AUTORITATEA NAȚIONALĂ PENTRU SOLUȚIONAREA CONTESTAȚIILOR

SIMED

Sistem Informațional pentru Managementul Electronic al Documentelor

TABEL DE CONȚINUT

Tabelul 1.1. prezintă acronimele și abrevierile utilizate în prezentul document.

Tabelul 1. Acronime și abrevieri utilizate în prezentul document.

Nr.	Abreviere/Acronim	Explicație
1	ToR	Termeni de Referință
2	ANSC	Autoritatea Națională pentru Soluționarea Contestațiilor
3	AGE	Agenția de Guvernare Electronică
4	FOD	Cadrul tehnologic guvernamental reutilizabil destinat dezvoltării și furnizării componentelor Front Office ale serviciilor electronice
5	PDSE	Platforma de dezvoltare a serviciilor electronice
6	PSP	Portalul Serviciilor Publice
7	MF	Ministerul Finanțelor
8	SFS	Serviciul Fiscal de Stat
9	CTIF	Centrul de Tehnologii Informaționale în Finanțe
10	AC	Autoritate contractantă
11	AP	Achiziție publică
12	DJ	Direcția Juridică
13	DTISD	Direcția tehnologii informaționale, statistică şi documentare
14	DSC	Decizie de soluționare a contestației
15	CSC	Complet de soluționare a contestației
16	STISC	Serviciul Tehnologia Informației și Securitate Cibernetică
17	MPass	Serviciul guvernamental de autentificare și control al accesului
18	MSign	Serviciul guvernamental de semnătură electronică
19	MConnect	Platforma guvernamentala de interoperabilitate și schimb de date
20	MCloud	Infrastructură informațională guvernamentală comună
21	MTender	Platforma națională de achiziții publice
22	MLog	Serviciul electronic guvernamental de jurnalizare
23	MNotify	Serviciul guvernamental de notificare electronică
24	MPay	Serviciul Guvernamental de plăti electronice
25	MDelivery	Serviciul guvernamental de livrare electronică a documentelor
26	API	Application Programming Interface – interfață de programare a aplicațiilor
27	CPV	Common Procurement Vocabulary (Vocabular Comun al Achizițiilor)

28	RBAC	Role-Based Access Control – controlul accesului bazat pe roluri
29	PDF/A	Portable Document Format for Archiving
30	UX/UI	User Experience / User Interface (Experiența Utilizatorului / Interfață Utilizator)
31	.NET	Platformă tehnologică utilizată pentru dezvoltarea componentelor aplicaționale ale SIMED și pentru asigurarea compatibilității cu FOD/PDSE
32	PO	Procedură operațională
33	SSD	Document de proiectare software
34	TLS/SSL	Transport Layer Security/Secure Sockets Layer

1. SCOPUL DOCUMENTULUI

Prezentul document definește Termenii de Referință pentru proiectarea, configurarea, adaptarea, dezvoltarea, integrarea, testarea, implementarea și punerea în funcțiune a Sistemului Informațional de Management Electronic al Documentelor în cadrul Autorității Naționale pentru Soluționarea Contestațiilor.

Documentul stabilește cadrul funcțional, tehnic, arhitectural și operațional necesar digitalizării integrate a proceselor administrative, documentare și decizionale ale ANSC, cu accent pe gestionarea electronică a întregului ciclu de viață al contestațiilor în domeniul achizițiilor publice, achizițiilor sectoriale și concesiunilor.

SIMED va fi realizat în baza principiului reutilizării prioritare a soluțiilor și componentelor guvernamentale existente. Componenta destinată interacțiunii cu utilizatorii externi – inclusiv contestatari, autorități contractante, operatori economici câștigători și alte părți interesate – va fi implementată prin reutilizarea, configurarea, adaptarea și, după caz, extinderea funcționalităților disponibile în cadrul platformei FOD/PDSE.

Dezvoltarea unor funcționalități noi pentru componenta Front Office va fi realizată numai în măsura în care cerințele funcționale specifice SIMED nu pot fi acoperite prin configurarea sau adaptarea componentelor FOD/PDSE existente. Necesitatea dezvoltării unor asemenea funcționalități va fi fundamentată printr-o analiză de decalaj, elaborată de Contractant, aprobată de ANSC și coordonată, după caz, cu Agenția de Guvernare Electronică.

Componenta instituțională Back Office a SIMED va fi configurată, adaptată și dezvoltată în conformitate cu fluxurile operaționale, procesele de lucru, competențele instituționale și regulile procedurale specifice ANSC. Aceasta va constitui nucleul operațional al sistemului și va asigura gestionarea documentelor, dosarelor, sarcinilor, termenelor, ședințelor, completelor de soluționare a contestațiilor, proiectelor de decizie, actelor procesuale și registrelor instituționale.

SIMED va asigura digitalizarea integrală și trasabilă a următoarelor procese:

- depunerea, recepționarea și înregistrarea contestațiilor;
- constituirea și gestionarea dosarului electronic al contestației;
- verificarea formală, repartizarea și examinarea contestațiilor;
- constituirea și administrarea completelor de soluționare;
- gestionarea conflictelor de interese, declarațiilor de abținere și cererilor de recuzare;

- organizarea și desfășurarea ședințelor;
- întocmirea, avizarea, semnarea și emiterea documentelor procesuale și a deciziilor;
- comunicarea electronică cu părțile implicate;
- publicarea informațiilor și documentelor de interes public;
- raportarea, analiza, auditarea și arhivarea dosarelor.

Sistemul va fi integrat în ecosistemul guvernamental de servicii electronice și va reutiliza, după caz, serviciile guvernamentale partajate, inclusiv MPass, MSign, MLog, MNotify, MDelivery, MPay, MPower, MConnect, MCloud, MCabinet și Portalul Serviciilor Publice, precum și datele și serviciile disponibile prin SIA RSAP/MTender și registrele de stat relevante.

Prezentul document constituie referința obligatorie pentru Autoritatea contractantă, Contractant, instituțiile implicate în integrarea sistemului, echipele tehnice, utilizatorii finali și celelalte părți participante la proiect. Acesta stabilește obiectivele, domeniul de aplicare, cerințele funcționale și nefuncționale, responsabilitățile, etapele de implementare, livrabilele și criteriile de acceptanță aplicabile SIMED.

1.1.Conținutul documentului

Documentul este structurat în mod logic și coerent pentru a acoperi toate componentele esențiale necesare fundamentării, proiectării și implementării Sistemului Informațional de Management Electronic al Documentelor (SIMED) în cadrul Autorității Naționale pentru Soluționarea Contestațiilor (ANSC). Conținutul este organizat astfel încât să ofere o înțelegere completă și detaliată asupra cerințelor și direcțiilor tehnico-funcționale ale viitorului sistem informațional.

În mod particular, documentul include:

- **Obiectivele sistemului** – definirea clară a finalităților urmărite prin dezvoltarea SIMED, cu accent pe eficientizarea fluxurilor documentare, digitalizarea procesului de soluționare a contestațiilor și îmbunătățirea trasabilității decizionale;
- **Arhitectura și infrastructura sistemului** – prezentarea arhitecturii funcționale, logice și tehnice a SIMED, bazată pe separarea componentelor Front Office și Back Office, reutilizarea cadrului și funcționalităților FOD/PDSE, expunerea controlată a interfețelor API, comunicarea bazată pe mesaje și integrarea cu serviciile guvernamentale partajate, SIA RSAP/MTender și registrele de stat relevante. Secțiunea include cerințele privind infrastructura MCloud, mediile de execuție containerizate, securitatea, disponibilitatea, scalabilitatea și continuitatea operațională.;
- **Cerințe funcționale și nefuncționale** – descrierea funcționalităților necesare gestionării contestațiilor, documentelor, dosarelor, deciziilor, ședințelor, comunicărilor și registrelor SIMED, precum și a cerințelor privind arhitectura bazată pe FOD/PDSE, stiva tehnologică compatibilă, securitatea, interoperabilitatea, performanța, disponibilitatea, scalabilitatea, mentenabilitatea, accesibilitatea și conformitatea cu standardele guvernamentale aplicabile;
- **Etapele de implementare** – tructurarea procesului de realizare a SIMED în etape succesive și controlabile, incluzând analiza componentelor FOD/PDSE existente, analiza de decalaj, proiectarea arhitecturii țintă, configurarea și adaptarea componentelor reutilizate, dezvoltarea funcționalităților specifice ANSC, integrarea, migrarea datelor, testarea, acceptanța, implementarea în MCloud și punerea în funcțiune;

- **Livrarea și mentenanța post-implementare** – stabilirea parametrilor pentru livrarea produsului final, a documentației aferente și a suportului tehnic, inclusiv cerințele de întreținere corectivă, adaptivă și preventivă în perioada de garanție;
- **Analiza riscurilor și planul de atenuare** – identificarea principalelor riscuri tehnice, instituționale sau de interoperabilitate și definirea măsurilor proactive de gestionare și răspuns, pentru a asigura continuitatea și stabilitatea operațională a sistemului.

Această structură avansată servește drept referință pentru toate părțile implicate în dezvoltarea SIMED și oferă suportul necesar pentru elaborarea ulterioară a documentației de achiziții și management de proiect.

1.2.Rolul ToR în procesul de achiziție

Termenii de Referință constituie componenta tehnico-funcțională principală a documentației de atribuire și reprezintă cadrul obligatoriu pentru selectarea unui operator economic responsabil de analiza, proiectarea, configurarea, adaptarea, extinderea, dezvoltarea, integrarea, testarea, implementarea și punerea în funcțiune a Sistemului Informațional de Management Electronic al Documentelor.

Obiectul achiziției nu presupune dezvoltarea izolată și integrală de la zero a tuturor componentelor SIMED. Contractantul va reutiliza și adapta funcționalitățile disponibile în cadrul FOD/PDSE pentru componenta de interacțiune cu utilizatorii externi și va configura și dezvolta componentele Back Office în conformitate cu procesele și regulile procedurale specifice ANSC.

Din perspectivă procedurală, ToR-ul are rolul de a traduce necesitățile instituționale și cerințele de modernizare digitală într-un set de specificații clare, exhaustive și verificabile, care stau la baza formulării ofertelor tehnice și financiare. Acesta permite alinierea formală a cadrului de referință între autoritatea contractantă și potențialii ofertanți, facilitând astfel un proces de achiziție previzibil, eficient și lipsit de ambiguități.

Prin delimitarea exactă a obiectivelor urmărite, a constrângerilor tehnologice, a cerințelor de interoperabilitate, securitate, mentenanță post-implementare și livrabile aferente, Termenii de Referință permit:

- verificarea conformității soluțiilor propuse cu principiul reutilizării componentelor guvernamentale existente și excluderea propunerilor care generează costuri suplimentare nejustificate prin dezvoltarea repetată a unor funcționalități disponibile în FOD/PDSE;
- **asigurarea comparabilității tehnice** între ofertele depuse, prin standardizarea cerințelor minime obligatorii și a formatului de răspuns;
- **filtrarea propunerilor neconforme** sau substandard, prin introducerea unor criterii clare de eligibilitate și performanță minimă acceptată;
- **susținerea transparenței și legalității** în procesul decizional, printr-un cadru de referință unic, accesibil și ușor de auditat;
- **alocarea riguroasă a riscurilor contractuale**, prin clarificarea responsabilităților și a condițiilor de livrare, testare, garanție și suport.

În mod particular, pentru ANSC, ToR-ul are și un rol strategic în corelarea nevoilor funcționale specifice (ex. digitalizarea procesului de soluționare a contestațiilor, trasabilitate decizională, integrarea cu MTender și alte platforme guvernamentale) cu soluțiile tehnologice moderne propuse de piață. Astfel, acesta

devine un mecanism de **orchestrare a cererii instituționale**, în care sunt articulate nu doar parametrii tehnici, ci și viziunea pe termen lung a instituției privind transformarea digitală, interoperabilitatea interinstituțională și conformitatea cu standardele europene de e-guvernare.

ToR-ul sprijină, de asemenea, componenta de evaluare a ofertelor, oferind un cadru obiectiv pentru punctarea soluțiilor propuse în funcție de relevanță, scalabilitate, valoare adăugată și sustenabilitate tehnologică. În acest mod, documentul contribuie direct la **asigurarea raportului optim calitate–preț** în utilizarea resurselor publice, respectând principiile de eficiență, transparență, concurență și nediscriminare prevăzute de legislația națională și europeană în domeniul achizițiilor publice.

1.3.Rolul ANSC în contextul inițiativei de digitalizare

ANSC este autoritatea publică autonomă, învestită cu competență exclusivă în examinarea și soluționarea contestațiilor aferente procedurilor de achiziții publice, achiziții sectoriale și concesiuni din Republica Moldova. În calitate de mecanism de apel administrativ specializat, ANSC deține un rol esențial în arhitectura națională de guvernanță a achizițiilor, asigurând aplicarea riguroasă a principiilor de legalitate, transparență procedurală, tratament egal, nediscriminare și concurență loială.

Prin exercitarea funcțiilor sale, Agenția oferă operatorilor economici un instrument formal, eficient și accesibil de revizuire administrativă a deciziilor emise de autoritățile contractante, contribuind astfel la corectarea eventualelor derapaje procedurale și la asigurarea unui cadru previzibil și echitabil pentru participarea la procedurile de achiziție. Deciziile ANSC sunt executorii și obligatorii, având forță juridică în relația cu părțile implicate și impact direct asupra validității procedurilor vizate.

În acest context, funcționarea transparentă, independentă și eficientă a ANSC constituie un element critic pentru consolidarea statului de drept, promovarea bunei guvernanțe și întărirea încrederii în integritatea sistemului de achiziții publice. De asemenea, aceasta reprezintă un vector important în procesul de armonizare a cadrului național cu standardele europene și cu acquis-ul comunitar, contribuind la asigurarea unei piețe publice competitive, corecte și sustenabile.

Soluționarea eficientă, transparentă și echitabilă a contestațiilor în domeniul achizițiilor publice reprezintă o componentă fundamentală a arhitecturii instituționale moderne, contribuind direct la menținerea integrității procesului de achiziție și la garantarea accesului operatorilor economici la remedii administrative eficiente. În acest context, Agenția Națională pentru Soluționarea Contestațiilor (ANSC), în calitate de autoritate publică cu atribuții exclusive în examinarea căilor de atac, se confruntă cu nevoia stringentă de a moderniza infrastructura sa informațională prin automatizarea completă a proceselor decizionale și documentare.

În forma actuală, fluxul de lucru asociat examinării contestațiilor este caracterizat printr-o combinație de procese manuale și suport digital fragmentar, ceea ce generează dificultăți în asigurarea trasabilității deciziilor, uniformității actelor emise, precum și în eficientizarea interacțiunii cu părțile implicate. Persistența formatelor nestructurate, lipsa standardizării documentare și limitările de interoperabilitate reduc scalabilitatea funcțională a instituției și cresc riscul erorilor de procesare.

Necesitatea creării Sistemului Informațional de Management Electronic al Documentelor (SIMED) derivă din cerința strategică de a transforma ANSC într-o instituție complet digitalizată, orientată spre eficiență decizională, guvernanță electronică și servicii centrate pe utilizator. Noul sistem va automatiza

integral circuitul procedural, de la recepția electronică a contestațiilor și agregarea datelor relevante, până la generarea automată a proiectelor de decizie și emiterea actelor finale cu valoare juridică.

Elementele definitorii ale justificării sistemului includ:

- **Digitalizarea completă a procesului decizional**: SIMED va integra un modul specializat de întocmire/generare automată a proiectelor de decizie ale Completelor de Soluționare a Contestațiilor (CSC), utilizând șabloane parametrizabile, logici prestabilite de prelucrare și date preluate contextual din dosarul digital al contestației;
- **Automatizarea și standardizarea actelor administrative**: toate documentele procesuale instituționale (procese-verbale, scrisori, ordine, puncte de vedere, notificări, decizii) vor fi convertite în formulare electronice structurate, completabile automat, validate juridic prin integrarea cu serviciile de semnătură electronică MSign și de notificare MNotify;
- **Crearea dosarului digital complet al contestației**: sistemul va agrega toate informațiile aferente unei contestații – documente justificative, metadate, istoric procedural – într-o entitate digitală unitară, accesibilă în funcție de roluri și drepturi definite;
- **Interoperabilitate extinsă cu platformele guvernamentale**: prin sincronizare bidirecțională cu MTender și interfețe API standardizate cu MPass, MConnect, MLog și registrele de interes public, se va asigura completarea automată a datelor aferente procedurilor de achiziție publică, validarea identității utilizatorilor și trasabilitatea documentelor.

SIMED va contribui substanțial la profesionalizarea procesului de examinare a contestațiilor prin:

- **Reducerea semnificativă a timpilor de procesare și redactare a actelor**;
- **Eliminarea erorilor umane și discrepanțelor documentare prin validări automate și controale de coerență**;
- **Creșterea capacității instituționale de răspuns în perioade de suprasolicitare (ex. campanii de achiziții sau alegeri)**;
- **Facilitarea auditului instituțional, a raportării și a arhivării conforme cu cerințele Legii nr. 467/2003 și ale altor acte normative relevante**.

Astfel, crearea sistemului nu reprezintă doar un pas tehnologic, ci o transformare instituțională majoră, menită să alinieze ANSC la standardele europene de e-Procurement, să consolideze rolul său ca garant al legalității în achiziții și să contribuie activ la modernizarea administrației publice din Republica Moldova.

Transformarea digitală a ANSC prin intermediul SIMED va fi realizată în conformitate cu principiul reutilizării infrastructurilor, platformelor și componentelor guvernamentale existente. În acest sens, componenta de interacțiune cu utilizatorii externi va fi implementată prin adaptarea funcționalităților disponibile în cadrul FOD/PDSE, iar componenta instituțională Back Office va fi configurată și dezvoltată în funcție de fluxurile operaționale, procesele de lucru și regulile procedurale specifice ANSC.

Prin această abordare, SIMED nu va constitui o soluție tehnologică izolată, ci o componentă integrată a ecosistemului digital guvernamental, interoperabilă cu serviciile electronice partajate, infrastructura MCloud, SIA RSAP/MTender și registrele de stat relevante. Reutilizarea componentelor existente va contribui la reducerea costurilor de dezvoltare și mentenanță, la accelerarea implementării, la uniformizarea experienței utilizatorilor și la creșterea sustenabilității tehnologice a sistemului.

1.4. Referințe și aspecte juridice

Proiectarea, dezvoltarea, implementarea și operarea Sistemului Informațional de Management Electronic al Documentelor în cadrul Autorității Naționale pentru Soluționarea Contestațiilor se va realiza în deplină conformitate cu legislația națională aplicabilă, respectând cele mai înalte standarde în materie de guvernanță digitală, securitate cibernetică și management al proceselor administrative publice.

A. Cadrul legislativ primar (achiziții publice și funcționarea ANSC)

1. Legea nr. 131 din 03.07.2015 privind achizițiile publice, cu modificările și completările ulterioare;
2. Legea nr. 121 din 05.07.2018 cu privire la concesiunile de lucrări și concesiunile de servicii;
3. Legea nr. 74 din 21.05.2020 privind achizițiile în sectoarele energeticii, apei, transporturilor și serviciilor poștale;
4. Hotărârea Parlamentului nr. 271 din 15.12.2016 cu privire la instituirea, organizarea și funcționarea Autorității Naționale pentru Soluționarea Contestațiilor;
5. Hotărârea Guvernului nr. 705 din 11.07.2018 cu privire la aprobarea conceptului tehnic al Sistemului Informațional Automatizat "Registrul de Stat al Achizițiilor Publice" (MTender);
6. Hotărârea Guvernului nr. 339 din 26.05.2017 pentru aprobarea Regulamentului cu privire la Dicționarul comun al achizițiilor publice (CPV).
7. Ordinele și reglementările aprobate de ANSC în aplicarea legislației privind contestațiile.

B. Reglementări tehnice privind infrastructura TIC guvernamentală și interoperabilitatea

8. Hotărârea Guvernului nr. 1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass);
9. Hotărârea Guvernului nr. 128/2014 privind platforma tehnologică guvernamentală comună (MCloud);
10. Hotărârea Guvernului nr. 405/2014 privind serviciul electronic guvernamental integrat de semnătură electronică (MSign);
11. Hotărârea Guvernului nr. 708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog);
12. Hotărârea Guvernului nr. 414/2018 privind măsurile de consolidare a centrelor de date în sectorul public și raționalizarea administrării sistemelor informaționale de stat;
13. Hotărârea Guvernului nr. 211/2019 privind platforma de interoperabilitate (MConnect);
14. Hotărârea Guvernului nr. 376/2020 privind serviciul guvernamental de notificare electronică (MNotify);
15. Hotărârea Guvernului nr. 656 din 05.09.2012 pentru aprobarea Programului privind Cadrul de Interoperabilitate;
16. Hotărârea Guvernului nr. 717/2014 privind platforma de dezvoltare a serviciilor electronice, inclusiv prevederile aplicabile reutilizării, configurării și adaptării funcționalităților Platformei de dezvoltare a serviciilor electronice;
17. Hotărârea Guvernului nr. 544/2019 pentru aprobarea Metodologiei de coordonare a achizițiilor în domeniul tehnologiei informației și comunicațiilor, inclusiv cerințele privind coordonarea documentației tehnice și a investițiilor TIC cu Agenția de Guvernare Electronică;

18. Hotărârea Guvernului nr. 677 din 08.10.2025 cu privire la consolidarea accesului la serviciile publice electronice în cadrul Portalului guvernamental integrat EVO utilizat la prestarea serviciilor publice electronice și aprobarea măsurilor necesare pentru implementarea Modelului Unitar de Design.

C. Reglementări privind securitatea informațională și protecția datelor

19. Hotărârea Guvernului nr. 1123/2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal;
20. Hotărârea Guvernului nr. 201/2017 privind cerințele minime obligatorii de securitate cibernetică pentru autoritățile publice;
21. Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal;
22. Ordinul Ministerului Tehnologiei Informației și Comunicațiilor nr. OMDI78/2006 privind aprobarea reglementării tehnice RT 38370656-002:2006 - Software Life Cycle Processes.
23. Standardul Republicii Moldova SM ISO/IEC/IEEE 14764:2022 - Inginerie software. Procese ale ciclului de viață al software-ului. Întreținere.
24. Standardul Republicii Moldova SM EN ISO/IEC 27001:2017 - Tehnologia informației. Tehnici de securitate. Sisteme de management al securității informației.
25. Standardul Republicii Moldova SM EN ISO/IEC 27002:2017 - Tehnologia informației. Tehnici de securitate. Cod de practică pentru controlul securității informației.
26. Standardul Republicii Moldova SM ISO/IEC 15408-1:2022 - Securitatea informației, securitatea cibernetică și protecția vieții private. Criterii de evaluare pentru securitatea IT. Partea 1: Introducere și model general.
27. Standardul Republicii Moldova SM ISO/IEC 15408-2:2022 - Securitatea informației, securitatea cibernetică și protecția vieții private. Criterii de evaluare pentru securitatea IT. Partea 2: Componente funcționale de securitate.
28. Standardul Republicii Moldova SM ISO/IEC 15408-3:2022 - Securitatea informației, securitatea cibernetică și protecția vieții private. Criterii de evaluare pentru securitatea IT. Partea 3: Componente de asigurare a securității;
29. Michael O. Leavitt, Ben Shneiderman, Research-Based Web Design & Usability Guidelines, https://www.usability.gov/sites/default/files/documents/guidelines_book.pdf;
30. World Wide Web Consortium (W3C) Recomandări privind calitatea conținutului paginilor web, vizualizarea corectă a informațiilor cu ajutorul browserelor de internet larg răspândite și compatibilitatea cu diferite platforme informatice (http://www.w3c.org);
31. Recomandările WCAG (Web Content Accessibility Guidelines) http://www.w3.org/TR/WCAG21/.

D. Documente de coordonare și conformitate instituțională

32. Avizul Agenției de Guvernare Electronică nr. 3011-609 din 12.06.2026 privind coordonarea Caietului de Sarcini/Termenilor de Referință pentru dezvoltarea Sistemului Informațional pentru Managementul Electronic al Documentelor;
33. Documentația tehnică, standardele, ghidurile de integrare și cerințele de reutilizare aferente FOD/PDSE, puse la dispoziție de Agenția de Guvernare Electronică pe parcursul implementării proiectului;

34. Documentația tehnică și condițiile de integrare aferente serviciilor guvernamentale MPass, MSign, MLog, MNotify, MDelivery, MPay, MPower, MConnect, MCabinet și celorlalte servicii guvernamentale utilizate de SIMED.

1.5. Principiile directoare ale dezvoltării SIMED în cadrul ANSC

- **Principiul legalității și conformității reglementare**: Dezvoltarea sistemului va respecta în mod riguros cadrul normativ național și angajamentele internaționale ale Republicii Moldova, inclusiv cele privind achizițiile publice, guvernanța digitală, protecția datelor cu caracter personal și interoperabilitatea administrativă. Codificarea logicii de afaceri în sistem va reflecta fidel prevederile legale, deciziile autorităților și normele metodologice aplicabile în activitatea ANSC.

- **Principiul digitalizării procesului end-to-end**: SIMED va acoperi digital întreg lanțul procedural al contestațiilor – de la înregistrarea inițială, generarea automată a dosarului, transmiterea notificărilor, desemnarea completelor CSC, până la emiterea și arhivarea deciziei finale. Fiecare etapă va fi automatizată, monitorizabilă și accesibilă printr-o interfață web securizată.

- **Principiul interoperabilității instituționale**: Sistemul va fi interoperabil cu platformele guvernamentale relevante (ex. MTender, MPass, MSign, MNotify, MConnect, MCloud), utilizând API-uri standardizate (REST/JSON, SOAP/XML), formate de date deschise și protocoale conforme cu Cadrul de Interoperabilitate al Guvernului. Această integrare va permite schimbul bidirecțional de date în timp real și sincronizarea automatizată cu registre publice și sisteme terțe.

- **Principiul reutilizării prioritare a platformelor și componentelor guvernamentale:** Dezvoltarea SIMED va urma abordarea „reuse before build", potrivit căreia funcționalitățile, componentele, serviciile și mecanismele deja disponibile în cadrul ecosistemului guvernamental vor fi reutilizate, configurate și adaptate înainte de a fi luată decizia dezvoltării unor componente noi. Pentru interacțiunea cu utilizatorii externi, Contractantul va reutiliza funcționalitățile disponibile în cadrul FOD/PDSE și va dezvolta componente noi numai pentru cerințele specifice SIMED care nu pot fi acoperite prin configurarea sau extinderea componentelor existente. Orice dezvoltare nouă va fi justificată printr-o analiză de decalaj și va fi supusă aprobării ANSC și, după caz, coordonării cu AGE.
- **Principiul modularității arhitecturale și al separării Front Office–Back Office:** Arhitectura SIMED va fi modulară, și bazată pe separarea clară a componentelor de interacțiune cu utilizatorii externi de componentele instituționale responsabile de procesarea internă. Componenta Front Office va reutiliza și adapta cadrul și funcționalitățile FOD/PDSE, iar componenta Back Office va implementa procesele, regulile de business și fluxurile procedurale specifice ANSC. Comunicarea dintre componente se va realiza prin API-uri documentate și, acolo unde este justificat, prin mecanisme de mesagerie asincronă. Componentele vor putea fi dezvoltate, testate, implementate, scalate și întreținute independent, fără afectarea nejustificată a celorlalte module ale sistemului.

