OFERTA TEHNICĂ

Compania Ofertantă: PNA SOFTWARE SRL

Proiect: Dezvoltarea Sistemului informațional „Registrul de stat VioData”

Beneficiarul: Agenția Națională de Prevenire și Combatere a Violenței Împotriva Femeilor și a Violenței în Familie (ANPCV)

72200000-7 | Nr. OCDS-B3WDP1-MD-1773235556761

1. Rezumat executiv

Prezenta propunere tehnică descrie soluția pentru proiectarea, dezvoltarea și implementarea Sistemului informațional „Registrul de stat VioData" (SI RS VioData), în conformitate cu Hotărârea Guvernului nr. 530/2025 cu privire la aprobarea Conceptului Sistemului informațional „Registrul de stat VioData" și a Regulamentului privind modalitatea de ținere a Registrului de stat VioData.

Problema identificată. În prezent, datele referitoare la cazurile de violență împotriva femeilor și violență în familie sunt gestionate fragmentat de multiple instituții - MAI, MMPS, MS, MJ, CNAJGS - prin sisteme și registre distincte. Această fragmentare împiedică monitorizarea integrată a cazurilor, evaluarea intervențiilor și fundamentarea politicilor publice pe baza datelor.

Soluția propusă. SI RS VioData va fi o platformă informațională centralizată, dezvoltată integral cu tehnologii open-source, destinată colectării, stocării, prelucrării și raportării datelor în domeniul prevenirii și combaterii violenței. Sistemul va include 9 module funcționale care acoperă integral contururile prevăzute în Concept: administrare, managementul raportării cazurilor, urmărirea cazurilor, urmărirea referirilor, caz de violență, evidența măsurilor de protecție, raportare și analiză, acces autorizat și gestionarea nomenclatoarelor.

Abordarea tehnologică. Propunem un stack .NET end-to-end (Blazor + ASP.NET Core + PostgreSQL), combinând API-uri REST (pentru integrarea cu serviciile guvernamentale) și GraphQL prin Hot Chocolate (pentru interogări dinamice, rapoarte și geo-etichetare), arhitectură modulară pe straturi, găzduire pe MCloud (Kubernetes) și integrare completă cu ecosistemul e-Guvernare (MPass, MSign, MLog, MNotify, MConnect). Metodologia de implementare este hibridă - etape secvențiale conform Conceptului, cu livrări iterative Agile în cadrul fiecărei etape.

Beneficii. Coordonare interinstituțională eficientă, dosar electronic unic per caz, raportare centralizată cu indicatori naționali, conformitate GDPR și legislație națională, trasabilitate completă și securitate avansată a datelor victimelor.

2. Înțelegerea sarcinii / obiectului contractului

2.1 Contextul actual

Violența împotriva femeilor și violența în familie reprezintă o problemă persistentă în Republica Moldova. Cadrul normativ național, în special Legea nr. 45/2007, stabilește mecanisme de prevenire și combatere, însă implementarea efectivă este îngreunată de fragmentarea sistemelor informaționale existente.

Principalele instituții implicate - ANPCV, MAI/IGP, MMPS/ATAS, MS, MJ, CNAJGS - gestionează date în sisteme separate, fără un mecanism unic de evidență și monitorizare. Profesioniștii din domeniu (asistenți sociali, personal medical, organe de drept) nu dispun de un instrument informațional comun care să permită gestionarea integrată a cazurilor.

2.2 Problema de business

- **Fragmentarea datelor:** fiecare instituție menține propriul registru, ceea ce face imposibilă o viziune de ansamblu asupra unui caz
- **Raportare inconsistentă:** lipsa standardizării proceselor de colectare și raportare conduce la date incomplete sau contradictorii
- **Coordonare deficitară:** referirile interinstituționale se realizează manual, fără trasabilitate și fără feedback asupra rezultatelor
- **Lipsa fundamentării:** factorii de decizie nu dispun de date agregate fiabile pentru elaborarea și evaluarea politicilor publice
- **Riscuri de confidențialitate:** gestionarea datelor sensibile ale victimelor în sisteme necorelate crește riscul de breșe sau accesări neautorizate

2.3 Necesități operaționale

SI RS VioData trebuie să răspundă următoarelor necesități operaționale fundamentale:

1. **Dosar electronic unic** - fiecare caz de violență trebuie gestionat printr-un dosar electronic centralizat, cu identificator unic, accesibil conform rolurilor
2. **Referiri interinstituționale** - sistemul trebuie să permită transmiterea și urmărirea referirilor între instituții (medicale, juridice, sociale, adăposturi)
3. **Alerte și notificări automate** - notificarea automată a părților implicate la schimbarea stării cazului, expirarea măsurilor de protecție sau necesitatea intervenției
4. **Raportare centralizată** - generarea de rapoarte statistice, indicatori naționali și tablouri de bord interactive pentru fundamentarea deciziilor
5. **Evidența măsurilor de protecție** - monitorizarea ordinelor de restricție și ordonanțelor de protecție, cu alerte de expirare
6. **Monitorizare violență online** - integrare cu instrumentul de monitorizare UNFPA pentru recepționarea rezultatelor de analiză a cazurilor de violență în mediul online

2.4 Mediul tehnic

Sistemul va opera în cadrul ecosistemului e-Guvernare al Republicii Moldova:

- **MCloud** - Platforma Cloud Guvernamentală pentru găzduire (Kubernetes)

- **MConnect** - Platforma guvernamentală de interoperabilitate pentru schimb de date cu 11 sisteme informaționale externe
- **MPass** - Serviciul guvernamental de autentificare și control al accesului
- **MSign** - Serviciul guvernamental de semnătură electronică
- **MNotify** - Serviciul guvernamental de notificare electronică
- **MLog** - Serviciul guvernamental de jurnalizare

2.5 Constrângeri

- Hotărârea Guvernului nr. 530/2025 - Conceptul SI „VioData" și Regulamentul registrului
- Regulamentul General privind Protecția Datelor (GDPR) (UE) 2016/679
- HG nr. 1123/2010 - cerințe privind securitatea datelor personale
- HG nr. 201/2017 - cerințe minime obligatorii de securitate cibernetică
- Legea nr. 45/2007 - prevenirea și combaterea violenței
- Modelul Unitar de Design (MUD) - standard național de design pentru soluțiile web guvernamentale
- Platforma eGov4Dev (https://egov-moldova.github.io/egov4dev/) - sursă oficială obligatorie de documentație tehnică, elaborată și administrată de Agenția de Guvernare Electronică. Prestatorul se obligă să analizeze și să aplice prevederile eGov4Dev în toate etapele ciclului de viață al sistemului (analiză, proiectare, dezvoltare, integrare, testare, punere în producție), inclusiv: principii de arhitectură guvernamentală, cerințe de interoperabilitate, descrierea serviciilor comune (MPass, MSign, MNotify, MLog, MConnect), bune practici de securitate și ghiduri pentru dezvoltatori. Nerespectarea acestor ghiduri constituie neconformitate tehnică în procesul de evaluare și acceptanță livrabilelor.

Aplicarea concretă a prevederilor eGov4Dev pe etapele de implementare:

Etapă	**Prevederi eGov4Dev aplicate**
I - Analiză	Principii arhitectură guvernamentală; cerințe interoperabilitate MConnect; identificarea SIA-urilor relevante din catalogul eGov4Dev
II - Proiectare	Ghid MUD (design UI/UX conform standardului național); specificații tehnice servicii comune (MPass SAML 2.0, MSign, MNotify, MLog, MConnect); ghid API design REST guvernamental
III - Dezvoltare	Bune practici securitate eGov4Dev; ghiduri de implementare pentru fiecare serviciu comun (.NET SDK, exemple de integrare); cerințe de accesibilitate WCAG
IV - Testare	Checklist conformitate eGov4Dev; criterii acceptanță interoperabilitate MConnect; scenarii de testare servicii comune
V - Lansare	Ghid deploy MCloud (Kubernetes, Helm); proceduri punere în producție conform eGov4Dev

VI - Mentenanță	Monitorizarea actualizărilor serviciilor comune publicate pe eGov4Dev; adaptarea integrărilor la versiunile noi ale API-urilor guvernamentale

2.6 Factori critici de succes

1. **Adopția de către utilizatori** - interfață intuitivă, instruire adecvată, suport continuu
2. **Interoperabilitate reală** - integrare funcțională (nu doar tehnică) cu sistemele existente prin MConnect
3. **Securitatea datelor victimelor** - protecție maximă a datelor sensibile, conformitate legislativă demonstrabilă
4. **Calitatea datelor** - mecanisme de validare, deduplicare și standardizare
5. **Sustenabilitate** - tehnologii open-source, documentație completă, transfer de cunoștințe

3. Matricea de conformitate

3.1 Cerințe funcționale

Ref.	Cerința (rezumat)	Modul de implementare
5.1.1	Interfață utilizator multilingvă (RO, RU, EN)	IStringLocalizer / IHtmlLocalizer cu resurse per modul; RO implicită cu acuratețe 100%; traduceri RU/EN gestionate prin fișiere .resx
5.1.2	Accesibilitate WCAG nivel A	MudBlazor cu suport accessibility built-in; audit automat axe-core în pipeline CI/CD; testare manuală cu screen reader
5.1.3	Suport dispozitive multiple (320px-1600px)	Design web adaptiv cu MudBlazor responsive grid (MudGrid, Breakpoint); breakpoints configurate; testare pe dispozitive reale și emulatoare
5.2.1	Administrarea utilizatorilor și rolurilor	CRUD complet utilizatori prin interfață grafică; RBAC cu ASP.NET Core Authorization Policies; integrare MPass SAML 2.0; roluri multiple per utilizator
5.2.2	Securitate, jurnalizare și audit	Jurnalizare automată a tuturor acțiunilor; integrare MLog; jurnale filtrabile, exportabile; audit ex-post per caz
5.3.1	Înregistrarea cazurilor de violență	Formular standardizat Blazor EditForm + FluentValidation; UUID automat; validare câmpuri obligatorii client+server; câmpuri violență online

5.3.2	Consimțământ și confidențialitate	Mecanisme de colectare consimțământ; acces restricționat pe roluri; jurnalizare accesări date personale
5.4.1	Monitorizarea ciclului de viață al cazului	State machine configurabil; stări: deschis/în desfășurare/referit/închis/respins/inactiv; reguli tranziție configurabile; jurnalizare
5.4.2	Evaluarea riscului și planul de intervenție	Formular evaluare risc structurat, versionat; plan intervenție cu acțiuni/termene/responsabili; istoric complet
5.5.1	Gestionarea referirilor	CRUD referiri per caz; tipuri serviciu selectabile; status actualizabil; istoric complet consultabil
5.5.2	Interoperabilitatea referirilor	Schimb date MConnect sincron + MConnect Events asincron; structură documentată; gestionare erori; principiul once-only
5.6.1	Evidența măsurilor de protecție	Evidență ordine restricție + ordonanțe protecție; corelare caz-agresor/victimă; alerte expirare; audit complet
5.6.2	Corelarea și vizualizarea măsurilor în fișa cazului	Vizualizare centralizată; blocare închidere caz cu măsuri active; excepții controlate prin roluri
5.7.1	Raportare operațională și statistică	Rapoarte standard + personalizate; indicatori naționali din Concept; export PDF/CSV/Excel; date violență online
5.7.2	Tablouri de bord și analiză	Tablouri de bord interactive ApexCharts.Blazor; filtrare dinamică; actualizare în timp real; accesibile conform rolului
5.8.1	Crearea și administrarea nomenclatoarelor	CRUD nomenclatoare prin interfață grafică; versionare; activare/dezactivare fără ștergere; jurnalizare
5.8.2	Utilizarea nomenclatoarelor în actele de evidență	Dropdown-uri controlate obligatorii; prevenirea valorilor libere; liste derulante cu căutare
5.9.1	Acces autorizat	Autentificare exclusiv MPass; interfață personalizată pe rol; funcționalități neautorizate inaccesibile
5.9.2	Acces public	Separare strictă date publice/confidențiale; zero acces public la date cu caracter personal
5.10.1-6	Documentele de bază ale registrului	Documente intrare/ieșire/tehnologice; ciclu complet de viață; trasabilitate; versionare; arhivare; rollback

5.11.1-6	Obiecte informaționale și identificatori	14 obiecte de bază; UUID v4 stabili; asociere IDNP; relații explicite; versionare; deduplicare; integritate referențială
5.12	Scenarii operaționale SO-01 - SO-09	Implementare completă fiecare scenariu ca flux end-to-end; state machines; business rules; jurnalizare
5.13.1-4	Interoperabilitate și schimb de date	MConnect REST sincron + Events asincron; 11 SIA externe; cache local Redis; gestionare erori; documentare completă

3.2 Cerințe nefuncționale

Ref.	**Cerința (rezumat)**	**Modul de implementare**
6.1	Tehnologii open-source și arhitectură modulară	.NET end-to-end (Blazor + ASP.NET Core); PostgreSQL; Docker; Kubernetes; module independente; conformitate MUD
6.2	Mediul de sistem (MCloud, CI/CD, monitoring)	MCloud Kubernetes; Docker multi-stage; Helm charts; Azure DevOps + GitLab CI/CD; Prometheus + Grafana; ELK Stack
NFR 03	Integrarea cu servicii guvernamentale	MPass (SAML 2.0), MSign (REST), MNotify (REST), MLog (REST), MConnect (REST + Events)
6.3	Interoperabilitate sistem	REST API documentat (OpenAPI/Swagger); JSON/XML/CSV; integrare forțe ordine, sănătate, servicii sociale; recepție date de la instrumentul de monitorizare UNFPA (violență online)
6.4	GPS Geo-etichetare	HTML5 Geolocation API; PostGIS (PostgreSQL); OpenStreetMap; API endpoints securizate
6.5	Securitatea sistemului	OWASP Top 10:2025; TLS 1.3; AES-256 at rest; ISO 27001; HG 201/2017; ASP.NET Core Security Middleware; rate limiting
6.6	Protecția datelor	GDPR (UE) 2016/679; HG 1123/2010; consimțământ explicit; privacy by design; drept la ștergere
6.7	Scalabilitate și fiabilitate	500 utilizatori simultani (scalabil 1000); HPA Kubernetes; 99.9% disponibilitate; failover; DR plan
6.8	Performanța sistemului	Dosar ≤2s; rapoarte ≤5s; notificări ≤1s; API intern ≤50ms; API extern ≤200ms; 1M+ înregistrări

6.9	Garanția și întreținerea	12 luni garanție; mentenanță corectivă + adaptivă; documentație actualizată; jurnal activități

4. Soluția tehnică propusă

4.1 Conceptul general

SI RS VioData este proiectat ca un sistem informațional pe straturi (layered architecture), dezvoltat integral cu tehnologii open-source și ecosistemul .NET, urmând principiile arhitecturii modulare și ale separării responsabilităților.

