- Audituri periodice ale sistemului și evaluarea vulnerabilităților: Se derulează evaluări tehnice recurente (evaluări de securitate, scanări de vulnerabilități, revizii de cod) pentru a identifica punctele slabe ale sistemului, neconformitățile față de cerințele de securitate și amenințările care pot afecta disponibilitatea serviciilor.
- Planuri de recuperare în caz de dezastru (DRP – Disaster Recovery Plan): Se dezvoltă, validează și actualizează planuri de restaurare a funcționalității sistemului în situații de avarie majoră, catastrofe sau pierderi de date. Aceste planuri includ testarea copiilor de rezervă, verificarea proceselor de restaurare, comutarea pe infrastructuri de rezervă și proceduri de răspuns în situații de urgență.
- Analiza incidentelor și prevenirea recurenței: Toate incidentele critice sau recurente fac obiectul unei analize post-incident (Root Cause Analysis – RCA), în scopul identificării cauzelor fundamentale, documentării lecțiilor învățate și formulării de măsuri preventive pentru evitarea apariției unor situații similare.
- Implicarea activă a echipei de suport în gestionarea incidentelor de securitate: Echipa de suport colaborează direct cu responsabilii pentru securitatea informației, participând la investigarea incidentelor, implementarea măsurilor corective și asigurarea unui răspuns prompt și coordonat la evenimentele de securitate.

ESCALADAREA RISCURILOR ȘI INCIDENTELOR

În situațiile în care un incident nu poate fi rezolvat în termenul agreat (conform SLA) sau necesită aprobări suplimentare din partea Clientului, se aplică procedura formalizată de escaladare, structurată pe niveluri de suport și criterii de prioritate:

De la linia a doua de suport către linia a treia: Escaladarea are loc în cazul în care incidentul nu poate fi remediat prin mijloace standard sau necesită o analiză tehnică aprofundată din partea specialiștilor de nivel superior.

De la linia a treia către Client sau dezvoltator extern: În cazul în care rezolvarea implică aprobarea unor modificări funcționale sau tehnice, acces la informații confidențiale sau intervenția titularului soluției/aplicației.

Conform priorității și nivelului de serviciu (SLA): Escaladarea se realizează ținând cont de nivelul de criticitate al incidentului și termenii contractuali agreați prin SLA. Toate acțiunile de escaladare sunt documentate în sistemul de management al solicitărilor (ticketing).

Notificarea Clientului și planificarea rezolvării: Pentru incidente care afectează procesele critice de business, se inițiază imediat informarea persoanelor de contact desemnate ale Clientului. Se analizează opțiunile de rezolvare temporară și permanentă, fiind elaborat un plan de acțiune comun și aprobat bilateral.

19.10.3 DISTRIBUIREA ROLURILOR ȘI A ZONELOR DE RESPONSABILITATE

Implementarea eficientă a proceselor de suport și mentenanță a produsului software depinde în mod direct de colaborarea structurată și clar definită între Client și Furnizor. Pentru a asigura transparența, promptitudinea și predictibilitatea activităților, părțile respectă următoarea delimitare a responsabilităților.

Responsabilitățile Furnizorului:

Furnizorul asigură suportul și mentenanța produsului software în conformitate cu prezenta metodologie și cu prevederile contractuale și se angajează să:

- Proceseze solicitările Clientului în concordanță cu nivelurile de serviciu agreate (SLA);
- Asigure informarea promptă și continuă cu privire la stadiul lucrărilor și statusul cererilor;
- Acorde suport Clientului, atunci când este necesar, în clarificarea cerințelor tehnice și a specificațiilor funcționale;
- Evalueze estimativ volumul de lucru și termenul de execuție pentru fiecare solicitare înainte de începerea activităților;
- Escaladeze incidentele sau aspectele care necesită implicarea directă a reprezentanților desemnați ai Clientului;
- Furnizeze rapoarte privind activitățile desfășurate, la o frecvență stabilită de comun acord (ex. săptămânal sau lunar);
- Mențină o comunicare regulată, constructivă și profesională cu reprezentanții Clientului.

Responsabilitățile Clientului:

Clientul, la rândul său, asigură premisele necesare pentru o colaborare eficientă și se angajează să:

- Transmită solicitările și cererile de suport prin canalele stabilite și conform procedurii aprobate;
- Pună la dispoziția Furnizorului informațiile, materialele, accesul la sisteme și alte resurse necesare desfășurării activităților;
- Notifice Furnizorul cu privire la orice modificări semnificative în cadrul proiectelor,
- proceselor de business utilizate sau infrastructurii tehnice;

- Recepționeze lucrările finalizate și să furnizeze feedback, atunci când este cazul;
- Efectueze plata serviciilor prestate de Furnizor în termenele și condițiile prevăzute în contract;
- Mențină o comunicare deschisă, coerentă și constructivă pe parcursul întregii colaborări.