- **Principiul compatibilității tehnologice cu FOD/PDSE:** Stiva tehnologică, arhitectura aplicațională, mecanismele de integrare și componentele dezvoltate pentru SIMED vor fi compatibile cu platforma FOD/PDSE și cu tehnologia .NET utilizată de aceasta. Soluția nu va introduce tehnologii, framework-uri sau dependențe care împiedică reutilizarea componentelor existente, integrarea cu ecosistemul guvernamental, mentenanța ulterioară sau actualizarea coordonată a platformei. Componentele suplimentare vor utiliza tehnologii standardizate, documentate și compatibile cu mediul guvernamental de găzduire.

- **Principiul dezvoltării iterative și adaptive**: SIMED va fi dezvoltat incremental, în etape clar definite, utilizând metodologii Agile sau DevSecOps, pentru a permite adaptarea rapidă la schimbările legislative, instituționale sau tehnologice. Arhitectura și codul sursă vor fi documentate extensiv, astfel încât sistemul să poată fi extins ușor cu noi funcționalități.

- **Principiul sustenabilității tehnico-operaționale**: Sistemul va fi proiectat pentru a asigura funcționare continuă, stabilitate în condiții de sarcină mare, reziliență la atacuri și ușurință în întreținere. Vor fi implementate politici de actualizare periodică, auditabilitate și monitorizare proactivă a performanței, astfel încât să se asigure o durată de viață operațională extinsă fără dependențe tehnologice critice.

- **Principiul protecției datelor și confidențialității**: SIMED va implementa măsuri de protecție by design și by default, asigurând confidențialitatea, integritatea și disponibilitatea datelor sensibile, inclusiv a celor cu caracter personal. Se vor aplica politici de acces granular (RBAC), criptare end-to-end, pseudonimizare selectivă, jurnale de audit inviolabile și proceduri de răspuns la incidente, în conformitate cu ISO/IEC 27001 și GDPR.

- **Principiul standardizării documentare**: Toate documentele procesuale utilizate în cadrul ANSC – formulare, decizii, note interne, scrisori oficiale – vor fi digitalizate și convertite în template-uri electronice dinamice (ex. PDF interactiv, XML, eForm), ce permit completarea automată pe baza datelor din sistem sau din surse interoperabile.

- **Principiul accesibilității și ergonomiei (UX/UI)**: Interfețele grafice ale SIMED vor fi optimizate pentru claritate, eficiență și utilizabilitate, atât pentru utilizatori interni (membrii CSC, secretariat, conducere) cât și pentru cei externi (operatori economici, reprezentanți AAP). Designul va fi conform standardelor WCAG 2.1, asigurând accesul universal și incluziunea digitală.

- **Principiul independenței tehnologice (vendor lock-out prevention)**: Sistemul va fi dezvoltat utilizând tehnologii deschise, fără licențieri restrictive, pentru a evita dependența de un anumit furnizor. Codul va fi livrat în întregime ANSC, însoțit de documentație completă, pentru a permite întreținerea și extinderea ulterioară de către orice actor calificat. Utilizarea obligatorie a unei stive compatibile cu tehnologia .NET și cu FOD/PDSE nu va limita drepturile ANSC asupra codului sursă,

documentației, datelor și artefactelor dezvoltate și nu va permite introducerea unor dependențe comerciale sau tehnice care ar crea o relație exclusivă cu Contractantul.

- **Principiul auditabilității și trasabilității**: Fiecare operațiune efectuată în sistem va fi înregistrată automat într-un jurnal de audit criptat, nemodificabil, asociat cu identitatea digitală a utilizatorului. Acest lucru va permite reconstituirea completă a istoricului fiecărui dosar și va facilita inspecțiile, litigiile sau controalele ulterioare.

- **Principiul transparenței active și al datelor deschise**: Datele relevante privind contestațiile soluționate, deciziile adoptate și statisticile agregate vor fi publicate în mod proactiv, într-un format deschis, accesibil publicului și reutilizabil (CSV, JSON, OC4IDS), promovând responsabilitatea publică și analiza independentă a performanței sistemului de contestații.

- **Principiul scalabilității și rezilienței infrastructurale**: SIMED va fi implementat pe o infrastructură elastică (on-premise sau MCloud), care să permită scalarea automată a resurselor în funcție de sarcină și să ofere disponibilitate ridicată (HA), continuitate operațională (BCP) și capacitate de recuperare în caz de dezastru (DR).

- **Principiul conformității cu Modelul Unitar de Design:** Interfețele publice și instituționale ale SIMED vor fi proiectate și implementate în conformitate cu Modelul Unitar de Design aprobat la nivel guvernamental, inclusiv cu cerințele aplicabile privind identitatea vizuală, structura paginilor, componentele UI reutilizabile, navigarea, accesibilitatea, experiența utilizatorului și integrarea cu ecosistemul Portalului guvernamental integrat EVO. Respectarea acestor cerințe va fi verificată la etapa de proiectare, prototipare, dezvoltare și acceptanță.

2. GUVERNANȚA ȘI ARHITECTURA COLABORATIVĂ A DEZVOLTĂRII, IMPLEMENTĂRII ȘI EXPLOATĂRII SISTEMULUI INFORMAȚIONAL

2.1. Părți implicate în guvernanța și ciclu de viață al sistemului

Proiectarea, configurarea, adaptarea, dezvoltarea, integrarea, testarea, implementarea, exploatarea și dezvoltarea ulterioară a Sistemului Informațional de Management Electronic al Documentelor implică participarea coordonată a mai multor entități publice, utilizatori și furnizori de servicii tehnologice.
Guvernanța SIMED va fi organizată astfel încât să existe o delimitare clară între:

- proprietatea și guvernanța funcțională a sistemului;
- coordonarea reutilizării platformelor și serviciilor guvernamentale;
- administrarea infrastructurii tehnologice;
- dezvoltarea și mentenanța aplicației;
- administrarea funcțională și operațională;
- introducerea și gestionarea datelor;

- utilizarea serviciilor electronice.

Principalele părți implicate în ciclul de viață al SIMED sunt:

- **Agenția Națională pentru Soluționarea Contestațiilor**, în calitate de Autoritate contractantă, beneficiar instituțional, proprietar funcțional al sistemului, proprietar al datelor gestionate în SIMED și administrator funcțional al proceselor operaționale. ANSC definește și aprobă cerințele funcționale, regulile de business, fluxurile procedurale, nomenclatoarele, documentele procesuale, politicile de acces și criteriile de acceptanță.
- **Agenția de Guvernare Electronică**, în calitate de autoritate competentă pentru coordonarea soluțiilor și investițiilor TIC guvernamentale și pentru facilitarea reutilizării componentelor FOD/PDSE și a serviciilor guvernamentale partajate. AGE va participa, în limitele atribuțiilor sale, la coordonarea modelului de reutilizare FOD/PDSE, a compatibilității arhitecturale și tehnologice și a integrării SIMED în ecosistemul guvernamental de servicii electronice.
- **Serviciul Tehnologia Informației și Securitate Cibernetică**, în calitate de furnizor și administrator al infrastructurii tehnologice guvernamentale utilizate pentru găzduirea SIMED. STISC va asigura resursele de infrastructură MCloud și serviciile tehnologice aferente, în limitele atribuțiilor sale și ale acordurilor de servicii aplicabile.
- **Ministerul Finanțelor**, în calitate de autoritate responsabilă de domeniul achizițiilor publice și de coordonarea instituțională a SIA RSAP/MTender, va participa la definirea și coordonarea mecanismelor de interoperabilitate dintre SIMED și SIA RSAP/MTender, inclusiv în ceea ce privește schimbul de date, identificatorii, statuturile și regulile de sincronizare.
- **Dezvoltatorul** , în calitate de operator economic selectat pentru realizarea SIMED, va fi responsabil de analiza componentelor FOD/PDSE disponibile, elaborarea analizei de decalaj, proiectarea arhitecturii țintă, configurarea și adaptarea componentelor reutilizate, dezvoltarea funcționalităților specifice ANSC, integrarea, testarea, implementarea, documentarea și asigurarea suportului în perioada contractuală.
- **Utilizatorii interni ANSC**, inclusiv conducerea ANSC, președinții și membrii completelor CSC, funcționarii Direcției Juridice, funcționarii DTISD, administratorii funcționali și alte categorii autorizate, vor utiliza componenta Back Office conform rolurilor, competențelor și drepturilor atribuite.
- **Utilizatorii externi autorizați**, inclusiv contestatarii, autoritățile contractante, operatorii economici câștigători, reprezentanții autorizați și alte părți procedurale, vor accesa serviciile SIMED prin componenta Front Office realizată prin reutilizarea și adaptarea funcționalităților FOD/PDSE.
- **Utilizatorii publici neautentificați**, inclusiv cetățeni, reprezentanți ai societății civile, mass-media, instituții academice și alte persoane interesate, vor avea acces numai la informațiile, documentele și datele publice disponibile prin Portalul Public SIMED.
- Cooperarea dintre părțile implicate va avea la bază principiile separării responsabilităților, reutilizării componentelor guvernamentale, interoperabilității, securității, trasabilității, protecției datelor și evitării dublării nejustificate a funcționalităților existente.

2.2. Autoritatea contractantă

Agenția Națională pentru Soluționarea Contestațiilor exercită rolul de Autoritate contractantă și beneficiar instituțional al proiectului SIMED.

În această calitate, ANSC este responsabilă de inițierea, organizarea, coordonarea și monitorizarea procedurii de achiziție și a contractului aferent realizării sistemului.

Responsabilitățile ANSC includ:

- definirea și aprobarea cerințelor funcționale, nefuncționale, operaționale și de securitate ale SIMED;
- aprobarea fluxurilor operaționale, proceselor de lucru și regulilor procedurale care urmează să fie configurate în Back Office;
- punerea la dispoziția Contractantului a documentelor, formularelor, nomenclatoarelor, procedurilor și informațiilor necesare realizării sistemului;
- facilitarea interacțiunii Contractantului cu AGE, STISC, Ministerul Finanțelor și celelalte entități implicate;
- coordonarea procesului de acces la documentația, componentele și mediile FOD/PDSE necesare proiectului;
- examinarea și aprobarea inventarului componentelor FOD/PDSE, a matricei de reutilizare și a analizei de decalaj elaborate de Contractant;
- aprobarea arhitecturii funcționale, logice, tehnice, de integrare, securitate și implementare;
- validarea prototipurilor și designului UI/UX pentru Front Office și Back Office;
- coordonarea, după caz, cu AGE a arhitecturii, designului, integrărilor și modelului de reutilizare FOD/PDSE;
- organizarea și coordonarea testării funcționale, testării integrărilor și testării de acceptanță de către utilizatori;
- verificarea conformității livrabilelor cu prevederile contractului și ale prezentului ToR;
- aprobarea sau respingerea motivată a livrabilelor intermediare și finale;
- organizarea punerii în funcțiune, stabilizării și recepției finale a sistemului;
- monitorizarea îndeplinirii obligațiilor de garanție, suport și remediere a defectelor.

ANSC va asigura coordonarea contractuală și acceptanța livrabilelor. Coordonarea anumitor aspecte tehnice cu AGE, STISC, Ministerul Finanțelor sau alți furnizori de servicii guvernamentale nu înlocuiește responsabilitatea ANSC de a aproba și recepționa contractual rezultatele proiectului.

ANSC va desemna o echipă de proiect și un responsabil de contract, care vor reprezenta instituția în relația cu Dezvoltatorul și celelalte părți implicate.

2.3. Proprietarul funcțional al sistemului și al resurselor informaționale

ANSC deține calitatea de proprietar funcțional și instituțional al SIMED și exercită autoritatea asupra proceselor, datelor, regulilor de business, configurațiilor și resurselor informaționale gestionate prin sistem. În această calitate, ANSC este responsabilă de:

- definirea viziunii strategice și a direcțiilor de dezvoltare a SIMED;
- aprobarea proceselor operaționale și a regulilor procedurale implementate;
- stabilirea politicilor de acces, utilizare, păstrare, publicare și arhivare a datelor;

- administrarea nomenclatoarelor, clasificatoarelor, șabloanelor și documentelor procesuale;
- aprobarea modificărilor funcționale și a priorităților de dezvoltare ulterioară;
- autorizarea integrărilor cu sisteme și servicii externe;
- asigurarea conformității utilizării sistemului cu cadrul normativ aplicabil.

ANSC va deține drepturi depline asupra:

- datelor introduse, generate, prelucrate și stocate în SIMED;
- configurațiilor funcționale specifice ANSC;
- nomenclatoarelor și regulilor de business instituționale;
- documentației elaborate în cadrul proiectului;
- codului sursă și componentelor dezvoltate în mod specific pentru SIMED, în condițiile stabilite de contract;
- extensiilor, adaptoarelor, interfețelor și mecanismelor de integrare dezvoltate în cadrul proiectului, în limitele regimului juridic aplicabil.

Componentele, modulele, bibliotecile și mecanismele FOD/PDSE existente anterior proiectului vor rămâne supuse regimului juridic și condițiilor de utilizare aplicabile platformei FOD/PDSE. Reutilizarea acestora în cadrul SIMED nu va determina transferul automat către ANSC al drepturilor de proprietate asupra componentelor guvernamentale preexistente.

Dezvoltatorul va documenta distinct:

- componentele FOD/PDSE reutilizate fără modificări;
- componentele FOD/PDSE configurate sau adaptate;
- componentele nou dezvoltate pentru SIMED;
- componentele software furnizate de terți;
- regimul de licențiere și drepturile aplicabile fiecărei componente.

Indiferent de modelul de reutilizare, ANSC va păstra controlul deplin asupra datelor, fluxurilor, configurațiilor și funcționalităților instituționale proprii.

2.4. Deținătorul infrastructurii tehnice

STISC va exercita, în limitele atribuțiilor sale și ale acordurilor de servicii aplicabile, rolul de furnizor și administrator al infrastructurii tehnologice guvernamentale utilizate pentru găzduirea și operarea SIMED.

În această calitate, STISC va asigura, după caz:

- punerea la dispoziție și administrarea resurselor de calcul, stocare, rețea și virtualizare în infrastructura MCloud;
- configurarea și administrarea componentelor de infrastructură aflate în responsabilitatea sa;
- disponibilitatea, redundanța și monitorizarea resurselor infrastructurale;
- aplicarea măsurilor de securitate la nivelul infrastructurii, rețelei și mediilor de găzduire;
- efectuarea operațiunilor de backup și restaurare la nivel de infrastructură, conform serviciilor furnizate;
- asigurarea mecanismelor de continuitate și recuperare în caz de dezastru la nivelul infrastructurii;
- furnizarea accesului tehnic controlat la mediile de dezvoltare, testare, preproducție și producție;

- colaborarea cu ANSC, AGE și Contractantul în procesul de instalare, configurare și punere în funcțiune a sistemului;
- monitorizarea și remedierea incidentelor care afectează resursele și serviciile infrastructurale aflate în responsabilitatea STISC.

STISC nu va avea, prin simpla calitate de furnizor al infrastructurii, responsabilitatea:

- administrării funcționale a fluxurilor SIMED;
- modificării regulilor de business;
- administrării nomenclatoarelor și documentelor procesuale;
- dezvoltării funcționalităților aplicației;
- mentenanței evolutive a codului SIMED;
- gestionării utilizatorilor și rolurilor funcționale;
- remedierii defectelor aplicaționale care țin de responsabilitatea Contractantului sau a administratorului aplicației.

2.5. Registratorii fluxurilor de date și documente procedurale

Registratorii SIMED sunt utilizatorii sau entitățile autorizate care, în funcție de poziția lor procedurală și de drepturile atribuite, introduc, transmit, validează, completează sau actualizează date și documente în cadrul fluxurilor electronice gestionate de sistem.

Calitatea de registrator este asociată contextului procedural și nu reprezintă un mecanism distinct de autentificare. Identitatea utilizatorilor va fi confirmată prin MPass, dreptul de reprezentare a unei persoane juridice va fi verificat, după caz, prin MPower sau prin alte surse oficiale, iar documentele pentru care este obligatorie semnarea vor fi semnate prin MSign.

Pentru fiecare operațiune, SIMED va verifica în mod cumulativ:

- identitatea utilizatorului autentificat;
- profilul instituțional sau organizațional;
- rolul funcțional atribuit în SIMED;
- dreptul de reprezentare, dacă utilizatorul acționează în numele unei persoane juridice;
- drepturile aplicabile dosarului și etapei procedurale;
- necesitatea aplicării semnăturii electronice.

Registratorii instituționali sunt grupați astfel:

- **Operatorii economici** (contestatarii) – acționează ca registratori inițiali, având dreptul de a depune contestații, de a anexa documente justificative, de a formula completări sau de a vizualiza istoricul procedural aferent dosarului propriu. Accesul lor este gestionat prin MPass și este supus autentificării calificate.
- **Autoritățile/entitățile contractante** (părțile contestate) – în calitate de registratori secundari, au dreptul de a încărca puncte de vedere, dovezi și observații oficiale, în termenele prevăzute de lege. Acțiunile lor sunt semnate electronic și devin parte a dosarului digital gestionat procedural.
- **Funcționarii ANSC** – acționează în calitate de registratori decizionali și administrativi, gestionând generarea automată sau asistată a documentelor oficiale (decizii, scrisori, convocări), validând

conținutul juridic, aplicând semnătura digitală și orchestrând circuitul documentar până la arhivare și închidere.

Această funcție instituțională este reglementată prin roluri și politici de acces (RBAC) definite la nivel de sistem, fiind corelată cu modelul de date și nivelurile de autorizare în SIMED. Orice intervenție a registratorului este jurnalizată integral, în scopul asigurării transparenței, auditabilității și nedisputabilității acțiunilor realizate în sistem.

Registratorii constituie pilonul funcțional al interacțiunii om-mașină în cadrul ecosistemului digital ANSC, contribuind la consolidarea unei infrastructuri semantice coerente și a unei administrații centrate pe date.

2.6. Rolul AGE în reutilizarea FOD/PDSE și integrarea guvernamentală

Agenția de Guvernare Electronică va participa la realizarea SIMED în calitate de autoritate responsabilă, în limitele competențelor sale, de coordonarea soluțiilor TIC guvernamentale, reutilizarea platformei FOD/PDSE și integrarea cu ecosistemul serviciilor electronice guvernamentale.

Interacțiunea dintre ANSC și AGE privind reutilizarea și adaptarea funcționalităților FOD/PDSE se va realiza potrivit cadrului normativ aplicabil Platformei de dezvoltare a serviciilor electronice.

Rolul AGE va include, după caz:

- facilitarea accesului ANSC și al Contractantului la documentația tehnică relevantă a FOD/PDSE;
- furnizarea sau facilitarea accesului la componentele, standardele, ghidurile și mecanismele de integrare disponibile;
- participarea la coordonarea modelului de reutilizare, configurare și adaptare a funcționalităților FOD/PDSE;
- examinarea, în limitele atribuțiilor sale, a arhitecturii propuse pentru componenta Front Office;
- participarea la coordonarea compatibilității stivei tehnologice SIMED cu tehnologia .NET și cu componentele FOD/PDSE;
- coordonarea integrării cu serviciile guvernamentale partajate aflate în aria sa de competență;
- participarea la coordonarea Modelului Unitar de Design și a componentelor UI reutilizabile;
- acordarea suportului metodologic privind utilizarea FOD/PDSE și conectarea la ecosistemul guvernamental;
- examinarea materialelor și documentelor prezentate pentru coordonare, potrivit procedurilor aplicabile;
- formularea recomandărilor tehnice și instituționale necesare asigurării compatibilității și evitării dezvoltărilor redundante.

AGE nu va substitui ANSC în rolul său de Autoritate contractantă, proprietar funcțional și beneficiar al sistemului și nu va prelua administrarea operațională a proceselor și datelor SIMED.

2.7. Dezvoltatorul responsabil de implementarea SIMED

Contractantul este operatorul economic selectat pentru proiectarea, configurarea, adaptarea, dezvoltarea, integrarea, testarea, implementarea și punerea în funcțiune a SIMED.

Contractantul va avea responsabilitatea integrală pentru livrarea unei soluții funcționale, securizate, documentate și compatibile cu arhitectura guvernamentală aplicabilă.

Contractantul va fi responsabil de:

- analiza documentației, componentelor și funcționalităților FOD/PDSE disponibile;
- elaborarea inventarului componentelor care pot fi reutilizate;
- elaborarea matricei de acoperire a cerințelor SIMED prin FOD/PDSE;
- realizarea analizei de decalaj dintre funcționalitățile disponibile și cerințele ANSC;
- justificarea tuturor componentelor propuse pentru dezvoltare nouă;
- proiectarea arhitecturii funcționale, aplicaționale, de date, integrare, securitate și implementare;
- reutilizarea, configurarea și adaptarea componentelor FOD/PDSE;
- dezvoltarea componentelor Back Office conform fluxurilor operaționale și regulilor procedurale ANSC;
- utilizarea unei stive tehnologice compatibile cu .NET și FOD/PDSE;
- realizarea integrărilor cu serviciile guvernamentale și sistemele externe;
- implementarea soluției în infrastructura MCloud;
- elaborarea codului sursă, testelor, scripturilor, configurațiilor și documentației tehnice;
- asigurarea securității aplicației și remedierea vulnerabilităților;
- migrarea și popularea datelor;
- instruirea utilizatorilor și administratorilor;
- acordarea suportului în perioada de stabilizare și garanție;
- remedierea defectelor și incidentelor conform nivelurilor de servicii agreate.

Dezvoltatorul va colabora cu ANSC, AGE, STISC, Ministerul Finanțelor și ceilalți furnizori de servicii sau date necesari implementării integrărilor.

Dezvoltatorul nu va înlocui componente FOD/PDSE reutilizabile cu soluții proprii și nu va dezvolta funcționalități paralele fără o justificare tehnică și funcțională aprobată de ANSC și coordonată, după caz, cu AGE.

2.8. Administratorul funcțional și operațional al sistemului

Administratorii funcționali și operaționali ai SIMED vor fi desemnați de ANSC și vor gestiona configurația aplicațională și funcțională a sistemului, fără a administra infrastructura fizică sau serviciile de găzduire aflate în responsabilitatea STISC.

Administratorii funcționali vor avea următoarele atribuții:

Administrarea profilurilor și rolurilor

- înregistrarea și administrarea profilurilor aplicaționale asociate identităților autentificate prin MPass;
- atribuirea, modificarea, suspendarea și revocarea rolurilor funcționale;
- asocierea utilizatorilor cu subdiviziuni, complete, instituții sau persoane juridice;
- configurarea drepturilor de acces conform modelului RBAC;
- verificarea segregării responsabilităților și evitarea rolurilor incompatibile;
- administrarea delegărilor interne și perioadelor de valabilitate ale rolurilor.

Administratorii SIMED nu vor crea mecanisme locale de autentificare și nu vor administra parole pentru utilizatorii care accesează sistemul prin MPass.

Administrarea configurației funcționale

- gestionarea nomenclatoarelor și clasificatoarelor;
- configurarea statuturilor și tranzițiilor procedurale;
- gestionarea termenelor și alertelor;
- configurarea șabloanelor de documente și notificări;
- administrarea completelor CSC și a structurii organizaționale;
- parametrizarea regulilor care pot fi modificate fără intervenție în codul sursă.

Administrarea operațională

- monitorizarea proceselor, sarcinilor și incidentelor aplicaționale;
- identificarea dosarelor blocate sau a fluxurilor întrerupte;
- acordarea suportului de nivelul 1 și 2 utilizatorilor;
- escaladarea incidentelor către Contractant, STISC, AGE sau alți furnizori, în funcție de natura incidentului;
- consultarea logurilor și rapoartelor de monitorizare, în limitele drepturilor atribuite.

Administrarea integrărilor

- monitorizarea operațională a schimburilor de date;
- consultarea statutului mesajelor și tranzacțiilor;
- relansarea controlată a operațiunilor eșuate, dacă această funcție este permisă;
- notificarea părților tehnice responsabile în cazul indisponibilității serviciilor externe.

Administratorii nu vor putea:

- modifica sau șterge jurnalele de audit;
- altera documente semnate electronic;
- modifica retroactiv date procedurale fără justificare și fără păstrarea istoricului;
- șterge definitiv dosare, contestații sau decizii în afara unei proceduri autorizate;
- acorda drepturi peste nivelul propriu de autorizare.

Toate acțiunile administratorilor vor fi jurnalizate și supuse auditului.

2.9. Utilizatorii sistemului

Accesul utilizatorilor autorizați la SIMED se va realiza prin MPass. MSign va fi utilizat pentru semnarea și verificarea documentelor electronice și nu va constitui un mecanism de autentificare în sistem.
Pentru fiecare utilizator autorizat, SIMED va gestiona un profil aplicațional asociat identității furnizate prin MPass. Profilul va include rolurile, drepturile, apartenența instituțională, subdiviziunea, calitatea procedurală și celelalte atribute necesare utilizării sistemului.
Pentru persoanele care acționează în numele unei persoane juridice, sistemul va verifica dreptul de reprezentare prin MPower sau prin alte surse oficiale disponibile și aprobate.
Utilizatorii externi vor utiliza interfețele Front Office implementate prin reutilizarea și adaptarea FOD/PDSE, iar utilizatorii interni ANSC vor utiliza componenta Back Office.

DIRECTOR GENERAL – utilizator strategic cu rol decizional superior

În calitate de autoritate executivă supremă a ANSC, Directorul General dispune de acces integral asupra funcționalităților critice ale sistemului, având capacitate de semnare digitală, validare instituțională și monitorizare macro-procedurală.

Funcționalități atribuite:

- **Validarea constituirii completelor CSC** prin emiterea Ordinului oficial generat și semnat digital (MSign), cu atribuirea automată a codurilor de identificare și a valabilității mandatului procedural;
- **Semnarea documentelor instituționale strategice**, inclusiv deciziile de soluționare a contestațiilor, corespondența interinstituțională, notificările către părți și ordinele cu caracter normativ, documente de ieșire;
- **Acces la panouri de control (dashboard-uri instituționale)** pentru vizualizarea statusurilor procedurilor în derulare, urmărirea termenelor critice, trasabilitatea deciziilor emise și livrarea notificărilor către actorii implicați (contestatari, autorități contractante, părți terțe);
- **Monitorizarea conformității și eficienței operaționale** a fluxurilor digitale, inclusiv prin generarea de rapoarte privind timpii de soluționare, încărcarea completelor și indicatorii de performanță instituțională (KPI);
- **Acces la toate modulele sistemului.**

Președintele CSC este membrul desemnat prin ordin oficial al Directorului General al ANSC, investit cu prerogative decizionale, organizatorice și de reprezentare formală în cadrul fiecărui complet constituit pentru examinarea și soluționarea contestațiilor în materie de achiziții publice. Acest rol este esențial în arhitectura decizională a Autorității, întrucât asigură corectitudinea procedurală, validitatea juridică și trasabilitatea documentară a activităților derulate în cadrul fiecărui dosar de contestație.