Straturile arhitecturale:

1. **Stratul de prezentare** (`VioData.Web`) - aplicație web Blazor (MudBlazor), responsivă, multilingvă, conformă MUD. Modulele autentificate (gestionare cazuri, referiri, măsuri de protecție, administrare) rulează pe **Blazor Server** - datele victimelor nu părăsesc niciodată serverul, autorizarea este aplicată server-side la fiecare interacțiune. Modulul public (statistici agregate anonimizate, secțiunea 5.9.2) rulează pe **Blazor WebAssembly** - zero date personale, scalare fără state server per utilizator, performanță superioară pentru utilizatori anonimi pe conexiuni lente
2. **Stratul API / Gateway** (`VioData.API`) - punct unic de intrare, autentificare MPass, rate limiting, routing, logging HTTP
3. **Stratul de aplicație** (`VioData.Application`) - orchestrarea cazurilor de utilizare, MediatR pentru comunicare inter-module, validări, reguli de business
4. **Stratul de domeniu** (`VioData.Domain`) - entități, interfețe, reguli de domeniu, value objects, domain events
5. **Stratul de date** (`VioData.Infrastructure`) - persistență: EF Core + PostgreSQL/PostGIS, Redis, Elasticsearch
6. **Stratul de integrare** (`VioData.Integration`) - adaptori MConnect (REST sincron + Events asincron), MPass, MSign, MNotify, MLog
7. **Stratul de securitate** - transversal; implementat prin ASP.NET Core Security Middleware (API), Authorization Policies (Application) și audit trail (Infrastructure)

Notă: VioData.Shared nu este un strat arhitectural, ci un shared kernel - conține DTO-uri, validări de suprafață FluentValidation (format, lungime, câmpuri obligatorii) și constante partajate între frontend și backend. Validările de business (unicitate, consistență cu baza de date, reguli de domeniu) rămân exclusiv în `VioData.Application`.

Direcția dependențelor:

```
VioData.Web -> VioData.API (HTTP)
VioData.API -> VioData.Application
VioData.Application -> VioData.Domain
VioData.Infrastructure -> VioData.Application (implementează interfețe)
VioData.Integration -> VioData.Application (implementează interfețe)
VioData.Shared <- (referit de Web, API, Application)
```

Domeniul (VioData.Domain) nu depinde de niciun alt proiect intern. Infrastructure și Integration nu sunt referite direct de Application - Application definește interfețe (ex: IUnitOfWork, IMConnectClient), iar Infrastructure/Integration le implementează prin Dependency Injection.

Structura soluției:

```
/src
  /VioData.Web            - Stratul de prezentare (Blazor Server pentru module
autentificate, Blazor WASM pentru modulul public, MudBlazor)
  /VioData.API            - Stratul API/Gateway (ASP.NET Core Web API, rate
limiting, logging, health checks)
  /VioData.Application    - Stratul de aplicație (MediatR, use cases, validări de
business)
  /VioData.Domain         - Stratul de domeniu (entități, interfețe, reguli, domain
events)
  /VioData.Infrastructure - Stratul de date (EF Core, PostgreSQL/PostGIS, Redis,
Elasticsearch)
  /VioData.Integration    - Stratul de integrare (MConnect, MPass, MSign, MNotify,
MLog)
  /VioData.Shared         - Shared kernel (DTOs, validări de suprafață
FluentValidation, constante)
/tests
  /VioData.UnitTests
  /VioData.IntegrationTests
  /VioData.E2ETests
```

4.2 Stiva tehnologică (Technology Stack)

Frontend:

- **Blazor Server** (module autentificate) + **Blazor WebAssembly** (modul public) - Server pentru datele sensibile ale victimelor (rendering server-side, zero expunere în browser); WebAssembly pentru pagina publică cu date agregate anonimizate (scalare fără conexiuni SignalR per utilizator anonim)
- MudBlazor - bibliotecă de componente UI reutilizabile (conformă MUD)
- Blazor EditForm + FluentValidation - gestionare formulare și validare (partajată cu backend)
- HttpClient + IMemoryCache - comunicare API și caching pe client
- Servicii Scoped + Dependency Injection (DI) - state management prin pattern-ul State Container, fără dependențe externe complexe, optimizat pentru fluxuri CRUD
- IStringLocalizer / IHtmlLocalizer - internaționalizare (RO, RU, EN) cu fișiere .resx
- MudBlazor Charts + ApexCharts.Blazor - vizualizări date și tablouri de bord
- QuestPDF - generare documente PDF
- Leaflet.Blazor + OpenStreetMap - hărți și vizualizări geospațiale

Backend:

- ASP.NET Core - framework aplicație (arhitectură modulară, dependency injection nativ)
- Hot Chocolate (GraphQL) - server GraphQL de înaltă performanță integrat nativ în ASP.NET Core, utilizat pentru expunerea datelor către interfața web, interogări dinamice complexe și tablouri de bord (implementat conform recomandărilor din caietul de sarcini cap. 6.3 și 6.4).
- Entity Framework Core - acces baze de date relaționale, migrări, type safety
- ITfoxtec.Identity.Saml2 - autentificare MPass (SAML 2.0)
- FluentValidation - validare DTOs declarativă (reguli partajate cu frontend)
- Hangfire + Redis - coadă de joburi pentru operații asincrone (notificări, MConnect Events, recepție date de la instrumentul de monitorizare UNFPA)

- Swashbuckle.AspNetCore - generare automată documentație OpenAPI/Swagger
- ASP.NET Core Health Checks - monitorizare stare conexiuni PostgreSQL, Redis, Elasticsearch și servicii externe (MConnect, MPass); expuse pe endpoint dedicat /health, integrate cu Prometheus + Grafana
- ASP.NET Core Security Middleware - securitate HTTP headers (HSTS, CSP, X-Frame-Options)
- AutoMapper - serializare/deserializare și mapare obiecte
- MediatR - comunicare inter-module bazată pe mesaje

Baze de date și stocare:

- PostgreSQL 16+ cu extensia PostGIS - baza de date principală, date relaționale și geospațiale
- Redis (StackExchange.Redis) - caching, sesiuni, coadă Hangfire, cache MConnect
- Elasticsearch (Elastic.Clients.Elasticsearch) - indexare și căutare rapidă jurnale și date operaționale

Infrastructură și DevOps:

- Docker - containerizare (multi-stage builds)
- Kubernetes - orchestrare (MCloud)
- Helm - gestionare deployment-uri Kubernetes
- Azure DevOps - gestionarea livrărilor, sarcinilor și erorilor; pipeline-uri automate
- GitLab - controlul versiunilor și integrare continuă
- Prometheus + Grafana - monitorizare metrici și alerte
- Elasticsearch + Logstash + Kibana (ELK) - centralizare și vizualizare logs

Justificarea alegerii stack-ului .NET:

Caietul de sarcini (secțiunea 6.1) recomandă ecosistemul .NET cu Blazor/MudBlazor și ASP.NET Core. Propunem stack .NET end-to-end (Blazor + ASP.NET Core) pe baza următoarelor argumente:

1. **Conformitate deplină cu caietul de sarcini** - stack-ul propus corespunde integral recomandărilor din secțiunea 6.1 a caietului de sarcini, care specifică explicit MudBlazor, Blazor Server/WebAssembly, ASP.NET Core, Entity Framework Core, FluentValidation și Swashbuckle
2. **Limbaj unic C#** - C# pe frontend (Blazor) și backend (ASP.NET Core) permite partajarea modelelor de validare (FluentValidation), a DTOs și a constantelor, reducând inconsistențele și efortul de dezvoltare
3. **Ecosistem enterprise matur** - ASP.NET Core este unul dintre cele mai performante și mature framework-uri enterprise, cu suport oficial Microsoft pe termen lung (LTS)
4. **Securitate și performanță** - ASP.NET Core oferă performanțe de vârf în benchmark-uri TechEmpower, dependency injection nativ, middleware pipeline optimizat și protecție built-in contra vulnerabilităților OWASP
5. **Sustenabilitate** - ecosistemul .NET beneficiază de suport pe termen lung (LTS), documentație extinsă și comunitate activă, asigurând mentenabilitate pe termen lung

4.3 Modulele sistemului

Sistemul este organizat în 9 module funcționale, fiecare corespunzând unui contur din Conceptul HG 530/2025. Implementarea detaliată a fiecărui modul este prezentată în secțiunea 5.

Modul	Scop principal

1. Administrare	Gestionare utilizatori/roluri (RBAC), configurare sistem, integrare MPass, interfață multilingvă, jurnalizare/audit
2. Managementul raportării cazurilor de violență	Formulare standardizate, UUID automat, clasificare tipuri violență, consimțământ, câmpuri violență online
3. Urmărirea cazurilor	Ciclul de viață al cazului (state machine), evaluare risc, plan intervenție
4. Urmărirea referirilor	Referiri către servicii medicale/juridice/sociale/adăpost, schimb date MConnect, principiul once-only
5. Caz de violență	Evidența plângerilor, denunțurilor, autodenunțurilor, sesizărilor și a altor informații despre actele de violență; evidența cazurilor înregistrate de violență împotriva femeilor și violență în familie
6. Evidența măsurilor de protecție	Ordine de restricție de urgență și ordonanțe de protecție emise de instanțele de judecată, monitorizare termene, blocare închidere caz
7. Raportare și analiză	Rapoarte standard/personalizate, tablouri de bord interactive, recepție rezultate analiză tendințe rețele sociale, export PDF/CSV/Excel
8. Acces autorizat	Autentificare MPass și control al accesului bazat pe roluri (RBAC), separare date publice/confidențiale
9. Gestionarea nomenclatoarelor	CRUD nomenclatoare prin interfață grafică, versionare, dezactivare fără ștergere

Monitorizarea violenței online este acoperită transversal prin Modulele 2 (câmpuri dedicate în fișa cazului), 3 (recepție rezultate de la sistemul terț de analiză a rețelelor sociale — 5.13 și SO-02) și 7 (rapoarte personalizate pe baza acestor date — 5.7.1.3), fără a constitui un contur distinct peste cele 9 prevăzute în Livrabil 5.

