OFERTĂ TEHNICĂ

pentru achiziția serviciilor de creare a Sistemului informațional „Registrul de Stat VioData”

(SI Registrul de Stat VioData)

Beneficiar:

Agenția Națională de Prevenire și Combatere a Violenței împotriva Femeilor și a Violenței în Familie (ANPCV)

Ofertant:

GHESAR

Chișinău, Republica Moldova

Data depunerii: mai 2026

Versiunea documentului: 1.0

Valabilitatea ofertei: 90 zile calendaristice

GHESAR®

Cuprins

1. Sumar Executiv

Prezenta Ofertă Tehnică este elaborată de GHESAR pentru achiziția serviciilor de creare a Sistemului informațional „Registrul de Stat VioData” (SI RS VioData), conform Caietului de sarcini emis de Agenția Națională de Prevenire și Combatere a Violenței împotriva Femeilor și a Violenței în Familie (ANPCV) și Conceptului aprobat prin Hotărârea Guvernului nr. 530/2025.

GHESAR este o companie cu peste 12 ani de experiență în dezvoltarea de soluții guvernamentale și de Registre de Stat în Republica Moldova, având implementate cu succes sisteme informaționale guvernamentale, dintre care majoritatea sunt integrate cu platforma MConnect și serviciile guvernamentale comune (MPass, MSign, MNotify, MLog). Echipa noastră dedicată proiectului numără 19 specialiști, care depășesc cumulativ cerințele minime ale caietului de sarcini.

Înțelegem că SI RS VioData este o componentă critică a mecanismului național de protecție a victimelor violenței bazate pe gen și violenței în familie. Sistemul va fi utilizat de profesioniști din mai multe sectoare (asistență socială, sănătate, ordine publică, justiție) și va prelucra date sensibile cu caracter personal cu cel mai înalt nivel de confidențialitate. Prin urmare, abordarea noastră este centrată pe trei axe fundamentale: (i) securitate și conformitate juridică (GDPR, HG 1123/2010, HG 201/2017, ISO/IEC 27001), (ii) interoperabilitate funcțională cu ecosistemul digital guvernamental (eGov4Dev, MConnect, MPass, MSign, MNotify, MLog), și (iii) ușurința utilizării de către specialiștii din teren, multe dintre cazuri fiind gestionate în condiții de urgență.

Propunem o metodologie hibridă – etapizată conform Conceptului SI „VioData”, cu livrări iterative Agile (Scrum cu sprint-uri de 2 săptămâni) – care asigură atât controlul riguros al livrabilelor contractuale, cât și flexibilitatea necesară pentru adaptarea iterativă la feedback-ul utilizatorilor. Durata totală propusă este de 17 luni pentru Etapele I-V, urmate de 12 luni de garanție și mentenanță (Etapa VI), conform cerințelor caietului de sarcini.

Stackul tehnologic propus respectă integral recomandările din capitolul 6.1 al caietului de sarcini: ASP.NET Core 8.0 (backend), MudBlazor, Svelte sau Angular (frontend), PostgreSQL 16 (date relaționale), Redis (caching), Elasticsearch + Kibana (loguri), Prometheus + Grafana (monitorizare), Docker + Kubernetes + Helm (orchestrare), Azure DevOps (CI/CD). Toate componentele vor fi găzduite pe Mcloud cu recomandări de administrare.

Documentul prezent detaliază calea, metodele și instrumentele care vor fi utilizate pentru proiectarea, dezvoltarea, integrarea, testarea, pilotarea, lansarea și mentenanța SI RS VioData, asigurând conformitatea cu toate cerințele funcționale și non-funcționale obligatorii. Planul de Proiect detaliat, livrat ca document separat, descrie cronologia, livrabilele și estimarea efortului pe etape.

2. Înțelegerea Contextului și a Obiectivelor

2.1. Contextul național

Republica Moldova depune eforturi sistematice pentru consolidarea mecanismului național de prevenire și combatere a violenței împotriva femeilor și a violenței în familie, conform Legii nr. 45/2007, Programului Național 2023-2027 și a obligațiilor asumate prin Convenția de la Istanbul - https://www.coe.int/ro/web/chisinau/10-years-of-the-istanbul-convention. Fragmentarea actuală a evidenței cazurilor între MAI/IGP, MMPS/ATAS, MS, MJ și CNAJGS îngreunează intervenția integrată centrată pe victimă, monitorizarea longitudinală a cazurilor și fundamentarea politicilor publice pe baza datelor.

Implementarea SI RS VioData reprezintă răspunsul instituțional la această fragmentare cu o platformă centralizată, interoperabilă cu sistemele sectoriale, care va asigura colectarea standardizată a datelor, gestionarea sigură a cazurilor și raportarea integrată, cu respectarea strictă a cadrului normativ privind protecția datelor cu caracter personal.

2.2. Obiectivele asumate

Conform caietului de sarcini, înțelegem că proiectul urmărește patru obiective strategice:

1. Îmbunătățirea colectării datelor – standardizarea formularelor, dezagregarea pe sex/vârstă/tip violență/mediu, audit periodic al calității datelor, eliminarea duplicatelor după caz automat dacă trece de un sistem riguros de filtrare și contrapunere unde sistemul este 100% sigura ca cazurile sunt identice, daca există o mică probabiltate precum că cazurile sunt diferite aceasta trece spre aprobarea manuală a operatorului.
2. Asigurarea confidențialității – criptare TLS 1.3 în tranzit și AES-256 în stocare, autentificare prin MPass, RBAC granular pe roluri și module, consimțământ explicit, jurnalizare completă MLog.
3. Coordonarea interinstituțională – integrare prin MConnect cu sisteme medicale, sociale, de ordine publică și justiție; notificare automată prin MNotify la schimbarea stării cazurilor sau emiterea măsurilor de protecție.
4. Sprijinirea procesului decizional – tablouri de bord interactive, indicatori naționali calculați automat, exporturi PDF/CSV/Excel, integrare cu sistem extern de analiză a rețelelor sociale pentru cazurile de violență online.

2.3. Părțile interesate și rolurile lor

Identificăm următoarele categorii de stakeholderi la etapa de ofertare cu care vom desfășura consultări structurate în Etapa I:

Categorie	Stakeholder	Rol în proiect
Deținător	ANPCV	Coordonare strategică, recepția livrabilelor

Furnizori de date	MAI/IGP, MMPS/ATAS, MS, MJ, CNAJGS	Surse primare, validare specificații, integrări sectoriale
Reglementator date	Agenția de Guvernare Electronică (AGE)	Integrări guvernamentale
Reglementator tehnic	STISC Serviciul Tehnologia Informației și Securitate Cibernetică	Găzduire MCloud,
Utilizatori finali	Manageri de caz, asistenți sociali, polițiști, medici, juriști	Validare UX, feedback pilotare, instruire
Furnizori specializați	ONG-uri, adăposturi, centre de consiliere	Validare fluxuri de referire, scenarii operaționale
DPO și autoritate	Centrul Național pentru Protecția Datelor cu Caracter Personal	Validare DPIA, controlul măsurilor de protecție a datelor

3. Profilul Companiei Ofertante

3.1. Date generale

Denumire legală	GHESAR
Forma juridică	Societate cu Răspundere Limitată, înregistrată în Republica Moldova
IDNO	1014600034005
Sediul social	Meșterul Manole7, Oficiul 9, Chișinău, Republica Moldova
Domeniu de activitate	Dezvoltare software, sisteme informaționale guvernamentale, integrare API, consultanță IT
Anul înființării	2014
Personal total	25 specialiști IT (dezvoltatori, arhitecți, QA, UX/UI, DevOps, BA, PM)
Certificări corporative	ISO/IEC 27001:2022 (managementul securității informației), ISO 9001:2015 (calitate), ISO/IEC 20000-1 (management servicii IT), ISO 14001
Acreditări guvernamentale	Scrisori de recomandare din partea MAI, STISC, MFA, etc.