În cadrul sistemului SIMED, Președintele CSC este definit ca utilizator cu nivel avansat de autorizare, având acces privilegiat la modulele de:

- organizare internă a completului;
- generare și validare a documentelor oficiale;
- decizie procedurală privind audierile;
- avizare și transmitere a actelor către părțile implicate.

Funcționalități și responsabilități alocate:

1. Coordonarea activității completului CSC

- Dirijează operațional întregul parcurs procedural de examinare a contestației atribuite;
- Atribuie roluri funcționale membrilor (ex. consilier raportor), gestionează conflictele de interese și se asigură de respectarea termenelor prevăzute în Procedura Operațională (ex: max. 20 zile lucrătoare pentru adoptarea deciziei);
- Supervizează fluxul electronic aferent fiecărui dosar (creare, alocare, înregistrare, urmărire).

2. Validarea documentelor și asumarea deciziei colective

- Semnează, prin MSign, toate comunicările oficiale din partea completului: solicitări de clarificări, invitații la ședință, cereri de puncte de vedere, etc.;
- Avizează și co-semnătureză, împreună cu ceilalți membri, proiectele Deciziilor de Soluționare a Contestației (DSC);

- Își asumă validitatea juridică a deciziilor emise, chiar și în cazul exprimării unor opinii separate de către alți membri CSC.

3. Organizarea și desfășurarea ședințelor de examinare

- Decide oportunitatea organizării ședinței publice de examinare (în format fizic sau online);
- Semnează invitațiile transmise automat prin SIMED către părți, reprezentanți legali, experți sau membri ai societății civile;
- Validează și semnează procesele-verbale ale ședinței (modelele 7.2, 7.3, 7.4 din PO), confirmând respectarea principiilor transparenței, contradictorialității și echității procedurale.

4. Supravegherea transmiterii deciziilor către părți

- Monitorizează livrarea automată a deciziei către contestatar, autoritatea contractantă, ofertanții terți și alte instituții implicate;
- Confirmă respectarea termenelor legale de transmitere și dispune asupra arhivării electronice a dosarului.

5. Controlul de legalitate și conformitate procedurală

- Verifică respectarea strictă a Procedurii Operaționale, inclusiv în cazuri speciale: abțineri, recuzări, conflicte de interese;
- Autorizează intervenții corective în sistem (de ex. în cazul erorilor materiale sau informaționale semnalate în decursul examinării);
- Asigură coerența dintre realitatea juridică a dosarului și reprezentarea sa digitală în SIMED.

Membrul CSC este un funcționar desemnat prin ordin oficial al Directorului General al ANSC, integrat într-un complet colegial în vederea examinării și soluționării contestațiilor depuse de operatorii economici în cadrul procedurilor de achiziții publice. Acest rol este guvernat de principiul colegialității, al legalității administrative și al imparțialității decizionale, fiind esențial pentru buna funcționare a mecanismului instituțional ANSC și a integrității procesului de atribuire a contractelor publice.

În cadrul platformei SIMED, membrul CSC este un utilizator cu profil funcțional specializat, având acces controlat la modulele de analiză, deliberare, semnătură electronică și emitere de decizii administrative, în corelare cu statutul său procedural.

Funcționalități și responsabilități alocate:

1. Acces documentar diferențiat și trasabilitate procedurală

- Are acces complet la contestațiile repartizate aleatoriu (cu logare securizată și identificare prin MPass);
- Vizualizează documentele transmise de contestatar, autoritatea contractantă și instituțiile terțe;
- Monitorizează automat termenul de introducere a contestației și a răspunsurilor aferente prin tablouri de bord și alerte instituționale.

2. Examinarea juridică a dosarului

- Efectuează verificări preliminare de admisibilitate: competența ANSC, calitatea de contestatar, respectarea termenelor;
- Analizează legalitatea și temeinicia contestației pe fond, inclusiv prin corelarea cu legislația în vigoare și jurisprudența internă a ANSC;

- Poate solicita completări de dosar, transmiterea de puncte de vedere suplimentare sau probe documentare, prin intermediul funcționalităților standardizate în SIMED.

3. Participare deliberativă colegială

- Participă la ședințele de deliberare (în format electronic sau fizic), cu drept de exprimare a opiniei juridice și vot decizional;
- Semnează procesele-verbale de ședință și are dreptul de a formula **opinie separată**, anexată la Decizia de Soluționare a Contestației (DSC);
- Poate modera, în cazuri delegate, secțiuni ale ședinței publice și interacționa cu părțile sau experții invitați.

4. Elaborarea Deciziei de Soluționare a Contestației (DSC)

- Dacă este desemnat **raportor**, întocmește proiectul deciziei, colaborând direct cu Direcția Juridică (DJ) și DTISD;
- Integrează în decizie datele și concluziile legale rezultate din examinare, în concordanță cu formatul digital predefinit;
- Transmite proiectul spre **semnare colegială** și spre încărcarea oficială în dosarul electronic al părților.

5. Responsabilități de conformitate și integritate instituțională

- Declară proactiv orice conflict de interese, incompatibilitate sau circumstanțe care impun abținerea, în conformitate cu articolele 5.5.1–5.5.4 din PO;
- Are obligația de a respecta termenele procedurale – 10 zile pentru decizii pe excepții, 20 zile pentru fond, cu extensie maximă de 10 zile justificabilă;
- Asigură corectitudinea și transparența procedurală a acțiunilor sale în SIMED, supuse auditului intern și extern.

6. Funcții digitale complementare în SIMED

- Utilizează semnătura electronică calificată prin MSign pentru toate documentele generate sau validate;
- Verifică transmiterea automatizată a deciziei către contestatar, autoritatea contractantă și părțile interesate;
- Contribuie la buna arhivare digitală a dosarului, prin validarea versiunii finale a documentelor și închiderea procedurală a cazului.

Funcționar DJ – utilizator autorizat din cadrul ANSC, cu atribuții de consiliere normativă, sprijin metodologic și control juridic al procesului de soluționare a contestațiilor. Acesta contribuie activ la fundamentarea legală a deciziilor emise de completele CSC și la asigurarea coerenței interne a jurisprudenței administrative dezvoltate de ANSC.

În cadrul sistemului SIMED, funcționarul DJ este definit ca utilizator expert cu rol consultativ avansat, având acces extins la modulele de documentare, deliberare, corectare și validare juridică a deciziilor.

Funcționalități și responsabilități alocate:

1. Acces extins la dosarele electronice și metadatele decizionale

---

- Vizualizează în regim complet toate elementele procedurale și documentele încărcate în dosarul digital (contestații, puncte de vedere, documente justificative, corespondență oficială);
- Accesează toate versiunile intermediare ale proiectelor de Decizie de Soluționare a Contestației (DSC), cu istoric de modificări, comentarii și avize interne;
- Are dreptul de a introduce observații și recomandări în fluxul digital de lucru al completului, fără a interfera decizional.

2. Furnizarea de expertiză juridică formală și informală

- Asigură asistență continuă membrilor completului CSC în analiza aspectelor de drept material și procedural;
- Interpretează dispozițiile aplicabile (Legea 131/2015, Codul administrativ, Legea contenciosului administrativ, legislația UE, etc.) și propune soluții corective în caz de aplicare eronată;
- Contribuie la dezvoltarea metodologiei interne de examinare și la uniformizarea practicii decizionale.

3. Participarea activă în etapa deliberativă

- Participă, la solicitare sau de drept, la ședințele de examinare a contestațiilor (inclusiv online), având rol consultativ;
- Contribuie la redactarea considerentelor juridice ale deciziilor, oferind clarificări în ceea ce privește fundamentarea legală;
- În cazuri speciale, cu acordul președintelui CSC, poate redacta parțial sau integral proiectul deciziei (cf. PO, pct. 6(4)c).

4. Validarea juridică a proiectului de decizie

- Verifică coerența logică, formală și legală a deciziilor emise de complet, în special a secțiunii de motivare și a dispozitivului;
- Confirmă conformitatea proiectului de decizie cu legislația aplicabilă, practica instituțională și principiile de drept public;
- Asigură includerea corectă a dispozițiilor privind căile de atac și termenele procedurale, în conformitate cu Codul administrativ.

Funcționar DTISD – utilizator autorizat din cadrul ANSC, exercită un rol strategic și operațional în cadrul procesului digitalizat de soluționare a contestațiilor, acționând ca pivot instituțional între dimensiunea administrativă, logistică și tehnologică a procedurii. Prin expertiza sa, DTISD asigură traiectoria completă a dosarului procedural – de la recepție și înregistrare până la comunicarea deciziei și arhivarea finală – contribuind esențial la trasabilitate, auditabilitate și continuitate instituțională.

În SIMED, DTISD este definit ca utilizator cu privilegii operaționale extinse, cu acces la modulele de înregistrare documentară, repartizare automată, redactare asistată, notificare și arhivare.

Funcționalități și responsabilități alocate:

1. Înregistrare oficială și evidență documentară

- Primește toate contestațiile (indiferent de canalul de transmitere) și le înregistrează în sistem, inclusiv în afara orelor de program;
- Aplică un identificator unic (ID de contestație) și marchează cu precizie data și ora depunerii;
- Asociază fiecare contestație completului CSC desemnat, conform logării sistemice și schemei de rotație aleatorie.

---

2. Repartizare digitală și notificare procedurală

- Activează funcționalitatea de **alocare aleatorie automatizată** către completele CSC prin algoritmul integrat al SIMED;
- Generează și transmite notificări instituționale către membrii CSC, inclusiv desemnarea consilierului raportor;
- Elaborează **rapoarte de activitate completă**, în format digital, pentru controlul intern și raportare managerială periodică.

3. Suport procedural, tehnologic și logistic

- Oferă asistență în desfășurarea ședințelor CSC (logistică fizică și digitală), asigurând accesul la echipamente, fișiere și instrumente de redare înregistrări;
- Colaborează cu membrii CSC pentru redactarea deciziei (DSC), respectând structura procedurală și modelele standardizate;
- Integrează și gestionează formularele predefinite (ex: modele 7.1–7.7) în cadrul fluxului digital procedural.

4. Transmiterea oficială a deciziilor și dovada notificării

- Înregistrează și expediază deciziile semnate digital către toate părțile implicate (contestatar, autoritate contractantă, operator economic câștigător, alte instituții relevante);
- Asigură publicarea deciziilor pe site-ul oficial al ANSC în termenul legal de 3 zile;
- Generează și arhivează dovezile de transmitere (semnături, confirmări electronice, jurnale de activitate).

5. Arhivarea digitală și fizică a dosarelor procedurale

- Închide dosarele de contestație, agregând documentele în format digital standardizat și în format fizic acolo unde este necesar;
- Asigură predarea dosarelor către autoritățile contractante sau alte entități, conform dispozițiilor legale;
- Monitorizează **integritatea metadatelor**, jurnalele de acțiuni și arhitectura digitală a fiecărui dosar pentru audit, control intern sau solicitări externe (ex: ANI, Curtea de Conturi, mass-media).

Contestatar - utilizator extern autorizat, acesta este definit ca agent economic (persoană juridică, asociație de întreprinderi sau reprezentant legal autorizat) care participă la proceduri de achiziții publice și care, în temeiul Legii nr. 131/2015, poate formula contestații împotriva actelor sau omisiunilor autorității contractante. În cadrul SIMED, acest rol se concretizează printr-o interfață digitală securizată, care asigură un cadru procedural unificat, complet dematerializat și interoperabil.

Accesul contestatarului la Cabinetul Personal Digital va fi realizat prin autentificare în MPass. Dreptul persoanei autentificate de a acționa în numele operatorului economic va fi verificat prin MPower sau prin alte surse oficiale de reprezentare. MSign va fi utilizat pentru semnarea contestației, anexelor și celorlalte documente pentru care semnătura electronică este obligatorie.

Funcționalități alocate și responsabilități procedurale

1. Autentificare și acces la spațiul procedural digital

- Autentificare prin MPass și activare a Cabinetului Digital Personal;

- Semnătură electronică a tuturor documentelor transmise prin MSign;
- Configurarea profilului procedural: notificări, reprezentanți autorizați, preferințe lingvistice și de comunicare.

2. Depunerea contestației prin formular electronic standardizat

- Completarea ghidată a formularului de contestație, cu câmpuri inteligente, validări automate și importuri directe din registrele MPublica, Mtender și e-Procurement;
- Încărcarea probelor și anexelor în format digital securizat (PDF/A, DOCX, XLSX, JPEG etc.), cu opțiuni de etichetare și clasificare automată;
- Confirmarea electronică a recepționării și obținerea unui **ID unic de înregistrare procedurală**.

3. Acces la corespondență, probe și documente generate

- Vizualizarea tuturor documentelor generate în sistem (răspunsuri de la AC, puncte de vedere, notificări de la ANSC, decizia finală);
- Interacțiune bidirecțională controlată cu părțile implicate (inclusiv drept de replică, completări solicitate, răspunsuri automate sau redactate);
- Urmărirea întregului flux decizional prin **panou de control contextualizat**, cu afișarea clară a etapelor parcurse, acțiunilor efectuate și termenelor rămase.

4. Monitorizarea procedurii în timp real și audit digital

- Alerte automate privind expirarea termenelor, necesitatea completării, emiterea deciziei;
- Acces securizat la istoricul de acțiuni și fișiere asociate dosarului procedural;
- Posibilitatea de descărcare a întregului dosar (în format arhivat) pentru arhivă proprie sau în vederea exercitării căilor de atac.

Autoritate contractantă – utilizator extern autorizat**,** este reprezentată de instituția publică beneficiară a fondurilor publice care a inițiat procedura de achiziție publică ce face obiectul unei contestații. În cadrul arhitecturii SIMED, autoritățile contractante sunt configurate drept utilizatori instituționali cu **acces securizat**, al căror rol procedural implică furnizarea punctului de vedere oficial și participarea activă la procesul de soluționare desfășurat de către ANSC.

Funcționalități alocate și responsabilități instituționale

1. Acces instituțional securizat și delimitat procedural

- Autentificare în platformă prin MPass și activarea unui **Cabinet Digital Instituțional**, cu semnătură electronică prin MSign;
- Configurarea reprezentanților oficiali ai AC cu drept de redactare, semnare și transmitere a documentelor.

2. Recepționarea și prelucrarea notificărilor oficiale

- Recepționarea automată a notificării electronice privind înregistrarea unei contestații împotriva procedurii lansate;
- Alerte privind termenul procedural pentru prezentarea punctului de vedere și posibile cereri de completări.

3. Redactarea și transmiterea punctului de vedere instituțional

- Încărcarea punctului de vedere oficial al autorității contractante, semnat electronic, cu indicarea poziției asupra fiecărui aspect contestat;
- Atașarea documentelor justificative relevante (ex: dosarul achiziției, nota conceptuală, procesul-verbal de evaluare, corespondenta cu ofertanții etc.);
- Posibilitatea consultării ghidurilor și modelelor instituționale puse la dispoziție în sistem.

---

4. Participare activă în procesul contradictorial

- Interacțiune digitală cu completul CSC: furnizarea răspunsurilor suplimentare, acceptarea invitațiilor la ședințe online (dacă este cazul);
- Vizualizarea dosarului digital și a pozițiilor exprimate de celelalte părți.

5. Acces la decizia finală și gestiune post-contestare

- Acces la decizia de soluționare a contestației (DSC), în format electronic, semnată digital;
- Posibilitatea descărcării documentului și distribuirea internă către conducere, unitatea juridică și alte structuri relevante;
- Arhivarea deciziei în sistemul propriu de management al documentelor sau integrarea acesteia în sistemele ERP instituționale.

Utilizator public este definit ca orice persoană fizică sau juridică, reprezentant al societății civile, mass-mediei, organizațiilor neguvernamentale, instituțiilor academice sau al altor entități interesate de supravegherea și înțelegerea procesului de soluționare a contestațiilor. Acest rol susține obiectivele de transparență proactivă, control democratic și responsabilizare instituțională, fiind reglementat de Legea nr. 982/2000 privind accesul la informația de interes public și de normele internaționale privind guvernanța deschisă.

Funcționalități disponibile în regim public (read-only)

1. Acces liber la interfața publică a sistemului

- Navigare directă, prin browser, la modulul public al sistemului SIMED fără înregistrare;
- Interfață web accesibilă, compatibilă cu dispozitivele mobile și adaptată conform standardelor de design UX/UI incluziv.

2. Vizualizarea contestațiilor în examinare

- Acces la lista actualizată a contestațiilor înregistrate și aflate în curs de soluționare;

3. Consultarea calendarului procedural și transmisiunilor publice

- Afișarea agendei ședințelor publice ale completelor CSC;
- Acces la transmisii video în direct (live-streaming), precum și la arhiva înregistrărilor ședințelor relevante.

4. Acces la deciziile finale și jurisprudența CSC

- Vizualizarea deciziilor adoptate, în format digital, semnate electronic, publicate în regim de transparență;
- Posibilitate de căutare, filtrare și descărcare în format PDF pentru uz documentar, cercetare sau monitorizare.

5. Acces la date statistice și rapoarte de activitate

- Vizualizarea indicatorilor cheie de performanță (KPI), volum de contestații, durată medie de soluționare etc.;
- Acces la grafice analitice, rapoarte anuale și sinteze instituționale publicate de ANSC, în format deschis (CSV, XLSX).

Administrator de sistem - reprezintă un actor uman autorizat, investit cu responsabilitatea de a configura, gestiona și supraveghea funcționarea tehnică a Sistemului Informațional de Management Electronic al Documentelor (SIMED). În cadrul arhitecturii instituționale a ANSC, administratorii de sistem activează în

regim privilegiat, exercitând atribuții de natură tehnico-funcțională, orientate spre **garantarea continuității** operaționale, securității informatice și guvernanței digitale coerente a procesului contestațional.

Rol general și poziționare în fluxul procedural

Administratorii de sistem își desfășoară activitatea în cadrul Direcției Tehnologii Informaționale, Statistică și Documentare (DTISD) a ANSC și, după caz, în colaborare cu STISC (pentru infrastructura MCloud), contribuind la:

- administrarea accesului și a drepturilor utilizatorilor în funcție de rolurile instituționale (CSC, DJ, AC, contestatar);
- configurarea fluxurilor digitale de lucru;
- actualizarea nomenclatoarelor și clasificatoarelor;
- intervenția în caz de disfuncționalități software sau arhitecturale;
- păstrarea conformității sistemului cu cerințele legale de audit, trasabilitate, protecție a datelor și interoperabilitate.

Funcționalități atribuite administratorului de sistem în SIMED

1. Managementul conturilor și al drepturilor de acces

- Crearea, modificarea și suspendarea conturilor utilizatorilor instituționali și externi;
- Administrarea profilurilor de utilizatori: Președinte CSC, membru CSC, DJ, DTISD, AC, contestatar;
- Atribuirea și revocarea rolurilor, în conformitate cu Ordinul Directorului General și regulile de segregare a responsabilităților;
- Definirea drepturilor de vizualizare, editare și semnare în cadrul fluxului procedural;

2. Configurarea și administrarea fluxurilor de lucru digitale

- Parametrizarea traseului digital al unei contestații: de la recepție → repartizare → examinare → decizie → comunicare → arhivare;
- Configurarea automată a termenelor procedurale în conformitate cu PO (ex. 20 zile lucrătoare pentru examinare în fond, +10 extensie);
- Activarea/dezactivarea componentelor funcționale în funcție de ciclurile instituționale;

3. Administrarea resurselor informaționale

- Întreținerea și actualizarea nomenclatoarelor utilizate (ex. tipuri contestații, motive de inadmisibilitate, clasificare AC);
- Gestionarea modelelor de decizii, formulare standardizate, template-uri de corespondență și procese-verbale;
- Configurarea rapoartelor statistice automate și personalizabile (KPI, fluxuri CSC, timpi de soluționare);

4. Supraveghere operațională și intervenție în timp real

- Monitorizarea stării de funcționare a SIMED și diagnosticarea alertelor de sistem;
- Intervenții tehnice pentru remedierea erorilor de interfață, blocajelor logice sau a fluxurilor întrerupte;
- Colaborare cu STISC pentru restartarea componentelor critice, actualizări software și mentenanță periodică;

5. Securitate informatică și audit

- Aplicarea politicilor de backup automat și restaurare în caz de dezastru (DRP);

- Generarea rapoartelor de audit (loguri de acces, modificări de date, traseul decizional);
- Implementarea măsurilor de protecție a datelor cu caracter personal (pseudonimizare, criptare, control acces);
- Participarea la testări de penetrare, simulări de atac și evaluări de risc cibernetic;

6. Asigurarea interoperabilității și conformității

- Validarea schimbului de date cu platformele externe guvernamentale: MTender, MConnect, MPass, MSign, MNotify;
- Configurarea canalelor de integrare API și monitorizarea fluxurilor bidirecționale;
- Confirmarea integrității semnăturilor electronice și a trasabilității deciziilor.

3. MODELUL FUNCȚIONAL AL SISTEMULUI

3.1. Arhitectura funcțională generală a SIMED

Sistemul Informațional de Management Electronic al Documentelor va fi realizat pe baza unei arhitecturi funcționale modulare, distribuite și interoperabile, construită în conformitate cu principiile FOD/PDSE și cu cerințele ecosistemului guvernamental de servicii electronice.

Arhitectura SIMED va asigura separarea clară dintre:

- componenta destinată interacțiunii cu utilizatorii externi și cu publicul – Front Office;
- componenta instituțională destinată procesării interne a contestațiilor și documentelor – Back Office;
- stratul de integrare și schimb de date;
- serviciile comune aplicaționale;
- stratul de date și management al documentelor;
- componentele de raportare, analiză și publicare;
- infrastructura tehnologică și serviciile guvernamentale partajate.

Componenta Front Office va fi realizată prin reutilizarea, configurarea, adaptarea și, numai atunci când este justificat, extinderea funcționalităților existente ale platformei FOD/PDSE. Aceasta va asigura interacțiunea electronică dintre ANSC și contestatari, autorități contractante, operatori economici câștigători, reprezentanți autorizați, alte părți procedurale și publicul larg.

Componenta Back Office va reprezenta nucleul funcțional și operațional al SIMED și va fi configurată și dezvoltată conform fluxurilor operaționale, proceselor de lucru, competențelor instituționale și regulilor procedurale specifice ANSC. Back Office-ul va asigura gestionarea completă a dosarului electronic al contestației, de la recepționare și înregistrare până la emiterea deciziei, comunicarea acesteia și arhivarea dosarului.

Comunicarea dintre Front Office și Back Office se va realiza exclusiv prin interfețe aplicaționale documentate și securizate. Pentru operațiunile care nu necesită procesare sincronă imediată, sistemul va utiliza mecanisme de comunicare bazate pe mesaje și procesare asincronă.

Front Office-ul nu va accesa direct bazele de date interne ale Back Office-ului. Toate operațiunile de creare, consultare, actualizare, transmitere sau preluare a datelor vor fi executate prin servicii aplicaționale autorizate, cu validarea identității, drepturilor și contextului procedural.

Arhitectura funcțională a SIMED va cuprinde următoarele componente principale:

1. Componenta Front Office pentru utilizatorii externi

Componenta va include:

- interfața publică accesibilă fără autentificare;
- Cabinetul Personal Digital al contestatarului;
- Cabinetul Digital Instituțional al autorității contractante;
- spațiul digital al operatorului economic câștigător sau al altei părți interesate;
- formularele electronice pentru depunerea contestațiilor și transmiterea documentelor;
- mecanismele de urmărire a dosarelor și termenelor;
- accesul la notificări, comunicări, ședințe și decizii;
- accesul la informațiile publice, registrele publice, rapoartele și statisticile ANSC.

2. Componenta instituțională Back Office

Componenta va include:

- gestionarea documentelor de intrare și ieșire;
- Registrul contestațiilor;
- dosarul electronic al contestației;
- Registrul deciziilor;
- Agenda ședințelor;
- gestionarea completelor CSC;
- repartizarea contestațiilor;
- gestionarea conflictelor de interese, declarațiilor de abținere și cererilor de recuzare;
- examinarea preliminară și examinarea în fond;
- gestionarea documentelor procesuale;
- elaborarea, avizarea și semnarea proiectelor de decizie;
- gestionarea sarcinilor, termenelor și alertelor;
- administrarea nomenclatoarelor, utilizatorilor, rolurilor și configurațiilor;
- raportarea operațională, managerială și statistică;
- arhivarea și închiderea dosarelor.

3. Stratul de integrare și interoperabilitate

Stratul de integrare va gestiona schimbul de date dintre SIMED și:

- FOD/PDSE;
- serviciile guvernamentale partajate;
- SIA RSAP/MTender;
- registrele de stat relevante;
- infrastructura MCloud;
- alte sisteme informaționale sau platforme autorizate.

Stratul de integrare va include servicii API, mecanisme de mesagerie, validarea mesajelor, transformarea și maparea datelor, gestionarea erorilor, reluarea operațiunilor eșuate, monitorizarea schimburilor și jurnalizarea tranzacțiilor.

4. Serviciile comune aplicaționale

Serviciile comune vor include cel puțin:

- gestionarea identității și accesului;
- gestionarea rolurilor și permisiunilor;
- generarea documentelor;
- semnarea și verificarea semnăturilor electronice;
- notificarea și livrarea documentelor;
- gestionarea termenelor și regulilor procedurale;
- jurnalizarea și auditul;
- căutarea și indexarea;
- gestionarea fișierelor și versiunilor;
- raportarea și exportul datelor;
- monitorizarea tehnică și operațională.

5. Stratul de date și management al documentelor

SIMED va utiliza un model de date unitar, documentat și extensibil, care va asigura corelarea dintre contestații, proceduri de achiziție, părți, documente, ședințe, complete, sarcini, termene și decizii.

Documentele vor fi stocate împreună cu metadatele, versiunile, semnăturile, marcajele temporale și istoricul operațiunilor. Fiecare document asociat unei contestații va deveni parte a dosarului electronic și va putea fi identificat, consultat și auditat în funcție de drepturile utilizatorului.

