TERMENI DE REFERINȚĂ
pentru dezvoltarea sistemului „e-Dosar”
în cadrul Ministerului Afacerilor Interne

CUPRINS

Abrevieri

Nr.	Abreviere/Acronim	Descriere
1.	*BD*	*Bază de Date*
2.	*ToR*	*Termeni de Referință*
3.	*OUP*	*Ofițerul de urmărire penală*
4.	*SOrUP*	*Șeful organului de urmărire penală*
5.	*S*	*statist/analist*
6.	*A*	*Analist*
7.	*P*	*Procuror*
8.	*OGUP*	*Ofițer desemnat membru în grupul de urmărire penală*
9.	*MAI*	*Ministerul Afacerilor Interne*
10.	*RICC*	*Registrul informației criminalistice și criminologice*
11.	*IDNP*	*Numărul de identificare al persoanei fizice, numărul unic din 13 cifre.*
12.	*IDNO*	*Numărul de identificare al persoanei juridice, numărul unic din 13 cifre.*
13.	*HG*	*Hotărârea Guvernului*
14.	*CPP*	*Cod de procedură penală*

A. Istoricul şi necesitatea

Toate activitățile desfășurate de MAI în cadrul procesului penal au la bază documente pe suport hârtie. Documentele procesuale sunt, ca regulă, redactate la calculator, imprimate și semnate ograf. Dosarul cauzei penale este gestionat pe suport hârtie și presupune acces fizic la acesta pentru activități procesuale. Toate schimburile de informații, în cadrul MAI, precum și în afara MAI, sunt efectuate în baza documentelor pe suport hârtie. Nu există sisteme informatice și tehnologii ce ar facilita procesul. Această stare de fapt afectează performanța operațională și instituțională pe domeniul urmăririi penale.

În domeniul guvernanței democratice, al justiției, al egalității și drepturilor omului, accentul este să se asigure că reformele dificile și complexe, care vizează consolidarea instituțiilor guvernamentale și a sectorului de ocrotire a normelor de drept, să rămână pe cale, iar sprijinul să fie oferit procesului de trecere de la formularea politică și legislativă la implementare practică.

Sistemul actual de colectare a datelor despre infracțiuni nu acoperă pe deplin necesitățile ofițerilor de urmărire penală prin lipsa in sistem a evidenței actelor procesuale la faza urmăririi penale, acesta de facto fiind un sistem destinat stocării informației statistice, despre evidență a infracțiunilor, cauzelor penale și persoanelor care au săvârșit infracțiuni.

Este posibilă ridicarea nivelului de calitate și simplificarea activității organelor de urmărire penală în cadrul exercitării procesului penal, prin excluderea sau reducerea semnificativă a fluxului de acte procesuale întocmite pe suport de hârtie în cadrul urmăririi penale.

Dezvoltarea sistemului informațional destinat susținerii digitale a procesului de urmărire penală în cadrul MAI, în scopul asigurării trecerii treptate la conceptul de „e –Dosar” este inclusă în Programul de activitate a Guvernului Republicii Moldova 2016-2018 în compartimentul V. ”Justiția și drepturile omului”, sub-compartiment B. ”Promovarea reformei organelor procuraturii, excluderea influenței politice și creșterea transparenței activității acestora”.

Totodată, măsura respectivă se regăseşte şi în Planul naţional de acţiuni în domeniul drepturilor omului pentru anii 2018–2022, aprobat prin Hotărârea Parlamentului nr.89/2018 (Acţiunea „Asigurarea accesului la justiţie prin implementarea dosarului electronic”), precum şi în Planul de acţiuni al Ministerului Afacerilor Interne pentru anul 2020 (Ordinul MAI nr.20/2020), la pct. 68 - implementarea „dosarului electronic” şi asigurarea interconectării sistemelor informaționale și de comunicare ale instituțiilor de drept și control”.

Ministerul Afacerilor Interne, fiind organul central de specialitate al administrației publice care asigură realizarea politicii guvernamentale în domeniile specifice, va putea produce schimbări pozitive la următoarele compartimente:

1) ordinea și securitatea publică;

2) managementul integrat al frontierei de stat;

3) combaterea criminalității organizate;

4) asigurarea respectării drepturilor și libertăților fundamentale ale omului, precum și apărarea proprietății publice și private;

SIA e-Dosar MAI va permite optimizarea activităților subdiviziunilor MAI responsabile de urmărirea penală. Va îmbunătăți disciplina și controlul instituțional asupra procesului de urmărire penală. Va îmbunătăți calitatea datelor produse în cadrul activităților de urmărire penală. Va crea premise pentru schimbul de date în formă electronică între MAI și alte organe de drept cu responsabilități în domeniul penal (ex. Procuratura, Instanțele de Judecată).

B. Descrierea serviciilor

1. Obiectivele și principiile proiectului

1.1 Obiectivele implementării SIA e-Dosar MAI

Obiective principale:

Pentru a realiza un serviciu polițienesc/de urmărire penală modern și profesionist și pentru a îmbunătăți capacitatea MAI de a funcționa eficient și productiv, a fost identificată necesitatea unui sistem informațional care să ofere funcționalități necesare organelor de urmărire penală din cadrul MAI în activitățile lor zilnice.

Sistemul va fi proiectat pentru a automatiza procesele în cadrul MAI (organele de urmărire penală) și pentru a servi funcționarilor acestora și instituțiilor cu care interacționează.

Sistemul urmărește următoarele obiective:

- Oferirea informațiilor corecte și actualizate funcționarilor MAI în activitățile lor zilnice;
- Oferirea unui mediu de colaborare sigur și fiabil, indiferent de locație;
- Oferirea unui flux de lucru eficient pentru gestionarea documentelor care conține un set de proceduri pentru monitorizarea și notificarea părților interesate cu privire la fiecare punct de reper major;
- Reducerea întârzierilor, mesajelor sau acțiunilor contradictorii din cauza lipsei de informații din partea factorilor de decizie;
- Asigurarea transparenței activităților și deciziilor din cadrul MAI.

Furnizorul trebuie să efectueze o analiză a tipurilor de documente și business-proceselor pentru departamentele țintă din cadrul MAI. Sistemul ar trebui să se concentreze pe conceptul dosarului electronic, precum și pe orice alte documente care sunt utilizate pentru a efectua operațiunile necesare în cadrul procesului de urmărire penală.

Obiective specifice:

- Crearea suportului informatic unitar pentru gestionarea într-o formă consolidată a necesarului de date și informații pentru fundamentarea deciziei pe timpul desfășurării activităților de urmărire penală, planificare, coordonare și conducere a acțiunilor de urmărire penală;
- Implementarea unui sistem modern de management al datelor și al ciclului lor de viaţă, cu posibilitatea înregistrării și afișării on-line în dinamica evoluției dosarului penal, inclusiv a detaliilor descriptive ale evenimentelor;
- Realizarea schimbului de informații în timp real pe timpul derulării anchetei penale, transmiterea operativă a informațiilor și înregistrarea cronologică a acestora.

Prin implementarea aplicației se va asigura o platformă informatică ce va integra aplicații informatice prin care conducerea ministerului și celelalte structuri ale MAI cu competenţe în gestionarea urmăririi penale, vor beneficia de:

- crearea unei baze de date la nivel central al MAI cu privire la evoluţia activităţilor de urmărire penală şi stocare centralizată a documentelor procesuale în format electronic;
- implementarea unor instrumente de analiză şi evaluare care să permită realizarea operativă a unor sinteze şi rapoarte necesare fundamentării deciziei;
- elaborarea unor rapoarte predefinite periodice cu privire la evoluţia activităţilor pe dosarele penale sau a activităţilor în dinamica lor;
- planificarea judicioasă a resurselor umane şi materiale în procesul de planificare a activităţilor de urmărire penală şi implicit pe timpul derulării acestora;
- simplificarea procesului de jurnalizarea a datelor şi informaţiilor pe timpul desfăşurării activităţilor de urmărire penală;
- crearea unui mecanism flexibil pentru înregistrarea, stocarea şi arhivarea datelor şi informaţiilor, atât în ceea ce priveşte raportarea evenimentelor cât şi a documentelor aferente procesului penal şi management al acţiunilor.

1.2 Principiile de elaborare a SIA e-Dosar MAI

Întru asigurarea obiectivelor înaintate *SIA e-Dosar MAI*, la proiectarea, realizarea şi implementarea acestuia trebuie să se țină cont de următoarele principii generale:

- **Principiul legitimităţii** – funcţiile şi operaţiunile executate în sistem de către utilizatorii acestuia sunt de natură legală, în conformitate cu drepturile omului şi legislaţia naţională.
- **Principiul autenticităţii** – datele stocate şi prezentate de către sistem sunt autentice. Autenticitatea acestora este certificată de prezența înregistrării de creare a acestora de către utilizatorii cu rolul Administrator de Sistem, precum şi de marca de timp (timestamp) a înregistrării.
- **Principiul identificării unice** – pachetelor de date actualizate li se atribuie un cod de clasificare la nivel de ţară prin care este posibilă identificarea univocă a setului de date încărcat.
- **Principiul auditului sistemului** – sistemul înregistrează informaţii despre orice modificări efectuate, pentru a face posibilă reconstituirea istoriei unei accesări la o etapă anterioară.
- **Principiul orientării spre utilizator** - structura, conţinutul, mijloacele de acces şi navigarea sunt focalizate spre eficiența și ușurința utilizării sistemului de către utilizatori.
- **Principiul flexibilităţii/scalabilităţii** – capacitatea de ajustare şi extindere rapidă a funcţionalităţilor existente ale sistemului fără costuri majore pentru conformare cu necesităţile în continuă schimbare.
- **Principiul utilizării standardelor deschise** - facilitează interoperabilitatea cu sisteme externe.
- **Principiul securităţii** - protejarea integrităţii, accesibilităţii şi confidenţialităţii informaţiei.

1.3 Referințe și aspecte legale pentru elaborarea SIA e-Dosar MAI

Analizând cadrul normativ-legislativ în vigoare al Republicii Moldova pot fi evidențiate un șir de acte, prevederile cărora trebuie luate în considerație la elaborarea *SIA e-Dosar MAI*. Pentru dezvoltarea, implementarea și funcționarea *SIA e-Dosar MAI* a fost identificat un set de 30 acte juridice și normative grupate în funcție de gradul de aplicabilitate după cum urmează:

- acte care reglementează procesele de business aferente activității *Ministerului Afacerilor Interne*;
- acte care reglementează inițiative și tehnologii TIC promovate de Republica Moldova și trebuie să fie implementate în cadrul sistemului informatic;
- acte generale care vor forma cadrul general de funcționare a sistemului informatic.

I. Acte de reglementare a proceselor de business de activitate a OUP din cadrul MAI:

În baza analizei efectuate pot fi delimitate un șir de acte legislative, normative și interne în baza cărora trebuie să fie modelate și implementate procesele de business ale *OUP al MAI* în *SIA*

e-Dosar MAI. De asemenea la această categorie de acte se referă și documente de analiză și viziuni de informatizare a proceselor de business. La categoria cadrului juridic care specifică procesele de business ce trebuie implementate și automatizate în cadrul *SIA e-Dosar MAI* se poate de menționat:

1. *Codul penal nr.985-XV din 18.04.2002*
2. *Codul contravențional nr.218 din 24.10.2008*
3. *Legea nr.320 din 27.12.2012 cu privire la activitatea Poliției și statutul polițistului*
4. *Codul de procedură penală*
5. *Ordin MAI nr. 243 din 18.08.2017 privind Sistemul de management al serviciilor de tehnologia informației și comunicațiilor în cadrul MAI*
6. *Ordin MAI nr. 244 din 18.08.2017 privind Sistemul de management al securității informație în cadrul MAI*
7. *Ordin MAI nr. 31 din 14.12.2017 cu privire la aprobarea Regulamentului privind controlul general al sistemelor informaționale ținute de către Serviciul TI al MAI*
8. *Legea Nr. 59 din 29.03.2012 privind activitatea specială de investigaţii*
9. *Legea nr. 50 din 22.03.2012 privind prevenirea și combaterea criminalității organizate*
10. *HG nr.778 din 27.11.2009 „Cu privire la aprobarea Regulamentului privind organizarea şi funcţionarea Ministerului Afacerilor Interne, structurii şi efectivului-limită ale aparatului central al acestuia";*
11. *HG Nr. 434 din 19.06.2012 cu privire la Poliţia de Frontieră*
12. *HG nr.283 din 24.04.2013 pentru aprobarea Regulamentului privind organizarea și funcționarea Inspectoratului General al Poliției al Ministerului Afacerilor Interne*
13. *HG nr.986 din 24.12.2012 cu privire la structura și efectivul-limită ale Inspectoratului General al Poliției*
14. *HG nr. 754 din 12 septembrie 2014 privind aprobarea Regulamentului privind organizarea şi funcţionarea Serviciului tehnologii informaţionale din subordinea Ministerului Afacerilor Interne*
15. *HG nr. 1340 din 04.12.2001 cu privire la Comisia pentru Situaţii Excepţionale a Republicii Moldova*

II. Acte de reglementare a inițiativelor TIC a Republicii Moldova:

La elaborarea *SIA e-Dosar MAI* considerăm oportună luarea în considerație și implementarea cerințelor și recomandărilor conținute în actele normativ-legislative privind inițiativele TIC ale Republicii Moldova. Întru respectarea cadrului de guvernare electronică promovat de Guvern trebuie să fie luate în considerație următoarele acte:

1. *Hotărârea Guvernului nr. 7104 din 20.09.2011 cu privire la aprobarea Programului strategic de modernizare tehnologică a guvernării (e-Transformare)*, Monitorul Oficial Nr. 156-159 din 23.09.2011;
2. *Hotărârea Guvernului nr. 128 din 20.02.2014 privind platforma tehnologică guvernamentală comună (MCloud)*, Monitorul Oficial Nr. 47-48 din 25.02.2014.
3. *Hotărârea Guvernului nr. 656 din 05.09.2012 cu privire la aprobarea Programului privind Cadrul de Interoperabilitate*, Monitorul Oficial Nr. 186-189 din 07.09.2012.
4. *Hotărârea Guvernului nr. 1090 din 31.12.2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass)*, Monitorul Oficial Nr. 4-8 din 10.01.2014.
5. *Hotărârea Guvernului nr. 405 din 02.06.2014 privind serviciul electronic guvernamental integrat de semnătură digitală (MSign),* Monitorul Oficial Nr. 147-151 din 06.06.2014.
6. *Hotărârea Guvernului nr. 280 din 24.04.2013 cu privire la unele acțiuni de implementare a Serviciului Guvernamental de Plăti Electronice (MPay)*, Monitorul Oficial Nr. 109 din 10.05.2013.

7. *Hotărârea Guvernului nr. 708 din 28.08.2014 privind serviciul electronic guvernamental de jurnalizare (MLog),* Monitorul Oficial Nr. 261-267 05.09.2014.

8. *Hotărârea Guvernului Nr. 916 din 06.08.2007 cu privire la Concepția Portalului Guvernamental,* Monitorul Oficial Nr. 127-130/952 din 17.08.2007.

9. *Hotărârea Guvernului nr. 330 din 28.05.2012 cu privire la crearea și administrarea portalului guvernamental unic al serviciilor publice*, Monitorul Oficial Nr. 104-108 din 01.06.2012.

10. *Legea Nr. 91 din 29.05.2014 cu privire la semnătura electronică și documentul electronic*, Monitorul Oficial Nr. 174-177 din 04.07.2014.

11. *Hotărârea Guvernului Nr. 945 din 05.09.2005 cu privire la centrele de certificare a cheilor publice,* Monitorul Oficial Nr. 123-125 din 16.09.2005.

12. *Hotărârea Guvernului Nr. 320 din 28.03.2006 pentru aprobarea Regulamentului privind modul de aplicare a semnăturii digitale în documentele electronice ale autorităților publice,* Monitorul Oficial Nr. 51-54 din 31.03.2006.

13. Legea cu privire la schimbul de date şi interoperabilitate nr. 142 din 19.07.2018, Monitorul Oficial nr. 295-308 din 10.08.2018.

Acte legislative ce reglementează accesul la informație

- Legea nr.982-XIV din 11 mai 2000 privind accesul la informaţie;
- Legea 133 din 08.07.11 privind protecţia datelor cu caracter personal
- Legea nr. 245 din 27.11.2008 cu privire la secretul de stat
- HG nr. 1176 din 26.08.2010 pentru aprobarea Regulamentului cu privire la asigurarea regimului secret în cadrul autorităţilor publice şi al altor persoane juridice
- Hotărîrea Guvernului Republicii Moldova nr. 1123 din 24.12.2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal
- HG nr. 201 din 07.04.2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică

Acte legislative în domeniul securității informației și TIC

- Legea nr.71-XVI din 22 martie 2007 cu privire la registre;
- Legea nr. 467-XV din 21.11.2003 cu privire la informatizare şi la resursele informaţionale de stat ;
- Legea nr. 216-XV din 29.05.2003 cu privire la Sistemul informaţional integrat automatizat de evidenţă a infracţiunilor, a cauzelor penale şi a persoanelor care au săvârşit infracţiuni;
- HG nr. 1202 din 17.10.2006 „Cu privire la aprobarea Concepţiei Sistemului integrat al organelor de drept";

Conceptualizarea, elaborarea și implementarea *SIA e-Dosar MAI* trebuie să fie realizate în conformitate cu standardele și metodologia națională, precum și recomandările și cerințele consacrate în sectorul TIC. Astfel, trebuie să se țină cont de următoarele reglementări și standarde:

1. *Standardul Republicii Moldova MR ISO/CEI/IEEE 15288:2015, „Ingineria sistemelor și software-ului. Procesele ciclului de viață al sistemului".*
2. *Reglementarea tehnică „Procesele ciclului de viață al software-lui" RT 38370656-002:2006*; Monitorul Oficial Nr. 95-97/335 din 23/06/2006.
3. *The Handbook on "Information and Communication Technologies in Parliamentary Libraries"*, Global Centre for Information and Communication Technologies in Parliament, July, 2012), http://www.ictparliament.org/attachements/handbook-libraries/handbook-libraries.pdf
4. Michael O. Leavitt, Ben Shneiderman, *Research-Based Web Design & Usability Guidelines*, https://www.usability.gov/sites/default/files/documents/guidelines_book.pdf

5. *Recomandările World Wide Web Consortium (W3C)* (http://www.w3c.org) privind calitatea conținutului paginilor Web, posibilitățile vizualizării corecte a informației, folosind exploratoare Internet larg utilizate, și compatibilitatea cu diferite platforme informatice;

6. *Recomandările W3C* (http://validator.w3.org) privind testarea paginilor WEB. Toate paginile WEB generate de *SIA e-Dosar MAI* se vor testa în conformitate cu aceste recomandări.

SIA e-Dosar MAI nu va fi un sistem izolat ci va interacționa cu sistemele informatice ale autorităților de drept ale Republicii Moldova. În acest sens este oportună utilizarea cadrului de interoperabilitate a Guvernului pentru realizarea conexiunilor cu sisteme informatice terțe sau utilizarea serviciilor de platformă furnizate de acesta.

Adițional, cadrul de interoperabilitate *MConnect* reglementat prin intermediul *Hotărârii Guvernului nr. 656 din 05.09.2012 şi Hotărârii Guvernului nr.211/2019 privind platforma de interoperabilitate (MConnect)* permite realizarea unei interacțiuni de tip sistem-sistem nu doar între soluțiile informatice găzduite în *MCloud*, ci și cu prestatori de servicii informatice în afara *MCloud.* În contextul *SIA e-Dosar MAI , MConnect* va servi în calitate de platformă prin intermediul căreia se va realiza interacțiunea automată cu sistemele externe în vederea preluării, verificării și inserării automate a datelor în cadrul proceselor de business ale *MAI.*

III. Acte generale aferente punerii în producție și funcționării *SIA e-Dosar MAI* :

Adițional la actele juridice și normative în baza cărora trebuie să fie dezvoltată și implementată soluția informatică destinată implementării conceptului de *SIA e-Dosar MAI* trebuie luate în considerație un set de acte juridice care impun măsuri organizaționale și constrângeri externe de funcționare a sistemului informatic. La această categorie de acte de care trebuie să țină cont *SIA e-Dosar MAI* se poate de menționat:

1. *Legea Nr. 467-XV din 21.11.2003 cu privire la informatizare și la resursele informaționale de stat*, Monitorul Oficial nr. 6-12/44 din 01/01/2004.

2. *Legea Nr. 71 din 22.03.2007 cu privire la registre*, Monitorul Oficial Nr. 70-73 din 25.05.2007.

3. *Legea Nr. 982-XIV din 11.05. 2000 privind accesul la informație*, Monitorul Oficial Nr. 88 art. Nr. 664 din 28.07.2000.

4. *Legea Nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal*, Monitorul Oficial Nr. 171-175 din 14.10.2011.

5. *Hotărârea Guvernului Nr. 1123 din 14.12.2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal*, Monitorul Oficial Nr. 254-256 din 24.12.2010.

6. *Hotărârea Guvernului Nr. 945 din 05.09.2005 cu privire la centrele de certificare a cheilor publice*, Monitorul Oficial Nr. 123-125 din 16.09.2005.

7. *Legea Nr. 982-XIV din 11.05. 2000 privind accesul la informație*, Monitorul Oficial Nr. 664 din 28.07.2000.

8. *Legea Nr. 1069-XIV din 22.06.2000 cu privire la informatică*, Monitorul Oficial Nr. 073 din , 05.07.2001.

9. *Legea Nr. 241-XVI din 15.11.2007 privind telecomunicațiile*, Monitorul Oficial Nr. 51-54 din 14.03.2008.

10. *Hotărârea Guvernului Nr. 967 din 09.08.2016 cu privire la mecanismul de consultare publică cu societatea civilă în procesul decizional*, Monitorul Oficial Nr. 265-276 din 19.08.2016

11. *Hotărârea Guvernului Nr. 840 din 26.07.2004 cu privire la crearea Sistemului de telecomunicații al autorităților administrației publice*, Monitorul Oficial Nr. 130 din 30.07.2004.

12. *Hotărârea Guvernului Nr. 735 din 11.06.2002 cu privire la sistemele speciale de telecomunicații ale Republicii Moldova*, Monitorul Oficial Nr. 79-81 din 20.06.2002.

13. *Ordinul Nr. 94 din 17.09.2009 al Ministerului Dezvoltării Informaționale cu privire la aprobarea unor reglementări tehnice (modul de evidență a serviciilor publice electronice, prestarea serviciilor publice electronice, asigurarea securității informaționale la prestarea*

serviciilor publice electronice, determinarea costului de elaborare şi implementare a sistemelor informaţionale automatizate), Monitorul Oficial Nr. 58-60 din 23.04.2010.

14. HG nr. 656 din 05.09.2012 „Cu privire la aprobarea Programului privind Cadrul de Interoperabilitate";

15. HG nr. 709 din 20.09.2012 „Cu privire la unele măsuri în domeniul e-Transformare a guvernării";

16. HG nr. 710 din 20.09.2012 „Cu privire la aprobarea Programului strategic de modernizare tehnologică a guvernării (e-Transformare)";

17. Standardul SM 12207:2005 „Procesele ciclului de viaţă al software-ului";

18. Ordinul MDI nr. 78 din 01.06.2006 „Cu privire la aprobarea reglementării tehnice "Procesele ciclului de viaţă al software-lui" RT 38370656 - 002:2006.

19. Alte legi, acte normative, standarde în vigoare în domeniul TIC.

O restricție juridică importantă ce trebuie respectată este asigurarea securității datelor cu caracter personal gestionate prin intermediul *SIA e-Dosar MAI. Legea nr. 133 din 08.07.2011 „Cu privire la protecția datelor cu caracter personal"* stipulează obligativitatea asigurării confidențialității datelor cu caracter personal. Mai mult decât atât, în conformitate cu această lege proprietarul *SIA e-Dosar MAI* este obligat să înregistreze sistemul informatic în *Registrul de stat al operatorilor de date cu caracter personal* care este gestionat de *Centrul Național pentru Protecția Datelor cu Caracter Personal*.

2. Managementul proiectului

2.1 Administrarea proiectului

Administrarea proiectului (luarea deciziilor) este realizată de către managerii de proiect, desemnaţi din partea Furnizorului şi Beneficiarului proiectului. Prin procesul decizional respectiv va fi asigurată continuitatea și coerența proiectului, managerii sunt responsabili de planificarea și supravegherea eficientă a proiectului; alocarea resurselor financiare, umane și de altă natură; agrearea activităților comune ale proiectului și programul activităților/pachetelor de lucru; evaluarea și confirmarea progresului; sugerarea acțiunilor preventive și corective, atunci când este cazul.

2.2 Ministerul Afacerilor Interne

Beneficiarul acestui proiect este Ministerul Afacerilor Interne al Republicii Moldova. MAI - organ central de specialitate al administrației publice care asigură realizarea politicii guvernamentale în următoarele principale domenii de activitate:

1) ordinea şi securitatea publică;
2) managementul integrat al frontierei de stat;
3) combaterea criminalităţii organizate;
4) gestionarea fluxului migraţional, azilului şi integrării străinilor;
5) asigurarea respectării drepturilor şi libertăţilor fundamentale ale omului, precum şi apărarea proprietăţii publice şi private;

În cadrul misiunii respective, MAI, care acționează în calitate de beneficiar al acestui proiect, va:

- Asigura prezentarea îndrumărilor/consultărilor (explicații legate de procesul de urmărire penală) Furnizorului pe toată perioada dezvoltării sistemului „e-Dosar";
- Efectua testarea sistemului, în comun cu Furnizorul, la toate etapele dezvoltării sistemului;
- Oferi sprijin instituțional pentru interconectarea sistemului „e-Dosar" cu alte sisteme de informații pentru a permite validarea datelor cu caracter personal, importarea și verificarea datelor relevante;
- Oferi informații și explicații despre alte sisteme informaționale conexe utilizate de MAI;

- Coopera strâns cu Furnizorul pentru dezvoltarea, testarea și pilotarea sistemului.

2.3 Furnizorul

Obigaţiile Furnizorului şi cerinţele faţă de acesta sunt redate în prezentul document, în special în capitolele *Cerințe pentru implementarea SIA e-Dosar MAI* şi *Cerințe pentru garanție, mentenanță și suport post-implementare*

2.4 Monitorizarea și raportarea

În timpul proiectului, Furnizorul va prezenta lunar (sau, după caz, mai frecvent) un raport de progres detaliat pentru a comunica progresul și starea dezvoltării, contribuind la identificarea punctelor forte și a punctelor slabe ale implementării proiectului. Raportul trebuie să ofere informații despre starea livrării activităților proiectului, produsele și rezultatele proiectului; precum și informații despre orice probleme reale sau potențiale și abateri de la planul de lucru aprobat și buget.

Toate rapoartele produse în timpul implementării proiectului vor fi furnizate în limba română, atât în format de hârtie, cât și în versiunea electronică.

Toate rapoartele produse de furnizor trebuie să satisfacă următoarele cerințe:

1) Integral în limba română;

2) Ușor de citit; imprimat cu culoarea neagră;

3) Fiecare pagină numerotată;

4) Un cuprins similar cu următorul:

a) Prefață;

b) Introducere;

- Scopul;
- Domeniu de aplicare;
- Definiții, acronime și abrevieri;
- Referințe;
- Prezentare generală a celorlalte părţi ale documentului;

c) Partea narativă a documentului;

d) Anexele;

5) Să conţină o foaie de titlu, care conține următoarele elemente;

a) Titlul proiectului: denumirea proiectului pentru care a fost întocmit raportul;

b) Titlul documentului: denumirea raportului;

c) Rezumat: un rezumat al raportului;

d) Versiunea documentului: versiunea raportului;

e) Data: data ultimei revizuiri a raportului;

f) Stare: Starea raportului. De exemplu, DRAFT sau APROBAT;

6) Să conţină o prefață care include tabele pentru fiecare dintre următoarele:

a) Persoanele implicate în pregătirea documentului: Lista persoanelor care au contribuit la elaborarea raportului;

b) Lista de revizuire: lista persoanelor care au revizuit și aprobat documentul;

c) Istoricul modificărilor: o înregistrare cronologică a detaliilor (versiunea, data și descrierea revizuirii) despre actualizările care au fost făcute raportului;

7) Să conțină un cuprins;

8) Să conţină un tabel de figuri (dacă este cazul);

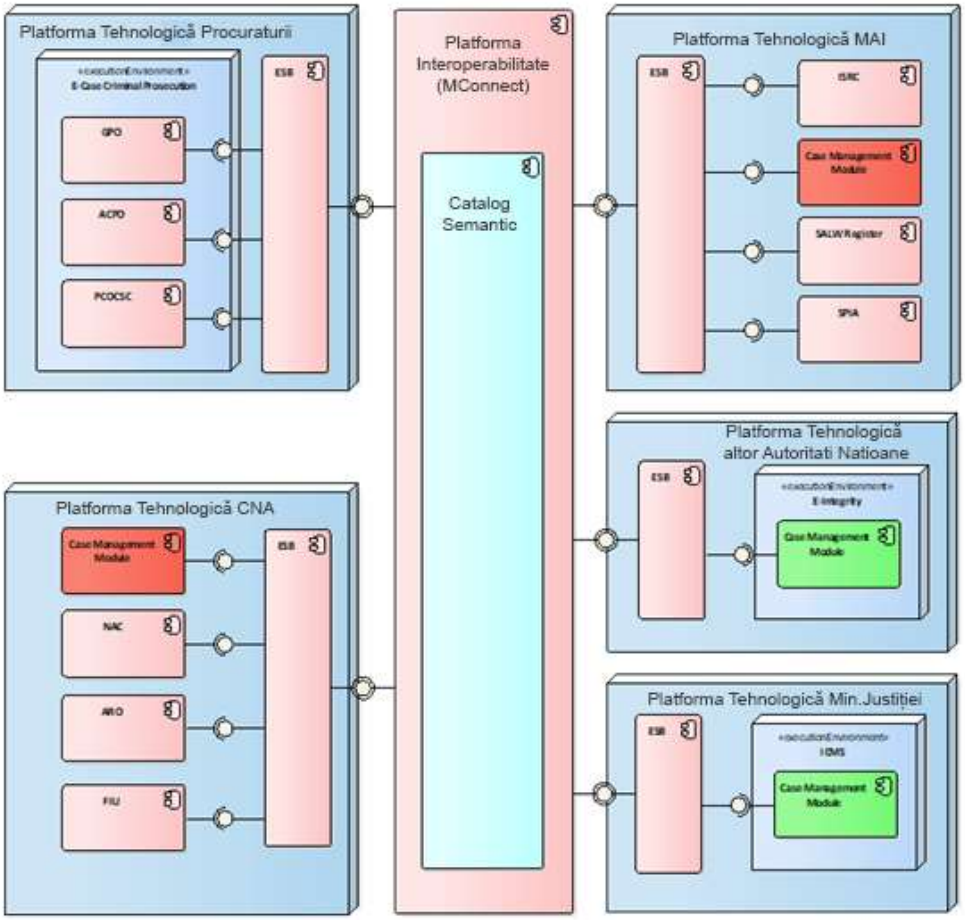
9) Au un tabel a tabelurilor (dacă este cazul);

10) Ultima pagină a fiecărui document va fi goală.

3. Descrierea sistemului

SIA e-Dosar MAI va furniza o interfață WEB, accesibilă prin intermediul unui explorator Internet de largă utilizare (MS Internet Explorer/MS Edge, Mozilla FireFox, Opera, Google Chrome sau Safari). Din punct de vedere funcțional se va dezvolta o soluție fiabilă și scalabilă atât în cazul creșterii numărului de utilizatori concurenți sau, cât și în cazul creșterii volumului de informație gestionată. La baza SIA e-Dosar MAI va sta o arhitectură client-server de 3 nivele (care exclude interacțiunea directă a aplicației cu baza de date) bazată pe tehnologiile WEB adecvate timpului. Întru asigurarea unui nivel adecvat al securității informaționale aplicația livrată trebuie să permită realizarea de conexiuni securizate între stațiile client și serverul de aplicație pentru asigurarea siguranței informației expediate (prin intermediul canalelor VPN și a sesiunilor TLS/SSL).

Figura 1. Amplasarea SIA e-Dosar MAI în infrastructura SIIOD



SIA e-Dosar MAI va fi instalat și va funcționa în cadrul platformei tehnologice MCloud, spațiul dedicat Ministerului de Interne. Întru asigurarea obiectivelor înaintate soluției informatice, la proiectarea, realizarea și implementarea SIA e-Dosar MAI trebuie să se țină cont de arhitectura descrisă în Figura 1.

După cum se vede în Figura 1, soluția de cooperare a resurselor pentru asigurarea funcționalității SIA e-Dosar MAI constă din 3 categorii de noduri distincte:

■ Infrastructura TIC a Ministerului de Interne (administrată de STI MAI) - infrastructura TIC care va găzdui SIA e-Dosar MAI.

■ Infrastructura TIC MCloud – infrastructura TIC a platformei tehnologice guvernamentale comune care formează cloud-ul guvernamental (MCloud).

■ Calculatoarele client – calculatoarele, de la care se va accesa de către utilizatori funcționalitățile SIA e-Dosar MAI.

Calculatoarele client trebuie să folosească în calitate de aplicație client pentru accesarea și utilizarea SIA e-Dosar MAI cel puțin 3 din cele mai populare exploratoare Internet, care satisfac cerințele minime HTML 5, CSS 3. Compatibilitatea cu MS Edge/MS Internet Explorer este obligatorie.

Conform diagramei de desfășurare din figura 1, SIA e-Dosar MAI constă din următoarele componente de bază:

■ Fluxuri de lucru destinate înregistrării evenimentelor/acţiunilor– interfață accesibilă utilizatorilor autorizați ai SIA e-Dosar MAI care furnizează totalitatea funcționalităților destinate suportului informatic al fluxurilor de lucru destinate gestiunii proceselor de business aferente desfășurării procesului penal.

■ Generare rapoarte și documente – funcționalitate destinată generării rapoartelor statistice destinate analizei și procesului de luare a deciziei și a documentelor tipizate aferente procesului penal.

■ Administrare și configurare SIA e-Dosar MAI – componenta care va furniza totalitatea funcționalităților de administrare a SIA e-Dosar MAI disponibile în mare parte utilizatorilor cu rol Administrator de SI.

3.1 Părțile implicate și utilizatorii SIA e-Dosar MAI

Posesorul SIA e-Dosar MAI

Posesorul SIA e-Dosar MAI este Ministerul Afacerilor Interne. În calitate de posesor al SIA e-Dosar MAI va putea atribui instituțiilor și persoanelor autorizate dreptul de administrare a portalului. De asemenea, Ministerul de Interne va asigura totalitatea activităților de suport, mentenanță și dezvoltare continuă a SIA e-Dosar MAI.

Deținătorul SIA e-Dosar MAI

Deținătorul (operatorul tehnico-tehnologic) SIA e-Dosar MAI este Serviciul Tehnologii Informaționale (STI) al MAI.

Utilizatorii SIA e-Dosar MAI

Rolurile umane ce interacționează cu SIA e-Dosar MAI sunt:

Ofițer de urmărire penală - actor uman, care reprezintă totalitatea utilizatorilor care dispun de roluri de bază în cadrul procesului penal, precum şi de totalitatea funcționalităților şi instrumentelor destinate realizării fluxurilor de lucru în cadrul gestiunii business-proceselor aferente desfășurării procesului penal.

Șef OUP – actor uman, care reprezintă totalitatea utilizatorilor cu rol decident (Seful organului de urmărire penală, inclusiv adjuncții acestuia care îi preiau atribuțiile)

Seful ierarhic superior - Conducator din Direcția Generală de Urmărire Penală din IGP, IGPF sau SPIA

Sistemul urmează a fi capabil de a fi dezvoltată o interfață externă prin care participanții la dosar să aibă posibilitatea de a vizualiza dosarul, iar, în caz de necesitate, să depună sesizări/plângeri/cereri (în cazul în care WfMS nu acoperă deja acest funcțional).

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

- utilizează Dashboard pentru accesul rapid la notificări și sarcinile relevante;
- administrează sistemul de nomenclatoare și metadate proprii sistemului;
- configurează fluxuri, formulare și șabloane de documente;
- generează rapoarte aferente auditului sistemului informatic și conținutului informațional al Bazei de Date a sistemului informatic;
- recepționează notificări;

Web serviciile expuse către platforma MConnect, precum și cele expuse de platforma MConnect trebuie să opereze cu date structurate pentru asigurarea procesării automate a acestora de către sistemele participante, dar și digitizarea completă a proceselor de business ale participanților, ca rezultat al schimbului de date.

Se va realiza interoperabilitatea, cel puțin, cu sisteme informaționale după cum urmează:

<table>
<tr><th>SIA</th><th>Descrierea interoperabilității</th></tr>
<tr><td>SI Semnalări (WfMS)</td><td>Preluarea fișei semnalării înregistrate în WfMS MAI</td></tr>
<tr><td>SIA RSP</td><td>Preluare date despre persoană fizică și actele de identitate ale acestuia după IDNP;
Căutarea persoanei după un set de parametri.</td></tr>
<tr><td>SIA RSUD</td><td>Preluare date de înregistrare din Registrul de Stat al UD după IDNO;
Preluare date de identitate a conducătorilor UD;</td></tr>
<tr><td>SI e-Dosar PG</td><td>Schimb de date bilateral, ce include:
Digitizarea fluxurilor de lucru interinstituționale aferente gestiunii cauzei penale (include sarcini și documente anexe) (ex. procesul de coordonare cu procurorul a începerii urmăririi penale);
Schimb de date bilateral privind conținutul dosarului penal în format electronic (eDosar al cauzei penale) (include: documente electronice calificate și copiile digitale ale documentelor pe suport hârtie);
Totodată, structura de date despre Dosarul penal va fi completată cu un set de câmpuri/variabile, după modelul de mai jos:
<table>
<tr><td>Documents</td><td>File</td><td></td><td>Fișierul cu documentele din dosarul penal în format electronic</td></tr>
<tr><td colspan="4">File</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>FileID</td><td>String</td><td>Da</td><td>Id-ul unic al fișierului</td></tr>
<tr><td>FileName</td><td>String</td><td>Da</td><td>Nume fișier</td></tr>
<tr><td>Title</td><td>String</td><td>Da</td><td>Titlu (Descrierea)</td></tr>
<tr><td>FileSize</td><td>String</td><td>Da</td><td>Mărimea</td></tr>
<tr><td>FileUrl</td><td>String</td><td>Da</td><td>Linkul de unde poate fi copiat fișierul</td></tr>
<tr><td>FileChecksum</td><td>String</td><td>Da</td><td>Hash pentru verificarea integrității fișierului</td></tr>
<tr><td>Type</td><td>String</td><td>Da</td><td>Tipul fișierului</td></tr>
</table>
</td></tr>
<tr><td>SIA RICC</td><td>Schimb de date în vederea obținerii codului de înregistrare a dosarului penal (punct 41, anexa nr. 2, Ordin comun nr. 121/254/286-O/95 din 18.07.2008);

Export date prevăzute de ordinul interdepartamental PG, MAI, SV, CNA nr. 121/254/286-O/95 din 18.07.2008 pentru export în SIA RICC (în limita informației digitizate la etapa respective a proiectului)

Sincronizare nomenclatoare tematice gestionate în SIA RICC</td></tr>
<tr><td>Sincronizarea nomenclatoarelor</td><td>lista acestora să fie identificată și consumată prin platforma de interoperabilitate (MConnect) de la autoritățile relevante.</td></tr>
</table>

Lista sistemelor și structura datelor cu care se realizează interoperabilitatea (seturi de date exacte care vor fi consumate din sistemele informaționale, cu specificarea metodelor și criteriilor, parametrilor de căutare) urmează să fie precizată și documentată la etapa de proiectare a sistemului informațional și consumată prin platforma de interoperabilitate (MConnect) de la autoritățile relevante

Sisteme informatice administrate de STI:

SIA Semnalări – soluția informatică de înregistrare a semnalărilor parvenite în adresa MAI și gestiune evenimente de ordine publică

RICC – „Registrul informației criminalistice și criminologice” (RICC) gestionat de MAI care reprezintă resursa informațională specializată ce include totalitatea informației sistematizate cu caracter criminal și care este format în baza Sistemului informațional integrat automatizat de evidență a infracțiunilor, a cauzelor penale și a persoanelor care au săvîrșit infracțiuni. Registrul întrunește cîteva baze de date și este destinat pentru formarea, acumularea, stocarea, actualizarea și analiza datelor despre starea criminalității și activitatea de combatere a acesteia în Republica Moldova.

Sisteme informatice externe:

PIGD *(Programul Integrat de Gestiune a Dosarelor)* - sistem informatic destinat informatizării proceselor de business ale instanțelor de judecată prin intermediul căruia *SIA e-Dosar MAI* va furniza și va recepționa documentele procesuale necesare obținerii acceptului în contextul controlului judiciar.

SIA e-Dosar „Urmărire Penală” – sistem informatic destinat automatizării proceselor de lucru ale procurorilor în desfășurarea procesului penal.

PDD (Portalul Datelor Deschise) - reprezintă portalul datelor guvernamentale deschise prin intermediul căruia *SIA e-Dosar MAI* va publica setul de date dezagregate și anonimizate.

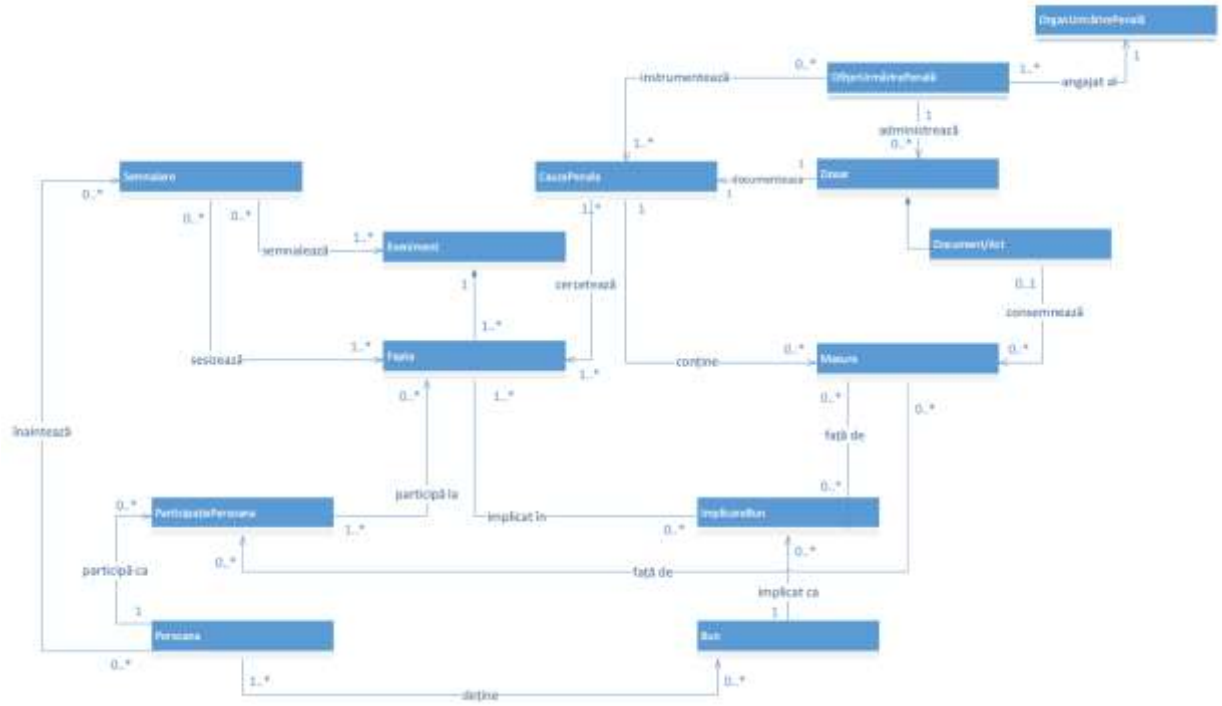
3.2 Conceptul dosarului electronic şi modelul funcţional al acestuia

Conceptul dosarului electronic reflectă dosarul pe suportul de hârtie din cadrul procesului de urmărire penală. Dosarul electronic este obiectul principal de date care reflectă cauza penală și conține informații cu privire la etapele urmăririi penale, statuturile acesteia, tipul infracțiunii, alte documente și descrierea care caracterizează un caz particular de urmărire penală.

Fiecare cauza penală se bazează pe articolele respective din legislație, astfel Furnizorul va implementa nomenclatoare respective în cadrul SIA e-Dosar MAI, astfel încât să permită funcționalitatea de referință care indică articole din legislație la inițierea procesului de urmărire penală. Furnizorului i se va oferi acces la sistemul actual care posedă astfel de nomenclaturi; ar fi necesară şi o analiză pentru a importa acea nomenclatură și a o interconecta cu noul SIA e-Dosar MAI.

În Figura 2 sunt expuse componentele (entitățile) de interes care vor sta la baza proiectării și dezvoltării *SIA e-Dosar MAI.* După cum se vede în Figura 2, elementul central al arhitecturii de date al *SIA e-Dosar MAI* îl constituie *Cauza penală*. Diagrama prezintă toate entitățile importante ale domeniului conceptual care vor fi reprezentate în sistemul informatic cerut și relațiile dintre acestea, inclusiv cardinalitatea și multiplicitatea.

Figura 2. Domeniul conceptual și obiectele informaționale ale SIA e-Dosar MAI



Întru asigurarea funcționalității în bune condiții a *SIA e-Dosar MAI* este necesară implementarea funcționalităților necesare gestiunii următoarelor obiecte informaționale:

- Cauza penală
- Dosar
- Fapta
- Măsura
- Bun
- Participant
- Eveniment

- Documentul procesual
- Raport
- Ofițer de urmărire penală
- Organ de urmărire penală

A fost modelată entitatea Semnalare ca o clasă generică pentru toate tipurile de intrări în sistem care semnalează una sau mai multe infracțiuni(fapte) dar care încă nu au fost clasificate ca fiind acte de sesizare sau nu corespund criteriilor minime pentru un act de sesizare, conform CPP. Această entitate nu este obligatorie, în sensul că nu în toate instanțele de business-proces vor exista semnalări, anumite cauze penale putând fi de exemplu a fi constituite prin disjungerea dintr-o cauză existentă, nu în baza unei semnalări.

În completarea modelului de mai sus, care prezintă o viziune statică asupra entităților, este important de menționat faptul că o Semnalare (dacă îndeplinește condițiile formale prevăzute în CPP) devine sesizare/act de de sesizare (plângerea, denunțul, autodenunțul sau autosesizarea, după caz) și se transformă într-o altă entitate din acest model, anume Document/Act în cadrul Dosarului. Acest tip de act este obligatoriu la nivel conceptual, în sensul în care nu poate exista proces penal în absența unei forme de sesizare. La nivelul sistemului informatic ce trebuie implementat însă, având în vedere faptul că sesizarea/autosesizarea poate fi înregistrată în afara sistemului MAI (de exemplu la Procuratură) implică faptul că vor exista Dosare în care nu vor exista Acte de Sesizare materializate în interiorul sistemului MAI. Însă și în aceste cazuri, având în vedere constrângerile privind evidența unică la nivel republican a sesizărilor, ofițerul de urmărire penală responsabil de cauză va avea acces la informația privind numărul unic de înregistrare și va putea ca atare genera în sistem această entitate, cel puțin cu acest atribut.

Au fost modelate două entități de legătură (echivalentul unei Association Class în modelarea object-oriented) care au însă un rol foarte important în procesul penal:

Participație Persoană, respectiv Implicare Bun. Pentru exemplificare, într-o cauză penală, o singură persoană poate avea mai multe participații (făptuitor a două dintre fapte și complice sau instigator la cea de a treia) iar măsurile și actele procesuale din cadrul procesului penal se vor lua individual, pentru fiecare participație. De exemplu, într-o astfel de cauză se poate lua decizia începerii urmăririi penale față de persoana respectivă cu privire la săvârșirea unei dintre fapte și decizia de neîncepere a urmăririi penale față de aceeași persoană cu privire la săvârșirea celei de a doua fapte. Din acest motiv, entitățile Faptă, Act Procesual, Măsură Procesuală nu sunt relaționate direct cu Persoana, ci cu entitatea Participație Persoană.

În mod similar cu entitatea Participație Persoană a fost modelată și entitatea **Implicare Bun**, deoarece un singur Bun poate fi implicat în mai multe moduri într-o cauză penală.

În entitatea **Persoană** sunt modelate toate persoanele care participă cu un rol sau altul la cauza penală. Aceste persoane sunt de mai multe tipuri (fizice, juridice) inclusiv persoane necunoscute (atunci când făptuitorul faptei sesizate nu este cunoscut sau victima nu poate fi identificată), iar această clasificare, împreună cu atributele acestei entități, este detaliată într-o diagramă separată mai jos.

Cauza penală reprezintă aparent același lucru cu Dosarul penal (de aici 1 la 1). Însă în realitate, în timp ce Dosarul este containerul fizic și colecția de documente din aceasta, (agregă toate documentele care au legatura cu cauza penala), CauzaPenală este obiectul, materia procesului penal (faptele pe care le-a infaptuit cineva si care fac obiectul urmaririi si apoi judecarii). In Ordinul 138 se marchează în mod explicit această distincție prin definiția dosarului penal: ”Dosarul penal – mapă, sau dispozitiv special adaptat pentru păstrarea tuturor actelor procedurale, altor documente, obiecte sau materiale, ce se referă la o cauză penală concretă”. Mai mult, la un moment dat se poate intampla ca o cauza penala, (gestionata intr-un dosar) sa fie transferata prin conexare intr-un alta dosar. Din acest motiv au fost modelate ca entități diferite, care sunt însă într-o relație 1 la 1.

Conform modelului, într-o semnalare pot fi sesizate una sau mai multe **Fapte**. De asemenea, aceeași Faptă poate fi sesizată prin una sau mai multe Semnalări, ceea ce înseamnă ca poate fi sesizată ca atare prin mai multe Acte de sesizare. Din acest motiv, atributul de Număr unic (în Registrul R1) este al Actului de sesizare, nu al faptei sesizate.

Figura 3 de mai jos prezintă în detaliu, pentru entitatea **Persoană** și alte entități, care intră în relație cu aceasta, următoarele elemente:

- atributele importante ale domeniului conceptual care vor fi implementate în sistemul informatic cerut
- relațiile dintre entități, inclusiv cardinalitatea și multiplicitatea.

Atributele prezentate în diagramă reprezintă setul minimal de atribute pe care sistemul informatic cerut trebuie să aibă capabilitatea să le implementeze, fără ca diagrama să reprezinte o specificație exhaustivă, limitativă. În acest sens, în timpul implementării, pe baza rezultatelor fazelor de analiză, proiectare și configurare/dezvoltate, setul de atribute poate fi extins și cu alte atribute care vor fi considerate necesare de către Beneficiarul sistemului informatic.