3.2. Conformitatea cu cerințele privind ofertantul

Demonstrăm îndeplinirea cumulativă a tuturor cerințelor minime din capitolul 7 al caietului de sarcini:

Cerință minimă (Caiet de sarcini)	Modul de îndeplinire
Persoană juridică înregistrată legal cu drept de activitate IT	SRL înregistrat în RM, certificat de înregistrare disponibil; cod CAEM 6201, 6202, 6209
Minimum 5 ani experiență în dezvoltare software	12 ani de activitate continuă (2014–2026)
Minimum 3 proiecte relevante în ultimii 3 ani	7 proiecte guvernamentale relevante implementate în 2023-2026; 3 dintre ele detaliate la pct. 3.3
Capacitatea de suport post-implementare, mentenanță, evoluție	Departament dedicat de suport (12 specialiști), SLA 24/7 disponibil, contracte active de mentenanță cu 9 instituții publice

3.3. Proiecte relevante (extras din portofoliu)

Proiect 1 — Elaborarea sistemului informațional automatizat „Registrul Patrimoniului Public”.

Beneficiar	Agenția Proprietății Publice
Perioadă	2021–2026, Dezvoltarea Anuală
Integrări	MPass, MSign, MConnect
Volum date	Patrimoniul Național, 99,99% disponibilitate
Relevanță VioData	Management dosare, RBAC, conformitate GDPR

Proiect 2 — Servicii de asistență, dezvoltare și mentenanță a sistemelor informaționale existente din cadrul DAC al MAEIE (SIA Consul, SIAGV)

Beneficiar	Ministerul Afacerilor Externe și Integrării Europene
Perioadă	2019–2026 Dezvoltarea Anuală
Stack	ASP.NET Core 8, .Net, MSSQL pe MCloud
Integrări	MPass (autentificare), MSign (semnare documente medicale), MConnect (RSP, IGP, IGM)
Volum date	Sutem de mii înregistrări dosare documente Naționale, dosare Vize electronice, certificat de securitate cibernetică AGE
Relevanță VioData	Date sensibile de vize, audit complet, integrare cu sisteme de Stat

Proiect 3 — Mentenanță și dezvoltare a Sistemului Informațional Automatizat „e-Cazier”

Beneficiar	Ministerul Afacerilor Interne
Perioadă	2023–2026
Stack	ASP.NET Core 7, Java pe MCloud
Integrări	MPass, MSign, MConnect (cu RSP, MDelivery, Msign, Mpass, sisteme externe judiciare)
Relevanță VioData	Gestionarea receptia si prelucrarea cazierelor judiciare, care pot fi tratate similar un caz/Dosar din VioData

Proiect 4 — Achiziționarea serviciilor de mentenanță și dezvoltare a Sistemului Informațional Automatizat „REC” Sistemului infromaţional automatizat de evidenţă a contravenţiilor, cauzelor contravenţionale, a persoanelor care le-au săvârșit și punctelor de penalizare

Beneficiar	Ministerul Afacerilor Interne
Perioadă	2023–2026
Stack	ASP.NET Core pe MCloud
Integrări	MPass, MSign, e-Data, Sisteme interne MAI, Registre guvernamentale (prin MConnect), Sisteme financiare / sancțiuni.

Relevanță VioData	Proiectul **REC (Registrul de evidență a contravențiilor)** prezintă o relevanță directă pentru implementarea și operarea sistemului VioData, în special prin continuitatea proceselor operaționale dintre gestionarea incidentelor și formalizarea acestora în cadrul procedurilor contravenționale.
	1. Continuitatea procesului operațional (end-to-end)
	În cadrul VioData:
	• este creat **cazul de incident** (violență în familie)
	• se colectează datele inițiale (persoane, locație, circumstanțe)
	Relevanță REC:
	• cazul din VioData poate genera **automat un caz administrativ** în REC
	• în REC se:
	  ○ creează **procesul-verbal contravențional**
	  ○ se inițiază procedura juridică
	Aceasta demonstrează capacitatea de:
	• integrare între sisteme operaționale și juridice
	• automatizare a fluxurilor instituționale

Proiect 5 — Mentenanță și dezvoltare a Sistemului Informațional Automatizat ”Registrul de Stat al Accidentelor Rutiere” (SIA RAR)

Beneficiar	Ministerul Afacerilor Interne
Perioadă	2023–2026
Stack	ASP.NET Core pe MCloud
Integrări	MPass, MSign, e-Data, Sisteme interne MAI, Registre guvernamentale (prin MConnect), Sisteme financiare / sancțiuni.
Caracteristici tehnice	Geo-tagging GPS, din portalul de crearea cazului de accident

Relevanță VioData	Proiectul **SIA RAR (Registrul de Stat al Accidentelor Rutiere)** demonstrează capacități tehnice și operaționale direct aplicabile în dezvoltarea și mentenanța sistemului VioData, prin următoarele dimensiuni: **1. Integrare cu ecosistemul guvernamental** SIA RAR este integrat cu: • **MPass** • **MSign** • **MConnect** • e-Data și sisteme interne MAI Relevanță pentru VioData: • VioData necesită exact același tip de interoperabilitate • reutilizare modele de integrare, securitate și schimb de date

4. Echipa de Proiect

Echipa propusă pentru SI RS VioData este formată din 11 specialiști cu experiență dovedită în proiecte guvernamentale similare, depășind cumulativ cerințele minime ale capitolului 7 din Caietul de sarcini. Toți membrii echipei sunt angajați full-time ai GHESAR și nu sunt dependenți de subcontractare critică pentru rolurile cheie.

4.1. Componența echipei și conformitatea cu cerințele

Rol	Cerință caiet	Profil propus (anonimizat)
Manager de Proiect (1)	Studii sup., 5+ ani IT, 3+ proiecte coordonate, metodologii PM	Management IT; 11 ani experiență; 6 proiecte guvernamentale; certificat PMP + PRINCE2 + Scrum Master PSM-II
Business Analyst (1)	Studii sup., 5+ ani BA, cerințe funcționale, use-case, BPMN	Sisteme Informatice; 8 ani BA; certificat IIBA CBAP; experiență REAS și 2 registre de stat; cunoștințe HG 530/2025
Arhitect IT (1)	Studii sup. IT, 5+ ani, 3+ ani arhitect, sisteme distribuite, API/microservicii	Computer Science; 25 ani; 6 ani arhitect; arhitect lead REAS și PNRISP;
Dezvoltatori Backend (3)	4+ ani, ASP.NET Core, EF Core, RDBMS/NoSQL, securitate	Toți cu 6-9 ani experiență .NET; expertiză MudBlazor, ASP.NET Core 8, Angular, EF Core, PostgreSQL, integrări MConnect;
Dezvoltatori Frontend (2)	3+ ani, framework-uri moderne, integrare API, accesibilitate	5-7 ani experiență Blazor/MudBlazor/Angular/VueJs,

		conformitate WCAG 2.1 AA, MUD (Modelul Unitar de Design)
Specialist UX/UI (1)	3+ ani, wireframes, prototipuri, design funcțional	6 ani UX/UI; certificat NN/g UX; experiență design pentru utilizatori vulnerabili (trauma-informed UX); aplicare MUD
Specialist QA / Testare (1)	3+ ani, testare funcțională, regresie, acceptanță	7 ani QA; experiență testare integrări MConnect, automatizare cu Playwright/xUnit
DevOps Engineer (1)*	Rol suplimentar dedicat – nu cerut explicit	8 ani DevOps; expertiză Kubernetes, Helm, Azure DevOps, Docker, Prometheus/Grafana;
Specialist Securitate Cibernetică (1)*	Rol suplimentar dedicat – pentru DPIA și pen-testing	9 ani securitate; certificat CISSP + CEH; experiență ISO 27001, OWASP, conformitate HG 201/2017

** Specialiști suplimentari neceruți obligatoriu de Caietul de sarcini, dar pe care îi includem ca diferențiator de calitate, având în vedere natura sensibilă a datelor și complexitatea integrărilor.*

4.2. Continuitatea echipei

Asumăm ferm angajamentul ca toți membrii echipei nominalizate să fie disponibili pentru proiect pe toată durata contractuală. Pentru orice situație de indisponibilitate temporară (concedii, deplasări, situații medicale), avem o rezervă internă de specialiști seniori cu calificări echivalente, asigurând înlocuirea fără impact asupra cronogramei. Substituirile vor fi notificate Beneficiarului cu cel puțin 5 zile lucrătoare înainte și aprobate de comun acord. CV-urile detaliate ale tuturor membrilor echipei vor fi prezentate la cerere.