4.4 Rolurile utilizatorilor

Rol	**Descriere**	**Acces principal**
Administrator de sistem	Gestionare utilizatori, roluri, nomenclatoare, configurare sistem	Modulul Administrare, Nomenclatoare
Manager de caz	Asistenți sociali, ofițeri poliție - gestionare cazuri, evaluări, planuri intervenție	Module 2, 3, 4, 5

Utilizator raportor	Medici, educatori, ONG-uri - raportare cazuri noi, actualizare informații	Modulul 2 (creare), Modulul 3 (vizualizare limitată)
Analist / Raportor	Personal ANPCV, decidenți - rapoarte, statistici, tablouri de bord	Modulul 6
Auditor	Verificare jurnale, audit ex-post, control conformitate	Jurnale audit, istoric modificări
Utilizator public	Acces la date agregate publice	Interfață publică (doar date anonimizate)

4.5 Fluxurile de lucru principale

Fluxurile de lucru implementează integral scenariile operaționale SO-01 - SO-09 din caietul de sarcini:

SO-01: Înregistrarea unui caz de violență

1. Utilizatorul autorizat se autentifică prin MPass
2. Inițiază crearea unui caz nou din interfața dedicată
3. Sistemul generează automat UUID-ul cazului (nemodificabil)
4. Utilizatorul completează formularul standardizat de raportare a incidentului 4a. Opțional: utilizatorul poate înregistra locația incidentului (adresă, localitate și/sau coordonate GPS) prin câmpul de geo-etichetare integrat în formular (HTML5 Geolocation API sau introducere manuală); funcționalitate cu respectarea cerințelor de protecție a datelor și controlului accesului
5. Sistemul validează datele (client + server): câmpuri obligatorii, formate, consistență
6. La salvare, cazul este setat în starea „Deschis"
7. Sistemul verifică potențiale duplicate (fuzzy matching pe IDNP/nume victimă) și avertizează
8. Toate acțiunile sunt jurnalizate automat în MLog

SO-02: Evaluarea riscului

1. Utilizatorul selectează un caz existent în starea „Deschis" sau „În desfășurare"
2. Inițiază evaluarea riscului din fișa cazului
3. Completează criteriile de evaluare conform metodologiei aplicabile
4. Sistemul calculează/înregistrează nivelul de risc
5. Pentru cazuri online: sistemul primește automat rezultatul de analiză de la instrumentul de monitorizare UNFPA (sistem extern) - VioData recepționează clasificarea violenței, nu o generează
6. Evaluarea este versionată și salvată - evaluările anterioare rămân accesibile
7. Evaluarea este obligatorie înainte de crearea planului de intervenție

SO-03: Elaborarea planului de intervenție

1. Utilizatorul selectează un caz evaluat (cu evaluare de risc completată)
2. Creează planul de intervenție
3. Definește acțiuni concrete, responsabili și termene pentru fiecare acțiune
4. Planul este salvat și asociat cazului
5. Planul este obligatoriu pentru cazurile active
6. Modificările sunt jurnalizate; istoricul planurilor este păstrat integral

SO-04: Monitorizarea și actualizarea cazului

1. Utilizatorul accesează fișa cazului
2. Actualizează informații relevante (inclusiv date recepționate de la instrumentul de monitorizare UNFPA, pentru cazuri cu componentă online)
3. Adaugă note, documente, observații
4. Modifică starea cazului conform regulilor de tranziție
5. Stările sunt controlate: tranzițiile nepermise sunt blocate
6. Toate modificările sunt salvate cu istoric complet

SO-05: Referirea către servicii și instituții

1. Utilizatorul inițiază o referire din fișa cazului
2. Selectează tipul de serviciu (medical, juridic, social, adăpost)
3. Completează datele necesare referirii
4. Sistemul transmite referirea (prin MConnect unde aplicabil)
5. Referirea primește identificator unic, este asociată cazului
6. Statusul referirii este actualizat pe măsură ce serviciul furnizează feedback

SO-06: Monitorizare ordine de restricție și ordonanțe de protecție

1. Sistemul verifică periodic existența măsurilor active (cron job)
2. Verifică termenele ordinelor de restricție și ordonanțelor de protecție din sistemele informaționale externe (prin MConnect)
3. Generează alertă înainte de expirare (MNotify)
4. Marchează ordinul/ordonanța ca „Expirat/ă" la termen
5. Actualizează starea în fișa cazului
6. Blochează închiderea cazului dacă există măsuri active

SO-07: Gestionarea nomenclatoarelor

1. Utilizatorul autorizat (administrator) accesează „Administrare nomenclatoare"
2. Creare: selectează „Nomenclator nou", completează denumire, descriere, adaugă valori inițiale, salvează
3. Modificare: selectează nomenclator existent, modifică/dezactivează valori
4. Datele istorice rămân intacte la modificare
5. Toate operațiunile sunt salvate cu versionare și jurnalizare

SO-08: Închiderea cazului

1. Utilizatorul solicită închiderea cazului
2. Completează justificarea închiderii
3. Sistemul validează condițiile: verifică absența măsurilor de protecție active, verifică completitudinea dosarului
4. Starea cazului se schimbă în „Închis"
5. Cazul este arhivat logic (nu este șters)
6. Cazurile închise nu pot fi șterse; redeschiderea este permisă doar cu rol autorizat
7. Toate acțiunile sunt jurnalizate

SO-09: Raportare și utilizare date agregate

1. Utilizatorul selectează perioada și criteriile de raportare
2. Sistemul agregă datele conform parametrilor
3. Indicatorii naționali sunt calculați automat
4. Raportul este generat și afișat
5. Raportul poate fi exportat în PDF, CSV sau Excel

4.6 Integrări

Integrări cu servicii e-Guvernare:

Serviciu	Protocol	Scop	Mecanism
MPass	SAML 2.0	Autentificare și autorizare utilizatori	ITfoxtec.Identity.Saml2; redirect SSO; preluare atribute utilizator și roluri
MSign	REST API	Semnătură electronică documente	Semnare documente de ieșire, rapoarte oficiale
MNotify	REST API	Notificări electronice	Alerte expirare măsuri protecție, schimbări stare caz, notificări referiri
MLog	REST API	Jurnalizare acțiuni și evenimente	Toate acțiunile utilizatorilor și evenimentele de sistem
MConnect	REST sincron + Events asincron	Interoperabilitate cu sisteme externe	Schimb date cu cele 11 SIA; cache local Redis

Integrări cu sisteme informaționale externe prin MConnect:

Sistem extern	Instituție	Direcția schimbului	Date schimbate	Mecanism
SIA Registrul de Stat al Populației	Agenția Servicii Publice	Consum	Date identificare persoane (IDNP, nume, adresă)	MConnect
SIA Registrul de Stat al Unităților Administrativ-Teritoriale	ASP	Consum	Clasificator localități, regiuni	MConnect
SI „eSocial"	MMPS	Bidirecțional	Date servicii sociale, prestații, planuri de intervenție, evitarea dublei raportări	MConnect
SI „Asistență Socială"	MMPS	Consum	Date servicii sociale acordate	MConnect

SI „Vulnerabilitatea energetică"	MMPS	Consum	Date vulnerabilitate energetică a persoanelor implicate	MConnect
SI Determinarea Dizabilității și Capacității de Muncă	CNDCCM	Consum	Informații dizabilitate victimă/agresor	MConnect
SI înregistrare statut de șomer	ANOFM	Consum	Date privind statutul de șomer	MConnect
SIA Asistența Medicală Primară	Ministerul Sănătății	Consum	Date medicale relevante cazului	MConnect
SIA Compania Națională de Asigurări în Medicină	CNAM	Consum	Informații asigurare medicală	MConnect
SIA Compania Națională de Asigurări Sociale	CNAS	Consum	Date asigurări sociale	MConnect
SI Registrul Informației Criminalistice și Criminogene	IGP	Consum	Antecedente penale, profil de risc al agresorului	MConnect
SI Evidența contravențiilor și cauzelor contravenționale	IGP	Consum	Sancțiuni contravenționale pentru acte de violență	MConnect
Registrul electronic CJF (Centrul de Justiție Familială)	IGP	Consum	Date adăposturi, centre de plasament/criză	MConnect
SI „Urmărire penală: E-Dosar"	Procuratura Generală	Consum	Stadiul urmăririi penale, măsuri preventive, decizii	MConnect
SI Programul Integrat de Gestionare a Dosarelor în Instanțe	ADJ	Consum	Ordonanțe de protecție, hotărâri și decizii judiciare	MConnect

SI Registrul agresorilor - violență în familie	IGP	Bidirecțional	Evidența agresorilor	MConnect
SI Migrație (IGM)	IGM	Consum	Date migrație persoane implicate	MConnect
SI Registrul persoanelor reținute, arestate și condamnate	ANP	Consum	Statut detenție agresor, dată eliberare (*în dezvoltare, fără capacitate de integrare la momentul actual)	Direct (viitor)
SI Management în Educație	MEC	Consum	Date instituție de învățământ, prezență, transferuri școlare minori (*fără capacitate MConnect la momentul actual)	Acord direct (viitor)
SIA CNAJGS	CNAJGS	Bidirecțional	Înregistrarea referirilor pentru asistență juridică gratuită (*nu este pe MConnect)	Acord direct pentru schimb de date
Instrument monitorizare UNFPA	UNFPA	Consum	Rezultate monitorizare cazuri potențiale de violență online (*în dezvoltare)	Acord direct pentru schimb de date

Principii de interoperabilitate implementate:

1. **Once-only** - datele sunt colectate o singură dată de la sursa primară și reutilizate
2. **Separarea rolurilor** - SI RS VioData are rol clar (furnizor/consumator) față de fiecare sistem
3. **Trasabilitate** - fiecare schimb de date este jurnalizat și auditat
4. **Securitate** - datele sunt protejate pe întreg fluxul de schimb (TLS, validare, autorizare)
5. **Standardizare** - schimbul se realizează exclusiv prin MConnect (interzis point-to-point)

4.7 Fluxurile de date

Fluxul principal de date:

Utilizator -> Frontend (Blazor) -> API Gateway (ASP.NET Core) -> Module aplicație -> PostgreSQL/Redis/Elasticsearch

Fluxul de interoperabilitate:

Modul aplicație -> Adaptor integrare -> Cache MConnect (Redis) -> MConnect API -> Sistem extern (SIA)

Fluxul asincron (notificări, evenimente):

Eveniment sistem -> Event Stream (Hangfire/Redis) -> Workers: Notificări (-> MNotify), Audit (-> MLog + Elasticsearch), Recepție UNFPA (-> Instrument monitorizare UNFPA)

Fluxul de raportare:

Date brute (PostgreSQL) -> Materialized views / Pre-computed aggregates -> Endpoint GraphQL (Hot Chocolate) care permite interogări precise și dinamice -> ApexCharts.Blazor vizualizări -> Export (PDF/CSV/Excel)

4.8 Rapoarte și tablouri de bord

Tablou de bord executiv (ANPCV):

- Numărul total cazuri pe perioadă, tip violență, regiune
- Tendințe și evoluții (grafice lineare)
- Distribuție geografică (hartă interactivă PostGIS + OpenStreetMap)
- Indicatori naționali conform Conceptului
- Statistici violență online

Tablou de bord operațional (manageri de caz):

- Cazurile active ale utilizatorului curent
- Cazuri cu măsuri de protecție ce expiră
- Referiri în așteptare
- Alerte și notificări
- Statistici personale (cazuri gestionate, timpi medii)

Rapoarte statistice:

- Rapoarte standard cu indicatorii naționali prevăzuți în Concept
- Rapoarte dezagregate pe: sex, vârstă, tip violență, mediu reședință, online/offline
- Rapoarte per instituție raportoare
- Rapoarte per regiune/localitate
- Rapoarte tendințe rețele sociale

Export: PDF (QuestPDF), CSV, Excel (ClosedXML) - pentru toate rapoartele.

4.9 Design responsive, accesibilitate și conformitate MUD

Design web adaptiv (320px-1600px) cu MudBlazor responsive grid, conformitate WCAG nivel A cu audit automat axe-core în CI/CD. Detaliile tehnice sunt prezentate în secțiunile 5.1.2 (accesibilitate) și 5.1.3 (suport dispozitive multiple).

Conformitate Modelul Unitar de Design (MUD):

Toate ecranele SI RS VioData sunt proiectate și implementate conform MUD. În faza de design, specialistul UX/UI lucrează direct cu biblioteca Figma oficială MUD pentru a construi wireframe-urile și prototipurile, asigurând că paleta de culori, tipografia și spacing-ul sunt identice cu standardul guvernamental înainte de a scrie orice linie de cod.

În implementare, variabilele CSS ale MUD (culori, spacing, tipografie) sunt importate din repository-ul GitLab oficial și aplicate prin MudThemeProvider - componentele MudBlazor nu conțin valori hardcodate, ci referențiază exclusiv acești tokens. Aceasta înseamnă că orice actualizare viitoare a standardului MUD se propagă automat în sistem printr-o singură modificare de configurație. Când AGE va lansa biblioteca Blazor nativă MUD (estimat 2026), tranziția va fi transparentă.

Elementele care țin de identitatea vizuală a instituției (culori secundare ANPCV, imagini, texte) sunt personalizate în limitele permise de MUD. Pentru componentele fără echivalent în MUD - formularul de evaluare a riscului, vizualizarea hărții cazurilor - echipa le proiectează respectând aceleași principii (grid, culori, tipografie) și le supune validării AGE înainte de implementare.