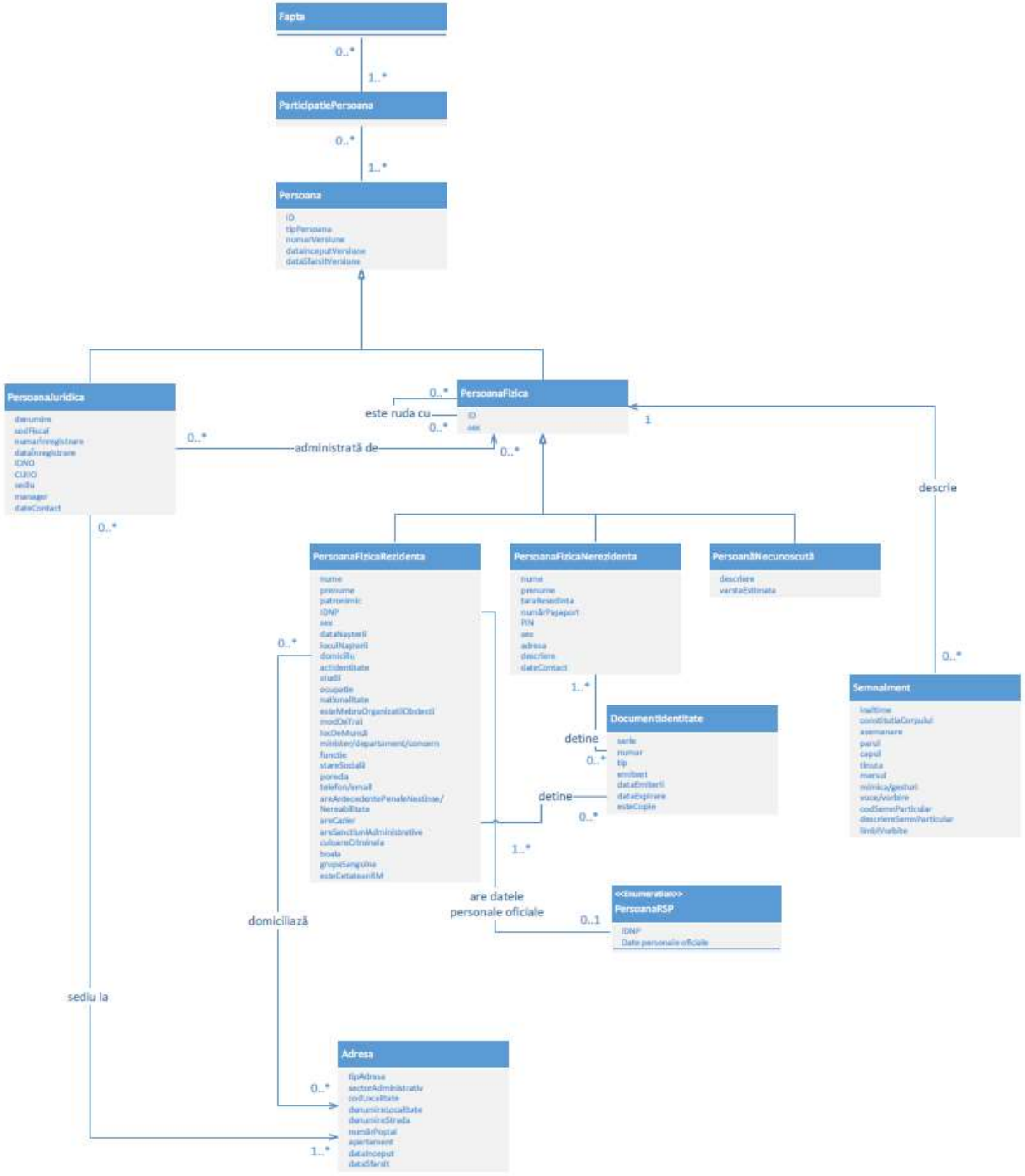


Figura 3.

În modelul de mai sus au fost reprezentate distinct principalele tipuri de persoane care vor fi gestionate în sistemul informatic, una din cele mai importante distincții fiind cea dintre **PersoanaFizică** și **PersoanaJuridică**, existând diferențe semnificative între atributele celor două subtipuri. La rândul său, PersoanaFizică este o generalizare a trei sub-tipuri importante, cele mai multe atribute fiind definite la nivelul persoanei fizice rezidente. Pentru acest tip de persoane, prin atributul IDNP, se stochează referință și la RSP - registrul național unic al persoanelor din Republica Moldova. Este important însă de precizat că pentru acest tip de persoană sistemul informatic nu va stoca doar o simplă referință la RSP, ci va stoca propria definiție a persoanei, conform celor rezultate în cercetarea penală, dar va permite în același timp identificarea definției oficiale a persoanei respective.

Persoanele necunoscute sunt un sub-tip de persoană fizică, cu atribute specifice (în principal cele legate de semnalmente) și se instanțiază individual în cadrul cauzei Penale. Cu alte cuvinte, atunci când în săvârșirea faptei este implicată o persoană necunoscută, ea va fi instanțiată ca o persoană, distinctă de alte alte instanțe de persoane de același tip, urmând ca pe parcursul cercetării penale să-i fie completate atributele, până devine o persoană cunocută, caz în care i se modifică tipul persoanei.

PersoanăFizicăNerezidentă reprezintă tot un tip de persoană fizică, cu atribute specifice persoanelor care se află temporar pe teritoriul Republicii Moldova și care sunt implicate într-o cauză penală.

3.3 Funcționalitățile furnizate de SIA e-Dosar MAI

Funcționalitățile furnizate de *SIA e-Dosar MAI* sunt:

UC01: Înregistrez sesizări

Reprezintă un caz de utilizare care se recepționează informația despre fapta care evenytual reprezintă infracțiune și se consemnează și se inregistrează plângerea, denunţul sau autodenunţul

UC02: Încep urmărirea penală

Reprezintă un caz de utilizare care reprezintă adoptarea deciziei de initiare sau refuz de initiere a urnaririi penale, consemnat în document procesual şi inregistrat in modul stabilit

UC03: Audiez persoane

Reprezintă un caz de utilizare care reprezintă activităţide audiere a părţilor procesuale (martor, victima, bănuit ş.a) în condiţiile legii cu perfectarea documentului procesual.

UC04: Dispun recunoaşterea calităţii

Reprezintă un caz de utilizare care reprezintă activităţide adoptare a unei decizii procesuale de confoirmare a statutului procesual a părţilor (victima, banuit s.a) in condiţiile legii cu perfectarea documentului procesual.

UC05: Consemnez declaraţiile persoanelor

Reprezintă un caz de utilizare care reprezintă activităţide audiere a părţilor procesuale (victima, banuit s.a) in condiţiile legii cu perfectarea documentului procesual dupa recunoaşterea calităţii.

UC06: Emit ordonanțe

Reprezintă un caz de utilizare care presupune adoptarea unei decizii procesuale de efectuare a activităţii speciale care vizează drepturile si obligaţiunile terţilor şi necesită sau nu avizarea procurorului ori instanţei judiciare.

UC07: Întocmesc procese-verbale

Reprezintă un caz de utilizare care presupune realizarea unei activităţi procesuale care vizează drepturile şi obligaţiunile terţilor cu intocmirea documentelor procesuale

UC08: Dispun efectuarea constatărilor și expertizelor

Reprezintă un caz de utilizare care presupune adoptarea unei decizii procesuale de efectuare a activităţii speciale care vizează implicarea specialiştilor care dispiun de cunoştinţe speciale necesare examinării unor dovezi sau tratarea unor fapte

UC09: Prezint documente procesuale spre aprobare procurorului

Reprezintă un caz de utilizare care presupune activităţile de prezentare a unor documente procesuale către procuror în vederea avizării sau acceptării acestora sau realizarea activităţilor procesuale

UC10: Contest indicațiile procurorului

Reprezintă un caz de utilizare care presupune activităţile de prezentare a contestaţiilor privind deciziile procesuale adoptate de către procuror

UC11: Recepționez cereri

Reprezintă un caz de utilizare care presupune recepționarea cererilor pentru efectuarea unor activităţi procesuale de la părţile implicate

UC12: Înaintez propuneri către procuror

Reprezintă un caz de utilizare care presupune prezentaea catre procuror a cererilor pentru efectuarea unor activităţi procesuale

UC13: Generez rapoarte statistice

Este o funcţionalitate accesibilă utilizatorilor sistemului care permite generarea rapoartelor planificate şi ad-hoc privind conţinutul informaţional al SIA e-dosar şi activitatea utilizatorilor. Rapoartele în cauză sunt utile pentru analiza bazei informaţionale a sistemului, performanţei activităţii participanţilor la evidenţa persoanelor străine şi anticiparea problemelor de securitate informaţională.

UC14: Analizez date

Reprezintă o funcţionalitate disponibilă ofițerului de urmarire penală, conducătorului acestuia, statistului ori analistului, precum şi a instituţiilor responsabile, utilizată pentru procesarea documentelor și datelor stocate SIA e-dosar

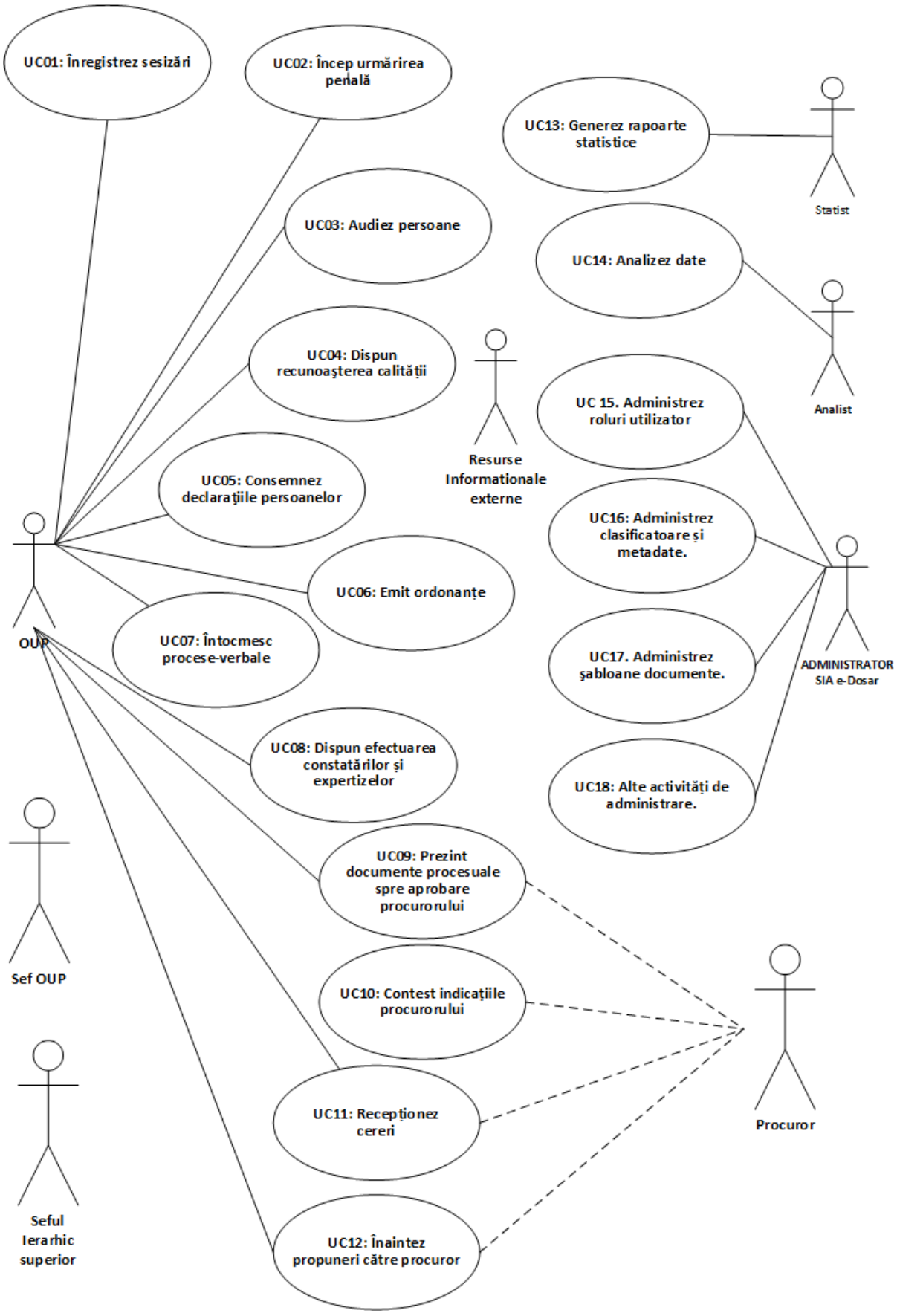
UC 15. Administrez roluri utilizator

Reprezintă un caz de utilizare care furnizează totalitatea funcţionalităţilor destinate Administratorului e-Dosar al MAI prin intermediul cărora acesta administrează lista de roluri şi drepturile asociate utilizatorilor autorizaţi. Sistemul va permite atașarea a mai multor roluri la un utilizator.

UC16: Administrez clasificatoare și metadate.

Reprezintă un caz de utilizare care furnizează totalitatea funcţionalităţilor destinate Administratorului SIA e-Dosar MAI prin intermediul cărora acesta administrează totalitatea clasificatoarelor şi metadatelor aferente soluţiei informatice (inclusiv interfaţa utilizator al sistemului informatic).

Figura 4. Cazurile de utilizare furnizate de SIA e-Dosar MAI



UC17. Administrez şabloane documente.

Reprezintă un caz de utilizare destinat Administratorului SIA e-Dosar MAI care descrie totalitatea funcţionalităţilor disponibile acestora pentru elaborarea modelelor de documente tipizate utilizabile în cadrul fiecărui tip de document de intrare sau ieşire.

UC18: Alte activități de administrare.

Reprezintă un caz de utilizare destinat Administratorului SIA e-Dosar MAI care descrie totalitatea funcţionalităţilor accesibile acestora, destinate administrării şi auditului SIA e-Dosar MAI: menţinerea listei şi integrităţii credenţialelor utilizatorilor pentru care interacţiunea se realizează prin intermediul certificatului digital şi extragerea rapoartelor din registrele de sistem în vederea analizei şi depistării unor eventuale probleme de securitate logică şi fizică a SIA e-Dosar MAI, etc.

Administratorului SIA e-Dosar MAI va dispune de un mecanism de administrare a profilurilor ale actorilor sistemului implicaţi în procesul de evidenţă a persoanelor străine. Acest mecanism va permite definirea parametrilor de acces la interfaţă, servicii, fişiere şi conţinutul bazei de date.

Cazul de utilizare de administrare a SIA e-Dosar MAI va implementa totalitatea funcţionalităţilor asigurării viabilităţii şi integrităţii SIA e-Dosar MAI (generarea copiilor de rezervă, restabilirea datelor, startarea/stoparea/restartarea serviciului, etc.).

Specificații privind cerințele față de componenta modelului proceselor de gestiune a cauzelor penale in vederea implementării unui flux automatizat de lucru la nivelul întregii organizații - WFMS (Work Flow Management System) sunt reflectate în anexa nr. 1 la aceste Termeni de Referință.

3.4 Interfața utilizatorului

SIA e-Dosar MAI trebuie să ofere o interfață utilizator ergonomică, intuitivă și accesibilă tuturor tipurilor de utilizatori (Utilizatori simpli și avansați). Interfața utilizator a sistemului informatic va fi accesată prin intermediul unui navigator Internet. *SIA e-Dosar MAI* trebuie să posede un design grafic intuitiv, agreabil, echilibrat și distinct optimizat pentru rezoluția minimă 1024x768 de lucru la calculatoarele de tip PC. De asemenea, interfața utilizator trebuie să fie responsivă pentru rezoluțiile dispozitivelor de tip smartphone și tabletă și optimizată pentru ecranele tactile. Pentru ușurința utilizatorilor, soluția informatică va dispune un sistem de ajutor contextual on-line, la nivelul fiecărei interfețe.

SIA e-Dosar MAI va furniza o interfață multilingvă (toate câmpurile și elementele incluse în clasificatoare vor fi disponibile în limba română, rusă și engleză). Procedurile de regăsire a informației și înregistrărilor vor fi realizate prin intermediul unor căutări simple (specificarea unor șiruri de căutare) sau a unor căutări de complexitate mai ridicată, prin intermediul cărora se poate realiza o filtrare mai exacta a informației (formulare QBE).

Adițional la modulul de căutare realizat pe baza principiului QBE care va da posibilitatea de a defini interogări sofisticate în mod vizual, interfața trebuie să ofere posibilitatea de a afina rezultatele căutării prin asigurarea posibilității filtrării datelor în lista cu rezultatele căutării. Mărimile indexate (valori din clasificatoare, nomenclatoare) trebuie să poată fi filtrate prin alegerea valorii din liste predefinite. Pentru câmpurile de tip numeric sau dată calendaristică trebuie să existe posibilitatea filtrării după valoarea exactă a caracteristicii căutate sau după masca de căutare.

Conținutul oricărui tabel cu rezultate sau formă electronică, în funcție de natura informației conținute, trebuie să poată fi exportat fie în format MS Execel, CSV, XML, JSON și PDF. Graficele vor fi bazate pe biblioteci recunoscute (Chart.js, HighCharts.js, Plotly.js, C3.js, etc.) fără

utilizarea Adobe Flash, și vor include opțiuni de personalizare (titlul, legende, zoom, tooltip, ajustarea la mărimea ecranului), vizualizare 2D sau 3D.

3.5 Documente utilizate în cadrul SIA e-Dosar MAI

Următoarele documente procesuale vor fi întocmite în cadrul SI e-Dosar MAI

#	**Denumire act**	**Tip act / referire normativă**	**Autor/ destinatar**
1.	Ordonanţa de începere a urmăririi penale	Act procedural Art. 274 CPP	OUP / Procuror
2.	Demers de prelungire a termenului de urmărire penală	Act procedural Art. 259 CPP	OUP / Procuror
3	Ordonanţa privind dispunerea expertizei	Act procedural Art. 144 CPP	OUP
4	Ordonanţa de percheziţie	Act procedural Art. 125 CPP	OUP/Procuror
5	Ordonanţa de ridicare	Act procedural Art. 126 CPP	OUP/Procuror(după caz)
6	Ordonanţa de punere sub sechestru	Act procedural Art. 205 CPP	OUP/Procuror
7	Ordonanţa de recunoaştere în calitate de parte vătămată	Act procedural Art. 59 CPP	OUP
8	Ordonanţă de recunoaştere în calitate de parte civilă	Act procedural Art. 61 CPP	OUP
9	Ordonanţă de recunoaştere în calitate de reprezentant legal	Act procedural Art. 77 CPP	OUP
10	Ordonanţa de recunoaştere în calitate de reprezentant	Act procedural Art. 79 CPP	OUP
11	Ordonanţa de recunoaştere în calitate de bănuit	Act procedural Art. 63 CPP	OUP
12	Ordonanţa de aplicare a măsurii procesuale de constrîngere	Act procedural Art.197, 198 CPP	OUP
13	Ordonanţa de aducere silită	Act procedural Art. 199 CPP	OUP
14	Ordonanţă de recunoaştere în calitate de corp delict	Act procedural Art. 160 CPP	OUP

15	Proces verbal de audiere a părţii vătămate	Act procedural Art. 111 CPP	OUP
16	Proces verbal de audiere a martorului	Act procedural Art. 109-110[1] CPP	OUP
17	Proces verbal de audiere a bănuitului	Act procedural Art. 103 CPP	OUP
18	Proces verbal de reţinere	Act procedural Art. 167 CPP	OUP/Procuror
19	Proces verbal de notificare despre dipunerea expertizei	Act procedural	OUP
20	Proces verbal de comunicare a raportului de expertiză	Act procedural	OUP
21	Proces verbal de confruntare	Act procedural Art. 113 CPP	OUP

Următoarele rapoarte vor fi întocmite în cadrul SI e-Dosar MAI:

#	**Denumire raport**	**Destinația**
1.	Raport privind depistarea bănuielii rezonabile despre comiterea infracţiunii	Şeful OUP
2	Raport privind propunerea de formare a grupului de ofiţeri de urmărire penală şi efectuarea urmăririi penale de către un grup de ofiţeri de urmărire penală	Procuror
3	Raport privind propunerea de transmitere a cauzei penale după competenţă	Procuror
4	Raport de iniţiere a procedurii de efectuare a percheziţiei	Procuror
5	Raport privind propunerea de ridicare a informaţiei de la instituţiile de telecomunicaţii	Procuror
6	Raport privind propunerea de scoatere a persoanei de sub urmărire penală	Procuror
7	Raport privind propunerea de încetare a urmăririi penale	Procuror
8	Raport privind propunerea de clasare a procesului penal	Procuror
9	Raport privind propunerea de suspendare a urmăririi penale	Procuror
10	Raport privind propunerea de punere sub învinuire	Procuror
11	Raport privind propunerea de terminare a urmăririi penale	Procuror
12	Raport privind propunerea de disjungere a cauzei penale	Procuror
13	Raport privind propunerea de conexare a cauzei penale	Procuror

14	Demers privind dispunerea efectuării măsurilor special de investigaţii	Procuror

3.6 Procesele supuse automatizării în cadrul SIA e-Dosar MAI

Tabelul de mai jos include procesele care vor fi automatizate în cadrul SIA e-Dosar MAI:

N/O	**Denumirea procesului**	**Participanţii şi rolurile lor în proces**	**Descrierea procesului**
1	Primirea şi înregistrarea sesizărilor cu privire la săvârşirea infracţiunii	Iniţiator: OUP Coordonator și decident: șeful OUP	Ofițerul de urmărire penală sesizat despre săvârșirea sau pregătirea despre săvârșirea infracţiunii, întocmeşte un proces verbal cu privire la consemnarea plângerii, denunţului sau autodenunţului şi dispune înregistrarea imediată a infracțiunii în Registrul nr. 1 de evidență a sesizărilor cu privire la infracțiuni. După înregistrare, ofițerul de urmărire penală prezintă imediat sesizările conducătorului organului de urmărire penală sau adjunctului acestuia, care organizează soluționarea lor în conformitate cu prevederile art. 274 Cod de procedură penală (în continuare CPP). În cazul în care ofițerul de urmărire penală constatat o bănuială rezonabilă cu privire la săvârșirea unei infracţiuni, acesta întocmeşte un proces-verbal în care consemnează cele constatate şi concomitent dispune înregistrarea imediată a autosesizării pentru a începe urmărirea penală. Persoanei care a depus plângerea sau denunţul ofițerul de urmărire penală îi eliberează imediat un certificat despre acest fapt. Conducătorul organului de urmărire penală retrage, în cazurile prevăzute de lege, prin ordonanță motivată materialele (sesizările) repartizate unui ofiţer de urmărire penală şi le transmite altui ofiţer de urmărire penală, cu informarea procurorului care conduce urmărirea penală.
2	Începerea urmăririi penale	Iniţiator și decident: OUP Coordonator și decident: șeful OUP	Ofițerul de urmărire penală sesizat în modul prevăzut în art. 262 şi art. 273 CPP, dispune imediat sau, după caz, în termen de 30 zile prin ordonanţă, începerea urmăririi penale, în cazul în care, din cuprinsul actului de sesizare sau al actelor de constatare rezultă o bănuială rezonabilă că a fost săvârşită o infracţiune şi nu există vreuna din circumstanţele care exclud urmărirea penală, informând despre aceasta persoana care a înaintat sesizarea sau organul respectiv. Ofițerul de urmărire penală eliberează victimei un certificat despre începerea urmăririi penale. Ordonanţa de începere a urmăririi penale, în termen de 24 de ore de la data începerii urmăririi penale, este adusă la cunoştinţă în scris procurorului care efectuează conducerea activităţii de urmărire penală, prezentându-i-se totodată şi dosarul respectiv.

			Conducătorul organului de urmărire penală după începerea urmăririi penale și pe parcursul acesteia retrage, în cazurile prevăzute de lege, prin ordonanţă motivată cauzele penale repartizate unui ofiţer de urmărire penală şi le transmite altui ofiţer de urmărire penală, cu informarea procurorului care conduce urmărirea penală.
3	Neînceperea urmăririi penale	Inițiator: OUP Decident: procurorul	Dacă din cuprinsul actului de sesizare rezultă vreunul din cazurile care împiedică pornirea urmăririi penale, ofițerul de urmărire penală înaintează procurorului actele întocmite cu propunerea de a nu porni urmărirea penală. Ofițerul de urmărire penală începe urmărirea penală în cazul în care procurorul consideră că nu sânt circumstanţe care împiedică urmărirea penală şi restituie actele, cu ordonanţa sa, pentru începerea urmăririi penale.
4	Audierea victimei	Inițiator: OUP	Ofițerul de urmărire penală audiază victima în condițiile prevăzute pentru audierea martorului, întocmind un proces-verbal. În cazurile în care victima minoră, în vârstă de până la 14 ani, urmează să fie audiată în cauzele penale privind infracţiunile cu caracter sexual, privind traficul de copii sau violenţa în familie, precum şi în alte cazuri în care interesele justiţiei sau ale minorului o cer, ofițerul de urmărire penală înaintează procurorului o propunere scrisă de audiere a acesteia în condițiile speciale prevăzute de art. 110^1 CPP.
5	Recunoaşterea şi audierea în calitate de parte vătămată	Inițiator şi decident: OUP	Ofițerul de urmărire penală obține acordul scris al victimei de recunoaștere în calitate de parte vătămată sau dezacordul scris cu această calitate. Dacă persoana fizică sau juridică şi-a dat acordul să fie recunoscută în calitate de parte vătămată şi se constată că i-a fost cauzat un prejudiciu, fizic sau material, ofițerul de urmărire penală emite o ordonanţă prin care dispune recunoaştere persoanei în calitate de parte vătămată. În cazul în care, după recunoaşterea persoanei ca parte vătămată, s-au constatat circumstanţe care atestă lipsa cauzării prejudiciului, ofițerul de urmărire penală încetează participarea acestei persoane ca parte vătămată în procedura respectivă prin ordonanţă motivată. După ce a recunoscut persoana în calitate de parte vătămată, ofițerul de urmărire penală purcede la audierea acesteia, întocmind în acest sens un proces-verbal de audiere a părţii vătămate. În cazurile în care partea vătămată minoră, în vârstă de până la 14 ani, urmează să fie audiată în cauzele penale privind infracţiunile cu caracter sexual, privind traficul de copii sau violenţa în familie, precum şi în alte cazuri în care interesele justiţiei sau ale minorului o cer, ofițerul de urmărire penală înaintează procurorului o propunere scrisă de audiere a acesteia în condițiile speciale prevăzute de art. 110^1 CPP.

6	Recunoaşterea în calitate de parte civilă	Iniţiator şi decident: OUP	Ofițerul de urmărire penală obține cererea scrisă a persoanei fizice sau juridice de chemare în judecată a bănuitului, învinuitului, inculpatului sau a persoanelor care poartă răspundere patrimonială pentru faptele acestuia. În vederea recunoașterii persoanei fizice sau juridice ofițerul de urmărire penală emite o ordonanță, dacă există suficiente temeiuri de a considera că persoanei vizate în urma infracţiunii i-a fost cauzat un prejudiciu material sau moral. Sistarea participării persoanei în calitate de parte civilă se decide de către ofițerul de urmărire penală prin ordonanță, dacă se constată că, după recunoașterea părţii civile, cererea de chemare în judecată a fost depusă de o persoană necorespunzătoare sau că, din alte motive, lipsesc temeiuri pentru ca persoana să aibă calitate de parte civilă.
7	Recunoaşterea şi audierea persoanei în calitate de bănuit	Iniţiator şi decident: OUP	În vederea recunoașterii în calitate de bănuit ofițerul de urmărire penală întocmește, după caz, unul din următoarele acte procedurale: 1) procesul-verbal de reținere; 2) ordonanţa de recunoaştere a persoanei în calitate de bănuit. Declaraţiile bănuitului, învinuitului se consemnează în procesul-verbal al audierii, întocmit în conformitate cu prevederile art. 260 şi 261 CPP. Despre prelungirea termenului de menţinere în calitate de bănuit mai mult de 3 luni, ofițerul de urmărire penală informează imediat bănuitul.
8	Admiterea, desemnarea şi înlocuirea apărătorului	Iniţiator: OUP Decident: procurorul	Ofițerul de urmărire penală solicită coordonatorului oficiului teritorial al Consiliului Naţional pentru Asistenţă Juridică Garantată de Stat desemnarea avocatului care acordă asistenţă juridică garantată de stat: 1) la cererea bănuitului, învinuitului; 2) în cazul în care participarea apărătorului la procesul penal este obligatorie, iar bănuitul, învinuitul, nu are apărător ales. Ofițerul de urmărire penală cere de la biroul de avocaţi înlocuirea apărătorului ales sau solicită oficiului teritorial al Consiliului Naţional pentru Asistenţă Juridică Garantată de Stat substituirea avocatului care acordă asistenţă juridică garantată de stat în următoarele situaţii dificile de desfăşurare a procesului penal: 1) dacă apărătorul ales nu poate să se prezinte în cazul reţinerii, audierii bănuitului; 2) dacă apărătorul ales nu poate să participe la desfăşurarea procesului în decurs de 5 zile din momentul anunţării lui. În cazul în care bănuitul/învinuitul depune cererea de renunțare la apărător ofițerul de urmărire penală o anexează la materialele cauzei şi informează procurorul pentru a decide asupra acesteia.
9	Recunoaşterea în calitate de parte civilmente responsabilă	Iniţiator şi decident: OUP	Persoana fizică sau juridică este recunoscută ca parte civilmente responsabilă prin ordonanța ofițerului de urmărire penală. Încetarea participării persoanei la proces în calitate de parte civilmente responsabilă se efectuează prin ordonanța ofițerului de urmărire penală în cazul în care se constată că,

			după recunoaşterea părţii civilmente responsabile, persoana respectivă nu poartă răspundere materială pentru prejudiciul material cauzat de către învinuit, inculpat sau că din alte motive lipsesc temeiuri pentru ca persoana să fie în calitate de parte civilmente responsabilă. Ofițerul de urmărire penală audiază partea civilmente responsabilă în calitate de martor, întocmind un proces-verbal.
10	Recunoaşterea în calitate de reprezentanți legali ai victimei, părţii vătămate, părţii civile, bănuitului, învinuitului	Iniţiator şi decident: OUP	Ofițerul de urmărire penală admite prin ordonanță în calitate de reprezentanți legali ai victimei, părții vătămată și bănuitului în cazul care aceștia sunt incapabili. În cazul în care victima, partea vătămată și bănuitul incapabili nu au reprezentanţi legali, ofițerul de urmărire penală prin ordonanță numește din oficiu ca reprezentant legal autoritatea tutelară. Dacă, după admiterea persoanei în calitate de reprezentant legal al victimei, părţii vătămate, părţii civile, bănuitului, învinuitului, se constată lipsa temeiurilor de a o menține în această calitate, ofițerul de urmărire penală dispune prin ordonanță motivată încetarea participării acesteia la proces în calitate de reprezentant legal. Reprezentantul legal poate fi audiat de către ofițerul de urmărire penală în calitate de martor, întocmindu-se în acest sens un proces-verbal.
11	Recunoaşterea în calitate de succesor al părții vătămate sau părții civile și audierea acestora	Iniţiator şi decident: OUP Decident: procurorul în cazul prevăzut de lege	Ofițerul de urmărire penală decide prin ordonanță privitor la recunoaşterea unei rude apropiate ca succesor al părţii vătămate sau al părţii civile, cu condiţia că ruda apropiată solicită această calitate. Atunci când mai multe rude apropiate solicită să fie recunoscute în această calitate, ofițerul de urmărire penală expediază solicitările procurorului pentru a lua decizia de a alege succesorul. Succesorul părţii vătămate sau al părţii civile poate fi audiat către ofițerul de urmărire penală în calitate de martor, întocmindu-se în acest sens un proces-verbal.
12	Audierea persoanei în calitate de martor	Iniţiator şi decident: OUP	În legătură cu audierea persoanei în calitate de martor, ofițerul de urmărire penală întocmește un proces-verbal în care consemnează declarațiile acestuia. Ofițerul de urmărire penală va întocmi o propunere scrisă procurorului de audiere a martorului, în condițiile prevăzute de art. 110 Cod de procedură penală (modalităţi speciale de audiere a martorului şi protecţia lui), dacă există motive temeinice de a considera că viaţa, integritatea corporală sau libertatea martorului ori a unei rude apropiate a lui sânt în pericol în legătură cu declarațiile pe care acesta le face într-o cauză penală privind o infracţiune gravă, deosebit de gravă sau excepţional de gravă. În cazurile în care martorul minor, în vârstă de până la 14 ani, urmează să fie audiat în cauzele penale privind infracţiunile cu caracter sexual, privind traficul de copii sau violenţa în familie, precum şi în alte cazuri în care interesele justiţiei sau ale minorului o cer, ofițerul de urmărire penală înaintează procurorului o propunere scrisă

			de audiere a acesteia în condițiile speciale prevăzute de art. 110^1 CPP.
13	Efectuarea confruntării	Inițiator și decident: OUP	Confruntarea se efectuează de către ofițerul de urmărire penală din oficiu sau la cererea participanților în proces. În cazul în care există divergențe între declarațiile persoanelor audiate în aceeași cauză, se procedează la confruntarea acestor persoane, inclusiv cu cele ale căror declarații sânt defavorabile bănuitului, învinuitului, dacă este necesar, pentru aflarea adevărului și înlăturarea divergențelor. Declarațiile persoanelor confruntate se consemnează de către ofițerul de urmărire penală într-un proces-verbal.
14	Verificarea declarațiilor la locul infracțiunii	Inițiator și decident: OUP	Pentru a verifica sau a preciza declarațiile martorului, părții vătămate, bănuitului, învinuitului despre evenimentele infracțiunii săvârșite într-un loc concret, ofițerul de urmărire penală este în drept să se prezinte la locul infracțiunii împreună cu persoana audiată și, după caz, cu apărătorul, interpretul, specialistul, reprezentantul legal și să propună persoanei audiate să descrie circumstanțele și obiectele despre care a făcut sau poate face și acum declarații. Despre verificarea declarațiilor la locul infracțiunii ofițerul de urmărire penală întocmește un proces-verbal.
15	Prezentarea persoanelor sau obiectelor spre recunoaștere	Inițiator și decident: OUP	În legătură cu prezentarea persoanei spre recunoaștere (inclusiv după fotografia acesteia, în cazul în care prezentarea persoanei este imposibilă) martorului, părții vătămate, bănuitului și învinuitului, ofițerul de urmărire penală întocmește un proces-verbal, cu excepția că cel recunoscut nu ia cunoștință la moment de procesul-verbal de recunoaștere și nu îl semnează. Proces-verbal va fi întocmit de ofițerul de urmărire penală și în cazul în care prezintă un obiect spre recunoaștere.
16	Cercetarea la fața locului	Inițiator și decident: OUP Decident: procurorul în cazul prevăzut de lege	Ofițerul de urmărire penală pentru a efectua cercetarea la fața locului a încăperii sau a domiciliului va obține inițial acordul în scris al proprietarului sau al posesorului ori, în lipsa acestuia, al unuia dintre membrii majori ai familiei sale. Dacă lipsește acordului în scris de cercetare la fața locului, ofițerul de urmărire penală va emite o ordonanță în acest sens pe care o va prezenta procurorului, însoțită de un raport cu propunerea de autorizare a cercetării la fața locului la judecătorul de instrucție. În cazurile infracțiunilor flagrante, precum și în cazurile ce nu permit amânare, ofițerul de urmărire penală solicită, în mod de excepție, procurorului să dispună prin ordonanță motivată efectuarea cercetării la fața locului în domiciliu. Judecătorul de instrucție trebuie să fie informat despre efectuarea acestei acțiuni în termen de 24 de ore, iar în scop de control, cu prezentarea materialelor cauzei penale în care sânt argumentate acțiunile de urmărire penală efectuate.

			Despre efectuarea cercetării la fața locului ofițerul de urmărire penală va întocmi un proces-verbal.
17	Examinarea corporală	Iniţiator şi decident: OUP Decident: procurorul în cazul prevăzut de lege	Pentru a efectua examinarea corporală ofițerul de urmărire penală urmează să obțină inițial consimțământul bănuitului, învinuitului, martorului sau părţii vătămate, pentru a constata dacă pe corpul lor există urme ale infracţiunii sau semne particulare, în cazul în care pentru aceasta nu este necesară expertiza judiciară medico-legală. Dacă bănuitul, învinuitul, martorul sau partea vătămată nu-și dau consimțământul pentru examinarea corporală, ofițerul de urmărire penală va emite o ordonanță motivată în acest sens pe care o va prezenta procurorului, însoțită de propunerea de a înainta judecătorului un demers în vederea autorizării acțiunii respective. În caz de infracțiune flagrantă, ofițerul de urmărire penală va solicita procurorului să emită o ordonanță cu privire la dispunerea examinării corporale însă, în termen de 24 de ore, judecătorul de instrucție urmează să fie informat despre acțiunea efectuată, cu prezentarea materialelor respective ale cauzei pentru controlul legalităţii acestei acţiuni. Privitor la efectuarea examinării corporale ofițerul de urmărire penală întocmește un proces-verbal.
18	Exhumarea cadavrului	Iniţiator şi decident: OUP Decident: procurorul	În vederea exhumării cadavrului ofițerul de urmărire penală emite o ordonanță motivată pe care o expediază procurorului cu propunerea de înaintare a demersului către judecătorul de instrucție pentru autorizarea acțiunii. Înainte de efectuarea exhumării cadavrului, ofițerul de urmărire penală va înștiința în scris rudele comunicând despre timpul efectuării acțiunii procesuale. Exhumarea cadavrului se materializează de către ofițerul de urmărire penală printr-un proces-verbal.
19	Reconstituirea faptei și experimentul în procedura de urmărire penală	Iniţiator: OUP	Organul de urmărire penală, din oficiu sau la cererea participanţilor la proces, precum şi instanţa de judecată, la cererea părţilor, considerând că este necesar pentru verificarea şi precizarea unor date, pot proceda la reconstituirea, integrală sau parţială, a faptei la faţa locului, cu participarea făptuitorului, prin reproducerea acţiunilor, situaţiei sau a altor circumstanţe în care s-a produs fapta. În scopul verificării şi precizării datelor ce au importanţă pentru cauza penală şi care pot fi reproduse în condiţiile efectuării unor experimente şi a altor activităţi de investigaţii, organul de urmărire penală este în drept să efectueze un experiment în procedura de urmărire penală. Despre efectuarea reconstituirii faptei şi experimentului ofițerul de urmărire penală întocmește proces-verbal.
20	Dispunerea şi autorizarea percheziţiei	Iniţiator și decident: OUP Decident: procurorul,	Pentru a efectua percheziție (inclusive percheziția corporal) ofițerul de urmărire penală va întocmi o ordonanță motivată pe care o va prezenta procurorului cu propunerea de înaintare judecătorului de instrucție a demersului de obținere a autorizației de efectuare a percheziției.

		în cazul prevăzut de lege	În cazurile ce nu suferă amânare sau în caz de delict flagrant, ofițerul de urmărire penală solicită procurorului să întocmească o ordonanță motivată de dispunere a percheziției, fără autorizarea judecătorului de instrucție. Percheziţia corporală se poate efectua fără întocmirea ordonanţei despre aceasta şi fără autorizaţia judecătorului de instrucție: 1) la reținerea bănuitului, învinuitului, inculpatului; 2) la aplicarea față de bănuit, învinuit, inculpat a măsurii preventive de arestare; 3) în cazul în care există suficiente temeiuri de a presupune că persoana prezentă în încăperea unde se efectuează percheziţia sau ridicarea poate purta asupra sa documente sau alte obiecte care pot avea importanță probatorie în cauza penală. La efectuarea percheziției în baza ordonanței motivate a procurorului ofițerul de urmărire penală va pune imediat la dispoziția acestuia materialele obținute în urma percheziției pentru a le prezenta judecătorului de instrucție. Percheziția se materializează de ofițerul de urmărire penală printr-un proces-verbal.
21	Efectuarea ridicării	Inițiatorul: OUP Decident: procurorul, în cazul prevăzut de lege.	Ofițerul de urmărire penală pentru a efectua ridicarea este obligat să întocmească inițial o ordonanță motivată. Ridicarea în domiciliu poate fi efectuată de către ofițerul de urmărire penală dor după obținerea permisiunii proprietarului care urmează să fie materializată printr-un acord scris. În cazul în care proprietarul nu-şi exprimă acordul pentru efectuarea ridicării în domiciliu, ofițerul de urmărire penală va prezenta ordonanța de ridicare procurorului, însoțită de propunerea de înaintare a demersului către judecătorul de instrucție de obținere a autorizației de efectuare a ridicării. Aceiași procedură de ridicare este specifică şi pentru ridicarea documentelor ce conţin informaţii care constituie secret de stat, comercial, bancar, precum şi a informaţiilor privitoare la convorbirile telefonice. Dacă obiectele sau documentele lipsesc la locul indicat în ordonanţa de ridicare, ofițerul de urmărire penală va solicita procurorului să dispună prin ordonanță efectuarea percheziției, fără autorizarea judecătorului de instrucție, întocmind despre aceasta un proces-verbal de efectuare a percheziției. În aceste situații, ofițerul de urmărire penală va prezintă actele întocmite în legătură cu percheziția procurorului pentru ca acesta să informeze imediat, dar nu mai târziu de 24 de ore, judecătorul de instrucție. Despre efectuarea ridicării ofițerul de urmărire penală va întocmi un proces-verbal de ridicare.
22	Dispunerea efectuării măsurilor speciale de investigaţie	Inițiator: OUP Decident: procurorul	Ofițerul de urmărire penală înaintează procurorului un demers de autorizare a următoarelor măsuri speciale de investigație: a) identificarea abonatului, proprietarului sau a utilizatorului unui sistem de comunicaţii electronice ori al unui punct de acces la un sistem informatic; b) urmărirea vizuală; c) controlul transmiterii banilor sau a altor valori materiale extorcate; d) investigaţia sub acoperire; e)

			supravegherea transfrontalieră; f) livrarea controlată; g) colectarea mostrelor pentru cercetarea comparată; h) cercetarea obiectelor şi documentelor; i) achiziţia de control. Ofițerul de urmărire penală solicită procurorului să înainteze un demers judecătorului de instrucție pentru autorizarea următoarelor măsuri speciale de investigație: cercetarea domiciliului şi/sau instalarea în el a aparatelor ce asigură supravegherea şi înregistrarea audio şi video, a celor de fotografiat şi de filmat; b) supravegherea domiciliului prin utilizarea mijloacelor tehnice ce asigură înregistrarea; c) interceptarea şi înregistrarea comunicărilor şi imaginilor; d) reţinerea, cercetarea, predarea, percheziţionarea sau ridicarea trimiterilor poştale; e) monitorizarea conexiunilor comunicaţiilor telegrafice şi electronice; f) monitorizarea sau controlul tranzacţiilor financiare şi accesul la informaţia financiară; g) documentarea cu ajutorul metodelor şi mijloacelor tehnice, precum şi localizarea sau urmărirea prin sistem de poziţionare globală (GPS) ori prin alte mijloace tehnice; h) colectarea informaţiei de la furnizorii de servicii de comunicaţii electronice. În cazul în care este necesară efectuarea măsurilor speciale de investigație cum sunt: a) chestionarea; b) culegerea informaţiei despre persoane şi fapte; c) identificarea persoanei, ofițerul de urmărire penală, prin dispoziție scrisă, va solicita conducătorului subdiviziunii specializate dispunerea şi efectuarea acestora. Asupra măsurilor speciale de investigație se dispune de către persoanele împuternicite (procuror, conducătorul subdiviziunii specializate) prin ordonanță, după caz, cu sau fără autorizarea judecătorului de instrucție. Efectuarea măsurilor speciale de investigație se consemnează într-un proces verbal de către ofițerul de investigație sau, după caz, de ofițerul de urmărire penală. Ofițerul de urmărire penală prezintă prin scrisoare organului abilitat prin lege extrasul din încheierea judecătorului de instrucţie, autentificat de către acesta, privind dispunerea efectuării interceptării comunicărilor. Recepționând informaţia obţinută în procesul interceptării şi înregistrării comunicărilor, ofițerul de urmărire penală, în termen de 24 de ore după expirarea termenului de autorizare a interceptării, întocmeşte la finele fiecărei perioade de autorizare, un proces-verbal privind interceptarea şi înregistrarea comunicărilor. La sfârşitul perioadei autorizate pentru interceptarea şi înregistrarea comunicării, ofițerul de urmărire penală prezintă procurorului procesul-verbal al interceptării şi suportul în original pe care a fost înregistrată informaţia. Ofițerul de urmărire penală este în drept să reţină, să cerceteze, să predea, să percheziţioneze sau să ridice trimiterile poştale în baza ordonanței procurorului, cu autorizarea judecătorului de instrucție.
	Efectuarea şi certificarea interceptării şi înregistrării comunicărilor		

	Reţinerea, cercetarea, predarea, percheziţionarea sau ridicarea trimiterilor poştale Monitorizarea conexiunilor comunicaţiilor telegrafice şi electronice		Ordonanţa cu privire la reţinerea, cercetarea, predarea, percheziţionarea sau ridicarea trimiterilor poştale cu autorizaţia respectivă se transmite de către ofiţerul de urmărire penală şefului instituţiei poştale. Despre fiecare examinare şi ridicare a trimiterilor poştale ofiţerul de urmărire penală întocmeşte un proces-verbal. Ofițerul de urmărire penală. fiind informat de către instituțiile care prestează servicii de livrare a corespondenţei electronice, a apelurilor de intrare şi ieşire sau a altor comunicări despre aflarea în posesia lor a comunicărilor ce urmează a fi supuse verificării, ia cunoștință imediat de conținutul acestora și, nu mai târziu de 48 de ore din momentul recepţionării informaţiei, adoptă o decizie privind ridicarea acesteia sau transmiterea ei pentru livrare ulterioară, cu fotografierea, copierea sau fixarea prin alt mijloc tehnic a conţinutului comunicării. Despre ridicarea informațiilor telegrafice sau electronice se întocmește un proces-verbal.
23	Dispunerea constatării tehnico-științifică și medico-legală	Iniţiator şi decident: OUP	Ofițerul de urmărire penală dispune efectuarea constatării tehnico-ştiinţifice printr-un demers în care stabileşte obiectul acesteia, formulează întrebările la care trebuie să se răspundă specialistul şi stabileşte termenul în care va fi efectuată lucrarea.
24	Dispunerea expertizelor	Iniţiator şi decident: OUP	Expertiza poate fi dispusă de către ofițerul de urmărire penală din oficiu sau la cererea părților. Considerând că este necesară efectuarea expertizei, ofiţerul de urmărire penală emite o ordonanţă de dispunere a efectuării acesteia şi printr-o scrisoare o expediază instituției de expertiză. Ordonanţa de dispunere a expertizei, inițial este adusă la cunoştinţa părţilor, fiind întocmit un proces-verbal de notificare despre dispunerea expertizei. Raportul de expertiză se aduce la cunoștința părților, întocmindu-se despre aceasta un proces-verbal de comunicare a raportului de expertiză. În cazul în care raportul expertului nu este clar sau are unele deficienţe, pentru înlăturarea cărora nu sânt necesare investigaţii suplimentare, ori a apărut necesitatea de a preciza metodele aplicate de către expert sau unele noţiuni, ofiţerul de urmărire penală este în drept să audieze expertul după regulile de audiere a martorului, întocmind despre aceasta un proces-verbal.
25	Recuzarea interpretului, traducătorului, specialistului, expertului;	Iniţiator şi decident: OUP	Recuzarea interpretului, traducătorului, specialistului şi expertului se soluţionează de către ofițerul de urmărire penală prin ordonanță motivată.
26	Colectarea mostrelor pentru		Despre colectarea mostrelor necesare pentru cercetarea comparativă, ofițerul de urmărire penală emite o ordonanţă

	cercetare comparativă		motivată, iar despre efectuarea acesteia întocmeşte un proces-verbal. În cazul în care bănuitul, învinuitul, partea vătămată sau martorul nu-şi dau acordul la prelevarea mostrelor de eliminări ale corpului sau a altor mostre biologice, ofiţerul de urmărire penală expediază ordonanţa de prelevare a mostrelor pentru cercetare comparativă procurorului cu propunerea de înaintare a demersului judecătorului de instrucţie pentru obţinerea autorizaţiei.
27	Restituirea corpurilor delicte	Iniţiator: OUP Decident: Procurorul	Ofiţerul de urmărire penală, cu încuviinţarea procurorului, până la soluționarea cauzei penale, dispune prin ordonanță (care se prezintă spre aprobare procurorului) restituirea către proprietarul sau posesorul legal: 1) a produselor uşor alterabile; 2) a obiectelor necesare acestuia pentru viaţa cotidiană; 3) a animalelor domestice, pasărilor, altor animale care necesită îngrijire permanentă; 4) a automobilului sau a unui alt mijloc de transport, dacă acesta nu a fost sechestrat pentru asigurarea acţiunii civile în cauza penală sau a posibilei confiscări speciale a bunurilor.
28	Contestarea indicațiilor procurorului	Iniţiator: OUP Decident: Procurorul ierarhic superior	Fiind în dezacord cu indicațiile procurorului cu privire la efectuarea unor acţiuni procesuale, ofiţerul de urmărire penală întocmește o contestație pe care o expediază procurorului ierarhic superior.
29	Abţinerea sau recuzarea ofiţerului de urmărire penală	Iniţiator: OUP Decident: procurorul	Ofiţerul de urmărire penală recepționează cererea de recuzare de la participanții procesului, investiți cu dreptul de recuzare. Totodată, dacă există motive de recuzare, ofiţerul de urmărire penală este obligat să întocmească declaraţia de abţinere de la efectuarea urmăririi penale. Declaraţia de abţinere sau cererea de recuzare se expediază în decurs de 24 ore procurorului care conduce urmărirea penală. Conducătorul organului de urmărire penală în baza ordonanţei procurorului de recuzare desemnează un alt ofiţer de urmărire penală pentru efectuarea urmăririi penale.
30	Reţinerea persoanei bănuite de comiterea infracţiunii	Iniţiator şi decident: OUP	În cazul reţinerii unei persoane bănuite de săvârşirea unei infracţiuni ofiţerul de urmărire penală, în termen de până la 3 ore de la momentul privării ei de libertate, întocmeşte un proces-verbal de reţinere. Persoana reținută poate fi supusă percheziţiei corporale, fără întocmirea unei ordonanțe și fără autorizarea judecătorului de instrucție. Despre efectuarea percheziției corporale ofițerul de urmărire penală întocmește un proces-verbal separat. Ofițerul de urmărire penală, în timp de o oră după reținerea persoanei, solicită în scris, inclusiv prin fax sau la telefon, oficiului teritorial al Consiliului Naţional pentru Asistenţă