5. Înțelegerea Cerințelor și Domeniul de Aplicare

5.1. Trasabilitatea cerințelor, matrice Concept, Caiet, Implementare

Pentru a asigura conformitatea integrală cu toate cerințele obligatorii, propunem elaborarea (în Etapa I) a unei Matrici de Trasabilitate Concept–Cerință–Use-case–Test, care va corela:

- fiecare cerință funcțională din capitolele 5.1–5.13 ale Caietului de sarcini
- cu prevederile Conceptului SI „VioData" aprobat prin HG 530/2025
- cu cele 9 scenarii operaționale (SO-01 – SO-09)
- cu cazurile de utilizare detaliate, criteriile de acceptanță și testele aferente
- cu livrabilul în care va fi implementată

Această matrice constituie instrumentul-cheie pentru recepția livrabilelor: nicio cerință obligatorie nu poate fi considerată finalizată fără referință univocă în matrice, criteriu de acceptanță bifat și raport de test atașat.

5.2. Domeniul de aplicare – module funcționale acoperite

SI RS VioData va include cele 9 conturi funcționale obligatorii prevăzute în Caietul de sarcini, fiecare implementat ca modul independent dar interconectat:

Cod	Contur funcțional	Componente principale
M1	**Administrare**	Gestionare utilizatori și roluri (RBAC), administrare baze de date, configurare interfață, audit, jurnalizare prin MLog
M2	**Managementul raportării cazurilor**	Înregistrare caz, formular standardizat, validare câmpuri, ID unic, instituție raportoare, consimțământ, fișa cazului online cu link postare
M3	**Urmărirea cazurilor**	Stări caz (deschis/în desfășurare/referit/închis/respins/inactiv), tranziții controlate, evaluare risc și letalitate, plan de intervenție
M4	**Urmărirea referirilor**	Referiri către servicii medicale/juridice/sociale/adăposturi, istoric complet, schimb de date prin MConnect (sincron + Events asincron)
M5	**Caz de violență**	Evidența plângerilor, sesizărilor, autodenunțurilor; corelare cu măsuri de protecție și hotărâri judecătorești
M6	**Evidența măsurilor de protecție**	Ordine de restricție de urgență, ordonanțe judecătorești, alerte expirare, blocare închidere caz cu măsuri active
M7	**Raportare și analiză**	Tablouri de bord interactive, indicatori naționali, rapoarte personalizate, export PDF/CSV/Excel, integrare analiză rețele sociale

M8	**Acces autorizat și interfață publică**	Autentificare exclusiv prin MPass, RBAC, separare strictă date publice/confidențiale, conformitate portal unic guvernamental
M9	**Gestionarea nomenclatoarelor**	Crearea/modificarea/dezactivarea nomenclatoarelor fără intervenție tehnică, versionare istorică, validare câmpuri

5.3. Obiectele informaționale gestionate

Modelul de date va fi proiectat în jurul celor 14 obiecte informaționale obligatorii (Cazul de violență, Victima, Agresor, Incident, Evaluare risc, Plan de intervenție, Referire, Serviciu furnizat, Raport/indicator, Document, Utilizator, Rol/permisiune, Nomenclator/clasificator, Înregistrare audit). Fiecare obiect va avea: identificator unic UUID v7 (timestamp + random number), versionare istorică imutabilă, asociere cu identificator național (IDNP) acolo unde este permis legal, jurnalizare completă a operațiunilor (CRUD), control acces granular pe rol și atribut, validare integritate referențială tehnică.

6. Metodologia de Dezvoltare – Calea Propusă

Caietul de sarcini impune o abordare hibridă: structură etapizată conform Conceptului HG 530/2025, combinată cu livrări iterative și incrementale Agile. Adoptăm exact această abordare, structurată pe trei niveluri:

6.1. Nivelul strategic – structura etapizată (Waterfall)

Pe nivelul strategic, derulăm proiectul în 6 etape contractuale obligatorii (I-VI), fiecare cu livrabile clar definite, criterii de acceptanță și recepție formală de către Beneficiar. Etapele I-V se execută în 17 luni (analiza detaliată, proiectare, dezvoltare, testare-pilotare, lansare-recepție), iar Etapa VI (garanție) se desfășoară pe 12 luni post-lansare.

6.2. Nivelul tactic – livrări incrementale (Agile/Scrum)

În cadrul Etapei III (Dezvoltare și Integrare) — etapa cu cea mai mare durată și complexitate — folosim cadrul Scrum cu sprint-uri de 2 săptămâni. La finalul fiecărui sprint livrăm un increment de produs demonstrabil (Definition of Done atins), permițând Beneficiarului să vadă progresul real, să dea feedback timpuriu și să prioritizeze backlog-ul. Modulele M1-M9 sunt dezvoltate într-o ordine prioritizată care maximizează valoarea timpurie:

5. Sprint 1-2: M1 Administrare (fundație — utilizatori, RBAC, MPass)
6. Sprint 3-5: M2 + M3 (managementul raportării și urmărirea cazurilor)
7. Sprint 6-7: M9 Nomenclatoare (cross-cutting), M5 Caz de violență
8. Sprint 8-9: M4 Referiri + M6 Măsuri de protecție (cu integrări MConnect)
9. Sprint 10-11: M7 Raportare și analiză + integrare analiză rețele sociale
10. Sprint 12-13: M8 finalizat, integrări complete MNotify, MSign, MLog; refinări

Această ordonare permite începerea testărilor de integrare cu MPass deja din Sprint 2, iar prima demo pentru Beneficiar la finalul Sprint 4 (luna 4 a proiectului).

6.3. Nivelul operațional – practici inginerești (DevSecOps)

La nivel operațional aplicăm un set integrat de practici DevSecOps care garantează calitatea continuă:

- Trunk-based development cu branch-uri scurte (max 2 zile) și pull request review obligatoriu (cel puțin 1 reviewer senior)
- Continuous Integration: la fiecare commit se rulează automat build, unit tests (țintă: ≥80% coverage), integration tests, static analysis (SonarQube), security scan (Trivy pe imagini, OWASP Dependency Check, Snyk pe pachete .NET și NPM)
- Continuous Delivery: pipeline-uri Azure DevOps care promovează automat în Dev → QA → Staging → Pilot → Production, cu aprobări manuale la trecerea spre Pilot și Production

- Infrastructure as Code: toate resursele MCloud (Kubernetes, Helm charts, ConfigMaps, Secrets cifrate cu SOPS/age) sunt versionate în Git
- Test-Driven Development pentru regulile de business critice (validări, tranziții stări, calculul indicatorilor)
- Code review etic: orice modificare care atinge fluxul de date personale ale victimelor este review-uită suplimentar de Specialistul Securitate
- Definition of Done: cod review-uit, teste verzi, securitate verificată, documentație actualizată, demo-uită Product Ownerului ANPCV

6.4. Ceremonii și instrumente de management

Ceremonie	Frecvență	Participanți	Obiectiv
Sprint Planning	Bisăptămânal	Echipa tehnică + PM + PO ANPCV	Selectare items din backlog, estimare
Daily Stand-up intern	Zilnic, 15 min	Echipa tehnică	Sincronizare, identificare blocaje
Sprint Review/Demo cu participarea Beneficiarului	La finalul fiecărui sprint	Echipa + PO + stakeholderi	Validare incrementală a livrărilor
Sprint Retrospective	La finalul fiecărui sprint	Echipa internă	Îmbunătățire continuă
Steering Committee	Lunar	PM + Director ANPCV + AGE	Decizii strategice, escaladări, KPI
Recepție etapă	La finalul fiecărei etape	Comisia de recepție ANPCV	Acceptanță formală a livrabilelor

Instrumente: Azure DevOps Boards (backlog, sprint, taskuri); Gitea, GitLab, Azure DevOps Repos (Git); Azure DevOps Pipelines (CI/CD); Confluence (documentație colaborativă); MS Teams (comunicare zilnică). Instrumentele selectate de nivel de corporatie vor fi selectate împreună cu Beneficiarul pentru a acorda comoditate.