5. Răspunsul la cerințele funcționale

5.1 Cerințe de utilizare și design

5.1.1 Interfață utilizator multilingvă

Implementare cu IStringLocalizer / IHtmlLocalizer din ASP.NET Core, cu fișiere de resurse (.resx) separate per modul funcțional:

- Limba implicită: română (acuratețe 100%)
- Limbi adiționale: rusă, engleză
- Fișiere de resurse .resx, gestionate per modul
- Comutare limbă dinamică fără reîncărcare pagină (RequestLocalizationMiddleware)
- Nomenclatoarele și valorile controlate sunt traduse în toate cele 3 limbi
- Validarea completitudinii traducerilor este inclusă în pipeline CI/CD

5.1.2 Accesibilitate

Conformare WCAG nivel A asigurată prin:

- Componente MudBlazor cu suport accessibility built-in (atribute ARIA, focus management)
- Navigare completă cu tastatura
- Contrast suficient text/fundal (raport minim 4.5:1)
- Texte alternative pentru elemente grafice
- Structură semantică HTML (headings, landmarks, labels)
- Audit automat axe-core în pipeline CI/CD - build-ul eșuează la violări nivel A
- Testare manuală cu screen reader (NVDA/VoiceOver)

5.1.3 Suport dispozitive multiple

- Design web adaptiv cu MudBlazor responsive grid (MudGrid, MudItem, Breakpoint)
- Breakpoints: 320px (smartphone), 576px, 768px (tabletă), 992px, 1200px, 1600px (desktop)
- Layout-uri adaptive: MudDrawer colapsabil pe mobile, MudTable cu scroll horizontal pe ecrane mici
- Formulare adaptate: câmpuri stacked pe mobile, grid pe desktop
- Testare pe dispozitive reale și emulatoare (Chrome DevTools)

5.2 Contur funcțional: Administrare

5.2.1 Administrarea utilizatorilor și rolurilor

Implementare:

- Interfață grafică dedicată pentru CRUD utilizatori (creare, modificare, activare, dezactivare, ștergere)
- Asociere utilizator cu unul sau mai multe roluri prin interfață drag-and-drop / multi-select
- Definirea drepturilor de acces în funcție de rol, modul și obiect informațional - matrice de permisiuni configurabilă
- Integrare MPass (SAML 2.0) via ITfoxtec.Identity.Saml2:
  - Autentificarea utilizatorilor prin redirect SSO
  - Preluarea atributelor utilizator din assertion SAML
  - Gestionarea rolurilor pe baza atributelor MPass + roluri locale
- Fiecare utilizator are cel puțin un rol activ
- Reflectare imediată a modificărilor rolurilor/drepturilor în comportamentul sistemului (invalidare cache sesiune)
- Blocare acces utilizatori fără rol valid

Tehnologii: ASP.NET Core Authorization Policies (RolesAuthorizationHandler, PermissionsHandler), policy-based authorization, Blazor CascadingAuthenticationState pentru starea rolurilor pe frontend.

Criterii de acceptanță validate: a) CRUD utilizatori fără intervenție tehnică b) Minimum 3 roluri cu drepturi distincte demonstrate c) Autentificare MPass funcțională d) Reflectare imediată modificări roluri e) Blocare acces fără rol valid

5.2.2 Securitate, jurnalizare și audit

Implementare:

- Jurnalizare automată a tuturor acțiunilor utilizatorilor și evenimentelor de sistem: autentificări, accesări/modificări date, schimbări stare cazuri, operațiuni administrative
- Integrare MLog prin REST API - fiecare eveniment este transmis sincron/asincron
- Structura înregistrării de audit: identificator utilizator, dată/oră, tip acțiune, obiect afectat, valori anterioare/noi
- Jurnale consultabile de utilizatori autorizați (rolul Auditor)
- Filtrare: pe utilizator, perioadă, tip acțiune, obiect
- Export jurnale: CSV, Excel
- Posibilitate audit ex-post pentru un caz selectat - reconstituirea cronologică a tuturor acțiunilor

Tehnologii: ASP.NET Core Action Filters / Middleware pentru capturare automată acțiuni, Hangfire pentru transmitere asincronă la MLog, Elasticsearch pentru stocare și căutare rapidă jurnale.

5.3 Contur funcțional: Managementul raportării cazurilor de violență

5.3.1 Înregistrarea cazurilor de violență

Implementare:

- Formular standardizat construit cu Blazor EditForm + validare FluentValidation (reguli partajate frontend-backend)
- Generare automată UUID v4 la inițierea cazului - unic, stabil, nemodificabil

- Câmpuri formular minim: date victimă (nume, IDNP, vârstă, sex, adresă), date agresor, tipul violenței (clasificator nomenclator), circumstanțele violenței, instituția raportoare (meniu prestabilit)
- Validare câmpuri obligatorii: pe client (feedback instant) și pe server (securitate)
- Blocarea salvării cazului dacă lipsesc câmpuri obligatorii
- Pentru violență online: câmpuri dedicate - link postare, canal/platformă monitorizare
- După salvare: cazul vizibil în lista de cazuri, accesibil conform rolului
- Verificare deduplicare: fuzzy matching pe IDNP/nume victimă - avertizare utilizator la potențiale duplicate
- Persistență și afișare corectă la reîncărcare

5.3.2 Consimțământ și confidențialitate

Implementare:

- Formular electronic de consimțământ pentru prelucrarea datelor cu caracter personal
- Înregistrare explicită: tip consimțământ, data, versiunea, persoana informată
- Acces la date sensibile controlat pe roluri - vizibilitate diferențiată (demonstrabilă între minimum 2 roluri)
- Toate accesările datelor cu caracter personal jurnalizate automat
- Informarea victimei privind modul de utilizare a datelor (text informativ afișat)

5.4 Contur funcțional: Urmărirea cazurilor

5.4.1 Monitorizarea ciclului de viață al cazului

Implementare:

- State machine implementat cu pattern configurat în baza de date (reguli de tranziție editabile de administrator):
  - Stări: Deschis -> În desfășurare -> Referit -> Închis / Respins / Inactiv
  - Reguli: ex. „Închis" doar dacă nu există măsuri de protecție active; „Referit" doar din „În desfășurare"
- Tranzițiile nepermise blocate automat - butonul de acțiune nu este afișat sau este dezactivat
- Fiecare schimbare de stare jurnalizată cu: utilizator, timestamp, starea anterioară, starea nouă, motivul
- Starea curentă vizibilă clar în interfață (badge colorat, label text)

Tehnologii: Tabel PostgreSQL case_state_transitions cu regulile de tranziție; ASP.NET Core service cu validare înainte de save; Blazor component cu butoane condiționate de tranzițiile permise.

5.4.2 Evaluarea riscului și planul de intervenție

Implementare:

- Formular evaluare risc cu criterii structurate (configurabile prin nomenclatoare)
- Asociere evaluare cu cazul concret (relație 1:N - un caz poate avea multiple evaluări)
- Versionare: fiecare evaluare nouă creează o versiune; versiunile anterioare accesibile readonly
- Evaluare obligatorie înainte de crearea planului de intervenție (validare la nivel de business rule)
- Plan de intervenție: tabel acțiuni cu coloane - descriere acțiune, responsabil (selectat din utilizatori), termen (date picker), status
- Import date din SI „eSocial" (prin MConnect): planurile de acțiune/intervenție personalizate sunt gestionate în modulul de management de caz din eSocial; VioData importă structura minimă: ID plan / ID caz, Statut caz, Lista acțiuni, Responsabil, Termen de implementare
- Planul actualizabil pe durata ciclului de viață al cazului

- Modificările salvate și jurnalizate

5.5 Contur funcțional: Urmărirea referirilor

5.5.1 Gestionarea referirilor

Implementare:

- Creare referire din fișa cazului: selectare tip serviciu (medical, juridic, social, adăpost) din nomenclator
- Fiecare referire: identificator unic, dată, tip serviciu, instituție destinatară, motiv, status
- Status actualizabil: Inițiată -> Transmisă -> Acceptată -> În curs -> Finalizată / Respinsă
- Istoric complet referiri vizibil per caz (tab dedicat în fișa cazului)
- Referirile corect corelate cu cazul (relație 1:N)

5.5.2 Interoperabilitatea referirilor

Implementare:

- Transmitere/recepționare date referiri prin MConnect REST API
- MConnect Events (asincron) pentru notificare schimbare status referire
- Structura datelor documentată în specificații OpenAPI
- Demonstrare schimb de date real sau simulat cu sistem extern
- Gestionare erori integrare: logging, retry cu exponential backoff, notificare utilizator
- Respectarea principiului once-only

5.6 Contur funcțional: Evidența măsurilor de protecție

5.6.1 Evidența măsurilor de protecție

Implementare:

- Formular evidență ordine de restricție de urgență: autoritate emitentă, număr/dată ordin, perioadă aplicare, tipuri restricții (nomenclator), statut (activ/expirat/revocat)
- Formular evidență ordonanțe de protecție: instanță emitentă, număr/dată ordonanță, perioadă, măsuri dispuse (nomenclator), statut
- Corelare: ordinele asociate cu cazul ȘI agresorul; ordonanțele asociate cu cazul ȘI victima
- Monitorizare automată termene: cron job verifică zilnic; alertă MNotify cu X zile înainte de expirare (configurabil); marcare automată „Expirat"
- Audit complet al tuturor operațiunilor

5.6.2 Corelarea și vizualizarea

Implementare:

- Secțiune dedicată în fișa cazului: vizualizare centralizată toate ordinele și ordonanțele active/istorice
- Validare business: blocare închidere caz dacă există măsuri active (eroare cu mesaj explicit)
- Excepții: utilizatori cu rol superior pot forța închiderea (cu justificare obligatorie, jurnalizată)
- Corelări realizate tehnic (foreign keys + business logic), nu doar procedural

5.7 Contur funcțional: Raportare și analiză

5.7.1 Raportare operațională și statistică

Implementare:

- Rapoarte standard predefinite: raportul standard obligatoriu este „Raportul statistic conform Setului de indicatori naționali în domeniul prevenirii și combaterii violenței împotriva femeilor și a violenței în familie", aprobat prin Hotărâre de Guvern; acesta acoperă toți indicatorii naționali din Concept; rapoartele dezagregate (per instituție raportoare, per regiune, per tip violență, tendințe violență online) sunt incluse ca rapoarte predefinite suplimentare în implementare
- Rapoarte personalizate: query builder vizual - selectare dimensiuni, metrici, filtre, perioadă
- Recepționare rezultate analiză tendințe rețele sociale -> rapoarte personalizate violență online
- Calcul indicatori: agregări PostgreSQL (materialized views pentru performanță) + Elasticsearch pentru serii temporale și căutare rapidă
- Filtrare: perioadă, regiune, tip violență, instituție, mediu (offline/online), sex, vârstă
- Export funcțional: PDF (QuestPDF cu template-uri), CSV (stream direct), Excel (ClosedXML)
- Verificare: datele din raport corespund datelor din sistem (teste automate de consistență)

5.7.2 Tablouri de bord și analiză

Implementare:

- Tablouri de bord construite cu MudBlazor Charts + ApexCharts.Blazor: grafice liniare, baruri, pie charts, heatmaps, hărți
- Configurabilitate prin filtre, indicatori și vizualizări: utilizatorul aplică filtre dinamice (perioadă, regiune, tip violență etc.), selectează indicatorii afișați și tipul de vizualizare (grafic liniar, bar, pie, hartă)
- Filtrare interactivă: datele se actualizează dinamic la schimbarea filtrelor
- Vizualizări lizibile și coerente pe toate dimensiunile de ecran
- Accesibilitate tablouri conform rolului (dashboard diferit per rol)
- Actualizare date: la fiecare accesare sau la interval configurabil (polling)

5.8 Contur funcțional: Crearea și administrarea nomenclatoarelor

5.8.1 Crearea, modificarea și administrarea nomenclatoarelor interne

Implementare:

- Interfață grafică dedicată în panoul de administrare
- Creare nomenclator: denumire, descriere, scop, lista valorilor permise (editabil inline), statut, data intrării în vigoare
- Adăugare valori noi: câmp text + salvare
- Modificare valori existente: edit inline
- Dezactivare valori: soft delete - valoarea nu mai apare în selecțiile noi, dar rămâne vizibilă în înregistrările istorice
- Activare/dezactivare nomenclator complet
- Fără intervenție tehnică necesară
- Jurnalizare: fiecare operațiune înregistrată cu utilizator, timestamp, valoare anterioară/nouă

5.8.2 Utilizarea nomenclatoarelor în actele de evidență

Implementare:

- Nomenclatoarele sunt încărcate automat în formularele relevante ca dropdown-uri cu căutare (MudSelect / MudAutocomplete)
- Prevenirea valorilor libere: câmpurile controlate de nomenclator nu permit input liber

- Validare server-side: valorile trimise sunt verificate contra nomenclatorului activ
- La dezactivarea unei valori din nomenclator: înregistrările existente rămân neafectate, noile înregistrări nu mai pot selecta valoarea

5.9 Contur funcțional: Acces autorizat și interfață publică

5.9.1 Acces autorizat

Implementare:

- Autentificare exclusiv prin MPass (SAML 2.0) - nu există login local
- La autentificare: preluare atribute utilizator, mapare roluri, creare sesiune
- Interfață personalizată pe rol: meniu lateral, dashboard, acțiuni disponibile - toate condiționate de permisiunile rolului
- Funcționalități neautorizate: nu sunt doar ascunse, ci inaccesibile (verificare pe server la fiecare request)
- Notificări afișate corect utilizatorilor vizați (filtrate pe rol/caz)

5.9.2 Acces public

Implementare:

- Pagină publică separată (rută diferită, fără autentificare)
- Afișează exclusiv date agregate și anonimizate (statistici generale, tendințe)
- Separare strictă la nivel de API: endpoint-uri publice nu au acces la tabelele cu date personale
- Zero acces public la date cu caracter personal - garantat prin arhitectura API-ului
- Accesul public respectă cadrul guvernamental privind portalurile unice de acces la servicii publice electronice (5.9.2.2)