			Juridică Garantată de Stat sau unor alte persoane împuternicite de acesta desemnarea unui avocat de serviciu pentru acordarea asistenţei juridice de urgenţă. Bănuitului i se înmânează în scris informaţia despre drepturile sale, acest fapt menționându-se într-un proces-verbal separat. Stabilind prezenţa unor vătămări sau leziuni corporale la persoana reținută, ofițerul de urmărire penală informează neîntârziat procurorul. Ofițerul de urmărire penală înaintează propunere procurorului cu privire la eliberarea bănuitului reţinut până la autorizarea arestării de către instanţă.
31	Informarea despre reținere	Inițiator și decident: OUP	Despre reţinerea minorului, ofițerul de urmărire penală comunică imediat părinţilor minorului sau persoanelor care îi înlocuiesc. Întocmind procesul-verbal de reţinere, imediat, dar nu mai târziu de 6 ore, ofițerul de urmărire penală este obligat să dea posibilitate persoanei reţinute să anunţe una din rudele apropiate sau o altă persoană, la propunerea reţinutului, despre locul unde acesta este deţinut sau o anunţă singur, întocmind despre aceasta un proces-verbal separat. Dacă persoana reținută este cetăţean al unui alt stat, ofițerul de urmărire penală va informa imediat, dar nu mai tîrziu de 6 ore, despre reţinere ambasada sau consulatul acestui stat, atunci când persoana reţinută o cere. Despre reţinerea unui militar, în termenul menționat în aliniatul precedent, ofițerul de urmărire penală informează unitatea militară, în care acesta îşi îndeplineşte serviciul militar, sau centrul militar unde este la evidenţă, implicit rudele apropiate sau o altă persoană, la propunerea reţinutului. Atunci când există necesitatea prevenirii unui risc grav pentru viaţa, libertatea sau integritatea fizică a unei persoane, asigurării secretului etapei începătoare a urmăririi penale, prevenirii prejudicierii procedurilor penale, prevenirii săvârşirii unei alte infracţiuni sau a protejării victimelor infracţiunilor, ofițerul de urmărire penală solicită procurorului să înainteze judecătorului de instrucție un demers cu privire la autorizarea amânării înştiinţării despre reţinere, pe un termen de până la 12 ore, cu excepţia cazului în care persoana reţinută este minoră. În termen de până la 3 ore de la reţinere, ofițerul de urmărire penală prezintă procurorului o comunicare în scris despre reţinere.
32	Luarea măsurilor de ocrotire	Inițiator și decident: OUP	Constatând că în urma reţinerii, rămân fără supraveghere minori sau alte persoane (recunoscute iresponsabile, persoane cărora li s-a instituit curatelă sau persoane care, din cauza vârstei, bolii sau din alte cauze, au nevoie de ajutor) pe care le are la întreţinere reţinutul ori bunurile acesteia, ofițerul de urmărire penală este obligat să transmită rudelor apropiate ale reținutului, în cazul în care își exprimă acordul, iar autorităților tutelare, precum și conducătorii instituţiilor medicale sau sociale de stat să le

			ceară să ia măsuri de ocrotire a persoanelor vizate, întocmind despre aceasta o ordonanță. Ofițerul de urmărire penală este obligat să asigure, de asemenea, supravegherea bunurilor persoanei reținute, inclusiv îngrijirea şi hrănirea animalelor domestice, la cerinţa şi din contul acestuia, dispunând prin ordonanță conducătorilor instituțiilor de stat supravegherea și îngrijirea bunurilor. Ofițerul de urmărire penală dispune prin ordonanță asupra măsurilor de ocrotire în privinţa persoanelor care se aflau sub ocrotirea părţii vătămate, în privinţa bunurilor şi domiciliului acesteia. Despre măsurile de ocrotire ofițerul de urmărire penală informează neîntârziat persoana reţinută, arestată preventiv sau arestată la domiciliu, precum şi alte persoane interesate.
33	Măsurile preventive	Iniţiator: OUP Decident: procurorul	Ofițerul de urmărire penală înaintează propuneri procurorului cu privire la alegerea, prelungirea, modificarea şi revocarea măsurilor preventive.
34	Obligarea de a se prezenta la organul de urmărire penală Aducerea silită Amenda judiciară Punerea sub sechestru	Iniţiator şi decident: OUP: Iniţiator şi decident: OUP Iniţiator: OUP Decident: Procurorul și judecătorul de instrucție	Pentru asigurarea desfăşurării normale a procesului penal, ofițerul de urmărire penală poate obliga în scris bănuitul, partea vătămată, martorul, precum şi alte persoane participante la proces să se prezinte la organul de urmărire penală la data şi ora fixată, iar în caz de schimbare a domiciliului, imediat să informeze despre aceasta. Aducerea forțată a persoanei la organul de urmărire penală se dispune de către ofițerul de urmărire penală prin ordonanță în cazurile prevăzute de lege. Ofițerul de urmărire penală, în cazurile în care constată abateri în cursul urmăririi penale, înaintează un demers judecătorului de instrucție pentru aplicarea amenzii judiciare. Pentru punerea bunurilor bănuitului sau învinuitului sub sechestru ofițerul de urmărire penală întocmește o ordonanță motivată pe care o prezintă procurorului cu propunerea de înaintare a demersului judecătorului de instrucție în vederea obținerii autorizației. În caz de delict flagrant sau de caz ce nu suferă amânare, ofițerul de urmărire penală va solicita procurorului să dispună prin ordonanță punerea bunurilor sub sechestru, fără autorizaţia judecătorului de instrucţie, prezentând ulterior imediat materialele procurorului pentru comunicarea judecătorului de instrucţie. Despre punerea bunurilor sub sechestru ofițerul de urmărire penală întocmește un proces-verbal.
35	Măsuri de protecție	Iniţiator şi decident: OUP	Ofițerul de urmărire penală, în cazurile prevăzute de Legea cu privire la protecţia martorilor şi altor participanţi la procesul penal, este obligat să aplice prin ordonanță *măsuri urgente* față de participantul la procesul penal aflat în stare de pericol care impune măsuri imediate de

		Decident: Procurorul, în cazurile prevăzute de lege	asigurare a securităţii, informând despre aceasta procurorul în decurs de 24 ore. De asemenea, în cazul în care se impune aplicarea *măsurilor de protecţie* ofițerul de urmărire penală va solicita procurorului să dispună asupra aplicării acestora. Ofițerul de urmărire penală este obligat să dispună imediat eliberarea ordinului de restricţie de urgenţă în privinţa agresorului, în caz de stabilire la locul faptei, ca urmare a evaluării riscurilor, a circumstanţelor din care rezultă o bănuială rezonabilă că au fost comise acte de violenţă în familie şi/sau persistă un pericol iminent de repetare sau comitere a acţiunilor violente. Dacă se constată, în cadrul urmăririi penale, că victima violenţei în familie, se află în pericol de a fi supusă violenţei sau altor acţiuni ilegale, inclusiv de distrugere a bunurilor sale, ofițerul de urmărire penală este obligat din oficiu sau la cererea victimei să intervină neîntârziat, înaintând un demers în instanța de judecată pentru eliberarea ordonanței de protecție.
36	Măsuri de înlăturare a condițiilor care au contribuit la săvârșirea infracțiunilor și altor încălcări ale legislației	Iniţiator și decident: OUP	Constatând existenţa unor cauze şi condiţii care au contribuit la săvârşirea infracţiunii, descoperind cazuri de încălcare a legislaţiei în vigoare sau a drepturilor şi libertăţilor omului, ofițerul de urmărire penală este obligat să sesizeze organul respectiv sau persoana cu funcţie de răspundere cu privire la luarea unor măsuri pentru înlăturarea acestor cauze şi condiţii, implicit organele de stat respective în privinţa încălcărilor de lege.
37	Citarea	Iniţiator și decident: OUP	Ofițerul de urmărire penală cheamă o persoană în fața organului de urmărire penală prin citație scrisă, notă telefonică sau telegrafică, prin telefax ori prin mijloace electronice, poșta electronică sau prin orice alt sistem de mesagerie electronică în cazul în care se dispune de mijloacele tehnice necesare pentru a dovedi că citaţia a fost primită.
38	Cererile și demersurilor în procesul penal	Iniţiator și decident: OUP	În caz de respingere, parţială sau totală, a cererii sau, după caz, a demersului organizaţiei obşteşti ori al colectivului de muncă, organul de urmărire penală adoptă o ordonanţă, care este adusă la cunoştinţă solicitantului.
39	Modificarea în actele procedurale, corectarea erorilor materiale și înlăturarea unor omisiuni vădite	Iniţiator și decident: OUP	În cazul unor erori materiale evidente din cuprinsul unui act procedural sau în cazul unei omisiuni vădite în care nu s-a pronunţat asupra sumelor pretinse de martori, experţi, interpreţi, traducători, apărători, asupra restituirii obiectelor, corpurilor delicte sau a ridicării măsurilor asiguratorii, precum şi a altor măsuri, ofițerul de urmărire penală corectează eroarea sau înlătură omisiunea vădită, întocmind despre aceasta un proces-verbal.
40	Termenele de urmărire penală	Iniţiator: OUP	În cazul în care este necesar a prelungi termenul de urmărire penală, ofițerul de urmărire penală întocmeşte un

		Decident: Procurorul	demers motivat în acest sens şi îl prezintă procurorului înainte de expirarea termenului fixat de acesta.
41	Efectuarea urmăririi penale de către mai mulţi ofiţeri de urmărire penală	Inițiator: șeful OUP	Conducătorul organului de urmărire penală, în cazul unor cauze complicate sau de mari proporţii, dispune prin ordonanță efectuarea urmăririi penale de către mai mulţi ofiţeri de urmărire penală, cu informarea procurorului.
42	Dispoziția și delegația ofițerului de urmărire penală	Inițiator și decident: șeful OUP	Ofițerul de urmărire penală dispune prin dispoziţie organelor de poliţie sau altor organe competente cu privire la reținere, aducerea forțată, arestare şi la alte acţiuni procesuale, precum şi le solicită ajutor la efectuarea acţiunilor de urmărire penală. Ofițerul de urmărire penală, în cazul în care anumite acţiuni de urmărire penală trebuie să fie efectuate în afara teritoriului în care se face urmărirea penală, poate să le efectueze personal sau să dispună, prin delegaţie, efectuarea acestor acţiuni altui organ respectiv. De asemenea, ofițerul de urmărire penală dispune prin delegație Agenţiei de Recuperare a Bunurilor Infracţionale efectuarea investigaţiilor financiare paralele în vederea urmăririi bunurilor infracţionale, acumulării probelor cu privire la acestea şi indisponibilizării lor în cazurile prevăzute de lege.
43	Verificarea competenței	Inițiator: OUP Decident: procurorul	Dacă ofițerul de urmărire penală constată că nu este competent a efectua urmărirea penală, imediat, dar nu mai târziu de 3 zile, trimite cauza procurorului care exercită conducerea urmăririi penale pentru a o transmite organului competent.
44	Conexarea și disjungerea cauzelor penale	Iniţiator: OUP Decident: Procurorul	În cazul în care se constată temeiuri pentru conexitate sau disjungere, ofițerul de urmărire penală întocmește un raport prin care propune procurorului adoptarea hotărârii respective.
45	Propunerea de punere sub învinuire	Iniţiator: OUP Decident: Procurorul	Ofițerul de urmărire penală, în cazul în care există suficiente probe că infracţiunea a fost săvârșită de o anumită persoană, întocmeşte un raport cu propunerea de a pune persoana respectivă sub învinuire și de alegere a măsurii preventive, pe care îl înaintează procurorului.
46	Scoaterea persoanei de sub urmărire penală	Iniţiator: OUP Decident: Procurorul	Stabilind existența temeiurilor prevăzute de lege, organul de urmărire penală înaintează procurorului un raport cu privire la propunerea de scoatere a persoanei de sub urmărirea penală.
47	Încetarea urmăririi penale	Iniţiator: OUP Decident: Procurorul	Stabilind unul din temeiurile prevăzute de lege, organul de urmărire penală înaintează procurorului un raport cu privire la propunerea de încetare a urmăririi penale.

48	Clasarea procesului penal	Iniţiator: OUP Decident: Procurorul	În cazul în care OUP/procurorul consideră că se întrunesc condițiile prevăzute de lege pentru, ofițerul de urmărire penală întocmește un raport cu propunerea de clasare a procesului penal, pe care îl prezintă procurorului.
49	Suspendarea și reluarea urmăririi penale	Iniţiator: OUP Decident: Procurorul	Atunci când există unul din temeiurile care împiedică continuarea şi terminarea urmăririi penale, ofițerul de urmărire penală înaintează procurorului propunerile sale împreună cu dosarul pentru a lua decizia de suspendare a urmăririi penale. La dispariția motivelor suspendării urmăririi penale sau atunci când a devenit necesară efectuarea unor acţiuni de urmărire penală, ofițerul de urmărire penală propune procurorului să reia urmărirea penală.
50	Investigaţiile în vederea căutării învinuitului	Iniţiator: OUP Decident: Procurorul	Dacă nu se cunoaşte locul unde se află persoana pusă sub învinuire, precum şi în cazul în care învinuitul, după înaintarea învinuirii, se ascunde de organul de urmărire penală, ofițerul de urmărire penală înaintează procurorului propunerea pentru dispunerea investigaţiilor în vederea găsirii învinuitului.
51	Terminarea urmăririi penale	Iniţiator: OUP Decident: Procurorul	Constatând că probele administrate sânt concludente şi suficiente pentru a termina urmărirea penală, organul de urmărire penală înaintează procurorului dosarul însoţit de un raport, în care consemnează rezultatul urmăririi, cu propunerea de a dispune una din soluţiile prevăzute în art. 291 Cod de procedură penală.

4. Infrastructura hardware și telecomunicații

Sistemul e-Dosar va funcționa cu echipamente întreținute de MAI în spațiile sale. Furnizorul va primi informații suplimentare despre echipamentele hardware disponibile.

5. Profilul companiei selectate

Ofertanții vor îndeplini următoarele cerințe minime:

• Minim cinci (5) ani de experiență solidă în proiectarea și dezvoltarea soluțiilor TIC de natură și complexitate similară.

• Experiență în dezvoltarea sistemelor informaţionale TIC.

Ofertantul furnizează următoarele informații în cadrul ofertei sale:

• Descrierea detaliată a companiei;
• Copia documentelor de înregistrare;
• Portofoliul companiei, specificând proiecte similare implementate;
• Descrierea unor soluții TIC similare;

Personal-cheie disponibil

Ofertantul va descrie personalul-cheie propus, luând în considerare următoarele poziții:

• Manager de proiect;
• Arhitect de sistem;
• Analist al business-proceselor.

Cerințe minime pentru funcția de manager de proiect:

• Diplomă universitară în domeniul TIC, cu cel puțin cinci (5) ani de experiență profesională, în special în managementul proiectelor;

• Cunoașterea eficientă a limbii române și engleze sunt esențiale;

• Experiență profesională dovedită în managementul de proiect prin realizarea a cel puțin trei (3) proiecte preferabile în dezvoltarea IT.

• Certificatele recunoscute în domeniul managementului proiectelor vor constitui un avantaj.

Cerințe minime pentru arhitectul sistemului:

• Diplomă universitară în domeniul TIC, cu cel puțin cinci (5) ani de experiență în arhitectura sistemelor;

• Cunoașterea eficientă a limbii române și engleze;

• Experiență dovedită ca arhitect de sistem în proiecte TIC care dezvoltă soluții TIC.

• Prezentarea în cadrul ofertei a certificatelor recunoscute în domeniul tehnologiilor vor reprezenta un avantaj.

Cerințe minime pentru poziția analistului business-proceselor:

• Diplomă universitară în domeniul TIC, cu cel puțin trei (3) ani de experiență în ingineria cerințelor și analiză business-proceselor în proiecte TIC;

• Cunoaștere excelentă a limbii române și ruse;

• Experiență profesională dovedită în dezvoltarea informațiilor similare în calitate de analist al business-proceselor.

6. Atenuarea riscurilor, monitorizarea și dezvoltarea sistemului e-Dosar

Beneficiarul recomandă dezvoltarea sistemului e-Dosar utilizând o metodologie de dezvoltare iterativă care presupune dezvoltarea prototipurilor sistemului informațional adăugând funcționalitățile de bază în mod incremental în timpul implementării proiectului.

Metodologia de dezvoltare iterativă presupune un model de dezvoltare ciclică, care facilitează controlul dezvoltării sistemului prin dezvoltarea de prototipuri pentru a diminua riscul apariției cerințelor funcționale, care nu au fost definite sau concepute la stadiul analizei funcționale. Fiecare iterație va avea ca scop dezvoltarea progresivă a noilor segmente de sistem, care sunt ulterior integrate pas cu pas cu funcționalitățile dezvoltate anterior și testate în comun cu Beneficiarul.

Pe parcursul fiecărui ciclu de iterație, Furnizorul împreună cu Beneficiarul vor testa noile funcționalități dezvoltate și vor revizui / ajusta funcționalitățile care urmează să fie dezvoltate, urmărind scopul creării unei viziuni comune a caracteristicilor sistemului e-Dosar.

C. Specificații tehnice, cerințe funcţionale şi nefuncţionale a SI „e-Dosar”

Acest capitol conține specificaţiile tehnice, redate prin tabele cu lista cerințelor obligatorii (OBL) şi celor dezirabile (DES), care trebuie întrunite de Ofertant. Nerespectarea acestor cerințe duce la descalificarea propunerii;

7. Cerinţele funcţionale

Cerințele funcționale ale cazului de utilizare UC01

Nr.	Obligativitate	Descrierea cerinței funcționale
1	*OBL*	*SIA e-Dosar MAI va furniza un mecanism de aplicare a criteriilor de filtrare individuale sau multiple de filtrare a datelor cu privire la cauze penale*
2	*OBL*	*Utilizatorii vor avea posibilitatea de a selecta operatorul în cazul criteriilor multiple (și, sau, se conține în, nu se conține în, în perioada, cu excepția perioadei, etc.).*
3	OBL	*În cazul câmpurilor de selecție cu valori multiple, portalul va utliza funcționalitatea auto-comlete cu AJAX server-side scripting pentru îmbunătățirea performanței.*
4	OBL	*Utilizatorii SIA e-Dosar MAI vor avea posiblitatea să grupeze și să salveze criteriile de căutare.*
5	OBL	*SIA e-Dosar MAI va prevedea un mecanism configurabil de restricționarea a numărul de elemente maxime care vor fi intoarse în rezultatul căutărilor.*
6	OBL	*Aplicația va folosi un mechanism de tip CAPTCHA pentru identificarea actorilor umani și evitarea accesărilor multiple din partea unor scripturi sau programe de tip roboți.*
7	OBL	*Administrator de System va dispune de functionalitatea de deconectare a mechanismului CAPTCHA sa de a mari gradul de complexitate a confirmarii.*
8	OBL	*SIA e-Dosar MAI va dispune de un mecanism de setare a dependenței câmpurilor (conditional fields). De exemlu, în cazul selectării teriroriului municipiului Chişinău, utilizatorul va avea posibilitatea să selecteze în cămpul cuvenit doar un Inspectorat de poliţie sau alt organ.*

Cerințele funcționale ale cazului de utilizare UC02

Nr.	Obligativitate	Descrierea cerinței funcționale
1	*OBL*	*SIA e-Dosar MAI va livra utilizatorilor un mecanism de generare a rapoartelor generale, a rapoartelor personalizate în baza criteriilor de filtrare descrise în UC01 și a rapoartelor comparative.*
2	*OBL*	*Rapoartele preconfigurate se vor genera preventiv, imediat după actualizarea datelor în sistem, pentru a micșora numărul de solicitări concomitente către Stocul de Date. Structura rapoartelor va fi coordonată și aprobată de către Ministerul Afacerilor Interne, în comun cu Biroul Naţional de Statistică.*
3	OBL	*Dezvoltatorul va configura cel puțin următoarele rapoarte cu privire la starea infracţionalităţii:* *Infractiuni inregistrate dupa tipul infractiunii,* *Infractiuni inregistrate pe categorii de infractiuni, in profil teritorial,* *Infractiuni inregistrate pe raioane, dupa tipul infractiunii,* *Infractiuni inregistrate la 100 000 locuitori, dupa tipul infractiunii, in profil teritorial,* *Infractiuni grave inregistrate dupa tipul infractiunii,* *Infractiuni grave pe categorii, in profil teritorial,*

Nr.	Obligativitate	Descrierea cerinței funcționale
		Infractiuni impotriva persoanelor dupa tipul infractiunii pe medii, *Infractiuni legate de droguri, in profil teritorial,* *Infractiuni impotriva copiilor dupa tipul infractiunii,*
4	OBL	*Rapoartele preconfigurate se vor genera pe perioada anului pentru care datele sunt cele mai recente. De exemplu, dacă datele cele mai recente se referă la luna Decembrie, 2018, raportul generat în Ianuarie 2019 va reflecta datele pentru perioada Ianuarie 2018-Decembrie 2018.*
5	OBL	*Rapoartele statistice vor putea fi generate pentru orice perioadă disponibilă. Dezvoltatorul va asigura migrarea datelor respective din RICC în Stocul de Date a SIA e-Dosar MAI.*
6	*OBL*	*SIA e-Dosar MAI va preîmtâmpina utilizatorii care vor selecta perioadele pentru care datele nu sunt disponibile sau nu sunt comparabile.*

Cerințele funcționale ale cazului de utilizare UC03

Nr.	Obligativitate	Descrierea cerinței funcționale
1	*OBL*	*SIA e-Dosar MAI va dispune de funcționalitatea de afișare a datelor în formă grafică.*
2	*OBL*	*Utilizatorii portalului vor avea posiblitatea de a exporta graficele afișate în format PNG sau JPG.*
3	OBL	*Utilizatorii vor selecta tipul graficului care va fi afișat (linie, plăcintă/pie, coloană, etc.).*
4	OBL	*Utilizatorii vor dispune de funcționalitatea de a mări/focalilza informația din grafic (zoom in/out), de deconectare a etichetelor/legendei.*
5	OBL	*SIA e-Dosar MAI va ajusta mărimea graficelor la dimensiunile ecranului utilizatorului.*
6	*OBL*	*SIA e-Dosar MAI va permite forarea datelor în adâncime, de la global, la detaliu, sau de la detaliu la global, cu ajutorul dispozitivului de indicare (mouse, trackball, etc.).*

Cerințele funcționale ale cazului de utilizare UC04

Nr.	Obligativitate	Descrierea cerinței funcționale
1	*OBL*	*Un utilizator care vizualizează un raport în cadrul sistemului, trebuie să-l poată exporta într-un fișier extern redactabil (MS Excel, PDF, XLS, CSV, DOC).*
2	*OBL*	*Toate vizualizările și rapoartele generate de SIA e-Dosar MAI trebuie să poată fi imprimate pe formatul de pagină indicat. Aplicația trebuie să dimensioneze automat documentele de ieșire pentru a se încadra în formatul indicat de utilizator (exemplu: A2/A3/A4/A5, portrait/landscape etc.).*
3	OBL	*Implicit, rapoartele vor fi extrase în format MS Excel.*
4	OBL	*Seturile de date de dimensiuni mari vor fi arhivate în mod automat pentru a micșora traficul prin intermediul rețelei.*
5	OBL	*Utilizatorii vor dispune de funcționalitatea de a se abona la notificările cu privire la actualizarea datelor.*

Cerințele funcționale ale cazului de utilizare UC05

Nr.	Obligativitate	Descrierea cerinței funcționale
1	*OBL*	*SIA e-Dosar MAI trebuie să fie în măsură să ofere un număr de rapoarte de statistică și ad-hoc, astfel încât Administratorii de Sistem să poată monitoriza activitatea utilizatorilor, performanța aplicației și gradul de utilizare a resurselor.*
2	*OBL*	*În total dezvoltatorul va implementa până la 4 categorii de rapoarte predefinite solicitate de beneficiar.*
3	OBL	*In faza de analiză, Dezvoltatorul va identifica și va coordona lista finală a rapoartelor necesare.*

Cerințele funcționale ale cazului de utilizare UC06

Nr.	Obligativitate	Descrierea cerinței funcționale
1	*OBL*	*SIA e-Dosar MAI va dispune de mecanism de gestiune a nomenclatoarelor, clasificatoarelor ce conțin totalitatea metadatelor destinate configurării sistemului și interpretării datelor stocate în Baza de Date.*
2	*OBL*	*SIA e-Dosar MAI va prelua nomenclatoarele şi clasificatoarele din RICC.*
3	OBL	*Pentru clasificatoarele specificate la FR 06.02 şi, după caz, specificate de Deținător, se vor limita drepturile de efectuare a modificărilor.*
4	OBL	*SIA e-Dosar MAI nu va permite eliminare unei categorii de metadate dacă aceasta este utilizată cel puțin într-o înregistrare a bazei de date.*
5	OBL	*SIA e-Dosar MAI va oferi mecanism de versionare a valorilor metadatelor și stabilite a intervalului de timp aferent validității valorilor metadator.*
6	*OBL*	*SIA e-Dosar MAI va permite configurarea clasificatoarelor liniare și ierarhice (în care unele valori pot avea valori părinte).*
7	*DES*	*SIA e-Dosar MAI va oferi mecanism de export şi import a clasificatoarelor din interfața utilizator în format XML și CSV. Drepturile de import și export vor fi atribuite utilizatorilor cu rolul de Administrator de Sistem.*
8	*DES*	*SIA e-Dosar MAI va furniza interfață destinată monitorizării funcționării curente (Heartbeat service).*
9	OBL	*Administratorul de Sistem va putea să genereze copiile de rezervă ale Stocului de Date și să restabilească funcționalitatea sistemului în baza acestor copii.*
10	OBL	*Dezvoltatorul va configura o procedură automatizată de rezervare a datelor (fișiere, cod sursă și baza de date)*

Cerințele funcționale ale cazului de utilizare UC07

Nr.	Obligativitate	Descrierea cerinței funcționale
1	*OBL*	*SIA e-Dosar MAI va publica automat seturile de date prin intermediul compartimentelor specializate ale Portalului Datelor Deschise (http://date.gov.md):* *Instituţii / Ministerul Afacerilor Interne:*

Nr.	Obligativitate	Descrierea cerinței funcționale
		https://date.gov.md/ckan/ro/dataset?sort=score+desc%2C+metadata_modified+desc&q=&organization=1138-ministerul-afacerilor-interne
2	*OBL*	*Administratorul de Sistem va putea defini și publica categoriile și structura seturilor de date care urmează a fi publicate.*
3	OBL	*SIA e-Dosar MAI va permite configurarea frecvenței de publicare a rapoartelor publice din interfața utilizator cu rolul de Administrator de Sistem.*
4	OBL	*Web serviciul/API-ul destinat publicării seturilor de date deschise, publice va fi disponibil și prin platforma de interoperabilitate (MConnect), în scopul publicării automatizate a datelor publice pe portalul www.date.gov.md.*
5	DES	*Documentaia completă cu instrucțiuni de integrare a API-ului www.date.gov.md va fi transmisă echipei de dezvoltatori selectate.*

Cerințele funcționale ale cazului de utilizare UC08

Nr.	Obligativitate	Descrierea cerinței funcționale
1	*OBL*	*SIA e-Dosar MAI va pune la dispoziția Administratorului de Sistem funcționalitatea de actualizare a Stocului de Date. Procedura de actualizare va fi una manuală sau automatizată. Operatorul tehnico-tehnologic va exporta setul de date din și îl va importa cu ajutorul unui script de import, care va ține cont de FR. 08.02.*
2	*OBL*	*Dezvoltatorul va propune o soluție de verificare a integrității datelor recepționate.*
3	OBL	*SIA e-Dosar MAI va notifica în mod automat utilizatorii abonați cu privire la apariția unui set de date actualizat.*
4	OBL	*Dezvoltatorul va configura un script de import a noului set de date în Stocul de Date.*
5	OBL	*Ofertantul câștigător va proiecta baza de date a SIA e-Dosar MAI ținând cont de volumul mare de date care va fi stocat și număr mare de utilizatori potențiali.*
6	*OBL*	*În scopul evitării unor incompatibilități ale datelor exportate din/în SIA e-Dosar MAI este necesar ca tipul și structura BD să fie coorodonată cu STI MAI.*
7	*DES*	*Dezvoltatorul va propune o soluție de desfășurare de tip high-availability cluster pentru baza de date proiectată.*

8. Cerinţele nefuncţionale

8.1 Cerințe de licențiere și proprietate intelectuală

Ministerul de Interne va deține toate drepturile necesare pentru utilizarea pe termen nelimitat a *SIA e-Dosar MAI* și a tuturor componentelor soft necesare bunei funcționări a *SIA e-Dosar MAI.*

Mai jos sunt specificate cerințele aferente licențierii și drepturilor de proprietate intelectuală aferente *SIA e-Dosar MAI* și componentelor soft necesare funcționării sistemului.

1. Vor fi asigurate următoarele medii de operare pentru SIA e-Dosar MAI :

Mediul de producție;

Mediul de testare.

2. Ofertantul va include în oferta sa licențele pentru toate produsele soft de tip COTS, necesare implementării și utilizării SIA e-Dosar MAI în mediile puse la dispoziție de MAI. Aici sunt incluse următoarele: sisteme de operare, sisteme de gestiune baze de date, biblioteci software, utilitare și alt soft de sistem.

3.Cantitatea licențelor oferite trebuie să permită accesarea și utilizarea SIA e-Dosar MAI (în orice mediu în care funcționează) de cel puțin 500 de utilizatori concurenți. Nu vor exista restricții cu privire la numărul tranzacții sau mod de accesare a SIA e-Dosar MAI (ex. limitări la accesare concurentă).

4. Ofertantul va transmite către MAI toate drepturile asupra dezvoltărilor, ajustărilor, configurărilor și personalizărilor efectuate pentru implementarea SIA e-Dosar MAI conform cerințelor. Acestea pot fi aferente produselor soft terțe licențiate, sau pot fi componente elaborate în cadrul proiectului.

5. Ofertantul va prezenta modelul său de licențiere propus pentru SIA e-Dosar MAI care trebuie să corespundă cerințelor LIPR 001 – LIPR 004. Ofertantul va descrie modelul de licențiere propus, argumentând de ce acesta este cel optim pentru MAI. Va prezenta o analiză comparativă cu alte modele de licențiere oferite de obicei pentru soluția ofertată.

8.2 Cerințe pentru arhitectura de sistem

Arhitectura *SIA e-Dosar MAI* trebuie să fie aliniată la necesitățile *MAI* în aspectele ce țin de flexibilitatea și mentenanța sistemului informatic. *Ministerul de Interne* optează pentru o arhitectură deschisă, modulară, bazată pe componente interoperabile. Aceste principii trebuie să fie vizibile la toate nivelele arhitecturii *SIA e-Dosar MAI.* Cerințe generale ale arhitecturii SIA e-Dosar MAI sunt următoarele***:***

1. Arhitectura SIA e-Dosar MAI trebuie să fie bazată pe standarde deschise.

2. Arhitectura SIA e-Dosar MAI trebuie să fie orientată pe servicii (SOA).

3. Arhitectura SIA e-Dosar MAI va fi concepută integrat, dezvoltată cu aplicarea celor mai bune practici în domeniu (exemplu: principii de arhitectură și arhitecturi de referință aliniate TOGAF 9.1).

4. Arhitectura SIA e-Dosar MAI va fi una de tip client-server, organizată în cel puțin 2 nivele verticale, divizate clar, astfel încât fiecare nivel superior să depindă doar de nivelul său inferior.

5. Arhitectura SIA e-Dosar MAI trebuie să fie adaptată la implementarea și utilizarea în mediile virtualizate.

8.3 Cerințe pentru Platforma tehnologică

Platforma tehnologică este formată din totalitatea componentelor software și hardware necesare pentru a asigura mediul de operare în care va rula *SIA e-Dosar MAI.* Platforma tehnologică include: platforme de dezvoltare și limbaje de programare în care este elaborat codul sistemului informatic, sisteme de gestiune a bazelor de date, sisteme de operare pe baza cărora pot

rula componentele sistemului, asigurare program specifică necesară a fi instalată pentru rularea corecta a sistemului informatic, platforma hardware pe care rulează componentele sistemului etc.

Pentru a avea sistemul scalabil, flexibil și ușor mentenabil, trebuie să existe un nivel minim de dependență a sistemului față de platforma tehnologică pe care rulează componentele sale.

8.4 Cerințe generale față de platforma tehnologică a SIA e-Dosar MAI

Mai jos sunt redate cerințele nefuncționale generale înaintate platformei tehnologice a SIA e-Dosar MAI.

1. Tehnologiile de platformă prezente în arhitectura SIA e-Dosar MAI trebuie să fie tehnologii larg cunoscute și implementate în R. Moldova. Cel puțin alți 3 furnizori trebuie să presteze servicii de menținere și dezvoltare soluții pe platformele respective pe piața locală.

2. Componentele SIA e-Dosar MAI trebuie să fie independente de platforma tehnologica pe care rulează.

3. Arhitectura sistemului trebuie să fie optimizată pentru rularea în medii de tipul cloud computing. Caracteristici ale unui sistem cu arhitectură orientată spre implementarea soluțiilor Cloud, sunt: conștient de latență, conștient de căderi de componente, paralelizabil, conștient de utilizarea resurselor.

4. Tehnologiile prezente la nivelul platformei tehnologice trebuie să fie omogene (număr minim de tehnologii diferite, exemplu: aceleași sisteme de operare pentru middleware și baza de date).

5. SIA e-Dosar MAI trebuie să suporte crearea, modificarea, procesarea, stocarea și accesarea textului în format Unicode.

6. Ofertantul va indica în oferta sa informația completă și exhaustivă privind platformele tehnologice suportate de aplicația sa și constrângerile relevante.

8.5 Cerințele de performanță

SIA e-Dosar MAI trebuie să dețină capacitatea de a procesa în timp util tranzacțiile efectuate de utilizatori. Mai jos sunt redate cerințele de performanță la care trebuie să răspundă *SIA e-Dosar MAI.*

1. Timpul de răspuns la o interogare tranzacțională utilizator nu trebuie să depășească 3 secunde (nu se refera și la generarea de rapoarte).

2. SIA e-Dosar MAI trebuie să poată gestiona până la 500 de sesiuni concurente cu posibilitatea scalabilității pînă la 1000 de sesiuni concurente.

3. Ofertantul va include în ghidurile de administrare și operare a SIA e-Dosar MAI informație privind procesele ce pot diminua performanța SIA e-Dosar MAI și recomandările sale privind rularea concurentă a acestor procese (exemplu: nu se recomanda rularea procesului X de generare a rapoartelor zilnice, simultan cu procesul Y de generare a copiei de rezervă).

4. Generarea rapoartelor și accesarea informației în scopul analizelor de business nu trebuie să afecteze performanța operațională a sistemului la nivelul procesării tranzacțiilor.

5. În documentația sistemului vor fi identificate rapoartele cu impact semnificativ asupra performanței și formulate recomandările Ofertantului privind generarea rapoartelor respective astfel încât să nu influențeze indicii de performanță a SIA e-Dosar MAI.

6. Ofertantul va indica în oferta sa valorile minime garantate pentru caracteristicele de performanță ale SIA e-Dosar MAI , cu referință la platforma tehnologica recomandată.

8.6 Cerințele pentru mentenabilitate

Pentru ca *SIA e-Dosar MAI* să fie disponibil și accesibil utilizatorilor la nivelul agreat, acesta trebuie să fie continuu monitorizat și menținut. Sistemul informatic trebuie să permită identificarea proactivă a problemelor și prevenirea acestora prin derularea facilă a activităților de mentenanță operațională la nivelul tuturor componentelor sistemului. Caracteristicile de mentenanță aferente *SIA e-Dosar MAI sunt:*

1. SIA e-Dosar MAI va deține mecanisme de monitorizare a nivelului de încărcare și funcționare pentru toate componentele cheie.

2. SIA e-Dosar MAI va genera notificări în cazul în care performanța componentelor sale degradează (exemplu: timpul de răspuns la interogările utilizatorilor depășește 10 secunde).

3. Toate erorile și excepțiile în funcționarea SIA e-Dosar MAI vor fi înregistrate.

4. Ofertantul va enumera mijloacele ce vor fi utilizate la depanarea tehnică a SIA e-Dosar MAI.

5. Ofertantul va pregăti mijloace ce facilitează funcțiile de administrare a SIA e-Dosar MAI :

- tratarea componentelor sistemului;
- restartarea componentelor sistemului,
- crearea copiei de rezervă a bazei de date și fișierelor de conținut,
- restaurarea funcționalității SIA e-Dosar MAI în baza copiei de rezervă indicată,

6. Codul sursa al SIA e-Dosar MAI va fi elaborat conform recomandărilor pentru scrierea codului sursa ușor de întreținut, inclusiv: bine structurat, însoțit de comentarii, variabile sugestive etc.

7. Arhitectura SIA e-Dosar MAI va permite implementarea într-o manieră simplistă pentru MAI a schimbărilor la nivelul sistemului. Perimetrul afectat de modificări va fi minim, iar componentele necesar a fi testate în rezultatul modificărilor, clar identificabile.

8. SIA e-Dosar MAI va permite definirea și rularea sarcinilor programate pentru activități de menținere operațională (exemplu: arhivare date, pregătire date pentru rapoarte operaționale, etc.).

8.7 Cerințele pentru scalabilitate

Pe parcursul utilizării *SIA e-Dosar MAI*, este posibil ca numărul de utilizatorilor concurenți să crească sau să scadă simțitor de la o perioadă la alta. Pentru a avea o utilizare rațională a resurselor de procesare, sistemul informatic trebuie să fie ușor scalabil (în sus și în jos). Cerințe privind caracteristicile de scalabilitate aferente *SIA e-Dosar MAI:*

1. SIA e-Dosar MAI va permite creșterea capacității de procesare fără a întrerupe funcționarea acestora. În acest scop, sistemul va suporta extinderea pe orizontală a capacității de procesare (exemplu: adăugarea de noi noduri server și efectuare balansare a încărcării).

2. SIA e-Dosar MAI va putea fi configurat pentru scalare automată la nivelul componentelor cheie (lag sensitive). Scalarea sistemului se va face atât în sus, cât și în jos.

3. SIA e-Dosar MAI trebuie să dețină posibilitatea de a deservi practic un număr nelimitat de sesiuni, cu condiția alocării corespunzătoare a resurselor de procesare și stocare date. Resursele vor fi alocate pe orizontală (alocare noi servere, fără creșterea performanței pe serverele existente).

8.8 Cerințele pentru asigurarea securității

SIA e-Dosar MAI trebuie să permită un control adecvat asupra riscurilor de securitate a informației aferente utilizării. Măsurile de securitate implementate trebuie să fie aliniate la

politicile de securitate aprobate și să asigure prevenirea, detectarea și reacționarea adecvata la incidentele de securitate.

În acest compartiment sunt stabilite cerințele privind caracteristicile de securitate aferente sistemului solicitate de *MAI*.

1. Arhitectura SIA e-Dosar MAI trebuie să fie concepută prin aplicarea unei abordări de tipul „Secure by design” (securitate prin design).
2. Arhitectura de securitate a SIA e-Dosar MAI trebuie să fie documentată la nivel tehnic.
3. Documentația va conține descris modelul de securitate implementat, componentele prezente și rolul fiecărei componente din punct de vedere al securității.
4. Accesul la funcțiile oferite utilizatorilor anonimi trebuie să fie controlat cu mijloace de protecție contra suprasolicitării serviciului de unul sau câteva noduri ale rețelei.
5. SIA e-Dosar MAI va fi securizat pentru OWASP Top 10 vulnerabilities (2017).
6. Acțiunile utilizatorilor trebuie să fie înregistrate în jurnale electronice.
7. SIA e-Dosar MAI va emite un semnal periodic care indică starea sa funcțională.
8. SIA e-Dosar MAI va înregistra centralizat toate excepțiile și erorile generate de componentele sale.
9. La producerea unei erori, SIA e-Dosar MAI va afișa utilizatorului un mesaj de eroare generic. Acesta poate conține un cod de eroare și un identificator unic al erorii, pentru a facilita implicarea serviciului de suport.
10. SIA e-Dosar MAI va deține instrumentele necesare pentru analiza și procesarea înregistrărilor aferente excepțiilor și erorilor.
11. SIA e-Dosar MAI va putea genera automat notificări către persoanele responsabile la producerea anumitor erori în funcționarea componentelor sale.
12. SIA e-Dosar MAI va avea implementate instrumente pentru executarea procedurilor de generare automată a copiilor de rezervă și gestiune a copiilor de rezervă istorice.
13. SIA e-Dosar MAI trebuie să dețină mecanisme de asigurare a integrității datelor în cazul căderilor la nivelul oricăror componente.
14. SIA e-Dosar MAI trebuie să dețină mecanisme de restabilire operativă a disponibilității și accesibilității în cazul unor incidente de continuitate.
15. Arhitectura SIA e-Dosar MAI trebuie să fie rezistentă la căderi de componente și să nu dețină puncte singulare de cădere (SPOF).
16. SIA e-Dosar MAI trebuie să dețină mecanisme de asigurare a integrității datelor în cazul unor căderi accidentale la nivelul oricăror componente ale sale.
17. SIA e-Dosar MAI trebuie să dețină mecanisme de restabilire operativă a disponibilității și accesibilității în cazul unor incidente de continuitate.

D. Programul de implementare SIA e-Dosar MAI

9. Fazele proiectului

Fazele proiectului vor corespunde reglementării tehnice **"Procesele ciclului de viaţă al software-ului" RT 38370656 - 002:2006 (***Publicat : 23.06.2006 în Monitorul Oficial Nr. 95-97 art Nr : 335*). Activitățile menționate în cadrul fiecărei faze reprezintă cerințe minime. Livrabilele indicate și criteriile de acceptanță ale livrabilelor sunt obligatorii. Conform cerințelor din secțiunea 8.1, Ofertantul va specifica în ofertă fazele de implementare și livrabilele produse. Pentru fiecare fază vor fi definite obiectivele, activitățile cheie, persoanele responsabile și instrumentele utilizate pentru realizarea activităților. Fiecare fază va fi planificată și coordonată cu *MAI*. Timeline a proiectului va include obligatoriu prezentările documentelor pentru aprobare către *MAI*. Termenii pentru examinarea și verificarea livrabililor de către *MAI* vor corespunde normelor stabilite de standardele interne ale Instituției.

9.1 Faza de analiză: activitățile cheie

Compartimentul dat conține cerințele privind activitățile cheie ale fazei de analiză în cadrul proceselor de dezvoltare și implementare a *SIA e-Dosar MAI.* Tabelul următor conține cerințele privind activitățile cheie ale fazei de analiză.

Cerințele privind activitățile cheie ale fazei de analiză

Nr.	Obligativitate	Cerință
1	*OBL*	*Ofertantul va valida necesitățile funcționale ale SIA e-Dosar MAI în cadrul etapei de analiză de business. În acest scop, Ofertantul va executa următoarele activități:* *revizuirea/analiza cerințelor de business;* *analiza proceselor de business relevante;* *analiza proceselor de raportare;* *revizuirea/analiza cerințelor pentru rapoarte;* *analiza infrastructurii curente software, hardware și de rețea.* *Lucrările se vor executa prin intervievări ale persoanelor responsabile din MAI și STI MAI, și analize a documentației relevante.*

Faza de analiză: livrabile

Compartimentul dat conține cerințele privind livrabilele fazei de analiză în cadrul proceselor de dezvoltare și implementare a *SIA e-Dosar MAI.* Tabelul de mai jos conține cerințele privind livrabilele fazei de analiză.

Cerințele privind livrabilele fazei de analiză

Nr.	Obligativitate	Cerință
1	*OBL*	*În rezultatul analizei de business, Furnizorul va prezenta în calitate de livrabil SRS care reprezintă un raport de analiză a situației „As-Is" și funcționalităților necesare, care poate conține precizări și propuneri în raport cu termenii de referință pentru implementarea SIA e-Dosar MAI.*
2	*OBL*	*Durata perfectării SRS nu va dura mai mult de 1 săptămână de la demararea proiectului.*
3	*DES*	*În baza SRS perfectat, MAI poate accepta ajustări la specificațiile funcționale și non-funcționale conform termenilor de referință.*

Faza de analiză: criterii de acceptanță a livrabilelor

Compartimentul dat conține cerințele privind criteriile de acceptanță a livrabilelor fazei de analiză în cadrul proceselor de dezvoltare și implementare a *SIA e-Dosar MAI.* Tabelul de mai jos conține cerințele privind criteriile de acceptanță a livrabilelor fazei de analiză.

Cerințele privind criteriile de acceptanță a livrabilelor fazei de analiză

Nr.	Obligativitate	Cerință
1	*OBL*	*Acceptanța livrabilelor fazei de analiză a proiectului va fi efectuată conform următoarelor criterii:* *Livrabilele sunt prezentate către MAI;*

Nr.	Obligativitate	Cerință
		MAI au prezentat aviz pozitiv și nu are observații privind deplinătatea și corectitudinea livrabilelor; *Actul de acceptanță a livrabilelor este semnat de ambele părți.*

9.2 Faza de proiectare tehnică: activități cheie

Compartimentul dat conține cerințele privind activitățile cheie ale fazei de proiectare a *SIA e-Dosar MAI.* Tabelul de mai jos conține cerințele privind activitățile cheie ale fazei de proiectare tehnică.

Cerințele privind activitățile cheie ale fazei de proiectare tehnică

Nr.	Obligativitate	Cerință
1	*OBL*	*La această etapă Ofertantul va elabora proiectul tehnic pentru SIA e-Dosar MAI (SDD), conform specificațiilor funcționale și non-funcționale. Ofertantul va executa cel puțin:* *definirea arhitecturii de sistem și nivelurile lui (particularitățile de implementare a nivelului de prezentare, nivelului de aplicații, nivelului de date și nivelului tehnologic);* *definirea particularităților tehnice pentru fiecare nivel de arhitectură a SIA e-Dosar MAI ;* *definirea în detaliu a modelului de date aferent SIA e-Dosar MAI ;* *maparea modelului de date la sursa de date existentă SIA TREZ.* *definirea particularităților de bază a interfeței de utilizator a SIA e-Dosar MAI ;* *definirea dezvoltărilor necesar a fi efectuate;*

Faza de proiectare tehnică: livrabile

Compartimentul dat conține cerințele privind livrabilele fazei de proiectare tehnică a *SIA e-Dosar MAI.* Tabelul de mai jos conține cerințele privind livrabilele fazei de proiectare tehnică.

Cerințele privind livrabilele fazei de proiectare tehnică

Nr.	Obligativitate	Cerință
1	*OBL*	*În rezultatul proiectării tehnice, Ofertantul va furniza în calitate de livrabil* ***Proiectul Tehnic (SDD)****. Proiectul tehnic este un document director al activităților de dezvoltare a SIA e-Dosar MAI care conține descrierea detaliată a următoarelor viziuni:* *Descrierea tehnologiei și metodelor de realizare a SIA e-Dosar MAI structurile de date și constrângerile acestora;* *descrierea modului de ineracțiune a elementelor sistemului* *interfața utilizator a SIA e-Dosar MAI care cuprinde conceptualizarea totalității componentelor interfeței utilizator;* *funcționalitățile SIA e-Dosar MAI care cuprinde descrierea detaliată a totalității scenariilor și algoritmilor de implementare a funcționalităților SIA e-Dosar MAI.*

Nr.	Obligativitate	Cerință
2	*OBL*	*Durata perfectării SDD nu va dura mai mult de 2 săptămâni de la demararea proiectului.*

Faza de proiectare tehnică: criterii de acceptanță a livrabilelor

Compartimentul dat conține cerințele privind criteriile de acceptanță a livrabilelor fazei de proiectare tehnică a *SIA e-Dosar MAI.* Tabelul de mai jos conține cerințele privind criteriile de acceptanță a livrabilelor fazei de proiectare tehnică.

Cerințele privind criteriile de acceptanță a livrabilelor fazei de proiectare tehnică

Nr.	Obligativitate	Cerință
1	*OBL*	*Acceptanța fazei de proiectare tehnică este condiționată de livrarea către MAI a Proiectului Tehnic (SDD) și responsabilii relevanți din partea MAI, STI MAI nu au observații privind deplinătatea și corectitudinea Proiectului Tehnic.*
2	*OBL*	*Acceptanța fazei de proiectare tehnică se încheie cu semnarea Actului de acceptanță de ambele părți.*

9.3 Faza de dezvoltare/configurare: activități cheie

Compartimentul dat conține cerințele privind activitățile cheie ale fazei de dezvoltare/configurare a *SIA e-Dosar MAI.* Tabelul următor conține cerințele privind activitățile cheie ale fazei de dezvoltare/configurare a *SIA e-Dosar MAI.*

Cerințele privind activitățile cheie ale fazei de dezvoltare

Nr.	Obligativitate	Cerință
1	*OBL*	*La această etapă Ofertantul va configura și ajusta (în cazul soluțiilor existente sau platformelor universale utilizate) sau va dezvolta și configura (în cazul dezvoltării de la zero) SIA e-Dosar MAI , conform specificațiilor Proiectului Tehnic.* *Ofertantul va executa cel puțin următoarele activități:* *instalarea mediilor de producție și de testare a SIA e-Dosar MAI (Sistem de Operare/SGBD/aplicații etc.);* *dezvoltarea, desfășurarea și configurarea SIA e-Dosar MAI conform SDD (proiectul tehnic).* *desfășurarea componentelor SIA e-Dosar MAI în mediile de operare pregătite.*
2	*OBL*	*Faza de dezvoltare/configurare a SIA e-Dosar MAI nu va depăși 2 luni calendaristice.*

Faza de dezvoltare/configurare: livrabile

Compartimentul dat conține cerințele privind livrabilele fazei de dezvoltare a *SIA e-Dosar MAI.* Tabelul următor conține cerințele privind livrabilele fazei de dezvoltare.

Cerințele privind livrabilele fazei de dezvoltare

Nr.	Obligativitate	Cerință
1	*OBL*	*Ofertantul va dezvolta și configura componentele SIA e-Dosar MAI conform specificațiilor funcționale și non-funcționale în:* *mediul de producție;* *mediul de testare;*
2	*OBL*	*Ofertantul va pregăti și livra documentație tehnică completă aferentă componentelor implementate.*
3	*OBL*	*Ofertantul va livra planul și scenariile de testare și va efectua testarea componentelor SIA e-Dosar MAI :* *unit testing;* *stress testing;* *load testing.*

Faza de dezvoltare/configurare: criterii de acceptanță a livrabilelor

Compartimentul dat conține cerințele privind criteriile de acceptanță a livrabilelor fazei de dezvoltare/configurare a *SIA e-Dosar MAI.* Tabelul următor conține cerințele privind criteriile de acceptanță a livrabilelor fazei de dezvoltare/configurare a *SIA e-Dosar MAI.*

Cerințele privind criteriile de acceptanță a livrabilelor fazei dezvoltare/configurare

Nr.	Obligativitate	Cerință
1	*OBL*	*Componente SIA e-Dosar MAI sunt implementate și configurate conform specificațiilor funcționale și non-funcționale în următoarele medii:* *mediul de producție;* *mediul de testare;*
2	*OBL*	*Documentația tehnică completă aferentă componentelor implementate ale SIA e-Dosar MAI este livrată.*
3	*OBL*	*Beneficiarul nu are observații sau obiecții privind calitatea livrabilelor.*
4	*OBL*	*Actul de acceptanță a livrabilelor fazei de dezvoltare/configurare este semnat de către Ofertant și MAI.*

9.4 Faza de testare de acceptanță: activități cheie

Compartimentul dat conține cerințele privind activitățile cheie în testarea de acceptanță a *SIA e-Dosar MAI.* Tabelul următor conține cerințele privind activitățile cheie ale fazei de testare de acceptanță.

Cerințele privind activitățile cheie ale fazei de testare de acceptanță

Nr.	Obligativitate	Cerință
1	*OBL*	*La această etapă toate componentele SIA e-Dosar MAI sunt implementate și configurate conform specificațiilor funcționale și non-funcționale.* *SIA e-Dosar MAI este disponibil și operațional în toate mediile în care a fost implementat.* *Ofertantul va organiza testarea de acceptanță a sistemului. În acest scop, acesta va executa cel puțin următoarele activități:*

Nr.	Obligativitate	Cerință
		definirea strategiei de testare și a procedurii de testare; *pregătirea planurilor detaliate de testare, inclusiv scenarii de testare;* *recepționarea erorilor depistate și înlăturarea acestora;* *pregătirea planului cu rezultatele finale ale testării, inclusiv statutul tuturor erorilor identificate.*
2	*OBL*	*Acoperirea cu unit teste pentru capabilitățile SIA e-Dosar MAI va fi minim 90%.*

Faza de testare de acceptanță: livrabile

Compartimentul dat conține cerințele privind livrabilele fazei de testare de acceptanță a *SIA e-Dosar MAI.* Tabelul de mai jos conține cerințele privind livrabilele fazei de testare de acceptanță.

Cerințele privind livrabilele fazei de migrare a datelor

Nr.	Obligativitate	Cerință
1	*OBL*	*Ofertantul va livra spre coordonare și acceptare către MAI planul de testare de acceptanță;*
2	*OBL*	*Ofertantul va livra spre coordonare și acceptare către MAI scenariile de testare pentru toate categoriile de teste (unit testing, stress testing, load testing.etc.).*
3	*OBL*	*Ofertantul va livra spre coordonare și acceptare către MAI raportul cu privire la rezultatele testării SIA e-Dosar MAI.*

Faza de testare de acceptanță: criterii de acceptanță a livrabilelor

Compartimentul dat conține cerințele privind criteriile de acceptanță a livrabilelor fazei de testare de acceptanță a *SIA e-Dosar MAI.* Tabelul următor conține cerințele privind criteriile de acceptanță a livrabilelor fazei de testare de acceptanță a *SIA e-Dosar MAI.*

Cerințele privind criteriile de acceptanță a *SIA e-Dosar MAI*

Nr.	Obligativitate	Cerință
1	*OBL*	*Ofertantul va efectua toate testele planificate conform Planului de testare și rezultatele finale ale acestora sunt acceptabile.*
2	*OBL*	*Acceptarea livrabilelor se va face dacă se vor descoperi zero nonconformități critice și mai puțin de 3 nonconformități majore.*
3	*OBL*	*Acceptarea va fi datată cu ziua când vor fi reSTI MAIicate toate nonconformitățile descoperite la livrare.*
4	*OBL*	*Actul de acceptanță a SIA e-Dosar MAI este semnat de către Ofertant, MAI.*

9.5 Faza de instruire și documentare: activități cheie

Compartimentul dat conține cerințele privind activitățile cheie în instruirea administratorilor și documentarea *SIA e-Dosar MAI.* Tabelul de jos conține cerințele privind activitățile cheie ale fazei de instruire și documentare.