Această distribuție clară a rolurilor și responsabilităților permite implementarea unui model eficient de guvernanță, contribuie la reducerea riscurilor operaționale și asigură exploatarea fiabilă a sistemului informațional.

20 LISTA DE CONFORMITATE CU CERINȚELE (CHECKLIST)

CERINȚELE FUNCȚIONALE (ETAPA 2)

Nr.	Denumirea cerinței (conform TOR)	Detaliile cerintei	Corespunde
1.	Cerințele funcționale ale cazului de utilizare UC01 „Evidența înștiințărilor despre infracțiuni”	Extindere/Integrare: Implementarea mecanismului de preluare automată a datelor pentru formularul R1 din SIA „e-Dosar”. Modul de interacțiune și schimb de date - *Alte sisteme externe*	Conform descrierii p.16
2.	Cerințele funcționale ale cazului de utilizare UC02 „Evidența cauzei penale”	Extindere/Integrare: Implementarea integrării cu sistemul extern PIGD pentru preluarea hotărârilor judecătorești și cu SIA „e-Dosar” pentru recepționarea datelor formularelor F1.0-F6.0. Modul de interacțiune și schimb de date - *Alte sisteme externe*	Conform descrierii p.16
3.	Cerințele funcționale ale cazului de utilizare UC05 “Căutarea interstatală / internațională a persoanelor”	Dezvoltare: Realizarea interoperabilității cu Banca Informațională Interstatală (CSI), ECRIS/ECRIS-TCN (țările UE) și cu partenerii internaționali (Interpol, Europol). Modul de interacțiune și schimb de date - *Căutare interstatală (CSI)* Modul de interacțiune și schimb de date - *Căutare internațională*	Conform descrierii p.16

4.	Cerințele funcționale ale cazului de utilizare UC06 „Conexarea persoanelor (regimul „Tot el”)”	Dezvoltare: Implementarea mecanismului „Tot el” pentru corelarea și unificarea identităților multiple ale persoanelor fizice în FOI și Baza de Date Centrală (CBD). Module de introducere a datelor - *Conexare a persoanelor (regimul „Tot el”)*	Conform descrierii p.16
5.	Cerințele funcționale ale cazului de utilizare UC07 „Registrul de evidență preventivă (evidența persoanelor defavorizate)”	Modul nou: Dezvoltarea registrului de evidență preventivă pentru capturarea persoanelor care reprezintă o amenințare potențială, dar nu sunt implicate în activități infracționale. Module de introducere a datelor - *Modul de Evidență preventivă a persoanelor defavorizate*	Conform descrierii p.16
6.	Cerințele funcționale ale cazului de utilizare UC08 „Căutarea armelor (identificate) pierdute / Evidența și controlul armelor și muniției”	Extindere/Integrare: Implementarea integrării cu sistemul extern RSA (Registrul de Stat al Armelor) pentru înregistrarea armelor furate. Modul de interacțiune și schimb de date - *Alte sisteme externe*	Conform descrierii p.16
7.	Cerințele funcționale ale cazului de utilizare UC14 „Fișierul operativ-informațional al persoanelor care au săvârșit infracțiuni (FOI)”	Modul nou: Implementarea integrală a modulului FOI, incluzând introducerea datelor de pe suport de hârtie, primirea datelor de la PIGD, căutarea, înregistrarea acțiunilor operatorilor și generarea rapoartelor. Modul Fișierul operativ-informațional al persoanelor care au săvârșit infracțiuni (FOI) Modul de interacțiune și schimb de date - *Alte sisteme externe*	Conform descrierii p.16
8.	Cerințele funcționale ale cazului de utilizare UC15 „Căutarea după obiecte și fișe (Z-spravka)”	Modul nou: Dezvoltarea aplicației „Z-spravka” pentru interogări de referință, căutări complexe, construirea arborelui de relații între obiecte și implementarea posibilității de a vizualiza datele șterse. Modul Z-spravka - Căutarea după obiecte și fișe Descriearea detaliata a se vedea in p.16 Modul Z-spravka	Conform descrierii p.16
9.	Cerințele funcționale ale cazului de utilizare UC16	Extindere: Aplicarea tuturor funcționalităților de gestionare a clasificatoarelor/nomenclatoarelor	Conform descrierii p.16