5.10 Documentele de bază ale registrului

Abordarea tehnică pentru gestionarea documentelor

Gestionarea documentelor de bază ale registrului VioData va fi implementată nativ în cadrul aplicației SI RS VioData, fără dependențe de sisteme DMS externe. Documentele sunt asociate obiectelor informaționale (cazuri, referiri, măsuri de protecție) și stocate în infrastructura MCloud, cu acces controlat prin rolurile RBAC existente. Funcționalități implementate:

- **Stocare și asociere documente**: upload, versionare și asociere document ↔ caz (relație directă în baza de date)
- **Control acces**: acces restricționat conform rolurilor VioData și autentificării MPass
- **Audit și jurnalizare**: jurnalizare completă a operațiunilor pe documente, integrare MLog
- **Export și interoperabilitate**: API REST pentru export documente în format standard

5.10.1 Clasificare

Sistemul gestionează trei categorii de documente:

- **Documente de intrare:** formulare de raportare a indicatorilor, cereri, sesizări, notificări, fișe de referire, date raportate de instituții partenere

- **Documente de ieșire:** notificări privind statutul cazului, decizii asupra cazurilor, rapoarte statistice și analitice, rapoarte de activitate
- **Documente tehnologice:** șabloane formulare, nomenclatoare/clasificatori, ghiduri utilizare, jurnale audit, politici utilizare sistem

5.10.2 Documente de intrare

- Creare și completare prin formulare electronice standardizate (Blazor EditForm)
- Fiecare document asociat unui caz/raportare/proces specific + identificator unic
- Validare automată conform regulilor de business: completitudine date, câmpuri obligatorii
- Versionare documente modificate (tabel document_versions)

5.10.3 Documente de ieșire

- Generare automată pe baza datelor din sistem (template engine)
- Vizualizare în sistem, descărcare PDF/CSV/Excel
- Transmitere prin MNotify
- Marcate cu dată, oră, autor; păstrate în arhiva electronică

5.10.4 Documente tehnologice

- Administrare prin interfață dedicată (permisă doar utilizatorilor autorizați)
- Jurnalizare, versionare, rollback la versiunea anterioară

5.10.5 Trasabilitate

- Trasabilitate completă: cine a creat, cine a modificat, când, în ce context
- Istoric complet consultabil per document
- Incluse în mecanismele de audit intern și extern

5.10.6 Arhivare

- Arhivare conform legislației naționale și regulamentelor interne
- Acces la documente arhivate controlat pe bază de rol
- Export documente arhivate pentru control și audit

5.11 Obiecte informaționale și identificatori

5.11.1 Obiectele informaționale de bază

Sistemul gestionează 14 obiecte informaționale:

Obiect	Descriere	Identificator
Caz de violență	Obiect principal - incident sau set incidente corelate	UUID v4
Victimă	Date persoană afectată	UUID v4 + IDNP (unde permis)
Agresor	Date persoană presupusă/confirmată agresor	UUID v4 + IDNP (unde permis)

Incident de violență	Eveniment concret, asociat unui caz	UUID v4
Evaluare de risc	Analiza riscurilor asociate cazului	UUID v4
Plan de intervenție	Măsuri stabilite pentru gestionarea cazului	UUID v4
Referire	Transmiterea cazului/victimei către serviciu/instituție	UUID v4
Serviciu furnizat	Serviciul efectiv acordat	UUID v4
Raport și indicator	Date agregate, indicatori, rezultate raportare	UUID v4
Document	Documente intrare, ieșire, tehnologice	UUID v4
Utilizator	Persoana autorizată să utilizeze sistemul	UUID v4 + IDNP
Rol și permisiune	Drepturile de acces	UUID v4
Nomenclator / clasificator	Liste controlate de valori	UUID v4
Înregistrare de audit (log)	Evidența activităților	UUID v7 (time-sortable)

5.11.2 Identificatori unici

- UUID v4 generat automat de sistem pentru toate obiectele informaționale (caz, victimă, agresor etc.)
- Excepție: înregistrările de audit utilizează UUID v7 (time-sortable) pentru performanță optimă la scriere secvențială și interogări pe intervale de timp
- Unicitate la nivel de sistem, stabilitate în timp (nu se modifică), imposibilitate reutilizare
- Utilizare în toate relațiile dintre obiecte
- Asociere cu IDNP (identificator național) pentru victimă, agresor, utilizator - unde permis legal
- Identificatorii interni utilizați în toate procesele operaționale

5.11.3 Relaționarea obiectelor

- Relații explicite implementate cu Entity Framework Core (foreign keys, relații N:M prin join entities):
  - Un caz poate include mai multe incidente
  - Un caz poate avea una sau mai multe victime
  - Un caz poate include unul sau mai mulți agresori
  - Un caz poate avea mai multe evaluări de risc, referiri, servicii furnizate
- Relațiile documentate în DbContext (Fluent API), trasabile, reflectate în interfața utilizator

5.11.4 Versionare și istoric

- Tabel entity_versions pentru obiecte critice: date victimă, evaluări risc, planuri intervenție, stări caz

- Istoric include: versiunea anterioară (JSON diff), utilizatorul, data/ora modificării
- Versiunile anterioare nu pot fi șterse (immutable audit trail)

5.11.5 Validare, deduplicare și integritate

- Validare la nivel de obiect: FluentValidation (reguli partajate FE+BE)
- Deduplicare: detectarea înregistrărilor similare pe IDNP + nume la creare victimă/agresor
- Avertizare utilizator la potențiale duplicate - utilizatorul decide dacă e duplicat sau nu
- Reguli deduplicare configurabile (prag similaritate, câmpuri comparate)
- Integritate referențială garantată tehnic: foreign keys PostgreSQL, cascade rules

5.11.6 Audit și securitate

- Orice creare, modificare, vizualizare sau ștergere logică jurnalizată automat
- Acces controlat pe bază de rol și permisiuni (ASP.NET Core Authorization Policies)
- Obiecte cu date cu caracter personal: mascare pentru roluri fără acces, protejate conform legislației

5.11.7 Registrul victimelor și agresorilor

Conform cerinței din Livrabil 5 punctul 3 („Gestionarea și evidența registrului victimelor și a agresorilor în cazurile de violență"), sistemul asigură funcționalitatea de registru distinct pentru victime și pentru agresori:

- listare și căutare a victimelor și agresorilor, separat;
- profil consolidat al victimei (cazuri asociate, referiri, servicii furnizate, măsuri de protecție);
- profil consolidat al agresorului (cazuri asociate, ordine de restricție, ordonanțe de protecție);
- acces controlat pe bază de rol și jurnalizare a consultărilor, conform 5.11.6.

5.12 Scenarii operaționale

Toate cele 9 scenarii operaționale (SO-01 - SO-09) sunt implementate integral, conform descrierilor din secțiunea 4.5.

Fiecare scenariu este:

- Implementat ca flux funcțional end-to-end
- Guvernat de reguli de business clare (configurabile)
- Controlat prin stări și tranziții (state machine)
- Jurnalizat complet (audit trail)
- Testat automat (unit + integration + E2E) și manual (UAT)

5.13 Interoperabilitate și schimb de date

Principiile de interoperabilitate, tabelul integrărilor și mecanismele de schimb sunt prezentate în secțiunea 4.6; arhitectura fluxurilor sincrone/asincrone și mecanismele de reziliență în secțiunea 7.4.

Scenarii operaționale de interoperabilitate: a) Preluare date din sisteme externe pentru completarea automată a cazului - la introducerea IDNP, sistemul interoghează automat Registrul Populației b) Transmitere date către alte sisteme în urma unei referiri - la crearea referirii, datele sunt transmise prin MConnect c) Notificare prin evenimente la schimbarea stării cazului - publicare eveniment MConnect Events d) Sincronizare periodică a datelor relevante - cron job pentru actualizare ordine/ordonanțe e) Recepționare feedback privind serviciile furnizate - consum evenimente de la sisteme externe

Documentare:

- Specificații API OpenAPI/Swagger pentru toate endpoint-urile
- Diagrame flux de date per integrare
- Scenarii de testare pentru fiecare integrare
- Toate integrările supuse testelor de interoperabilitate și demonstrate în cadrul recepției

6. Răspunsul la cerințele nefuncționale

6.1 Tehnologii open-source și arhitectură

Stack-ul tehnologic complet este prezentat în secțiunea 4.2. Toate componentele sunt open-source: ecosistemul .NET (MIT), PostgreSQL (PostgreSQL License), Redis (BSD), Elasticsearch (SSPL/Elastic License), Docker și Kubernetes (Apache 2.0). Zero costuri de licențiere pentru componente software.

Arhitectură modulară:

- ASP.NET Core modules: fiecare contur funcțional = proiect/modul independent cu interfețe clare
- Interfețe interschimbabile: modulele comunică prin interfețe (dependency injection nativ ASP.NET Core), permițând înlocuirea/actualizarea individuală
- Frontend: component library internă (Razor Class Library), componente Blazor lazy-loaded

Conformitate Modelul Unitar de Design (MUD):

Abordarea completă privind MUD este detaliată în secțiunea 4.9. Non-conformitatea cu MUD blochează acceptanța livrabilului.

6.2 Mediul de sistem

Platforma Cloud Guvernamentală - MCloud:

- Găzduire pe Kubernetes (MCloud)
- Două medii pe MCloud: dezvoltare (development) și producție
- Atât mediul de dezvoltare, cât și mediul de producție sunt găzduite în MCloud, conform clarificărilor autorității contractante
- Mediu local Docker Compose: disponibil opțional pentru activități de debugging individual al dezvoltatorilor, fără a înlocui mediul de dezvoltare din MCloud

Containerizare și orchestrare:

- Docker multi-stage builds: build stage (dotnet publish) -> production stage (imagine minimă .NET Runtime Alpine)
- Kubernetes: deployment-uri separate pentru frontend (Blazor Server), backend (ASP.NET Core API), workers (Hangfire)
- Helm charts: gestionare deployment-uri cu versiuni controlate, revenire rapidă, configurare declarativă
- Health checks: liveness + readiness probes pentru fiecare serviciu (ASP.NET Core Health Checks)

CI/CD și DevOps:

- Azure DevOps: gestionarea livrărilor, sarcinilor și erorilor
- GitLab CI/CD: pipeline automate per commit

  - Stage 1: dotnet format + analyzers
  - Stage 2: unit tests + integration tests (dotnet test)
  - Stage 3: build Docker images (dotnet publish)
  - Stage 4: deploy development (automat) / producție (manual approval)
- GitLab: controlul versiunilor, code review, merge requests
- Branching strategy: main -> develop -> feature branches; merge cu squash

Monitorizare și SRE:

- Centralizare prin Azure DevOps
- Prometheus: colectare metrici (request rate, error rate, latency, resource usage)
- Grafana: dashboards vizualizare metrici, alerte
- ELK Stack (Elasticsearch + Logstash + Kibana): centralizare logs, vizualizare, căutare
- Alerting: Grafana alerts -> email / MNotify pentru echipa tehnică

6.3 Interoperabilitate

- REST API documentat complet cu OpenAPI 3.0 / Swagger (auto-generat de Swashbuckle.AspNetCore) - dedicat integrărilor cu MConnect și serviciile guvernamentale
- GraphQL API (Hot Chocolate) - furnizează o schemă puternic tipizată pentru interogările aplicației web client (Blazor) și pentru extragerea dinamică a datelor destinate raportării, implementat în conformitate cu cerința de a utiliza standarde din industrie
- Formate date: JSON (primar), CSV și XML pentru export
- Standarde respectate: REST, JSON Schema, HTTP status codes standard Tabelul complet al integrărilor (sisteme externe, direcția schimbului, mecanisme) este prezentat în secțiunea 4.6; arhitectura fluxurilor și reziliența în secțiunea 7.4.

6.4 GPS Geo-etichetare

Frontend:

- HTML5 Geolocation API pentru captarea coordonatelor din browser (cu consimțământul utilizatorului)
- Vizualizare hărți: Leaflet.Blazor + OpenStreetMap (open-source, zero costuri licență, integrare nativă în ecosistemul Blazor)
- Componente hartă: marcaje cazuri, heatmap zone, clustering
- API endpoints securizate (REST / GraphQL) pentru actualizarea/interogarea locațiilor

Backend:

- PostgreSQL cu extensia PostGIS pentru stocare și indexare geospațială
- Tip de date: POINT (latitudine/longitudine) pentru fiecare caz/incident
- Interogări geospațiale: proximitate, zonare, agregări pe regiune
- API endpoints securizate pentru actualizarea/interogarea locațiilor (REST, autorizate pe rol)

6.5 Securitatea sistemului

OWASP Top 10:2025 - măsuri specifice:

1. Broken Access Control: RBAC cu ASP.NET Core Authorization Policies, verificare pe fiecare request, principiul least privilege

2. Security Misconfiguration: ASP.NET Core Security Middleware (HSTS, CSP, X-Frame-Options), CORS restrictiv, headers securitate, configurații hardened pentru prod; toate secretele (credențiale, API keys, connection strings) injectate ca variabile de mediu la runtime prin secrets manager centralizat - fără hardcodare (detalii în secțiunea 11.8)
3. Software Supply Chain Failures: Dependabot, dotnet list package --vulnerable automat, verificare integritate pachete NuGet
4. Cryptographic Failures: TLS 1.3, AES-256 at rest, mascare date sensibile, fără algoritmi deprecați
5. Injection: Entity Framework Core (parameterized queries), validare FluentValidation, input sanitization, System.Text.Json (nu XML)
6. Insecure Design: threat modeling la nivel de arhitectură, separare responsabilități, defense-in-depth
7. Authentication Failures: MPass (SSO guvernamental), sesiuni securizate, rate limiting la autentificare, blocaj cont după tentative eșuate
8. Software or Data Integrity Failures: System.Text.Json cu JsonSerializerOptions restrictive, validare semnături pentru actualizări, CI/CD pipeline securizat
9. Security Logging and Alerting Failures: jurnalizare completă MLog, Elasticsearch, alerte automate pe evenimente suspecte, retenție loguri audit
10. Mishandling of Exceptional Conditions: gestionare uniformă a excepțiilor (middleware global), fără expunere stack trace în producție, fallback-uri sigure

Conformitate:

- ISO/IEC 27001: principii de management al securității informațiilor implementate
- HG nr. 201/2017: cerințe minime obligatorii de securitate cibernetică respectate

Detaliile privind criptarea, managementul vulnerabilităților, practicile de dezvoltare securizată și gestionarea incidentelor sunt prezentate în secțiunea 11.