Cerințele privind activitățile cheie ale fazei de instruire și documentare

Nr.	Obligativitate	Cerință
1	*OBL*	*Ofertantul va elabora și livra programa de instruire pentru Administratorii de Sistem.*
2	*OBL*	*Ofertantul va stabili de comun acord cu MAI* ***Planul de organizare a sesiunii de instruire****.*
3	*OBL*	*Ofertantul va efectua instruirea Administratorilor conform planului. Instruirea va fi efectuată în limba Română.*

Faza de instruire și documentare: livrabile

Compartimentul dat conține cerințele privind livrabilele fazei de instruire și documentare a *SIA e-Dosar MAI.* Tabelul următor conține cerințele privind livrabilele fazei de instruire și documentare.

Cerințele privind livrabilele fazei de instruire și documentare

Nr.	Obligativitate	Cerință
1	*OBL*	*Faza de instruire și documentare presupune asigurarea următoarelor categorii de livrabile:* *instruire în administrarea și configurarea SIA e-Dosar MAI (utilizatorii cu rol Administrator de Sistem);* *ghid complet destinat exploatării și administrării SIA e-Dosar MAI.*
2	*OBL*	*Ofertantul va pregăti și livra cel puțin următoarele documente însoțitoare ale SIA e-Dosar MAI :* *document de arhitectură tehnică a SIA e-Dosar MAI ;* *ghidul de administrare a SIA e-Dosar MAI ;* *ghidul de instalare a SIA e-Dosar MAI ;* *ghidul de configurare și menținere operațională a tuturor componentelor SIA e-Dosar MAI ;* *ghiduri pentru dezvoltatori, în limita componentelor admise pentru dezvoltare interna pe partea MAI;*
3	*OBL*	*Ghidurile trebuie să fie complete, detaliate și actualizate.*
4	*OBL*	*Ofertantul va livra codul sursă și bibliotecile aferente dezvoltărilor efectuate pentru SIA e-Dosar MAI. Codul sursă va conține suficiente comentarii pentru a putea fi înțeles de angajații MAI și STI MAI.*

Faza de instruire și documentare: criterii de acceptanță

Compartimentul dat conține cerințele privind criteriile de acceptanță a livrabilelor fazei de instruire și documentare a *SIA e-Dosar MAI.* Tabelul de mai jos conține cerințele privind criteriile de acceptanță a livrabilelor fazei de instruire și documentare a *SIA e-Dosar MAI.*

Cerințele privind criteriile de acceptanță a livrabilelor fazei de instruire și documentare

Nr.	Obligativitate	Cerință
1	*OBL*	*Ofertantul trebuie să efectueze sesiunile de instruire a administratorilor conform Planului agreat în comun acord cu MAI.*
2	*OBL*	*Documentația SIA e-Dosar MAI trebuie să fie completă și livrată în forma solicitată de MAI.*

Nr.	Obligativitate	Cerință
3	*OBL*	*Codul sursă pentru dezvoltările efectuate la SIA e-Dosar MAI va fi livrat.*
4	*OBL*	*Bibliotecile necesare compilării codului sursă sau funcționării SIA e-Dosar MAI va fi livrat.*
5	*OBL*	*Actul de acceptanță a instruirilor și documentației trebuie să fie semnat de către Furnizor, MAI.*

9.6 Faza de lansare în producție: activități cheie

Compartimentul dat conține cerințele privind activitățile cheie pentru lansarea în producție a *SIA e-Dosar MAI.* Tabelul următor conține cerințele privind activitățile cheie pentru lansarea în producție a *SIA e-Dosar MAI.*

Cerințele privind activitățile cheie ale fazei de instruire și documentare

Nr.	Obligativitate	Cerință
1	*OBL*	*Ofertantul va participa la toate etapele de punere în producție a SIA e-Dosar MAI. În acest scop, Ofertantul va executa cel puțin următoarele acțiuni:* *va elabora Planul de lansare în producție (planul de cut-over);* *va elabora planul de roll-back (unde este aplicabil);* *va actualiza seturile de date ce au fost generate/modificate în sistemele actuale după executarea procedurii de populare cu date inițiale;* *va oferi suport la executarea Planului de lansare în producție;* *va înlătura operativ erorile și defecțiunile apărute în funcționarea SIA e-Dosar MAI.*

Faza de lansare în producție: livrabile

Compartimentul dat conține cerințele privind livrabilele fazei de lansare în producție a *SIA e-Dosar MAI.* Tabelul următor conține cerințele privind lansarea în producție a *SIA e-Dosar MAI.*

Cerințele privind livrabilele fazei de lansare în producție a *SIA e-Dosar MAI*

Nr.	Obligativitate	Cerință
1	*OBL*	*Ofertantul va perfecta și coordona cu MAI Planul de lansare în producție a SIA e-Dosar MAI.*
2	*OBL*	*SIA e-Dosar MAI este lansat în producție.*

Faza de lansare în producție: criterii de acceptanță

Compartimentul dat conține cerințele privind criteriile de acceptanță a livrabilelor fazei de lansare în producție a *SIA e-Dosar MAI.* Tabelul demai jos conține cerințele privind criteriile de acceptanță a livrabilelor fazei de lansare în producție a *SIA e-Dosar MAI.*

Cerințele privind criteriile de acceptanță a livrabilelor fazei de testare în producție a *SIA e-Dosar MAI*

Nr.	Obligativitate	Cerință
1	*OBL*	*SIA e-Dosar MAI este disponibil și funcțional.*

Nr.	Obligativitate	Cerință
2	*OBL*	*Actul de acceptanță în producție a SIA e-Dosar MAI este semnat de Ofertant, MAI.*

Faza de testare în producție a *SIA e-Dosar MAI*

Compartimentul dat conține cerințele privind perioada de testare în producție a *SIA e-Dosar MAI.* Tabelul de mai jos conține cerințele privind perioada de testare în producție a *SIA e-Dosar MAI.*

Cerințele privind perioada de testare în producție a *SIA e-Dosar MAI*

Nr.	Obligativitate	Cerință
1	*OBL*	*Ofertantul va oferi suportul on-site pentru o perioadă de 3 luni după lansarea în producție, pentru fixarea erorilor și deficiențelor în funcționarea SIA e-Dosar MAI. Pe parcursul acestei perioade SIA e-Dosar MAI se consideră testat în producție.*
2	*OBL*	*Pe parcursul perioadei de testare în producție a SIA e-Dosar MAI , Ofertantul va efectua activități de dezvoltare pentru înlăturarea erorilor și deficiențelor, va analiza înregistrările de jurnalizare în vederea prevenirii unor eventuale probleme, va efectua ajustări la interfața utilizator și modulele critice ale SIA e-Dosar MAI.*

Faza de acceptanță finală a *SIA e-Dosar MAI*

Compartimentul dat conține cerințele privind acceptanța finală a *SIA e-Dosar MAI.* Tabelul de mai jos conține cerințele privind acceptanța finală a *SIA e-Dosar MAI.*

Cerințele privind acceptanța finală a *SIA e-Dosar MAI*

Nr.	Obligativitate	Cerință
1	*OBL*	*Acceptanța finală a implementării SIA e-Dosar MAI se va consemna în baza **Actului de acceptanță finală** semnat de către Ofertant, MAI, cu condiția îndeplinirii următoarelor condiții:* *perioada de testare în producție a expirat;* *toate erorile, deficiențele și problemele de gravitate 1 sunt înlăturate;* *sunt mai puțin de 10 erori și probleme de gravitate 2 neînlăturate;* *nici un scenariu de testare nu va corupe integritatea datelor.*
2	*OBL*	*O eroare sau problemă aferentă SIA e-Dosar MAI este considerată de gravitate 1 dacă aceasta blochează sau face dificilă utilizarea funcționalităților cheie ale portalului.* *O eroare sau problemă aferentă SIA e-Dosar MAI este considerată de gravitate 2 dacă aceasta blochează sau face dificilă utilizarea funcționalităților pentru care însă există opțiuni alternative (workarounds).*

10. Cerințe pentru garanție, mentenanță și suport post-implementare

Scopul serviciilor de suport și mentenanță post-implementare a SIA e-Dosar MAI este de a asigura pentru Ministerul de Interne următoarele obiective:

■ Funcționalitatea oferită de SIA e-Dosar MAI va fi aliniată în timp la necesitățile MAI

■ Incidentele și problemele apărute în procesul de exploatare a SIA e-Dosar MAI vor fi adresate și soluționate în timp util;

■ Dificultățile în exploatarea SIA e-Dosar MAI vor putea fi depășite corect și în timp util, fără a afecta funcționarea portalului.

Pentru atingerea acestor obiective, serviciile de suport și mentenanță post-implementare urmează să fie prestate de Ofertant conform cerințelor stabilite în acest caiet de sarcini.

Ofertantul trebuie să descrie activitățile ce vor fi desfășurate de acesta pentru a răspunde acestor cerințe, prezentând informație suficient de detaliată despre modul în care intenționează să presteze serviciile solicitate la nivelul cerut, precum și informație privind capacitățile sale tehnice, organizatorice și de competență, ce confirmă capacitatea să de a presta la nivelul cerut.

MAI așteaptă ca oferta pentru serviciile de suport și mentenanță post-implementare să fie bazată pe cele mai bune practici în domeniul managementului proiectelor și managementul serviciilor TI (exemplu: ISO 20000, ITIL etc.).

Cerințele generale de garanție, mentenanță și suport post-implementare

Compartimentul dat conține cerințele generale ale proceselor de garanție, mentenanță și suport post-implementare a *SIA e-Dosar MAI.* Tabelul următor conține toate cerințele generale de garanție, mentenanță și suport post-implementare a *SIA e-Dosar MAI.*

Cerințele generale de garanție, mentenanță și suport

Nr.	Obligativitate	Cerință
1	*OBL*	*Parte a contractului pentru livrarea și implementarea SIA e-Dosar MAI , Ofertantul va presta servicii de garanție, mentenanță și suport pentru portalul dezvoltat pentru un termen de 12 luni din data acceptanței finale a SIA e-Dosar MAI.*
2	*OBL*	*Prețul contractului inițial de dezvoltare și implementare a SIA e-Dosar MAI va include toate serviciile de garanție, suport și mentenanță post-implementare, cu excepția serviciilor de dezvoltare suplimentară în afara obiectivelor SRS și SDD.*
3	*OBL*	*Toate erorile de funcționare a SIA e-Dosar MAI depistate pe parcursul perioadei de garanție vor fi remediate din contul Ofertantului.*
4	*OBL*	*După un an de prestare a serviciilor de garanție, mentenanță și suport post-implementare, MAI poate solicita prelungirea prestării serviciilor.* *Ofertantul este obligat să accepte prestarea ulterioară a serviciilor, pentru cel puțin 1 an, în condițiile ce rezultă din acești Termeni de referință și estimările ofertei (exemplu: nivel servicii, preț servicii etc.).*

10.1 Serviciile de suport pentru SIA e-Dosar MAI în perioada de garanție

Serviciile de suport sunt prestate de *Ofertant* în vederea depășirii incidentelor produse ca urmare a exploatării *SIA e-Dosar MAI* , în vederea soluționării problemelor depistate pe parcursul exploatării *SIA e-Dosar MAI* și în scopul utilizării corecte și eficiente a *SIA e-Dosar MAI.*

Un incident aferent *SIA e-Dosar MAI* este orice eveniment ce a afectat sau ar fi putut afecta funcționarea normală a portalului. O problemă aferenta *SIA e-Dosar MAI* este o cauza ce a dus sau poate duce la producerea unui incident.

O solicitare de consultanță este o adresare din partea *MAI sau STI MAI* către *Ofertant* în vederea obținerii suportului consultativ la utilizarea, configurarea și menținerea în funcțiune a *SIA e-Dosar MAI.*

Serviciile de suport sunt destinate să asigure utilizarea în timp a *SIA e-Dosar MAI* la parametri de calitate necesari. Parametrii de calitate pentru funcționarea *SIA e-Dosar MAI* sunt:

- **Disponibilitatea** – capacitatea portalului și a componentelor sale de a primi interogări din partea utilizatorilor și de a răspunde în timp util la aceste interogări;
- **Utilizabilitatea** – capacitatea portalului de a funcționa corect, livrând către utilizatori serviciile scontate;
- **Performanța** – capacitatea portalului de a răspunde la interogările legitime la parametri stabiliți;
- **Securitatea** – capacitatea portalului de a asigura integritatea și disponibilitatea datelor stocate și gestionate.

Acest compartiment stabilește cerințele pentru serviciile de suport cu utilizarea terminologiei de mai sus. Tabelul următor conține cerințele serviciilor de suport pe care trebuie să le presteze *Ofertantului* pe parcursul perioadei de garanție, mentenanță și suport.

Cerințele privind serviciile de suport pentru *SIA e-Dosar MAI*

Nr.	Obligativitate	Cerință
1	*OBL*	*Ofertantul va oferi suport MAI la soluționarea incidentelor aferente SIA e-Dosar MAI , indiferent de cauzele care au dus la apariția incidentului (exemplu: erori în aplicație, probleme la nivel de soft de sistem, probleme în aplicații externe).* *În acest scop, în funcție de specificului fiecărui caz de incident în parte, Ofertantul poate întreprinde următoarele acțiuni:* *recepționarea de la MAI a informației despre incidentul produs și contextul producerii acestuia;* *localizarea incidentului și identificarea activităților imediate ce trebuie să fie întreprinse în vederea diminuării impactului incidentului;* *identificarea cauzelor incidentului și stabilirea acțiunilor necesar a fi întreprinse în vederea înlăturării incidentului;* *ghidarea MAI în vederea întreprinderii acțiunilor pentru diminuarea impactului incidentului și soluționarea acestuia în limita de timp stabilită;* *prezentarea informației detaliate către MAI privind cauzele incidentului, raționamentul acțiunilor întreprinse și acțiunile planificate pentru a preveni repetarea incidentelor similare;* *examinarea necesității de înregistrare a unei noi probleme aferente SIA e-Dosar MAI (în cazul înregistrării problemei, Ofertantul o va gestiona conform cerințelor aferente serviciilor de suport pentru soluționarea problemelor).*

Nr.	Obligativitate	Cerință
2	*OBL*	*Ofertantul va presta servicii de suport pentru soluționarea problemelor înregistrate la nivelul aplicației. În acest scop, în funcție de specificul fiecărui caz în parte, Ofertantul poate întreprinde următoarele acțiuni:* *recepționarea și colectarea informației aferente problemei, simptome, efecte, condiții specifice;* *analiza și localizarea problemei la nivelul componentelor SIA e-Dosar MAI , identificarea interdependențelor ce contribuie la manifestarea problemei sau sunt afectate de problemă;* *identificarea soluțiilor temporare pentru a diminua efectele problemei și ghidarea MAI în vederea aplicării acestora;* *identificarea soluțiilor aferente problemei, comunicarea regulata cu MAI privind progresele făcute în vederea identificării soluțiilor;* *în cazul în care soluțiile țin de configurări la nivelul aplicației, va fi efectuată ghidarea MAI în vederea implementării acestora;* *în cazul în care soluțiile presupun modificări la nivelul codului program al SIA e-Dosar MAI , acestea vor operate de Ofertant și implementate în cadrul serviciilor de Mentenanță în limita de timp stabilită.*
3	*OBL*	*Ofertantul va presta servicii de suport consultativ la utilizarea SIA e-Dosar MAI de către MAI. În acest scop, în funcție de specificul necesităților de consultanță ale MAI, Furnizorul poate întreprinde următoarele acțiuni:* *recepționarea solicitării de consultanță din partea MAI și a informației aferente contextului în care este necesara consultanța;* *identificarea soluțiilor și validarea acestora în mediul de testare;* *oferirea răspunsurilor complete și corecte privind modul în care trebuie să acționeze MAI la exploatarea SIA e-Dosar MAI , conform solicitării de consultanță.*

10.2Serviciile de mentenanță pentru SIA e-Dosar MAI în perioada de garanție

Serviciile de mentenanță trebuie să fie prestate de *Ofertant* în scopul menținerii în timp a portalului la parametri de funcționare optimi. În acest scop, *Ofertantul* poate veni cu actualizări și modificări la nivelul aplicațiilor și noilor versiuni ale aplicației și componetelor aferente.

Actualizări ale *SIA e-Dosar MAI* sunt modificări la nivelul aplicațiilor, transmise către *MAI* la inițiativa *Ofertantului* și destinate să îmbunătățească performanța aplicațiilor, să înlăture probleme, erori și vulnerabilități cunoscute *Ofertantului*.

Versiuni noi (*new releases*) sunt pachete de software aferente *SIA e-Dosar MAI* , transmise către *MAI* la inițiativa *Ofertantului* și care conțin toate modificările efectuate anterior la nivelul aplicației și componetelor aferente. Suplimentar, pot conține modificări și actualizări, componente noi de aplicație, ce nu au fost prezente în versiunile vechi ale portalului.

Cerințele privind serviciile de mentenanță pentru *SIA e-Dosar MAI*

ID	Obligativitate	Cerință
PIR 008	*M*	*Ofertantul va presta, în caz de necesitate, servicii de actualizare a SIA e-Dosar MAI și de livrare a versiunilor noi.*

ID	Obligativitate	Cerință
PIR 009	*M*	*În acest scop Ofertantul va pregăti pachetele software și documentația aferentă actualizărilor și noilor versiuni.*

10.3Nivelul serviciilor aferente SIA e-Dosar MAI (service level)

Nivelul serviciilor de suport și mentenanța post-implementare stabilește cerințele privind parametrii la care trebuie să fie prestate aceste servicii de către *Ofertant*.

Serviciile de suport

Parametrii ce caracterizează nivelul serviciilor de suport sunt următorii:

- **Timpul de Răspuns (TR)** - este timpul în care *Ofertantul* va reacționa la o solicitare de suport, va diagnostica situația și va stabili acțiunile necesar a fi întreprinse pentru soluționare;
- **Timpul de Soluționare (TS)** – este timpul obiectiv în care se așteaptă că *Ofertantul* va întreprinde acțiunile în zona sa de responsabilitate pentru a soluționa complet solicitarea *MAI*.

Solicitările *MAI* pentru servicii de suport și mentenanță post-implementare sunt clasificate din punct de vedere al importanței acestora pentru *MAI*. Importanța pentru *MAI* este apreciată în funcție de impactul (produs sau probabil) al evenimentului ce a generat necesitatea plasării solicitării asupra parametrilor de calitate pentru funcționarea *SIA e-Dosar MAI*.

Clasificarea importanței solicitărilor de suport a *MAI*

Clasificare	Impactul asupra parametrilor de calitate pentru funcționarea aplicațiilor
Critică	*Disponibilitatea: portalul este indisponibil pentru toți sau majoritatea utilizatorilor.* *Utilizabilitatea: funcții cheie de business nu pot fi utilizate. Nu există proceduri și funcționalități alternative.* *Performanța: timpul de răspuns la interogările utilizatorilor fac practic indisponibilă exploatarea portalului.* *Securitatea: există riscuri majore de compromitere a integrității sau disponibilității datelor.*
Înaltă	*Disponibilitatea: portalul este indisponibil pentru o bună parte din utilizatori.* *Utilizabilitatea: funcții cheie pot fi utilizate limitat.* *Performanța: timpul de răspuns la interogările utilizatorilor afectează în măsura semnificativă desfășurarea proceselor cheie.* *Securitatea: există riscuri înalte de compromitere a integrității sau disponibilității datelor.*
Ordinară	*Disponibilitatea: portalul este indisponibil pentru o parte din utilizatori.* *Utilizabilitatea: funcționalitatea portalului poate fi utilizată limitat.* *Performanța: timpul de răspuns la interogările utilizatorilor afectează în măsură moderată desfășurarea proceselor cheie.* *Securitatea: există riscuri de compromitere a integrității sau disponibilității datelor.*
Joasă	*Disponibilitatea: portalul este indisponibil pentru un număr limitat de utilizatori.* *Utilizabilitatea: funcționalitatea portalului este afectată nesemnificativ.*

Clasificare	Impactul asupra parametrilor de calitate pentru funcționarea aplicațiilor
	Performanța: timpul de răspuns la interogările utilizatorilor este mai mare decât cel obișnuit. Nu este afectată desfășurarea proceselor cheie. *Securitatea: există riscuri minore de compromitere a integrității sau disponibilității datelor.*

La plasarea unei solicitări pentru servicii de suport și mentenanță post-implementare, *MAI* stabilește clasificarea pentru solicitare. *MAI* va atașa informația succintă pentru a explica clasificarea efectuată. *MAI* va putea reclasifica solicitările plasate, în funcție de modificările în contextul aferent solicitărilor.

- *Ofertantul* va presta servicii de suport în zilele lucrătoare conform legislației din Republicii Moldova, în intervalul de timp 08:00 – 18:00.
- Nivelul serviciilor de suport prestate de *Ofertant* trebuie să corespundă cerințelor specificate în tabelul de mai jos

Durata soluționării solicitărilor de suport a *MAI*

Nr.	Obligativitate	Clasificarea solicitării plasate de MAI	Timpul de Răspuns (TR)	Timpul de Soluționare (TS)
1	*OBL*	*Critică*	*5 min*	*60 min*
2	*OBL*	*Înaltă*	*60 min*	*Finele zilei*
3	*OBL*	*Ordinară*	*24h*	*3 zile*
4	*OBL*	*Joasă*	*3 zile*	*Cel mai bun efort**

* *Ofertantul* va depune tot efortul în vederea soluționării cat mai rapide a solicitării pentru servicii, activând în regim normal. Timpul limita pentru soluționarea solicitării va fi comunicat și acceptat de *MAI*. Modificări ulterioare a timpului limita sunt permise doar cu acceptul *MAI*.

Serviciile de mentenanță

Parametrii ce caracterizează nivelul serviciilor de mentenanță oferite de *Ofertant* în perioada de garanție a *SIA e-Dosar MAI* sunt descriși în tabelul de mai jos

Cerințe pentru serviciile de mentenanță a *SIA e-Dosar MAI* în perioada post-implementare

ID	Obligativitate	Cerință
PIR 014	*M*	*Ofertantul va comunica MAI graficul său de emitere a actualizărilor și noilor versiuni. Pentru actualizări, Ofertantul urmează să notifice MAI cu cel puțin o săptămână în prealabil. Pentru noile versiuni, Ofertantul urmează să notifice MAI cu cel puțin 1 lună în prealabil.*
PIR 015	*M*	*Pentru menținerea SIA e-Dosar MAI în stare funcțională, Ofertantul poate efectua lucrări de mentenanță la nivelul componentelor TI aferente portalului. Tipul lucrărilor de mentenanță și angajamentele Ofertantului privind coordonarea acestora cu MAI, perioada și durata acestora sunt stabilite în tabelul următor:*

ID	Obligativitate	Cerință
		<table><tr><th>Tipul lucrărilor de mentenanță</th><th>Notificare Beneficiar</th><th>Perioadă și durată lucrări</th></tr><tr><td>Lucrări de mentenanță ordinare</td><td>Cu 5 zile în prealabil.</td><td>Sunt efectuate în afara perioadei de disponibilitate garantată pentru SIA e-Dosar MAI. Durata acestor lucrări nu va depăși 4 ore.</td></tr><tr><td>Lucrări de mentenanță majore</td><td>Cu 10 zile în prealabil.</td><td>Sunt efectuate în afara perioadei de disponibilitate garantată pentru SIA e-Dosar MAI. Durata acestor lucrări nu va depăși 24 ore.</td></tr><tr><td>Lucrări de mentenanță urgente</td><td>Cu notificarea imediat ce a apărut necesitatea inițierii lor.</td><td>Pot fi efectuate în orice perioadă. Durata acestora nu va depăși 2 ore.</td></tr></table>

10.4Terminarea contractului

În cazul în care părțile decid să nu prelungească contractul pentru servicii de suport și mentenanță post-implementare, activitatea *MAI* nu trebuie să fie afectată. *MAI* trebuie să dețină posibilitatea de a contracta un alt *Furnizor* sau să preia intern suportul și menținerea *SIA e-Dosar MAI.*

Tabelul următor conține cerințele aferente condițiilor de terminare a relațiilor contractuale între *Ofertant, MAI* privind serviciile de mentenanță și suport în perioada post-implementare a *SIA e-Dosar MAI.*

Cerințe de încetare a contractului de prestare a serviciilor de mentenanță și suport în perioada post-implementare pentru *SIA e-Dosar MAI*

Nr.	Obligativitate	Cerință
1	*OBL*	*În cazul în care se preconizează pierderea efectului contractului pentru servicii de suport și mentenanță post-implementare, Ofertantul trebuie să asigure cel puțin:* *toate codurile sursă (sau fișierele de configurare în cazul soluțiilor COTS) aferente SIA e-Dosar MAI sunt transmise către MAI.* *Codurile sursă/configurațiile transmise trebuie să fie acelea în baza cărora au fost produse componentele SIA e-Dosar MAI ce sunt rulate la momentul încetării contractului în mediul de producție al MAI (autenticitatea și integritatea fișierelor menționate va fi confirmata prin semnătura Ofertantului);* *toata documentația aferentă SIA e-Dosar MAI este actualizată și transmisă către MAI;* *toate înregistrările aferente solicitărilor MAI efectuate pe partea Furnizorului (pentru incidente, probleme, consultanta, modificări, etc.)*

Nr.	Obligativitate	Cerință
		sunt exportate în format agreat în comun (exemplu: CSV, XLS etc.) și transmise către MAI; *Ofertantul va păstra pentru un termen de un an calendaristic toate înregistrările produse pe parcursul prestării serviciilor, codurile sursă și documentația aferentă SIA e-Dosar MAI.*

SPECIFICAȚII PRIVIND CERINȚELE FAȚĂ DE COMPONENTA MODELULUI PROCESELOR DE GESTIUNE A CAUZELOR PENALE

CUPRINS

INTRODUCERE

Scopul documentului

Acest document este/a fost realizat în conformitate cu Contractul nr. 26/15 din 25.02.2015 cu privire la definirea proceselor de business din cadrul MAI in vederea implementării unui flux automatizat de lucru la nivelul întregii organizații - WFMS (*Work Flow Management System*).

Prezentul document definește procesele de lucru operaționale aferente gestiunii Cazurilor Penale și cuprinde următoarele aspecte, definite în calitate de livrabile în cadrul proiectului:

a) ***Stabilirea modelului operațional,*** care include documentarea activităților enumerate conform cerințelor BPMN v.2, realizata pentru procesele de business conform situației la zi' (diagrama "Asls") si reingineria proceselor de business prin definirea viziunii viitoare (diagrama "ToBe").

Documentarea business proceselor se va face la un nivel detaliat, pentru ca informațiile rezultate din analiza sa poată sa fie transpuse într-un sistem de tip WFMS.

Reingineria business proceselor se va realiza doar în aspectele pentru care nu este definit *"status quo"* de către MAI, pentru anumite componente ale proceselor (spre exemplu: modificarea organigramei, modul de acces la anumite tipuri de informație, etc).

Pentru procesele din cadrul diagramei "ToBe" se vor prezenta referințe ale actelor normative (inclusiv cele interne existente sau care trebuie elaborate) care stă la baza fiecărei componente a procesului de business.

Diagrama "ToBe" va prezenta interfețele cu procesele de business externe si va indica entitatea / partenerul cu care MAI interacționează, incluzând totodată și o descriere generică a fluxului informațional care să permită definirea interfeței în WFMS.

b) ***Proiectarea Bazei Informaționale*** prin metoda mixtă (Input și Output) care include următoarele:

i. Identificarea listei informațiilor de intrare și caracteristicile acesteia, astfel:
   - identificarea listei informației structurate (documente) relevante proceselor;
   - identificarea informației nestructurate care poate fi și este necesar de formalizat (definit drept document);
   - identificarea surselor digitale relevante activității care pot fi real utilizate,

ii. Formalizarea surselor de date de intrare/ ieșire utilizate, astfel:
   - Definirea șabloanelor documentelor de intrare / ieșire;
   - Definirea regulilor de validare a datelor de intrare la nivel de document / compartiment proprietar al documentului / indicator /etc.

iii. Identificarea și definirea listei și descrierea nomenclatoarelor utilizate în procesul de lucru.

c) ***Definirea modelului de securitate,*** care va include:
   - Definirea modelului de roluri;
   - Definirea modelului de granulare a informației stocate - cel mai înalt nivel de detaliere a datelor stocate reieșind din necesitatea de indexare și limitare a accesului;
   - Definirea modelului de validare a documentelor, deciziilor, etc;

- Definirea modelului de criptare a datelor;
- Mecanismul de utilizare a semnăturii digitale.

d) ***Analiza RACI*** (Responsible, Accountable, Consulted, and Informed)

e) ***Diagrama stărilor si matricea CRUD*** realizata pentru fiecare stare (operațiunile ce vor fi efectuate de diferite roluri cu obiectele informaționale: cine va crea / modifica / valida / autoriza /anula un document).

f) ***Definirea recomandărilor aferente cerințelor nefuncționale*** pentru soluția WFMS

g) Noțiuni și Abrevieri

CPP - Codul de Procedura Penala

CP-Codul Penal

MAI - Ministerul Afacerilor Interne al Republici Moldova

STI -Serviciul Tehnologii Informaționale din cadrul MAI

WFMS - *Workflow Management System:* Sistem informatic pentru gestiunea fluxurilor de lucru

BPM - Business Process Management: Gestiunea proceselor de business

Cauză penală - proces penal desfășurat de organul de urmărire penală și de instanța judecătorească într-un caz concret referitor la una sau mai multe infracțiuni săvârșite sau presupus săvârșite

OUP - Ofițerul de urmărire penală

OrUP - Organul de urmărire penală

Cadrul legal

Cadrul legislativ-normativ care reglementează procesul de gestiune a cauzelor penale este stabilit de:

- Codul de Procedură Penală al Republicii Moldova (CPP)
- Ordinul interdepartamental nr.121/254/286-0/95 din 18.07.2008 „Privind evidența unică a infracțiunilor, a cauzelor penale și a persoanelor care au săvârșit infracțiuni"
- Ordinul IGP nr, 138 din 11.11.2013 „Privind aprobarea instrucțiunilor referitoare la organizarea activității de urmărire penală în cadrul Inspectoratului General al Poliției al MAI"
- Ordinul DPF nr. 22 din 25.01.2013 „Privind aprobarea Instrucțiunilor referitoare la organizarea activității de urmărire penală în cadrul Departamentului Poliției de Frontieră al MAI (cu modificări ulterioare prin ord. DPF nr.251 din 20.06.2013)

Acte legislativ-normative relevante proceselor de gestiune a Cauzelor Penale:

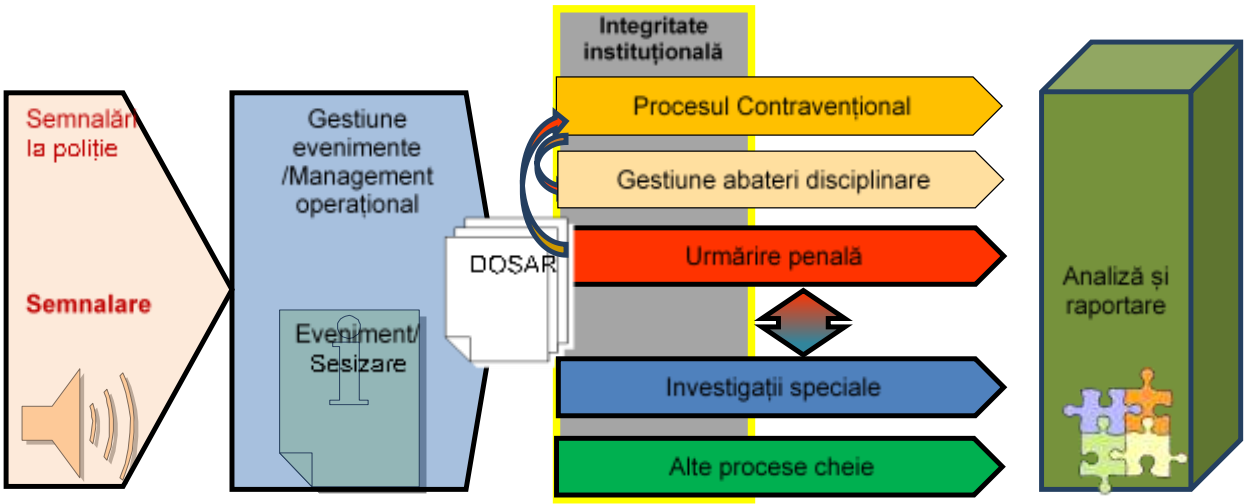
- Codul penal nr.985-XV din 18.04.2002
- Legea nr.320 din 27.12.2012 cu privire la activitatea Poliției și statutul polițistului
- Legea nr.333-XVI din 10.11.2006 cu privire la statutul ofițerului de urmărire penală
- Legea nr.283 din 28.12.2011 cu privire la Poliția de Frontieră
- Legea nr.105-XVI din 16.05.2008 cu privire la protecția martorilor și altor participanți la procesul penal
- Legea nr. 50 din 22.03.2012 privind prevenirea și combaterea criminalității organizate
- Legea nr.216-XV din 29.05.2003 cu privire la Sistemul informațional integral automatizat de evidență a infracțiunilor, a cauzelor penale și a persoanelor care au săvârșit infracțiuni
- Legea Nr. 91 din 27.06.2014 privind semnătura electronică și documentul electronic
- Hotărârea Guvernului nr. 1109 din 06.12.2010 „Pentru aprobarea Concepției de reformare a

Ministerului Afacerilor Interne și a structurilor subordonate și desconcentrate ale acestora

- Hotărârea Guvernului nr. 778 din 27.11.2009 „Cu privire la aprobarea Regulamentului privind organizarea și funcționarea Ministerului Afacerilor Interne, structurii și efectivului-limită ale aparatului central al acestuia";
- Hotărârea Guvernului nr. 693 din 30.08.2017 „cu privire la organizarea şi funcţionarea Ministerului Afacerilor Interne";
- Hotărârea Guvernului nr. 283 din 24.04.2013 pentru aprobarea Regulamentului privind organizarea și funcționarea Inspectoratului General al Poliției al Ministerului Afacerilor Interne
- Hotărârea Guvernului nr.434 din 19.06.2012 cu privire la Poliția de Frontieră
- HG Nr. 716 din 28.08.2014 pentru aprobarea Regulamentului cu privire la Registrul persoanelor reținute, arestate și condamnate
- Legea nr.3 din 25.02.2016 „Cu privire la procuratură"
- Legea nr.59 din 29.03.2012 „Cu privire la activitatea specială de investigații",
- Statutului disciplinar al polițistului aprobat prin Hotărârea Guvernului nr. 502 din 09.07.2013,
- Hotărârea Guvernului nr.986 din 24.12.2012 „Cu privire la structura și efectivul-limită ale Inspectoratului General al Poliției al MAI",
- Regulamentul privind organizarea și funcționarea Direcției generale urmărire penală (în continuare DGUP) a IGP al MAI
- Regulamentul privind organizarea și funcționarea organului de urmărire penală al Ministerului Afacerilor Interne instituit în cadrul Departamentului Poliției de Frontieră (Ordinul MAI nr. 666 din 04.10.2014),
- Ordinul MAI nr.300 din 15 octombrie 2014 „ Cu privire la aprobarea Regulamentului privind organizarea și funcționarea Serviciului protecție internă și anticorupție al Ministerului Afacerilor Interne";
- Ordinul comun nr. 121 / 254 / 286-0 / 95 din 18 iulie 2008 "Cu privire la evidența unică a infracțiunilor, a cauzelor penale și a persoanelor care au săvîrșit infracțiuni"

Alinierea la arhitectura TIC de viitor

Locul și rolul proceselor operaționale de gestiune a Cauzelor Penale în Arhitectura TIC de viitor a MAI poate fi prezentată în următorul mod:



În acest mod procesul de gestiune a Cauzelor Penale intervine după clasificarea semnalărilor de evenimente sau alte stări de fapt ca fiind sesizări de infracțiuni. Obiectivele proceselor constau în aplicarea prevederilor cadrului legislativ-normativ cu privire la infracțiuni.

MODELUL PROCESELOR EXISTENTE ÎN DOMENIUL ANALIZAT (BUSINESS PROCESS "AS IS")

Sfera de cuprindere

Sfera de cuprindere funcțională a sistemului informatic cerut prin prezentul caiet de sarcini este dată de un *business-proces* foarte important din activitatea MAI, anume gestiunea cauzelor penale.

Metodologia de derulare a acestui *business-proces* este reglementată printr-o lege și trei acte normative importante:

Codul de Procedură Penală al Republicii Moldova (CPP)

- Ordinul interdepartamental nr.121/254/286-0/95 din 18.07.2008 „Privind evidența unică a infracțiunilor, a cauzelor penale și a persoanelor care au săvârșit infracțiuni"
- Ordinul IGP nr. 138 din 11.11.2013 „Privind aprobarea instrucțiunilor referitoare la organizarea activității de urmărire penală în cadrul Inspectoratului General al Poliției al MAI"
- Ordinul DPF nr. 22 din 25.01.2013 privind aprobarea Instrucțiunilor referitoare la organizarea activității de urmărire penală în cadrul Departamentului Poliției de Frontieră al MAI (cu modificări ulterioare prin ord. DPF nr.251 din 20.06.2013)

Business-proces-ul are ca scop evidența derulării procesului de urmărire penală, de la inițierea lui prin sesizarea sau autosesizarea organului de urmărire penală până la terminarea lui prin una din modalitățile prevăzute în lege, după caz:

- refuzul de a începe urmărirea penală, trimiterea cauzei în judecată,
- încetarea urmăririi penale,
- clasarea cauzei penale
- liberarea de răspundere penală în urma suspendării condiționate.

Prin evidența derulării se vor înțelege următoarele aspecte:

- Evidența tuturor actelor procesuale primite și întocmite de către organul de urmărire penală pe parcursul derulării procesului de urmărire penală

Evidența tuturor acțiunilor de urmărire penală și măsurilor luate de organul de urmărire penală pe parcursul derulării procesului de urmărire penală

- Evidența entităților implicate în procesul penal: persoane, fapte, bunuri și a circumstanțelor relevante privind cauza penală (timp, locație etc.)

Acest *business-proces* se derulează în cadrul următoarelor categorii de structuri din cadrul MAI, care îndeplinesc funcția de organ de urmărire penală și constituie ca atare sfera de cuprindere instituțională a *business-procesului* analizat:

- Direcția Urmărire Penală din cadrul Departamentului Poliției de Frontieră (DPF)
- Secțiile de urmărire penală a Direcțiilor regionale ale DPF, care își desfășoară activitatea sub coordonarea metodologică a Direcției urmărire penală a DPF
- Direcția Generală de Urmărire Penală din cadrul Inspectoratului General al Poliției (IGP)
- Secțiile de urmărire penală din cadrul inspectoratelor raionale ale Poliției, care își desfășoară activitatea sub coordonarea metodologică a Direcției Generale de Urmărire Penală de la nivelul IGP
- Secțiile de Urmărire penală din cadrul subdiviziunilor constituite la nivel central în cadrul IGP și specializate

pe anumite tipuri de infracționalități (Combaterea Traficului de Ființe Umane și Combaterea Criminalității Informaționale), pentru fapte în competența lor.

- Secția urmărire penală a Serviciului protecție internă și anticorupție al Ministerului Afacerilor Interne

Notă: *Subdiviziunile teritoriale aflate la un nivel inferior nivelului de inspectorat (de exemplu posturile de politie) nu au competență de urmărire penală ci doar de constatare, conform art. 273 din Codul de Procedură Penală (CPP).*

Un aspect important al sferei de cuprindere instituționale derivă din faptul că prin CPP (art.52, al. l, p.3)," Procurorul exercită conducerea acțiunilor de urmărire penală efectuate de organul de urmărire penală". Implicațiile acestui rol al Procuraturi asupra implementării sistemului informatic al MAI sunt următoarele:

- Modelul logic al sistemului informatic al MAI trebuie să fie compatibil (nu neapărat identic, ci compatibil) cu cel care este folosit de Procuratură
- în anumite faze ale business-proces-ului informatizat va trebui să fie prevăzute interfețe de comunicare cu sistemul informatic al Procuraturii, pentru a facilita, prin intermediul celor două sisteme informatice care comunică între ele, exercitarea de către procurorul de caz a atribuțiilor sale legale de „conducere a acțiunilor de urmărire penală".

Vor exista instanțe de *business-proces* în care pași din proces vor fi executați în afara sferei de cuprindere a sistemului informatic (fiind executate de către Procuror, care nu este un utilizator al sistemului informatic al MAI). Pentru aceste situații, în modelul informatic al *business-proces-ul*ui va trebui prevăzută posibilitatea marcării acestor faze printr-un scenariu de utilizare alternativ, cu alte cuvinte prin documentarea pasului respectiv în sistemul informatic al MAI, nu prin realizarea/execuția pasului în sistemul informatic.

Modul de lucru actual si diagrame de proces

Organele de urmărire derulează astăzi *business-process-ul* aproape exclusiv în formă letrică (pe hârtie) cu excepția organizării și gestiunii unei evidențe electronice unice și centralizate la nivel național, de către o subdiviziune a MAI specializată în acest sens, numită astăzi Serviciul Tehnologii Informaționale (STI) (în actul normativ care reglementează evidența unică, această subdiviziune este menționată cu numele *Direcția informații și evidențe operative)* care gestionează un registru unic al infracțiunilor, cauzelor penale și persoanelor care au săvârșit infracțiuni (așa numitul „Registru al informației criminalistice și criminologice – „R.I.C.C.") prin culegerea în sistem informatic a datelor completate de către organul de urmărire penală în fișe/formulare standard (formularele 1.1.1, 2.0, 2.1., 2.2, și 2.7 conform instrucțiunilor din Ordinul interdepartamental nr.121/254/286-0/95.)

Având în vedere stilul de lucru descris mai sus, în realitate astăzi se derulează trei *business-procese* paralel, fiecare din ele având finalități diferite:

1. Gestiunea cauzei penale, având ca output final dosarul înaintat în instanță sau, după caz, dosarul finalizat prin încetarea, clasarea sau liberarea de răspundere penală.
2. înregistrarea sesizărilor, având ca output înregistrarea sesizării infracțiunii în așa numitul Registru 1 al unității și Registrul de sesizări la nivel național precum și decizia organului de urmărire penală față de sesizarea

respectivă în sensul începerii urmăririi penale sau refuzului de începere a urmăririi penale.

3. înregistrarea infracțiunilor, cauzelor penale și persoanelor care au săvârșit infracțiuni, având ca output final evidența centralizată de la STI al MAI, unică la nivel național

Cele trei procese sunt corelate și se influențează reciproc, prima fiind de fapt activitatea principală și celelalte două fiind secundare, de tip administrativ, însă care impun niște constrângeri formale în activitatea de urmărire penală.

Din punctul de vedere al ciclului de viață, se disting 3 faze mari:

- **faza** sesizării, la finalul căreia organul de urmărire penală a realizat toate demersurile **legale** pentru ca fapta sesizată să fie înregistrată conform prevederilor CPP și procedurilor interne
- faza premergătoare urmăririi penale (putând fi numită și faza cercetării prealabile) la finalul căreia

o fie este emisă ordonanța de începere a urmăririi penale (de către ofițerul de urmărire penală sau de către procuror, după caz) o fie Procurorul emite o ordonanță de neîncepere a urmăririi penale și dispune clasarea procesului penal (cf. art. 274 CPP).

- faza urmăririi penale, care este inițiată prin decizia de începere a urmăririi penale, luată de către ofițerul de urmărire penală sau de către Procuror, după caz, și se finalizează prin trimiterea în judecată sau încetarea urmăririi penale, clasarea sau liberarea de răspundere penală, după caz.

Acest ciclu deviată este reprezentat în diagrama de tip BPMN 2.0 de mai jos:

Faza înregistrării sesizării este cel mai puțin standardizată și procedurizată în momentul de față fiind parțial derulată anterior procesului penal. Din acest motiv, etapa respectivă de proces este reprezentată în diagrama de mai sus ca fiind la rândul ei compusă din:

Preluarea semnalărilor

- ***Înregistrarea sesizărilor formulate conform CPP***

Prin preluarea semnalărilor se înțelege orice tip de interacțiune în formă scrisă sau orală a unităților MAI cu persoane care semnalează infracțiuni, interacțiune care premerge înregistrarea unei sesizări care respectă toate criteriile formale și procedurale ale unui act de sesizare conform CPP. Astfel, în această fază infracțiunile sunt semnalate prin:

- ***Apeluri telefonice***

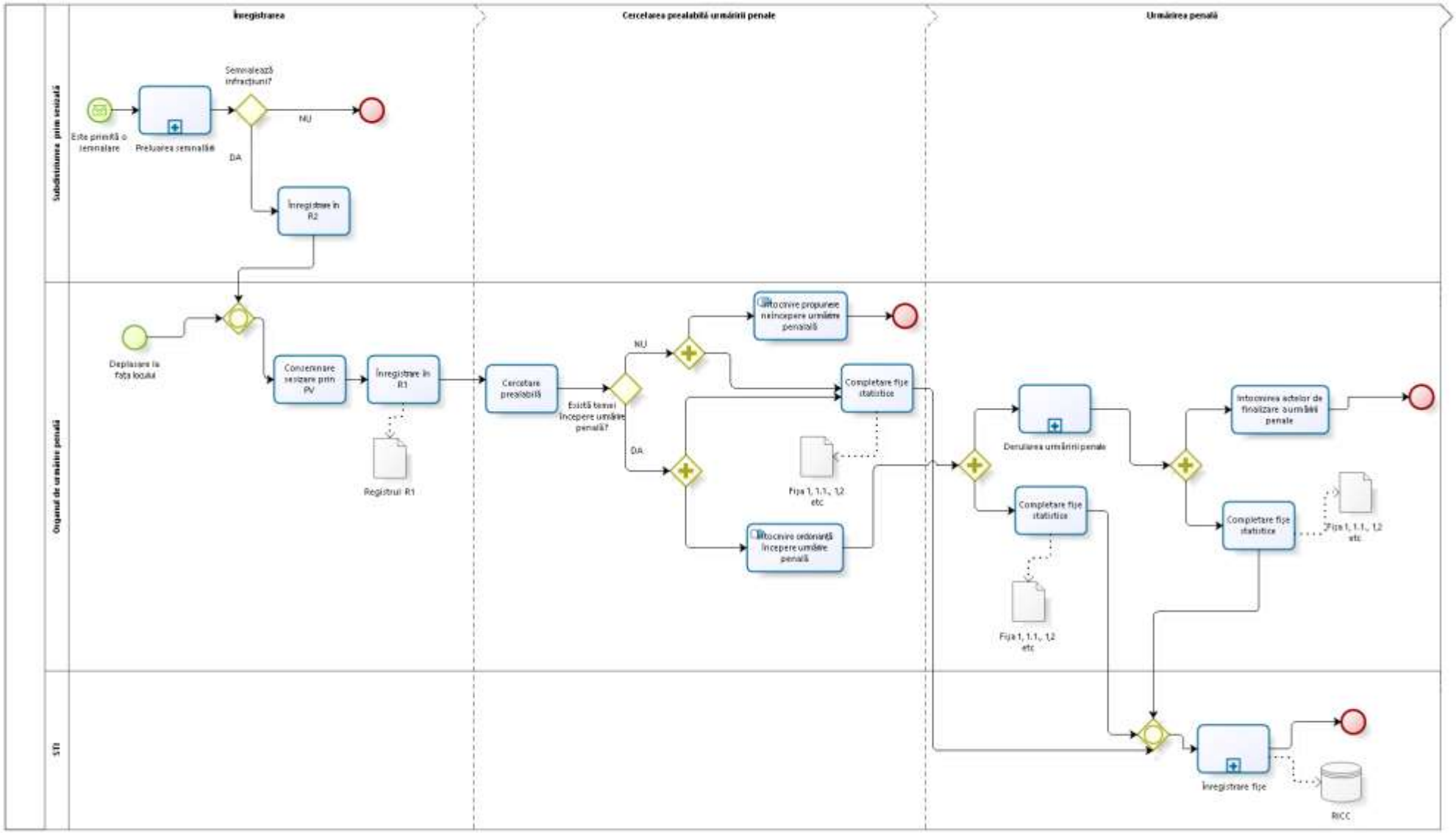
Petiții scrise care nu îndeplinesc condițiile formale pentru o sesizare conform CPP, însă conțin descrierea unor infracțiuni

- ***Mesaje electronice primite prin email, fax sau altă formă de corespondență electronica***
- ***Audiențe***

Discuții la fața locului dintre persoanele care semnalează și angajați ai MAI

- **Sesizări care respectă condițiile CPP** dar care nu au fost înaintate direct unui organ de urmărire penală ci unei unități de Poliție care nu are competențe în acest domeniu și le înregistrează în registrul propriu de petiții generale.

În funcție de tipul faptei și de competența teritorială, toate aceste semnalări sunt aduse la cunoștința unui organ de urmărire penală, care:


Înregistrarea
Cercetarea prealabilă urmăririi penale
Urmărirea penală
Subdiviziunea prin sesizării
Organul de urmărire penală
STI
Este primită o sesizare
Prelucrarea semnalării
Semnalează infracțiuni?
NU
DA
Înregistrare în R2
Deplasare la fața locului
Consemnare sesizare prin PV
Înregistrare în R1
Registrul R1
Cercetare prealabilă
Există temei începere urmărire penală?
NU
DA
Întocmire propunere neîncepere urmărire penală
Întocmire ordonanță începere urmărire penală
Completare fișe statistice
Fișa 1, 1.1., 1.2 etc
Derularea urmăririi penale
Completare fișe statistice
Fișa 1, 1.1., 1.2 etc
Întocmirea actelor de finalizare urmăririi penale
Completare fișe statistice
Fișa 1, 1.1., 1.2 etc
Înregistrare fișe
RICC

a) Fie înregistrează actul de sesizare ca atare în Registrul de sesizări R1 (dacă semnalarea a respectat de la început condițiile formale și procedurale ale unei sesizări conform prevederilor CPP)

b) Fie întocmește unul sau mai multe procese verbale de consemnare a plângerii sau denunțului sau autodenunțului luate nemijlocit de către ofițerul de urmărire penală de la petentul petiției (semnalării) inițiale care a fost înregistrată în R2.

Ca atare, această etapă a procesului se finalizează în momentul în care este generat în format letric un act de sesizare care respectă criteriile definite în CPP și sesizarea este înscrisă în Registrul R1.

Etapa a doua a business-procesului principal se finalizează când se ia, printr-o ordonanță (finală și necontestată) decizia cu privire la începerea sau neînceperea urmăririi penale (ordonanța finală fiind emisă, după caz, fie de ofițerul de urmărire penală fie de către un procuror). Un al doilea output obligatoriu al acestei etape (în cazul începerii urmăririi penale) este dat de înregistrarea infracțiunilor, cauzelor penale și persoanelor care au săvârșit infracțiuni în evidența națională organizată de STI din cadrul MAI, pe baza fișelor completate de către ofițerul de urmărire penală.

Etapa a 3-a, care nu se derulează decât pentru cauzele penale care la finalul etapei 2 au generat o ordonanță de începere a urmăririi penale, echivalează cu gestiunea cauzei penale până la soluționarea ei sub o formă sau alta, conform soluțiilor prevăzute în CPP. Conform modului de lucru actual, output-urile acestei etape sunt exclusiv în formă letrică și constau din toate documentele și actele procedurale completate și îndosariate în dosarul cauzei penale.