7. Arhitectura Tehnică Propusă

7.1. Principii arhitecturale

Arhitectura SI RS VioData este construită pe șapte principii fundamentale, derivate din cerințele Caietului de sarcini, prevederile eGov4Dev și bunele practici industriale:

11. Modularitate – fiecare contur funcțional (M1-M9) este implementat ca modul independent, cu interfață clar definită, înlocuibil sau actualizabil fără reproiectarea altor module.
12. Domain-Driven Design (DDD) – modelul de domeniu reflectă obiectele informaționale obligatorii și regulile de business reale; bounded contexts pentru fiecare modul.
13. Once-only – datele sunt colectate o singură dată din sursa primară; reutilizarea lor se face exclusiv prin MConnect.
14. Defense in depth – securitate aplicată stratificat: rețea, aplicație, date, identitate, audit.
15. Privacy by design – minimizarea datelor, pseudonimizare, drepturi GDPR implementate nativ; DPIA elaborat înainte de Etapa II.
16. Observabilitate – logging structurat (JSON), metrici Prometheus, distributed tracing (OpenTelemetry), corelare prin trace ID.
17. Conformitate eGov4Dev – aplicarea integrală a recomandărilor de pe https://egov-moldova.github.io/egov4dev/, inclusiv Modelul Unitar de Design (MUD).

7.2. Arhitectura logică pe straturi

Conform capitolului 5 al caietului, sistemul respectă arhitectura pe straturi (UI – Application – Data – Integration – Security – Deployment) și o îmbogățește prin separarea în patru straturi logice și un strat transversal de securitate:

Strat	Componente principale	Tehnologii
Prezentare (UI)	Aplicație web responsive (320–1600px), MUD, WCAG 2.1 nivel A+, multilingv (RO/RU/EN), interfață publică separată	Blazor + MudBlazor 6.x, .NET 8, Angular
Aplicație	Servicii REST (OpenAPI/Swagger), reguli de business, validare (FluentValidation), state machine pentru ciclu de viață caz, BFF (Backend for Frontend)	ASP.NET Core 8, MediatR (CQRS), FluentValidation, Hangfire (joburi în fundal), GoLang, Rust.
Domeniu	Modele de domeniu pe DDD, agregate (Caz, Victima,	.NET 8, MediatR Notifications, MassTransit pentru evenimente

	Agresor, etc.), evenimente de domeniu, politici	
Date	Persistență relațională, indexare full-text, geo-spațial, cache, search distribuit, arhivă imutabilă	PostgreSQL 16 + PostGIS, Entity Framework Core 8, Redis, Elasticsearch
Integrare	Adaptoare către MPass, MSign, MNotify, MLog, MConnect (sincron + Events asincron); analiză rețele sociale	.NET HttpClient, IdentityServer4 (relying party), MassTransit + RabbitMQ, Polly (retry/circuit breaker)
Securitate (transversal)	Autentificare federată MPass, RBAC granular, autorizare bazată pe atribute (ABAC), criptare în repaus și tranzit, audit MLog	Microsoft.AspNetCore.Authentication.OpenIdConnect, OpenPolicyAgent (opțional pentru ABAC) conform Ghidului de Integrarea MPASS prezentat de AGE
Implementare	Containerizare, orchestrare, IaC, observabilitate, DR/BCP	Docker, Kubernetes, Helm, Azure DevOps Pipelines, Prometheus + Grafana, Elasticsearch + Kibana

7.3. Diagrama logică (descriere textuală)

Diagrama de arhitectură va fi livrată în Documentul de Proiectare a Sistemului (Etapa II) ca diagramă C4 (Context, Container, Component, Code). Componentele principale ale sistemului:

- Reverse Proxy / API Gateway (Traefik sau NGINX) – terminare TLS 1.3, rate limiting, mTLS pentru servicii interne
- Aplicația Web Frontend – Blazor WASM servită din Kubernetes ca SPA
- API VioData Core – ASP.NET Core, expune endpoints REST, gestionează modulele M1-M9
- Serviciu Integrări – adaptoare separate pentru fiecare integrare guvernamentală, deployabile independent
- Serviciu Notificări – consumă evenimente de domeniu și emite notificări către MNotify
- Serviciu Raportare – pre-agregare offline, generare PDF/CSV/Excel, expunere endpoint pentru tablouri de bord
- Bază de date primară (PostgreSQL 16) – stocare relațională, replicare master/standby, backup zilnic
- Cache (Redis Cluster) – session store, caching obiecte de domeniu rar modificate (nomenclatoare)
- Elasticsearch + Kibana – căutare full-text în cazuri, vizualizare loguri operaționale
- Message broker (RabbitMQ) – pentru fluxuri asincrone interne în cazul în care volumul de date este mare și este jutificată implementarea acestia.

- Archive Store Min.io (S3-compatibil pe MCloud) – stocare imutabilă pentru documente, evidențe, exporturi

7.4. Multi-tenancy și separarea de medii

Conform cap. 6.2 al caietului, vom configura cel puțin două medii izolate pe MCloud:

- Mediul de dezvoltare/QA – include Dev, QA și Staging; date sintetice; acces echipa tehnică
- Mediul de producție – inclusiv un sub-mediu Pilot izolat de Producția națională, ambele cu date reale; acces controlat MPass

Toate mediile rulează în clustere Kubernetes separate DEV/PROD, cu Network Policies stricte. Promovarea între medii se face exclusiv prin pipeline-uri Azure DevOps sau DevOps SelfHosted cu aprobări multinivel.

8. Stack Tehnologic

Selecția tehnologiilor respectă integral recomandările cap. 6.1 al Caietului de sarcini, optând pentru tehnologii open-source sau cu licență permisivă, cu suport comunitar matur și prezență stabilă pe ecosistemul guvernamental MD.

Categorie	Tehnologie aleasă	Justificare
Frontend framework	Blazor WebAssembly + MudBlazor 6.x	Recomandat explicit în caiet; permite reutilizare cod C# între FE și BE;
Backend framework	ASP.NET Core 8.0 (LTS)	LTS până 2026, performanță, securitate, suport Microsoft
ORM	Entity Framework Core 8	Recomandat în caiet; migrații versionate; suport tranzacții
Validare	FluentValidation 11	Recomandat în caiet; reguli declarative, testabile
Documentație API	Swashbuckle (OpenAPI 3.1)	Recomandat în caiet; standard industrial
Bază de date principală	PostgreSQL 16 cu PostGIS	Recomandat în caiet; open-source; suport geo-spațial pentru geo-tagging GPS (cap. 6.4)
Cache distribuit	Redis 7 (Cluster)	Recomandat în caiet; SLA performanță (latență ≤50ms intra-sistem)
Search & log analytics	Elasticsearch 8 + Kibana 8	Recomandat în caiet; full-text RO/RU/EN; vizualizare loguri
Monitorizare/metrici	Prometheus + Grafana	Recomandat în caiet; alerting; SLI/SLO tracking
Containerizare	Docker	Recomandat în caiet; portabilitate medii
Orchestrare	Kubernetes + Helm	Recomandat în caiet; auto-scaling pentru ≥1000 utilizatori simultani
CI/CD	Azure DevOps + GitLab/Gitea OpenSource (mirror)	Recomandat în caiet; integrare cu Microsoft Identity, Boards, Pipelines
Mesagerie internă	RabbitMQ + MassTransit	Decuplare evenimente; pattern outbox pentru consistență

Background jobs	Hangfire	Joburi recurente (rapoarte, sincronizări, alerte expirare)
Hărți / geolocație	OpenStreetMap (Leaflet) + HTML5 Geolocation API	Recomandat în caiet; opțiune privacy-friendly fără dependență cloud public
Generare PDF	QuestPDF (open-source, comercial gratuit pentru entități publice)	Conform MUD; rapoarte standard; suport multilingv
Generare Excel	ClosedXML / EPPlus (LGPL)	Export rapoarte și liste cazuri

Toate componentele open-source vor fi livrate cu codul sursă și documentația (cap. 8 — predarea codului sursă). Licențele tuturor componentelor sunt verificate ca fiind compatibile cu utilizarea guvernamentală (MIT, Apache 2.0, BSD, MPL 2.0, LGPL).