6.6 Protecția datelor

Conformitate GDPR (UE) 2016/679 și HG nr. 1123/2010: privacy by design, minimizare date, consimțământ explicit, drept de acces și ștergere (soft delete + anonimizare), portabilitate (JSON/CSV), clasificare pe niveluri de sensibilitate, jurnalizare completă. Detaliile sunt prezentate în secțiunea 11.7.

6.7 Scalabilitate și fiabilitate

Scalabilitate:

- Design: 500 utilizatori simultani (target nominal), scalabil la 1.000 în situații de urgență
- Scalare orizontală pe Kubernetes conform necesităților de trafic
- PostgreSQL: connection pooling (Npgsql / PgBouncer)
- Redis: caching distribuit

Fiabilitate:

- Disponibilitate target: 99.9% (≤8.76 ore downtime/an) conform cerinței 6.7
- Health checks: Kubernetes liveness + readiness probes
- Failover și recuperare în caz de dezastru conform cerinței 6.7 din caietul de sarcini
- Backup automat: PostgreSQL backup zilnic (pg_dump) + WAL archiving pentru point-in-time recovery

6.8 Performanța sistemului

Metrică	SLA cerut	Soluție tehnică
Încărcare dosar de caz	≤ 2 secunde	Redis cache pentru date frecvent accesate; EF Core query optimization; lazy loading componente
Generare rapoarte standard	≤ 5 secunde	Materialized views PostgreSQL; pre-computed aggregates; cache rapoarte
Notificări în timp real	≤ 1 secundă	MNotify API
Latență API intern	≤ 50 ms	Npgsql connection pooling; Redis cache; ASP.NET Core middleware optimizat
Latență API extern (MConnect)	≤ 200 ms	Cache MConnect local (Redis cu TTL); request timeout configurabil
Procesare analiză la nivel de caz	≤ 10 secunde	Elasticsearch agregări; PostgreSQL window functions
Suport volume date	1M+ înregistrări	Indexare PostgreSQL (B-tree, GiST pentru PostGIS); paginare cursor-based; Elasticsearch pentru full-text search
Sincronizare date externe	≤ 1 sec/înregistrare	Hangfire workers paraleli; batch processing

Strategie de optimizare:

- Monitorizare query-uri lente (pg_stat_statements) și optimizare continuă
- Cache multi-nivel: browser (HTTP cache), aplicație (Redis), baza de date (materialized views)

6.9 Garanția și întreținerea sistemului

Garanție de 12 luni după încetarea contractului, cu mentenanță corectivă și adaptivă. Detaliile complete - SLA, categorii de mentenanță, delimitarea față de funcționalitate nouă, canale de suport și transfer de cunoștințe - sunt prezentate în secțiunea 13.

7. Arhitectura soluției

7.1 Arhitectura pe straturi

SI RS VioData utilizează o arhitectură pe straturi (layered architecture), cu separare clară a responsabilităților. Tehnologiile specifice per strat sunt detaliate în secțiunea 4.2.

Stratul 1: Interfață web pentru utilizatori (User Interface Layer)

- Module autentificate: **Blazor Server** cu MudBlazor, conformă MUD - rendering server-side, datele victimelor nu sunt niciodată expuse în browser; comunicare UI↔server prin conexiune SignalR persistentă
- Modul public (5.9.2): **Blazor WebAssembly** - date agregate anonimizate, fără state server per utilizator anonim, scalare independentă

Stratul 2: API Gateway

- ASP.NET Core Web API entry point
- Expune interfețele de comunicare permise: REST (pentru MConnect și servicii eGov) și GraphQL (pentru interfața web și rapoarte dinamice).
- Middleware pipeline: HSTS -> CORS -> Authentication -> Authorization -> Rate Limit -> Validation -> Controller / GraphQL Resolver

Stratul 3: Strat de aplicație (Application Layer)

- 9 module ASP.NET Core independente (unul per contur funcțional)
- Fiecare modul: Controllers -> Services -> Repositories (Clean Architecture)
- Event-driven communication între module (MediatR notifications)

Stratul 4: Strat de date (Data Layer)

- PostgreSQL 16+ (date relaționale + PostGIS), Redis (caching, coadă Hangfire), Elasticsearch (full-text search, jurnale audit)
- Entity Framework Core: acces type-safe, migrări, seeding

Stratul 5: Strat de integrare (Integration Layer)

- Adaptori dedicați per serviciu extern (pattern Adapter)
- Hangfire workers pentru operații asincrone
- Polly (circuit breaker) pentru reziliență la indisponibilitate sisteme externe

Stratul 6: Strat de securitate (Security Layer)

- Transversal - prezent pe toate straturile (detalii în secțiunile 6.5 și 11)

7.2 Modelul de date conceptual

Entitățile principale și relațiile:

- **Caz** (1) -> (N) **Incident** - un caz conține multiple incidente
- **Caz** (N) <-> (M) **Victimă** - un caz poate avea mai multe victime; o victimă poate apărea în mai multe cazuri
- **Caz** (N) <-> (M) **Agresor** - similar, relație N:M

- **Caz** (1) -> (N) **Evaluare risc** - multiple evaluări versionare
- **Caz** (1) -> (N) **Plan intervenție** - multiple planuri pe durata ciclului de viață
- **Caz** (1) -> (N) **Referire** -> (1) **Serviciu furnizat**
- **Caz** (1) -> (N) **Ordin restricție** <-> **Agresor**
- **Caz** (1) -> (N) **Ordonanță protecție** <-> **Victimă**
- **Caz** (1) -> (N) **Document**
- **Utilizator** (N) <-> (M) **Rol** -> (N) **Permisiune**

Toate entitățile: UUID primary key, timestamps (created_at, updated_at), soft delete (deleted_at), created_by/updated_by.

7.3 Arhitectura de securitate

Securitatea este implementată transversal, pe 7 niveluri:

1. **Perimetru (Network):** firewall MCloud, WAF
2. **Aplicație:** security middleware, CORS restrictiv, rate limiting, input sanitization
3. **Autentificare:** MPass SAML 2.0, sesiuni securizate (HttpOnly, Secure, SameSite cookies)
4. **Autorizare:** RBAC granular pe fiecare endpoint și resursă
5. **Date:** criptare at rest, mascare date sensibile, clasificare niveluri acces
6. **Audit:** jurnalizare completă, alerte la comportament anomal
7. **Cod:** SAST, dependency scanning, code review obligatoriu

Detaliile tehnice pentru fiecare nivel sunt prezentate în secțiunile 6.5 (OWASP Top 10) și 11 (controlul accesului, criptare, jurnale audit, managementul vulnerabilităților, practici de dezvoltare securizată).

7.4 Arhitectura integrărilor

Fluxul sincron (MConnect REST):

1. Modulul aplicație necesită date externe (ex: date persoană la introducere IDNP)
2. Verificare cache Redis (TTL configurat per tip de date)
3. Dacă miss: request MConnect REST API -> sistem extern
4. Răspuns stocat în cache + returnat la modul
5. Logging schimb de date -> audit

Fluxul asincron (MConnect Events):

1. Eveniment în sistem (ex: schimbare stare caz)
2. Publicare eveniment în Hangfire
3. Worker procesează: transmite eveniment MConnect Events
4. Sisteme externe abonate primesc notificarea
5. Feedback recepționat asincron -> actualizare caz

Reziliență:

- Circuit breaker: dacă un sistem extern e indisponibil, request-urile sunt oprite temporar (nu se acumulează timeout-uri)
- Retry cu exponential backoff: operațiuni eșuate sunt reîncercate automat
- Dead letter queue: operațiuni care eșuează repetat sunt mutate în coadă separată pentru investigare
- Monitoring: alerte Grafana la rata crescută de erori integrare

8. Metodologia și abordarea de implementare

8.1 Abordare hibridă

Conform cerințelor caietului de sarcini, implementarea urmează o abordare hibridă:

Componenta secvențială (etapizată):

- 6 etape majore conform Conceptului HG 530/2025
- Fiecare etapă are livrabile definite și criterii de acceptanță
- Recepția livrabilelor la finalul fiecărei etape

Componenta iterativă (Agile):

- Sprint-uri de 2 săptămâni în cadrul etapelor III și IV
- Ceremonies Agile: daily standup (15 min), sprint planning, sprint review (demo), retrospective
- Demo-uri la fiecare sprint pentru feedback Beneficiar
- Backlog management: user stories derivate din cerințele funcționale și scenariile operaționale

Versionare cod:

- GitLab repository (solution .NET)
- Branching strategy: main (producție) -> develop (integrare) -> feature/* (dezvoltare)
- Merge cu squash + code review obligatoriu
- Tags pentru release-uri

8.2 Instrumente de management

- **Azure DevOps:** gestionarea livrărilor, sarcinilor, erorilor și pipeline-uri automate
- **GitLab:** controlul versiunilor, code review, merge requests
- **Confluence / Notion / Azure Boards:** vizualizare Kanban per sprint
- **Comunicare:** canale dedicate (email, videoconferință) conform modalităților din caiet

9. Planul de lucru și calendarul de implementare

9.1 Etapele de implementare

Etapa	Perioada de realizare	Descriere și activități cheie	Livrabile	Costuri (MDL incl. TVA)

I - Inițiere și analiză detaliată	2 luni	Consultări stakeholders (ANPCV, MAI, MMPS, MS, MJ, CNAJGS); validare cerințe funcționale/operaționale; analiza interoperabilității (documentare API MConnect pentru fiecare SIA); analiza riscurilor; evaluare volum migrare date istorice	Raport de inițiere; Raport de evaluare a nevoilor; Specificație funcțională detaliată; Matrice trasabilitate Concept-Cerință-Use-case; Evaluare riscuri	**392'700**
II - Proiectare	2 luni	Arhitectura sistemului; modelul informațional (DbContext / EF Core Fluent API); fluxurile operaționale detaliate; design UI/UX (wireframes, prototipuri); specificații integrare MConnect; specificații API OpenAPI	Document proiectare sistem; Modele date și diagrame; Design UI/UX; Specificații interoperabilitate; Raport TCO	**599'760**
III - Dezvoltare și integrare	7 luni	**Etapa 3.1 - Fundație tehnică și platformă eGov (Sprint 1-3)** **Etapa 3.2 - Core business cazuri și integrări de consum (Sprint 4-7)** **Etapa 3.3 - Referiri, măsuri protecție și integrări bidirecționale (Sprint 8-10)** **Raportare, analiză, integrare UNFPA și hardening (Sprint 11-14)**	Versiuni incrementale funcționale la fiecare sprint; Cod sursă; Documentație tehnică; API-uri integrate	**4'026'960**
		Etapa 3.1 - Fundație tehnică și platformă eGov (Sprint 1-3): *setup MCloud + CI/CD; Modul Administrare (schema RBAC, audit); Modul Acces autorizat cu MPass funcțional; integrare MLog + MNotify;* ***strat de integrare MConnect (adaptor framework, Redis cache, Polly circuit breaker, dead letter queue); prima integrare MConnect operațională - SIA Registrul de Stat al Populației (IDNP lookup)****; Modul Nomenclatoare.*		1'150'254
		Etapa 3.2 - Core business cazuri și integrări de consum (Sprint 4-7): *Modul Raportare cazuri (cu IDNP MConnect operațional); Modul*		1'150'254