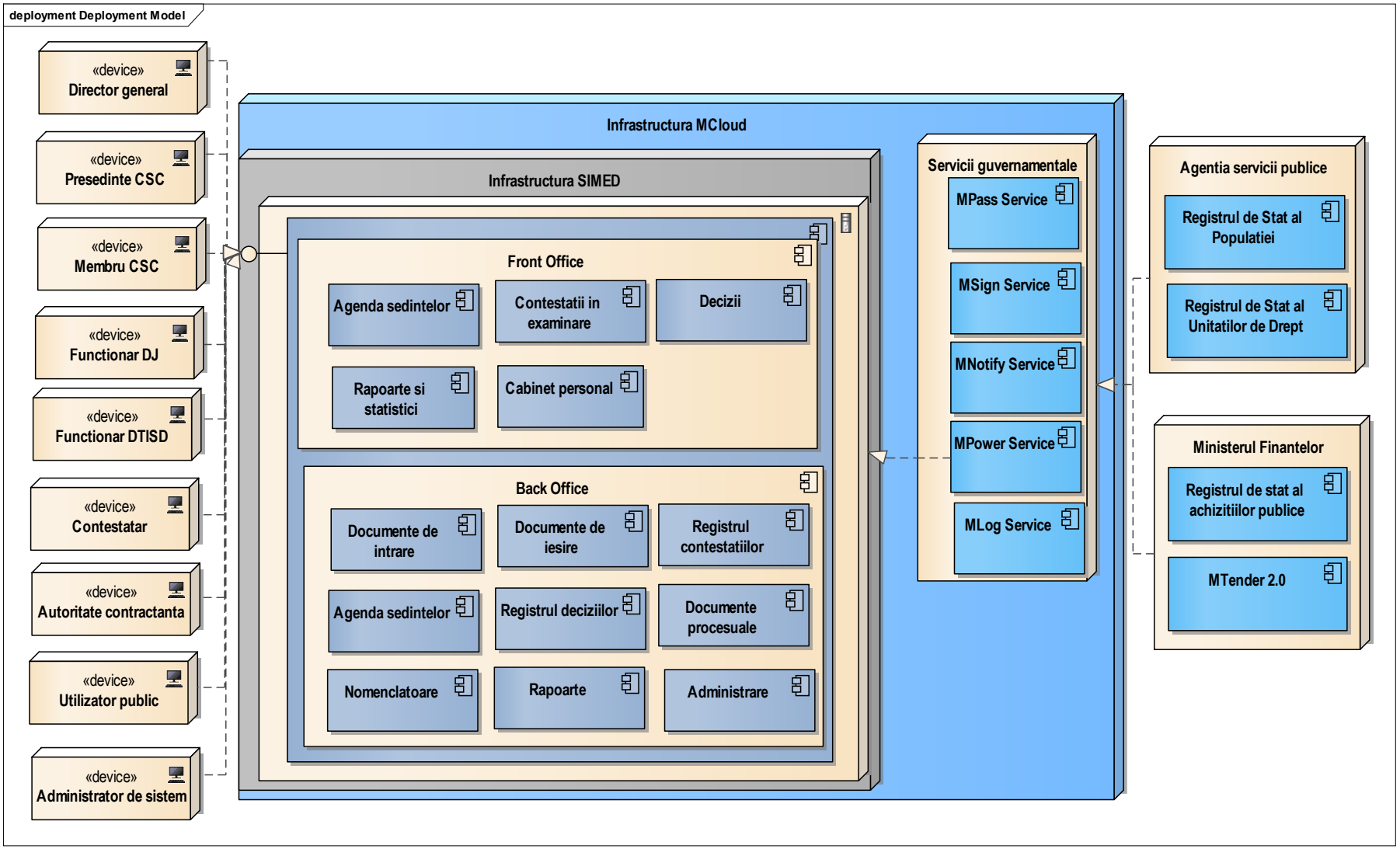
6. Componenta de raportare și analiză

Aceasta va prelua date structurate din modulele operaționale și va permite:

- generarea rapoartelor standardizate;
- configurarea rapoartelor instituționale;
- calcularea indicatorilor de performanță;
- analiza volumului și duratei contestațiilor;
- analiza deciziilor și motivelor de contestare;
- publicarea statisticilor agregate;
- exportul datelor în formate deschise.

Arhitectura va fi proiectată astfel încât modulele și serviciile să poată fi configurate, dezvoltate, testate, implementate, actualizate și scalate independent, fără afectarea nejustificată a întregului sistem.

Contractantul va elabora, în etapa de analiză și proiectare, arhitectura funcțională detaliată, arhitectura aplicațională, arhitectura de integrare, arhitectura datelor, arhitectura de securitate și arhitectura de implementare. Acestea vor fi prezentate sub formă de diagrame, modele și descrieri tehnice și vor fi aprobate de ANSC și coordonate, după caz, cu AGE și STISC.


deployment Deployment Model
«device»
Director general
«device»
Presedinte CSC
«device»
Membru CSC
«device»
Functionar DJ
«device»
Functionar DTISD
«device»
Contestatar
«device»
Autoritate contractanta
«device»
Utilizator public
«device»
Administrator de sistem
Infrastructura MCloud
Infrastructura SIMED
Front Office
Agenda sedintelor
Contestatii in examinare
Decizii
Rapoarte si statistici
Cabinet personal
Back Office
Documente de intrare
Documente de iesire
Registrul contestatiilor
Agenda sedintelor
Registrul deciziilor
Documente procesuale
Nomenclatoare
Rapoarte
Administrare
Servicii guvernamentale
MPass Service
MSign Service
MNotify Service
MPower Service
MLog Service
Agentia servicii publice
Registrul de Stat al Populatiei
Registrul de Stat al Unitatilor de Drept
Ministerul Finantelor
Registrul de stat al achizitiilor publice
MTender 2.0

3.2. Funcționalitățile componentei Front Office

Componenta Front Office a SIMED reprezintă punctul unic de interacțiune electronică dintre ANSC și utilizatorii externi ai sistemului.
Front Office-ul va fi realizat prin reutilizarea, configurarea și adaptarea funcționalităților existente ale platformei FOD/PDSE. Dezvoltarea unor componente noi va fi permisă numai pentru funcționalitățile specifice ANSC care nu pot fi acoperite prin componentele existente și numai în baza analizei de decalaj aprobate.
Componenta Front Office va fi separată funcțional și tehnic în:

1. **interfața publică, accesibilă fără autentificare;**
2. **spațiile digitale destinate utilizatorilor externi autentificați.**

3.2.1. Interfața publică

Interfața publică va permite accesul fără autentificare la informațiile și documentele care, potrivit cadrului normativ și politicilor ANSC, au caracter public.
Funcționalitățile publice vor include cel puțin:

- consultarea contestațiilor aflate în examinare;
- consultarea informațiilor publice din Registrul contestațiilor;
- consultarea deciziilor ANSC;
- căutarea full-text în conținutul și metadatele deciziilor;
- filtrarea contestațiilor și deciziilor după criterii configurabile;
- consultarea agendei ședințelor;
- accesul la informații privind data, ora, completul și părțile implicate în ședințele publice;
- accesul la procesele-verbale și înregistrările publice, în condițiile aprobate de ANSC;
- consultarea rapoartelor, statisticilor și indicatorilor publici;
- descărcarea datelor și documentelor în formatele permise;
- accesul la informații de asistență, instrucțiuni, ghiduri și întrebări frecvente;
- accesul la date deschise și interfețe publice, în cazurile aprobate.

Datele publicate vor fi extrase din Back Office prin servicii API dedicate. Înainte de publicare, sistemul va aplica regulile privind protecția datelor, anonimizarea, pseudonimizarea, clasificarea documentelor și limitarea accesului.
Nicio informație internă, confidențială, nevalidată sau neaprobată pentru publicare nu va putea fi accesată din Front Office.

3.2.2. Cabinetul Personal Digital

Cabinetul Personal Digital va constitui spațiul securizat prin care utilizatorii externi autentificați vor interacționa cu ANSC.

Autentificarea se va realiza prin MPass. Dreptul unei persoane de a acționa în numele unei persoane juridice va fi verificat, după caz, prin MPower sau prin alte surse oficiale aprobate. MSign va fi utilizat pentru semnarea documentelor, nu pentru autentificarea utilizatorului.
Cabinetul Personal Digital va oferi funcționalități diferențiate în funcție de rolul și poziția procedurală a utilizatorului.

Pentru contestatar

Contestatarul va putea:

- identifica și selecta procedura de achiziție vizată;
- iniția o contestație privind documentația de atribuire sau rezultatele procedurii;
- completa formularul electronic de contestație;
- prelua automat datele procedurii disponibile din SIA RSAP/MTender;
- salva formularul în stare de proiect;
- încărca documente și probe;
- valida completitudinea formularului și anexelor;
- semna documentele prin MSign;
- transmite contestația către ANSC;
- primi confirmarea electronică a transmiterii și, ulterior, a înregistrării;
- consulta starea și etapele dosarului;
- primi și consulta solicitări, notificări și comunicări;
- transmite completări, clarificări, observații și alte documente;
- consulta informațiile privind ședințele;
- accesa și descărca decizia finală;
- consulta istoricul documentelor și acțiunilor proprii;
- descărca dosarul propriu, în limitele drepturilor acordate.

Pentru autoritatea contractantă

Autoritatea contractantă va putea:

- consulta contestațiile care o vizează;
- accesa documentele dosarului puse la dispoziția sa;
- primi notificări privind depunerea și înregistrarea contestației;
- completa și transmite punctul de vedere;
- încărca documentele procedurii de achiziție;
- răspunde solicitărilor ANSC;
- transmite completări, clarificări și dovezi;
- primi convocări și informații privind ședințele;
- consulta și descărca decizia;
- urmări termenele și obligațiile procedurale;
- consulta istoricul comunicărilor și transmiterilor.

Pentru operatorul economic câștigător sau altă parte interesată

Utilizatorul va putea, în funcție de drepturile acordate:

- consulta informațiile și documentele puse la dispoziția sa;
- primi notificări privind implicarea în dosar;

- transmite puncte de vedere și documente;
- răspunde solicitărilor ANSC;
- consulta agenda și informațiile privind ședința;
- accesa decizia și comunicările aferente.

3.2.3. Funcționalități commune

Componenta Front Office va asigura:

- interfață multilingvă în limbile română, rusă și engleză;
- navigare și formulare conforme Modelului Unitar de Design;
- afișare responsive pe desktop, tabletă și dispozitive mobile;
- validarea datelor la nivel de interfață și server;
- salvarea proiectelor nefinalizate;
- încărcarea controlată și verificarea fișierelor;
- mesaje clare privind erorile și acțiunile necesare;
- suport contextual și instrucțiuni;
- afișarea stării operațiunilor și transmiterilor;
- notificări privind termenele și evenimentele dosarului;
- trasabilitatea documentelor transmise și primite;
- acces la confirmări și dovezi de expediere;
- protecția datelor și limitarea accesului la propriile dosare;
- integrarea cu serviciile guvernamentale aplicabile.

Front Office-ul nu va implementa mecanisme locale paralele pentru autentificare, semnare, notificare, livrare sau plată în cazul în care funcționalitățile respective sunt disponibile prin serviciile guvernamentale reutilizabile.

Contractantul va documenta, pentru fiecare funcționalitate Front Office:

- componenta FOD/PDSE reutilizată;
- configurația sau adaptarea necesară;
- integrarea cu Back Office;
- datele transmise și recepționate;
- regulile de acces;
- funcționalitățile noi propuse;
- justificarea dezvoltării noi.

3.3. Funcționalități componentei Back Office

Componenta Back Office reprezintă nucleul instituțional și operațional al SIMED și este destinată exclusiv utilizatorilor interni autorizați ai ANSC. Configurarea și dezvoltarea Back Office-ului se vor realiza conform fluxurilor operaționale, proceselor de lucru, atribuțiilor instituționale și regulilor procedurale specifice ANSC.

Back Office-ul va utiliza o abordare integrată de management al proceselor, dosarelor și documentelor și va asigura gestionarea completă a ciclului de viață al contestației.
Componenta Back Office va include următoarele categorii funcționale:

3.3.1. Funcționalități transversal

Back Office-ul va asigura:

- autentificarea utilizatorilor prin MPass;
- aplicarea drepturilor prin modelul RBAC al SIMED;
- administrarea profilurilor, rolurilor și apartenenței organizaționale;
- tablouri de bord personalizate în funcție de rol;
- gestionarea sarcinilor individuale și colective;
- gestionarea termenelor și alertelor;
- căutarea globală în dosare, documente și registre;
- gestionarea documentelor și versiunilor;
- generarea documentelor din șabloane;
- semnarea documentelor prin MSign;
- notificarea utilizatorilor și părților;
- livrarea documentelor;
- jurnalizarea și auditarea operațiunilor;
- raportarea și exportul datelor;
- gestionarea configurațiilor și nomenclatoarelor.

Nu fiecare acțiune internă va fi semnată electronic. Acțiunile vor fi jurnalizate și marcate temporal, iar semnătura electronică va fi aplicată documentelor și operațiunilor pentru care aceasta este obligatorie juridic sau procedural.
Această ultimă propoziție trebuie introdusă deoarece actualul text sugerează că fiecare acțiune din audit trail ar fi „semnată digital”, ceea ce nu este necesar.

3.3.2. Managementul documentelor

Back Office-ul va asigura:

- recepționarea documentelor din Front Office;
- înregistrarea documentelor recepționate prin e-mail, poștă sau depunere fizică;
- clasificarea și indexarea documentelor;
- atribuirea numerelor de intrare și ieșire;
- asocierea automată sau manuală a documentelor cu dosarele;
- gestionarea documentelor de intrare, ieșire și interne;
- controlul versiunilor;
- gestionarea documentelor semnate;
- vizualizarea și descărcarea documentelor;
- păstrarea istoricului modificărilor;
- aplicarea regulilor de retenție și arhivare;
- exportul controlat al dosarului și documentelor.

3.3.3. Managementul ciclului de viață al contestației

Back Office-ul va automatiza și controla cel puțin următoarele etape:

1. recepționarea contestației;
2. verificarea formală și înregistrarea;
3. constituirea dosarului electronic;
4. verificarea competenței și admisibilității;
5. repartizarea contestației;
6. desemnarea completului și a raportorului;
7. verificarea conflictelor de interese;
8. solicitarea documentelor și punctelor de vedere;
9. examinarea preliminară;
10. examinarea în fond;
11. planificarea și desfășurarea ședințelor;
12. deliberarea;
13. elaborarea proiectului de decizie;
14. avizarea și semnarea deciziei;
15. înregistrarea și comunicarea deciziei;
16. publicarea datelor și documentelor aprobate;
17. închiderea și arhivarea dosarului.

Stările, tranzițiile, termenele, condițiile, acțiunile obligatorii și drepturile utilizatorilor vor fi configurabile în limitele stabilite de ANSC.

Sistemul nu va permite trecerea la o etapă procedurală următoare dacă nu sunt îndeplinite condițiile obligatorii, cu excepția cazurilor în care un utilizator autorizat aplică o derogare justificată și jurnalizată.

3.3.4. Repartizarea contestațiilor

Sistemul va permite repartizarea automată și transparentă a contestațiilor către completele CSC, în baza unui algoritm aprobat de ANSC.

Algoritmul va putea lua în considerare:

- componența completelor active;
- disponibilitatea membrilor;
- volumul de muncă;
- rotația echitabilă;
- specializarea, dacă este aplicabilă;
- conflictele de interese;
- abținerile și recuzările;
- imposibilitatea temporară de participare.

Rezultatul repartizării, datele utilizate și eventualele intervenții manuale vor fi jurnalizate integral.

3.3.5. Spațiul digital de lucru al completului CSC

Pentru fiecare contestație repartizată, membrii completului vor avea acces la un spațiu digital de lucru care va include:

- dosarul electronic complet;
- documentele primite de la părți;
- informațiile preluate din SIA RSAP/MTender;
- sarcinile și termenele;
- notele și comentariile interne;
- proiectele de documente;
- istoricul modificărilor;
- instrumentele de colaborare;
- agenda ședințelor;
- funcțiile de elaborare și aprobare a deciziei.

Drepturile de acces vor fi delimitate în funcție de rolul de președinte, membru, raportor, funcționar DJ, funcționar DTISD sau alt rol autorizat.

3.3.6. Motorul de reguli și termene procedural

SIMED va include un mecanism configurabil pentru aplicarea regulilor procedurale, care va permite:

- calcularea automată a termenelor;
- suspendarea, reluarea sau prelungirea termenelor;
- generarea alertelor;
- identificarea termenelor apropiate sau depășite;
- validarea etapelor obligatorii;
- verificarea completitudinii datelor;
- declanșarea automată a acțiunilor;
- prevenirea tranzițiilor nepermise;
- documentarea excepțiilor și derogărilor.

Regulile configurabile nu vor putea modifica sau înlocui prevederile legale. Orice modificare a regulilor va fi versionată, aprobată și jurnalizată.

3.3.7. Elaborarea documentelor procesuale și a deciziilor

Back Office-ul va include un generator de documente și un spațiu colaborativ de redactare care va permite:

- generarea documentelor pe baza șabloanelor configurabile;
- completarea automată cu date din dosar;
- inserarea datelor procedurii de achiziție;
- redactarea și editarea controlată;
- adăugarea observațiilor și comentariilor;
- compararea versiunilor;
- urmărirea modificărilor;

- avizarea documentelor;
- transmiterea spre semnare;
- semnarea individuală sau succesivă, potrivit fluxului;
- generarea versiunii finale PDF/A;
- verificarea semnăturilor;
- înregistrarea automată în registrele relevante;
- asocierea documentului final cu dosarul contestației.

Sistemul va păstra toate versiunile intermediare și va identifica autorul, data și obiectul fiecărei modificări.

3.3.8. Registrele SIMED

Back Office-ul va include cel puțin:

- Registrul documentelor de intrare;
- Registrul documentelor de ieșire;
- Registrul contestațiilor;
- Registrul deciziilor;
- Registrul ședințelor;
- Registrul documentelor procesuale;
- Registrul completelor CSC;
- Registrul utilizatorilor și rolurilor;
- Registrul notificărilor și livrărilor;
- Registrul operațiunilor de audit.

Registrele vor utiliza date comune și identificatori unici, fără duplicarea necontrolată a acelorași informații.

3.3.9. Administrarea funcțională

Utilizatorii autorizați vor putea administra, fără intervenție în codul sursă, în limitele aprobate:

- nomenclatoarele;
- tipurile de documente;
- șabloanele;
- statuturile procedurale;
- termenele;
- notificările;
- structura organizațională;
- completele CSC;
- rolurile și drepturile;
- parametrii rapoartelor;
- regulile configurabile;
- datele de contact și alte setări operaționale.

Modificările configurațiilor vor fi versionate și jurnalizate și vor putea intra în vigoare la o dată stabilită.

3.3.10. Raportarea și analiza

Back Office-ul va permite:

- generarea rapoartelor instituționale;
- configurarea criteriilor de filtrare;
- calcularea indicatorilor operaționali;
- monitorizarea încărcării completelor;
- monitorizarea termenelor;
- analiza contestațiilor și deciziilor;
- analiza motivelor și obiectelor contestate;
- exportul în formate standard;
- alimentarea controlată a componentei publice de raportare.

Datele publice vor fi furnizate Front Office-ului numai după aplicarea regulilor de validare, anonimizare și aprobare.

3.4. Interfața utilizator a sistemului

Interfața cu utilizatorul a SIMED va fi proiectată și implementată în conformitate cu Modelul Unitar de Design aplicabil serviciilor publice electronice și cu regulile, componentele și mecanismele reutilizabile disponibile în cadrul FOD/PDSE.
Contractantul va reutiliza cu prioritate componentele vizuale, structurile de pagină, modelele de navigare, formularele, mesajele, controalele și celelalte elemente UI disponibile în FOD/PDSE.
Dezvoltarea unor componente UI noi va fi permisă numai atunci când:

- componenta necesară nu există în FOD/PDSE;
- componenta existentă nu poate fi configurată sau extinsă;
- necesitatea este demonstrată prin analiza de decalaj;
- soluția propusă respectă Modelul Unitar de Design;
- componenta este aprobată de ANSC și coordonată, după caz, cu AGE.

Interfața va asigura o experiență unitară pentru:

- publicul neautentificat;
- contestatari;
- autorități contractante;
- operatori economici câștigători;
- conducerea ANSC;
- membrii CSC;
- funcționarii DJ și DTISD;
- administratorii funcționali.

Interfața va respecta următoarele principii:

- claritate și simplitate;
- navigare predictibilă;
- orientare pe sarcinile utilizatorului;
- consistență între module;
- accesibilitate;
- adaptare la rol și context;
- reducerea introducerii repetitive a datelor;
- mesaje de eroare clare și acționabile;

- confirmarea operațiunilor importante;
- afișarea vizibilă a stării proceselor;
- prevenirea acțiunilor eronate;
- transparența termenelor și etapelor procedurale.

Componenta Front Office va fi disponibilă în limbile română, rusă și engleză. Versiunea implicită va fi limba română. Back Office-ul va fi disponibil cel puțin în limba română.
Toate elementele dependente de limbă, inclusiv etichetele, mesajele, notificările, șabloanele și textele de asistență, vor fi gestionate separat de codul aplicației.
Interfața va fi responsive și va funcționa corespunzător pe desktop, laptop, tabletă și dispozitive mobile. Funcționalitățile esențiale ale Front Office-ului nu vor fi eliminate sau limitate nejustificat pe dispozitive mobile.
Interfața publică și cabinetele utilizatorilor externi vor respecta cel puțin nivelul AA al WCAG 2.1. Cerințele de accesibilitate vor fi verificate la etapa de proiectare, dezvoltare și acceptanță.
Interfața va include:

- suport contextual;
- instrucțiuni și exemple;
- contacte de asistență;
- URL-uri clare și prietenoase;
- navigare prin tastatură;
- etichete accesibile;
- contrast corespunzător;
- mesaje de validare asociate câmpurilor;
- indicatori vizibili privind câmpurile obligatorii;
- confirmarea salvării și transmiterii;
- afișarea stării documentelor și dosarelor.

Contractantul va elabora:

- harta experienței utilizatorilor;
- fluxurile de utilizator;
- wireframe-urile;
- prototipurile interactive;
- machetele responsive;
- matricea rol–ecran–acțiune;
- inventarul componentelor FOD/PDSE reutilizate;
- lista componentelor noi;
- ghidul de utilizare a componentelor;
- matricea de conformitate cu Modelul Unitar de Design și cerințele de accesibilitate.

Prototipurile și designul vor fi aprobate de ANSC înainte de dezvoltarea finală. Componentele care afectează experiența externă, reutilizarea FOD/PDSE sau conformitatea cu Modelul Unitar de Design vor fi coordonate, după caz, cu AGE.
Toate modificările semnificative ulterioare ale designului aprobat vor fi documentate, justificate și supuse revalidării.

3.5. Interoperabilitatea și integrarea sistemului

SIMED va fi proiectat ca un sistem informațional deschis și interoperabil, integrat în ecosistemul guvernamental de servicii electronice și capabil să schimbe date în mod securizat, controlat și trasabil cu platformele și registrele relevante.

Integrarea va fi realizată în conformitate cu:

- documentația tehnică oficială a serviciului sau sistemului integrat;
- condițiile de acces și utilizare stabilite de furnizorul serviciului;
- cadrul guvernamental de interoperabilitate;
- cerințele de securitate și protecție a datelor;
- acordurile și deciziile instituționale aplicabile.

Sistemul va aplica o abordare API-first. Funcționalitățile cheie necesare interacțiunii cu Front Office-ul și cu alte sisteme autorizate vor fi expuse prin API-uri documentate și securizate.
API-urile vor utiliza cu prioritate:

- REST;
- HTTPS;
- JSON;
- OpenAPI;
- standarde deschise pentru identificatori, date, ore și codificări.

SOAP/XML va fi utilizat numai în cazurile în care serviciul extern integrat impune acest protocol.
Pentru procesele asincrone, SIMED va utiliza mecanisme de mesagerie care să asigure:

- transmiterea fiabilă;
- identificarea unică a mesajelor;
- evitarea procesării duplicate;
- reluarea operațiunilor eșuate;
- gestionarea cozilor de eroare;
- jurnalizarea tranzacțiilor;
- monitorizarea stării mesajelor.

3.5.1. Integrarea cu FOD/PDSE

Integrarea dintre componentele Front Office reutilizate din FOD/PDSE și Back Office-ul SIMED va asigura:

- transmiterea contestațiilor și documentelor;
- preluarea statuturilor și etapelor dosarului;
- transmiterea solicitărilor și comunicărilor;
- preluarea notificărilor și informațiilor privind ședințele;
- accesul controlat la decizii și documente;
- sincronizarea datelor de profil și rol;
- schimbul datelor necesare Cabinetului Personal Digital;
- publicarea controlată a informațiilor din registrele SIMED.

Contractantul va utiliza componentele, protocoalele, modelele de date și mecanismele de integrare puse la dispoziție pentru FOD/PDSE.
Orice extensie sau modificare a mecanismelor standard FOD/PDSE va fi documentată și coordonată cu ANSC și AGE.

3.5.2. Integrarea cu serviciile guvernamentale partajate

SIMED va reutiliza următoarele servicii, în funcție de aplicabilitatea acestora:

- **MPass** va fi utilizat pentru autentificarea utilizatorilor autorizați ai Front Office-ului și Back Office-ului. SIMED nu va implementa un mecanism paralel de autentificare prin nume de utilizator și parolă pentru utilizatorii care trebuie autentificați prin MPass.

  Profilurile, rolurile și drepturile aplicaționale vor fi corelate cu identitatea furnizată prin MPass.
- **MPower** va fi utilizat, după caz, pentru verificarea dreptului unei persoane de a acționa în numele unei persoane juridice. MPower nu va substitui modelul intern RBAC al SIMED și nu va fi utilizat ca unic mecanism de administrare a rolurilor interne ANSC.

- **MSign** va fi utilizat pentru:
  - semnarea contestațiilor;
  - semnarea anexelor și completărilor, dacă este necesar;
  - semnarea punctelor de vedere;
  - semnarea documentelor procesuale;
  - semnarea proceselor-verbale;
  - semnarea deciziilor;
  - verificarea semnăturilor electronice.

- **MLog** va fi utilizat pentru transmiterea și păstrarea evenimentelor relevante potrivit documentației și regulilor serviciului. Integrarea cu MLog nu va exclude obligația SIMED de a păstra propriile loguri tehnice, operaționale, de securitate și audit.

- **MNotify** va fi utilizat pentru transmiterea notificărilor privind:
  - recepționarea și înregistrarea contestației;
  - solicitările de completare;
  - transmiterea punctelor de vedere;
  - expirarea sau apropierea termenelor;
  - programarea și modificarea ședințelor;
  - emiterea și comunicarea deciziei;
  - alte evenimente aprobate de ANSC.

- **MDelivery** va fi utilizat, în măsura în care este aplicabil și disponibil, pentru livrarea oficială a documentelor electronice și păstrarea dovezilor de expediere, livrare sau recepționare.

SIMED va păstra legătura dintre document, destinatar, canalul de livrare, data transmiterii și confirmarea primită.

- **MPay** va fi utilizat numai dacă, în baza cadrului normativ și a deciziei ANSC, depunerea sau procesarea contestației presupune o plată.

În acest caz, SIMED va permite:

- generarea solicitării de plată;
- redirecționarea către serviciul MPay;
- preluarea confirmării;
- asocierea plății cu contestația;
- verificarea statutului plății;
- reconcilierea și auditarea operațiunii.

- **MConnect** va fi utilizat pentru schimbul de date cu registrele și sistemele informaționale de stat, în cazurile în care seturile de date necesare sunt disponibile prin platforma de interoperabilitate.

- **MCloud** va constitui mediul țintă de găzduire și operare a SIMED. Arhitectura va fi hardware agnostică, containerizată și compatibilă cu mediile și serviciile tehnice puse la dispoziție de AGE/STISC.

3.5.3. Integrarea cu SIA RSAP/MTender

Integrarea cu SIA RSAP/MTender va asigura, în funcție de datele și serviciile disponibile:

- identificarea procedurii de achiziție;
- verificarea participării operatorului economic;
- preluarea datelor autorității contractante;
- preluarea obiectului achiziției;
- preluarea codurilor CPV și loturilor;
- preluarea tipului și statutului procedurii;
- preluarea informațiilor privind ofertanții și rezultatele;
- corelarea contestației cu identificatorul procedurii;
- transmiterea către SIA RSAP/MTender a informațiilor sau deciziilor pentru care există temei juridic și mecanism tehnic aprobat.