9. Strategia de Integrare cu Servicii și Sisteme Guvernamentale

Integrările reprezintă coloana vertebrală a SI RS VioData – fără ele, sistemul nu și-ar atinge obiectivele de coordonare interinstituțională. Strategia noastră este structurată pe 5 axe de integrare, fiecare cu metodă proprie, scenariile aferente și criteriile de validare.

9.1. Principii generale de integrare

- Once-only: orice dată deținută primar de un alt sistem (de ex.:. identitatea cetățeanului în Registrul de Stat al Populației) NU este reintrodusă manual în VioData – ea este preluată prin MConnect.
- Point-to-point interzis: schimburile de date interinstituționale se desfășoară EXCLUSIV prin platformele guvernamentale (MConnect pentru date, MConnect Events pentru notificări asincrone).
- Fail-safe: orice indisponibilitate a unui serviciu extern este detectată, jurnalizată, notificată și nu blochează funcționarea critică a VioData (cu fallback procedurale).
- Trasabilitate end-to-end: fiecare apel între sisteme are corelation ID propagat și este jurnalizat în MLog.
- Documentare API: toate API-urile sunt documentate OpenAPI 3.1, versionate semantic (semver) și păstrează compatibilitate inversă pentru cel puțin o versiune.

9.2. Integrări cu serviciile guvernamentale comune

9.2.1. MPass – autentificare și autorizare

Metodă: OAuth 2.0 + OpenID Connect (OIDC) Authorization Code Flow cu PKCE pentru aplicația Blazor WASM, refresh token pentru sesiuni lungi. Implementarea folosește Microsoft.AspNetCore.Authentication.OpenIdConnect, configurat conform ghidului eGov4Dev pentru MPass. Rolurile sistemului VioData sunt mapate pe claim-urile MPass (preluare automată), iar drepturile granulare sunt aplicate intern în VioData (RBAC). Logout federat este implementat conform OIDC RP-Initiated Logout.

Scenarii: autentificare standard, single sign-on între aplicațiile guvernamentale, sesiune expirată cu reluare automată, schimbare rol, conturi ne-MPass blocate.

9.2.2. MSign – semnătură electronică calificată

Metodă: API REST MSign integrat în fluxurile aplicative pentru semnarea documentelor de ieșire (rapoarte, decizii, fișe de referire) și a documentelor formale interne. Fluxul folosește redirecționare către MSign cu pachet PDF/XML (XAdES/PAdES), validare semnătură la întoarcere, stocare semnătură detașată sau încorporată. Vom implementa biblioteca de validare locală pentru verificarea semnăturilor primite din alte sisteme.

Scenarii: semnare ordin/raport oficial; semnare formular consimțământ digital; semnare proces-verbal de recepție internă.

9.2.3. MNotify – notificări electronice

Metodă: API REST MNotify integrat printr-un microserviciu propriu de Notificări, care consumă evenimente de domeniu emise de modulele M2-M6 și transformă în mesaje MNotify (email, SMS, mesaj în portal). Șabloanele sunt configurabile prin nomenclator (M9), multilingve (RO/RU/EN) și conțin doar identificatori de caz – fără date personale sensibile în mesaj.

Scenarii: notificare la schimbarea stării cazului către manageri și instituții implicate; alertă expirare ordin de restricție / ordonanță de protecție; alertă risc letal ridicat; confirmare referire transmisă; confirmare consimțământ înregistrat.

9.2.4. MLog – jurnalizare guvernamentală

Metodă: middleware ASP.NET Core care interceptează toate operațiunile relevante (autentificări, accesări date, modificări, ștergeri logice, operațiuni administrative, schimbări de stare, accesări obiecte personale) și emite înregistrări structurate către MLog prin API REST. Local păstrăm o copie cu Elasticsearch pentru analize operaționale, dar sursa de adevăr legală este MLog.

Câmpuri: identificator utilizator, timestamp ISO 8601, tip acțiune, obiect afectat, IP sursă, user agent, modul, corelation ID, severitate. Filtrare și export disponibile direct din interfață pentru utilizatori autorizați.

9.2.5. MConnect – platforma de interoperabilitate

Metodă: integrare oficială ca participant la MConnect (publicare servicii și consum servicii). Folosim atât canalul sincron (request/response) cât și componenta MConnect Events pentru fluxuri asincrone (publish/subscribe), conform cap. 5.5.2.1 al caietului. Implementăm un adaptor MConnect Client (.NET) care abstractizează complexitatea protocolului și expune servicii REST interne curate către modulele de business.

9.3. Integrări sectoriale prin MConnect

Sector	Sistem-țintă (orientativ)	Date schimbate	Sens / mod
Identitate	RSP – Registrul de Stat al Populației	Date IDNP, nume, naștere, domiciliu (în limita legală)	Consum / sincron
Sănătate	AIS, sisteme spitalicești	Referiri către spital, examinare medico-legală, asistență medicală oferită	Bidirecțional / sincron + Events
Ordine publică	RIA / sisteme MAI-IGP	Ordine de restricție de urgență, statut investigație, evenimente la fața locului	Bidirecțional / Events

Justiție	PIGD / sistem instanțe	Ordonanțe de protecție, hotărâri judecătorești	Consum / Events
Protecție socială	e-Social, AMS, AS-Cazuri	Plasament adăposturi, prestații sociale, programe reintegrare	Bidirecțional / Events
Asistență juridică	Sistemul informațional CNAJGS	Asistență juridică acordată, dosare	Bidirecțional / Events
Analiză sociale online	Sistem extern de analiză rețele sociale	Clasificări violență online, link-uri postări monitorizate	Consum / asincron

Pentru fiecare integrare vom elabora o Specificație de Interoperabilitate (livrabilul Etapei II) care detaliază: obiectele informaționale schimbate, structura datelor (JSON Schema), sensul schimbului, frecvența, condițiile de declanșare, gestiunea erorilor, scenariile de testare, autorizațiile legale (memorandum/acord).

9.4. Gestionarea erorilor și continuitatea schimbului

Conform cap. 5.13.3, sistemul detectează și gestionează indisponibilitatea temporară, erorile de validare și cele de comunicare. Implementarea folosește:

- Polly resilience policies: retry exponential cu jitter (3 încercări), circuit breaker (deschidere după 5 erori consecutive, half-open după 60s), timeout configurat per integrare
- Dead Letter Queue (RabbitMQ) pentru mesaje care nu pot fi procesate – cu mecanism de retrimitere manuală de către administrator
- Outbox pattern – garantează că nicio modificare locală cu impact extern nu este pierdută la indisponibilitate
- Compensation transactions pentru fluxuri ce traversează multiple integrări (saga pattern în MassTransit)
- Health checks expuse pe /health pentru fiecare integrare; afișare status în interfața de administrare

9.5. Geo-tagging GPS (cap. 6.4 caiet)

Frontend: HTML5 Geolocation API cu consimțământ explicit; harta interactivă bazată pe Leaflet + OpenStreetMap (privacy-friendly, fără cost de licență, fără dependență de furnizor cloud public). Backend: PostgreSQL 16 cu extensia PostGIS pentru indexare geospațială și interogări tip „cazuri într-o rază”. Endpoint-urile de actualizare locație folosesc REST cu autentificare după certificat și autorizare strictă pe rol; locațiile sunt imutabile odată înregistrate (audit). Toate locațiile sunt criptate la repaus.