		Urmărire cazuri (state machine, evaluare risc, plan intervenție); integrare MSign pentru documente; integrări MConnect consum incrementale - eSocial, IGP criminogene, CNAM, CNAS, ANOFM, SIA AMP.		
		Etapa 3.3 - Referiri, măsuri protecție și integrări bidirecționale (Sprint 8-10): *Modul Caz de violență; Modul Referiri (MConnect + acord direct CNAJGS); Modul Evidența măsurilor de protecție (cron expirare + alertare MNotify); integrări bidirecționale MConnect - eSocial, IGP Registru agresori, ADJ ordonanțe, Procuratura E-Dosar, IGM.*		1’150’254
		Etapa 3.4 - Raportare, analiză, integrare UNFPA și hardening (Sprint 11-14): *Modul Raportare și analiză (dashboards, materialized views, export); integrare asincronă UNFPA (recepție date violență online); interfață publică Blazor WASM (date agregate); performance tuning; pregătire trecere Etapa IV*		575’484
IV - Testare și pilotare	2 luni	Testare funcțională completă (SIT); testare interoperabilitate (MConnect + SIA-uri); testare securitate (OWASP ZAP + penetration testing); testare performanță; pilotare cu ANPCV	Raport testare; Raport pilotare; Raport integrare; Raport penetration testing; Remedierea neconformităților	**835’380**
V - Lansare și recepție	1 lună	Deploy producție MCloud; instruire administratori (16h) + utilizatori (24h); migrare date (dacă aplicabil); asistență lansare; recepție finală	Sistem funcțional în producție; Raport instruire; Materiale instruire (manuale, video); Raport lansare; Cod sursă final	**357’000**

VI - Garanție și mentenanță	12 luni	Suport corectiv; remedierea defectelor; patch-uri securitate; actualizări minore; mentenanță documentație	Raport remedieri corective; Jurnal activități mentenanță; **Plan de inițiere**: strategie întreținere continuă, protocoale răspuns incidente, raport vulnerabilități penetration testing, cod sursă final	**928’200**

Durată totală dezvoltare (Etapele I-V): 14 luni

Durată totală inclusiv garanție: 26 luni

9.2 Jaloane (milestones)

Jalon	**Moment**	**Criteriu de acceptanță**
M1 - Specificație validată	Sfârșitul Etapei I	Specificația funcțională aprobată de ANPCV
M2 - Arhitectură aprobată	Sfârșitul Etapei II	Documentul de proiectare aprobat; prototipuri UI validate
M3 - Fundație + prima integrare MConnect	Sfârșitul Etapei 3.1 (Sprint 3)	Administrare + MPass + nomenclatoare funcționale; strat integrare MConnect operațional cu prima integrare (SIA RSP - IDNP lookup) demonstrată end-to-end
M4 - Core business cu integrări consum	Sfârșitul Etapei 3.2 (Sprint 7)	Gestionare cazuri end-to-end funcțională cu date reale din MConnect (eSocial, IGP, CNAM, CNAS)
M5 - Sistem complet	Sfârșitul Etapei 3.4 (Sprint 14)	Toate cele 9 module funcționale, integrări MConnect bidirecționale operative, integrare UNFPA activă, interfață publică livrată
M6 - Pilotare reușită	Sfârșitul Etapei IV	ANPCV confirmă funcționalitatea; teste securitate trecute
M7 - Lansare națională	Sfârșitul Etapei V	Sistem în producție, utilizatori instruiți, recepție semnată

9.3 Dependențe critice

1. **Acces MConnect sandbox** - necesar din Etapa II pentru specificații; din Etapa 3.1 (Sprint 1) pentru construirea stratului de integrare și prima integrare operațională (SIA RSP)
2. **Acces MCloud** - necesar din Etapa 3.1 (Sprint 1) pentru deployment pe mediul de dezvoltare
3. **Validare cerințe ANPCV** - necesar la fiecare sprint review pentru feedback
4. **Disponibilitate API-uri SIA externe** - integrările sunt eșalonate pe sub-etape (3.1: SIA RSP; 3.2: eSocial, IGP, CNAM, CNAS, ANOFM, SIA AMP; 3.3: integrări bidirecționale ADJ, IGP Registru agresori, Procuratura, IGM); disponibilitatea fiecărui API este necesară la începutul sub-etapei aferente
5. **Acord direct UNFPA** pentru recepția datelor de violență online - necesar din Etapa 3.4 (Sprint 11)
6. **Date migrare** - volumul și formatul trebuie confirmate în Etapa I

9.4 Estimarea de efort

Estimarea de efort este corelată cu etapele de implementare din 9.1, componența echipei din RFP cap. 7 și cerințele funcționale (SO-01 – SO-09, cele 9 contururi, 14 obiecte informaționale, 14+ integrări prin MConnect). Unitatea de bază este **om-ziua (OZ)** = 8 ore lucrătoare. Conversie: 1 lună ≈ 21 OZ.

9.4.1 Efort total pe etape

Etapă	Perioadă	Efort (OZ)	Efort (OO)	Pondere
Etapa I – Inițiere și analiză	2 luni	142	1.136	5,5%
Etapa II – Proiectare	2 luni	220	1.760	8,4%
Etapa III – Dezvoltare și integrare ➢ Etapa 3.1 ➢ Etapa 3.2 ➢ Etapa 3.3 ➢ Etapa 3.4	7 luni • 2 luni • 2 luni • 2 luni • 1 lună	1.468	11.744	56,4% • 16,11% • 16,11% • 16,11% • 8,06 %
Etapa IV – Testare și pilotare	2 luni	304	2.432	11,7%
Etapa V – Lansare și recepție	1 lună	131	1.048	5,0%
Subtotal dezvoltare (I–V)	**14 luni**	**2.265**	**18.120**	**87,0%**
Etapa VI – Garanție și mentenanță	12 luni	340	2.720	13,0%
TOTAL (I–VI)	**26 luni**	**2.605**	**20.840**	**100%**

9.4.2 Efort defalcat pe rol și etapă (om-zile)

Efortul este distribuit pe cele 7 roluri din componența minimă obligatorie prevăzută în RFP cap. 7.

Rol	I	II	III	IV	V	VI	Total
Manager de proiect	40	38	73	40	26	85	302
Analist de business	42	40	103	30	30	10	255
Arhitect IT	25	45	130	32	18	35	285
Dezvoltator backend (x3 în Etapa III)	10	25	501	78	25	110	749
Dezvoltator frontend (x2 în Etapa III)	—	15	294	30	10	55	404
Specialist UX/UI	15	42	73	10	10	—	150
Specialist QA / testare (x2 în Etapa III)	10	15	294	84	12	45	460
Total	**142**	**220**	**1.468**	**304**	**131**	**340**	**2.605**

9.4.3 Efort defalcat pe activitate (om-zile)

Activitate	OZ	Pondere	Corelare cu cerințele
Analiză cerințe și nevoi	177	6,8%	RFP cap. 3, 5; Livrabil 1, 2
Proiectare (arhitectură, model date, UI/UX, TCO)	185	7,1%	RFP cap. 5.11; Livrabil 3, 4
Dezvoltare module funcționale (9 contururi)	1.150	44,1%	RFP cap. 5.2–5.9; Livrabil 5
Integrare (MConnect, MPass, MSign, MLog, MNotify, UNFPA, 14+ SIA)	318	12,2%	RFP cap. 5.13, NFR 03, 6.3; Livrabil 7
Testare (SIT, UAT, performanță, securitate, pentest)	304	11,7%	RFP cap. 6.5; Livrabil 6, 10
Instruire, lansare și documentație finală	131	5,0%	RFP cap. 8; Livrabil 8, 9

Garanție și mentenanță (12 luni)	340	13,0%	RFP cap. 6.9; Livrabil 10
Total	**2.605**	**100%**	

9.4.4 Efort pe cerințe funcționale (rezumat modular)

Defalcarea efortului de **dezvoltare pură** (1.150 OZ, fără analiză/proiectare/integrare/testare) pe cele 9 contururi funcționale:

Contur / Modul	**Cerințe acoperite**	**OZ dezvoltare**
1. Administrare (utilizatori, roluri, audit)	5.2.1, 5.2.2	110
2. Managementul raportării cazurilor	5.3.1, 5.3.2	160
3. Urmărirea cazurilor (ciclu viață, risc, plan intervenție)	5.4.1, 5.4.2	170
4. Urmărirea referirilor	5.5.1, 5.5.2	100
5. Evidența măsurilor de protecție	5.6.1, 5.6.2	110
6. Raportare și analiză (dashboards, export, indicatori)	5.7.1, 5.7.2	170
7. Gestionarea nomenclatoarelor	5.8.1, 5.8.2	60
8. Acces autorizat și interfață publică	5.9.1, 5.9.2	90
9. Documente de bază și obiecte informaționale (transversal)	5.10, 5.11	100
Frontend comun (layout MUD, componente partajate, i18n, WCAG)	5.1.1–5.1.3	80
Total dezvoltare		**1.150**

9.4.5 Ipoteze și baze de calcul

1. **Normă:** 1 om-zi = 8 ore efective; 1 lună = 21 zile lucrătoare.
2. **Echipă de vârf (Etapa III):** 3 dev backend cu suport ocazional pentru activități transversale (~3,4 FTE efectiv), 2 dev frontend, 2 QA, cu PM/BA/UX parțial (0,5–0,7 FTE) și Arhitect IT aproape full-time (~0,9 FTE).
3. **Productivitate:** randament sprint de 2 săptămâni ajustat cu ~15% overhead (ceremonii Agile, code review, documentație).

4. **Mentenanță (VI):** 340 OZ alocați pentru mentenanță corectivă și adaptivă pe 12 luni, conform categoriilor descrise în 13.1.
5. **Rezerve nemateriale (buffere):** incluse la nivel de etapă (±10% pentru I–II, ±15% pentru III, ±20% pentru IV pentru remedieri pilotare). Bufferele nu sunt defalcate separat, ci distribuite per rol.
6. **Excluderi:** migrare date istorice (dacă volumul depășește 50.000 înregistrări – efort suplimentar estimat separat după Etapa I), achiziție infrastructură MCloud (asumată de Beneficiar), licențe servicii externe STISC (certificate, secrets manager).

10. Asigurarea calității și testarea

10.1 Strategia de testare

Piramida de testare:

1. **Unit tests (baza):** xUnit + Moq - testare funcții individuale, services, validators
   - Acoperire funcționalitate principală și reguli de business
   - Rulare: la fiecare commit (CI/CD)
   - Responsabilitate: dezvoltatori
2. **Integration tests:** WebApplicationFactory + test database PostgreSQL (Testcontainers)
   - Testare endpoints API end-to-end
   - Testare integrări (MConnect mock, MPass mock)
   - Rulare: la fiecare merge request
3. **E2E tests:** Playwright
   - Testare fluxuri complete (SO-01 - SO-09)
   - Rulare: nightly + înainte de release
4. **Testare performanță:**
   - Verificare cerințe de performanță: latență, throughput, error rate
   - Rulare: Etapa IV + ad-hoc
5. **Testare securitate:**
   - OWASP ZAP: scan automat vulnerabilități
   - Penetration testing
   - Dependency audit: dotnet list package --vulnerable automat în CI
   - Analiză statică cod (SAST) integrată în pipeline
6. **UAT (User Acceptance Testing):** cu ANPCV în faza pilot
   - Scenarii de testare bazate pe SO-01 - SO-09
   - Feedback colectat structurat
   - Remedierea neconformităților înainte de lansare

10.2 Standarde și procese

- **Code review:** obligatoriu pentru fiecare merge request (minim 1 reviewer)
- **Standarde codare:** .editorconfig + dotnet format + Roslyn analyzers configurate strict; verificare automată în CI
- **Definition of Done:** cod funcțional + teste + code review + documentație actualizată
- **Managementul defectelor:** Azure DevOps Work Items cu labels (severity, priority, module)
- **Criterii de acceptanță:** definite per user story; testele automate validează criteriile
- **Release management:** semantic versioning (semver); changelog automat; deploy development automat, producție cu aprobare manuală

11. Securitatea informației și protecția datelor

11.1 Controlul accesului

- **Autentificare:** exclusiv MPass (SAML 2.0) - zero credențiale locale stocate
- **Autorizare:** RBAC implementat cu ASP.NET Core Authorization Policies
  - Matrice: Rol -> Permisiune -> Resursă -> Acțiune (CRUD + export)
  - Verificare pe fiecare request API (Authorization Handlers + [Authorize] attributes)
  - Verificare pe frontend (componente Blazor condiționate de permisiuni via AuthorizeView)
  - Principiul least privilege: fiecare rol are doar permisiunile strict necesare

11.2 Criptare

- **În tranzit:** TLS 1.3 obligatoriu pe toate conexiunile (frontend <-> backend, backend <-> DB, backend <-> MConnect). Certificatele TLS/SSL și certificatele X.509 pentru mecanismele de mutual TLS utilizate în interoperabilitate vor fi furnizate și gestionate de STISC (Serviciul Tehnologia Informației și Securitate Cibernetică), conform arhitecturii guvernamentale. Prestatorul asigură implementarea tehnică a mecanismelor de securitate utilizând certificatele puse la dispoziție.
- **At rest:** AES-256 pentru baza de date PostgreSQL (transparent data encryption)
- **Chei și secrete:** injectate ca variabile de mediu la runtime prin secrets manager centralizat dedicat, fără acces al dezvoltatorilor la valorile de producție; rotație periodică automatizată. Detalii în secțiunea 11.8.