Așa cum a fost menționat inițial, în paralel cu *business-proces-ul* principal, cel de realizarea a activităților și întocmire a actelor prevăzute în CPP pentru soluționarea cauzei penale, are loc un proces administrativ paralel, care are ca obiectiv culegerea datelor statistice relevante din cauzele respective și înregistrarea acestora într-o bază de date centralizată la nivel național. Ca atare, în modelul de mai sus, în paralel cu activitățile de cercetare/urmărire penală grupate pe fazele majore, au fost ilustrate activități de întocmire a fișelor statistice (de către Ofițerul de urmărire penală). în modul de lucru actual, aceasta presupune că activitatea de întocmire a fișelor statistice generează de fiecare dată *out-put*-uri în formă letrică care devin apoi *input* pentru sub-procesul derulat la nivelul STI, de înregistrare a acestor fișe într-o bază de date electronică, numită R.I.C.C.

Ce fișe se completează și în ce condiții, precum și formularistica sunt prevăzute în reglementările specifice din cadrul Ordinului comun nr. 121 / 254 / 286-0 / 95 din 18 iulie 2008 "Cu privire la evidența unică a infracțiunilor, a cauzelor penale și a persoanelor care au săvîrșit infracțiuni". Pentru scopul acestui document, analiza AS IS nu necesită detaliere suplimentară pe acest subiect, deoarece modelarea TO BE va modifica prezumtiv semnificativ această activitate administrativă, ținând cont că va avea loc implementarea unei evidențe electronice direct la nivelul dosarului.

MODELUL ENTITĂȚILOR ÎN DOMENIUL ANALIZAT

Sistemul informatic WFMS va permite stocarea in baza de date a doua categorii de informații referitoare la procedura penală:

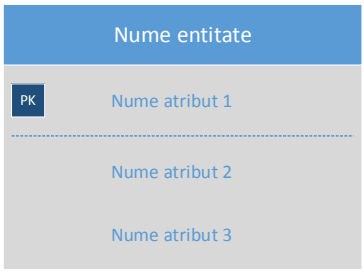
> Informația structurata - aceasta va fi înregistrată sub forma unor atribute ale unor obiecte relaționate, relevante procesului penal, pentru care modelul logic de date propus este prezentat mai departe in cadrul acestei secțiuni;

> Informația nestructurata - aceasta va fi înregistrată prin intermediul unor documente in format electronic, rezultate in urma obținerii unei copii scanate a unui document original tipărit (documentele scanate vor putea sa aibă mențiunea „conform cu originalul" certificată prin semnătură digitală).

Sursele de date

Datele care vor fi gestionate in cadrul sistemului informatic vor avea următoarele surse de generare:

- Date conținute in nomenclatoarele existente in cadrul sistemului informatic WFMS;
- Datele introduse manual in sistemul informatic WFMS prin intermediul ecranelor utilizator;
- Datele furnizate automat de alte sisteme informatice prin interfețe specializate de schimb de date (spre exemplu: servicii web);
- Date conținute in nomenclatoarele proprii unor alte sisteme informatice / baze de date, obținute prin interogare si furnizate prin interfețe specializate de schimb de date (spre exemplu: servicii web);
- Date obținute prin digitizarea (OCR-izare) unor documente in formă tipărită;
- Diagrama de mai jos reprezintă entitățile logice din cauza penală și relațiile dintre ele. Fiecare din aceste entități este reprezentată printr-un simbol grafic de tipul



N.B.: *Pentru a permite citirea facilă a modelului entităților, în diagrama în care sunt prezentate toate entitățile și relațiile dintre ele, numită Diagrama generală a entităților, nu au fost trecute și atributele entităților, acestea fiind reprezentate exclusiv în diagramele care detaliază cât o entitate principală (ex. Diagrama detaliată a Persoanei etc).*

Relațiile dintre entități sunt reprezentate prin linii care marchează la fiecare capăt multiplicitatea entității în relația cu entitatea legată, astfel:

*1..**	Una sau mai multe entități de la acest capăt al relației intră în relație cu entitatea de la celălalt capăt al relației
*0..**	Zero sau mai multe entități de la acest capăt al relației intră în relație cu entitatea de la celălalt capăt al relației
0..1	Zero sau cel mult o entitate de la acest capăt al relației intră în relație cu entitatea de la celălalt capăt al relației
1	0 singură entitate și numai una de la acest capăt al relației intră în relație cu entitatea de la celălalt capăt al relației

În diagrama principală a fost definite printr-o etichetă de tip text relația dintre două entități, linia de legătură între două entități fiind cu orientare (săgeată la capăt) pentru a indica dinspre care entitate spre care se aplică denumirea relației respective.

Pe lîngă relațiile dintre entități care sunt explicitate prin eticheta poziționată pe relație, modelul mai include 3 tipuri de relații care sunt explicitate prin simbolul de la capătul ei:

	**Compunerea**: reprezentată printr-un simbol de tip romb plin, indică faptul că o entitate este compusă din entități de tipul celor care aparțin clasei care se află la celălalt capăt al relației. Spre exemplificare, un dosar este compus din unul sau mai multe acte/documente, iar acest lucru a fost reprezentat printr-o relație de compunere, care unește în diagramă entitate **Dosar** de entitatea **Document/Act**
	**Agregarea**: este o relație asemănătoare cu prima, reprezentată de această dată cu un romb gol. Diferența între compunere și agregare este că în timp ce în cazul compunerii vorbim de relația dintre parte și întreg, în care partea nu poate exista dacă dispare întregul, la agregarea vorbim de o colecție, în care un membru al colecției poate exista și dacă dispare colecția. Spre exemplificare, mai mulți infractori se pot agrega într-un grup infracțional organizat. Dispariția grupului (de exemplu prin destructurarea lui) nu duce automat la dispariția persoanelor care l-au constituit inițial.
	**Generalizarea**: reprezentată printr-un triunghi gol, indică faptul că o entitate este o generalizare a mai multor entități diferite. Spre exemplificare, Persoana este o generalizare pentru mai multe tipuri de persoane: cetățeni ai R. Moldova, persoane juridice, cetățeni străini, etc.

Toate diagramele respecta notațiile UML pentru diagramele de clase. Modelul prevăzut în prezenta documentație este ceea ce se cheamă *"conceptual domain model"* in care sunt reprezentate entitățile logice, cu atributele lor, si relațiile dintre entități. Aceasta modelare a entităților logice din domeniul analizat nu trebuie confundată cu modelarea unei scheme fizice in baza de date, ci o precede pe aceasta, fiind un *layer de* abstractizare. Astfel, o entitate logica din model (de exemplu **Persoana)** poate fi implementata in schema de date fizica prin mai multe tabele (de exemplu pentru a stoca in tabele diferite tipurile diferite de persoane, sau pentru a stoca versiunile, sau din alte motive dezvoltatorul sistemului poate decide implementarea pe mai multe tabele, chiar daca logic e o entitate). La fel de bine se poate întâmpla si invers: mai multe entități logice diferite sa fie stocate într-un singur tabel, sau chiar toate entitățile sa fie stocate într-un singur tabel, iar o coloana din acest tabel sa indice de fapt ce entitate este înregistrarea respectiva.

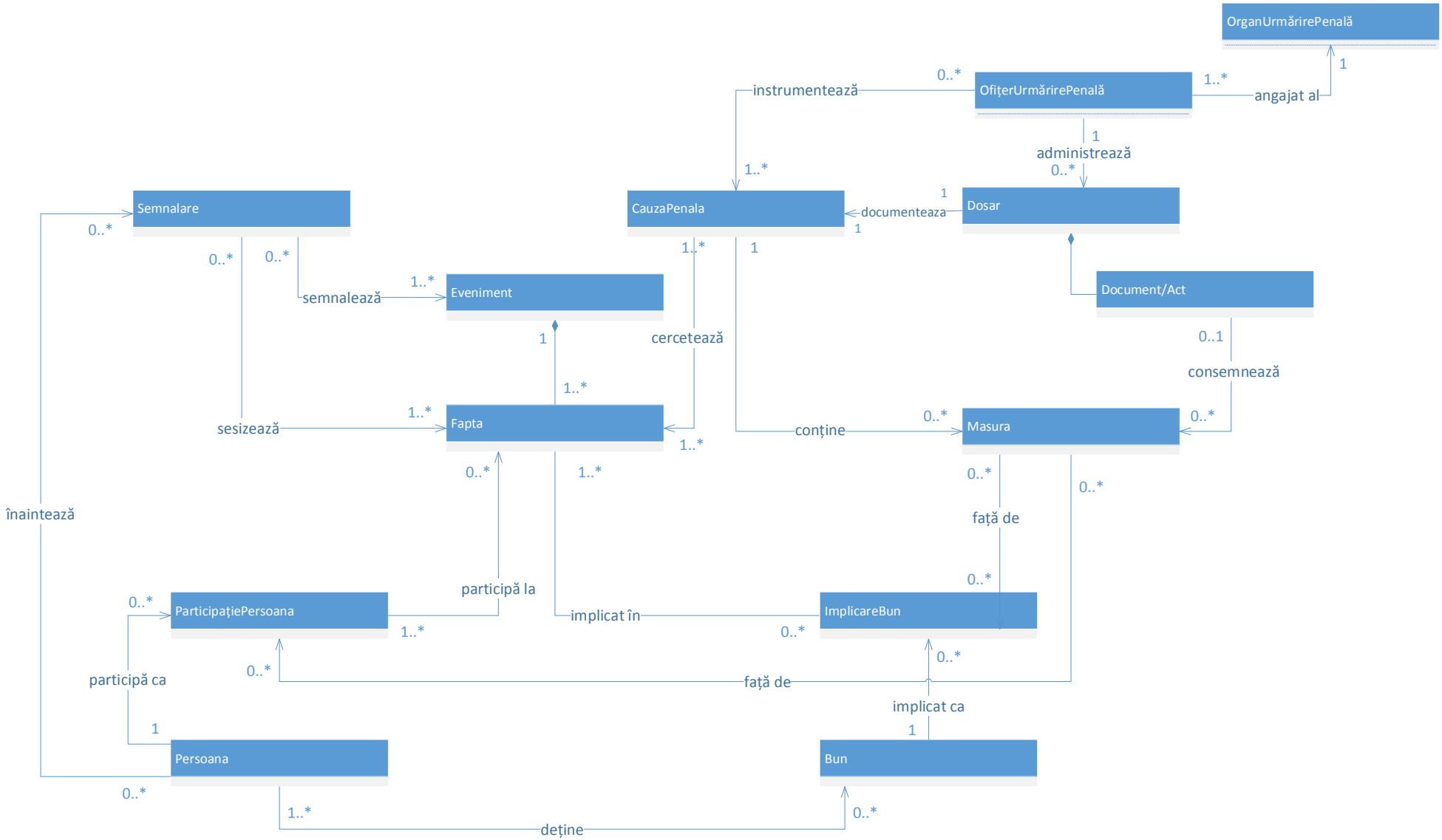
Indiferent dacă aceste entități reprezintă sau nu o entitate concretă din realitate (cum e cazul **Persoanei, Bunului** etc) sau o entitate de tip abstract (ex. **Cauza Penala)** sau chiar o **entitate** de tip logic, cum este cazul **Participației Persoanei,** reprezentarea lor în acest **model** indică faptul că Furnizorul sistemului informatic trebuie să modeleze aceste entități în **modelul** de implementare al aplicației informatice. în acest sens, modelul prezentat mai **jos** este un model prescriptiv, de tipul "TO BE" care se constituie în specificații de **implementare.** Pe de altă parte, acest model nu este limitativ, în sensul în care în sistemul informatic nu vor fi modelate exclusiv aceste entități, ci este unul minimal, în sensul în care în sistemul informatic vor fi modelate cel puțin aceste entități.

Diagrama generală a entităților

Diagrama următoarele prezintă toate entitățile importante ale domeniului conceptual care vor fi reprezentate în sistemul informatic cerut și relațiile dintre acestea, inclusiv cardinalitatea și multiplicitatea.

Explicații

1. A fost modelată entitatea **Semnalare** ca o clasă generică pentru toate tipurile de intrări în sistem care semnalează una sau mai multe infracțiuni(fapte) dar care încă nu au fost clasificate ca fiind acte de sesizare sau nu corespund criteriilor minime pentru un act de sesizare, conform CPP. Această entitate nu este obligatorie, în sensul că nu în toate instanțele de *business-proces* vor exista semnalări, anumite cauze penale putând fi de exemplu a fi constituite prin disjungerea dintr-o cauză existentă, nu în baza unei semnalări.
2. în completarea modelului de mai sus, care prezintă o viziune statică asupra entităților, este important de menționat faptul că o **Semnalare** (dacă îndeplinește condițiile formale prevăzute în CPP) devine sesizare/act de de sesizare (plângerea, denunțul, autodenunțul sau autosesizarea, după caz) și se transformă într-o altă entitate din acest model, anume **Document/Act** în cadrul **Dosarului.** Acest tip de act este obligatoriu la nivel conceptual, în sensul în care nu poate exista proces penal în absența unei forme de sesizare. La nivelul sistemului informatic ce trebuie implementat însă, având în vedere faptul că sesizarea/autosesizarea poate fi înregistrată în afara sistemului MAI (de exemplu la Procuratură) implică faptul că vor exista Dosare în care nu vor exista Acte de Sesizare materializate în interiorul sistemului MAI. însă și în aceste cazuri, având în vedere constrângerile privind evidența unică la nivel republican a sesizărilor, ofițerul de urmărire penală responsabil de cauză va avea acces la informația privind numărul unic de înregistrare și va putea ca atare genera în sistem această entitate, cel puțin cu acest atribut.
3. Au fost modelate două entități de legătură (echivalentul unei Association Class în modelarea object-oriented) care au însă un rol foarte important în procesul penal: **Participație Persoană,** respectiv **Implicare Bun.** Pentru exemplificare, într-o cauză penală, o singură persoană poate avea mai multe participații (făptuitor a două dintre fapte și complice sau instigator la cea de a treia) iar măsurile și actele procesuale din cadrul procesului penal se vor lua individual, pentru fiecare participație. De exemplu, într-o astfel de cauză se poate lua decizia începerii urmăririi penale față de persoana respectivă cu privire la săvârșirea unei dintre fapte și decizia de neîncepere a urmăririi penale față de aceeși persoană cu privire la săvârșirea celei de a doua fapte. Din acest motiv, entitățile **Faptă, Act Procesual, Măsură Procesuală** nu sunt relaționate direct cu **Persoana,** ci cu entitatea **Participație Persoană.**
4. În mod similar cu entitatea **Participație Persoană** a fost modelată și entitatea **Implicare Bun,** deoarece un singur **Bun** poate fi implicat în mai multe moduri într-o cauză penală.
5. În entitatea **Persoană** sunt modelate toate persoanele care participă cu un rol sau altul la cauza penală. Aceste persoane sunt de mai multe tipuri (fizice, juridice) inclusiv persoane necunoscute (atunci când făptuitorul faptei sesizate nu este cunoscut sau victima nu poate fi identificată), iar această clasificare, împreună cu atributele acestei entități, este detaliată într-o diagramă separată mai jos.


OrganUrmărirePenală
OfițerUrmărirePenală
instrumentează
angajat al
administrează
Semnalare
CauzaPenala
documenteaza
Dosar
Document/Act
semnalează
Eveniment
cercetează
consemnează
sesizează
Fapta
conține
Masura
înaintează
față de
participă la
implicat în
ParticipațiePersoana
ImplicareBun
participă ca
față de
implicat ca
Persoana
Bun
deține

6. **Cauza penală** reprezintă aparent același lucru cu Dosarul penal (de aici 1 la 1). însă în realitate, în timp ce Dosarul este containerul fizic și colecția de documente din aceasta, (agregă toate documentele care au legătura cu cauza penala), CauzaPenală este obiectul, materia procesului penal (faptele pe care Ie-a înfăptuit cineva si care fac obiectul urmăririi si apoi judecării). In Ordinul 138 se marchează în mod explicit această distincție prin definiția dosarului penal: "Dosarul penal - mapă, sau dispozitiv special adaptat pentru păstrarea tuturor actelor procedurale, altor documente, obiecte sau materiale, ce se referă la o cauză penală concretă". Mai mult, la un moment dat se poate întâmpla ca o cauza penala, (gestionata într-un dosar) sa fie transferata prin conexare intr-un alta dosar. Din acest motiv au fost modelate ca entități diferite, care sunt însă într-o relație 1 la 1.

7. Conform modelului, într-o semnalare pot fi sesizate una sau mai multe **Fapte.** De asemenea, aceeași **Faptă** poate fi sesizată prin una sau mai multe Semnalări, ceea ce înseamnă ca poate fi sesizată ca atare prin mai multe **Acte de sesizare.** Din acest motiv, atributul de **Număr unic** (în Registrul RI) este al **Actului de sesizare,** nu al faptei sesizate.

Diagrama detaliată a Persoanei și a entităților care se relaționează cu aceasta

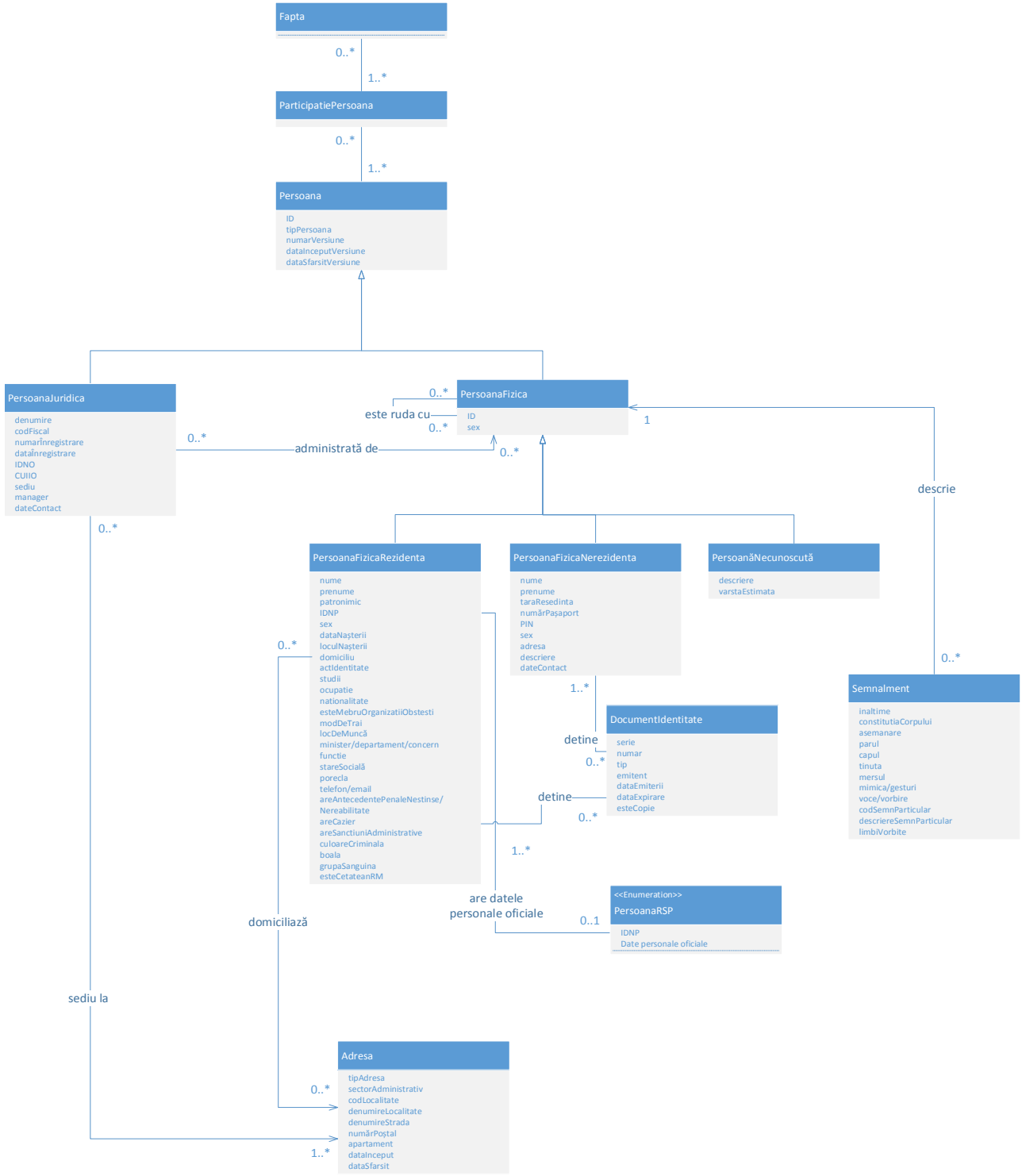
Diagrama următoarele prezintă în detaliu, pentru entitatea **Persoană** și alte entități, care intră în relație cu aceasta, următoarele elemente:

- atributele importante ale domeniului conceptual care vor fi implementate în sistemul informatic cerut
- relațiile dintre entități, inclusiv cardinalitatea și multiplicitatea.

Atributele prezentate în diagramă reprezintă setul minimal de atribute pe care sistemul informatic cerut trebuie să aibă capabilitatea să le implementeze, fără ca diagrama să reprezinte o specificație exhaustivă, limitativă. în acest sens, în timpul implementării, pe baza rezultatelor fazelor de analiză, proiectare și configurare/dezvoltate, setul de atribute poate fi extins și cu alte atribute care vor fi considerate necesare de către Beneficiarul sistemului informatic.

Explicații

1. în modelul de mai sus au fost reprezentate distinct principalele tipuri de persoane care vor fi gestionate în sistemul informatic, una din cele mai importante distincții fiind cea dintre PersoanaFizică și PersoanaJuridică, existând diferențe semnificative între atributele celor două subtipuri. La rândul său, PersoanaFizică este o generalizare a trei sub-tipuri importante, cele mai multe atribute fiind definite la nivelul persoanei fizice rezidente. Pentru acest tip de persoane, prin atributul IDNP, se stochează referință și la RSP - registrul național unic al persoanelor din Republica Moldova. Este important însă de precizat că pentru acest tip de persoană sistemul informatic nu va stoca doar o simplă referință la RSP, ci va stoca propria definiție a persoanei, conform celor rezultate în cercetarea penală, dar va permite în același timp identificarea definției oficiale a persoanei respective.



2. Persoanele necunoscute sunt un sub-tip de persoană fizică, cu atribute specifice (în principal cele legate de semnalmente) și se instanțiază individual în cadrul cauzei Penale. Cu alte cuvinte, atunci când în săvârșirea faptei este implicată o persoană necunoscută, ea va fi instanțiată ca o persoană, distinctă de alte instanțe de persoane de același tip, urmând ca pe parcursul cercetării penale să-i fie completate atributele, până devine o persoană cunoscută, caz în care i se modifică tipul persoanei.

3. PersoanăFizicăNerezidentă reprezintă tot un tip de persoană fizică, cu atribute specifice persoanelor care se află temporar pe teritoriul Republicii Moldova și care sunt implicate într-o cauză penală.

Diagrama detaliată a Faptei și a entităților care se relaționează cu aceasta

Diagrama următoarele prezintă în detaliu, pentru entitatea **Faptă** și alte entități, care intră în relație cu aceasta, următoarele elemente:

- atributele importante ale domeniului conceptual care vor fi implementate în sistemul informatic cerut
- relațiile dintre entități, inclusiv cardinalitatea și multiplicitatea.

Atributele prezentate în diagramă reprezintă setul minimal de atribute pe care sistemul informatic cerut trebuie să aibă capabilitatea să le implementeze, fără ca diagrama să reprezinte o specificație exhaustivă, limitativă. în acest sens, în timpul implementării, pe baza rezultatelor fazelor de analiză, proiectare și configurare/dezvoltate, setul de atribute poate fi extins și cu alte atribute care vor fi considerate necesare de către Beneficiarul sistemului informatic.

Explicații

1. Un eveniment este compus din una sau mai multe fapte, săvârșite în aceeași locație și în același interval de timp și care fac obiectul unei semnalări.
2. în situațiile în care semnalarea respectă criteriile formale definite de CPP pentru o sesizare, faptele sunt sesizate prin intermediul semnalării, care este în același timp și act de sesizare.
3. O parte din atributele care definesc modul de producere a faptei sunt cel mai bine implementate la nivelul entității **ParticipațiePersoană.** De exemplu, modul de operare poate fi diferit pentru fiecare participant la săvârșirea unei fapte atunci când mai multe persoane sunt implicate, motiv pentru care este implementat la nivelul acestei entități.
4. O cauză penală poate proveni dintr-o altă cauză penală în urma disjungerii sau conexării unor cauze penale, motiv pentru care în diagramă a fost reprezentată această relație autoreferențială pentru entitatea **CauzăPenală.**
5. în această diagramă sunt reprezentate distinct principalele tipuri de bunuri care vor fi gestionate în sistemul informatic, pentru a evidenția principalele atribute care sunt de interes pentru a fi gestionate distinct în sistemul informatic. Pentru tipul de bun **AltTipDeBun,** vor fi gestionate doar atributele generice, definite la nivelul clasei **Bun,** în timp ce pentru celelalte tipuri de bunuri, care reprezintă niște tipuri de interes deosebit pentru activitatea de combatere a infracțiunilor, pe lângă atributele generice vor fi gestionate în sistemul informatic și atributele specifice fiecărui din aceste tipuri. Enumerarea acestor tipuri în diagramă nu este exhaustivă, ci mai degrabă ilustrativă, pentru a indica tipuri diferite de bunuri, inclusiv unele tipuri de bunuri imateriale, de exemplu Avantajele, dar și o categorie ce poate fi asimilată bunurilor prin analogie, adică Servicii. Există și alte categorii similare, precum privilegii, funcții, demnități, care nu au fost figurate în diagramă explicit, însă toate acestea vor fi considerate oricum incluse sub categoria generică de AltTipdeBun, nefiind necesare atribute specifice care să ducă la modelarea ca o clasă distinctă.
6. Pe lângă atributele care descriu Bunul din punct de vedere fizic si valoric bunurile, a fost modelat și un atribut care are importanță din punct de vedere penal, anume un atribut de tip boolean care indică dacă bunul respectiv* reprezintă sau nu o remunerare ilicită.

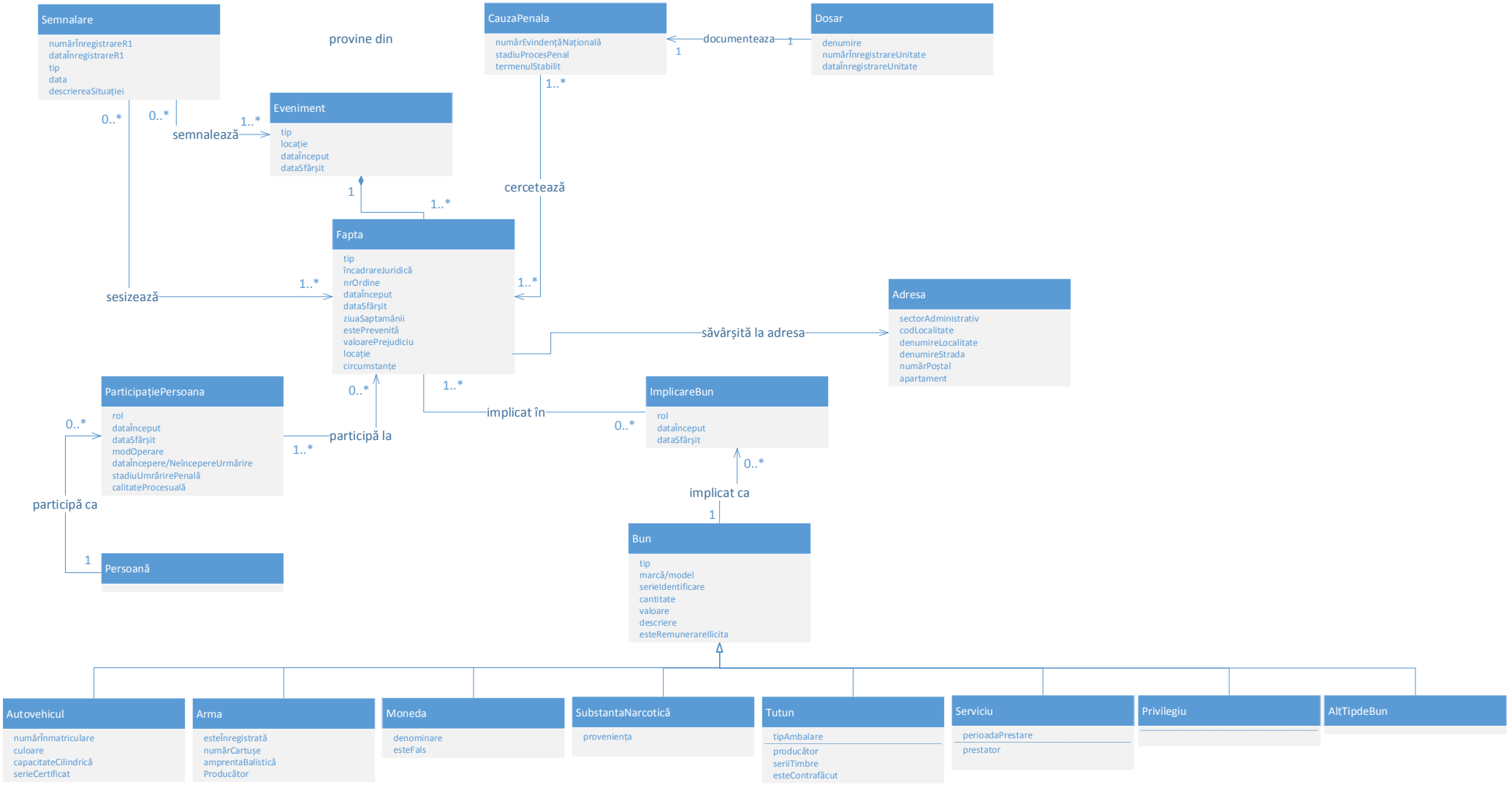

Semnalare
numărÎnregistrareR1
dataÎnregistrareR1
tip
data
descriereaSituației
provine din
CauzaPenala
numărEvindențăNațională
stadiuProcesPenal
termenulStabilit
documenteaza
Dosar
denumire
numărÎnregistrareUnitate
dataÎnregistrareUnitate
Eveniment
tip
locație
dataÎnceput
dataSfârșit
semnalează
cercetează
Fapta
tip
încadrareJuridică
nrOrdine
dataÎnceput
dataSfârșit
ziuaSaptamânii
estePrevenită
valoarePrejudiciu
locație
circumstanțe
sesizează
săvârșită la adresa
Adresa
sectorAdministrativ
codLocalitate
denumireLocalitate
denumireStrada
numărPoștal
apartament
ParticipațiePersoana
rol
dataÎnceput
dataSfârșit
modOperare
dataÎncepere/NeîncepereUrmărire
stadiuUmrărirePenală
calitateProcesuală
participă la
implicat în
ImplicareBun
rol
dataÎnceput
dataSfârșit
participă ca
implicat ca
Persoană
Bun
tip
marcă/model
serieIdentificare
cantitate
valoare
descriere
esteRemunerarellicita
Autovehicul
numărÎnmatriculare
culoare
capacitateCilindrică
serieCertificat
Arma
esteÎnregistrată
numărCartușe
amprentaBalistică
Producător
Moneda
denominare
esteFals
SubstantaNarcotică
proveniența
Tutun
tipAmbalare
producător
seriiTimbre
esteContrafăcut
Serviciu
perioadaPrestare
prestator
Privilegiu
AltTipdeBun

Diagrama detaliată a Actelor și Măsurilor

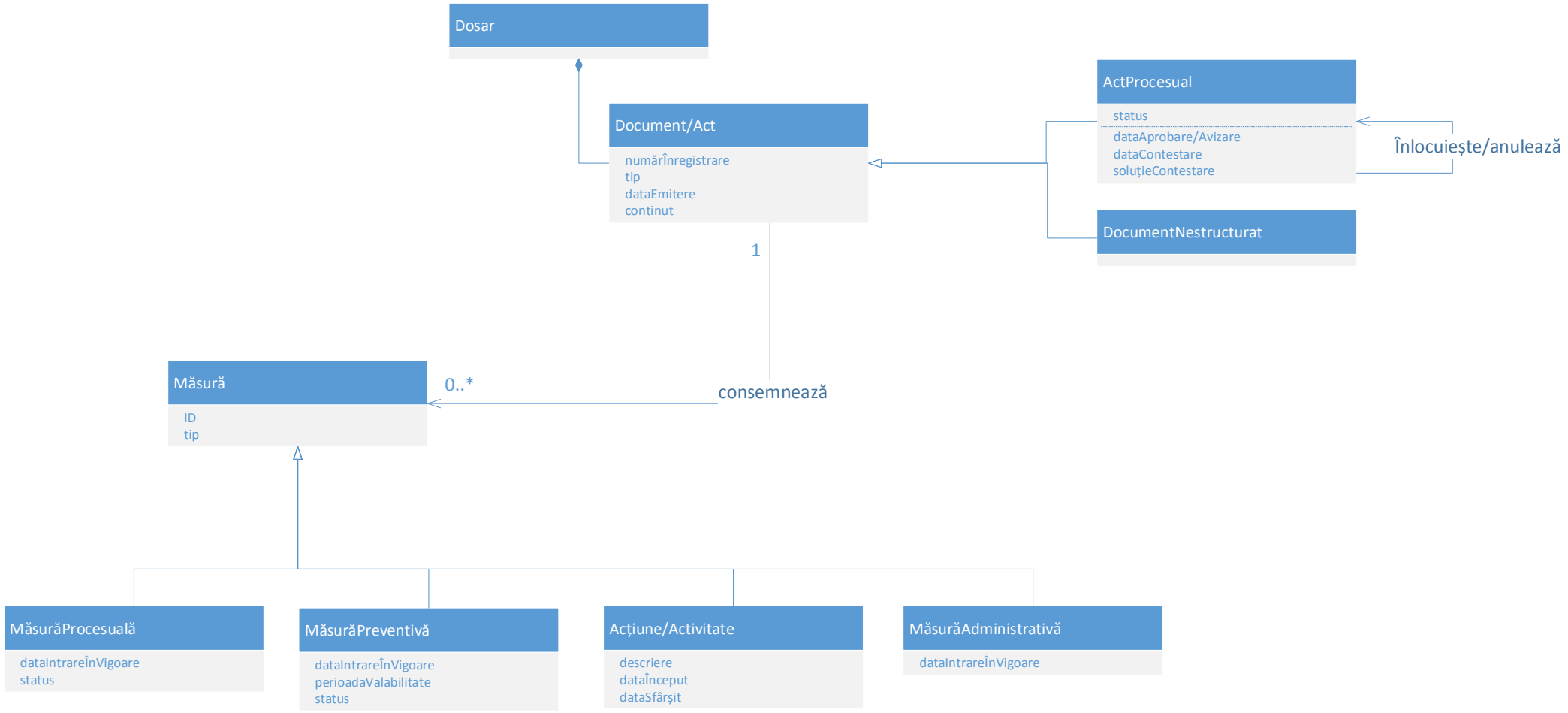
Diagrama următoarele prezintă în detaliu, pentru două entități importante ale domeniului, **Măsură și Act/Document Faptă,** următoarele elemente:

- atributele importante ale domeniului conceptual care vor fi implementate în sistemul informatic cerut
- relațiile dintre entități, inclusiv cardinalitatea și multiplicitatea.

Atributele prezentate în diagramă reprezintă setul minimal de atribute pe care sistemul informatic cerut trebuie să aibă capabilitatea să le implementeze, fără ca diagrama să reprezinte o specificație exhaustivă, limitativă. în acest sens, în timpul implementării, pe baza rezultatelor fazelor de analiză, proiectare și configurare/dezvoltate, setul de atribute poate fi extins și cu alte atribute care vor fi considerate necesare de către Beneficiarul sistemului informatic.

Explicații

1. Un **ActProcesual** poate intra în relația cu un alt **ActProcesual** atunci când, de exemplu, într-o fază ulterioară emiterii primului act procesual este emis un altul care anulează sau suspendă efectele primului act procesual. Această relație a fost ilustrată la nivelul diagramei prin relația **înlocuiește/anulează.**
2. Au fost incluse în model și tipuri de măsuri care nu sunt neapărat consemnate printr-un act procesual sau printr-un document. în acest mod, prin evidența măsurilor în dosar pot fi înregistrate și alte activități, specifice cercetării penale, dar care nu sunt prevăzute în CPP ca măsuri luate prin intermediul unor acte procesuale (de exemplu acțiuni preventive, sau analize operaționale realizate în dosar, interogări ale unor baze de date etc.)


Dosar
Document/Act
numărÎnregistrare
tip
dataEmitere
continut
ActProcesual
status
dataAprobare/Avizare
dataContestare
soluțieContestare
Înlocuiește/anulează
DocumentNestructurat
1
Măsură
ID
tip
0..*
consemnează
MăsuraProcesuală
dataIntrareÎnVigoare
status
MăsuraPreventivă
dataIntrareÎnVigoare
perioadaValabilitate
status
Acțiune/Activitate
descriere
dataÎnceput
dataSfârșit
MăsuraAdministrativă
dataIntrareÎnVigoare

MODELUL PROCESELOR CARE VOR FI INFORMATIZATE (BUSINESS PROCESS "TO BE")

Prin implementarea sistemului informatic, vor fi operate următoarele modificări semnificative asupra modului în care se va derula activitatea de gestiune a dosarului:

1. Activitățile administrative care în procesul de lucru actual au ca scop înregistrarea datelor din cauzele penale în evidența centralizată de la STI al MAI pe baza procesării formularisticii definite în Ord. 254 vor fi modificate substanțial, deoarece evidența primară va fi deja condusă într-un sistem informatic unic, unde se vor regăsi în format electronic, structurat, majoritatea informațiilor care astăzi se completează în formularistica respectivă pentru a fi culese și introduse apoi într-o evidență electronică. Păstrarea modului actual de lucru ar implica redundanța activităților de gestiune a fișelor, prin generarea lor din sistemul informatic și culegerea datelor în interfața RICC. Ca atare, această componentă manuală a procesului AS IS este înlocuită de o componentă automatizată de generare a actelor de evidență primară din sistemul informatic și în final de transmitere automată a datelor în RICC.

N.B. Această modificare nu înseamnă dispariția RICC în sine, datorită faptului că în RICC sunt introduse și spețe care nu sunt gestionate în cadrul MAI (de exemplu direct de Procuratura) iar RICC este o evidență republicană, nu departamentală.

2. Toate actele procesuale și documentele vor putea fi generate din sistemul informatic, pe baza completării template-urilor (formularelor) în mod automat cu datele gestionate la nivelul dosarului electronic și ulterior, acolo unde va fi cazul, completarea în documentul electronic de către utilizator a secțiunilor care nu pot fi populate automat cu date structurate gestionate în dosarul electronic. Ca atare, aceste acte și documente în formă letrică vor fi *output* al sistemului informatic, pentru a putea fi apoi utilizate în procesul penal conform reglementărilor din CPP. De exemplu, ordonanța de începere a urmăririi penale, procesul-verbal de reținere, ordonanța de aducere silită, raportul cu propunerea de punere sub învinuire sau de terminare a urmăririi penale vor fi generată de către ofițerul de urmărire penală din sistemul informatic, pe baza unui flux de emitere acte procesuale și documente.

N.B. Această modificare de stil de lucru nu va însemna pe de altă parte dispariția totală a documentelor generate inițial în formă letrică. Atât datorită faptului că vor exista dosare deja gestionate pe stilul actual de lucru care vor fi preluate în noul sistem, cât și datorită faptului că anumite documente sunt generate în afara MAI (de exemplu de procuror), vor exista în continuare documente în formă letrică care vor fi doar luate în evidență (sub forma metadatelor și eventual a imaginii scanate) în dosarul electronic.

3. Evidențele de tip registru vor fi la rândul lor un rezultat al gestiunii informației și nu un scop în sine, așa cum este acum organizată activitatea. De exemplu, Registrul 1 va fi un output de tip raport, nu un document care se completează de către un responsabil. Evident, cel puțin până la modificarea reglementărilor (în special a Ord. 254) registrele în formă letrică vor continua să existe și să fie completate manual, conform modului de lucru actual. însă sistemul informatic trebuie să aibă de la început capabilitatea de a genera automat sau de a permite vizualizarea datelor sub forma registrelor electronice care vor respecta structura și regulile logice ale registrelor actuale.

4. Activitățile de avizare/aprobare realizate de către conducătorii organelor de urmărire penală vor fi transferate în mediu informatic, sub formă de faze în ciclul de viață al actelor procesuale și documentelor simple, în măsură în care reglementările vor fi modificate pentru a permite avizarea în formă electronică.

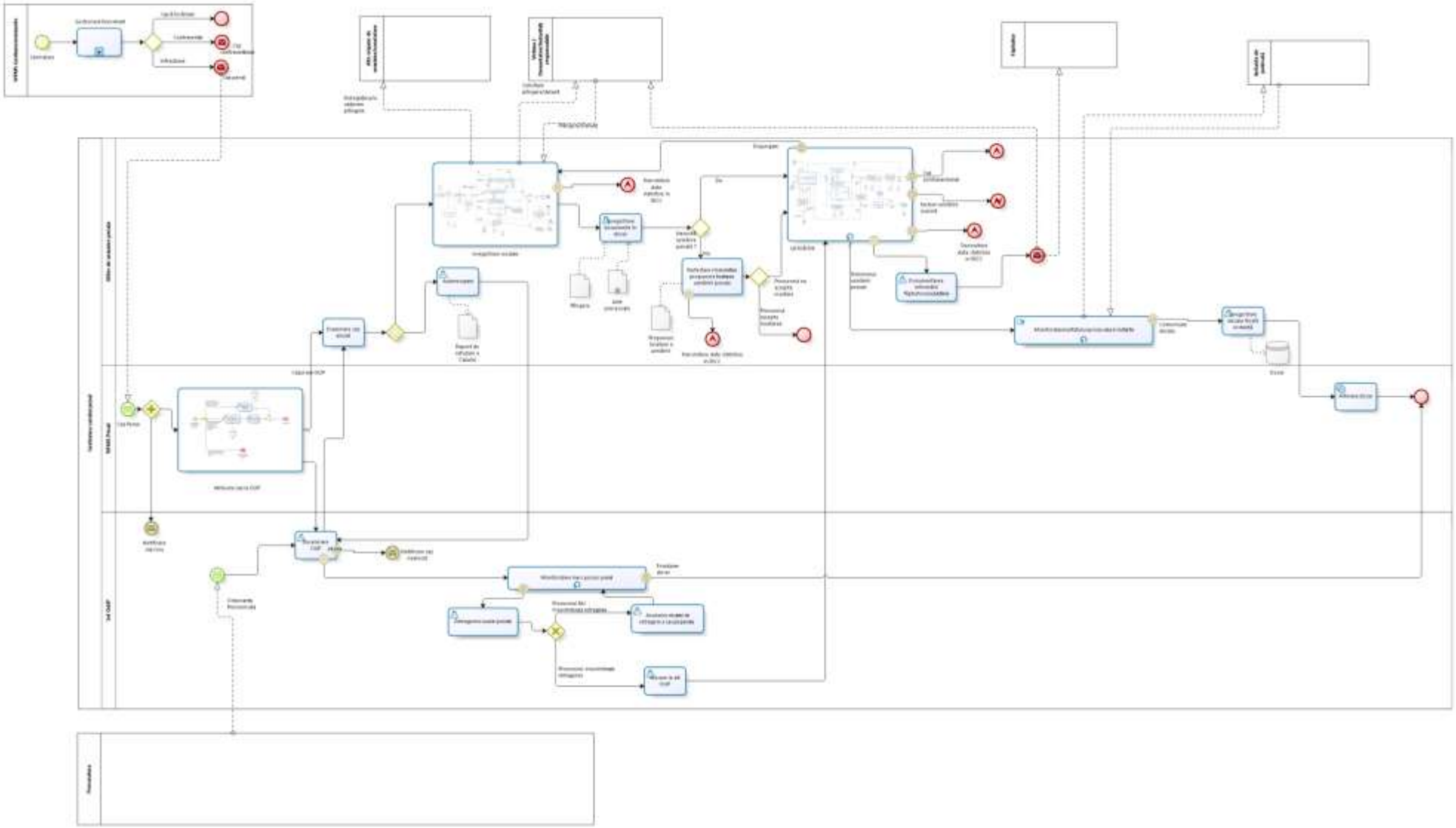
Sistemul informatic trebuie să aibă capabilitatea de a implementa acest tip de activitate, chiar dacă în perioada inițială de utilizare a sistemului avizările vor fi făcute și în formă letrică.

Diagramele de mai jos reprezintă procesele de business rezultate în urma implementării sistemului informatic cerut. Prima diagramă este o vedere generală asupra procesului, iar următoarele descriu cele mai importante sub-procese ale acestuia:

Conform și celor menționate în diagrama de arhitectură TIC, business-proces-ul de gestiunea a cauzelor penale este precedat de un business-proces care va fi materializat într-un modul WFMS distinct care va unifica gestiunea evenimentelor (notat cu **WFMS Gestiune Evenimente** în diagramă), indiferent de natura faptelor semnalate în evenimente, ca atare inclusiv când aceste fapte sunt de natură penală. în acest modul vor fi gestionate atât evenimentele în derulare (situații operative) cât și evenimentele semnalate post-factum (ca atare și prin intermediul formelor scrise de semnalare, care pot fi clasificate ulterior ca fiind sesizări de infracțiuni).

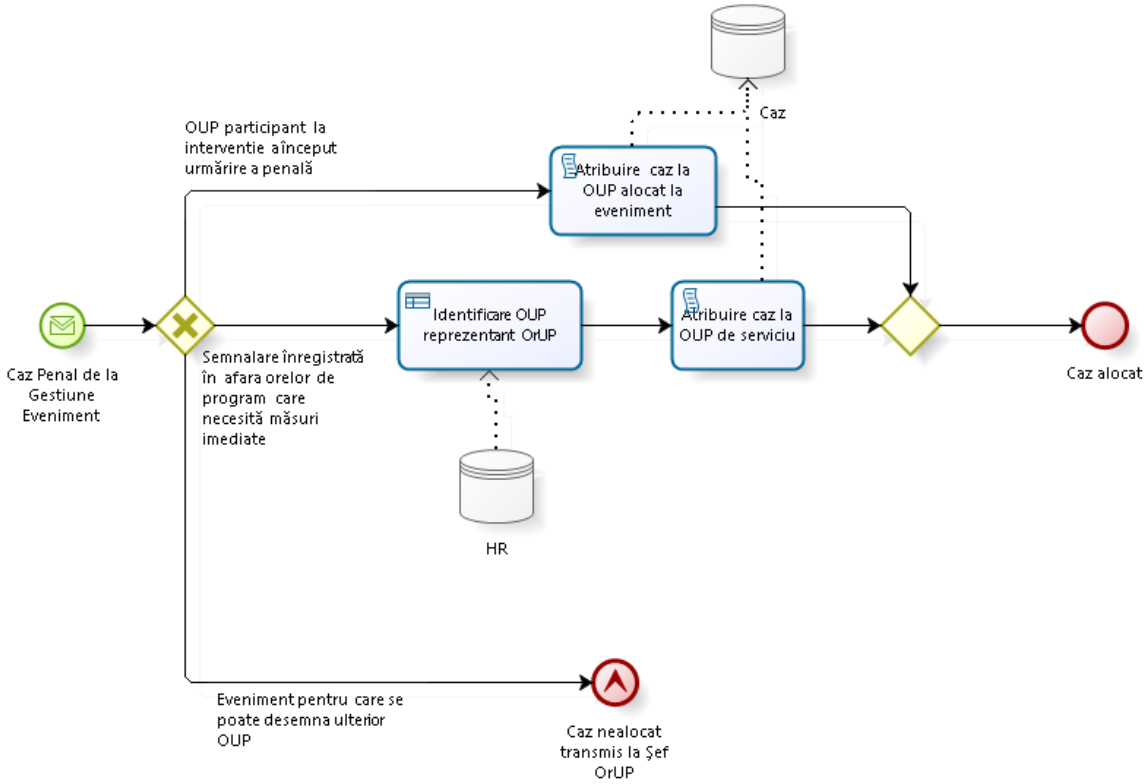
Conform celor modelate în diagrama de mai sus, atunci când în cadrul gestiunii evenimentelor sunt semnalate organelor MAI fapte de natură penală, la finalul acestui *business-proces* se inițiază propriu-zis *business-proces-ul* de Gestiune a cauzelor penale. Ca atare, și implementarea TO BE va urmări să deruleze separat fază premergătoare înregistrării sesizării, la fel ca în cazul proceselor AS IS.

În diagrama sunt figurate ca output-uri de tip mesaj la diferite faze actele de evidență primară (așa numitele fișe statistice) care sunt transmise către RICC, datele respective având ca destinație finală evidența electronică RICC, motiv pentru care pentru aceste evenimente de tip mesaj s-a marcat finalizarea de tip escaladare, cu descrierea "Transmitere date statistice în RICC". în practică, sistemul informatic WFMS ce urmează a fi implementat trebuie să aibă capabilități multiple pentru a răspunde acestei cerințe. Având în vedere prevederile Ordinului 254, care presupun asumarea răspunderii de către OUP și de către conducătorul organului de urmărire penală cu privire la date înscrise în actele de evidență primară (fișele/formele 1, 1.1, 2.0, 2.1, 2.2 și 2.7) prin intermediul semnăturii pe documentul analog, se estimează că cel puțin în prima perioadă a utilizării noului sistem informatic, aceste acte vor continua să fie tipărite și semnate. Ca atare, sistemul va trebui să aibă capabilitatea de a genera aceste acte pe bază de șabloane, prin extragerea automată a datelor structurate din dosarul electronic gestionat de OUP. Șabloanele vor permite și editarea manuală de către OUP a anumitor secțiuni din formular care nu pot fi completate în mod automat din datele structurate. în același timp, pentru a fi pregătit pentru situația în care reglementările vor fi modificate pentru a acorda semnăturii electronice a OUP și a șefului OrUP aceeași valoare legală ca semnăturii analogice, sistemul va trebui să permită utilizatorilor să semneze electronic aceste acte și să le salveze în formă electronică autentică. De asemenea, pentru a permite implementarea ulterioară a unui proiect de interoperabilitate cu RICC, sistemul WFMS va trebui să aibă interfețe de interoperabilitate (de tip web service) care să permită transmiterea automatizată a actelor de evidență primară în formă electronică și autentică, inclusiv a seturilor de date. în acest mod, se va permite în final optimizarea întregului flux informațional și evitarea redundanței în culegerea de date electronice în cele două sisteme. Specificațiile detaliate privind implementarea acestor cerințe vor fi elaborate în momentul derulării implementării sistemului, în funcție și de evoluția reglemen-



tărilor pe acest subiect pentru a valorifica potențialul gestiunii informației în mediu electronic. în diagramele detaliate de sub-proces, aspectele legate de generarea actelor de evidență primară și transmiterea către RICC a datelor statistice primare sunt evidențiate de asemenea la un nivel mai mare de detaliere, indicându-se și activitățile care au ca rezultat aceste out-put-uri.