Contractantul nu va presupune existența unor endpoint-uri, câmpuri sau operațiuni care nu sunt confirmate de documentația oficială SIA RSAP/MTender.
În etapa de analiză, Dezvoltatorul va elabora specificația detaliată a integrării și matricea datelor schimbate, care vor fi coordonate cu ANSC, Ministerul Finanțelor și entitatea responsabilă de operarea sistemului.

3.5.4. Integrarea cu registrele de stat

SIMED va putea prelua date din:

- Registrul de stat al populației, RSP;
- Registrul de stat al unităților de drept, RSUD;

4. CERINȚE FUNCȚIONALE

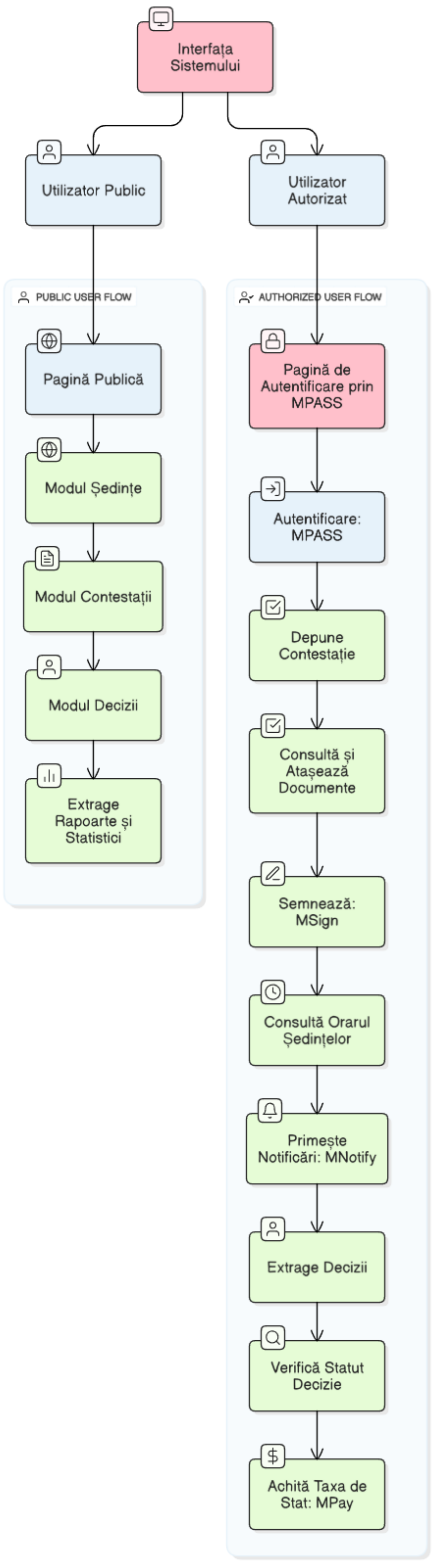
4.1. Cerințe funcționale pentru Portalul Public (Front Office)

Componenta Front Office a Sistemului Informațional de Management Electronic al Documentelor va reprezenta punctul unic de interacțiune electronică dintre Agenția Națională pentru Soluționarea Contestațiilor și utilizatorii externi ai sistemului, inclusiv contestatarii, autoritățile contractante, operatorii economici câștigători, reprezentanții autorizați, alte părți interesate și publicul larg.
Componenta Front Office va fi realizată prin reutilizarea, configurarea, adaptarea și, după caz, extinderea funcționalităților și componentelor disponibile în cadrul platformei FOD/PDSE. Contractantul nu va dezvolta de la zero funcționalități care sunt deja disponibile și pot fi reutilizate sau adaptate în cadrul FOD/PDSE.
Dezvoltarea unor funcționalități sau componente noi va fi permisă numai în situațiile în care cerințele funcționale specifice SIMED nu pot fi acoperite prin configurarea, adaptarea sau extinderea componentelor existente. Necesitatea dezvoltării unor asemenea funcționalități va fi justificată de Contractant prin analiza de decalaj, aprobată de ANSC și coordonată, după caz, cu Agenția de Guvernare Electronică.
Front Office-ul va utiliza conceptele și mecanismele arhitecturale aplicabile FOD/PDSE, inclusiv separarea dintre Front Office și Back Office, expunerea funcționalităților prin API-uri documentate, comunicarea bazată pe mesaje pentru procesele asincrone și integrarea cu serviciile guvernamentale partajate.
Componenta Front Office nu va accesa direct bazele de date sau resursele interne ale componentei Back Office. Schimbul de date și documente dintre cele două componente va fi realizat prin servicii aplicaționale securizate, cu verificarea identității utilizatorului, a drepturilor de acces și a contextului procedural.
Componenta Front Office va fi disponibilă, în funcție de categoria utilizatorilor, în următoarele regimuri de acces:

1. acces public, fără autentificare, pentru consultarea informațiilor și documentelor cu caracter public;
2. acces autorizat, prin Cabinetul Personal Digital, pentru contestatari, autorități contractante, operatori economici câștigători și alte părți procedurale;
3. acces prin redirecționare sau integrare cu alte puncte guvernamentale de acces la servicii electronice, inclusiv MCabinet și Portalul Serviciilor Publice, dacă aceste integrări sunt aplicabile și aprobate.

Interfața publică a SIMED va fi disponibilă la adresa web stabilită de ANSC, inclusiv, după caz, la adresa https://contestatii.ansc.md. Adresa finală, configurația domeniului și mecanismele de redirecționare vor fi stabilite și aprobate la etapa de proiectare și implementare.
Componenta Front Office va respecta Modelul Unitar de Design aplicabil serviciilor publice electronice și va reutiliza cu prioritate structurile de pagină, componentele vizuale, formularele, elementele de navigare, mesajele și mecanismele de interacțiune disponibile în cadrul FOD/PDSE.
Toate ecranele, formularele și fluxurile principale de utilizator vor fi prezentate inițial sub formă de prototipuri interactive. Prototipurile vor fi aprobate de ANSC și, după caz, coordonate cu AGE înainte de dezvoltarea sau configurarea finală.
Componenta Front Office va fi realizată în regim responsive și va asigura funcționarea corespunzătoare pe desktop, laptop, tabletă și dispozitive mobile. Interfețele destinate utilizatorilor externi vor respecta cel puțin nivelul AA al standardului WCAG 2.1.

Funcționalitățile disponibile în Front Office sunt organizate în module tematice, fiecare reflectând un flux procedural bine definit în cadrul ciclului de soluționare a contestațiilor și acces la metadatele publice conforme Legii 131/2015 privind achizițiile publice și normelor ANS



4.1.1. Principii funcționale generale ale componentei Front Office

Funcționalitățile componentei Front Office vor fi organizate astfel încât să asigure o interacțiune unitară, securizată și trasabilă între utilizatorii externi și componenta instituțională Back Office a SIMED.
Pentru fiecare funcționalitate Front Office, Contractantul va identifica și documenta:

- componenta sau funcționalitatea FOD/PDSE care urmează să fie reutilizată;
- configurațiile necesare;
- adaptările sau extensiile necesare;
- datele transmise către și recepționate din Back Office;
- serviciile guvernamentale utilizate;
- rolurile și drepturile de acces;
- regulile de validare;
- evenimentele care vor fi jurnalizate;
- notificările și confirmările generate;
- funcționalitățile care necesită dezvoltare nouă și justificarea acestora.

Componenta Front Office va respecta următoarele reguli funcționale generale:

1. Autentificarea utilizatorilor autorizați va fi realizată prin serviciul guvernamental MPass.
2. Dreptul persoanei autentificate de a acționa în numele unei persoane juridice va fi verificat, după caz, prin MPower sau prin alte surse oficiale aprobate.
3. MSign va fi utilizat pentru semnarea și verificarea documentelor electronice și nu va constitui un mecanism de autentificare a utilizatorului.
4. Notificările privind evenimentele procedurale vor fi transmise prin MNotify, în conformitate cu scenariile și șabloanele aprobate de ANSC.
5. Livrarea oficială a documentelor electronice va fi realizată, după caz, prin MDelivery sau prin alte canale oficiale aprobate, cu păstrarea dovezii transmiterii și recepționării.
6. Datele privind procedurile de achiziție vor fi preluate din SIA RSAP/MTender prin serviciile și interfețele oficiale puse la dispoziție de entitatea responsabilă de operarea sistemului.
7. Datele preluate din registrele de stat vor fi utilizate numai în limitele necesare realizării procesului procedural și în conformitate cu drepturile de acces și principiul minimizării datelor.
8. Orice transmitere a unei contestații, completări, punct de vedere sau alt document procedural va genera o confirmare electronică, identificabilă printr-un număr sau identificator unic și prin data și ora transmiterii.
9. Datele și documentele transmise de utilizator vor fi validate înainte de transmiterea către Back Office. Validarea la nivelul interfeței nu va exclude validarea repetată la nivelul serviciilor Back Office.
10. Utilizatorii vor putea salva în stare de proiect formularele care nu au fost încă semnate și transmise, dacă fluxul respectiv permite salvarea ca draft.
11. Utilizatorii vor avea acces numai la dosarele, documentele și operațiunile pentru care dețin drepturi explicite.
12. Datele și documentele publicate fără autentificare vor fi furnizate din Back Office numai după validarea, clasificarea și, după caz, anonimizarea acestora.

13. Toate operațiunile relevante vor fi jurnalizate, inclusiv autentificarea, accesarea dosarelor, crearea și modificarea proiectelor, încărcarea documentelor, semnarea, transmiterea și descărcarea documentelor.
14. În cazul indisponibilității temporare a unui serviciu extern, Front Office-ul va informa utilizatorul într-un mod clar și va evita pierderea nejustificată a datelor deja completate.
15. Pentru operațiunile asincrone, utilizatorul va putea consulta starea procesării, inclusiv stările „În procesare", „Transmis", „Recepționat", „Procesat" sau „Eșuat", după caz.
16. Interfața va prezenta mesaje clare privind erorile, câmpurile necompletate, documentele neacceptate, lipsa drepturilor și acțiunile necesare pentru continuarea procesului.
17. Funcționalitățile Front Office vor fi disponibile în limbile română, rusă și engleză, iar limba implicită va fi limba română.
18. Configurațiile, textele, șabloanele de notificare și elementele multilingve vor fi administrate separat de codul sursă, în măsura permisă de arhitectura FOD/PDSE.

4.1.2. Modulul public „Ședințe"

Fluxul digital al acestui modul este proiectat pentru a asigura transparența deplină asupra programului ședințelor de examinare a contestațiilor desfășurate de către Completul de Soluționare a Contestațiilor (CSC) în cadrul ANSC. Sistemul expune un set de endpointuri RESTful, securizate dar accesibile publicului (read-only), care interoghează baza de date din Back-Office pentru a extrage, în mod asincron, metadatele aferente fiecărei ședințe programate. Datele sunt serializate în format JSON standardizat, compatibil cu specificațiile OpenAPI, ceea ce permite integrarea ușoară cu componentele Front-Office.
Interfața utilizatorului este construită modular, pe un framework modern (React / Vue.js), și oferă trei modalități alternative de afișare a conținutului:

1. **Listă simplă** – o vizualizare cronologică compactă, optimizată pentru acces rapid și previzualizare pe dispozitive mobile.
2. **Grid interactiv (tabel dinamic)** – componentă centrală, de tip data grid interactiv, cu suport pentru:
    - căutare full-text în toate câmpurile indexate (obiectul achiziției, autoritate contractantă, complet etc.),
    - filtrare multi-nivel pe server (an, lună, zi, interval orar),
    - sortare pe coloane multiple (ex. dată, complet, autoritate),
    - paginare configurabilă (cu opțiuni per page: 10 / 25 / 50 / toate),
    - caching local pentru optimizarea performanței și reducerea numărului de request-uri redundante.
3. **Calendar interactiv** – vizualizare de tip „agenda" și „calendar lunar", generată printr-o librărie precum FullCalendar sau Day.js, în care fiecare ședință este reprezentată ca eveniment, cu posibilitatea de a vedea detaliile la hover sau click (ex. tooltip, pop-up sau drawer lateral).

În toate cele trei moduri de afișare, datele prezentate sunt consistene, agregate în funcție de utilizarea platformei și preferințele persistente ale utilizatorului (memorate local). Fiecare înregistrare de ședință este generată dinamic pe baza informațiilor disponibile și include următoarele câmpuri:

- **Titlul ședinței**, compus automat în funcție de obiectul contestației;

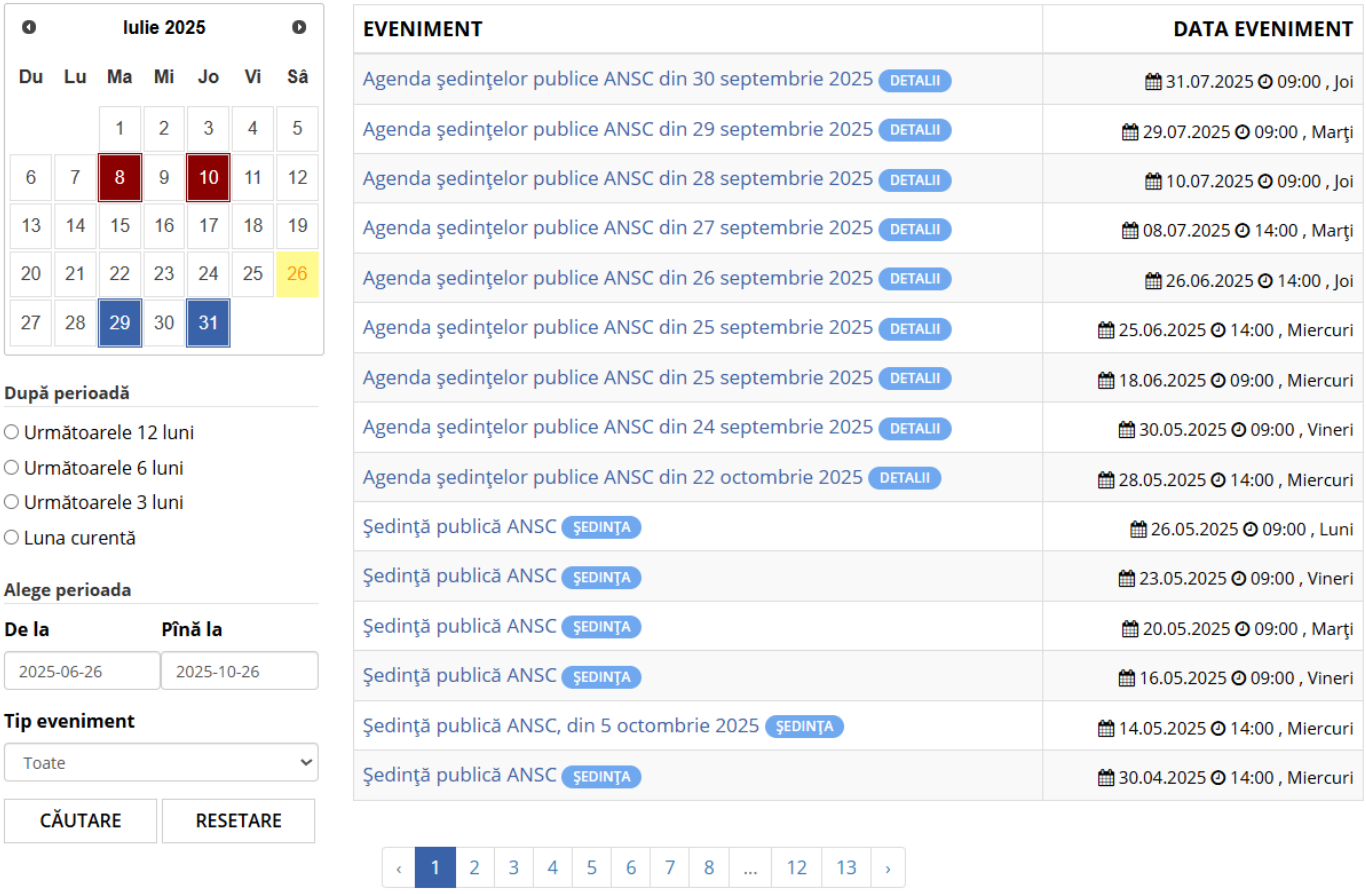
- **Număr oficial unic**, utilizat ca identificator intern și extern (referință procedurală);
- **Dată și oră exactă**, afișată în format timestamp standardizat UTC+2;
- **Părțile implicate**: denumirea contestatarului și autorității contractante;
- **Numărul de înregistrare a contestației**, se extrage automat din Back Office;
- **Obiectul achiziției**, cu afișarea codului CPV și a denumirii procedurii;
- **Completul de soluționare alocat**, cu trimitere directă către profilul public al completului respectiv;
- **Fișiere atașate**, dacă sunt disponibile:
    - procesul-verbal al ședinței, semnat digital (PDF + MSign);
    - înregistrări audio / video (livrate prin stream embedded cu fallback pentru descărcare în format MP4).

La nivel tehnic, fiecare tip de vizualizare utilizează un layer de abstracție pentru managementul stării aplicației (state management – Redux, Vuex sau echivalent), astfel încât utilizatorul poate comuta între listă, grid și calendar fără a reîncărca pagina, iar filtrările și căutările aplicate se păstrează coerent în toate modurile.

Accesul la acest modul este deschis și anonim, fără a fi necesară autentificarea sau crearea unui cont. Totodată, sistemul include protecție împotriva suprasolicitării (rate limiting) și logare pasivă pentru audit anonim al activităților de consultare, în vederea îmbunătățirii UX și monitorizării performanței.

Exemplu nr.1- de afișare a Agendei ședințelor

Exemplu nr.2- de afișare a Agendei ședințelor



4.1.3. Modulul public „Contestații”x

Modulul „Contestații” reprezintă un registru public digital, conceput pentru a asigura transparența operațională a activității ANSC în procesul de examinare a contestațiilor în materie de achiziții publice. Interfața acestui modul este orientată către publicul larg – inclusiv operatori economici, autorități contractante, jurnaliști, cercetători, organizații civice și orice parte interesată – și nu necesită autentificare prealabilă, fiind disponibilă în regim de acces deschis.

Platforma permite consultarea în timp real a tuturor contestațiilor aflate în proces de examinare sau înregistrate în cursul anului curent, prezentându-le într-un format tabular interactiv, intuitiv și scalabil. Datele afișate în tabelul public sunt extrase automatizat, în regim asincron, din componenta Back-Office al ANSC printr-un set de API-uri REST securizate, ce oferă răspunsuri în format JSON structurat. Sincronizarea este orchestrată printr-un mecanism de actualizare incrementală (delta sync), ceea ce permite atât performanță ridicată în randare, cât și consistență datelor.

Fluxul digital al acestui modul este susținut de o interfață tabulară avansată, dezvoltată prin tehnologii moderne de frontend (ex: React.js cu react-virtualized sau Angular + CDK Tables), cu logica de procesare asincronă, suport pentru filtrare la nivel de server (server-side filtering) și optimizare de performanță prin virtualizare de rânduri (row virtualization). Acest setup tehnologic permite gestionarea eficientă a dataset-urilor de mari dimensiuni, fără a afecta latența client-side.

Utilizatorii pot executa interogări complexe printr-un sistem de căutare multi-câmp și multi-criterial, incluzând:

- **Autoritatea contractantă** – autocomplete asistat prin integrarea cu registrul MConnect sau RSPJ;
- **Contestatar** – căutare după denumirea legală a operatorului economic sau ID fiscal;
- **Număr procedură** – validare sintactică a formatului, cu fallback în cazul formelor atipice.

Rezultatele sunt livrate în mod incremental (lazy loading) cu actualizări asincrone la fiecare modificare de filtru, fără reîncărcarea completă a interfeței, și sunt organizate în coloane dinamice cu funcționalitate de sortare interactivă și export tabelar în formate XLSX, CSV sau PDF.

Structura tabelului interactiv și câmpurile afișate:

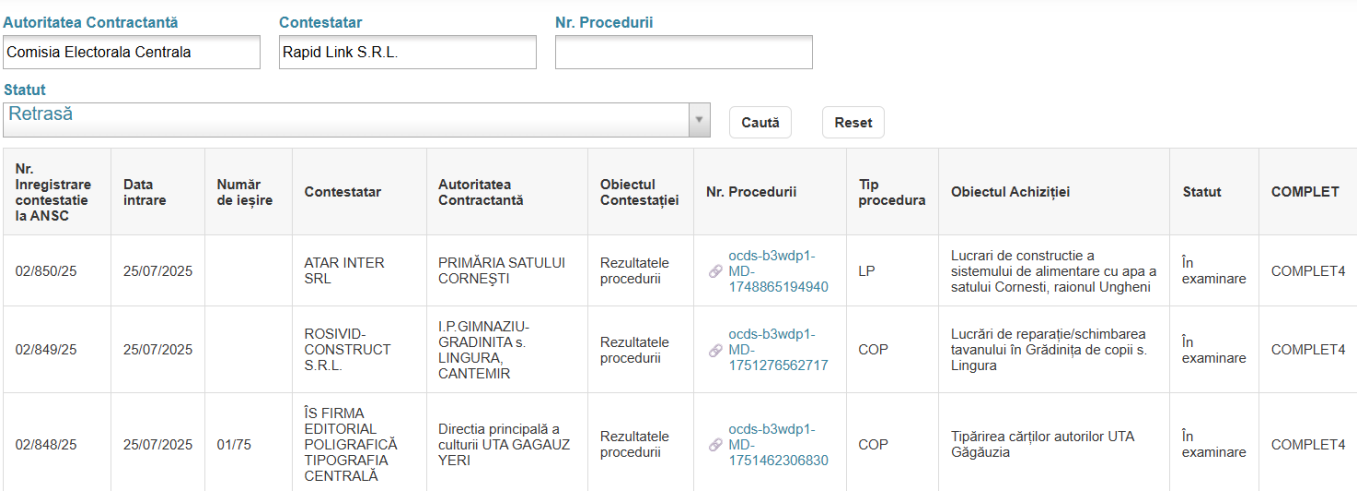
1. **Nr. înregistrare contestație la ANSC**– Identificator unic generat de sistemul intern ANSC la înregistrarea contestației; este afișat ca hyperlink către dosarul electronic public al contestației.
2. **Data intrare**– Data calendaristică și ora la care contestația a fost înregistrată în sistemul ANSC, în format timestamp ISO 8601.
3. **Număr de ieșire**– Numărul oficial atribuit în momentul transmiterii notificării către părțile implicate; generat automat din modulul de corespondență digitală.
4. **Contestatar**– Denumirea completă a entității juridice contestatare; poate include și codul de identificare fiscală pentru claritate.
5. **Autoritatea contractantă**– Numele complet al autorității vizate în contestație; afișarea este standardizată pe baza nomenclatorului MConnect.
6. **Obiectul contestației**– Este de fapt **titlul achiziției publice** asociate procedurii contestate, preluat automat din platforma MTender, și afișat ca text standardizat. Nu reprezintă un rezumat juridic, ci exact titlul atribuit în anunțul de participare de către autoritatea contractantă.
7. **Numărul procedurii**– Identificatorul formal al procedurii de achiziție publică, așa cum a fost definit în sistemul MTender. Este afișat cu hyperlink parametrizat care redirecționează utilizatorul către pagina procedurii respective în SIA RSAP.
8. **Tip procedură**– Tipologia juridică a procedurii (ex: licitație deschisă, apel de oferte, cerere de oferte, negociere fără publicare), extrasă automat din descriptorul asociat în MTender și afișată conform standardului EU-SIGMA.
9. **Obiectul achiziției**– Domeniul și categoria achiziției, afișat sub forma unei denumiri standardizate + cod CPV (Common Procurement Vocabulary), extrase din metadatele procedurii.
10. **Statut**– Reprezintă stadiul procedural actual al contestației. Valorile sunt definite printr-un nomenclator intern ANSC și pot include stări precum: „În analiză preliminară”, „În examinare”, „Decizie emisă”, „Arhivată”, „Contestatație retrasă” etc.
11. **Complet**– Denumirea completului CSC responsabil de examinarea contestației, cu hyperlink către profilul instituțional și istoricul deciziilor emise de acel complet.

Funcționalități suplimentare:

- **Export avansat** – utilizatorul poate exporta datele filtrate în XLSX, CSV sau PDF, printr-un endpoint de generare server-side. Exportul include opțiuni avansate de includere/excludere coloane și format de data.
- **Caching local** – rezultate recente sunt stocate temporar în browser prin IndexedDB sau Web Storage pentru performanță sporită la reinterogări frecvente.

- **Design accesibil** – toate elementele UI sunt conforme cu WCAG 2.1 AA, cu suport pentru navigare cu tastatura și screen-readere, pentru a asigura incluziune digitală maximă.

Modulul „Contestații" va păstra în totalitate forma tabelară și structura de coloane a tabelului existent pe pagina oficială ANSC, secțiunea „Contestații" (https://ansc.md/ro/contestatii/2025), servind ca referință vizuală și funcțională pentru afișarea inițială. Toate îmbunătățirile descrise în acest document se vor adăuga peste acest format de bază, fără a modifica structura cunoscută publicului, ci doar extinzându-i funcționalitatea și experiența de utilizare.



Nr. Inregistrare contestatie la ANSC	Data intrare	Număr de ieșire	Contestatar	Autoritatea Contractantă	Obiectul Contestației	Nr. Procedurii	Tip procedura	Obiectul Achiziției	Statut	COMPLET
02/850/25	25/07/2025		ATAR INTER SRL	PRIMĂRIA SATULUI CORNEȘTI	Rezultatele procedurii	ocds-b3wdp1-MD-1748865194940	LP	Lucrari de constructie a sistemului de alimentare cu apa a satului Cornesti, raionul Ungheni	În examinare	COMPLET4
02/849/25	25/07/2025		ROSIVID-CONSTRUCT S.R.L.	I.P.GIMNAZIU-GRADINITA s. LINGURA, CANTEMIR	Rezultatele procedurii	ocds-b3wdp1-MD-1751276562717	COP	Lucrări de reparație/schimbarea tavanului în Grădinița de copii s. Lingura	În examinare	COMPLET4
02/848/25	25/07/2025	01/75	ÎS FIRMA EDITORIAL POLIGRAFICĂ TIPOGRAFIA CENTRALĂ	Directia principală a culturii UTA GAGAUZ YERI	Rezultatele procedurii	ocds-b3wdp1-MD-1751462306830	COP	Tipărirea cărților autorilor UTA Găgăuzia	În examinare	COMPLET4

4.1.4. Modulul public „Decizii ANSC"

Modulul „Decizii" al Front Office-ului reprezintă un instrument esențial pentru asigurarea transparenței instituționale și a accesului nediscriminatoriu la informațiile publice privind soluționarea contestațiilor în domeniul achizițiilor publice. Acest modul este destinat utilizatorilor publici neautentificați și nu implică necesitatea de autentificare prin MPass sau integrarea cu servicii guvernamentale de identificare. Accesul este complet deschis, în regim de *read-only*, fiind aliniat cu principiile guvernanței deschise și cu prevederile legislației privind accesul la informație.