11.3 Jurnale de audit

- **Capturare automată:** ASP.NET Core Action Filters pe toate controller-ele
- **Conținut:** utilizator, timestamp, acțiune, resursa afectată, IP, user agent, valori anterioare/noi
- **Stocare:** Elasticsearch (căutare rapidă) + transmitere MLog
- **Retenție:** conform legislației în vigoare
- **Acces:** doar rolul Auditor; filtrare și export funcțional

11.4 Managementul vulnerabilităților

- **Dependabot/Renovate:** actualizare automată dependențe cu vulnerabilități cunoscute
- **dotnet list package --vulnerable:** rulare automată în CI, build eșuează la vulnerabilități critice
- **SAST:** analiză statică cod sursă la fiecare merge request
- **OWASP ZAP:** scan periodic în mediul de dezvoltare
- **Penetration testing:** realizat în Etapa IV, cu raport de vulnerabilități, metode de atac și recomandări (Livrabil 10)

11.5 Practici de dezvoltare securizată

- **Threat modeling:** realizat în Etapa II (proiectare) - identificare suprafețe de atac
- **Secure code review:** checklist OWASP Top 10:2025 la fiecare merge request
- **Input validation:** pe fiecare layer (frontend, API gateway, service, database)
- **Output encoding:** Blazor escape automat, CSP headers
- **Error handling:** mesaje generice către utilizator, detalii doar în logs securizate

11.6 Gestionarea incidentelor

Conform cerințelor din caietul de sarcini:

- **Notificare:** partea care constată incidentul notifică imediat cealaltă parte
- **Coordonare:** măsuri comune de diminuare impact
- **Conservare probe:** colectare fișiere log, copii de rezervă depline, Registru deținere probe
- **Raport post-incident:** rapoarte individuale + plan de acțiuni prevenire
- **Canale:** telefon, email, videoconferință (conform modalităților din caiet)

11.7 Conformitate GDPR și legislație națională

- **Principii GDPR implementate:** legalitate, echitate, transparență; limitarea scopului; minimizarea datelor; exactitate; limitarea stocării; integritate și confidențialitate
- **Consimțământ:** formular electronic, înregistrare audit, posibilitate retragere
- **Drept de acces:** funcționalitate export date personale per victimă
- **Drept la ștergere:** anonimizare (soft delete + randomizare date identificabile)

11.8 Gestionarea centralizată a secretelor

Toate credențialele, cheile de criptare, token-urile de acces și connection string-urile sunt gestionate printr-un secrets manager centralizat, compatibil cu infrastructura guvernamentală. Nu există secrete hardcodate în cod sursă, imagini Docker sau fișiere de configurare.

Principii aplicate:

- Secretele sunt injectate ca variabile de mediu la runtime
- Accesul dezvoltatorilor la secretele de producție este zero
- Mediile non-producție utilizează seturi de secrete separate
- Aplicația suportă reîncărcarea secretelor fără restart de serviciu

Tipuri de secrete gestionate:

Categorie	Exemple
Credențiale bază de date	user/password per serviciu
API keys servicii eGov	MConnect, MNotify, MLog, MSign
Chei criptare aplicație	ASP.NET Core Data Protection keys
Token-uri inter-servicii	JWT signing keys

La recepția finală, ANPCV primește accesul de administrator al secrets manager-ului, documentația operațională și training-ul aferent.

12. Evaluarea riscurilor și măsuri de diminuare

Nr.	Risc	Probabilitate	Impact	Măsura de diminuare	Responsabil
R1	Întârzieri integrare MConnect/SIA - API-uri externe indisponibile sau slab documentate	Mare	Mare	Sandbox testing din Etapa II; adaptori modulari cu mock-uri pentru dezvoltare independentă; circuit breaker pattern	Arhitect IT
R2	Disponibilitate limitată stakeholders ANPCV pentru validare cerințe și sprint review	Medie	Mediu	Calendar consultări fixat din Etapa I; comunicare asincronă (documente partajate); buffer timp inclus în plan	Manager proiect
R3	Migrare date istorice complexe - volum mare, formate nestructurate (PDF scanat, Excel)	Medie	Mediu	Evaluare detaliată volum/format în Etapa I; echipă data entry/validation separată dacă necesar; migrare incrementală	Analist business
R4	Schimbări cerințe în timpul dezvoltării	Medie	Mediu	Abordare Agile cu sprint reviews; proces formal change request; matrice trasabilitate actualizată	Manager proiect
R5	Performanță sub SLA la volume mari de date	Scăzută	Mare	Testare performanță în Etapa IV; caching agresiv (Redis + materialized views); query optimization	Dezvoltator backend

R6	Vulnerabilități de securitate descoperite în testare	Scăzută	Foarte mare	OWASP Top 10:2025 compliance din design; SAST în CI/CD; penetration testing; remediere prioritară	Arhitect IT
R7	Indisponibilitate MCloud sau resurse insuficiente	Scăzută	Mare	Dezvoltare locală cu Docker Compose; solicitare resurse cu marjă; plan escalare	Arhitect IT

13. Suport, garanție și mentenanță

13.1 Perioada de garanție

- **Durată:** 12 luni după încetarea contractului, conform cerinței din caietul de sarcini. Garanția acoperă integral etapa VI din planul de implementare.
- **Acoperire:** remediere gratuită a tuturor defectelor și incidentelor raportate de Beneficiar
- **Mentenanță corectivă:** remedierea bug-urilor și incidentelor raportate față de specificațiile agreate
- **Mentenanță adaptivă:** asigurată pe toată durata garanției, acoperind:
  - Actualizări ale interfețelor API ale serviciilor guvernamentale comune (MPass, MSign, MNotify, MLog, MConnect)
  - Adaptarea configurațiilor la modificările tehnice survenite în MCloud
  - Aplicarea patch-urilor de securitate pentru tehnologiile utilizate (.NET, PostgreSQL, Docker, Kubernetes)
  - Ajustări ale formatelor de raportare sau nomenclatoarelor interne rezultate din modificări ale cadrului normativ care nu alterează arhitectura de bază
- **Delimitarea mentenanță adaptivă vs. funcționalitate nouă:** orice solicitare care introduce un nou Obiect Informațional, un nou Contur Funcțional nespecificat în Conceptul aprobat prin HG nr. 530/2025, sau care modifică fluxul operațional end-to-end (Use Case) necesitând reproiectarea bazei de date constituie funcționalitate nouă și face obiectul art. 76 din Legea nr. 131/2015 (act adițional)
- **Documentație:** menținută actualizată pe toată durata garanției (arhitectură, fluxuri, API-uri)
- **Jurnal activități:** registru detaliat al tuturor intervențiilor (actualizări, patch-uri, rezolvări probleme)

13.2 Canale de suport

Suportul tehnic în perioada de garanție se acordă prin:

- Intervenții tehnice telefonice, prin email sau alte mijloace electronice (inclusiv videoconferință)
- Intervenții on-site la sediul Beneficiarului sau Prestatorului, când necesar
- Remedierea defectelor se realizează cu prioritate, în funcție de impactul asupra funcționării sistemului

13.3 Actualizări și patch-uri

- Patch-uri de securitate: identificate și aplicate pe durata celor 12 luni de garanție, cu testare completă înainte de deploy
- Actualizări dependențe: periodic, cu testare completă înainte de deploy

13.5 Transfer de cunoștințe

La finalizarea proiectului, Beneficiarul primește:

- Cod sursă complet (GitLab repository)
- Documentație completă: arhitectură, fluxuri, API-uri (OpenAPI/Swagger via Swashbuckle), model date
- Credențiale de acces: toate conturile și cheile de acces
- Parametri funcționali și configurări aplicate
- Manuale utilizator (per rol) + ghiduri administrare
- Video-uri instruire
- Proceduri de deployment, backup, disaster recovery

13.6 Instruire și dezvoltarea capacităților

Instruirea utilizatorilor se realizează conform cerințelor din RFP:

- **Administratori:** 16 ore instruire tehnică
- **Utilizatori:** 24 ore instruire funcțională
- **Grupuri de utilizatori:** programele de instruire sunt adaptate diferitelor grupuri, cum ar fi administratorii de sistem, managerii de caz, asistenții sociali, profesioniștii din domeniul sănătății și ofițerii de aplicare a legii
- **Materiale:** ghiduri de instruire cu instrucțiuni pas cu pas, video ghid și scenarii pentru învățare practică
- **Documentație:** documentație detaliată și actualizată a sistemului, precum și manuale de utilizare cu instrucțiuni pas cu pas, disponibile în format digital

13.7 Plan de inițiere

La finalizarea contractului, Prestatorul predă **Planul de inițiere**, care consolidează:

1. **Strategia de întreținere continuă** - planul de actualizări programate (patch-uri securitate, actualizări dependențe, actualizări interfețe API servicii comune) și procedura de gestionare a solicitărilor de schimbare
2. **Protocoale de răspuns la incidente** - proceduri documentate pentru incidente tehnice (conform SLA din secțiunea 13.2) și pentru încălcări de securitate a datelor (conform secțiunii 11.6), inclusiv lanțul de notificare și obligațiile GDPR (notificare ANPDCP în 72h)
3. **1 an mentenanță adaptivă și corectivă** - conform secțiunilor 13.1-13.4
4. **Cod sursă final** - repository GitLab complet cu tag de versiune finală, incluzând toate branch-urile de producție și documentația de build
5. **Raport de penetration testing** - documentează vulnerabilitățile descoperite, metodele de atac utilizate, severitatea (CVSS), statusul remedierii și recomandările pentru îmbunătățirea securității; livrat la finalizarea Etapei IV

14. Mod de lucru, modalități de intervenție și soluționarea divergențelor

14.1 Mod de lucru

Pe tot parcursul prestării serviciilor se păstrează o comunicare corectă între echipa Prestatorului și cea a Beneficiarului. Toate operațiunile se desfășoară în condițiile maxime de securitate cibernetică, cu respectarea strictă a legislației în vigoare.

14.2 Modalități de intervenție

Pe perioada contractului vor fi disponibile din partea Prestatorului următoarele modalități de intervenție în cazul incidentelor și pentru operațiuni normale de întreținere:

a) intervenții tehnice și recomandări telefonice, prin e-mail sau prin alte mijloace de comunicație electronică, inclusiv videoconferință; b) intervenții on-site la sediul Beneficiarului sau/și al Prestatorului, în situațiile în care specialiștii apreciază că este necesară o astfel de abordare.

14.3 Soluționarea divergențelor

Orice divergențe apărute între Părți vor fi soluționate cu efort comun și prin strânsă conlucrare, aplicând următoarele reguli:

- Părțile formează un grup comun de lucru în scopul soluționării divergențelor. De comun acord, în grupul de lucru pot fi acceptați reprezentanți ai părților terțe, inclusiv experți independenți. La necesitate, părțile pregătesc probele electronice relevante pentru aspectele ce au devenit obiect de divergență.
- Grupul de lucru se convoacă și examinează subiectul divergențelor și probele existente, aplicând prevederile Contractului și prezentele reguli.
- Concluzia grupului de lucru este fixată în baza unui proces-verbal, semnat de membrii grupului de lucru.

14.4 Securitatea informației

În cazul unui incident de securitate a informației, Partea care constată incidentul notifică imediat și cealaltă Parte, dacă aceasta poate fi de asemenea afectată. Părțile coordonează măsurile necesare pentru diminuarea impactului și soluționarea incidentului.

La solicitarea Beneficiarului, Prestatorul întreprinde acțiunile de rigoare în scopul colectării și conservării probelor necesare investigării incidentului și probării juridice a responsabilității, inclusiv:

a) colectarea și conservarea fișierelor log ce conțin informația privind accesul la nivelul componentelor de rețea; b) efectuarea copiilor de rezervă depline pentru softul aplicativ și stocarea acestora în condiții ce asigură integritatea copiilor efectuate; c) menținerea formalizată a Registrului privind deținerea probelor conservate.

După soluționarea incidentului, Părțile întocmesc rapoarte individuale privind gestiunea incidentului și, de comun acord, un plan de acțiuni pentru prevenirea repetării incidentelor similare.

15. Scoaterea din exploatare

SI RS VioData este proiectat pentru a permite scoaterea din exploatare controlată, sigură și auditată:

15.1 Export și migrare

- **Export baza de date:** SQL dump complet + export CSV per tabel
- **Export obiecte informaționale:** API-uri dedicate de extragere (REST, format JSON)
- **Export documente:** descărcare în masă a documentelor stocate
- **Export jurnale audit:** export complet în format CSV/JSON

15.2 Arhivare

- Arhivare date și documente conform legislației privind arhivarea documentelor electronice
- Respectarea termenelor de păstrare conform registrelor de stat și protecției datelor cu caracter personal
- Arhivă accesibilă readonly pe perioada legală de retenție

15.3 Dezactivare controlată

- **Blocare introducere date noi:** flag de configurare care dezactivează operațiunile de scriere, păstrând accesul readonly
- **Oprire controlată servicii:** procedură documentată de shutdown gradual (workers -> API -> frontend)
- **Ștergere sigură:** posibilitate de ștergere sigură și ireversibilă a datelor la cererea Beneficiarului, cu audit trail al operațiunii de ștergere

Digitally signed by Filat Natalia
Date: 2026.05.04 00:20:39 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

FILAT Natalia

Administrator „PNA SOFTWARE” S.R.L