Primul sub-proces care este detaliat în modelarea TO BE este **Atribuire caz la OUP** (Ofițer de Urmărire Penală), conform următoarei logici:



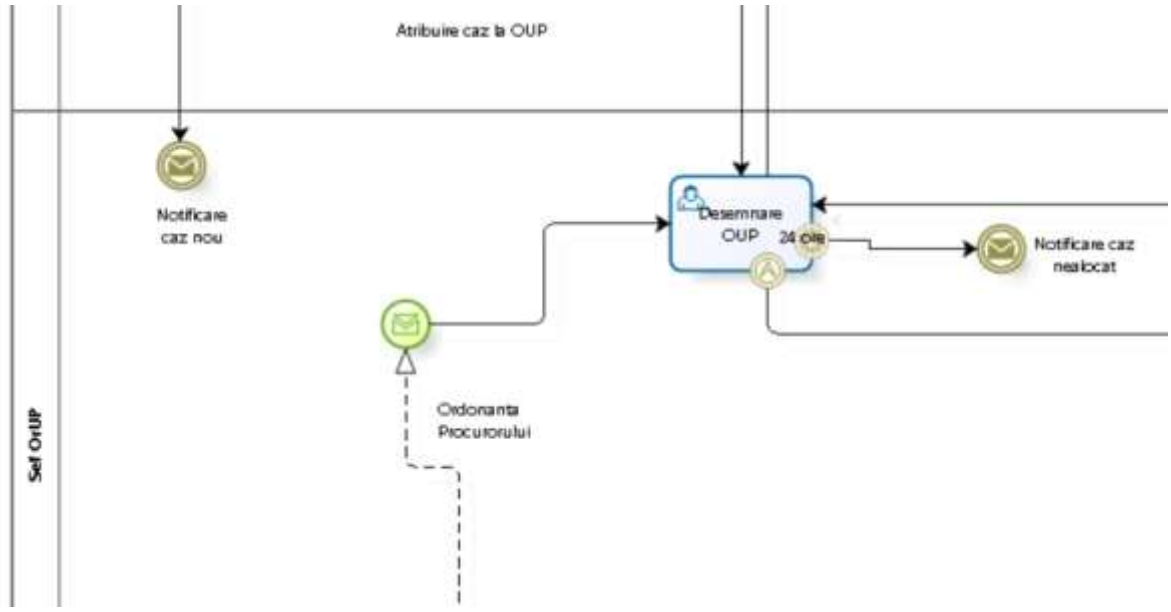
Astfel, în sub-procesul de alocare a OUP se vor executa mai multe scenarii, care sunt dependente de modul în care a fost gestionat evenimentul, de natura actelor procesuale întocmite deja la fața locului și de structura de conducere a unității MAI la momentul înregistrării semnalării și care vor avea două rezultate posibile:

A) Dacă ofițerul de UP care a intervenit la fața locului (în cadrul unei intervenții la fața locului la un eveniment de către grupa operativă) sau a fost de serviciu la unitate și a preluat sesizarea a început deja urmărirea penală (în situații în care luarea măsurilor nu poate fi amânată pentru ziua următoare), ofițerul respectiv devine astfel automat și ofițerul de urmărire penală responsabil de caz (în sensul prevăzut în C.P.P. Art. 57), fără a mai fi nevoie de o repartizare de către Șeful Organului de urmărire penală.

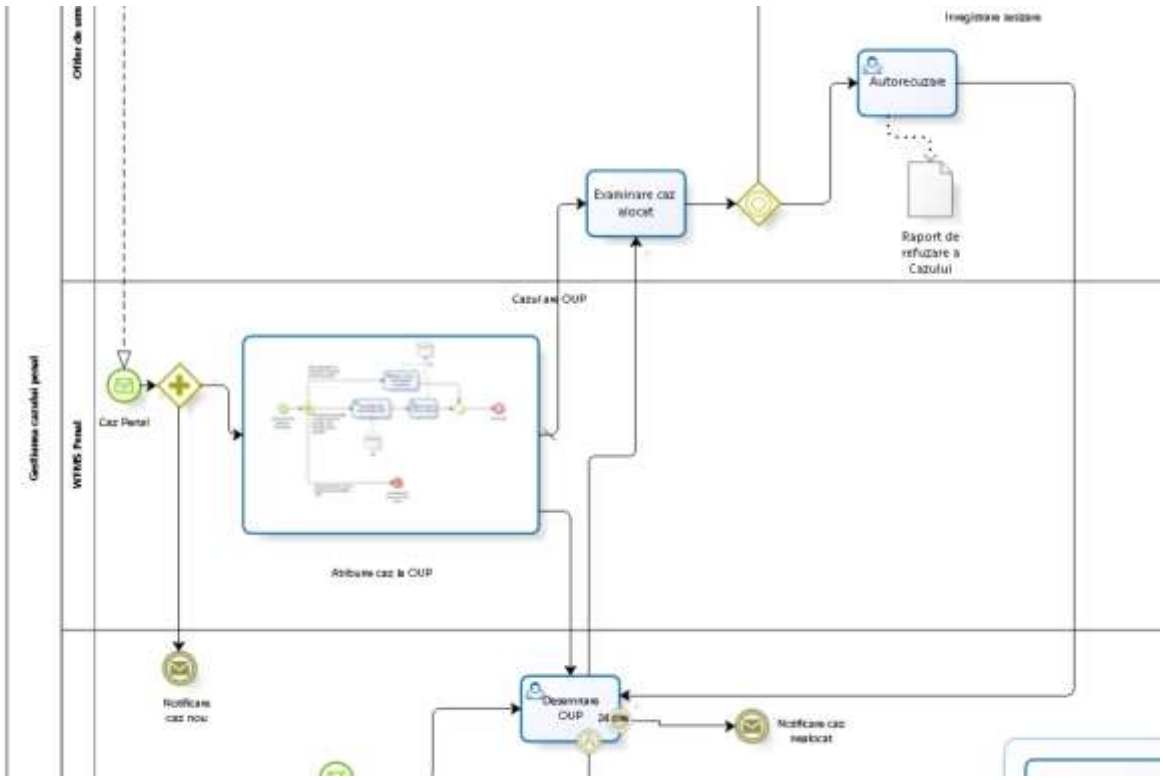
B) Dacă procesul penal este încă în faza de sesizare, și nu au fost încă întocmite acte de către un ofițer de urmărire penală ci doar de către organe de constatare sau doar au fost făcute înregistrări la secretariate (cancelarii) ale unității, cauza penală ajunge la Șeful Organului de urmărire penală în vederea desemnării de către acesta ofițerului de urmărire penală responsabil de cauză. Acest scenariu este marcat în graf-ul de mai sus prin condiția "Eveniment pentru care se poate desemna ulterior OUP" și pe această ramură sub-procesul se finalizează prin trimiterea cazului la șeful Organului de urmărire penală fără ca acest caz să aibă alocat un ofițer de urmărire penală.

în scenariul B) cauza penală ajunge pe flux la Șeful Organului de urmărire penală, care trebuie să o atribuie

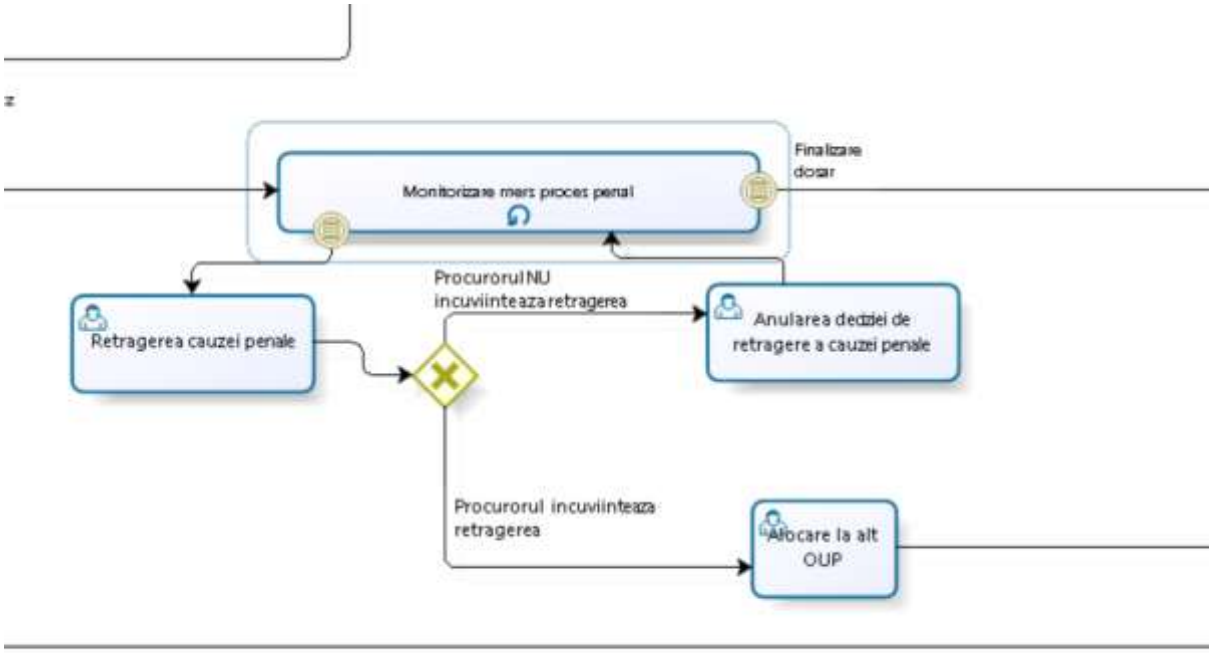
în mod explicit unui ofițer responsabil. Tot în acest scenariu ajunge fluxul și dacă o cauză a fost repartizată organului de urmărire prin ordonanța procurorului de stabilire a competenței sau dacă procurorul emite o ordonanță în baza Art. 4 al. 4 legea 333/noiembrie 2006 prin care adoptă propunerea includerii în grupul de urmărire penală a unor ofițeri care nu sunt de urmărire penala, dar care temporar primesc statut de OUP. Aceste situații sunt reprezentate în graficul de nivel înalt prin extrasul următor, acțiunea de alocare a unui ofițer de urmărire penală de către Șeful Organului de urmărire penală fiind " Desemnare OUP":



Există posibilitatea ca în anumite situații (indisponibilitate, incompatibilități) ofițerul de urmărire penală să se autorecuze, în baza unui raport de refuzare a cazului. Dosarul ajunge iar la Șeful Organului de urmărire penală. Șeful ia act de autorecuzare si schimba OUP. Schimbarea se poate întâmpla in aceste condiții în situația in care încă nu a început urmărirea penală (ne aflam in cele 30 de zile in care încă nu a început urmărirea penală). Această situație este reprezentată în proces după cum urmează:



Pe de altă parte în logica de proces există și scenariul retragerii cazului de către Șeful Organului de urmărire penală, reprezentat în diagramă prin secțiunea de mai jos:



Retragerea poate fi făcută doar în anumite condiții prevăzute în lege (reprezentate în diagramă prin eveniment de tip condiție care poate apărea în timpul monitorizării de către Șef a procesului penal). însă această decizie a șefului poate fi anulată de către Procuror (în diagramă este reprezentată această situație pe ramura " Procurorul NU încuviințează retragerea", caz în care practic decizia este anulată și OUP rămâne responsabil de cauza penală respectivă. Dacă Procurorul încuviințează retragerea, șeful execută acțiunea de alocare la alt OUP care va continua cu urmărirea penală din punctul în care a ajuns sub responsabilitatea ofițerului anterior.

Ulterior alocării inițiale a ofițerului de urmărire penală, un alt sub-proces important este cel de înregistrare a sesizării, conform prevederilor CPP, conform logicii din diagrama de mai jos. Sunt trei *out-put-uri* importante în această fază a procesului de lucru: pe de o parte sesizarea conformă cu CPP (cu cazul particular când aceasta este chiar documentul inițial depus de petiționar în cazul în care au fost respectate toate condițiile formale pentru o sesizare a faptelor penale sau cu situația mai răspândită când sesizarea este perfectată de către ofițerul de urmărire penală, conform cerințelor legale), apoi înregistrarea sesizării în registrul RI de evidență a sesizărilor de fapte penale, conform prevederilor legale privind această evidență și în cele din urmă actele de evidență primară prevăzute în Ord. 254, care au ca finalitate realizarea unei evidențe republicane a infracțiunilor prin intermediul bazei de date RICC. în procesul TO-BE, registrul RI este generat prin înregistrări electronice, realizate chiar de către Ofițerul de urmărire penală responsabil de cauza penală respectivă, odată ce sunt îndeplinite toate condițiile pentru a avea o sesizare de fapte penale în accepțiunea CPP. La fel, actele de evidență primară sunt în primul rând electronice, forma letrică (analogă) a acestora fiind de fapt un output din evidența electronică care va subzista cel mult până la modificarea Ord. 254 pentru a permite asumarea datelor din evidența primară prin intermediul semnăturii electronice. în diagramă, acest

aspect este reprezentat printr-o activitate specifică, denumită **Generarea și semnarea actelor de evidență primară (fișele statistice),** care se execută la finalul subprocesului și care are ca *output* atât actele/ formularele propriu-zise (prin generarea lor la comandă, pe bază de șabloane populate cu date din dosarul electronic al cauzei penale și acolo unde este cazul completate cu secțiuni introduse manual de către OUP), pentru a fi semnate de către OUP și Șeful OrUP, cât și mesaj electronic (pachet de date) care se transmite prin interfețe electronice automate în RICC:

în diagrama acestui sub-proces sunt reprezentate mai multe scenarii posibile de înregistrare a sesizării:

A) Atunci când semnalarea evenimentului este conformă cu cerințele CPP privind elementele care trebuie formalizate într-un denunț/plângere/autodenunț, se înregistrează sesizarea pe baza acesteia, direct.

B) Atunci când semnalarea faptelor de natură penală nu a întrunit elementele obligatorii ale unei sesizări, Ofițerul de urmărire penală face demersurile necesare pentru a prelua de la semnalantul inițial o sesizare conformă, materializată prin PV de preluare sesizare iar înregistrarea sesizării se va face pe baza acestui document formal.

Pentru a reprezenta această logică, diagrama de proces include un nod decizional de tip "Exclusive Gateway" în care OUP evaluează răspunsul la întrebarea " Sesizare conformă art. 262-264 CPP ?" și pe ramura cu "DA" nu mai întocmește un alt document ci continuă cu înregistrarea sesizării în R1 în timp ce pe ramura cu "NU" realizează acțiunile de preluare/perfectare a sesizării conforme și abia apoi continuă cu înregistrarea sesizării în R1.

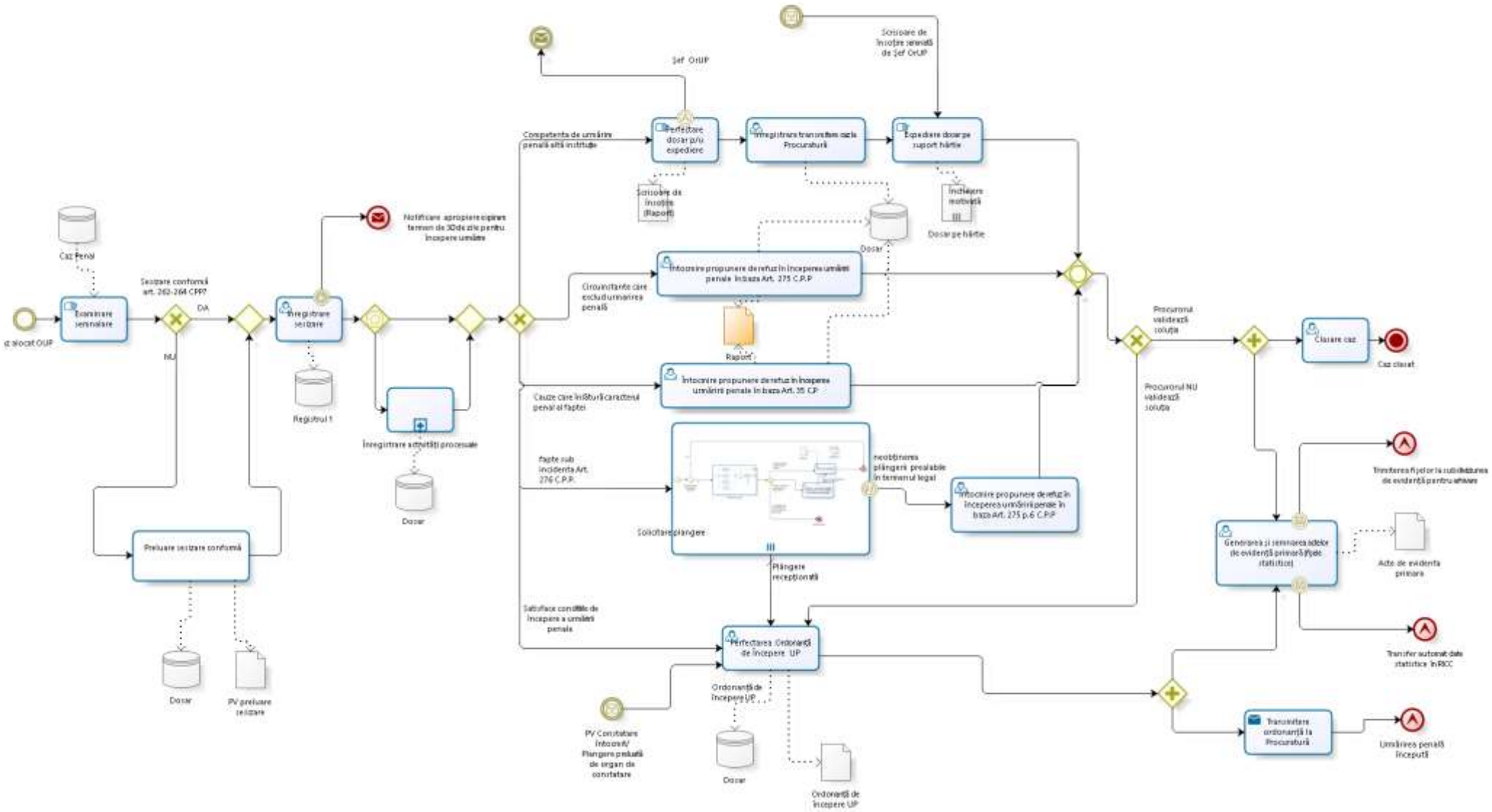
Prin înregistrarea sesizării este declanșat practic procesul penal iar ofițerul de urmărire penală alocat la caz este cel care face următorii pași necesari în procesul de business, în funcție de speță.

Având în vedere că din momentul înregistrării sesizării începe să decurgă intervalul de 30 de zile în care se poate face începerea urmăririi penale, diagrama prezintă un eveniment de tip "timp" prin care se reprezintă automat în sistemul informatic faptul că se apropie termenul respectiv. Modalitatea de notificare, intervalul de timp după înregistrarea sesizării la care va fi generată notificarea și alte asemenea elemente vor fi itemi de configurare ai soluției informatice conform specificațiilor finale care vor fi definite în proiectul de implementare.

Inclusiv începând din această fază, Ofițerul de urmărire penală poate întocmi diverse acte procesuale, după cum consideră necesar în cauză, în baza in baza art. 1 alin. 3 si art. 279 al. 1 CPP, acte pe care le înregistrează în Dosarul penal electronic, conform diagramei, prin activitatea reprezentată ca sub-proces "înregistrare activități procesuale".

Ulterior înregistrării sesizării și constituirii dosarului penal, OUP trebuie să rezoluționeze dacă se începe sau nu urmărirea penală, în funcție de situația specifică din cauza respectivă, în diagramă sunt reprezentate următoarele scenarii posibile:

A) OUP constată ca organul de urmărire penală pe care îl reprezintă nu are competența de urmărire penală pentru faptele sesizate, propune declinarea competenței și transmite cazul penal către Procuratură, pentru alocarea la alt Organ de urmărire penală.

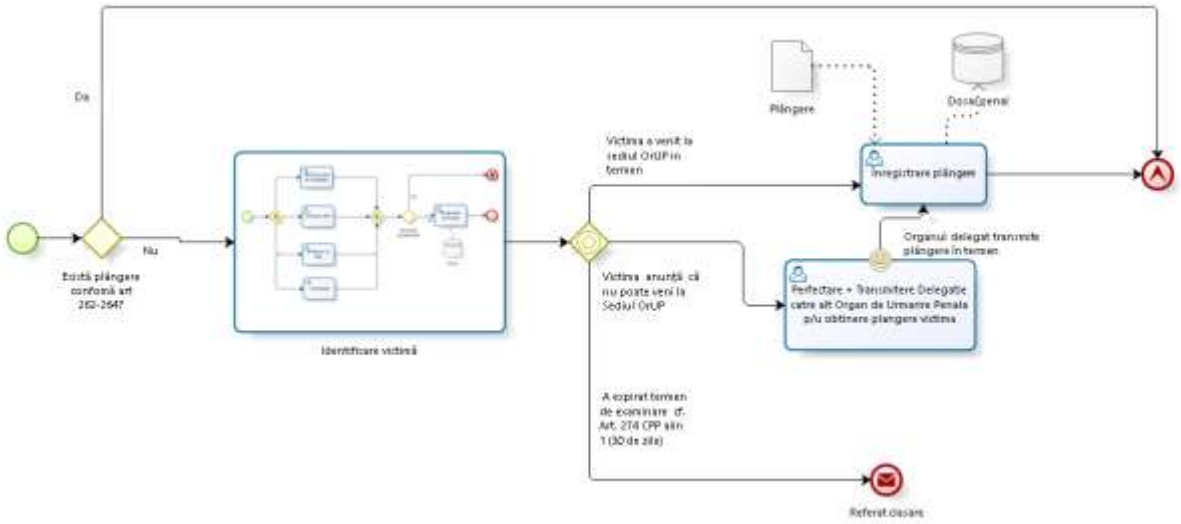

Caz Penal
Sesizare conformă art. 262-264 CPP?
DA
NU
Examinare sesizare
Preluare sesizare conformă
Dosar
PV preluare sesizare
Înregistrare sesizare
Registrul 1
Notificare apropiere expirare termen de 30de zile pentru începere urmărire
Înregistrare activități procesuale
Dosar
Competența de urmărire penală altă instituție
Șef OUP
Perfectare dosar p/u expediere
Înregistrare transmitere către Procuratură
Expediere dosar pe suport hârtie
Scrisoare de înaintare (Raport)
Dosar
Închidere motivată
Dosar pe hârtie
Scrisoare de înaintare semnată de Șef OUP
Întocmire propunere de refuz în începerea urmăririi penale în baza Art. 275 C.P.P
Raport
Circumstanțe care exclud urmărirea penală
Întocmire propunere de refuz în începerea urmăririi penale în baza Art. 35 C.P.
Cauze care înlătură caracterul penal al faptei
Fapte sub incidența Art. 276 C.P.P.
Solicitare plângere
neobținerea plângerii prealabile în terminul legal
Întocmire propunere de refuz în începerea urmăririi penale în baza Art. 275 p.6 C.P.P
Plângere recepționată
Satisface condițiile de începere a urmăririi penale
Perfectarea Ordonanță de începere UP
Ordonanță de începere UP
Dosar
Ordonanță de începere UP
PV Constatare întocmirii/ Plângere preluată de organ de constatare
Procurorul validează soluția
Procurorul NU validează soluția
Clasare caz
Caz clarat
Generarea și semnarea adeze de evidență primară/fișele statistice)
Acte de evidență primară
Transferarea fișelor la subdiviziunea de evidență pentru urmărire
Transfer automat date statistice în RIEC
Transmitere ordonanță la Procuratură
Urmăriree penală începută

B) OUP constată că faptele sesizate nu au avut loc sau nu au caracter ilicit sau nu întrunesc sub o altă formă prevederile Codului Penal pentru a fi încadrate ca infracțiuni (inclusiv în situațiile prevăzute la Art. 35 CP.), sau constată circumstanțe care exclud urmărirea penală (conform Art. 275 C.P.P) acesta va consemna această . decizie și va genera din sistem Ordonanța de neîncepere a urmăririi penale.

C) OUP constată că au fost sesizate fapte pentru care este obligatorie plângerea prealabilă a victimei conform Art. 276 C.P.P și pentru că persoana care a depus sesizarea care a fost înregistrată în R1 nu este victima va proceda la obținerea acestei plângeri, sub-proces descris în diagrama de mai jos. Ramura nu se execută dacă această plângere a victimei fost deja obținută în fazele anterioare (i.e. depunerea sesizării), caz în care se execută ramura D descrisă în continuare.

D) OUP constată că poate începe urmărirea penală, generează din sistem Ordonanța de începere a urmăririi penale și o transmite procurorului (ramura aceasta a procesului se poate executa inclusiv pentru scenarii în care este obligatorie plângerea victimei dar ea există deja din faza depunerea sesizării și ca atare nu mai este necesară execuția ramurii C descrisă mai sus).

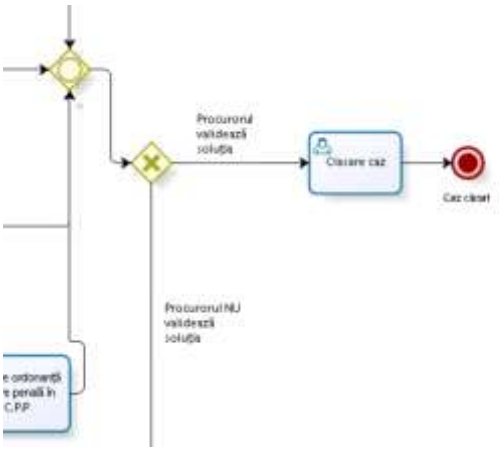
Pentru situațiile în care este plângerea este obligatorie (cf. art. 263 alin. (2) și 276 CPP) este figurat un sub-proces dedicat, conform diagramei de mai jos:



Conform diagramei de mai sus, primul gateway presupune evaluarea situație din punctul de vedere al conformității prevederilor art. 262-264. Dacă din faze anterioare ale procesului penal (mai precis, din faza de sesizare) există deja o plângere a victimei care este în formă scrisă și conformă cu cerințele formale privind sesizarea faptelor penale, atunci practic această ramură nu se mai execută, fiind îndeplinite condițiile privind existența plângerii prealabile pentru a putea începe urmărirea penală a faptelor respective. Dacă din fazele anterioare ale procesului nu există o astfel de plângere, se execută activitățile de identificare a victimei și în funcție de situație (reprezentată în diagramă prin trei ramuri) se încearcă obținerea plângerii fie direct de către OUP fie prin intermediul unei delegări, dacă victima nu poate intra în contact direct cu OUP (de exemplu se află în altă localitate și nu este deplasabilă). în oricare din cele două situații, rezultatul este plângerea înregistrată. Dacă însă acest rezultat nu este obținut în termenul maxim prevăzut de 30 de zile de la înregistrarea sesizării în R1, urmărirea penală nu mai poate fi începută și procesul se finalizează prin clasarea

cauzei, în absența unei plângeri care respectă criteriile obligatorii prevăzute în CPP art 263. Scenariul de bază însă pe aceste spețe este obținerea și înregistrarea plângerii, situație în care se perfectează Ordonanța de începere a urmăririi penale, așa cum a fost indicat în diagrama anterioară.

în ceea ce privește scenariile A și B de mai sus, când OUP propune declinarea sau neînceperea urmăririi penale, există posibilitatea ca Procurorul să încuviințeze soluțiile propuse de OUP, situație în care procesul se finalizează cu clasarea cauzei penale respective:

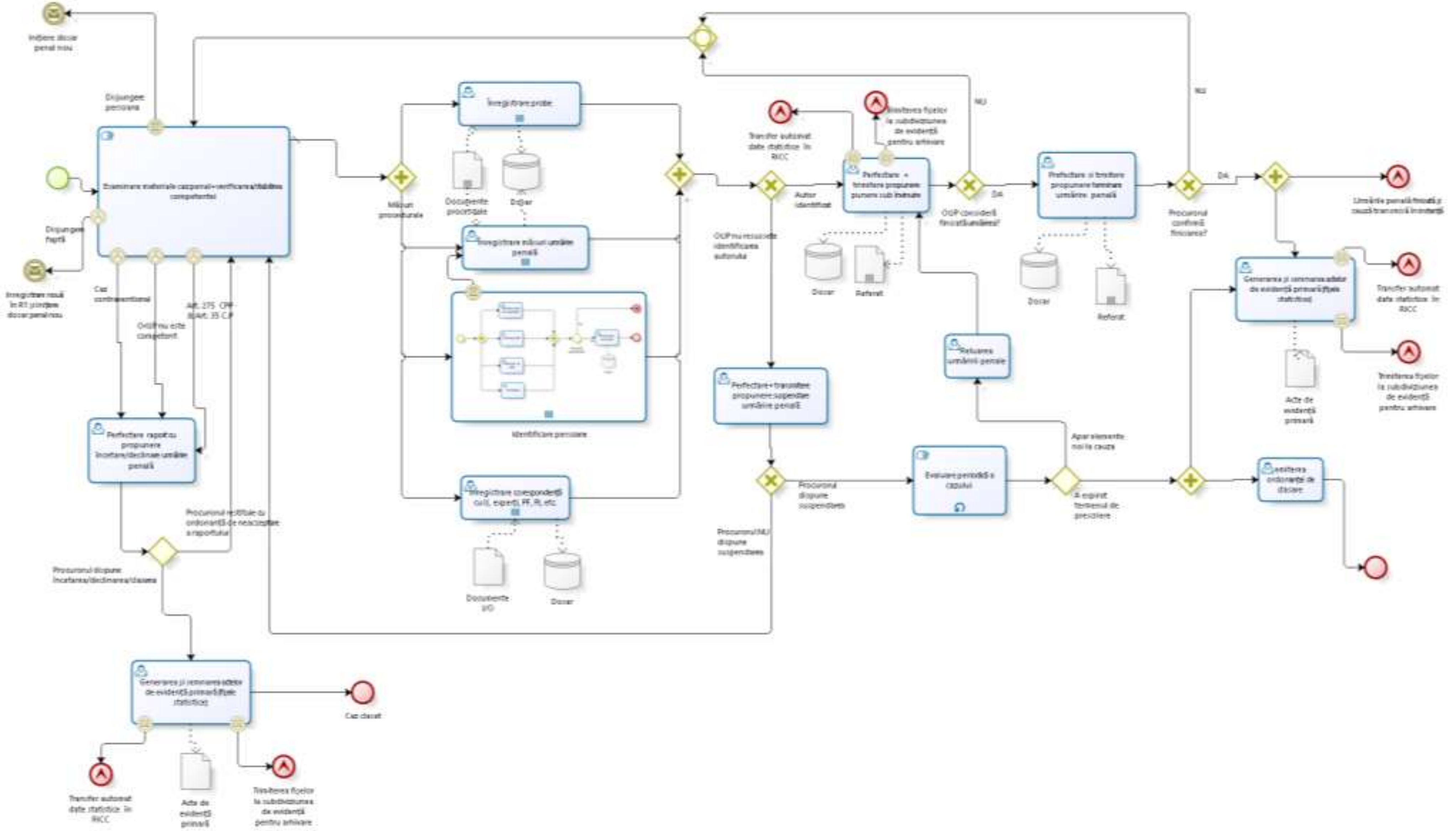


însă există și situația în care Procurorul (sau un superior al lui) să nu încuviințeze soluția de clasare prin neîncepere sau cea de declinare propuse, caz în care fie o restituie organului de urmărire penala cu ordonanța de pornire a urmăririi întocmită chiar de procuror, fie o restituie cu o ordonanță de neacceptare a raportului OUP si indicație pentru pornire cu efectul este ca OUP va emite actul procesual de pornire a urmăririi penale. Mai există și posibilitatea ca Procurorul să dea indicații de efectuare acțiuni de investigații suplimentare (dacă nu au expirat încă cele 30 de zile de la înregistrarea sesizării) pentru a relua apoi același arbore decizional care are ca rezultat fie începerea, fie clasarea.

Odată începută urmărirea penală, business-proces-ul continuă cu o etapă majoră, în care Ofițerul de urmărire penală gestionează dosarul penal, întocmind și înregistrând toate actele procedurale specifice urmăririi penale, conform diagramei de mai jos:

Așa cum rezultă din modelarea de mai sus, scenariul de bază în acest sub-proces constă în înregistrarea tuturor actelor, măsurilor, probelor și documentelor culese și/sau perfectate pe parcursul urmăririi penale până la identificarea tuturor persoanelor implicate, punerea sub învinuire a făptuitorilor, output-ul final fiind referatul cu propunerea de terminare a urmăririi penale. Aceste activități se vor realiza în atâtea iterații câte e nevoie până pe fiecare nod de decizie intermediar se va intra pe scenariul pozitiv, inclusiv în ceea ce privește confirmarea procurorului.

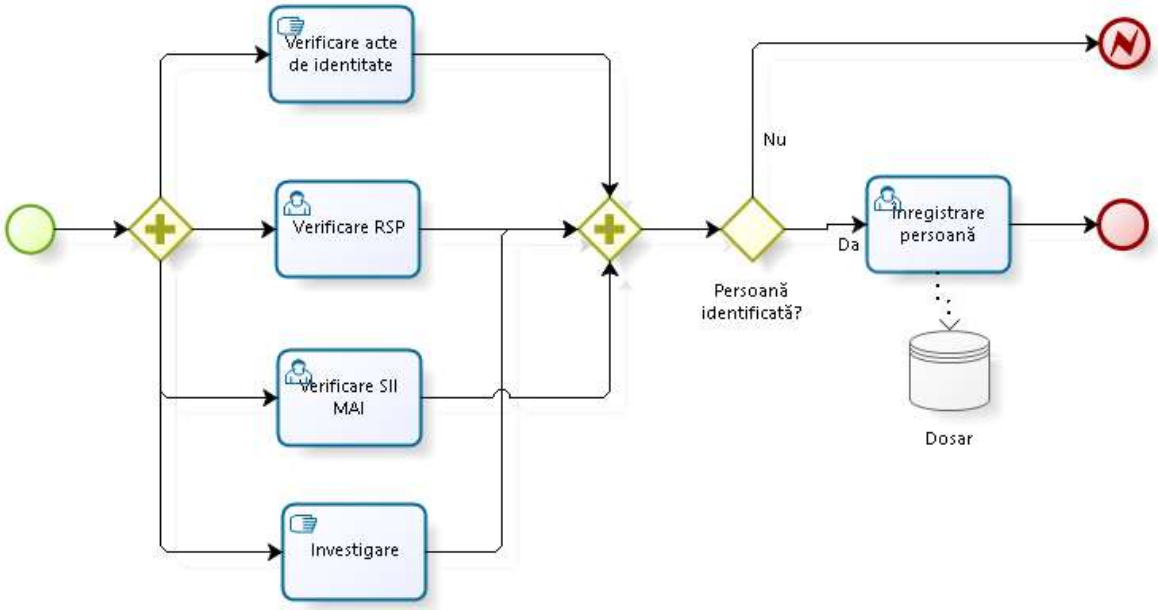
În acest sub-proces sunt posibile și scenariile de excepție, în care în urma parcurgerii unor activități de urmărire, decizia este de încetare a urmăririi penale (inclusiv dacă se constată natura contravențională a faptelor sau dacă se constată circumstanțe care exclud urmărirea penală conform CPP art. 275 sau care înlătură caracterul penal al faptei, conform art. 35 din CP) sau de declinare a competenței către alt organ de urmărire penală, finalizată prin trimiterea dosarului la Procuratură (cu condiția ca Procuratura să nu restituie cu o ordonanță care nu confirmă propunerea ofițerului de urmărire penală, caz în care continuă procesul de urmărire penală de către același ofițer)


Înregistrare probe
Documente procedurale
Dosar
Mijloace procedurale
Înregistrare mijloace de urmărire penală
Identificare persoane
Înregistrare corespondență cu IL, experți, PF, PJ, etc.
Documente I/O
Dosar
Transfer automat date statistice în RICC
Autor identificat
Perfectare și transmitere propunere punere sub învinuire
Dosar
Referat
NU
DA
Perfectare și transmitere propunere terminare urmărire penală
Dosar
Referat
NU
DA
Procurorul confirmă finisarea?
Urmărire penală finisată, cauza transmisă în instanță
Transfer automat date statistice în RICC
Acte de evidență primară
Reluarea urmării penale
Perfectare și transmitere propunere suspendare urmărire penală
Procurorul dispune suspendarea
Evaluare periodică a cazului
Apar elemente noi la cauza
A expirat termenul de prescriere
Emiterea ordonanței de clasare
Procurorul NU dispune suspendarea
Perfectare raport cu propunere încetare/declinare urmărire penală
Art. 275 CPP
Caz contravențional
Procurorul dispune încetarea/declinarea/clasarea
Caz clasat
Transfer automat date statistice în RICC
Acte de evidență primară

Un alt scenariu de excepție important este dat de situația când OUP nu reușește identificarea autorului și propune suspendarea urmăririi penale. De pe această ramură, în funcție și de dispoziția Procurorului care confirmă sau nu confirmă propunerea OUP, procesul se poate suspenda până la reluarea urmăririi sau, după caz, până la expirarea termenului de prescripție (caz în care se finalizează prin clasarea cauzei), sau dacă Procurorul dispune continuarea efectuării de acte de urmărire penală, se întoarce în această fază.

De asemenea, mai sunt posibile și ieșiri din această fază prin ordonanțe de disjungere. în funcție de tipul disjungerii (după faptă sau după persoană) se vor genera doar dosare penale noi sau chiar și înregistrări noi de fapte penale în registrul R1.

Unul dintre sub-procesele care este detaliat în această fază este cel de identificare a persoanei, deoarece rezultatul acestui proces este input în finalizarea etapei prin punerea sub învinuire:



Astfel, toate activitățile se pot derula în paralel, până la obținerea identității reale și certe a persoanei și înregistrarea acesteia, cu participația corespunzătoare în sistemul informatic, în cadrul informațiilor structurate din dosarul electronic.

Sistemul informatic trebuie să prevadă în același timp capabilitățile de a respecta cerințele privind generarea actelor de evidență primară prevăzute în Ord. 254, care au ca finalitate realizarea unei evidențe republicane a infracțiunilor prin intermediul bazei de date RICC. în diferite faze ale sub-procesului de urmărire penală figurat mai sus, ofițerul de urmărire penală responsabil de cauza penală respectivă, trebuie să aibă capabilitatea de a genera actele de evidență primară sunt în primul rând electronice, forma letrică (analogă) a acestora fiind de fapt un output din evidența electronică care va subzista cel mult până la modificarea Ord. 254 pentru a permite asumarea datelor din evidența primară prin intermediul semnăturii electronice. în diagramă, acest aspect este reprezentat printr-o activitate specifică, denumită **Generarea și semnarea actelor de evidență primară (fișele statistice),** care se execută pe diferite ramuri la finalul sub-procesului și care are ca *output* atât actele/formularele propriu-zise (prin generarea lor la comandă, pe bază de șabloane populate cu date din dosarul electronic al cauzei penale și acolo unde este cazul completate cu secțiuni introduse

manual de către OUP), pentru a fi semnate de către OUP și Șeful OrUP, cât și mesaj electronic (pachet de date) care se transmite prin interfețe electronice automate în RICC. De asemenea, acest tip de output-uri este figurat în diagramă și în faza de punere sub învinuire. Pe de altă parte, pentru a permite adaptarea sistemului la orice modificări ulterioare ale procedurilor privind datele statistice, sistemul informatic trebuie să aibă capabilitatea ca prin configurare, acest tip de output-uri să poată fi realizate în orice fază a fluxului de lucru principal,

ȘABLOANELE DOCUMENTELOR DE INTRARE SI IEȘIRE

Următoarele documente tipizate sunt documente de ieșire în diferite faze ale procesului:

1. fișa infracțiunii constatate (forma nr.l) cf. Anexei 2 la Ordinul 121/254.;
2. fișa cu privire la desfășurarea urmăririi penale și alte rezultate ale urmăririi penale (forma nr.1.1); cf. Anexei 2 la Ordinul 121/254.;
3. fișa victimei infracțiunii (forma nr.2.0); cf. Anexei 2 la Ordinul 121/254.;
4. fișa alfabetică a persoanei fizice, care a săvîrșit infracțiunea forma nr.l-pf; cf. Anexei 2 la Ordinul 121/254.;
5. fișa alfabetică a persoanei juridice, care a săvîrșit infracțiunea forma nr.l-pj; cf. Anexei 2 la Ordinul 121/254.;
6. fișa persoanei fizice, care a săvîrșit infracțiunea (forma nr. 2.1) cf. Anexei 2 la Ordinul 121/254;
7. fișa persoanei juridice, care a săvîrșit infracțiunea (forma nr. 2.2); cf. Anexei 2 la Ordinul 121/254.;
8. fișa exteriorului și semnalmentelor persoanei neidentificate, care a săvîrșit infracțiunea (forma nr. 2.7); cf. Anexei 2 la Ordinul 121/254.;

Toate aceste documente vor fi generate de către Ofițerul de urmărire penală în cadrul procesului informatizat. Ele nu vor fi completate în formă letrică, ci vor fi generate din sistemul informatic, pe baza datelor completate în cadrul procesului de lucru. în momentul în care reglementările în vigoare (în special Ordinul 121/254) vor fi modificat/înlocuit pentru a fi corelate cu capabilitățile generate de sistemul informatic, aceste documente nu vor mai fi generate din sistem, conform procesului de business definite pentru "TO BE". Pentru perioada intermediară însă sistemul va trebui să aibă capabilitatea de a genera aceste documente pe baza datelor structurate gestionate în cauza penală.

Al doilea set de documente de tip output în sistemul informatic este constituit din actele generate de către ofițerul de urmărire penală, sau încărcate pe baza actelor primite de la procuror sau de la alte persoane implicate în procesul penal:

1. ordonanța de începere a urmăririi penale,
2. propunerea de neîncepere a urmăririi penale
3. ordonanța de stabilire a termenului urmăririi penale,
4. procesul verbal de autosesizare/constatare
5. procesul verbal de consemnare plângere/denunț/autodenunț
6. ordonanța cu privire la prelungirea termenului urmăririi penale;
7. procesul-verbal de cercetare la fața locului cu anexele respective;
8. ordonanța de recunoaștere în calitate de parte vătămată
9. ordonanța de recunoaștere în calitate de parte civilă,
10. procesul verbale de audiere a părții vătămate
11. procesul verbal de audiere a părții civile;
12. procesul verbal de audiere a martorilor;
13. procesul verbal de audiere a părților civilmente responsabile;

14. dovada de înmânare a citațiilor;
15. ordonanța de aducere silită;
16. procesul-verbal de reținere,
17. ordonanța de aducere silită,
18. raportul cu propunerea de punere sub învinuire;
19. raportul de terminare a urmăririi penale
20. procesul-verbal al confruntărilor
21. procesele-verbale privind verificarea declarațiilor la fața locului,
22. procesul verbal de reconstituire a faptei
23. procesul verbal de efectuare a experimentului;
24. procesul verbal de efectuare a ridicărilor,
25. procesul verbal de efectuare a percheziției
26. procesul verbal de sechestrare a corespondenței,
27. procesul verbal de interceptare și înregistrare a comunicărilor telefonice, sau altor convorbiri, la examinarea obiectelor și documentelor, recunoașterea în calitate și soluțiile cu privire la corpurile delicte, examinarea corporală, prezentarea spre recunoaștere (pe viu, după fotografie), exhumarea cadavrului, și după caz a altor acțiuni procedurale;
28. ordonanța de dispunere a constatărilor tehnico-științifice sau medico-legale,
29. ordonanța și procesul-verbal cu privire ridicarea mostrelor,
30. ordonanța de dispunere a expertizei,
31. procesele-verbale de comunicare părților despre numirea expertizei,
32. raportul de expertiză,
33. procesul-verbal de audiere a expertului,
34. procesul-verbal de notificare a raportului de expertiză, a declarației expertului privind imposibilitatea prezentării concluziei.
35. ordonanța de recunoaștere în calitate de bănuit,
36. procesul-verbal de reținere,
37. ordonanța de aplicare a măsurii preventive,
38. procesul-verbal de comunicare a drepturilor bănuitului și procesul verbal de audiere a acestuia,
39. raportul cu propunerea și ordonanța de punere sub învinuire,
40. procesul-verbal deînmânare și comunicare a drepturilor învinuitului,
41. procesul-verbal de audiere a acestuia,
42. ordonanțele, cu privire la aplicarea, prelungirea, încetarea, înlocuirea, sau revocarea măsurilor preventive;

Toate documentele de mai sus pot fi, în unele scenarii de utilizare, și documente de input în sistem. însă în aceste scenarii, doar imaginea documentului va fi input, datorită faptului că documentul a fost generat inițial în formă letrică și este preluat în dosarul electronic sub formă scanată. Cu toate acestea, si in acest caz, pentru

documentele scanate ca input in sistem, trebuie asociate si metadate/atribute ale documentului care vor fi stocate ca date structurate asociate imaginii documentului respectiv.

NOMENCLATOARE

In cadrul sistemului informatic se vor utiliza următoarele nomenclatoare principale:

1. Nomenclatorul de fapte penale (infracțiuni): va fi structurat conform Codului Penal, pentru fiecare tip de faptă fiind introdusă și referința la încadrarea juridică exactă.
2. Nomenclatorul organizațional MAI, în care vor fi prevăzute toate instituțiile, subdiviziunile care participă la procesele de business, inclusiv relația ierarhică dintre ele. Acest nomenclator este foarte important, deoarece o componentă a logicii de drepturi de acces la datele din dosarele electronice se bazează pe relațiile de ierarhie modelate în acest nomenclator între diferite subdiviziuni;
3. Nomenclatorul de tipuri de sesizări
4. Nomenclatorul de tipuri de participație a persoanei
5. Nomenclatorul de tipuri de implicare a bunului
6. Nomenclatorul de tipuri de persoane
7. Nomenclatorul de tipuri de bunuri
8. Nomenclatorul de tipuri de acte procesuale
9. Nomenclatorul de tipuri de măsuri
10. Nomenclatorul de adrese pentru locații;
11. Nomenclatorul de unități teritoriale

Nomenclatoarele vor fi actualizate periodic de către administratorul sistemului informatic, regula de bază fiind că odată intrat în producție sistemul, înregistrările din nomenclatoare nu sunt șterse, ci doar retrase, pentru a nu mai putea fi folosite în continuare însă pentru a permite vizualizarea înregistrărilor mai vechi din sistemul informatic care conțin referințe la valoare de nomenclator retrasă.

MATRICEA RACI

Pentru procesul de business definit în versiunea TO BE, matricea responsabilităților pe fiecare fază din proces este după cum urmează (în matrice sunt incluse exclusiv acțiunile realizate de actorii de mai jos în sistemul informatic în calitate de utilizatori):

Nr.	Denumire acțiune	OUP	SOrUP	S	P	A	OGUP
1	atribuire (automata) caz la OUP		**A**	-		-	-
2	desemnare OUP		**R**	-		-	-
3	retragerea cauzei penale		**R**	-		-	-
4	anularea deciziei de retragere a cauzei penale		**R**				
5	alocare la alt OUP		**R**	-		-	-
6	autorecuzare	R	**I**	-		-	-
7	înregistrare documente în dosar	R	**A**	-		**I**	**I**
8	perfectare+transmitere propunere încetarea urmăririi penale	R	**A**			**I**	**I**
9	documentarea informării făptuitorului/victimei	R	**A**			**I**	**I**
10	înregistrare decizie finală instanță	R	**A**	-		**I**	**I**
11	înregistrare sesizare	R	**A**	**I**		**I**	-
12	înregistrare activități procesuale	**R**	**A**	**I**		**I**	**I**
13	înregistrare transmitere caz la Procuratură	R	**A**				
14	întocmire propunere ordonanță neîncepere urmărire penală	**R**	**A**	**I**		**I**	**I**
15	perfectarea Ordonanță de începere UP	R	**A**	**I**		**I**	**I**
16	clasare caz	**R**	**A**	**I**		**I**	**I**
17	înregistrare plângere	**R**	**A**	**I**		**I**	**I**
18 .	perfectare + transmitere delegație către alt Organ de Urmărire Penala p/u obținere plângere victima	R	**A**		**I**		
19	Perfectare +propunere încetare/declinare urmărire penală	R	**A**	**I**	**I**		
20	înregistrare probe	R	**A**	-	**I**		
21	înregistrare măsuri urmărire penală	R	**A**		**I**		
22	înregistrare corespondență cu IJ, experți, PF, PJ, etc.	R	**A**				
23	perfectare + transmitere propunere suspendare urmărire penală	R	**A**	**I**	**I**		
24	perfectare + trimitere propunere punere sub învinuire	R	**A**		**I**		
25	perfectare si trimitere propunere terminare urmărire penală	R	**A**	**I**	**I**		
26	reluarea urmăririi penale	**R**	**A**	-	**I**		
27	perfectare referat de clasare	**R**	**A**	-	**I**		
28	verificare RSP	**R**	-	-	-	-	-
29	verificare în MAI	R	-	p	-	-	-
30	înregistrare persoană	R	**A**	**I**		**I**	**I**

Legendă:

***R** - responsible : este actorul în proces care efectuează acțiunea respectivă*

A - accountable: este actorul care se asigură că acțiunea a fost efectuată (verifică sau similar)

C - consulted: este actorul a cărui expertiză/opinie este cerută în luarea unei decizii în cadrul procesului, aprobă sau avizează

I - informed: este actorul în proces are acces la informația generată în activitatea respectivă

OUP - ofițerul de urmărire penală

***SOrUP** - șeful organului de urmărire penală*

S - statist/analist, care este angajat desemnat cu atribuții vizualizare/consultare a datelor din cadrul ST1 si/sau entității în cadrul căreia este instituit organul de urmărire penală

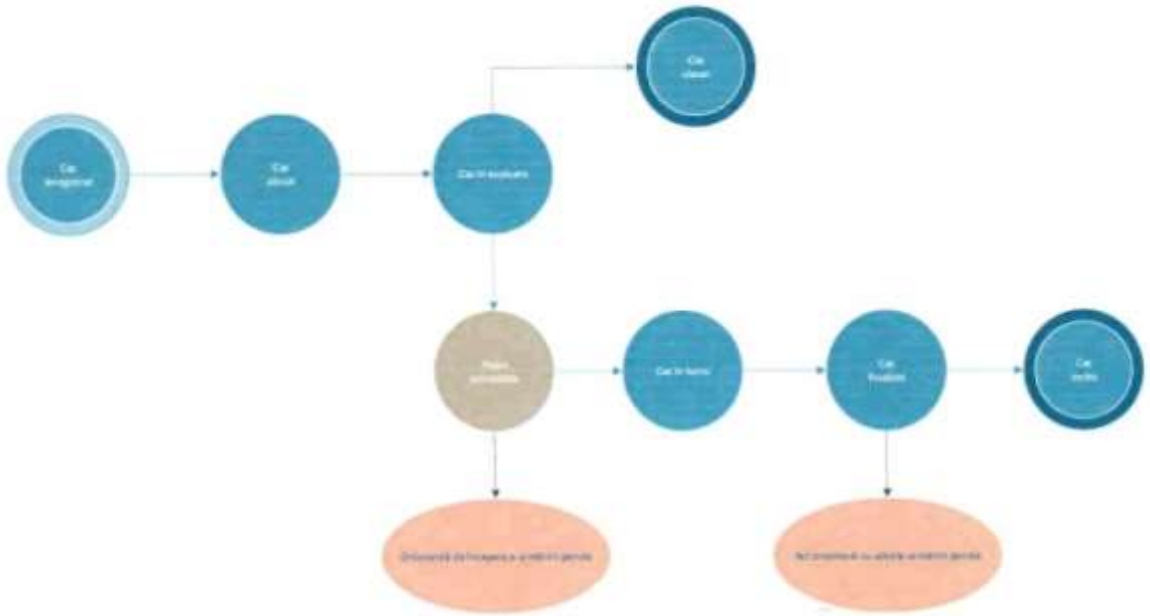
A - analist

P- Procuror (acest actor este introdus în matrice din perspectiva faptului că sistemul MAI va fi interoperabll la un moment dat cu sistemul Procuraturii, caz în care prin intermediul Interfețelor de aplicație procurorul de caz poate avea acces la Informația gestionată în sistemul MAI).

OGUP - Ofițer desemnat membru în grupul de urmărire penală

DIAGRAMA STĂRILOR SI MATRICEA CRUD

Stările aferente cazului penal, rezultate in urma derulării proceselor, precum si relațiile dintre acestea sunt prezentate in diagrama următoare:



In diagrama s-au prezentat stările principale pentru cazul penal si o stare intermediara cu privire la fapta, care este importanta din punct de vedere al derulării fluxului procesului penal pe o ramură sau alta.

Matricea CRUD pentru obiectele bazei de date este prezentata in tabelul următor, pentru fiecare stare identificata a procesului penal.