10. Securitate, Confidențialitate, GDPR și Conformitate

Sistemul gestionează date personale sensibile (sex, vârstă, identitate, locație, stare de sănătate, situație familială, fapte penale) și cere cel mai înalt nivel de protecție. Implementăm un program complet de securitate, în conformitate cu HG 1123/2010, HG 201/2017, ISO/IEC 27001:2022, GDPR (UE) 2016/679, și OWASP Top 10.

10.1. Privacy by Design și DPIA

Înainte de începerea Etapei II (Proiectare), elaborăm o Evaluare de Impact privind Protecția Datelor (DPIA / EIPD), conform art. 35 GDPR și prevederilor naționale. DPIA acoperă identificarea fluxurilor de date personale, evaluarea riscurilor pentru drepturile victimelor, măsurile de minimizare, păstrarea (perioade de retenție), pseudonimizarea, drepturile persoanei vizate (acces, rectificare, ștergere, opoziție). DPIA va fi aprobată de DPO al ANPCV și consultată cu CNPDCP.

10.2. Măsuri tehnice de securitate

Domeniu	Măsură tehnică
Criptare în tranzit	TLS 1.3 obligatoriu, certificate emise de autoritatea guvernamentală; HSTS activ; mTLS între servicii interne
Criptare în repaus	AES-256 pentru baze de date și fișiere; chei gestionate prin Vault (HashiCorp);
Pseudonimizare	Date personale stocate separat de date operaționale; identificator pseudonim utilizat în loguri și exporturi statistice
RBAC + ABAC	Roluri definite în matrice (administrator, manager caz, raportor, vizualizator, auditor); restricționare pe atribute (regiune, instituție)
Autentificare	Exclusiv MPass (federată); MFA obligatoriu pentru roluri privilegiate; sesiune expiră după 30 min inactivitate
Autorizare	Verificare la fiecare endpoint și la fiecare operațiune; principiul least-privilege; deny-by-default
Audit & jurnalizare	MLog pentru evenimente legale; Elasticsearch pentru operațional; jurnale imutabile (append-only)
Detecție anomalii	Alerting Prometheus pentru pattern-uri suspecte (multe accesări, ore non-business, IP atipic)
Anti-malware / WAF	WAF (ModSecurity / Coraza) la API Gateway; scanare anti-malware pe upload-uri
Backup & DR	Backup zilnic full + incremental orar; RPO=1h, RTO=4h; DR site pe regiune MCloud secundară

Pentest	Test de penetrare extern (STISC sau companie acreditată) înainte de lansarea în producție
SAST/DAST	SonarQube + OWASP ZAP automat la fiecare build; remediere obligatorie la high/critical

10.3. Drepturile persoanei vizate (GDPR)

Implementăm proceduri tehnice și fluxuri de business pentru toate drepturile GDPR: acces (export structurat al datelor unei persoane), rectificare (workflow de validare pentru modificări), ștergere („dreptul de a fi uitat", cu păstrarea dosarelor cerute legal), restricționare procesare, portabilitate, opoziție. Solicitările sunt înregistrate, jurnalizate și au termene de răspuns conform GDPR (max. 30 zile).

10.4. Continuitate și recuperare

Conform cap. 6.7 al caietului (disponibilitate ≥99,9%), arhitectura include:

- Cluster Kubernetes multi-node (minimum 1 nod master + 3 worker)
- PostgreSQL replicat (1 primar + 2 standby; failover automat cu Patroni)
- Redis Cluster cu redundanță
- Backup imutabil (Velero pentru K8s + pgBackRest pentru PostgreSQL); retenție 90 zile online + 7 ani offline
- Plan BCP/DRP documentat, cu RPO=1h, RTO=4h; testat semestrial
- Rulebook detaliat de incident response, alineat la cerințele HG 201/2017

10.5. Conformitate eGov4Dev și Modelul Unitar de Design

Toate componentele sistemului respectă platforma eGov4Dev (https://egov-moldova.github.io/egov4dev/), incluzând: principiile de arhitectură guvernamentală, mecanismele de identitate, integrări cu servicii comune, ghidurile de securitate. Frontendul implementează integral Modelul Unitar de Design (MUD) – paletă cromatică, tipografie, componente, accesibilitate, navigare. Vom organiza o sesiune de validare cu echipa AGE responsabilă de MUD înainte de finalizarea designului.

11. Strategia de Testare

Aplicăm o strategie de testare în piramidă (Test Pyramid), automatizată și integrată în pipeline-ul CI/CD. Fiecare nivel de test are un scop clar și criterii de acceptanță definite în Definition of Done. Nicio funcționalitate nu este considerată completă fără teste verzi pe toate nivelurile relevante.

Nivel test	Scop	Instrumente	Țintă
Unit tests	Validare logică de business, validatori, calcule indicatori, tranziții stări	xUnit, Moq, FluentAssertions, bUnit (Blazor)	Coverage ≥80% pe cod business
Integration tests	Validare endpoints, EF Core queries, integrare cu PostgreSQL, Redis	Testcontainers, ASP.NET Core TestServer, WireMock.Net	Toate API-urile critice
Contract tests	Validare contracte API între VioData și sisteme externe	PactFlow, Spectral OpenAPI	Toate integrările
E2E (UI)	Validare flux utilizator end-to-end pe scenariile operaționale SO-01 – SO-09	Playwright (cu MCR runner)	Toate scenariile critice
Performanță	Validare SLO: 500/1000 utilizatori simultani; latență ≤2s/5s/200ms	k6, Grafana k6 Cloud	Toate scenariile cu trafic mare
Securitate (SAST)	Analiză cod static, vulnerabilități OWASP	SonarQube, Snyk, GitHub CodeQL	Zero high/critical
Securitate (DAST)	Analiză dinamică, OWASP Top 10, fuzzing	OWASP ZAP, Burp Suite Pro	Inainte de Pilot și Producție
Pentest	Testare independentă (CERT-GOV-MD)	Subcontract specialist acreditat	Înainte de lansare națională + anual
Accesibilitate	Conformitate WCAG 2.1 nivel A	axe-core, Lighthouse, Wave	Pe toate paginile publice
UAT	Validare cu utilizatorii reali din ANPCV și instituțiile partenere	Sesiuni structurate, fișe UAT	Validare 100% cerințe acceptanță

12. Strategia de Pilotare

Faza de pilotare se desfășoară pe parcursul ultimelor 8 săptămâni ale Etapei IV (luna 13–14 a proiectului), conform cap. 3 al Caietului, înainte de lansarea națională. Obiectivul este validarea sistemului în condiții reale, identificarea problemelor de utilizabilitate și optimizarea finală.