1. **Preluarea automată a datelor din Back Office**. Sistemul funcționează pe baza unei integrări bidirecționale cu Back Office-ul SIMED, unde sunt gestionate și arhivate deciziile oficiale emise de completurile CSC. Aceste decizii sunt exportate în timp real prin intermediul unui API REST securizat, în format JSON standardizat, care alimentează automat componenta Front Office. Transferul este realizat asincron, folosind mecanisme de polling incremental sau Webhooks pentru actualizare imediată.
2. **Indexare și motor de căutare semantică**. Fiecare decizie este supusă unui proces de indexare semantică, cu analiza sintactică a conținutului pentru a permite interogări full-text și filtrare avansată. Se utilizează un motor de căutare după următoarele câmpuri, care sunt și punctele de intrare pentru filtrare și sortare în interfața utilizatorului:
   - **Contestatar** – căutare după denumirea sau IDNO entității care a depus contestația (autocomplete activat);

- **Autoritatea contractantă** – entitatea publică vizată în decizie, cu sugestii live din registrul MConnect;
- **CSC (Completul de soluționare)** – selecție sau căutare după numele completului / membrilor;
- **Obiectul achiziției** – CPV și descriere, analizate semantic;
- **Statutul deciziei** – admisă, respinsă, parțial admisă, anulată etc., cu etichete vizuale distincte;
- **Conținutul deciziei** – permite interogare full-text în corpul deciziei (decizia motivată);
- **Critici și motive de contestație** – analizate pe baza sintagmelor extrase automat din text (ex. „lipsa justificării punctajului");
- **Obiectul contestației** – denumirea exactă a achiziției din MTender;
- **Numărul contestației (Nr. înregistrare la ANSC)** – identificator unic, permite sortare cronologică și căutare directă.

3. **Interfață tabulară interactivă cu rânduri expandabile (Expandable Row Table)** Pentru a evita congestia vizuală cauzată de cele 15 câmpuri obligatorii, modulul utilizează o interfață tabulară de tip *Expandable Row Table*. Aceasta permite afișarea unui subset esențial de coloane la nivelul de bază (Ex: Nr. decizie, Data adoptării, Contestatar, Autoritatea contractantă, Statut), iar printr-un gest de interacțiune (ex: clic pe rând sau icon de expandare), se afișează o sub-secțiune extinsă cu toate detaliile rămase.

Avantajele afișării de tip expandable row

- **Ergonomie și UX îmbunătățită**: Se evită utilizarea scroll-ului orizontal excesiv care afectează lizibilitatea, mai ales pe ecrane de dimensiuni reduse (ex. tablete, laptopuri).
- **Performanță**: Vizualizarea inițială se bazează pe virtualizarea rândurilor (row virtualization), ceea ce permite redarea rapidă a zeci sau sute de înregistrări fără suprasarcină de redare pe client.
- **Claritate contextuală**: Utilizatorii pot analiza rapid câmpurile critice, iar detaliile extinse sunt disponibile la cerere, fără a încărca inutil interfața.
- **Modularitate**: Designul suportă încărcarea asincronă a detaliilor extinse doar la cerere, ceea ce reduce traficul inițial și optimizează timpii de răspuns.

Descrierea coloanelor tabelului (metadate structurate)

1. **Nr. decizie** – Identificatorul unic al deciziei emise, generat automat și asociat cu hyperlink către fișierul deciziei în format PDF semnat digital.
2. **Data adoptării** – Data oficială de adoptare a deciziei, exprimată în format ISO (YYYY-MM-DD).
3. **Contestatar** – Denumirea oficială a persoanei juridice sau fizice care a depus contestația.
4. **Autoritatea contractantă** – Entitatea publică vizată de contestație, afișată cu denumirea legală completă.
5. **Obiectul contestației** – Titlul extrase din MTender care descrie achiziția contestată.
6. **Elementele contestației** – Descriere sintetică a motivelor invocate de contestatar.
7. **Complet** – Denumirea și codul completului decizional, cu hyperlink către profilul său (dacă este disponibil).
8. **Nr. procedurii** – Codul sau identificatorul unic al procedurii de achiziție, cu link direct către MTender 2.0.
9. **Conținutul deciziei** – Sumar al raționamentului și al concluziilor instanței administrative.
10. **Tip procedură** – Clasificarea tipului de procedură (ex: licitație deschisă, negociere, apel de oferte).

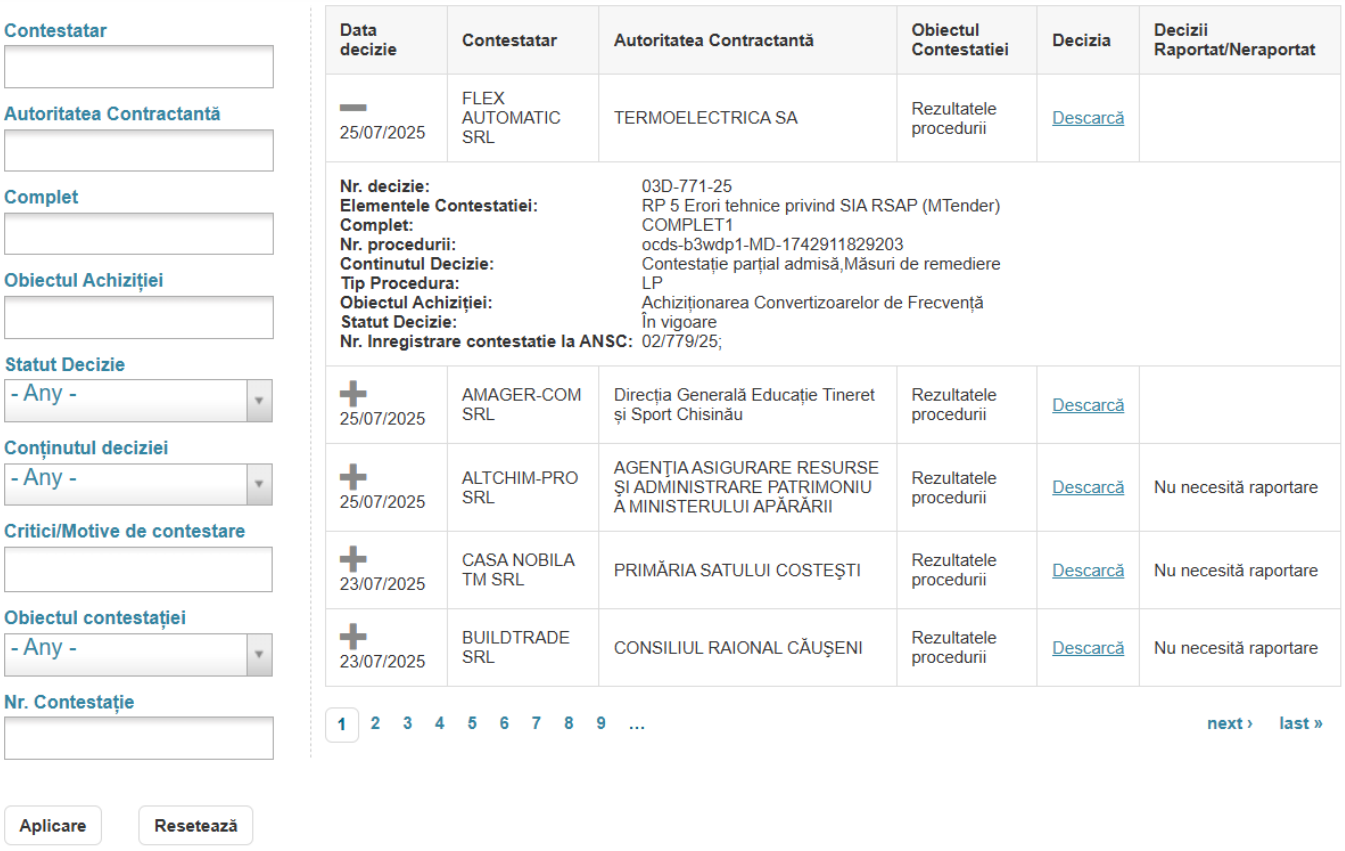
11. **Obiectul achiziției** – Denumirea bunurilor/serviciilor/lucrărilor achiziționate, însoțită de codul CPV aferent.
12. **Statut** – Rezultatul procedural al deciziei: admisă, respinsă, admisă parțial, anulată.
13. **Decizia (document)** – Link către documentul oficial în format PDF, semnat digital prin MSign, cu timestamp și hash SHA256.
14. **Decizii Raportat/Neraportat** – Indicator privind dacă decizia a fost raportată în sistemul de monitorizare.
15. **Nr. înregistrării contestației la ANSC** – Codul oficial al contestației care a generat decizia.

Viewer Decizie PDF și Metadate

La selectarea unei înregistrări, utilizatorul poate accesa decizia integrală într-un viewer PDF integrat în platformă, care oferă următoarele funcții:

- Redare inline fără a deschide fișierul într-o aplicație externă.
- Zoom, rotire, imprimare și descărcare.
- Afișare a metadatelor: timestamp-ul semnăturii, hash-ul criptografic, completul și versiunea semnăturii MSign.

Modulul „Decizii” va păstra în totalitate forma tabelară și structura de coloane a tabelului existent pe pagina oficială ANSC, secțiunea „Decizii” (https://www.ansc.md/ro/content/decizii-2025) , servind ca referință vizuală și funcțională pentru afișarea inițială. Toate îmbunătățirile descrise în acest document se vor adăuga peste acest format de bază, fără a modifica structura cunoscută publicului, ci doar extinzându-i funcționalitatea și experiența de utilizare, cum ar fi funcționalitatea de căutare, prezentă pe fiecare coloană.



4.1.5. Modulul public Rapoarte și Vizual Analytics

Modulul 4 –Rapoarte și Vizual Analytics reprezintă componenta analitică vizuală a Front Office-ului SIMED, dezvoltată pentru publicul general și orientată spre transparență decizională, inteligibilitate analitică și guvernanță deschisă în domeniul contestațiilor din achizițiile publice. Fiind o interfață read-only destinată utilizatorilor neautentificați, dashboard-ul facilitează explorarea datelor agregate privind activitatea decizională a ANSC printr-un set de vizualizări dinamice, bazate pe tehnologii moderne de vizualizare și procesare distribuită.

Implementarea modulului presupune un **pipeline digital** bine orchestrat, compus din următoarele etape funcționale:

1. Colectarea și centralizarea datelor (Back Office → Data Lake)

- Datele brute sunt extrase periodic (prin cron jobs sau webhook triggers) din modulele structurale ale Back Office-ului: **Registrul Contestațiilor** și **Registrul Deciziilor**.
- Informațiile colectate includ metadate, timestamp-uri, clasificări procedurale, coduri CPV, statuturi decizionale, identificatori unici etc.
- Acestea sunt ingestate într-un **data lake analitic** (bazat pe tehnologii precum PostgreSQL + TimescaleDB, BigQuery sau ElasticStack), unde sunt prevalidate și normalizate pentru analize ulterioare.

2. Prelucrarea asincronă și agregarea datelor

- Un modul de **ETL asincron** (Extract–Transform–Load) procesează datele în loturi, aplicând transformări semantice și agregări pe multiple dimensiuni (timp, tip achiziție, autoritate, statut).
- Se generează fișiere JSON optimizate pentru vizualizare rapidă, folosind tehnici de batch caching și minificare.
- Rapoartele predefinite sunt accesibile prin **RESTful API-uri**, cu latență minimă și suport pentru cache-control și lazy refresh.

3. Generarea vizualizărilor interactive

- În interfața Front-End, datele sunt încărcate asincron prin AJAX/Fetch API, afișate în **grafice interactive și panouri analitice** construite cu:
    - ApexCharts – pentru trenduri și serii temporale;
    - ECharts – pentru reprezentări complexe tip heatmap, scatter și radar;
    - Chart.js – pentru bar chart, pie chart și stacked comparisons.
- Utilizatorul poate naviga între vizualizări folosind **tab-uri tematice**, **slider temporal** (date picker), **tooltip contextual** și **filtrare multiplă**.

Dashboard-ul este structurat modular, pe secțiuni tematice (Ex: Contestații, Decizii, Autorități, Obiecte CPV), afișate într-un **grid reactiv**, compatibil cu toate dimensiunile de ecran (responsive layout). Designul favorizează:

- **Minimalism funcțional** – afișarea doar a indicatorilor esențiali, cu opțiune de drill-down;
- **Interactivitate incrementală** – animații fluide, tooltip contextual, zoom pe axele X/Y;

- **Exportabilitate extensivă** – fiecare grafic și raport poate fi exportat ca SVG, PNG, PDF sau în format tabelar Excel (XLSX).

Tipuri de rapoarte și statistici puse la dispoziția publicului larg:

1. Numărul total de contestații depuse în perioada selectată
2. Numărul de contestații aflate în examinare
3. Distribuția contestațiilor după statut procedural
4. Distribuția contestațiilor după tipul procedurii achiziției
5. Distribuția contestațiilor în funcție de obiectul contestației
6. Top 10 contestatari activi
7. Top 10 autorități contractante contestate
8. Distribuția contestațiilor după domeniul achiziției (CPV)
9. Evoluția lunară a volumului de contestații
10. Contestații multiple asupra aceleiași proceduri de achiziție
11. Numărul total de decizii emise într-un interval selectat
12. Distribuția deciziilor după rezultat
13. Timpul mediu de soluționare a unei contestații
14. Distribuția deciziilor după completul CSC
15. Distribuția deciziilor după tipul procedurii contestate
16. Distribuția deciziilor în funcție de obiectul contestației
17. Top 10 contestatari cu cele mai multe decizii admise
18. Top 10 autorități contractante cu cele mai multe decizii negative
19. Distribuția deciziilor pe domenii CPV
20. Rata de admitere a contestațiilor pe fiecare autoritate contractantă

4.1.6. Arhitectura funcțională și regimul de acces al cabinetului personal digital

Cabinetul Personal Digital reprezintă punctul unic, securizat și personalizat de interacțiune dintre utilizatorii autorizați și Agenția Națională pentru Soluționarea Contestațiilor (ANSC), fiind integrat în componenta Front Office a Sistemului Informațional de Management Electronic al Documentelor (SIMED). Acest spațiu digital este destinat exclusiv entităților eligibile, înregistrate în calitate de utilizatori autorizați în sistem și validate tehnic în baza profilului atribuit:

- **Contestatari** – operatori economici care formulează contestații împotriva documentației de atribuire sau a rezultatului procedurii de achiziție;
- **Autorități contractante** – instituții publice supuse contestației în calitate de organizatori ai procedurilor de achiziție;
- **Operatori economici câștigători** – actori contractuali implicați în calitate de părți terțe interesate în contestațiile care vizează rezultatul unei proceduri.

Accesul la Cabinetul Personal se realizează printr-un mecanism de autentificare federată avansată, utilizând serviciul guvernamental MPass în combinație cu semnătura electronică calificată furnizată prin MSign. La validarea identității digitale, sistemul generează un token criptografic JWT, care asigură, pe întreaga durată a sesiunii, integritatea comunicării, non-repudierea acțiunilor și trasabilitatea completă a tuturor operațiunilor efectuate.

După autentificare, utilizatorul este direcționat în mod automat către interfața Cabinetului Personal Digital – un spațiu digital adaptiv, conceput pentru a susține digitalizarea completă a fluxurilor procedurale privind

contestațiile în domeniul achizițiilor publice. Funcționalitățile disponibile sunt adaptate automat în funcție de rolul atribuit utilizatorului în cadrul sistemului.

Funcționalități disponibile pentru agentul economic în calitate de contestatar

Pentru operatorii economici care intenționează să depună o contestație, Cabinetul oferă o suită de funcționalități digitale specializate:

- Depunerea contestației prin completarea unui formular digital standardizat, diferit în funcție de obiectul contestației (documentele de atribuire/anunț de participare sau rezultatele procedurii);
- Pentru depunerea contestațiilor asupra rezultatelor procedurii, sistemul afișează automat doar acele achiziții la care compania a depus ofertă, identificându-le pe baza verificării codului fiscal (IDNO) în baza de date MTender;
- Pentru contestațiile privind documentația de atribuire, utilizatorul are acces la un motor de căutare integrat cu MTender, care permite identificarea procedurii prin MTender ID sau alte criterii;
- Încărcarea documentelor justificative în format electronic, cu validare automată a dimensiunii, extensiei și structurii semnăturii digitale (unde este cazul);
- Semnarea digitală a contestației și a anexelor prin MSign, cu generarea automată a versiunii PDF/A arhivabilă;
- Transmiterea criptată a dosarului procedural către sistemul Back Office al ANSC, cu confirmare automată de recepționare;
- Vizualizarea cronologică a etapelor de examinare, inclusiv data înregistrării, cereri de completare, programări pentru ședințe publice, notificări și decizia finală;
- Recepționarea notificărilor oficiale prin intermediul serviciului MNotify (e-mail, SMS sau notificare web);
- Acces la arhiva digitală a contestațiilor proprii, cu versiuni semnate, marcaj temporal (timestamp) și trasabilitate completă.

Funcționalități disponibile pentru autoritatea contractantă în calitate de parte contestată

Pentru autoritățile contractante vizate de o contestație, Cabinetul Personal asigură un cadru digital sigur pentru participarea procedurală:

- Acces instant la contestațiile care le vizează, imediat după depunerea acestora de către operatorul economic;
- Vizualizarea integrală a dosarului procedural, inclusiv conținutul contestației, anexe și metadate aferente;
- Transmiterea punctului de vedere oficial printr-un formular electronic dedicat, cu posibilitatea anexării de documente justificative;
- Semnarea electronică a răspunsului și transmiterea acestuia într-un canal securizat, cu stocare automată și disponibilitate imediată pentru completul ANSC și pentru contestatar;
- Primirea notificărilor generate de sistem privind cereri suplimentare (ex: clarificări, completări) și transmiterea electronică a răspunsurilor în termenul procedural stabilit;
- Acces la decizia ANSC și la notificările asociate, cu arhivare automată, dovadă de transmitere și trasabilitate.

Prin această structură funcțională, Cabinetul Personal Digital devine un instrument centralizat de interacțiune procedurală, care înlocuiește schimburile tradiționale pe hârtie cu o platformă digitală complet integrată, oferind transparență, eficiență, trasabilitate și conformitate cu cadrul legal aplicabil contestațiilor din domeniul achizițiilor publice.

4.1.7. Depunerea contestației, (rezultatele procedurii)

1. Autentificare inițială prin MPass și validare identitate cu MSign

La accesarea portalului Front Office SIMED, utilizatorul inițiază procesul de autentificare unică, în conformitate cu cerințele privind identificarea electronică sigură:

- Sistemul lansează automat fluxul de autentificare prin serviciul guvernamental MPass, utilizând protocolul OAuth 2.0/OpenID Connect, cu redirectare securizată către furnizorul de identitate;
- Utilizatorul selectează certificatul digital calificat din trusa de semnătură (smartcard, token USB, HSM sau certificat în cloud) și autorizează accesul;
- MSign este apelat pentru validarea semnăturii electronice asociate certificatului – operațiune ce confirmă posesia legitimă și valabilitatea juridică a identității;
- La finalizarea cu succes a autentificării, sistemul generează un token criptografic JWT (JSON Web Token) semnat, cu durată de viață limitată și scope specific aplicației, care conține:
    - IDNP-ul persoanei autentificate;
    - Numele complet și prenumele;
    - Adresa de e-mail asociată contului;
    - Serialul certificatului digital;
    - Timestamp de autentificare și autoritatea emitentă;
- Acest token este ulterior atașat tuturor cererilor de rețea ale utilizatorului (`via antet Authorization: Bearer <token>`), asigurând mecanismele de:
    - autenticitate a identității;
    - integritate a sesiunii;
    - non-repudiere a acțiunilor în cadrul Cabinetului Personal Digital.

Acest proces garantează că numai utilizatorii cu identitate digitală verificată și drepturi legale asociate unei entități economice pot accesa funcționalitățile sensibile ale sistemului SIMED.

2. Verificarea statutului juridic al persoanei autentificate

Imediat după finalizarea procesului de autentificare prin MPass și validarea identității digitale prin MSign, sistemul declanșează un mecanism suplimentar de control pentru a verifica legitimitatea procedurală a utilizatorului în raport cu entitatea economică vizată. Această etapă este esențială pentru a asigura că doar persoanele cu drepturi legale pot iniția sau semna contestații în numele unei companii. Verificarea se desfășoară în următoarea secvență logică:

Identificarea entității economice asociate: Sistemul determină automat IDNO-ul companiei corespunzător utilizatorului autentificat, pe baza mapării existente între IDNP și una sau mai multe entități economice înregistrate. În cazul în care utilizatorul are drepturi asupra mai multor companii, acestea sunt listate pentru selecție.

Validarea rolului juridic al persoanei: Se inițiază un apel către un serviciu de verificare a autorității de reprezentare:

- **Pentru reprezentanți legali (Administrator / Director):** sistemul interoghează în timp real **Registrul de Stat al Persoanelor Juridice** sau un serviciu echivalent interoperabil, pentru a verifica dacă IDNP-ul este asociat formal cu funcția de conducere a companiei selectate;
- **Pentru persoane împuternicite:** sistemul apelează **serviciul MPower**, verificând existența unui **mandat digital valid** care confirmă împuternicirea expresă a utilizatorului (IDNP) de a acționa în numele companiei (IDNO), pentru perioada curentă. Se validează:
    - IDNO companie;
    - IDNP utilizator;
    - tipul dreptului delegat (ex: semnare contestații);
    - data expirării mandatului;

- emitentul mandatului.

Decizie de autorizare:

- Dacă validarea este reușită (rol conform și mandat activ), sistemul procedează la inițializarea Cabinetului Personal Digital, personalizat pentru compania selectată și însoțit de privilegiile corespunzătoare;
- În caz contrar, accesul este refuzat, iar sistemul returnează un răspuns de eroare HTTP 403 – Forbidden, cu motivul specific („Utilizator neautorizat pentru această entitate juridică"). Încercarea este logată în jurnalul de audit, cu detalii privind:
  - IDNP și IDNO implicate;
  - tipul solicitării;
  - adresa IP și timestamp;
  - cauza blocării (ex: rol inexistent, mandat expirat, lipsă de asociere).

Această etapă este un mecanism critic de control al accesului în sistem, care asigură respectarea principiilor de identitate funcțională, non-repudiere și responsabilitate juridică, conform cadrului legal în vigoare. Astfel, doar utilizatorii cu atribuții legale sau mandat digital valid pot opera în numele entităților juridice în procedurile desfășurate prin SIMED.

3. Inițializarea Cabinetului Personal și preluarea procedurilor de achiziții din MTender

După validarea identității digitale și confirmarea statutului juridic al utilizatorului în raport cu entitatea economică selectată, sistemul procedează la inițializarea contextuală a Cabinetului Personal Digital pentru agentul economic, configurând interfața în funcție de drepturile sale operaționale.

În cadrul acestei inițializări, sistemul declanșează în mod asincron procesul de identificare a procedurilor de achiziție relevante pentru contestații, prin următoarele acțiuni tehnice:

- Se execută un apel REST autenticat către serviciul de interogare al platformei MTender:

```
GET /api/mtender/proceduri-active?IDNO=XXXXXXXX
Headers: Authorization: Bearer <JWT>
```

- API-ul MTender procesează cererea și returnează un payload JSON care conține lista completă a procedurilor în care compania identificată prin IDNO a participat în calitate de ofertant, împreună cu următoarele metadate relevante:
  - OCID (Open Contracting IDentifier) – identificator unic al procedurii;
  - Titlul achiziției – denumirea completă a obiectului contractului;
  - Autoritatea contractantă – denumirea instituției publice emitente;
  - Tipul procedurii – ex. licitație deschisă, cerere de ofertă, dialog competitiv;
  - Data publicării rezultatului – folosită ulterior pentru calculul termenului legal de contestație;
  - Status procedură – ex. „finalizată", „anulat", „adjudecat";
  - Număr ofertanți – pentru afișarea contextuală în interfața utilizatorului.

Datele recepționate sunt mapate într-o structură tabulară interactivă, vizibilă în dashboard-ul Cabinetului, cu funcționalități de sortare, filtrare și selecție a procedurii vizate. Utilizatorul poate astfel identifica rapid achizițiile asupra cărora are dreptul legal să formuleze contestație, pe baza participării confirmate în procesul competitiv.

Această etapă asigură filtrarea procedurală automată în baza participării reale, reducând riscul de contestații neeligibile și pregătind fundamentul pentru inițierea asistată a formularului de contestație în etapa următoare.

4. Afișarea procedurilor eligibile și inițierea contestației

După preluarea procedurilor în care operatorul economic a participat cu ofertă, sistemul Front Office SIMED afișează aceste informații într-o interfață interactivă destinată selecției rapide a obiectului contestației:

- Procedurile de achiziție sunt prezentate într-un tabel dinamic cu funcționalități avansate de filtrare și sortare, după criterii precum: titlul achiziției, autoritatea contractantă, data publicării rezultatului, status procedural, cod CPV;
- Utilizatorul selectează procedura pentru care consideră că au fost încălcate drepturile sale legitime;
- La selecție, sistemul declanșează inițializarea Formularului digital de contestație – Rezultatul procedurii, construit conform unui șablon standardizat ANSC și prepopulat automat cu metadatele relevante extrase din MTender, inclusiv:
    - Denumirea completă a autorității contractante;
    - Titlul și descrierea obiectului achiziției;
    - Tipul procedurii (ex. Licitație Publică – LP, Cerere de Ofertă – COP, Negociere fără Publicare – NFP);
    - Numărul de identificare al procedurii și OCID-ul asociat;
    - Codul CPV principal atribuit contractului;
    - Identitatea operatorului economic contestatar (nume entitate, IDNO), preluată din contextul sesiunii;
    - Mecanismul prin care a fost identificată presupusa încălcare – selectabil dintr-o listă (ex. rezultatul evaluării, nepublicarea punctajelor, lipsa justificării respingerii etc.).

Formularul este editabil în câmpurile dedicate descrierii faptei contestate și fundamentării juridice. Această etapă constituie punctul de inițiere formală a contestației, pregătind structura documentară ce urmează a fi completată, semnată și transmisă prin canale digitale securizate.

5. Completarea formularului de contestație și atașarea documentelor justificative

După inițializarea formularului digital, utilizatorul accesează secțiunea de completare a conținutului contestației, structurată logic în câmpuri predefinite, cu validatori de conținut și asistență contextuală:

- Subiectul contestației este introdus direct în formular, în câmpuri dedicate, după următoarea structură:
    - Argumente factuale – descrierea detaliată a situației contestate și a circumstanțelor în care a fost identificată presupusa încălcare a drepturilor legitime;
    - Fundamentare juridică – menționarea și explicarea normelor legale, articolelor din Legea achizițiilor publice sau din alte acte normative relevante care susțin contestația;
    - Observații suplimentare – elemente factuale, interpretări tehnice sau aspecte de procedură relevante pentru examinarea cazului.
- În secțiunea de încărcare a documentelor procesuale, utilizatorul atașează fișiere justificative relevante (ex. oferte respinse, notificări primite, extrase MTender, corespondență oficială), cu următoarele constrângeri tehnice:
    - Număr maxim fișiere: 10;
    - Dimensiune totală cumulată: 25 MB;
    - Formate permise: PDF, DOCX, JPG, PNG.
- La încărcare, sistemul declanșează automat procesul de validare a fișierelor:
    - Verificare tip MIME, pentru a preveni încărcarea fișierelor nepermise sau potențial periculoase;
    - Verificare dimensiune individuală și cumulativă;
    - Detecție automată a coruperii fișierelor (checksum intern și testare deschidere);

- Afișarea mesajelor de eroare detaliate în caz de încălcare a regulilor de încărcare.