Legendă:

OUP *- ofițerul de urmărire penală*

OG - ofițerul de gardă, care înregistrează semnalările primite de subdiviziune

SOrUP *- Șeful organului de urmărire penală (inclusiv adjuncții acestuia care îi preiau atribuțiile)*

S - statist (din cadrul STI)

A — analist

SIS *- Șeful ierarhic superior (ie. Director din Direcția Generală de Urmărire Penală din IGP)*

OGUP - Ofițer desemnat membru în grupul de urmărire penală

Nr.	Obiectul din baza de date	Create	Read	Update	Delete
0.1	*Semnalare*	OUP, OG	OUP, OG	OUP, OG	-
Stare: „Caz înregistrat"					
1.1	Eveniment	OUP, OG	SOrUP, OUP, OG	OUP, OG	-
1.2	Fapta	OUP, OG	SOrUP, OUP, OG	OUP, OG	-
1.3	Persoana	OUP, OG	SOrUP, OUP, OG	OUP, OG	-
1.4	ParticipарePersoana	OUP, OG	SOrUP, OUP, OG	OUP, OG	-
1.5	Bun	OUP, OG	SOrUP, OUP, OG	OUP, OG	-
1.6	ImplicareBun	OUP, OG	SOrUP, OUP, OG	OUP, OG	-
Store: „Caz alocat"					
2.1	CauzaPenală	SOrUP	SOrUP, OUP	OUP	-
2.2	OfițerUrmărirePenală	SOrUP,	SOrUP, OUP,	SOrUP	-

Nr.	Obiectul din baza de date	Create	Read	Update	Delete
		WFMS			
2.3	SubunitateMAI	WFMS	SOrUP, OUP	-	-
Stare: „Caz în evaluare"					
3.1	CauzaPenală	OUP,	SOrUP, OUP,	OUP,	-
3.2	Fapta	OUP,	SOrUP, OUP,	OUP,	-
3.3	Persoana	OUP,	SOrUP, OUP,	OUP,	-
3.4	ParticipарePersoana	OUP,	SOrUP, OUP,	OUP,	-
3.5	Bun	OUP,	SOrUP, OUP,	OUP,	-
3.6	ImplicareBun	OUP,	SOrUP, OUP,	OUP,	-
3.7	Măsură	OUP,	SOrUP, OUP,	OUP,	-
3.8	Act/Documente	OUP,	SOrUP, OUP,	OUP,	-
3.9	Dosar	OUP,	SOrUP, OUP,	OUP,	-
Stare: „Fapta constatata"					
4.1	CauzaPenală	OUP,	SOrUP, OUP,	OUP,	-
4.2	Fapta	OUP,	SOrUP. OUP,	OUP,	-
4.3	Persoana	OUP,	SOrUP, OUP,	OUP,	-
4.4	ParticipарePersoana	OUP,	SOrUP, OUP,	OUP,	-
4.5	Bun	OUP,	SOrUP, OUP,	OUP,	-
4.6	ImplicareBun	OUP,	SOrUP, OUP,	OUP,	-
4.7	Măsură	OUP,	SOrUP, OUP,	OUP,	-
4.8	Act/Documente	OUP,	SOrUP, OUP,	OUP,	-
4.9	Dosar	OUP,	SOrUP, OUP,	OUP,	-
Stare: „Caz clasat"					
5.1	Semnalare	-	SOrUP, OUP,	-	-
5.2	CauzaPenală	-	SOrUP, OUP,	-	-
5.3	Fapta	-	SOrUP, OUP,	-	-
5.4	Persoana		SOrUP, OUP,	•	-
5.5	ParticipарePersoana	-	SOrUP, OUP,	-	-
5.6	Bun	-	SOrUP, OUP,	-	-
5.7	ImplicareBun	-	SOrUP, OUP,	-	-
5.8	Măsură	-	SOrUP, OUP,	-	-
5.9	Act/Documente	-	SOrUP, OUP,	-	-
5.10	Dosar	-	SOrUP, OUP,	-	-
Stare: „Caz în lucru"					
6.1	Eveniment	**-**	SOrUP, OUP, SIS	OUP,	-
6.2	Fapta	OUP,	SOrUP, OUP, SIS	OUP,	-
6.3	CauzaPenală	OUP,	SOrUP, OUP, SIS	OUP,	-
6.4	Dosar	OUP,	SOrUP, OUP, SIS	OUP.	-
6.5	Document/Act	OUP,	SOrUP, OUP, SIS	OUP,	-
6.6	Măsura	OUP,	SOrUP, OUP, SIS	OUP,	-
6.7	Persoana	OUP,	SOrUP, OUP, SIS	OUP,	-
6.8	ParticipарePersoana	OUP,	SOrUP, OUP, SIS	OUP,	-
6.9	Bun	OUP.	SOrUP, OUP, SIS	OUP,	-
6.10	ImplicareBun	OUP,	SOrUP, OUP, SIS	OUP,	-
Stare: ..Caz finalizat"					
7.1	Eveniment	-	SOrUP, OUP, OG, A, S, SIS	-	-
7.2	Fapta	-	SOrUP, OUP, OG, A, S, SIS	-	-
7.3	CauzaPenală	-	SOrUP, OUP, A, S, SIS	-	-
7.4	Dosar	-	SOrUP, OUP, A, S, SIS	-	-
7.5	Document/Act	-	SOrUP, OUP, A, S, SIS	-	-

Nr.	Obiectul din baza de date	Create	Read	Update	Delete
7.6	Măsura	-	SOrUP, OUP, A, S, SIS	-	-
7.7	Persoana	-	SOrUP, OUP, A, S, SIS	-	-
7.8	ParticipatePersoana	-	SOrUP, OUP, A, S, SIS	-	-
7.9	Bun	-	SOrUP, OUP, A, S, SIS	*	-
7.10	ImplicareBun		SOrUP, OUP, A, S, SIS	-	-

Notă:
Utilizatorii din categoria SIS au acces temporar și exclusiv la dosarele la care le-a fost acordat accesul în mod explicit, în baza unei ordonanțe a procurorului de caz, cu excepția cazurilor finalizate, unde au acces permanent

Utilizatorii din categoria OGUP au acces exclusiv la documentele procesuale generate de aceștia în cadrul cauzei.

In cadrul sistemului informatic WFMS se vor regăsi doua tipuri de documente:

- Documente generate din WFMS;
- Documente in forma letrica, a căror copie scanata vor fi atașate la dosarul penal electronic;

Sistemul informatic WFMS va permite asocierea unei stări pentru fiecare document in parte. Stările vor putea fi selectate dintr-un nomenclator de stări, disponibil sub forma de lista in cadrul sistemului informatic.

Pentru documentele generate din WFMS stările specifice sunt următoarele:

- "In lucru";
- "Finalizat";
- "Revizuit";
- "înregistrat";
- "Aprobat";
- "Transmis";
- "Anulat";
- "Arhivat";
- "Creat" (pentru situații când documentul este generat automat de sistemul informatic, dar acesta încă nepreluat în lucru de utilizator);
- "la Control" / "în așteptarea răspunsului";

Lista de valori pentru nomencatorul stărilor prezentata anterior nu este completa, aplicația trebuind sa permită adăugarea unor stări suplimentare in lista si/sau ștergerea unor stări existente din lista.

Stările pentru documentele in forma letrica:

- "Copie document";
- "Copie autentica document" - cu mențiunea "conform cu originalul" si semnata digital de persoana (utilizatorul) care autentifica documentul;

MODELUL DE SECURITATE ȘI GESTIUNE ROLURI

Modelul de securitate care trebuie implementat în soluția informatică trebuie să respecte principiul restricționării accesului la informație conform nevoii de cunoaștere și competențelor atribuite oficial. în acest sens, accesul la informațiile gestionate în sistemul informatic trebuie controlat în două scenarii distincte:

1. Accesul la informațiile dintr-o cauză penală specifică.
2. Afișarea rezultatului unei căutări la nivelul întregului set de date (căutări de tip *search).*

În ceea ce privește primul scenariu, accesul la datele dintr-o cauză penală specifică, accesul va fi restricționat prin intersecția a patru logici de drepturi:

Apartenența utilizatorului la un grup sau profil de utilizatori care are acces la tipul de informație respectiv sau la funcționalitatea care permite vizualizarea/editarea informației respective (pentru exemplificare, doi utilizatori care au profiluri diferite pot avea dreptul de a accesa în sistem aceeași cauză penală, însă unul dintre profiluri permite accesul la un set limitat de date și metadate, în timp ce celălalt profil permite accesul la întregul set de date și metadate din cauza penală). Pentru fiecare rol definit se vor stabili permisiuni (drepturi) cu privire la modul de accesare a informației din sistemul informatic. Aceste permisiuni sunt următoarele: creează, citește, modifica si șterge informația, la nivel de obiect din baza de date si la nivel de atribut al obiectului.

- Apartenența ofițerului/agentului care deține contul de utilizator la o subdiviziune a MAI care are drept de acces la cauza penală respectivă. De exemplu, un utilizator care are profilul de conducător de organ de cercetare penală va avea acces exclusiv la cauzele instrumentate de organul respectiv, nu la toate cauzele penale.
- Stadiul curent al cauzei penale. Pentru exemplificare, accesul la anumite date și funcționalități este acordat doar când cauza penală ajunge într-o anumită fază pe flux. Sau, invers, după ce cauza penală trece de o anumită fază (ex. este trimisă în instanță) sunt eliminate restricțiile de accesare a informației din cauza penală.

Rolul pe care îl are ofițerul/agentul în cauza penală (participă sau nu la urmărirea penală în cauza respectivă).

Sistemul informatic cerut trebuie să aibă capabilitatea de a modela și configura toate aceste tipuri de logici de restricționare a accesului la date și funcționalități.

În ceea ce privește limitarea accesului la informațiile accesibile în sistem în baza căutărilor de tip *search,* sistemul trebuie să aibă capabilitate să evalueze următoarele limitări ale accesului pe fiecare cauză penală înregistrată în sistem:

- Nivel maxim de restricționare a accesului: ca rezultat la o căutare în setul de date, indiferent de criteriile folosite, sistemul nu returnează nicio înregistrare a unei cauze penale care are această proprietate activată, chiar dacă ea corespunde criteriilor de căutare, cu excepția situației în care căutarea este efectuată chiar de către titularul informației
- Nivel mediu de restricționare a accesului: ca rezultat la o căutare în setul de date, sistemul va returna doar persoana de contact care deține informații despre entitățile căutate conform criteriilor de căutare folosite de utilizator.

- Nivel redus de restricționare a accesului: ca rezultat la o căutare în setul de date, sistemul va returna doar anumite date nepersonale (de exemplu: mod de operare, locația, perioada) suplimentar cu afișarea titularului de informație
- Acces total: vor fi accesibile spre vizualizare toate elementele conținute în pachetul informațional respectiv.

Sistemul informatic cerut trebuie să aibă capabilitatea de a calcula dinamic proprietățile cauzelor penale din perspectiva afișării la căutare, pe baza metadatelor și atributelor acestora, și să returneze rezultatele căutărilor conform acestor proprietăți.

La definirea utilizatorului in sistemul informatic, acestuia i se vor asocia unul sau mai multe roluri, preluând implicit permisiunile asociate rolului / rolurilor respectiv(e) sub forma unei reuniuni a drepturilor.

Activitatea utilizatorului in sistemul informatic va fi jurnalizata prin intermediul „log-urilor". In cadrul acestor log-uri se vor regăsi minimal următoarele informații:

- Amprenta de timp (data / ora);
- Utilizatorul (contul de utilizator);
- Acțiunea desfășurată (creează / citește / modifica / șterge);
- Obiectul si atributul care a suferit acțiunea;

SPECIFICAȚII PRIVIND CERINȚELE FAȚĂ DE SOLUȚIA INFORMATICĂ DE PLATFORMĂ DESTINATĂ AUTOMATIZĂRII BUSINESS PROCESELOR

Conținut

1 INFORMAȚII GENERALE

1.1 Abordare și metodologie

Prezentele cerințe sunt relevante în contextul acceptării de către Beneficiar a unei soluții de platforma WFMS propuse a fi implementate.

Furnizorul va avea o abordare metodologică asupra întregului proces de implementare și va descrie în cadrul ofertei sale modul în care intenționează să asigure derularea controlată a proiectului.

Metodologia de implementare *va cuprinde:*

✓ Cadrul general de abordare propus pentru implementarea contractului.

✓ Strategia și metodologia de lucru pentru activitatea de dezvoltare/implementare a soluției propuse.

Strategia implementării *va cuprinde obligatoriu două etape distincte*:

1. Implementarea unui prototip funcțional cu funcționalități de bază;

2. Analiză detaliată, proiectarea și implementarea funcționalităților complete, plecând de la prototipul funcțional.

1.2 Strategie de implementare - prototip funcțional

Autoritatea contractantă dorește implementarea unor platforme software a căror viabilitate să fi fost deja confirmată prin utilizarea cu succes pentru managementul unor activități similare la nivelul unor structuri de tipul: ordine publică, management situații de urgență, aplicații militare sau similar. O astfel de abordare reduce substanțial riscul implementării, precum și durata acesteia și permite utilizarea unei experiențe și a unui know-how deja existent în cadrul unor produse utilizate în cadrul unor instituții cu atribuții similare, pentru managementul unor activități similare. De asemenea, se solicită existența unui prototip evolutiv, care să permită echipei de utilizatori cheie ai Autorității contractante accesul la funcționalitățile de bază ale viitorului sistem informatic cât mai devreme în cursul implementării proiectului, urmând ca etapele de analiză detaliată și proiectare a modalității de configurare a sistemului informatic să se poată face plecând de la acest prototip funcțional.

Prototipul funcțional prezentat trebuie să dispună de setul minim de funcționalități solicitate pentru platforma software conform prezentei achiziții, set de funcționalități care va fi verificat în etapa de evaluare a ofertelor tehnice. La momentul organizării sesiunii de verificare a funcționalităților platformei ofertate (ca parte a procesului de evaluare a ofertelor tehnice), ofertanții sunt liberi să aleagă infrastructura hardware pe care vor instala platforma software în scopul demonstrării funcționalităților minimale solicitate, însă infrastructura software va trebui să fie identică cu cea ofertată (aceleași sisteme de operare, același RDBMS, același server software de aplicații – dacă este cazul etc.).

Platforma software standard care va fi ofertată în vederea implementării business proceselor și care va fi verificată ca parte a procesului de evaluare a ofertelor tehnice nu va trebui să fie, la acel moment, personalizată conform cerințelor Beneficiarului, aceasta însemnând că nu trebuie neapărat să aibă interfețele traduse în limba română sau să implementeze funcționalitățile specifice MAI, ci unele similare, conform cerințelor din fișa de date a achiziției. Personalizarea platformei se va realiza ulterior, pe parcursul derulării implementării.

1.3 Cerințe față de arhitectura funcțională a soluției

Arhitectura funcțională propusă de Ofertant trebuie să asigure o abordare de integrare a tuturor datelor într-o bază de date unică și a tuturor fluxurilor operaționale într-un sistem informatic unic. În cazul prezentării unei soluții alternative integrarea se va asigura la nivel de procese și obiecte informaționale. Schimbul de date trebuie asigurat în timp real.

Platforma va asigura posibilitatea federalizării zonelor de lucru (resurse: oameni, echipamente, planuri de acțiuni, etc. În conformitate cu structura organizatorică desconcentrată (cel puțin la nivel de instituții subordonate MAI) cu posibilitatea gestiunii (directe sau prin delegare resurse) centralizate în caz de necesitate (ex. situați de criză).

2 CERINȚE FAȚĂ DE COMPONENTELE FUNCȚIONALE ALE SOLUȚIEI

2.1 Evidență operativă

Orice semnalare , dacă presupune desfășurarea unor activități complexe din partea personalului specializat (lucrător de poliție judiciară, criminalist, analist de informații etc) este transformată într-un Dosar în lucru. Dosarele pot fi generate și independent fără a exista semnalări și pot fi catalogate pe diverse criterii (lucrări penale, lucrări contravenționale, lucrări diverse, comisii rogatorii, delegări etc.). Modulul Gestiune dosare permite lucrul colaborativ între mai mulți utilizatori ai sistemului și versionarea informațiilor din dosare.

Acest modul permite organizarea semnalărilor pe diferite categorii (fapte diverse, penale și contravenționale de ex.) și transferul acestora de la o unitate la alta (fiecare unitate își vede propriul registru).

2.1.1 Evidență registre unitate

Toate semnalările sunt rezoluționate de către managerii unităților la care au fost înregistrate, iar aplicația oferă posibilitatea de completare a datelor privind dispozițiile managerilor și distribuția semnalărilor pe unități, subunități și polițiști.

2.1.2 Evidență lucrări și dosare

Sistemul asigură structurarea informațiilor cu privire la fapte în cadrul unui dosarul. Dosarul asigură conexiunea proceselor de gestiune semnalări și evenimente cu celelalte procese specifice din cadrul MAI, respectiv: gestiunea cauzelor penale, procedura contravențională, abateri disciplinare sau investigații speciale.

Sistemul suportă anexarea la dosar a unul sau mai multe acte/documente. Acest fapt se reflect și la nivel de relații între obiectele informaționale ale sistemului printr-o relație de compunere care unește entitate **Dosar** de entitatea **Document/Act**

2.2 Rapoarte și statistici

Aplicația conține instrumente specializate pentru realizarea de rapoarte standard precum și ad-hoc pe baza informațiilor conținute la nivelul bazelor de date.

Sistemul trebuie să ofere posibilitatea generării de rapoarte predefinite. Un raport predefinit trebuie să fie caracterizat cel puțin prin următoarele:

- numele raportului
- categoria raportului
- fișierul cu macheta asociată raportului
- macheta raportului trebuie să conțină cel puțin:
- una sau mai multe zone de tip text
- una sau mai multe zone cu elemente grafice specifice instituției și contextului (de ex: sigla instituției, alte însemne grafice)
- dimensiunile raportului
- contextul predefinit asociat raportului; contextul trebuie să fie selectabil din lista de contexte predefinite la nivelul sistemului;

Sistemul trebuie să ofere posibilitatea configurării următoarelor categorii de rapoarte predefinite:

- analize predefinite parametrizate pe baza unuia sau mai multor atribute; ex: selectează elementele din [nume_categorie] care au [atribut1] > [valoare1] și [atribut2] < [valoare2];
- analize predefinite parametrizate pe bază de unul sau mai multe atribute și selecție;
- analize predefinite pe bază de selecție;

2.3 Matrice organizațională

Aplicația înregistrează si evidențiază intr-o forma organizata si logica entitățile componente ale organizației si relațiile ierarhice dintre acestea. Acestea pot fi particularizate, denumite, georeferentiate, șterse sau se pot insera noi unități.

Aplicația trebuie să poată defini organigrame pentru diferite categorii de structuri componente ale MAI din domeniul ordinii și siguranței publice (inclusiv cu relații de subordonare intre ele) și să permită actualizarea acestora și păstrarea istoricului modificărilor realizate.

Aplicația asigură mecanisme de gestiune istorică a subordonării componentelor de structură. Se va asigura posibilitatea modificării subordinii. Aplicația va dispune de mecanisme de neadmitere a subordinii multiple.

2.3.1 Gestiune și evidență personal

Aplicația înregistrează si evidențiază intr-o forma organizata si logica personalul component al unei entități din matricea organizaționala. Pentru fiecare se pot introduce elemente particularizate, customizabile referitoare la nume/prenume, grad/funcție, poziție in statul de organizare, indicativ, aptitudini, abilități, disponibilitate –CO, CM, CS-, alte comentarii, poate fi detașat, mutat, indisponibilizat, tura de lucru, etc. Toate aceste operațiuni sunt înregistrate de aplicație intr-un istoric personal. Funcție de personalul disponibil aplicația realizează planificarea lunara, zilnica si echipele.

Înregistrarea resurselor umane presupune întreținerea prin interfețe specializate a structurii instituționale la nivel de organigramă a unității/lor, a posturilor și a personalului alocat pentru fiecare unitate.

Pentru fiecare structură în parte, se va realiza o organigramă la nivel de structură funcțională (serviciu/birou/compartiment independent) unde se păstrează informații despre categoriile de personal (ofițeri/subofițeri/maiștri militari/personal civil etc.)

Aplicația va genera statul de funcții/organizare. Acesta conține succesiunea compartimentelor organizatorice ale unității (începând cu comanda unității), iar pentru fiecare structură în parte din organigramă se vor detalia posturile prevăzute, începând cu funcțiile de conducere și apoi cele de execuție, pe baza unor nomenclatoare de funcții și grade, precum și a nivelelor de ierarhizare a structurilor și a surselor de finanțare pentru fiecare categorie de personal/structură

Aplicația trebuie să permită gestiunea, pentru fiecare post prevăzut în statul de funcții, pe lângă datele specifice statului de funcții și a altor informații (grad nume și prenumele celui ce încadrează postul etc.), precum și aflarea situației încărcării cu personal pe fiecare stat.

Aplicația va asigura evidența unor caracteristici suplimentare cu privire la persoană precum:

- **Istoric alocări**, completare automată a istoricului modificării alocării persoanei respective (unitate, tip activitate, etc.);
- **Indisponibilitate**, în care se pot înregistra manual date referitoare la indisponibilitatea persoanei precum și motivul acestei indisponibilități;
- **Abilități**, în care se pot înregistra manual abilitățile persoanei;
- **Echipamente**, în care se pot adăuga manual/ vizualiza echipamentele din dotarea persoanei.

2.4 Gestiune utilizatori, drepturi și roluri

Sistemul dispune de funcțional care realizează administrarea utilizatorilor, drepturilor și rolurilor la nivelul sistemului, funcție de competența materială și teritorială.

Aplicația este customizata funcție de drepturile si rolurile pe care fiecare tip de utilizator le poate avea in aplicație, astfel încât funcție de dispozițiile interne, un utilizator poate avea de la un singur rol si un singur drept pana la mai multe roluri si drepturi generale.

Sistemul susține roluri de administratori de zone de competențe. Vor fi accesibile minim următoarele nivele de administratori:

- Administrator național
- Administrator local de structură – are acces doar la o ramură din structura definită în Matricea organizațională.

Crearea utilizatorilor în aplicație este realizată de către Administratorul național.

2.5 Gestiune nomenclatoare

Se va pune la dispoziția utilizatorilor facțional de lucru cu nomenclatoarele dinamice pentru toate interfețele sistemului informatic. Lucru cu nomenclatoarele dinamice prevede: crearea, definirea valorilor, modificare, completare liste de valori și atribute.

Sistemul va asigura minim următoarele tipuri de nomenclatoare:

- Nomenclatoare simple de tip listă de valori
- Nomenclatoare de tip ierarhic (arbore)
- Nomenclatoare complexe (ex. nomenclatorul de fapte) care au formular particularizat de editare

Toate nomenclatoarele pot fi editate de către utilizatori desemnați, pe baza unor drepturi alocate de către administratorul principal.

Aplicația va dispune de facțional de căutare în valorile nomenclatorului după mască.

2.5.1 Gestiune nomenclatoare - liste de valori

Aplicația este predefinita cu liste de valori referitoare la personal, echipamente, auto, misiuni, matrice organizaționala, roluri in tura/misiune, tipuri de unități, etc. si este customizabila pentru fiecare dintre acestea, putând fi introduse noi valori, cu atributele aferente.

2.5.2 Gestiune nomenclatoare de tip arbore

Aplicația asigură posibilitatea formării și gestiunii nomenclatoarelor de tip ”arbore”. Spre deosebire de nomenclatoarele simple (listele de valori), cele de tip arbore conțin și relația ”părinte-copil” dintre valorile din nomenclator.

Aplicația va susține nomenclatoare de tip arbore de un număr nelimitat de nivele.

3 SPECIFICAȚII NON-FUNCȚIONALE

3.1 Generalități

Acest capitol stabilește cerințele privind caracteristicile non-funcționale ce trebuie să le dețină softul aplicativ solicitat în cadrul acestei achiziții, precum este expus în continuare.

3.2 Arhitectura de sistem

Arhitectura sistemului trebuie să fie aliniată la necesitățile Beneficiarului ce țin de flexibilitatea și mentenabilitatea acestuia. Beneficiarul optează pentru o arhitectură deschisă, modulară, bazată pe componente interoperabile. Aceste principii trebuie să fie vizibile la toate nivelele arhitecturii sistemului.

3.2.1 Cerințe generale

La acest punct sunt formulate cerințele generale aferente arhitecturii sistemului:

ID	Criteriu	Cerință
CNF.1.	Obligatorie	Arhitectura sistemului trebuie să fie bazată pe standarde deschise.
CNF.2.	Opțională	Arhitectura sistemului trebuie să fie orientată spre servicii (SOA).
CNF.3.	Opțională	Arhitectura sistemului va fi concepută integrat, dezvoltată cu aplicarea celor mai bune practici în domeniu (ex. TOGAF).
CNF.4.	Obligatorie	Arhitectura sistemului va fi de tipul client-server, organizată în cel puțin 3 nivele verticale, divizate clar, astfel încât fiecare nivel superior să depindă doar de nivelul său inferior.

CNF.5.	Opțională	Arhitectura sistemului trebuie să fie adaptată la implementarea și utilizarea în mediile virtualizate.
CNF.6.	Opțională	Caracteristici ale unui sistem cu arhitectură orientată spre implementare în medii virtualizate, sunt: conștient de latență, conștient de căderi de componente, paralelizabil, conștient de utilizarea resurselor.
CNF.7.	Obligatorie	Comunicarea între toate componentele sistemului se va face securizat, utilizând în acest scop interfețele interne ale componentelor sistemului.

3.2.2 Nivelul de prezentare

Nivelul de prezentare este responsabil pentru asigurarea interacțiunii utilizatorului cu funcțiile de business ale sistemului. Acest nivel de arhitectură gestionează modul în care utilizatorii accesează și utilizează funcțiile sistemului atât în scop de business, cât și în scop administrativ.

Sistemul urmează să fie accesat doar de către angajații Beneficiarului, din cadrul rețelei corporative a MAI. Suplimentar, va comunica cu alte sisteme ale MAI prin interfețe externe (cerințe relevante sunt stabilitate la capitolul „Interoperabilitate").

Următoarele sunt cerințele aferente arhitecturii sistemului pentru nivelul de prezentare.

ID	Criteriu	Cerință
CNF.8.	Obligatorie	Soluția software va asigura un mecanism de acces unificat (schimbarea mediului de lucru se face fără re-autentificare).
CNF.9.	Obligatorie	Aplicația client va putea fi rulată în medii de operare standard sau cu configurări minime din partea Beneficiarului (ex. doar soft standard de sistem).
CNF.10.	Obligatorie	Va fi livrată o aplicație client mobilă, ce va permite realizarea unor activități pe teren ale utilizatorilor, de ex. măsurarea energiei electrice.
CNF.11.	Opțională	Nivelul de prezentare nu va implementa reguli de business, cu excepția validării datelor de intrare.
CNF.12.	Obligatorie	Soluția informatică va permite o privire de ansamblu tablou de bord asupra tuturor evenimentelor, adunărilor publice, acțiunilor și misiunilor planificate sau în desfășurare, precum și definirea și vizualizarea unor indicatori statistici cu privire la activitățile gestionate cu ajutorul platformei.
CNF.13.	Obligatorie	Toate interfețele grafice cu utilizatorii ale platformei SI vor fi localizate în limba română și vor folosi o terminologie adaptată mediului și vocabularului profesional al celor care îl vor utiliza. Etichetele câmpurilor vor putea fi programabile, iar dicționarul asociat acestor etichete va fi stabilit împreună cu utilizatorii, în cadrul etapei de analiză din cadrul implementării, în funcție de caracteristicile concrete ale soluției achiziționate.
CNF.14.	Obligatorie	Sistemul informatic va beneficia de o funcționalitate de ajutor contextual (help online)

3.2.3 Nivelul de business logică

La acest nivel de arhitectură este implementată funcționalitatea de bază a sistemului. Nivelul de business logică conține logica de business relevantă. Logica de business este responsabilă de accesarea, procesarea și transformarea datelor din aplicație, gestionează regulile de business și asigură consistența și corectitudinea datelor. Nivelul de business logică este accesat de nivelul de prezentare pentru a face funcțiile de business ale sistemului disponibile pentru utilizator. De asemenea, poate oferi aceste funcții către aplicațiilor externe, prin intermediul interfețelor aplicative care de asemenea sunt parte componentă a nivelului logicii de business.

O arhitectură de tip SOA presupune un nivel înalt de granularitate la nivelul blocurilor componente pentru Business logic. Fiecare bloc logic oferă funcțiile sale prin intermediul interfețelor interne sau / și externe deținute. Acestea pot fi accesate de alte componente business logic, componente ale nivelul de prezentare, sau interfețe externe.

Următoarele sunt cerințele aferente arhitecturii pentru nivelul de business logică.

ID	Criteriu	Cerință
CNF.15.	Obligatorie	Nivelul de business logică trebuie să fie complet independent în raport cu nivelul de prezentare și aplicații ce accesează nivelul logicii de business în mod direct (prin intermediul interfețelor aplicative).
CNF.16.	Opțională	Nivelul de business logică trebuie să dețină o arhitectură complet modulară, bazată pe componente reutilizabile și interfețe abstracte. Nu trebuie să existe funcționalități identice realizate de componente diferite la nivelul acesta (ex. data access).
CNF.17.	Opțională	Nivelul de business logică trebuie să conțină și să aibă delimitate componentele de tip ”business workflow” și componentele de tip ”business entity”.
CNF.18.	Opțională	Accesarea componentelor de tip ”business entity” se va face prin intermediul componentelor de tip ”business workflow”.
CNF.19.	Obligatorie	Entitățile de business trebuie să fie clar identificate la nivelul logicii de business și încapsulate în componente de tip ”business entities”.
CNF.20.	Obligatorie	Componentele de tip ”business entity” trebuie să fie integre și să conțină toate datele și logica de business aferentă entității de business de care ține, necesară pentru efectuarea operațiunilor de business, aplicarea regulilor de business relevante și pentru menținerea integrității și corectitudinii datelor conținute.
CNF.21.	Obligatorie	Componentele aferente nivelul de business logică trebuie să comunice intre ele prin interfețe / funcții interne dedicate (tight coupling).
CNF.22.	Obligatorie	Componentele aferente nivelul de business logică trebuie să fie accesibile pentru aplicațiile externe doar prin intermediul interfețelor aplicative externe definite în acest scop.
CNF.23.	Obligatorie	Arhitectura nivelului de business logică va permite accesul concurent la funcțiile sistemului.

3.2.4 Nivelul de date

La acest nivel de arhitectură sunt stocate și accesate datele a sistemului. Datele sunt accesibile prin intermediul serviciilor de gestiune a bazelor date (SGBD). La nivelul SGBD sunt stabilite regulile de integritate pentru date. Nivelul de date trebuie să asigure ca datele vor putea fi accesate doar de entitățile autorizate, iar datele vor rămâne integre și corecte.

Nivelul de date trebuie să asigure datele necesare sistemului pentru furnizarea funcționalităților și serviciilor de business solicitate de REDNV. Următoarele sunt cerințele aferente arhitecturii pentru nivelul de date.

ID	Criteriu	Cerință
CNF.24.	Obligatorie	Modelul de date implementat la nivelul de date trebuie să fie normalizat. Datele nu vor fi stocate redundant, relațiile de integritate intre date vor fi complet și corect definite și implementate, pornind de la rolul de business al datelor.
CNF.25.	Obligatorie	Modelul de date trebuie să asigure posibilitatea migrării datelor din sistemele existente în cadrul MAI.
CNF.26.	Obligatorie	Datele sistemului trebuie să poată fi accesate doar prin intermediul componentelor conținute de nivelul de business logică.
CNF.27.	Obligatorie	Datele stocate în cadrul sistemului trebuie să fie neutre și independente în raport cu nivelul Business logic.
CNF.28.	Obligatorie	Arhitectura de date trebuie să fie optimizată din punct de vedere al accesării datelor pentru efectuare tranzacții și pentru analize și raportări.
CNF.29.	Obligatorie	Modelul de date implementat la nivelul de date trebuie să fie adecvat documentat. Documentația trebuie să conțină atât descrierea tehnică a nivelului de date (structuri baze de date, obiecte ale bazei de date, relații de integritate, etc.), cât și descrierea semantică (asocierea structurilor de date la entitatea de business și proprietăți ale acestora). Descrierea semantică a datelor trebuie

		să fie disponibilă pentru utilizatori în cadrul sistemului, acolo unde este utilă (ex. configurarea rapoartelor).
CNF.30.	Obligatorie	Arhitectura sistemului trebuie să asigure integritatea și corectitudinea datelor la accesarea și modificarea datelor simultan de mai multe entități (utilizatori, procese interne, aplicații externe).

3.2.5 Nivelul tehnologic

La acest nivel de arhitectură sunt plasate componentele soft și hard necesare pentru rularea componentelor sistemului ce fac parte din nivelele de mai sus (nivelul de date, nivelul de logica de business și nivelul de prezentare).

Nivelul tehnologic al arhitecturii trebuie să asigure disponibilitatea și accesibilitatea componentelor sistemului.

Următoarele sunt cerințele aferente arhitecturii pentru nivelul tehnologic.

ID	Obligativitate	Cerință
CNF.31.	Obligatorie	Arhitectura tehnologică a sistemului s trebuie să dețină un nivel înalt de rezistență la căderi, să nu conțină puncte singulare de cădere (SPOF).
CNF.32.	Obligatorie	Arhitectura tehnologică trebuie să asigure utilizarea rațională și balansată a resurselor de procesare.

3.3 Platforma tehnologică

Platforma tehnologică este formată din totalitatea componentelor soft și hard necesare pentru a asigura mediul de operare în care va rula aplicația. Platforma tehnologică include: platforme de dezvoltare și limbaje de programare în care este elaborat codul sistemului, servicii de gestiune a bazelor de date, sisteme de operare pe baza cărora pot rula componentele sistemului WFMS, soft special de sistem necesar a fi instalat pentru rularea corecta a sistemului WFMS, platforma hardware pe care pot rula componentele sistemului WFMS, etc.

Pentru a avea sistemul WFMS scalabil, flexibil și ușor mentenabil, trebuie să existe un nivel minim de dependență a sistemului Core față de platforma tehnologică pe care rulează componentele sale.

3.3.1 Cerințe generale

La acest punct sunt formulate cerințele generale aferente platformei tehnologice.

ID	Obligativitate	Cerință
CNF.33.	Obligatorie	Componentele sistemului trebuie să fie independente de platforma tehnologica pe care rulează (cu excepția cazurilor când asemenea cerințe rezultă explicit din acest Caiet de sarcini).
CNF.34.	Opțională	Arhitectura sistemului trebuie să fie optimizată pentru rularea în medii de tipul cloud computing. Caracteristici ale unui sistem cu arhitectură orientată spre implementare în Cloud, sunt: conștient de latență, conștient de căderi de componente, paralelizabil, conștient de utilizarea resurselor.
CNF.35.	Obligatorie	Tehnologiile prezente la nivelul platformei tehnologice trebuie să fie omogene (număr minim de tehnologii diferite, ex. diferite sisteme de operare pentru middleware și data base).
CNF.36.	Obligatorie	Sistemul WFMS trebuie să suporte crearea, modificarea, procesarea, stocarea și accesarea textului în format Unicode.
CNF.37.	Obligatorie	Ofertantul va indica în oferta sa informație completă privind platformele tehnologice suportate de aplicația sa.

3.3.2 Nivelul de prezentare

La acest punct sunt stabilite cerințele aferente tehnologiilor prezente la nivel de nivelul de prezentare.

ID	Obligativitate	Cerință

CNF.38.	Obligatorie	Sistemul WFMS trebuie să fie accesibil pentru orice utilizator conectat la rețeaua interna a MAI, utilizând tehnica de calcul standard deținută la locul de munca (stații desktop, calculatoare portabile, imprimante).
CNF.39.	Obligatorie	Toate vizualizările și rapoartele din sistemul WFMS trebuie să poată fi imprimate pe formatul de pagină indicat. Sistemul trebuie să dimensioneze automat documentele de ieșire pentru a se încadra în formatul indicat de utilizator (ex. A2/3/4, portrait / landscape, etc.). Va exista una sau mai multe opțiuni pentru tipul documentelor de ieșire (PDF, XML, XLS, DOC).
CNF.40.	Obligatorie	Sistemul WFMS client trebuie să poată fi rulat în medii de operare Windows XP/Vista /7 și mai noi.
CNF.41.	Obligatorie	Aplicația client mobilă va putea fi rulată în sistemele de operare din familia Android 4.1 și mai sus.
CNF.42.	Opțională	Partea de client a sistemului Core trebuie fie independentă de mediul de operare pe care rulează (ex. accesate prin browser web).

3.3.3 Nivelul de business logică

La acest punct sunt stabilite cerințele aferente tehnologiilor prezente la nivel de nivelul de business logică.

ID	Obligativitate	Cerință
CNF.43.	Obligatorie	Componentele ce formează nivelul de business logică trebuie să fie elaborate în limbaje de programare moderne, de uz larg la moment (ex. Java, C# etc.).
CNF.44.	Obligatorie	Tehnologiile prezente la acest nivel trebuie să permită integrarea componentelor ce sunt sau va fi dezvoltate de REDNV prin interfețele puse la dispoziție.

3.3.4 Nivelul de date

La acest punct sunt stabilite cerințele aferente tehnologiilor prezente la nivel de date.

ID	Obligativitate	Cerință
CNF.45.	Obligatorie	Sistemul trebuie să suporte sistemul de gestiune a bazelor de date MS SQL 2008, sau mai nou.

3.3.5 Nivelul tehnologic

La acest punct sunt stabilite cerințele aferente tehnologiilor prezente la nivelul tehnologic.

ID	Obligativitate	Cerință
CNF.46.	Obligatorie	Toate componentele sistemului WFMS (ex. middleware, baze de date) trebuie să poată fi rulate pe sisteme de operare Windows Server 2008 r2 sau mai noi.
CNF.47.	Obligatorie	Componentele sistemului WFMS trebuie să poată fi rulate pe orice platformă hardware (ex. HP Unix servers, Windows Servers, Oracle / Sun server, etc.).
CNF.48.	Obligatorie	Pentru rularea sistemului WFMS va fi necesar de echipamentul standard, disponibil pentru a fi liber achiziționat pe piață de către SPCSE.
CNF.49.	Obligatorie	Ofertantul va include în oferta sa informație detaliată privind platforma tehnologică recomandată (in limita alternativelor disponibile), ținând cont de necesitățile MAI stabilite în acest caiet de sarcini. În cazul ofertei câștigătoare, aceasta va fi luata la baza pentru stabilirea platformei tehnologice aferentă sistemului WFMS.

3.4 Interoperabilitate

Interoperabilitatea sistemului WFMS reprezintă caracteristica acestora de a comunica cu alte aplicații. Arhitectura TIC MAI stabilește interfețele ce trebuie să existe intre WFMS și alte sisteme MAI. La acest punct sunt stabilite cerințele privind caracteristicile de interoperabilitate a sistemului.

ID	Obligativitate	Cerință
CNF.50.	Obligatorie	Toate interfețele sistemului WFMS trebuie să fie bazate pe standarde deschise. Toate fluxurile de mesaje între Sistem și entități externe se vor realiza cu utilizarea standardelor deschise.
CNF.51.	Obligatorie	Toate interfețele sistemului WFMS furnizate vor putea interacționa cu aplicațiile externe atât în regim real, cat și în regim off-line.
CNF.52.	Obligatorie	Interfețele sistemului WFMS furnizate vor permite cuplarea slaba cu aplicațiile externe (comunicare în baza de mesaje).
CNF.53.	Opțională	Sistemul WFMS va deține interfețe standard pentru accesarea tuturor funcțiilor de business cheie ale sistemului WFMS (ex. generare documente, generare tranzacții, accesare informații despre entitățile de business stocate în cadrul sistemului WFMS). Interfețele respective trebuie să permită gestiunea entităților de business cu aplicarea tuturor regulilor de business relevante și cu utilizarea tuturor proprietăților aferente entităților de business.
CNF.54.	Opțională	Sistemul WFMS va deține interfețe standard pentru exportul datelor în cadrul instrumentelor de tipul Data Warehouse.
CNF.55.	Obligatorie	Toate interfețele sistemului WFMS trebuie să fie adecvat documentate (ex. cu aplicarea modelului Web Services Description Language).
CNF.56.	Obligatorie	Sistemul WFMS va deține posibilitatea de a crea mesaje email conform formularelor prestabilite și de a le expedia către destinatarii indicați prin intermediul serverului de posta electronica setat în configurațiile sistemului.
CNF.57.	Obligatorie	Sistemul WFMS va conține API pentru generare de facturi către o aplicație externă și API pentru primirea informației privind plățile încasate.

3.5 Performanță

Sistemul trebuie să dețină capacitatea de a procesa în timp util tranzacțiile efectuate de Beneficiar, conform volumetriei rezultate din activitatea Beneficiarului. La acest punct sunt stabilite cerințele de performanță la care trebuie să răspundă sistemul solicitat de Beneficiar.

ID	Obligativitate	Cerință
CNF.58.	Obligatorie	Furnizorul va include în ghidurile de administrare și operare a sistemului informație privind procesele ce pot impacta performanța Sistemului și recomandările sale privind rularea concurentă a acestor procese (ex. nu se recomanda rularea procesului X de generare a rapoartelor zilnice, simultan cu procesul Y de reevaluare a valorilor mobiliare).
CNF.59.	Obligatorie	Generarea rapoartelor și accesarea informației în scopul analizelor de business nu trebuie să afecteze performanța operațională a sistemului la nivelul procesării tranzacțiilor. În documentația sistemului vor fi identificate rapoartele cu impact semnificativ asupra performanței și formulate recomandările furnizorului privind generarea rapoartelor respective astfel încât să nu impacteze caracteristica de performanță a sistemului.
CNF.60.	Obligatorie	Ofertantul va indica în oferta sa valorile minime garantate pentru caracteristicele de performanță ale sistemului, ținând cont de platforma tehnologica recomanda de ofertant.
CNF.61.	Obligatorie	Aplicația trebuie să dețină capacitate de a procesa cel puțin 2 milioane de tranzacții pe zi.

CNF.62.	Obligatorie	Aplicația trebuie să poată gestiona până la 500 de conexiuni simultane (conexiuni utilizator și sisteme externe).
CNF.63.	Obligatorie	Timpul de răspuns la o interpelare tranzacțională utilizator / serviciu extern nu trebuie să depășească o secundă (nu se refera și la generarea de rapoarte).
CNF.64.	Obligatorie	Aplicația va deține capacitatea de a procesa tranzacțiile atât în regim real, cât și în regim off-line (batch).

3.6 Flexibilitate

Sistemul trebuie să dețină capacitate de a fi adaptat în timp la noi necesități de business. Este preferabil că acest fapt să fie posibil prin ajustări de configurație în sistem (versus modificări în cod), în acest fel minimizând costurile de ajustare pe partea Beneficiarului.

La acest punct sunt stabilite cerințele privind caracteristicile de flexibilitate aferente sistemului solicitate de Beneficiar.

ID	Obligativitate	Cerință
CNF.65.	Obligatorie	Aplicația va permite configurarea vizualizărilor și formelor utilizator. Aplicația va permite crearea de noi forme utilizator pentru accesarea logicii de business a sistemului.
CNF.66.	Obligatorie	Aplicația va permite configurarea rapoartelor existente (ex. ajustare set de date, formatare).
CNF.67.	Obligatorie	Aplicația va permite definirea rapoartelor utilizator (ex. definire set de date, format rapoarte, definire câmpuri calculate).
CNF.68.	Opțională	Aplicația va permite configurarea indicatoarelor și modalităților de prezentare grafică a datelor în Dashboard.
CNF.69.	Opțională	Aplicația va permite configurarea generării automate a rapoartelor. Generarea automată se va produce la anumite evenimente în cadrul sistemului sau la anumite momente în timp. Rapoartele generate vor putea fi stocate în cadrul sistemului sau expediate către adresele de email / sau utilizatorii setați.
CNF.70.	Opțională	Aplicația va permite definirea și configurarea entităților de business stocate în cadrul sistemului (ex. definirea de noi proprietăți).
CNF.71.	Opțională	Aplicația va permite configurarea rulării programate a procedurilor de sistem în funcție de parametri de timp sau de executare a anumitor evenimente în sistem. Sistemul va permite instalarea și configurarea noilor proceduri de sistem.
CNF.72.	Obligatorie	Aplicația va permite definirea și configurarea fluxurilor de business (ex. consecutivitate operațiuni, transformări de stare pentru proprietățile entităților de business, documente și înregistrări generate, notificări, roluri implicate și operațiuni permise, etc.).
CNF.73.	Obligatorie	Aplicația va permite definirea și gestiunea informației normative de referință utilizate în cadrul sistemului. Sursa de date pentru informația de referință poate fi internă sau externă (ex. BD externa, web serviciu extern, fișier extern).
CNF.74.	Obligatorie	Configurările sistemului trebuie să poată fi efectuate în interfețe utilizator comode pentru administratori.
CNF.75.	Opțională	Sistemul trebuie să permită integrarea componentelor dezvoltate de către Beneficiar. Aceste componente vor avea acces la funcțiile și proprietățile publice ale componentelor sistemului.
CNF.76.	Obligatorie	Sistemul trebuie să permită definirea stărilor în care se poate afla un obiect informațional. Drepturile de acces trebuie să permită stabilirea ope-

		rațiunilor permise utilizatorului, în funcție de stările admise pentru obiectul informațional (Sistemul trebuie să aibă mecanism de detectare a conflictelor în cazul în care se modifică stările pentru care sunt setate drepturi).

3.7 Utilizabilitate

Interfața sistemului trebuie să fie prietenoasă pentru utilizatori, ușoară și intuitivă în utilizare. Timpul necesar pentru instruire în vederea utilizării sistemului trebuie să fie minim. Utilizatorii vor avea acces în orice moment la informație de suport pentru a facilita utilizarea corecta a sistemului.

La acest punct sunt stabilite cerințele privind caracteristicile de utilizabilitate aferente sistemului solicitate de Beneficiar.

ID	Obligativitate	Cerință
CNF.77.	Obligatorie	Toate funcțiile de business accesibile utilizatorilor sistemului Sistemul trebuie să poată fi accesate prin interfețe utilizator grafice.
CNF.78.	Obligatorie	Sistemul trebuie să dețină interfețe utilizator prietenoase, intuitive și comode în utilizare pentru utilizatorii de business și utilizatorii cu roluri administrative. Informația necesară utilizatorului în scopul îndeplinirii atribuțiilor de serviciu trebuie să fie ușor și comod accesibilă pentru utilizator. Interfețele utilizator pentru Sistem trebuie să dețină stiluri unice de design grafic. Elementele grafice și textele folosite trebuie să fie utilizate consecvent din punct de vedere al semnificației asociate acestora.
CNF.79.	Obligatorie	Toate interfețele utilizatorilor trebuie să fie dezvoltate cel puțin în limba română.
CNF.80.	Obligatorie	Sistemul trebuie să permită definirea sau traducerea centralizată a termenilor specifici utilizați în cadrul sistemului (ex. Delete = Eliminare). Acești termeni vor fi preluați în modul respectiv în toate cazurile de utilizare a lor în cadrul sistemului.
CNF.81.	Obligatorie	Aplicația va permite salvarea intermediară a lucrului și operațiunilor inițiate de utilizator (automat sau la cererea utilizatorului).
CNF.82.	Obligatorie	Sistemul trebuie să dețină funcție integrată de căutare a datelor. Va fi asigurată căutarea simplă a înregistrărilor (după specificare a șirurilor de căutare) și căutarea complexă (cu posibilitate de a crea interogări, interpelări în mod vizual QBE (Query by Example). Interfața utilizator trebuie să asigure posibilitatea filtrării și sortării informațiilor prezentate în rezultatele căutării. Mărimile indexate (valori din clasificatoare) vor fi filtrate prin selectare valorii din liste predefinite. Pentru câmpurile de tip numeric sau dată calendaristică trebuie să existe posibilitatea filtrării conform valorii exacte a caracteristicii căutate (egal cu, toate în afară de) sau conform criteriilor logice (mai devreme de , mai mic de, mai mare de, etc.) Trebuie să existe posibilitatea filtrării rezultatelor conform măștii, de ex.: „323*” - toate secvențele care se încep cu șirul de caractere „323”**,** ”*Core” - toate secvențele care se sfârșesc cu șirul de caractere „SISTEMUL” sau ”*SISTEMUL*” - toate secvențele care au în conținut șirul de caractere „SISTEMUL”. Conținutul oricărui tabel cu rezultate trebuie să poată fi exportat în format XLS, CSV, PDF.
CNF.83.	Obligatorie	Sistemul va permite anexarea fișierelor la obiecte informaționale, sau referințelor la fișiere stocate pe server de fișiere / web pentru toate obiectele informaționale implicit. Această funcționalitate va fi utilizată de utilizatori

		în dependență de setări a profilului de acces. Fișele atașamentelor vor conține un set de atribute: data creării, data modificării, persoana responsabilă, mărime.
CNF.84.	Obligatorie	Utilizatorii sistemului vor avea acces la ajutor de context (context-sensitive help) în toate interfețele ale sistemului.
CNF.85.	Obligatorie	La utilizarea funcțiilor de definire și configurare rapoarte, utilizatorii trebuie să poată accesa dicționarul de date stocat în cadrul sistemului.

3.8 Mentenabilitate

Pentru ca Sistemul să fie disponibil și accesibil utilizatorilor de business la nivelul agreat, acestea trebuie să fie continuu monitorizate și menținute. Sistemul trebuie să permită identificarea proactivă a problemelor și prevenirea acestora prin derularea facilă a activităților de mentenanță operațională la nivelul tuturor componentelor sistemului.

La acest punct sunt stabilite cerințele privind caracteristicile de mentenabilitate aferente sistemului solicitate de Beneficiar.

ID	Obligativitate	Cerință
CNF.86.	Opțional	Sistemul va deține mecanisme de monitorizare a nivelului de încărcare și funcționare pentru toate componentele cheie (ex. componente nivelului de logică de business și nivelului de date).
CNF.87.	Opțional	Sistemul va genera notificări în cazul în care nivelul de încărcare pe anumite componente depășește praguri critice (ex. pentru o anumita perioada, nivelul mediu de încărcare a fost mai mult de 90%).
CNF.88.	Obligatorie	Toate erorile și excepțiile în funcționarea sistemului vor fi înregistrate și gestionate conform cerințelor stabilite la punctul „Exception handling”.
CNF.89.	Obligatorie	Codul sursa al sistemului va fi elaborat conform recomandărilor pentru scrierea codului sursa ușor mentenabil, inclusiv: bine structurat, însoțit de comentarii, variabile sugestive, etc.
CNF.90.	Obligatorie	Arhitectura sistemului va permite implementarea intr-o manieră simplistă pentru Beneficiar a schimbărilor la nivelul sistemului. Perimetrul afectat de modificări va fi minim, iar componentele necesar a fi testate în rezultatul modificărilor, clar identificabile.
CNF.91.	Obligatorie	Sistemul va permite definirea și rularea sarcinilor programate pentru activități de menținere operațională (ex. arhivare date istorice).
CNF.92.	Obligatorie	Arhitectura sistemului va permite implementarea noilor versiuni livrate de furnizor fără a afecta configurările existente, componentele implementate de Beneficiar și interfețele cu sistemul externe implementate.
CNF.93.	Obligatorie	Sistemul va putea fi purtat ușor din mediul de producție în alte medii de operare în vederea asigurării proceselor de testare și dezvoltare a sistemului. Documentația aferenta sistemului trebuie să descrie acest proces.
CNF.94.	Obligatorie	Sistemul va deține proceduri de prelucrare a tuturor erorilor generate. Erorile produse la funcționarea sistemului vor fi înregistrate și accesibile pentru analiza ulterioară și îmbunătățirea calității funcționării Sistemului.

3.9 Scalabilitate

Pe parcursul utilizării sistemului, este posibil ca numărul de tranzacții procesate să crească sau să scadă simțitor de la o perioadă la alta (de ex. facturare lunară furnizare EE). Pentru a avea o utilizare rațională a resurselor de procesare, sistemul solicitat de Beneficiar trebuie să fie ușor scalabil (în sus și în jos).

La acest punct sunt stabilite cerințele privind caracteristicile de scalabilitate aferente sistemului solicitate de Beneficiar.