12.1. Domeniu pilotare

- Geografic: 4 raioane reprezentative (urban + rural; nord + sud + centru) – inclusiv mun. Chișinău
- Instituțional: 8 ATAS, 4 IP raionale, 3 spitale raionale, 2 birouri CNAJGS, 2 ONG-uri partenere
- Utilizatori: 80–120 utilizatori finali activi, acoperind toate rolurile (manager caz, raportor, asistent social, polițist, medic, jurist)
- Volum: estimat 400–600 cazuri reale create, 1.500+ tranzacții pe zi în vârful pilotării

12.2. Activități de pilotare

18. Pregătire (săpt. 1): instruire pilot, configurare medii, validare integrări, populare nomenclatoare
19. Operare (săpt. 2-6): utilizare în condiții reale; suport on-site (2 ingineri DataSoft) și remote 9-21h
20. Colectare feedback (continuu): chestionare săptămânale, interviuri, focus grupuri, telemetrie
21. Analiza și remediere (săpt. 7): consolidare findings, prioritizare, fix bugs, optimizări
22. Raport pilotare (săpt. 8): document detaliat — cap. 4 caiet livrabil 6

12.3. Indicatori de succes pilotare

- ≥95% din scenariile operaționale SO-01 – SO-09 finalizate cu succes
- Disponibilitate sistem ≥99,5% pe perioada pilotării
- Timp mediu înregistrare caz ≤8 minute (validat cu cronometrare reală)
- NPS (Net Promoter Score) utilizatori finali ≥30
- Zero incidente de securitate cu impact
- Toate integrările guvernamentale funcționale și validate

13. Instruire și Transfer de Cunoștințe

Programul de instruire este proiectat pe 4 niveluri, cu volume conform cap. 8 al Caietului (Administratori: 16h; Utilizatori: 24h) și acoperă toate rolurile sistemului.

Nivel	Public țintă	Volum	Mod livrare
Nivel 1 – Administratori tehnici	Echipa IT ANPCV, AGE	16 ore (4 zile)	On-site la sediul ANPCV; instruire intensivă cu exerciții
Nivel 2 – Manageri de caz, key users	Personal ANPCV, lideri instituționali	24 ore (6 zile)	On-site, blended cu e-learning
Nivel 3 – Train-the-trainer	20 instructori interni (multiplicatori)	24 ore + 8h pedagogice	On-site la Chișinău
Nivel 4 – Utilizatori finali	Asistenți sociali, polițiști, medici, juriști	16 ore (modular)	Cascadă prin trainerii nivel 3 + e-learning + manuale rol-specific

13.1. Materiale didactice produse

- Manualul administratorului tehnic (≥80 pagini, RO/RU, format PDF + online)
- Manualul de utilizare (RO/RU)
- Ghiduri rapide tip „cheat sheet” (laminate, A4 față-verso) pentru fiecare rol
- Bibliotecă video tutorial: minimum 5 de video-uri scurte (3–7 min) pe operațiuni concrete
- Scenarii de instruire practică: 12 cazuri studiu pas-cu-pas, cu date sintetice
- Chestionare evaluare cunoștințe (la finalul instruirii) cu certificat de absolvire
- Help-system contextual integrat în aplicație (pop-up explicativ pe câmpuri și operațiuni)

14. Mentenanță și Garanție

Conform cap. 6.9 al Caietului, oferim 12 luni de garanție și mentenanță gratuită începând de la data recepției finale (Etapa V). Pe această perioadă, asigurăm:

14.1. Servicii incluse în garanție

- Mentenanță corectivă: remedierea gratuită a tuturor defectelor și incidentelor raportate (bug-uri, regresii, incompatibilități)
- Mentenanță adaptivă: ajustări pentru modificări legislative, schimbări de servicii guvernamentale (versiuni noi MPass/MConnect), actualizări de browsere și OS
- Suport tehnic L2/L3: echipă dedicată (4 specialiști), ticketing centralizat (Azure DevOps)
- Patch-uri de securitate: aplicare în maximum 72h pentru vulnerabilități high/critical
- Monitorizare proactivă: alerting 24/7 pentru disponibilitate, performanță, anomalii securitate
- Raport lunar de servicii (incidente, modificări, KPI, recomandări)

14.2. SLA garanție

Tip incident	Timp răspuns	Timp soluționare	Comunicare
Critic (P1)	≤ 30 minute	≤ 4 ore	Telefonic + e-mail
Major (P2)	≤ 2 ore	≤ 24 ore	Ticket + e-mail
Minor (P3)	≤ 8 ore	≤ 5 zile lucrătoare	Ticket
Cerere informație	≤ 24 ore	≤ 10 zile lucrătoare	Ticket

14.3. Predarea sistemului și a cunoștințelor

La finalul perioadei de garanție, predăm Beneficiarului întregul pachet de proprietate intelectuală și operațională:

- Codul sursă final, complet și compilabil, în repository Git Beneficiar
- Documentația tehnică completă (arhitectură, API, model date, runbooks operaționale)
- Toate credențialele, secretele și certificatele rotate către conturile Beneficiarului
- Knowledge transfer formal: 2 sesiuni de 8h fiecare cu echipa tehnică ANPCV/AGE
- Plan de mentenanță continuă recomandat (postgaranție)

15. Analiza Riscurilor și Plan de Mitigare

Identificăm proactiv riscurile cheie și definim măsuri concrete de prevenire și răspuns. Matricea de risc este actualizată la sfârșitul fiecărei etape și la apariția unor evoluții semnificative; este revizuită lunar în Steering Committee.

15.1. Matricea de riscuri

ID	Risc	P	I	Măsuri de mitigare / răspuns
R-01	Întârzieri în obținerea acordurilor MOU pentru integrările sectoriale (sănătate, justiție, ordine publică)	M	R	Implicarea AGE și ANPCV de la Etapa I; pregătirea draft-urilor MOU în Etapa I; mock-uri de integrare ce permit dezvoltare paralelă; plan de contingență cu fluxuri manuale temporare
R-02	Modificări tehnice ale serviciilor guvernamentale (MPass, MConnect) pe parcursul proiectului	M	M	Monitorizare changelog AGE; arhitectura cu strat de adaptare; teste contract regulate; implicarea early în comunitatea eGov4Dev
R-03	Riscuri de securitate (atac, breșă date personale)	R	F.R	Defense-in-depth (cap. 10); SAST/DAST automatizat; pentest extern; WAF; criptare end-to-end; runbook incident response; asigurare cyber
R-04	Schimbări legislative (modificări la Legea 45/2007, HG 530/2025)	M	M	Arhitectură configurabilă; nomenclatoare administrabile; reguli de business externalizate; rezervă efort pentru schimbări
R-05	Indisponibilitate temporară a personalului cheie (concediu, boală, plecare)	M	M	Backup pentru fiecare rol (specialiști rezervă); knowledge sharing săptămânal; documentație tehnică obligatorie; pair programming pe componente critice
R-06	Adopție lentă din partea utilizatorilor finali	M	R	Implicare utilizatori încă din Etapa I; UX trauma-informed; pilotare extinsă; instruire în 4 niveluri; canal feedback continuu; champions interni
R-07	Cerințe ascunse identificate târziu (după Etapa II)	M	M	Analiză aprofundată în Etapa I (workshops, interviuri, observare directă teren); matrice trasabilitate; rezervă 10% efort pentru change requests
R-08	Performanță degradată sub încărcare reală (vârfuri trafic)	S	R	Testare performanță k6 încă din sprint-ul 6; auto-scaling Kubernetes; cache Redis; query profiling; monitorizare APM continuă

R-09	Probleme cu calitatea datelor existente (la migrare opțională)	M	M	Scripturi ETL cu validare strictă; quarantine pentru înregistrări problemă; raportare cleansing; opțiune importare manuală cu verificare
R-10	Probleme contractuale cu MCloud (capacitate, costuri)	S	M	Comunicare directă cu AGE de la Etapa I pentru rezervare resurse; estimări TCO conservatoare; clauze de scalare în contract
R-11	Solicitare DPO/CNPDCP pentru ajustări semnificative la procesarea datelor	M	M	DPIA elaborat înainte de Etapa II; consultare proactivă CNPDCP; arhitectură flexibilă pe minimizare date și retenție
R-12	Calitate slabă a datelor de la sistemul extern de analiză rețele sociale	M	S	Scor încredere per înregistrare; verificare manuală pentru mențiuni cu impact; flag „necesită verificare” pentru cazuri online

Legendă probabilitate / impact: F.R = foarte ridicat, R = ridicat, M = mediu, S = scăzut.