Formularul și atașamentele pot fi salvate temporar într-o stare de tip *draft*, oferind utilizatorului posibilitatea de a reveni și a edita înainte de semnare și transmitere. Acest mecanism susține coerența logică a conținutului și respectarea cerințelor de formă ale dosarului de contestație.

6. Aplicarea semnăturii electronice și transmiterea contestației

După completarea formularului și atașarea documentelor justificative, sistemul pregătește dosarul contestației pentru semnare electronică calificată, conform cerințelor legale privind valabilitatea actelor procedurale transmise digital.

- Conținutul formularului este serializat automat în:
  - XML – structurat conform schemei XSD utilizate de ANSC pentru procesare automată;
  - PDF/A – versiune arhivabilă și lizibilă, destinată conservării și examinării umane.
- Semnarea digitală se realizează prin integrarea cu serviciul MSign:
  - Se calculează un hash criptografic al documentului;
  - Utilizatorul autorizează semnătura prin certificatul său calificat;
  - MSign aplică semnătura electronică calificată (PKCS#7), împreună cu timestamp-ul oficial și identificatorul certificatului.
- Documentul semnat este înregistrat în SIMED ca o instanță digitală validă a contestației, arhivată în zona de lucru a Cabinetului Personal Digital. Această etapă nu echivalează cu înregistrarea oficială la ANSC – este doar o validare internă în cadrul sistemului, care precede transmiterea formală către completul de soluționare.
- Sistemul generează:
  - Un UUID unic al contestației;
  - Hash SHA-256 al documentelor semnate;
  - Înregistrarea completă a metadatelor (data semnării, utilizator, IP, IDNO, IDNP) în jurnalul de audit

1. **Afișarea stării curente în Cabinet**
   - Contestația este afișată automat în secțiunea „Contestații active”, cu toate metadatele relevante (ID contestație, OCID procedură, dată depunere, stadiu procedural);
   - Se activează modulul de urmărire a statutului procedural în timp real, care reflectă dinamica dosarului: înregistrare, validare, examinare prealabila, examinare în fond, solicitări suplimentare, ședință, decizie;
   - Utilizatorul primește notificări automate (via MNotify) privind cererile ANSC de completare sau transmitere de documente procesuale;
   - Accesează și completează formulare digitale standardizate, preconfigurate în funcție de tipul solicitării (răspuns, clarificare, observație procedurală);
   - Semnează electronic orice document transmis către ANSC, direct din interfața Cabinetului, prin integrarea cu MSign;
   - Atașează documente justificative suplimentare în formate acceptate, cu validare automată a formatului, dimensiunii și consistenței cu cererea primită;
   - Primește notificări privind calendarul ședințelor publice ale Consiliului de Soluționare a Contestațiilor (CSC) aferente dosarului său, inclusiv data, ora, linkul de acces (dacă este cazul) și formatul participării;

- Este informat imediat ce decizia CSC este emisă, având acces la textul deciziei în format PDF semnat digital și arhivat;
- Poate consulta oricând istoricul complet al dosarului, inclusiv toate versiunile documentelor transmise/primite, cu marcaje temporale (timestamp), jurnale de audit și status de livrare/recepționare;
- În cazul existenței mai multor contestații simultane, poate filtra, sorta și accesa dosarele direct din interfața Cabinetului, în funcție de criterii precum: data depunerii, stadiu procedural, autoritate contractantă, sau tipul contestației.

4.1.8. Depunerea contestației, (documentele de atribuire/anunțul de participare)

Fluxul tehnic asociat depunerii unei contestații asupra documentației de atribuire sau anunțului de participare este, în linii mari, identic cu fluxul aplicabil în cazul contestațiilor referitoare la rezultatele procedurii, cu următoarele diferențe esențiale aplicabile punctului 3: selectarea obiectului contestației.
În cazul contestațiilor care vizează documentele de atribuire, nu este necesară participarea prealabilă la procedura de achiziție, ceea ce înseamnă că orice operator economic interesat se poate autentifica în Cabinetul Personal Digital din Front Office-ul SIMED și poate iniția o contestație, indiferent dacă a depus sau nu o ofertă pentru procedura vizată.
Pentru a evita importul exhaustiv și inutil al tuturor procedurilor publicate în MTender (care ar supraîncărca interfața Cabinetului), sistemul va pune la dispoziție un modul specializat de căutare asincronă a procedurii, activat doar în acest caz.
După autentificarea în sistem (MPass + MSign) și validarea statutului juridic, utilizatorul selectează opțiunea „Depune contestație –> Documente de atribuire / Anunț de participare". În locul preluării automate a procedurilor de achiziții din Mtender (ca în cazul depunerii contestației pe rezultatele procedurii), sistemul activează o interfață dedicată pentru căutarea manuală a achiziției publice vizate, cu filtrare asincronă.
Modulul de căutare asincronă permite identificarea precisă și importul selectiv al unei proceduri de achiziție relevante din sistemul MTender, utilizând următorul criteriu tehnic:

- **ID MTender (OCID)** – identificator unic de procedură generat conform standardului OCDS (ex.: ocds-b3wdp1-MD-1748262122481), introdus manual sau selectat din sugestiile oferite de interfață.

Odată cu selectarea validă a procedurii, sistemul inițiază automat procesul de extragere a metadatelor aferente (denumirea procedurii, autoritatea contractantă, cod CPV, tipul și statutul procedurii), pe baza cărora se preconfigurează **formularul electronic de contestație**.
Fluxul operațional ulterior – **completarea, semnarea digitală cu MSign și transmiterea securizată a contestației** – respectă aceleași standarde procedurale și pași tehnologici ca în cazul depunerii contestației asupra rezultatului procedurii, asigurând coerență, conformitate și trasabilitate integrală în cadrul Front Office-ului SIMED.
Această abordare modulară permite sistemului să trateze distinct cele două tipuri fundamentale de contestații și să mențină performanța optimă a Cabinetului Personal Digital, oferind în același timp acces deschis și conform cu legislația pentru operatorii economici care contestă actele preliminare ale unei proceduri de achiziție publică.

4.2. Cerințe funcționale pentru componenta instituțională Back Office

Componenta instituțională Back Office reprezintă nucleul funcțional și operațional al Sistemului Informațional de Management Electronic al Documentelor și este destinată utilizatorilor interni autorizați ai Autorității Naționale pentru Soluționarea Contestațiilor.

Back Office-ul va asigura gestionarea integrată a proceselor administrative, documentare, procedurale și decizionale ale ANSC, aferente întregului ciclu de viață al contestațiilor în domeniul achizițiilor publice, achizițiilor sectoriale și concesiunilor, începând cu recepționarea și înregistrarea contestației și până la emiterea deciziei, comunicarea acesteia, închiderea și arhivarea dosarului electronic.
Configurarea, adaptarea și dezvoltarea componentei Back Office vor fi realizate în funcție de:

- fluxurile operaționale ale ANSC;
- procesele de lucru ale subdiviziunilor și utilizatorilor interni;
- atribuțiile și competențele instituționale;
- regulile procedurale aplicabile soluționării contestațiilor;
- termenele stabilite de cadrul normativ;
- rolurile și drepturile utilizatorilor;
- nomenclatoarele și clasificatoarele instituționale;
- documentele, formularele și șabloanele utilizate de ANSC;
- cerințele privind trasabilitatea, auditul și arhivarea documentelor.

Componenta Back Office va fi configurată și adaptată astfel încât fluxurile, statuturile, termenele, sarcinile, documentele și regulile procedurale să reflecte în mod exact activitatea ANSC. Contractantul nu va implementa fluxuri generice care nu corespund proceselor instituționale și nu va modifica regulile procedurale fără aprobarea prealabilă a ANSC.
Back Office-ul va utiliza o stivă tehnologică compatibilă cu platforma FOD/PDSE și cu tehnologia .NET utilizată de aceasta. Componentele aplicaționale principale, serviciile backend, API-urile și mecanismele de integrare vor fi dezvoltate utilizând C# și .NET/ASP.NET Core într-o versiune Long-Term Support aflată în suport activ, în conformitate cu cerințele stabilite în Capitolul 5 privind stiva tehnologică guvernamentală.
Componenta Back Office va fi separată funcțional și tehnic de componenta Front Office. Front Office-ul destinat utilizatorilor externi va fi realizat prin reutilizarea și adaptarea funcționalităților FOD/PDSE, iar Back Office-ul va asigura procesarea internă și gestionarea oficială a datelor și documentelor procedurale.
Comunicarea dintre Front Office și Back Office se va realiza exclusiv prin:

- API-uri securizate, documentate și versionate;
- servicii aplicaționale autorizate;
- mesaje și evenimente pentru operațiunile asincrone;
- mecanisme de integrare aprobate în cadrul arhitecturii SIMED.

Front Office-ul nu va accesa direct bazele de date, sistemele de stocare, registrele interne sau alte resurse tehnice ale Back Office-ului. Orice solicitare de creare, consultare, modificare, transmitere sau descărcare a datelor și documentelor va fi procesată prin serviciile aplicaționale ale Back Office-ului, cu verificarea identității utilizatorului, a rolului, a drepturilor de acces și a contextului procedural.
Back Office-ul va constitui sursa oficială și autoritativă pentru datele și documentele procedurale gestionate de SIMED, inclusiv pentru:

- contestații;
- dosarele electronice ale contestațiilor;
- documentele de intrare și ieșire;
- documentele procesuale;
- părțile implicate;
- procedurile de achiziție asociate;
- completele de soluționare a contestațiilor;
- repartizarea contestațiilor;
- ședințele și procesele-verbale;
- termenele și sarcinile procedurale;
- proiectele și versiunile deciziilor;

- deciziile finale;
- notificările și comunicările;
- statuturile și istoricul procesării;
- registrele și rapoartele instituționale.

Datele afișate în Front Office, în Cabinetele Digitale sau în interfața publică vor fi furnizate de Back Office prin API-uri și vor reflecta informațiile oficiale gestionate de acesta. Publicarea datelor și documentelor se va realiza numai după aplicarea regulilor privind validarea, aprobarea, clasificarea, anonimizarea, protecția datelor cu caracter personal și accesul la informațiile publice.

Back Office-ul va asigura un model unitar al dosarului electronic, în cadrul căruia toate datele, documentele, sarcinile, termenele, acțiunile, comunicările, ședințele și deciziile aferente aceleiași contestații vor fi corelate prin identificatori unici și vor putea fi urmărite pe întregul ciclu procedural.

Fiecare operațiune relevantă efectuată în Back Office va fi jurnalizată și va păstra cel puțin:

- identitatea utilizatorului sau a serviciului care a inițiat operațiunea;
- data și ora operațiunii;
- tipul acțiunii efectuate;
- obiectul informațional afectat;
- valorile anterioare și valorile noi, după caz;
- statutul procesării;
- rezultatul operațiunii;
- motivul modificării sau anulării, atunci când este aplicabil;
- identificatorul tehnic de corelare a tranzacției.

Back Office-ul va utiliza MPass pentru autentificarea utilizatorilor interni autorizați. Drepturile funcționale vor fi acordate și verificate conform modelului de control al accesului bazat pe roluri implementat în SIMED. MSign va fi utilizat pentru semnarea și verificarea documentelor electronice pentru care semnătura este obligatorie și nu va fi utilizat ca mecanism de autentificare.

Componenta Back Office va permite gestionarea parametrilor și configurațiilor funcționale care pot fi modificate fără intervenție asupra codului sursă, inclusiv nomenclatoare, șabloane, termene, statuturi, alerte, notificări, structuri organizaționale, componența completelor și alte reguli configurabile aprobate de ANSC. Modificarea configurațiilor funcționale va fi permisă numai utilizatorilor autorizați și va fi supusă versionării și jurnalizării. Modificările nu vor produce efecte retroactive asupra dosarelor și documentelor deja finalizate, cu excepția cazurilor aprobate expres și documentate.

În cazul indisponibilității temporare a Front Office-ului sau a unui serviciu guvernamental extern, Back Office-ul va continua să permită executarea operațiunilor interne care nu depind în mod direct de serviciul indisponibil. Operațiunile de integrare eșuate vor fi înregistrate, monitorizate și, după caz, reluate controlat, fără duplicarea datelor sau pierderea trasabilității.

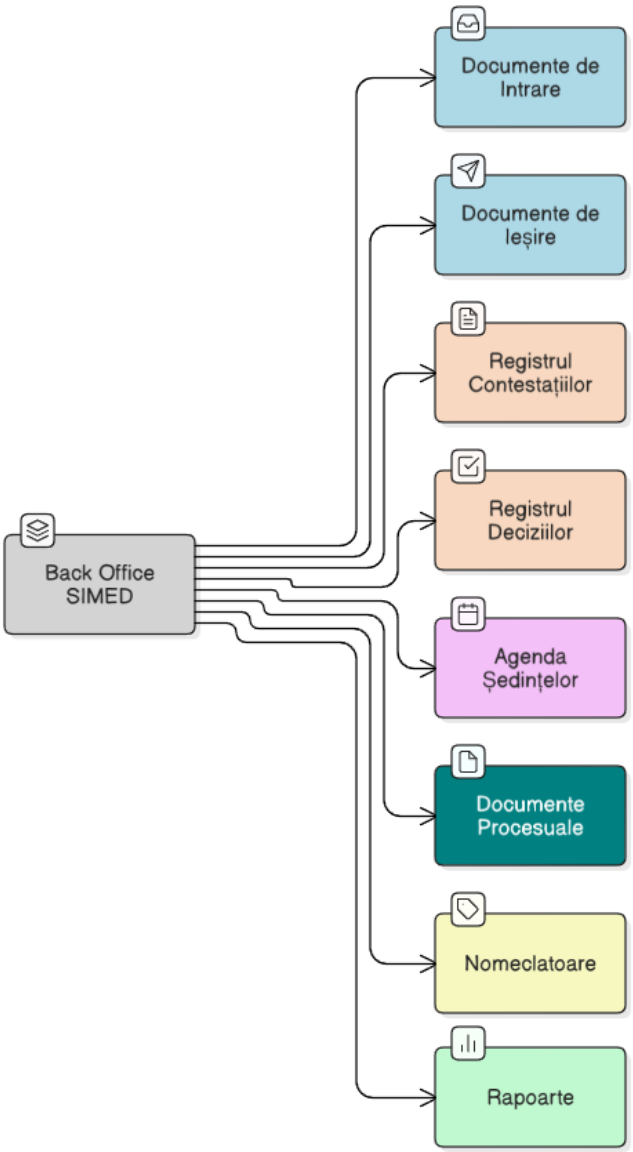
Back Office-ul va include următoarele module funcționale principale:

1. **Documente de intrare** – pentru recepționarea, înregistrarea, clasificarea, verificarea și asocierea documentelor primite cu dosarele și procesele corespunzătoare;
2. **Documente de ieșire** – pentru elaborarea, avizarea, semnarea, înregistrarea, expedierea și urmărirea documentelor emise de ANSC;
3. **Registrul contestațiilor** – pentru evidența oficială și gestionarea ciclului de viață al contestațiilor și al dosarelor electronice;
4. **Registrul deciziilor** – pentru gestionarea proiectelor, versiunilor, avizării, semnării, înregistrării, comunicării și publicării deciziilor ANSC;
5. **Agenda ședințelor** – pentru planificarea, organizarea, desfășurarea și evidența ședințelor completelor de soluționare a contestațiilor;

6. **Documente procesuale** – pentru generarea, redactarea, avizarea, semnarea, transmiterea și arhivarea documentelor aferente procesului de soluționare a contestațiilor;
7. **Nomenclatoare** – pentru administrarea centralizată și versionată a clasificatoarelor, statuturilor, tipurilor de documente, termenelor și altor valori de referință utilizate în SIMED;
8. **Rapoarte** – pentru generarea rapoartelor operaționale, manageriale, statistice și publice pe baza datelor oficiale gestionate de sistem;
9. **Administrare** – pentru gestionarea profilurilor aplicaționale, rolurilor, drepturilor, structurii organizaționale, completelor CSC, parametrilor, șabloanelor, configurațiilor și integrărilor sistemului.

Modulele Back Office vor utiliza același model de date și aceiași identificatori oficiali pentru a evita duplicarea și inconsistența informațiilor. Datele comune vor fi înregistrate o singură dată și reutilizate în toate modulele în care sunt necesare.

Contractantul va detalia, la etapa de analiză și proiectare, relațiile dintre module, entitățile informaționale gestionate, regulile de business, statuturile, tranzițiile, rolurile, permisiunile, API-urile și mesajele utilizate. Modelul funcțional detaliat va fi aprobat de ANSC înainte de implementarea finală.



4.2.1. Documente de intrare

Modulul „Documente de Intrare” reprezintă un element fundamental în cadrul componentei Back Office a Sistemului Informațional de Management Electronic al Documentelor (SIMED), fiind dedicat prelucrării centralizate și eficiente a tuturor materialelor documentare recepționate de Agenția Națională pentru Soluționarea Contestațiilor (ANSC). Acesta este conceput ca o interfață de interoperabilitate instituțională, care asigură înregistrarea, clasificarea și integrarea documentelor primite în fluxurile operaționale ale instituției, într-un mod coerent și complet auditat.
Modulul este construit pentru a răspunde unui spectru larg de scenarii de recepție, incluzând documente transmise prin poștă, curier, e-mail, sistemele guvernamentale de comunicații (MConnect, MDelivery), precum și prin canale digitale dedicate – precum interfața Front Office a SIMED. Prin acest mecanism, ANSC beneficiază de un cadru robust pentru recepția și prelucrarea automată sau asistată a documentelor provenite de la diverși expeditori: instituții ale administrației publice, autorități contractante, operatori economici, organizații ale societății civile și cetățeni.
Funcționalitatea esențială a modulului constă în consolidarea într-un registru electronic unic a tuturor documentelor primite, cu alocarea automată a metadatelor obligatorii – precum data și ora recepției, tipul documentului, entitatea expeditorului, canalul de transmitere, referințele interne sau externe – și cu stabilirea automată a conexiunii cu dosare sau proceduri aflate în derulare. Această abordare permite nu doar trasabilitatea completă a circuitului documentar, ci și integrarea contextuală a documentelor în cadrul proceselor decizionale și procedurale ale Autorității.
Modulul este susținut de o logică tehnologică flexibilă, capabilă să distingă automat tipurile de documente administrative, contestații formale, solicitări de clarificare, puncte de vedere, notificări, corespondență generală sau anexe tehnice, pentru a asigura o clasificare temeinică și un tratament procedural adecvat fiecărui caz în parte. Fiecare document este înregistrat într-o fișă electronică de evidență, ce permite validarea datelor, atașarea de fișiere, asocierea cu actori relevanți din sistem (contestatar, autoritate contractantă, terț implicat), precum și inițierea automată a fluxurilor de lucru interne, conform regulilor prestabilite.
Arhitectura acestui modul sprijină eficient corelarea între fluxurile de lucru documentare și ciclul de viață al procedurilor de contestație, facilitând deciziile rapide, organizarea arhivei electronice, precum și auditarea proceselor în conformitate cu cerințele legale și bunele practici în domeniul managementului documentelor.

REGULI LOGICE ȘI INTEGRARE PROCEDURALĂ

1. Înregistrarea unui document de intrare – general

Această regulă se aplică oricărui document oficial recepționat de ANSC prin orice canal – fizic, electronic sau alt mijloc de comunicare – care nu este asociat unei contestații în materie de achiziții publice. Câmpurile obligatorii din fișa de înregistrare:

- **Număr intern de înregistrare** – generat automat de sistem, unic, incremental, pe anul calendaristic curent;
- **Data înregistrării** – preluată automat din sistemul informatic (cu opțiune de selectare manuală de către utilizator, în cazuri justificate);
- **Expeditor** – selectabil din nomenclatorul oficial de entități (autorități publice centrale și locale, agenți economici, ONG-uri, persoane fizice), cu funcționalitate de autocomplete și filtrare avansată;
- **Număr de ieșire al documentului (la expeditor)** – introdus manual;
- **Data emiterii documentului de către expeditor** – selectabilă din calendar interactiv;
- **Tip document** – selectat din nomenclatorul oficial (ex: scrisoare oficială, solicitare informație, punct de vedere, notificare, sesizare, etc.);

- **Conținut / Obiectul documentului** – descriere text liber, până la 2000 caractere;
- **Modalitate de recepționare** – opțiuni predefinite (poștă, e-mail, depus fizic la anticameră, fax, MConnect, MDelivery etc.);
- **Executor (responsabil)** – selectabil din structura organizațională a ANSC (cu căutare și filtrare după departament și funcție);
- **Termen de executare** – selectabil dintr-un nomenclator de termene standardizate sau stabilit manual;
- **Stare document** – nou, în lucru, procesat, clasat, transmis, arhivat (gestionat automat pe baza ciclului de viață);
- **Fișiere atașate** – suport pentru încărcarea documentelor scanate, format PDF sau Office.

În baza acestei fișe, documentul este salvat în Registrul Documentelor de Intrare, unde i se va asocia un cod arhivistic unic, fiind păstrat în funcție de metadate precum: anul, luna și canalul de recepționare.

2. Înregistrarea unui document de intrare asociat unei contestații, depus prin Cabinet Personal.

Pentru cazurile în care documentul de intrare este transmis către ANSC prin intermediul componentei Front Office->Cabinet Personal și este asociat **în unei proceduri de contestație**, sistemul activează logica de **preluare automată și asociere contextuală** pe baza metadatelor transmise din Front Office sau completate de operatorul uman.

Câmpuri din fișa de înregistrare, cu preluare automată acolo unde este posibil:

- **Număr intern de înregistrare** – generat automat de sistem;
- **Data înregistrării** – preluată automat;
- **Expeditor** – preluat automat din profilul Cabinetului Personal Digital (AC, contestatar, câștigător), dacă documentul provine din Front Office; în caz contrar, completat manual din nomenclator;
- **Număr și dată de ieșire ale expeditorului** – completate manual sau preluate automat dacă sunt incluse în metadatele atașate;
- **Număr contestație** – preluat automat din metadatele documentului digital, dacă documentul este transmis prin Front Office;
- **Număr procedură achiziție** – preluat automat (dacă este inclus în metadate), sau completat manual;
- **Cod CPV și LOT** – selectate din nomenclator, dacă nu au fost preluate automat;
- **Tip document** – selectat din nomenclator oficial (ex: notificare suplimentară, răspuns, solicitare de amânare, etc.);
- **Conținut** – completat manual;
- **Executor responsabil** – selectat din lista de utilizatori activi;
- **Termen de executare** – completat conform prioritizării interne;
- **Canal de recepționare** – determinat automat sau selectabil (ex: Front Office, MDelivery, e-mail, etc.);
- **Fișiere atașate** – obligatorii, în format PDF/A sau compatibil Office.

Documentul astfel înregistrat este automat asociat dosarului digital al contestației respective, păstrând și referința în Registrul General al Documentelor de Intrare. Sistemul generează automat legătura între document și entitatea de referință (contestația, procedura, autoritatea), pentru a asigura trasabilitate completă.

3. Înregistrarea unui document de intrare asociat unei contestații (depus fizic sau trimis pe e-mail)

În cazul în care un document de intrare este transmis **prin poșta electronică oficială** a ANSC sau **depus fizic la anticamera instituției**, iar acesta este **asociat unei proceduri de achiziție publică contestate**, funcționarul desemnat din cadrul Direcției Tehnologii Informaționale și Securitate Digitală (DTISD) este responsabil de **completarea integrală a fișei de înregistrare a documentului**.

Procesul presupune următoarele acțiuni și reguli logice:

Completarea fișei de înregistrare – câmpuri obligatorii:

- **Număr intern de înregistrare** - generat automat de sistem, în baza unui contor unic, secvențial.
- **Data înregistrării** - preluată automat din sistemul informatic; utilizatorul poate modifica manual doar în limitele reglementate de procedură.
- **Expeditor** - selectat din nomenclatorul de entități publice/private (autocomplete), sau introdus manual dacă este un expeditor neînregistrat anterior.
- **Număr de ieșire** al expeditorului: introdus manual, conform mențiunilor din antetul documentului.
- **Data documentului la expeditor** - selectată prin calendar (date picker).
- **Tipul documentului** - ales din nomenclatorul oficial (de ex. cerere, contestație, adresă, notificare, etc.).
- **Conținut / Obiect** - descriere sintetică a conținutului documentului.
- **Executor desemnat** - selectat din organigrama digitală a instituției (funcționalitate de căutare rapidă).
- **Departament responsabil** - selectat din structura organizatorică a ANSC.
- **Termen de executare** - definit prin selector de dată (calendar) sau ales din termene standardizate configurabile.
- **Modalitate de recepționare** - selectat din lista de opțiuni – e-mail, poștă fizică, depunere la anticameră, alt canal.
- **Document scanat / atașat** - atașarea documentului în format PDF/DOC, cu posibilitatea adăugării de anexe multiple.

Asocierea documentului la contestație:

Pentru documentele ce conțin informații ce permit identificarea unei contestații deja existente, se vor completa următoarele câmpuri suplimentare:

- **Numărul contestației**: selectat din nomenclatorul contestațiilor active, care va prelua deja automat următoarele câmpuri
    - **Contestatar**
    - **Numărul procedurii de achiziție**
    - **CPV**
    - **LOT**:
    - **Denumirea autorității contractante**:

După finalizarea procesului de înregistrare, documentul va fi salvat simultan:

- în **Registrul Documentelor de Intrare**;
- în **Registrul Contestațiilor->dosarul digital al contestației** relevante, dacă a fost asociat corect.

Trasabilitatea documentului, istoricul modificărilor și atribuțiile executorului vor fi stocate și disponibile pentru audit, înregistrări statistice și verificări intern.

Totodată, indiferent de procedura de depunere și înregistrare a documentului, sistemul permite, în mod opțional, ca funcționarul responsabil din cadrul DTISD să realizeze manual asocierea unui document de intrare la o contestație existentă. În acest caz, documentul respectiv va fi integrat automat în dosarul digital aferent procedurii, asigurând coerența procedurală și integritatea arhivei instituționale.