ID	Importanță	Cerință

CNF.95.	Opțional	Sistemul va permite creșterea capacității de procesare fără a întrerupe funcționarea acestora. În acest scop, sistemul va suporta extinderea pe orizontală a capacității de procesare (ex. adăugarea de noi servere pentru serverele de sistemul și efectuare balansare a încărcării).
CNF.96.	Opțională	Sistemul va putea fi configurat pentru scalare automată la nivelul componentelor cheie (lag sensitive). Scalarea sistemului se va face atât în sus, cât și în jos.
CNF.97.	Obligatorie	Sistemul trebuie să dețină posibilitatea de a deservi practic un număr nelimitat de tranzacții, cu condiția alocării corespunzătoare a resurselor de procesare și stocare date. Resursele vor fi alocate pe orizontală (alocare noi servere, fără creșterea performanței pe serverele existente).
CNF.98.	Obligatorie	Fiecare componenta de tip server va putea lucra în sistem de high avalibility. Pentru aceasta licențele ofertate vor asigura, fără costuri suplimentare, extinderea instanțelor (mașini virtuale de tip server) sistemului cu până la cel puțin 5 servere pentru fiecare licență de tip server ofertată. Astfel, beneficiarul va putea, în funcție de încărcarea sistemului și de disponibilitatea resurselor hardware să extindă arhitectura, fără costuri suplimentare.

3.10 Securitate

Sistemul trebuie să permită un control adecvat asupra riscurilor de securitate a informației aferente utilizării. Măsurile de securitate implementate trebuie să fie aliniate la politicile de securitate aprobate în cadrul organizației Beneficiarului și să asigure prevenirea, detectarea și reacționarea adecvata la incidentele de securitate. Sistemul trebuie să implementeze o abordare de tipul ”Multi-layered security” (Securitate de mai multe nivele) la nivelul sistemului și să dețină capacitatea de a se integra în modelul instituțional al Beneficiarului pentru managementul securității informației (bazat pe familia de standarde ISO 27000).

La acest punct sunt stabilite cerințele privind caracteristicile de securitate aferente sistemului solicitate de Beneficiar.

3.10.1 Arhitectura de securitate

ID	Importanță	Cerință
CNF.99.	Obligatorie	Arhitectura sistemului trebuie să fie concepută prin aplicarea unei abordări de tipul „Secure by design” (Securitate prin design).
CNF.100.	Obligatorie	Arhitectura de securitate a sistemului trebuie să fie documentată la nivel tehnic.
CNF.101.	Obligatorie	Documentația va conține descris modelul de securitate implementat, componentele prezente și rolul fiecărei componente din punct de vedere al securității.
CNF.102.	Obligatorie	Documentația va conține specificațiile privind plasarea la nivel de rețea a componentelor sistemului și recomandările furnizorului privind regulile de acces la nivel de rețea necesar a fi setate de Beneficiar în vederea accesului securizat la toate componentele sistemului (ex. matrice de comunicare între servicii).
CNF.103.	Obligatorie	Toate procesele de sistem aferente componentelor sistemului vor rula cu privilegii minime necesare executării sarcinilor atribuite.
CNF.104.	Obligatorie	Toate credențialele de acces utilizate de aplicație trebuie să fie configurabile în interfețele administrative. Sistemul nu va conține credențiale de acces hard-coded.
CNF.105.	Obligatorie	Sistemul nu va conține stocate la nivelul componentelor sale (în baza de date, fișiere de configurație) credențiale de acces în formă deschisă.
CNF.106.	Obligatorie	Toate interfețele externe ale sistemului vor fi accesate cu aplicarea metodelor sigure de autentificare (ex. certificate X.509).

3.10.2 Autentificare

ID	Importanță	Cerință

CNF.107.	Obligatorie	Sistemul va permite accesarea funcțiilor sistemului doar după autentificarea cu succes a utilizatorului/administratorului. Sistemul va oferi suport pentru cel puțin următoarele metode de autentificare: În bază de ID și parolă, Windows authentication (integrare cu Active Directory). Sistemul va permite utilizatorilor schimbarea parolelor individuale.
CNF.108.	Obligatorie	Sistemul va permite înregistrarea utilizatorilor și a informației de profil aferentă acestora (ex. ID, parola, nume, prenume, email, etc.).
CNF.109.	Obligatorie	Parolele utilizatorilor trebuie să fie protejate în cadrul sistemului. Metoda de protejare a parolelor trebuie să asigure imposibilitatea interceptării, deducerii sau recuperării acestora.
CNF.110.	Obligatorie	Sistemul va permite definirea și implementarea seturilor de politici de utilizare a parolelor. Politicile trebuie să permită setarea cerințelor cel puțin pentru: complexitatea parolei, obligativitatea schimbării parolei, durata de viață a parolei, utilizarea repetată a parolelor, numărul de încercări de autentificare eșuată, dicționar de parole interzise. Aplicația va furniza utilizatorului în timp util informație cu privire la aplicarea politicilor de utilizare a parolelor (ex. mesaj de expirare a parolei în n zile).
CNF.111.	Opțională	Sistemul va permite aplicarea diferențiată a politicilor de utilizare a parolelor pentru diferite grupe de utilizatori.
CNF.112.	Obligatorie	Sistemul va permite blocarea, dezactivarea sau suspendarea conturilor utilizatorilor la nivel de aplicație.
CNF.113.	Obligatorie	Sistemul va putea fi integrat cu serviciul de directoare implementat în cadrul Beneficiarului (in cadrul Beneficiarului este utilizată soluția MS Active Directory). La crearea unui nou cont de utilizator, Sistemul va avea opțiunea de selectare din lista de utilizatori disponibili în cadrul serviciului de directoare
CNF.114.	Opțională	Sistemul va putea fi integrat cu servicii externe de tipul „ISP" (Identity Services Providers). În acest scop, vor fi utilizate standardele și protocoalele deschise în domeniu (ex. SAML). Metodele de autentificare ce trebuie să fie susținute cu implicarea unui ISP extern sunt: a. ID și parola; b. Certificate X.509; c. OTP (One Time Password).
CNF.115.	Obligatorie	Acces prin aplicația client mobilă se va efectua în baza credențialelor de acces ale unui utilizator și o cheie unică setată în configurația aplicației client. Comunicarea cu serverul Sistemului va fi criptată.
CNF.116.	Opțională	Sistemul va permite aplicarea diferențiată a metodelor de autentificare, în funcție de resursele accesate (ex. implicit ID și parola, adițional OTP pentru interfața administrativa).
CNF.117.	Obligatorie	Sistemul va permite setarea numărului de conexiuni simultane ce pot fi inițiate de un utilizator.
CNF.118.	Obligatorie	Sistemul va permite setarea timpului de expirare a sesiunilor utilizatorilor în caz de inactivitate.
CNF.119.	Obligatorie	Sistemul va deține mecanisme eficiente de prevenire a preluării neautorizate a sesiunilor active inițiate de utilizatorii legitimi.
CNF.120.	Obligatorie	Sesiunea de lucru în sistemul va fi blocată la solicitarea utilizatorului sau automat, la expirarea sesiunii utilizatorului.

3.10.3 Autorizare

ID	Importanță	Cerință
CNF.121.	Obligatorie	Sistemul va permite gestiunea granulară a drepturilor de acces la toate obiectele sistemului și operațiunile posibile asupra acestora (ex. entități de business,

		proprietăți ale entităților de business, forme, meniuri, rapoarte, operațiuni de creare / citire / actualizare / eliminare).
CNF.122.	Obligatorie	Metoda de autorizare în cadrul sistemului se va baza pe principiul „este interzis tot ce nu este explicit permis”.
CNF.123.	Obligatorie	Sistemul va permite definirea grupelor de utilizatori și roluri în cadrul sistemului, și asocierea utilizatorilor la aceste grupe și roluri.
CNF.124.	Obligatorie	Sistemul va permite acordarea drepturilor de acces la nivel de utilizator, grupe și roluri de utilizator. O grupă va putea conține mai multe subgrupe / roluri. Un utilizator poate fi asociat uneia sau mai multor grupe și roluri, drepturile sale de acces fiind determinate cumulativ.
CNF.125.	Obligatorie	Sistemul va permite acordarea drepturilor de acces bazate pe reguli de business (ex. modificarea documentului doar dacă utilizatorul este autor, sau dacă operațiunea se face intr-un anumit interval de timp).
CNF.126.	Obligatorie	Sistemul va permite delegarea temporară a drepturilor deținute de un utilizator, către un alt utilizator. Delegarea va putea fi efectuată cu păstrarea sau suspendarea drepturilor deținute de utilizatorul către care se deleagă drepturile.
CNF.127.	Opțională	Sistemul va permite segregarea activităților administrative (ex. administrator 1 modifica, administrator 2 confirma).
CNF.128.	Obligatorie	Sistemul va deține vizualizări și rapoarte privind drepturile de acces existente în Sistem. Acestea vor putea fi parametrizate în funcție de cel puțin următorii parametri: grupa utilizator / rol în cadrul sistemului, ID utilizator, entitate de business, proprietate aferentă entității de business, operațiuni admise.

3.10.4 Validarea datelor de intrare și de ieșire

ID	Importanță	Cerință
CNF.129.	Obligatorie	Sistemul va deține mecanisme adecvate pentru a preveni manipularea datelor de intrare (intrări utilizator, intrări de la aplicații externe).
CNF.130.	Obligatorie	Toate operațiunile de modificare date de business critice în cadrul sistemului vor fi efectuate prin intermediul documentelor, conform fluxului de business stabilit pentru aceste documente (ex. transfer sold client de pe un cont pe alt cont al său).
CNF.131.	Obligatorie	Sistemul va efectua validarea completă și independentă a datelor pe partea de nivelul de prezentare, nivelul de business logică, nivelul de date, în scopul asigurării și menținerii integrității, completitudinii și corectitudinii datelor.
CNF.132.	Obligatorie	Toate afișările de informație din cadrul sistemului trebuie să însoțite de un marcaj de securitate, conform unui clasificator stabilit în acest sens în cadrul sistemului.
CNF.133.	Obligatorie	Datele confidențiale nu vor fi stocate și accesate nesecurizat în cadrul sistemului (ex. În fișiere log, caching).
CNF.134.	Obligatorie	Sistemul va deține mecanisme de protejare adițională a datelor deosebit de confidențiale (ex. afișarea mascată a datelor, stocarea în formă criptată, autentificarea repetată, etc.).
CNF.135.	Obligatorie	Sistemul va deține proceduri de rutină pentru verificarea și detectarea posibilelor coruperi a relațiilor de integritate a datelor.
CNF.136.	Obligatorie	Sistemul va deține mecanisme adecvate pentru a preveni manipularea datelor stocate în cadrul aplicației.

3.10.5 Auditul și monitorizarea de securitate

ID	Importanță	Cerință
CNF.137.	Obligatorie	Sistemul va deține componente de audit ce vor colecta și gestiona centralizat înregistrările de audit la nivelul fiecărui modul Sistemul.

CNF.138.	Obligatorie	Componenta de audit va permite configurarea granulară a politicilor de audit.
CNF.139.	Obligatorie	Sistemul va permite stabilirea politicilor de audit la nivel de obiect / entitate de business și la nivel de eveniment.
CNF.140.	Obligatorie	Sistemul va permite stabilirea caracteristicilor specifice evenimentelor ce trebuie să fie înregistrate (ex. produse intr-un anumit interval de timp, o anumita valoare a proprietarii entității de business).
CNF.141.	Obligatorie	Sistemul va permite auditarea oricărui eveniment, la nivelul oricărui obiect sau entitate de business din cadrul sistemului.
CNF.142.	Obligatorie	Fiecare înregistrare de audit va conține cel puțin: a. Momentul în timp al producerii evenimentului; b. Subiectul evenimentului (ID utilizator); c. Obiectul sau entitatea de business afectata; d. Evenimentul produs; e. Adresa IP a sursei ce a inițiat evenimentul.
CNF.143.	Obligatorie	Înregistrările de audit nu vor conține informație de business confidențială (ex. parole introduse la încercările eșuate).
CNF.144.	Obligatorie	Erorile ce pot apărea la fixarea înregistrărilor de audit nu trebuie să afecteze funcționarea normală a sistemului.
CNF.145.	Obligatorie	Componenta de audit va utiliza ceasul de sistem setat la nivelul sistemului de operare în care rulează componenta de audit.
CNF.146.	Obligatorie	Componenta de audit va deține un mecanism de arhivare a înregistrărilor de audit istorice. Procesul de arhivare va putea fi parametrizat (frecvența, vechime date, format arhivare, destinație, etc.).
CNF.147.	Opțională	Sistemul va putea genera automat notificări către persoanele responsabile la producerea anumitor evenimente de securitate, conform configurațiilor setate.
CNF.148.	Opțională	Componenta de audit va putea fi integrată în baza standardelor deschise cu soluții de tipul SIEM (Security Incident and Event Management) în vederea preluării înregistrărilor de audit produse în cadrul sistemului, de către soluțiile respective.
CNF.149.	Obligatorie	Sistemul va permite fixarea versiunilor istorice ale datelor, ce vor fi considerate deosebit de senzitive.
CNF.150.	Obligatorie	Activități de schimbare stări și responsabili înregistrări vor fi jurnalizate.
CNF.151.	Obligatorie	Sistemul va deține instrumente comode pentru accesarea și procesarea evenimentelor log înregistrate, inclusiv filtrarea înregistrărilor de audit după orice câmp deținut și exportul acestora în format uzual. Instrumentele de audit ale sistemului vor putea fi utilizate și în scopul importului arhivelor cu fișiere de audit pentru activități de analiza ocazionale.
CNF.152.	Obligatorie	Sistemul va deține mecanisme sigure de protejare a integrității informației de audit înregistrate.

3.10.6 Gestiunea excepțiilor și erorilor

ID	Importanță	Cerință
CNF.153.	Obligatorie	Sistemul va înregistra centralizat toate excepțiile și erorile produse la funcționarea sistemului Sistemul.
CNF.154.	Obligatorie	La producerea unei erori, aplicația va afișa utilizatorului un mesaj de eroare generic. Acesta poate conține un cod de eroare și un identificator unic al erorii, pentru a facilita implicarea serviciilor de suport.
CNF.155.	Obligatorie	Sistemul va deține instrumentele necesare pentru analiza și procesarea înregistrărilor aferente excepțiilor și erorilor.

CNF.156.	Opțională	Sistemul va putea genera automat notificări către persoanele responsabile la producerea anumitor erori în funcționarea sistemului.

3.11 Reziliență și continuitate

Sistemul trebuie să dețină servicii de tipul „heart beat”, prin intermediul cărora va putea fi monitorizată disponibilitatea sistemului de către servicii externe.

ID	Importanță	Cerință
CNF.157.	Opțională	Sistemul va avea implementate instrumente pentru executarea procedurilor de copiere de rezervă și gestiune a copiilor de rezervă istorice.
CNF.158.	Obligatorie	Sistemul trebuie să dețină mecanisme de asigurare a integrității datelor în cazul căderilor la nivelul oricăror componente.
CNF.159.	Obligatorie	Sistemul trebuie să dețină mecanisme de restabilire operativă a disponibilității și accesibilității sistemului Sistemul în cazul unor incidente de continuitate.
CNF.160.	Obligatorie	Arhitectura sistemului trebuie să fie rezistentă la căderi de componente și să nu dețină puncte singulare de cădere (SPOF).
CNF.161.	Obligatorie	Sistemul trebuie să dețină mecanisme de asigurare a integrității datelor în cazul unor căderi accidentale la nivelul oricăror componente ale sale.
CNF.162.	Obligatorie	Sistemul trebuie să dețină mecanisme de restabilire operativă a disponibilității și accesibilității în cazul unor incidente de continuitate.

4 SPECIFICAȚII PENTRU SERVICII DE SUPORT ȘI MENTENANȚĂ POST-IMPLEMENTARE

4.1 Servicii de suport

Serviciile de suport sunt prestate de furnizor în vederea depășirii incidentelor produse în legătură cu utilizarea aplicațiilor, în vederea soluționării problemelor ivite la utilizarea aplicațiilor și în scopul utilizării corecte și eficiente a aplicațiilor de către Beneficiarul.

Un ***incident*** aferent sistemului este orice eveniment ce a afectat sau ar fi putut afecta funcționarea normală a Sistem.

O ***problemă*** aferenta Sistemului este o cauza ce a dus sau poate duce la producerea unui incident.

O ***solicitare de consultanță*** este o adresare din partea Beneficiarul către furnizor în vederea obținerii suportului consultativ la utilizarea, configurarea și menținerea Sistemului.

Serviciile de suport sunt destinate să asigure utilizarea în timp a sistemului la parametri de calitate necesari Beneficiarul.

Parametri de calitate pentru funcționarea Sistemului sunt:

- **Disponibilitatea** – capacitatea sistemului și a componentelor sale de a primi interpelări din partea entităților autorizate și de a răspunde în timp util la aceste interpelări;
- **Utilizabilitatea** – capacitatea sistemului de a funcționa corect, livrând către utilizatori și entități autorizate serviciile scontate;
- **Performanța** – capacitatea sistemului de a răspunde la interpelările legitime la parametri stabiliți;
- **Securitatea** – capacitatea sistemului de a asigura confidențialitatea, integritatea și disponibilitatea informației stocate în cadrul sistemului.

La acest punct sunt stabilite cerințele pentru serviciile de suport cu utilizare a terminologiei de mai sus.

ID	Condiție	Cerință
CSP.1.	Obligator	Furnizorul va oferi suport Beneficiarul la soluționarea incidentelor aferente sistemului, indiferent de cauzele ce au dus la apariția incidentului (ex. erori în aplicație, probleme la nivel de soft de sistem, probleme în aplicații externe). În acest scop, în funcție de specificului fiecărui caz de incident în parte, furnizorul poate întreprinde următoarele acțiuni: a. Recepționarea de la Beneficiarul a informației despre incidentul produs și contextul producerii acestuia; b. Localizarea incidentului și identificarea activităților imediate ce trebuie să fie întreprinse în vederea diminuării impactului incidentului; c. Identificarea cauzelor incidentului și stabilirea acțiunilor necesar a fi întreprinse în vederea înlăturării incidentului; d. Ghidarea Beneficiarul în vederea întreprinderii acțiunilor pentru diminuarea impactului incidentului și soluționarea acestuia în limita de timp stabilita; e. Prezentarea informației detaliate către Beneficiarul privind cauzele incidentului, raționamentul acțiunilor întreprinse și acțiunile planificate pentru a preveni repetarea incidentelor similare; f. Examinarea necesității de înregistrare a unei noi probleme aferente Sistem. In cazul înregistrării problemei, furnizorul o va gestiona conform cerințelor aferente serviciilor de suport pentru soluționarea problemelor.
CSP.2.	Obligator	Furnizorul va presta servicii de suport pentru soluționarea problemelor înregistrate la nivelul aplicațiilor. In acest scop, în funcție de specificului fiecărui caz în parte, furnizorul poate întreprinde următoarele acțiuni: a. Recepționarea și colectarea informației aferente problemei, simptome, efecte, condiții specifice; b. Analiza și localizarea problemei la nivelul componentelor aplicației. Identificarea interdependențelor ce contribuie la manifestarea problemei sau sunt afectate de problema; c. Identificarea soluțiilor temporare pentru a diminua efectele problemei și ghidarea Beneficiarul în vederea aplicării acestora; d. Identificarea soluțiilor aferente problemei. Comunicarea regulata cu Beneficiarul privind progresele făcute în vederea identificării soluțiilor; e. In cazul în care soluțiile țin de configurări la nivelul aplicației, ghidarea Beneficiarul în vederea implementării acestora; f. In cazul în care soluțiile presupun modificări la nivelul aplicațiilor, acestea vor dezvoltate de furnizor și implementate în cadrul serviciilor de Mentenanță în limita de timp stabilita.
CSP.3.	Obligator	Furnizorul va presta servicii de suport consultativ la utilizarea aplicației de către Beneficiarul. In acest scop, în funcție de specificul necesitaților de consultanta ale Beneficiarul, furnizorul poate întreprinde următoarele acțiuni: a. Recepționarea solicitării de consultanță din partea Beneficiarul și a informației aferente contextului în care este necesara consultanța; b. Identificarea soluțiilor și validarea acestora în mediile de test ale furnizorului; c. Oferirea răspunsurilor complete și corecte privind modul în care trebuie să acționeze Beneficiarul la utilizarea sistemului, conform solicitării de consultanță.

4.2 Servicii de mentenanță

Serviciile de mentenanță sunt prestate de furnizor în scopul menținerii în timp a aplicațiilor la parametri de funcționare optimi. În acest scop, Furnizorul poate veni cu actualizări și modificări la nivelul aplicațiilor și noi versiuni ale aplicațiilor.

Actualizări ale sistemul Sistem sunt modificări la nivelul aplicațiilor, transmise către Beneficiarul la inițiativa furnizorului și destinate să îmbunătățească performanța aplicațiilor, să înlăture probleme, erori și vulnerabilități cunoscute furnizorului.

Versiuni noi (new releases) sunt pachete de software aferente sistemului, transmise către Beneficiarul la inițiativa furnizorului și care conțin toate modificările efectuate anterior la nivelul aplicațiilor. Suplimentar, pot conține modificări și actualizări, componente noi de aplicație, ce nu au fost prezente în versiunea veche a aplicațiilor.

ID	Condiție	Cerință
CSP.4.	Obligator	Furnizorul va presta servicii de actualizare a sistemului și de livrare a versiunilor noi. In acest scop furnizorul va pregăti pachetele software și documentația aferentă actualizărilor și noilor versiuni. Implementarea tuturor actualizărilor și noilor versiuni se va efectua conform cerințelor stabilite la punctul „Change management”.

4.3 Servicii de dezvoltare

Serviciile de dezvoltare sunt prestate de furnizor la solicitarea Beneficiarul în scopul alinierii aplicațiilor la necesitățile de afacere în schimbare ale Beneficiarul.

O solicitare de modificare / dezvoltare este o adresare din partea Beneficiarul către furnizor în scopul obținerii modificărilor la nivelul funcționalităților sistemului sau în scopul livrării de funcționalități noi pentru aplicații. O solicitare din partea Beneficiarul se va considera ca fiind de modificare / dezvoltare doar în cazul în care funcționalitatea solicitată nu este furnizată de aplicație sau este furnizată diferit decât solicită Beneficiarul. În ultima categorie nu intră solicitările aferente corectării funcționalităților ce prezintă o problemă aferentă Sistemului (conform definiției de mai sus).

Serviciile de dezvoltare vor fi achitate de Beneficiarul suplimentar la suma contractului, în funcție de volumul serviciilor prestate.

ID	Condiție	Cerință
CSP.5.	Obligator	Furnizorul va presta servicii de modificare și dezvoltare a sistemului furnizat. Perimetrul modificărilor va include cel puțin: • Modificări la nivel de nivelul de prezentare; • Modificări la nivelul logicii de business; • Modificări la nivel de date.
CSP.6.	Obligator	Parte a serviciilor de modificare și dezvoltare ale Sistemului, furnizorul va efectua: • Recepționarea solicitării de modificare cu descrierea specificațiilor funcționale aferente; • Elaborarea proiectului tehnic aferent solicitării și coordonarea acestuia cu Beneficiarul; • Efectuarea modificărilor și dezvoltărilor la nivelul componentelor sistemului.
CSP.7.	Obligator	Implementarea modificărilor și dezvoltărilor la nivel de sistem se va efectua conform cerințelor stabilite la punctul „Managementul schimbărilor”.
CSP.8.	Obligator	Ofertantul va descrie în oferta sa modelul propus pentru gestiunea solicitărilor de modificare și dezvoltare și metodele aplicate pentru estimarea prețurilor pentru beneficiar. Informația inclusa în ofertă trebuie să fie suficientă pentru a aprecia ca relația dintre Beneficiarul și furnizor în procesul de prestare a serviciilor de dezvoltare va fi una transparenta și corectă.
CSP.9.	Obligator	Parte a serviciilor de menținere operațională și dezvoltare pentru Sistem, Ofertantul va oferi servicii de dezvoltare pentru Sistem. Serviciile de dezvoltare vor include: • Modificarea funcționalității existente în cadrul Sistemului (ex. self service pentru prestatorii de servicii publice la înregistrarea unui nou serviciu); • Implementarea de noi funcționalități în cadrul Sistemului (ex. implementare de noi instrumente de plată).

ID	Condiție	Cerință
		Orice dezvoltare pentru softul aplicativ aferent Sistemului va fi inițiată în baza unei solicitări din partea Beneficiarului. Solicitarea va fi însoțită de specificațiile funcționale pentru modificarea cerută. Implementarea oricărei modificări aferente Sistemului va trece prin procesul de management al schimbărilor agreat cu Beneficiarul. Pentru modificările la nivelul softului aplicativ, procesul va prevedea cel puțin: • Implementarea în mediul de testare al Beneficiarului. Unit testing de către Beneficiar; • Implementarea în mediul de testare al Beneficiarului. Testarea de acceptanță, cu implicarea utilizatorilor Sistem; • Implementarea în mediul de producție al Sistemului, conform procedurii de management al schimbărilor stabilite; • Revizuirea finală și acceptarea finală a modificării. Ofertantul va include în oferta sa numărul de om-zile specificate în documentația standard de licitație pentru servicii de dezvoltare anual. Costul acestor servicii va fi inclus în prețul serviciilor, conform modelului agreat între părți. Servicii de dezvoltare adiționale celor incluse, vor putea fi solicitate de Beneficiar și oferite de Ofertant în baza acordurilor adiționale semnate între Părți. Ofertantul va specifica în oferta sa modelul de stabilire a prețului pentru asemenea servicii, precum și tarifele aplicate.

5 NIVELUL SERVICIILOR AFERENTE SISTEMULUI (SERVICE LEVEL)

Nivelul serviciilor de suport și mentenanța post-implementare stabilește cerințele privind parametrii la care trebuie să fie prestate aceste servicii de către furnizor.

5.1 Servicii de suport

Parametrii ce caracterizează nivelul serviciilor de suport sunt următorii:

- **Timp de Răspuns (TR)** - este timpul în care furnizorul va reacționa la o solicitare de suport, va diagnostica situația și va stabili acțiunile necesar a fi întreprinse pentru soluționare.

- **Timp de Soluționare (TS)** – este timpul obiectiv în care se așteaptă ca furnizorul va întreprinde acțiunile în zona să de responsabilitate pentru a soluționa complet solicitarea Beneficiarul.

Solicitările Beneficiarul pentru servicii de suport și mentenanță post-implementare sunt clasificate din punct de vedere al importanței acestora pentru Beneficiarul. Importanța pentru Beneficiarul este apreciată în funcție de impactul (produs sau probabil) al evenimentului ce a generat necesitatea plasării solicitării asupra parametrilor de calitate pentru funcționarea aplicațiilor (vezi definițiile mai sus). Din acest punct de vedere, solicitările Beneficiarul vor fi clasificate pe următoarea scară:

Clasificare	Impactul asupra parametrilor de calitate pentru funcționarea aplicațiilor
Critică	*Disponibilitatea*: sistemul este indisponibil pentru toți sau marea majoritate a utilizatorilor de business. Tranzacții importante sunt necesare a fi efectuate cat mai curând posibil (ordin de ore). *Utilizabilitatea*: funcții cheie de business nu pot fi utilizate. Nu există proceduri și funcționalități alternative. *Performanța*: timpul de răspuns la interpelările utilizatorilor fac practic aplicația indisponibilă. *Securitatea*: există riscuri majore de compromitere a confidențialității, integrității sau disponibilității informației.
Înaltă	*Disponibilitatea*: sistemul este indisponibil pentru o bună parte din utilizatori. Tranzacții și operațiuni importante sunt necesare a fi efectuate până la începutul următoarei zile. *Utilizabilitatea*: funcții cheie de business pot fi utilizate limitat.

	Performanța: timpul de răspuns la interpelările utilizatorilor afectează în măsura semnificativă desfășurarea proceselor de business cheie. *Securitatea*: există riscuri înalte de compromitere a confidențialității, integrității sau disponibilității informației.
Ordinară	*Disponibilitatea*: sistemul este indisponibil pentru o parte din utilizatori. Sunt tranzacții și operațiuni ce trebuie să fie executate în următoarele trei zile. *Utilizabilitatea*: funcționalitatea de business a sistemului poate fi utilizată limitat. *Performanța*: timpul de răspuns la interpelările utilizatorilor afectează în măsură moderată desfășurarea proceselor de business. *Securitatea*: există riscuri de compromitere a confidențialității, integrității sau disponibilității informației.
Joasă	*Disponibilitatea*: aplicația este indisponibilă pentru un număr limitat de utilizatori. Nu sunt tranzacții și operațiuni ce trebuie executate în următoarele trei zile. *Utilizabilitatea*: funcționalitatea de business a aplicației este afectată nesemnificativ. Există proceduri și funcționalități alternative. *Performanța*: timpul de răspuns la interpelările utilizatorilor este mai mare decât cel obișnuit. Nu este afectată desfășurarea proceselor de business. *Securitatea*: există riscuri minore de compromitere a confidențialității, integrității sau disponibilității informației.

La plasarea unei solicitări pentru servicii de suport și mentenanță post-implementare, Beneficiarul stabilește clasificarea pentru solicitare. Beneficiarul va atașa scurta informație pentru a explica clasificarea efectuată. Beneficiarul va putea reclasifica solicitările plasate, în funcție de modificările în contextul aferent solicitărilor.

1. Furnizorul va presta servicii de suport în zilele lucrătoare conform legislației din R. Moldova, în intervalul de timp 08:00 – 18:00.

2. Nivelul serviciilor de suport prestate de furnizor trebuie să corespundă următoarelor cerințe:

Clasificarea solicitării plasate de Beneficiarul	Timpul de Răspuns (TR)	Timpul de Soluționare (TS)
Critică	5 min	60 min
Înaltă	60 min	Finele zilei
Ordinară	24h	3 zile
Joasă	3 zile	Cel mai bun efort*

** furnizorul va depune tot efortul în vederea soluționării cat mai rapide a solicitării pentru servicii, activând în regim normal. Timpul limita pentru soluționarea solicitării va fi comunicat și acceptat de Beneficiarul. Modificări ulterioare a timpului limita sunt permise doar cu acceptul Beneficiarul*.

5.2 Servicii de mentenanță

Nivelul serviciilor de mentenanță oferite de furnizor va corespunde următoarelor cerințe:

ID	Condiție	Cerință
CSP.10.	Obligator	Furnizorul va aplica o politică de minimizare a frecvenței de emitere a actualizărilor la nivelul aplicațiilor. Politica aplicată de furnizor va permite Beneficiarul să aplice noile actualizări lunar. Excepție pot fi actualizările destinate să înlăture probleme critice și de securitate la nivelul Sistemului.
CSP.11.	Obligator	Furnizorul va aplica o politica de neobligativitate a implementării noilor versiuni ale aplicațiilor. Politica aplicata de furnizor va permite Beneficiarul să implementeze noi versiuni ale aplicațiilor odată la trei ani.
CSP.12.	Obligator	Furnizorul va comunica Beneficiarul graficul său de emitere a actualizărilor și noilor versiuni. Pentru actualizări, furnizorul urmează să notifice Beneficiarul cu cel puțin o luna în prealabil. Pentru noile versiuni, furnizorul urmează să notifice Beneficiarul cu cel puțin 6 luni în prealabil.

<table>
<tr><th>ID</th><th>Condiție</th><th>Cerință</th></tr>
<tr><td>CSP.13.</td><td>Obligator</td><td>Pentru menținerea Sistemului în stare funcțională, Ofertantul poate efectua lucrări de mentenanță la nivelul componentelor TI aferente Sistemului. Tipul lucrărilor de mentenanță și angajamentele Ofertantului privind coordonarea acestora cu Beneficiarul, perioada și durata acestora sunt stabilite în tabelul de mai jos.
<table>
<tr><th>Tipul lucrărilor de mentenanță</th><th>Notificare Beneficiar</th><th>Perioadă și durată lucrări</th></tr>
<tr><td>Lucrări de mentenanță ordinare</td><td>Cu 5 zile în prealabil.</td><td>Sunt efectuate în afara perioadei de disponibilitate garantată pentru Sistem. Durata acestor lucrări nu va depăși 4 ore.</td></tr>
<tr><td>Lucrări de mentenanță majore</td><td>Cu 10 zile în prealabil.</td><td>Sunt efectuate în afara perioadei de disponibilitate garantată pentru Sistem. Durata acestor lucrări nu va depăși 24 ore.</td></tr>
<tr><td>Lucrări de mentenanță urgente</td><td>Cu notificarea imediat ce a apărut necesitatea inițierii lor.</td><td>Pot fi efectuate în orice perioadă. Durata acestora nu va depăși 2h.</td></tr>
</table></td></tr>
</table>

5.3 Servicii de dezvoltare

Nivelul serviciilor de dezvoltare oferite de furnizor va corespunde următoarelor cerințe:

ID	Condiție	Cerință
CSP.14.	Obligator	Furnizorul va reacționa la o solicitare de dezvoltare din partea Beneficiarul în maxim 3 zile.
CSP.15.	Obligator	Furnizorul va veni cu estimările de buget și conceptul soluției în maxim 10 zile.
CSP.16.	Obligator	Prestarea Serviciilor de dezvoltare se efectuează exclusiv în baza planului aprobat de Beneficiar privind prestarea Serviciilor de dezvoltare. În caz de necesitate planul de soluționare poate fi modificat, cu acordul Părților, fapt menționat în noul plan, care va conține referința la planul inițial
CSP.17.	Informativ	Serviciile respective vor fi prestate conform unui tarif fix per oră. Tariful per oră pornește de la premiza că Prestatorul va pune la dispoziția Beneficiarului, pentru perioada respectivă, toți specialiștii, în orice combinație, necesari pentru realizarea sarcinii puse. De asemenea specialiștii vor dispune de toate mijloacele materiale, nemateriale și organizatorice necesare realizării sarcinii.
CSP.18.	Informativ	Tariful trebuie să fie format reieșind din premiza că una și aceiași sarcină poate fi realizată de diferiți specialiști cu nivel diferit de calificare și respectiv costuri diferite. Beneficiarul optează pentru un termen mai îndelungat de realizare a modificărilor cu costuri mai mici.. Beneficiarul este conștient că în cazul respectiv nivelul de calificare a specialiștilor va influența durata de executare a sarcinii, dar acest fapt nu trebuie să influențeze calitatea rezultatului.
CSP.19.	Obligator	Un Serviciu de dezvoltare se consideră prestat în momentul confirmării acceptării soluției de către Persoana responsabilă din partea Beneficiarului.
CSP.20.	Obligator	Termenul de prestare a Serviciului de dezvoltare bugetat include doar timpul necesar Prestatorului colectării informației, documentării, analizei și prestării nemijlocite a serviciului și poate fi diferit de intervalul de timp total dintre momentul enunțului acestuia și acceptării rezultatului.
CSP.21.	Obligator	Furnizorul va livra soluția în timpul agreat cu Beneficiarul, aplicând principiul „the best effort”.
CSP.22.	Obligator	Furnizorul va permite Beneficiarul setarea priorităților pentru solicitările de dezvoltare și revizuirea ulterioară a acestora. Revizuirea priorităților solicitărilor va face posibilă revizuirea termenelor de livrare a soluțiilor de către furnizori.

6 MANAGEMENTUL SERVICIILOR DE SUPORT

ID	Condiție	Cerință
CSP.23.	Obligator	Prestarea serviciilor de către Furnizorul selectat către Beneficiarul se va face considerând standardele ISO 20000 și setul de practici ITIL v3.0. Furnizorul trebuie să dețină capacitatea de a interacționa cu Beneficiarul conform celor mai bune practici stabilite. De asemenea, trebuie să dețină procese și capabilități interne de a presta operațional conform practicilor menționate în domeniu.
CSP.24.	Obligator	Serviciile de suport vor fi prestate în baza unui Acord de prestare servicii, ce va fi anexa la Contractul semnat între Părți. Acordul va stabili nivelul serviciilor de suport și mentenanță post-implementare, în baza cerințelor incluse în acest caiet de sarcini.
CSP.25.	Obligator	Furnizorul va deține un Centru de suport clienți către care vor fi direcționate toate solicitările din partea Beneficiarului. Programul de lucru și organizarea activității Centrului de suport trebuie să asigure prestarea serviciilor de suport și mentenanță post-implementare la nivelul stabilit în acest caiet de sarcini.
CSP.26.	Obligator	Furnizorul trebuie să poată demonstra accesul în timp util a Centrului de suport la specialiști certificați de către producătorii soluțiilor aplicative furnizate.
CSP.27.	Obligator	Serviciile de suport vor fi prestate la distanță. La necesitate, specialiștii Furnizorului se vor deplasa la sediul Beneficiarul.
CSP.28.	Obligator	Pentru prestarea serviciilor de suport și mentenanță post-implementare, furnizorul va pune la dispoziția Beneficiarul o platforma aplicativă, disponibilă pentru Beneficiarul prin rețeaua Internet. Platforma aplicativa va fi adecvat securizata. Toate interacțiunile intre furnizor și Beneficiarul în cadrul prestării serviciilor de suport și mentenanță post-implementare se vor efectua prin intermediul platformei respective.
CSP.29.	Obligator	Furnizorul va monitoriza calitatea serviciilor de suport și mentenanță post-implementare și va reacționa la abaterile admise în vederea prevenirii acestora.
CSP.30.	Obligator	Furnizorul va prezenta rapoarte lunare către Beneficiarul privind serviciile prestate și nivelul acestora. Rapoartele vor conține și informație cu privire la acțiunile întreprinse de furnizor sau planificate, în vederea îmbunătățirii calității serviciilor.
CSP.31.	Obligator	Furnizorul va prezenta trimestrial către Beneficiarul actul de acceptanță a serviciilor de suport și mentenanță post-implementare. Actul de acceptanță va conține volumul și suma serviciilor prestate. Actul de acceptanță va fi însoțit de raportul privind serviciile prestate și nivelul acestora.
CSP.32.	Obligator	Plata serviciilor de suport și mentenanță post-implementare se va efectua trimestrial, după prestarea serviciilor, în baza actului de acceptanta și a raportului privind serviciile prestate.

6.1 Managementul schimbărilor

Toate modificările aferente sistemului de prestarea serviciilor de suport și mentenanță post-implementare vor fi gestionate conform unui proces matur de management al schimbărilor.

Următoarele sunt cerințele aferente procesului de management al schimbărilor.

ID	Condiție	Cerință
CSP.33.	Obligator	In oferta sa, ofertantul va include informație privind abordarea propusă pentru managementul schimbărilor la nivelul aplicațiilor.
CSP.34.	Obligator	Furnizorul va propune Beneficiarului procedura de management al schimbărilor aferente aplicațiilor. Procedura va fi coordonata și acceptata de Beneficiar.
CSP.35.	Obligator	Procedura de management al schimbărilor trebuie să prevadă cel puțin următoarele activități în responsabilitatea furnizorului: g. Testarea modificărilor în mediul de testare al furnizorului; h. Pregătirea planului de implementare a modificărilor; i. Pregătirea planului de roll back în cazul modificărilor eșuate;

ID	Condiție	Cerință
		j. Pregătirea documentației tehnice aferente modificărilor, inclusiv: scopul modificărilor, componente afectate, ghidul de implementare, ghidul de aplicare a planului de roll back, ghidul de follow-up al modificărilor; k. Pregătirea documentației tehnice detaliate aferente modificărilor. Documentația va include descrierea modificărilor, componentele afectate, instrucțiunile de instalare, planul de rollback în caz de eșec, procedurile de follow up pentru asigurarea implementării corecte a modificărilor; l. Actualizarea documentației utilizator și documentației tehnice aferente aplicațiilor și transmiterea acesteia către Beneficiar; m. Furnizarea pachetelor software aferente modificărilor. Furnizarea fișierelor ce conțin codul sursa aferent modificărilor. Autenticitatea și integritatea pachetelor software și a codului sursa trebuie să fie asigurata cu aplicarea semnăturii digitale a furnizorului (code signing); n. Reacționarea imediata în cazul depistării erorilor în modificările implementate și corectarea lor într-un timp cât mai scurt.
CSP.36.	Obligator	În procesul de menținere operațională și dezvoltare a Sistemului, Ofertantul urmează să efectueze un șir de modificări la nivelul componentelor aferente Sistemului (componente de sistem și soft aplicativ). Toate modificările efectuate de Ofertant la nivelul Sistemului vor fi implementate conform unui proces de comun agreat pentru managementul schimbărilor. Modificările ce pot avea impact semnificativ asupra parametrilor de calitate ai serviciului Sistemului vor fi autorizate de Beneficiar. Elemente obligatorii pentru acest tip de modificări, vor fi: • Testarea în mediul de testare; • Planul de implementare a modificării; • Planul de roll back; • Revizuirea post-implementare. Ofertantul va duce evidența tuturor modificărilor aferente Sistemului într-un Registru al modificărilor. Beneficiarul va avea acces de citire la acest Registru.

6.2 Asigurarea calității

Calitatea serviciilor de suport și mentenanță post-implementare influențează în mod direct calitatea utilizării aplicațiilor de către Beneficiarul. Furnizorul trebuie să poată demonstra ca aceste servicii vor fi prestate la nivelele stabilite.

ID	Condiție	Cerință
CSP.37.	Obligator	Furnizorul va prezenta la început de an un plan de asigurare a calității serviciilor de suport și mentenanță post-implementare. Planul va conține indicatorii de performanta pentru servicii, riscurile ce pot afecta indicatorii de performanta, acțiunile preventive implementate pentru gestiunea riscurilor și masurile de mitigare a riscurilor reziduale. Planul prezentat de furnizor trebuie să fie ulterior acceptat de Beneficiar. Planul de calitate va fi revizuit de furnizor cel puțin anual, sau în cazurile în care se vor constata abateri importante în prestarea serviciilor la nivelul stabilit.
CSP.38.	Obligator	Ofertantul va include în oferta informație privind abordarea să în privința planului de asigurare a calității serviciilor de suport și mententanță post-implementare.
CSP.39.	Obligator	Furnizorul va efectua auditări anuale a capabilității sale de a presta servicii de suport și mentenanță post-implementare la nivelul stabilit. Auditările trebuie să fie efectuate de entități independente în raport cu furnizorul. Metodologia de audit aplicata trebuie să fie aliniata la cele mai bune practici în domeniu (ex. SAS 70, ITIL, standarde ISACA, etc.). Rapoartele de audit vor fi prezentate către Beneficiar, împreuna cu planurile de acțiuni pentru remedierea neajunsurilor identificate de auditor.

ID	Condiție	Cerință
CSP.40.	Obligator	Ofertantul trebuie să elaboreze și să mențină în stare actuală un plan de calitate al serviciilor de menținere operațională a Sistemului. Planul trebuie să considere următoarele categorii de riscuri: • Riscuri operaționale (pierderea capacității Ofertantului de a presta la nivelul stabilit, riscuri la nivelul proceselor interne ale Ofertantului); • Riscuri tehnologice (riscuri ce pot afecta disponibilitatea, accesibilitatea, performanța și securitatea Sistem). Planul de calitate trebuie să conțină informație detaliată despre riscurile identificate, măsurile ce vor fi implementate de Ofertant în vederea prevenirii acestora, riscurile reziduale și măsurile de reacție planificate în cazul realizării riscurilor reziduale. Planul de calitate urmează să fie actualizat cel puțin anual, sau la orice schimbare majoră la nivelul componentelor Sistem sau la nivelul proceselor aferente menținerii Sistemului. Ofertantul va prezenta Beneficiarului Planul de calitate în ultima să actualizare. La etapa de prezentare a ofertei, Ofertantul trebuie să descrie cum va produce Planul de calitate al serviciilor. Oferta va avea un avantaj competitiv dacă Ofertantul anexează la aceasta Planul de calitate, iar acesta corespunde necesităților Beneficiarului.

6.3 Garanții de performanță (Performance warranties)

ID	Condiție	Cerință
CSP.41.	Informativ	Beneficiarul poate solicita garantarea serviciilor prin prezentarea unei scrisori de garanție bancară pentru prestarea la nivelul agreat a serviciilor de suport și mentenanță post-implementare.

6.4 Soluționarea divergențelor

Orice divergențe ivite între Părți vor fi soluționate cu efort comun și prin strânsă conlucrare între Părți. În acest scop, vor fi aplicate următoarele reguli:

1) Părțile vor forma 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.

2) La necesitate, părțile vor pregăti probele electronice relevante pentru aspectele ce au devenit obiect de divergență.

3) Grupul de lucru se va convoca și va examina subiectul divergențelor și probele existente la subiect. Părțile vor aplica prevederile Contractului și prezentele Reguli în scopul clarificării tuturor aspectelor disputate și identificării unei soluții echitabile pentru divergențele ivite. În acest scop, pot fi ascultate, sau obținute în scris, opiniile membrilor externi, convocați în grupul de lucru, precum și rezultatele de expertiză ale probelor electronice existente.

4) Concluzia grupului de lucru va fi fixată în baza unui proces - verbal, semnat de membrii grupului de lucru din partea ambelor părți.

Identificarea unei soluții echitabile pentru ambele Părți, în limite angajamentelor asumate ale Părților, este preferabilă în toate situațiile de divergență. În cazul în care o asemenea soluție nu poate fi identificată, părțile vor aplica prevederile Contractului pentru soluționarea litigiilor.

6.5 Raportarea privind nivelul serviciilor

Se optează pentru prestarea transparentă a Serviciilor. În acest scop, Prestatorul va prezenta cu regularitate Beneficiarului rapoarte privind conținutul și nivelul Serviciilor acordate.

ID	Condiție	Cerință
CSP.42.	Informativ	Ofertanții vor formula propuneri privind conținutul rapoartelor de monitorizare a serviciilor. Structura rapoartelor respective este stabilită de Prestator.

<table>
<tr><td>CSP.43.</td><td>Informativ</td><td>Rapoartele prezentate, regularitatea și modalitatea de prezentare a acestora, este stabilită în tabelul de mai jos.
<table>
<tr><th>Tip raport</th><th>Conținut</th><th>Destinație</th><th>Regularitatea</th></tr>
<tr><td>Raport privind volumul serviciilor</td><td>Tipul solicitării, durata soluționării și tarifele aplicate.</td><td>Raportul este prezentat în scopul asigurării transparenței privind prestarea Serviciilor la nivelul agreat de Prestator.</td><td>Lunar, în formă electronică.
La solicitarea Beneficiarului, pe suport de hârtie.</td></tr>
<tr><td>Raport privind solicitările de modificare</td><td>Propunerile de modificare a Serviciilor</td><td>Raportul este prezentat în scopul asigurării transparenței dezvoltării SIF.</td><td>Lunar, în formă electronică.
La solicitarea Beneficiarului, pe suport de hârtie.</td></tr>
<tr><td>Raport privind nivelul serviciilor.</td><td>Nivelul de disponibilitate a SGPE, întreruperi planificate, incidente raportate, solicitări de suport.</td><td>Raportul este prezentat în scopul asigurării transparenței privind prestarea serviciilor la nivelul agreat de Prestator.</td><td>Lunar, în formă electronică, disponibil în Sistemul Service Desk.
La solicitarea Beneficiarului, pe suport de hârtie.</td></tr>
</table></td></tr>
</table>

6.6 Securitatea informației

ID	Condiție	Cerință
CSP.44.	Obligator	Ofertantul trebuie să conlucreze și să coopereze în vederea gestiunii proactive a riscurilor de securitate a informației ce pot afecta serviciile Prestatorului și sistemele Beneficiarului, dependente de serviciile Prestatorului.
CSP.45.	Obligator	Prestatorul este responsabil pentru securitatea tehnologică și funcțională a sistemelor informatice supuse mentenanței, în limitele sarcinilor de mentenanță îndeplinite
CSP.46.	Obligator	Beneficiarul este responsabil pentru utilizarea securizată a serviciilor oferite de Prestator.
CSP.47.		În cazul unui incident de securitate a informației, partea ce a constatat incidentul va notifica imediat și cealaltă parte, dacă aceasta poate fi de asemenea afectată de incident. Părțile vor coordona măsurile necesar a fi întreprinse în scopul diminuării impactului incidentului și soluționării acestuia.
CSP.48.		La solicitarea Beneficiarului, Presatorul va întreprinde acțiunile de rigoare în scopul colectării și conservării probelor ce pot fi necesare la investigarea incidentului și la probarea juridică a responsabilității pentru incident. În acest scop, Prestatorul, la solicitarea Beneficiarului, poate efectua: - Colectarea și conservarea fișierelor log ce conțin informația privind accesul la nivelul componentelor de rețea; - Efectuarea copiilor de rezervă depline pentru sistemele informatice supuse mentenanței, stocarea acestora în condiții ce asigură integritatea copiilor de rezervă efectuate; - Întocmirea proceselor - verbale cu participarea a cel puțin 3 specialiști din partea Prestatorului, privind efectuarea copiilor de rezervă. Prezența reprezentanților Beneficiarului este solicitată; Menținerea formală a Registrului privind deținerea probelor conservate (chain of custody).
CSP.49.		După soluționarea unui incident de securitate, părțile vor întocmi rapoarte individuale privind gestiunea incidentului. De comun acord vor întocmi un plan de acțiuni pentru prevenirea repetării incidentelor similare.

7 TERMINAREA CONTRACTULUI

În cazul în care părțile decid să nu prelungească contractul pentru servicii de suport și mentenanță post-implementare, afacerea Beneficiarul nu trebuie să fie afectată. Beneficiarul trebuie să dețină posibilitatea de a contracta un alt furnizor sau să preia intern suportul și menținerea aplicațiilor.

ID	Condiție	Cerință
CSP.50.	Obligator	În cazul în care se preconizează pierderea efectului contractului pentru servicii de suport și mentenanță post-implementare, furnizorul trebuie să asigure cel puțin: a. Toata documentația aferentă aplicațiilor este actualizată și transmisă către Beneficiar; b. Toate înregistrările aferente solicitărilor Beneficiarului efectuate pe partea furnizorului (pentru incidente, probleme, consultanta, modificări, dezvoltări, etc.) sunt exportate în format comun (ex. CSV, XLS) și transmise către Beneficiar; c. Furnizorul va păstra pentru un termen de un an calendaristic toate înregistrările produse pe parcursul prestării serviciilor, codurile sursă și documentația aferentă aplicațiilor.
CSP.51.	Obligator	Pentru un termen de un an calendaristic după expirarea contractului de suport, furnizorul va fi dispus să coopereze cu terțe părți autorizate de Beneficiar, în vederea prestării către Beneficiar a serviciilor de suport și mentenanță post-implementare. In acest scop furnizorul va asigura cel puțin furnizarea oricărei informații deținute ce ar ajuta la îmbunătățirea serviciilor.
CSP.52.	Obligator	Ofertantul va include în oferta sa informație cu privire la abordarea propusă pentru încetarea serviciilor de suport și menținerea post-implementarea, ținând cont de cerințele și necesitățile Beneficiarului.
CSP.53.	Obligator	Contractul semnat în baza acestui concurs de achiziții urmează să fie pentru un termen de 24 luni. Oricare din părți poate în orice moment solicita rezilierea contractului semnat. În acest scop, partea ce dorește rezilierea contractului va notifica cealaltă parte despre intenția să cu cel puțin 3 luni în prealabil.
CSP.54.	Obligator	Toate datele păstrate în bazele de date aferente Sistemului sunt proprietatea Beneficiarului. În cazul rezilierii contractului, Ofertantul urmează să pună la dispoziția Beneficiarului o procedură de export al datelor într-un format de comun agreat cu Beneficiarul. Formatul selectat trebuie să permită Beneficiarului importul integral al datelor în cadrul altor soluții similare soluției pentru Sistem a Ofertantului.
CSP.55.	Obligator	Softul aplicativ aferent Sistemului este furnizat de Ofertant și constituie proprietatea intelectuală a acestuia pentru toată perioada de prestare a serviciilor. Beneficiarul obține dreptul de utilizare neexclusivă pe termen nelimitat a softului aplicativ, fără drept de multiplicare și distribuire, în următoarele situații: - Contractul este reziliat în rezultatul nerespectării de către Ofertant a obligațiunilor și angajamentelor sale; - Termenul de valabilitate al contractului a expirat. La semnarea contractului, părțile vor semna un acord adițional de tipul ”Escrow agreement”, ce va stabili modul în care codul sursă ajunge în posesia Beneficiarului în situațiile menționate. Costurile aferente implementării acordului de tipul ”Escrow agreement” sunt suportate de Ofertant.