	„Gestionarea clasificatoarelor /nomenclatoarelor”	(creare, editare, export) și pentru clasificatoarele specifice modulului FOI. Module de Serviciu - *Extindere pentru FOI*	
10.	Cerințele funcționale ale cazului de utilizare UC17 „Gestionarea utilizatorilor”	Extindere: Atribuirea de drepturi și roluri speciale, specifice funcționalităților modulului FOI, fără a modifica principiul de gestionare unitară a utilizatorilor la nivelul întregului sistem. Extinderea pentru toate rolurile din etapa 2 Module de Serviciu - *Modul de Gestionare utilizatorilor*	Conform descrierii p.16
11.	Cerințele funcționale ale cazului de utilizare UC18 «Logarea/ Jurnalizarea activităților utilizatorilor»	Funcție nouă: Implementarea mecanismului de jurnalizare (Logare) a tuturor evenimentelor de business critice sau sensibile aferente utilizării regimului FOI și Z-spravka, cu integrare obligatorie prin serviciul guvernamental MLog. Module de Serviciu - *Modul de Jurnalizare*	Conform descrierii p.16
12.	Cerințele funcționale ale cazului de utilizare UC19 «Generarea rapoartelor standard parametrizate»	Modul nou: Dezvoltarea modulului de generare a rapoartelor standard parametrizate (statistice și prestabilite) și a funcționalității de transmitere automată (prin e-mail) a acestora în diverse formate (PDF, DOCX, XML, Excel). Modul Z-spravka - Generarea a rapoartelor standard	Conform descrierii p.16
13.	Cerințele funcționale ale cazului de utilizare UC20 «Crearea unor interogări aleatoriu în baza de date»	Funcție nouă: Crearea unui instrument specializat pentru generarea de rapoarte personalizate (ad-hoc) și interogări aleatorii în baza datelor consolidate din RICC. Modul Z-spravka - Rapoarte personalizate și interogări	Conform descrierii p.16
14.	Cerințele funcționale ale cazului de utilizare UC21 «Gestionarea condițiile logice de validare»	Extindere: Configurarea logicii și regulilor de validare (verificări logice) de către administrator, aplicabile datelor introduse, în special în modulul FOI. Modul de verificare a condițiilor logice Module de Serviciu - *Modul de Gestionare verificărilor logice*	Conform descrierii p.16

15.	Cerințele funcționale ale cazului de utilizare UC22 „Vitrina de date”	Component nou: Dezvoltarea „Vitrinei de date” pentru gestionarea atributelor, obiectelor și referințelor încrucișate (crosslinks), asigurând integrarea datelor din BPD în BDI pentru aplicația „Z-spravka”. Modul Vitrina de Date	Conform descrierii p.16
16.	Cerințele funcționale ale cazului de utilizare UC23 „Secțiuni BD «Statistica penală»”	Funcție nouă: Dezvoltarea funcționalității de creare a „Secțiunilor BD Statistica penală” (copii needitabile lunare) și implementarea mecanismului de transfer al bazei pentru anul următor (PPL/FOND). Baza de Date - Secțiuni BD «Statistica penală»	Conform descrierii p.16
17.	Cerințele funcționale ale cazului de utilizare UC24 „Migrarea datelor” (completă)	Funcție nouă: Migrarea completă a datelor istorice ale obiectelor de informație primară din sistemele vechi în BDI, incluzând validarea, transformarea, gestionarea erorilor și verificarea integrității legăturilor după migrare.	Conform descrierii p.16
18.	Cerințele funcționale ale cazului de utilizare UC25 „Urmărirea motivului ștergerii înregistrărilor în CDB”	Funcție nouă: Urmărirea și înregistrarea motivului pentru ștergerea fiecărei înregistrări din Baza de Date Centrală (CDB), asigurând trasabilitate și acces securizat pentru audit. Module de Serviciu - *Modul de Jurnalizare*	Conform descrierii p.16

FUNCTIONALITATI ADITIONALE PROPUSE

Nr.	Denumirea functionalitatii	Descriere funcțională (Lucrări Etapa 2)
1.	Extinderea integrarii cu sisteme externe Transmiterea datelor din SIA RICC New către RICC existent, din noile formulare care vor fi dezvoltate în Etapa 2.	Conform descrierii p.16
2	Extinderea modulului de administrare Gestionarea parametrilor necesari pentru funcționarea funcționalităților dezvoltate în Etapa 2.	Conform descrierii p.16