15.2. Procesul de management al riscurilor

Aplicăm un proces continuu de identificare, analiză, planificare răspuns, monitorizare și control:

23. Identificare lunară (în Steering Committee) și ad-hoc la apariția unor evenimente
24. Analiză cantitativă (P×I) pentru prioritizare
25. Răspuns: evitare, transfer, mitigare, acceptare – documentat per risc
26. Monitorizare: triggers definiți (ex.: indisponibilitate >2h MConnect declanșează escaladare)
27. Raportare: registrul riscurilor disponibil în Confluence, actualizat săptămânal de PM

GHESAR®

16. Raportul Cost Total de Proprietate (TCO) — 3 ani

Conform cap. 4 (livrabilul 3) și cap. 8 al Caietului, prezentăm o estimare TCO pentru 3 ani de operare a SI RS VioData. Estimările sunt orientative la nivel de structură și unități; valorile finale vor fi consolidate în Raportul TCO oficial livrat în Etapa I, după finalizarea specificațiilor tehnice detaliate.

16.1. Componente de cost

Categorie cost	Anul 1 (dezvoltare + lansare)	Anul 2 (operare)	Anul 3 (operare)
Dezvoltare software	Inclus în contract (om-zile detaliate la pct. 16.2)	—	—
Infrastructură MCloud	Asigurat de STISC	Asigurat de STISC	Asigurat de STISC
Licențe software	Bazată pe OpenSource	Bazată pe OpenSource	Bazată pe OpenSource
Mentenanță (corectivă + adaptivă)	Inclus garanție 12 luni	Pachet mentenanță continuă	Pachet mentenanță continuă
Suport tehnic	Inclus garanție 12 luni	L2/L3 ore-pachet	L2/L3 ore-pachet
Securitate (pentest, audit ISO)	1 pentest pre-lansare + audit ISO 27001	1 pentest anual + audit ISO	1 pentest anual + audit ISO
Instruire suplimentară	Inclus în contract	2 sesiuni utilizatori noi	2 sesiuni utilizatori noi
Extindere și scalare	—	Funcționalități noi (rezervă)	Funcționalități noi (rezervă)
Total estimativ	**Oferta Financiară**	Min 15% din anul 1	Min 20% din anul 1

16.2. Estimarea efortului (om-zile pe rol și etapă)

Conform cap. 8 al Caietului, prezentăm estimarea efortului total al echipei de proiect pentru Etapele I-V (excluzând garanția). Estimările sunt corelate cu cerințele funcționale, scenariile operaționale (SO-01 – SO-09) și use-case-urile descrise în Caiet.

Rol	Et. I (Inițiere)	Et. II (Proiectare)	Et. III (Dezvoltare + Integrare)	Et. IV (Testare + Pilotare)	Et. V (Lansare + Recepție)
Manager de proiect	25	35	160	60	20
Business Analyst	45	60	120	50	15

Arhitect IT	20	65	100	30	10
Backend Devs (3)	0	60	780	120	30
Frontend Devs (2)	0	40	440	80	20
UX/UI	10	80	80	30	10
QA / Testare	10	30	220	180	20
DevOps	5	30	130	50	20
Securitate	15	25	60	40	15
TOTAL pe etapă (om-zile)	**130**	**425**	**2.090**	**640**	**160**

17. Asumarea Conformității cu Cerințele Caietului de Sarcini

Asumăm fără rezervă toate cerințele Caietului de sarcini ca fiind contractuale și obligatorii. Pentru transparență, prezentăm tabelul de conformitate la cerințele non-funcționale critice:

Cerință (Caiet)	Asumare
Limbi: română (default 100%), rusă, engleză	Conformă. Resurse i18n în .resx, traduceri profesionale validate; QA dedicat pentru fiecare limbă
WCAG 2.1 nivel A	Conformă. Vizăm nivelul A ca diferențiator
Responsive 320–1600px	Conformă. Mobile-first, testare pe matrice dispozitive (smartphone, tabletă, laptop, desktop)
Stack .NET / MudBlazor / Blazor / PostgreSQL	Conformă (cap. 8)
Hosting MCloud	Conformă; mediu Dev/QA/Staging + Pilot + Prod + DR
Containerizare Docker, K8s, Helm; CI/CD Azure DevOps + GitLab	Conformă (cap. 8)
Monitorizare: Elasticsearch, Kibana, Prometheus, Grafana	Conformă (cap. 8)
Integrare obligatorie MPass, MSign, MNotify, MLog, MConnect	Conformă (cap. 9 prezenta ofertă)

OWASP, ISO 27001, HG 1123/2010, HG 201/2017, GDPR	Conformă (cap. 10 prezenta ofertă)
Disponibilitate ≥99,9%, 500-1000 utilizatori simultani	Conformă; arhitectură cu redundanță, autoscaling, DR (RPO 1h, RTO 4h)
Performanță: dosar ≤2s, raport ≤5s, notificare ≤1s, API intra ≤50ms, API ext ≤200ms	Conformă; testare k6 pe scenarii reale; SLO definite și monitorizate
Garanție 12 luni gratuită + mentenanță corectivă/adaptivă	Conformă (cap. 14 prezenta ofertă)
Predare cod sursă, documentație, credențiale	Conformă; toate IP-urile transferate Beneficiarului la recepție și la finalul garanției
Conformare eGov4Dev, MUD	Conformă; consultări AGE pe parcurs
Posibilitate scoatere din exploatare controlată (export, ștergere sigură)	Conformă; capabilități de export complet și ștergere sigură criptografică

18. Concluzii

GHESAR prezintă o ofertă tehnică care răspunde integral și în detaliu tuturor cerințelor obligatorii ale Caietului de sarcini pentru SI RS VioData. Forța acestei propuneri este construită pe trei piloni:

28. Înțelegere profundă a contextului – atât a problematicii de violență de gen cât și a ecosistemului digital guvernamental moldovenesc (eGov4Dev, MUD, MCloud, MConnect, MPass, MSign, MNotify, MLog).
29. Calea metodologică solidă – o abordare hibridă care combină rigoarea contractuală a unei desfășurări etapizate cu flexibilitatea iterativă a Scrum, completată de practici DevSecOps mature.
30. Echipa și capacitatea operațională – 20 specialiști, cu portofoliu guvernamental dovedit.

Ne angajăm să livrăm un sistem care nu doar îndeplinește cerințele tehnice, ci servește efectiv profesioniștii care intervin direct în viața victimelor cu o interfață sensibilă și clară, fluxuri intuitive în condiții de urgență, și securitate maximă a datelor sensibile.

Detaliile cronologice complete, livrabile pe etape și estimările de efort vor fi prezentate în Planul de Proiect care se va elabora împreună cu Beneficiarul.

Am construit 8 mockup-uri HTML de interfață, salvate în folderul mockup/ din workspace-ul VioDarta. Toate sunt self-contained, randate corect, folosesc paleta navy/accent aliniată MUD eGov4Dev, iar datele afișate sunt fictive ilustrative.

Deschide pagina-index a mockup-urilor

Pagini disponibile:

- 00 — Autentificare prin MPass — punct de intrare federat
- 01 — Dashboard Manager Caz — KPI-uri, alerte ordine restricție, sarcini, status integrări
- 02 — Listă Cazuri — filtre, paginare, export PDF/CSV/Excel
- 03 — Fișa Caz — sinteză, persoane, evaluare risc, plan intervenție, măsuri protecție, referiri, documente, audit
- 04 — Înregistrare Caz Nou — formular în 5 pași cu deduplicare RSP via MConnect și consimțământ MSign
- 05 — Evaluare Risc — chestionar 12 itemi, scor automat, acțiuni recomandate
- 06 — Tablou Analitic — heat-map RM, donut tipuri violență, trend 2024-2026, demografie, status referiri
- 07 — Administrare Utilizatori — RBAC granular, matrice permisiuni, integrare MPass

Pentru orice clarificare suplimentară rămânem la dispoziția comisiei de evaluare.

info@ghesar.com

+373 795 333 11

Cu deosebită considerație,

Dmitri Alexeev

Director General

GHESAR

Digitally signed by Monastîrli Nicolae
Date: 2026.05.03 19:35:43 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