CERINȚELE NON-FUNCȚIONALE

Nr.	Denumirea cerinței (conform TOR)	Corespunde (Da/Nu)
A. Cerințe de Licențiere și		

Proprietate Intelectuală		
19.	Cerințe de Licențiere și proprietate intelectuală (CNF.5, CNF.6, CNF.3) (Asigurarea drepturilor de utilizare nelimitată a softului și a licențelor pentru 500 de utilizatori concurenți).	Da, Stiva tehnologică a se vedea in p.9 Licențiere și Proprietate Intelectuală
B. Specificații tehnice și Arhitectura		
20.	Stiva tehnologică (Componentele SI trebuie dezvoltate utilizând limbaje de programare moderne C#, ASP.NET Core, Microsoft SQL Server, Redis, Kubernetes).	Da, Stiva tehnologică a se vedea in p.7 Stiva tehnologică
21.	Cerințe pentru Arhitectura de sistem (Arhitectura trebuie să fie multistrat, orientată pe servicii (SOA), bazată pe standarde deschise și să permită extinderea funcționalităților).	Da, Descrierea detaliata se vedea in p.10 Arhitectura
22.	Cerințe pentru Platforma tehnologică (Arhitectura optimizată pentru rularea în medii Cloud computing (M-Cloud) și independentă de platformă).	Da, Descrierea detaliata se vedea in p.6 Platforma tehnologică
23.	Cerințe generale față de stiva tehnologică a SIA RICC (Sistemul trebuie să suporte formatul Unicode, să fie bazat pe tehnologii deschise și omogene).	Da, Descrierea detaliata se vedea in p.6 Suport pentru Formatul Unicode (UTF-8)
24.	Cerințe de Interoperabilitate (Utilizarea standardelor deschise, interacțiune în timp real și includerea API-urilor pentru integrarea cu MConnect și sisteme externe).	Da, Descrierea detaliata se vedea in p.6 Interoperabilitate
25.	Transformarea și migrarea datelor (Metodologia detaliată pentru transferul și maparea datelor istorice trebuie să fie definită și implementată).	Da, Descrierea detaliata se vedea in p.15 Transformarea și migrarea datelor
C. Operațiune și Performanță		
26.	Cerințele de Performanță (Timpul de răspuns la interogările tranzacționale nu trebuie să depășească	Da,

	3 secunde. Sistemul trebuie să gestioneze până la 500 de sesiuni concurente).	Descrierea detaliata se vedea in p.6 Performanță sistemului
27.	Cerințele pentru Mentenabilitate (Arhitectura să permită implementarea simplistă a schimbărilor cu impact minim și să dețină mecanisme de monitorizare și jurnalizare a erorilor).	Da, Descrierea detaliata se vedea in p.14 Mentenabilitate și ușurință în administrare
28.	Cerințele pentru Scalabilitate (Sistemul să permită creșterea capacității de procesare fără întrerupere, prin scalare orizontală).	Da, Descrierea detaliata se vedea in p.6 Scalabilitate
D. Securitate și Conformitate		
29.	Cerințele pentru Asigurarea securității (Arhitectura concepută prin „Secure by design”, protecție împotriva OWASP top 10, autentificare prin MPASS și autorizare bazată pe principiul „este interzis tot ce nu este explicit permis”).	Da, Descrierea detaliata se vedea in p.12 Asigurarea securității
30.	Cerințele pentru Reziliență și continuitate (Implementarea instrumentelor de *backup* și *gestiune* a copiilor de rezervă; arhitectura să nu dețină puncte singulare de cădere (SPOF)).	Da, Descrierea detaliata se vedea in p.6 Reziliență și continuitate
E. Utilizabilitate și Flexibilitate		
31.	Cerințele pentru Utilizabilitate (Interfețe utilizator prietenoase, intuitive și comode, dezvoltate cel puțin în limba română).	Da, Descrierea detaliata se vedea in p.13 Utilizabilitate
32.	Cerințele pentru Flexibilitate (Sistemul să permită configurarea *vizualizărilor* și *rapoartelor* și *definirea fluxurilor de business* fără modificarea codului sursă).	Da, Descrierea detaliata se vedea in p.6 Flexibilitate
33.	Infrastructura hardware și telecomunicații (Operarea pe platforma guvernamentală MCloud).	Da, Descrierea detaliata se vedea in p.8 Infrastructura hardware și telecomunicații