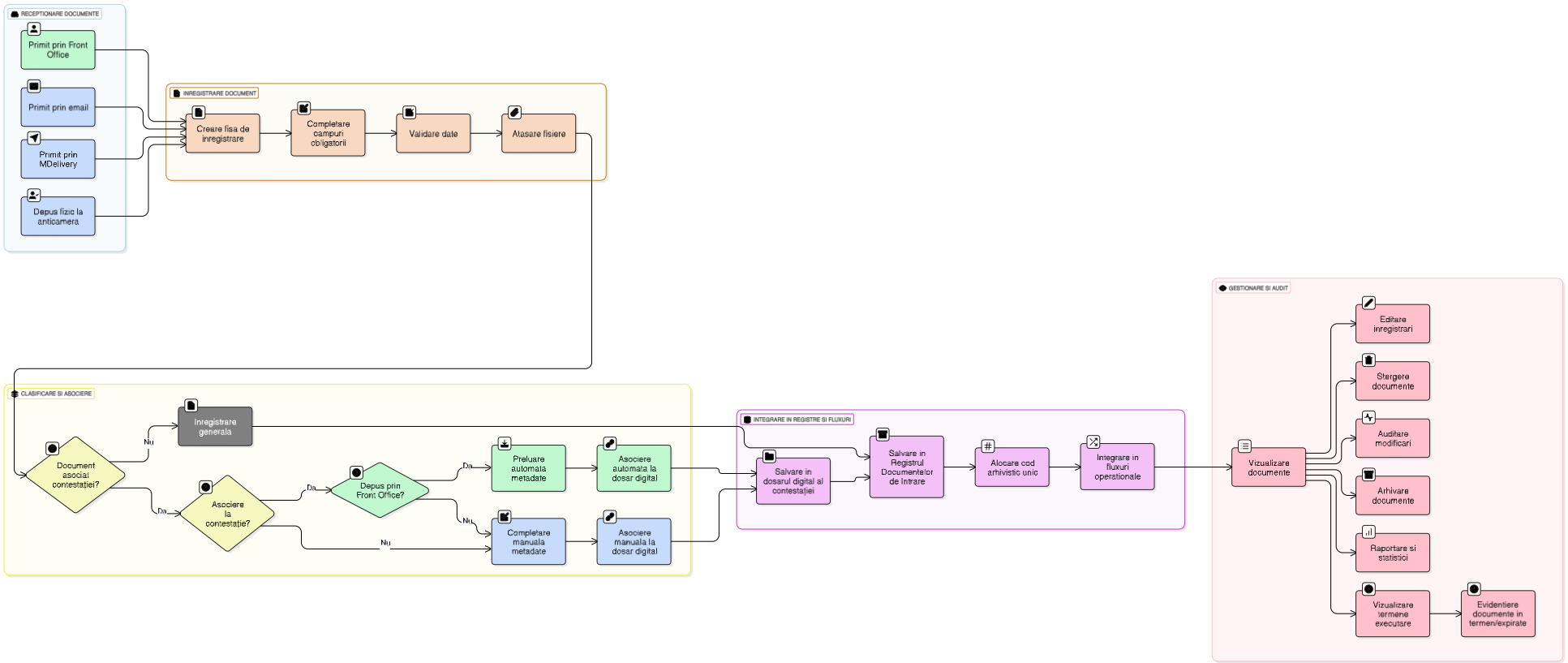
Toate documentele de ieșire vor fi afișate într-o interfață tabelară dinamică, cu funcționalități avansate de sortare, căutare și filtrare aplicabile individual pe fiecare coloană. Sistemul va include obligatoriu un mecanism de paginare și afișare configurabilă a numărului de înregistrări per pagină.

Utilizatorii autorizați vor avea posibilitatea de a:

- edita înregistrările documentelor de ieșire (cu păstrarea istoricului modificărilor);
- șterge documente în cazuri justificate, în conformitate cu politicile de audit și control intern.

Tabelul de bord al modulului va include o vizualizare sintetică a termenelor de executare asociate fiecărui document. Vor fi evidențiate distinct:

- documentele aflate în termen, documente expirat


RECEPTIONARE DOCUMENTE
Primit prin Front Office
Primit prin email
Primit prin MDelivery
Depus fizic la anticamera
INREGISTRARE DOCUMENT
Creare fisa de inregistrare
Completare campuri obligatorii
Validare date
Atasare fisiere
CLASIFICARE SI ASOCIERE
Inregistrare generala
Document asociat contestației?
Da
Nu
Asociere la contestație?
Da
Nu
Depus prin Front Office?
Da
Nu
Preluare automata metadate
Asociere automata la dosar digital
Completare manuala metadate
Asociere manuala la dosar digital
INTEGRARE IN REGISTRE SI FLUXURI
Salvare in dosarul digital al contestației
Salvare in Registrul Documentelor de Intrare
Alocare cod arhivistic unic
Integrare in fluxuri operationale
GESTIONARE SI AUDIT
Vizualizare documente
Editare inregistrari
Stergere documente
Auditare modificari
Arhivare documente
Raportare si statistici
Vizualizare termene executare
Evidentiere documente in termen/expirate

Fișa electronică a documentului de intrare

Pentru fiecare document recepționat, sistemul va crea o fișă electronică de evidență care va include cel puțin:

- identificatorul unic intern;
- identificatorul tehnic al transmiterii, dacă este aplicabil;
- numărul oficial de intrare;
- data și ora recepționării;
- data și ora înregistrării oficiale;
- canalul de recepționare;
- tipul și categoria documentului;
- numărul și data documentului expeditorului;
- expeditorul;
- datele de contact ale expeditorului, dacă sunt necesare;
- persoana în numele căreia se acționează;
- obiectul sau descrierea succintă;
- nivelul de acces și clasificarea documentului;
- contestația și dosarul asociat;
- procedura de achiziție asociată;
- subdiviziunea și executorul responsabil;
- termenul de examinare sau executare;
- fișierele și anexele;
- datele privind semnătura electronică;
- starea verificării;
- statutul documentului;
- istoricul operațiunilor;
- notificările și confirmările generate.

Câmpurile obligatorii vor fi configurate în funcție de tipul documentului și canalul de recepționare.

Clasificarea și asocierea documentelor

Sistemul va permite clasificarea automată sau asistată a documentelor în categorii precum:

- contestație;
- completare la contestație (se va selecta o contestație din Registru);
- punct de vedere;
- răspuns la solicitarea ANSC;
- document al procedurii de achiziție;
- cerere de recuzare;
- declarație de abținere;
- retragere a contestației;
- solicitare de clarificare;
- probă sau anexă;
- corespondență instituțională generală;
- alt tip configurat în nomenclator.

Documentul va fi asociat automat cu o contestație sau un dosar atunci când mesajul recepționat conține un identificator valid și suficient pentru realizarea asocierii.

Funcționarul autorizat va putea efectua sau corecta manual asocierea în cazurile în care:

- identificatorul nu este prezent;
- identificatorul este eronat;

- există mai multe dosare posibile;
- documentul a fost recepționat printr-un canal nedigital;
- asocierea automată nu poate fi realizată cu suficientă certitudine.

Asocierea sau reasocierea manuală va necesita selectarea dosarului, indicarea motivului și păstrarea istoricului complet.
După asociere, documentul va deveni parte a dosarului electronic și va fi disponibil utilizatorilor interni și externi numai în limitele drepturilor aplicabile.

Statutele documentelor de intrare
Modulul va utiliza statuturi configurabile, distincte de statuturile contestației. Acestea vor include cel puțin:

- Recepționat;
- În curs de verificare;
- Necesită clarificare;
- Respins tehnic;
- Validat;
- Înregistrat;
- Neasociat;
- Asociat dosarului;
- Repartizat;
- În examinare;
- Executat;
- Închis;
- Marcat ca introdus eronat;
- Anulat.

4.2.2. Documente de ieșire

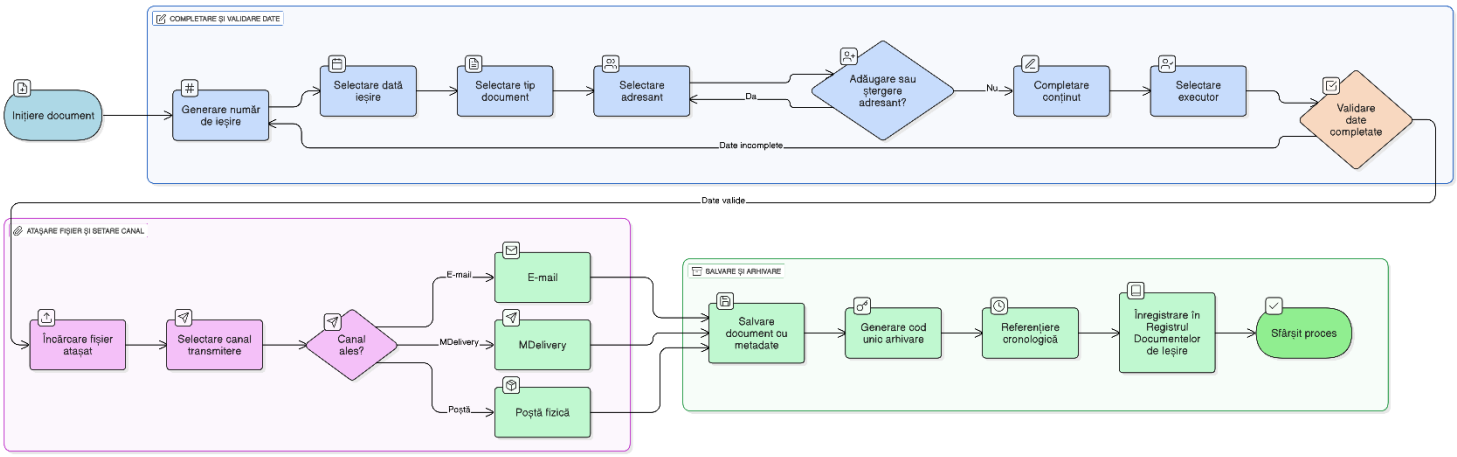
Modulul „Documente de Ieșire" este o componentă integrată a platformei instituționale Back Office SIMED, dedicată managementului digital al tuturor actelor oficiale emise de Agenția Națională pentru Soluționarea Contestațiilor (ANSC). Acest modul gestionează documentele de ieșire în contextul corespondenței instituționale, al activităților operaționale și al procesului de soluționare a contestațiilor în materie de achiziții publice, indiferent de canalul de expediere sau statutul procedural al documentului.
Sistemul oferă suport complet pentru întocmirea, etichetarea, arhivarea și transmiterea electronică a documentelor de ieșire, fiind conectat la mecanismele interne de procesare documentară și integrat cu nomenclatoarele instituționale, registrele digitale și canalele naționale de comunicare (ex. MDelivery, MSign). Platforma permite o asociere contextuală automată sau manuală a documentelor cu entitățile relevante (agenți economici, autorități contractante, APL, APC, cetățeni), asigurând trasabilitate, auditabilitate și conformitate procedurală.
Documentele de ieșire sunt clasificate în trei mari categorii funcționale, fiecare având un flux logic propriu.
REGULI LOGICE ȘI INTEGRARE PROCEDURALĂ
1. Document de ieșire general (neasociat contestațiilor și independent de documentele de intrare)
Acest tip de document este utilizat pentru comunicări instituționale uzuale, care nu sunt generate ca urmare a unei contestații și nu reprezintă răspunsuri directe la documente de intrare. Exemple: corespondență interinstituțională, informări, opinii oficiale, invitații.

- **Nr. de ieșire** – generat automat de sistem, incremental, pe anul curent (resetat anual conform normativului ANSC);
- **Data ieșirii** – preluată automat prin selector de dată (cu posibilitate de corecție controlată);

- **Adresant** – selectabil din nomenclatorul oficial de entități externe (autocomplete), cu posibilitate de adăugare/stergere multipli adresanți;
- **Tip document** – selectat din nomenclatorul instituțional (ex: răspuns oficial, scrisoare, informare);
- **Conținut** – completat manual de utilizator;
- **Executor** – utilizatorul responsabil cu elaborarea documentului;
- **Fișier atașat** – încărcare document final semnat sau pregătit pentru semnare;
- **Canal de transmitere** – e-mail, MDelivery, poștă fizică etc.

Documentul este salvat împreună cu metadatele sale în Registrul Documentelor de Ieșire, fiind identificat printr-un cod unic de arhivare și referențiat cronologic, AN/LUNA.

Flux digital al documentului de ieșire general (neasociat contestațiilor și independent de documentele de intrare).



2. Document de ieșire asociat unei contestații

Acest document este emis în cadrul unei proceduri de soluționare a contestațiilor, fiind parte integrantă a dosarului digital al unei contestații (ex: solicitări de informații, solicitări de prezentare a documentelor procesuale, invitații la ședințe).

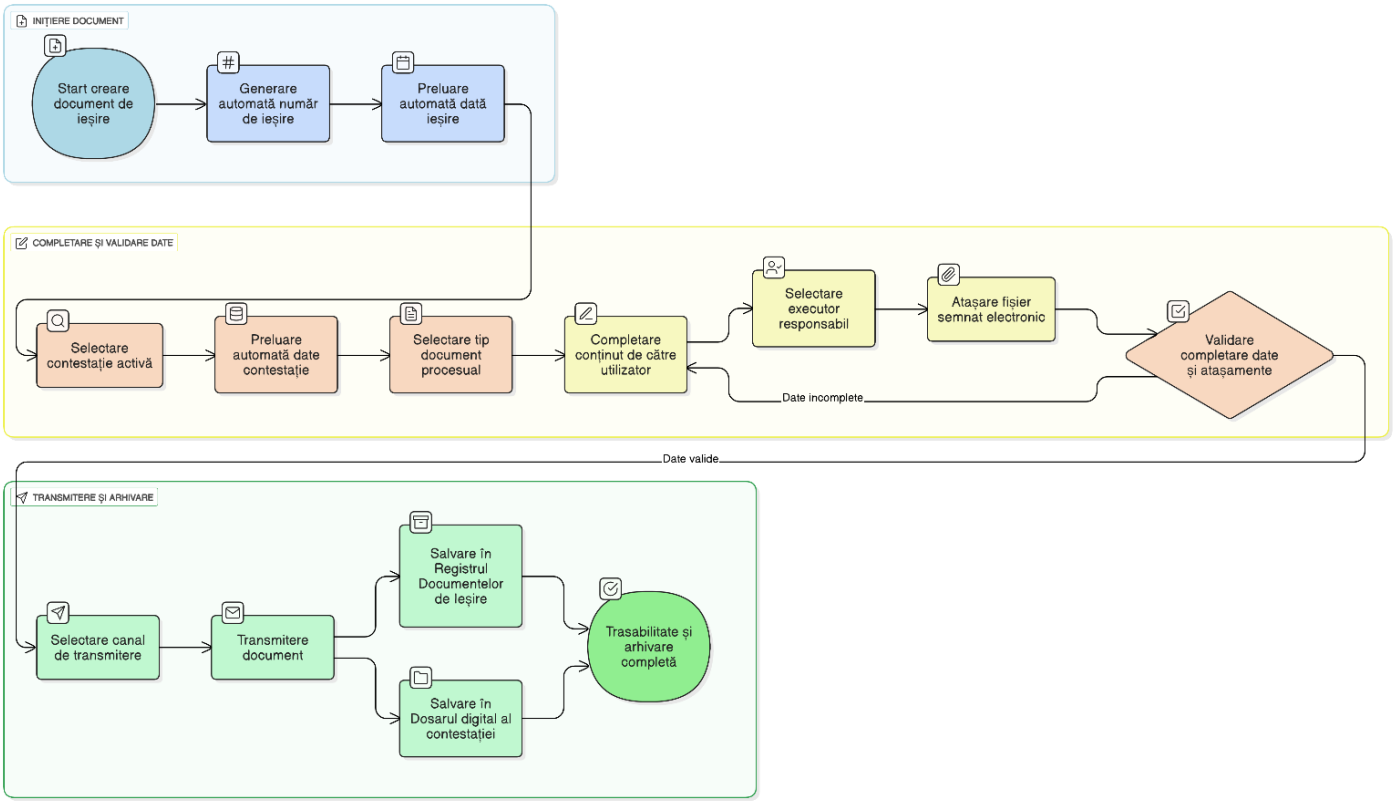
- **Nr. de ieșire** – generat automat;
- **Data ieșirii** – preluată automat;
- **Număr contestație -** selectat din nomenclatorul contestațiilor active, care va prelua deja automat următoarele câmpuri
    - **Adresant care este și Contestatar**
    - **Numărul procedurii de achiziție**
    - **CPV**
    - **LOT**
- **Tip document** – selectat din nomenclatorul documentelor procesuale;
- **Conținut** – completat de utilizator;
- **Executor** – responsabil desemnat;
- **Fișier atașat** – obligatoriu (semnat electronic, dacă este cazul);
- **Canal de transmitere** – selectat (MDelivery, e-mail etc.);

Documentul va fi salvat simultan în:

- Registrul Documentelor de Ieșire;
- Dosarul digital al contestației;

Astfel, se asigură trasabilitatea completă și arhivarea procedurală în cadrul SIMED, cu menținerea istoricului de emitere și semnături digitale asociate.

Flux digital al documentului de ieșire asociat unei contestații.



3. Document de ieșire emis ca răspuns la un document de intrare

Se aplică situațiilor în care ANSC formulează un răspuns oficial sau o reacție instituțională la o solicitare/document oficial primit anterior (care poate sau nu să aibă legătură cu o contestație).

- **Nr. de ieșire** – generat automat;
- **Data ieșirii** – preluată automat;
- **Adresant** – selectat din nomenclatorul de entități publice/private (autocomplete), sau introdus manual dacă este un expeditor neînregistrat anterior;
- **Document de intrare asociat** – selectat prin funcționalitate de asociere contextuală (autocomplete și listă recentă);
- **Tip document** – selectat din nomenclator;
- **Conținut** – opțional preluat parțial din documentul primit, cu posibilitate de editare;
- **Executor** – implicit același cu cel responsabil de documentul de intrare (editabil);
- **Fișier atașat** – obligatoriu, semnat electronic unde este cazul;
- **Canal de ieșire** – selectat conform specificului (e-mail, poștă, MDelivery etc.)

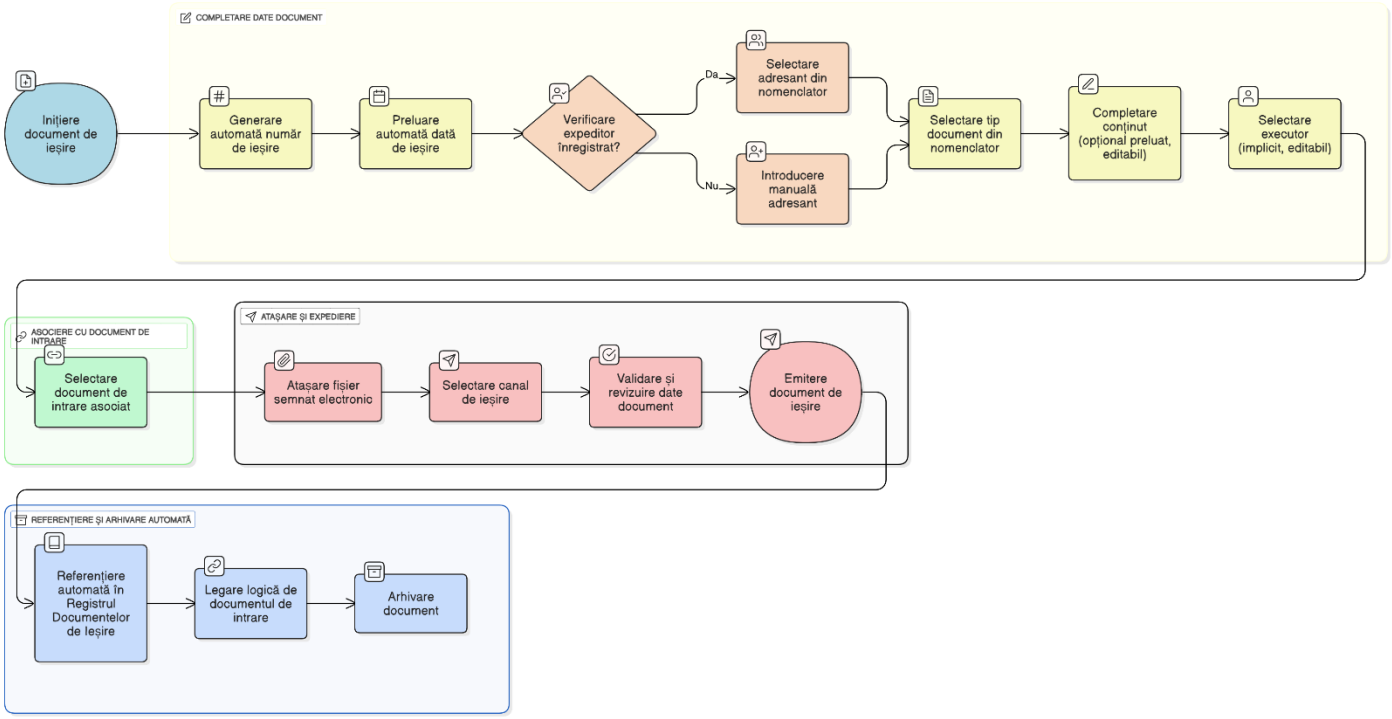
Documentul este automat referențiat în Registrul Documentelor de Ieșire și legat logic de documentul de intrare printr-un ID comun. Trasabilitatea bi-direcțională este esențială pentru audit, arhivare și verificare instituțională.

Toate documentele de ieșire vor fi afișate într-o interfață tabelară dinamică, cu funcționalități avansate de sortare, căutare și filtrare aplicabile individual pe fiecare coloană. Sistemul va include obligatoriu un mecanism de paginare și afișare configurabilă a numărului de înregistrări per pagină.

Utilizatorii autorizați vor avea posibilitatea de a:

- edita înregistrările documentelor de ieșire (cu păstrarea istoricului modificărilor);
- șterge documente în cazuri justificate, în conformitate cu politicile de audit și control intern.

Flux digital al documentului de ieșire emis ca răspuns la un document de intrare



4.2.3. Registrul Contestațiilor

Modulul „Registrul Contestațiilor” reprezintă componenta centrală a infrastructurii digitale SIMED, responsabilă de administrarea completă, standardizată și auditabilă a contestațiilor formulate în domeniul achizițiilor publice. Conceput pe arhitectură modulară, extensibilă și interoperabilă, acest registru electronic consolidează toate fluxurile operaționale aferente ciclului de viață al unei contestații – de la depunere până la arhivarea deciziei finale – în cadrul unui ecosistem procedural integrat, corelat cu toate modulele funcționale ale sistemului (Documente de Intrare, Ieșire, Decizii, Ședințe, Dashboard).
Registrul servește atât ca bază de date instituțională, cât și ca interfață activă pentru funcționarii autorizați ANSC, oferind o experiență de utilizare asistată, inteligentă și contextualizată. Astfel, fiecare contestație este automat corelată cu un **dosar digital unic**, în cadrul căruia sunt agregate cronologic toate documentele aferente procesului decizional: acte procedurale, corespondență oficială, notificări, puncte de vedere și alte documente suport.
Arhitectura interfeței și experiența utilizatorului
Interfața grafică este implementată sub forma unui **tabel inteligent, expandabil**, optimizat pentru acces rapid, sortare avansată și vizualizare incrementală. Structura este bazată pe rânduri extensibile (*expandable rows*) care expun doar atributele principale ale fiecărei contestații în modul implicit, permițând detalierea suplimentară la acțiune utilizator (hover, click, expand). Acest mecanism reduce aglomerarea vizuală și susține focalizarea pe acțiunile critice.
Funcționalitățile UI includ:

- **căutare avansată full-text și logică combinată (AND/OR) pe multiple coloane**;
- **filtrare și sortare granulară** pe fiecare câmp tabelar;

- **paginare asincronă configurabilă** și afișare customizabilă a numărului de rânduri;
- **filtru temporal asistat** (date picker, selecție rapidă pe intervale prestabilite);
- **acțiuni directe contextuale**: vizualizare dosar, adăugare documente, export, modificări administrative.

Câmpuri cheie afișate în registru (versiune extensibilă)

1. Data transmiterii în sistem;
2. Data înregistrării la ANSC;
3. Număr unic de înregistrare;
4. Contestatar;
5. Autoritatea contractantă;
6. Câștigător;
7. Număr procedură achiziție;
8. Cod CPV;
9. LOT;
10. Obiectul contestației;
11. Tipul procedurii de achiziție;
12. Completul desemnat (CSC);
13. Data repartizării către CSC;
14. Tipul deciziei adoptate;
15. Canal de depunere;
16. Mentiuni administrative (comentarii interne);
17. Stare dosar (complet / incomplet);
18. Acțiuni (Vizualizare dosar, export, atașare document etc, Solicită documente, Aplica Msign, Emite Decizie, Mențiuni, Solicită ședință);

Statuturi procedurale (valori dinamice configurabile)

Sistemul gestionează o gamă complexă de statuturi ale contestațiilor, menite să reflecte fidel evoluția procedurală și juridică a fiecărui caz. Acestea includ, fără a se limita la:

- Retrasă
- Număr anulat
- În examinare
- Decizie adoptată
- Contestație retrasă
- Examinare preliminară
- În așteptarea dosarului
- Restituită spre corectare
- Nu ține de competența ANSC
- În examinare, procedură suspendată
- În așteptarea explicațiilor de la AC
- Contestație retrasă – motiv neprecizat
- Contestație retrasă – motivul situației excepționale din țară
- Contestație retrasă – pentru a nu pereclita activitatea AC
- Contestație retrasă – argumentele AC acceptate de contestatar
- Contestație retrasă – procedură anulată, contestație rămasă fără obiect
- Contestație retrasă – măsuri de remediere efectuate de AC, contestație rămasă fără obiect

Această granularitate permite analiza comparativă, monitorizarea eficientă și fundamentarea deciziilor instituționale în baza statisticilor generate în timp real.

Funcționalități avansate de guvernanță procedurală

Modulul include un set extins de instrumente digitale pentru asigurarea eficienței operaționale și integrității procesuale:

- **Crearea automată a dosarului digital** imediat la înregistrarea contestației;
- **Clasificarea documentelor asociate** în: intrări, ieșiri, corespondență auxiliară, note CSC;
- **Monitorizare termene procedurale** (alerte privind documente întârziate, dosare incomplete, lipsa programării ședinței etc.);
- **Asociere automată de documente** provenite din alte module pe baza metadatelor (CPV, nr. contestație, AC);
- **Asociere manuală asistată** de operatori autorizați, în cazurile ambigue;
- **Mecanism de adăugare a mențiunilor** – note interne, observații, recomandări, marcaje CSC;
- **Export fișă contestație / dosar digital** în format standard (PDF/A, XML, ZIP);
- **Jurnal de activitate** și loguri de modificări per contestație, cu identificare de utilizator și timestamp;
- **Rapoarte automatizate** – pentru conducerea instituției, evaluare CSC, raportări externe.

Ciclul de viață și arhivarea automată

Toate înregistrările și documentele procesuale aferente contestațiilor sunt păstrate într-o structură standardizată și versionabilă, iar la finalul fiecărui exercițiu anual:

- Sistemul declanșează procesul de **arhivare automată** a contestațiilor închise, într-un format compatibil cu Arhiva Electronică a Statului;
- Administratorul ANSC poate iniția **arhivarea manuală** pentru contestații selectate sau întregul registru, aplicând semnătura digitală instituțională.

Contestațiile depuse prin intermediul **Cabinetului Personal Digital** din componenta Front Office a SIMED sunt recepționate și înregistrare automat în modulul „Registrul Contestațiilor” din cadrul Back Office. Acestea sunt înregistrate inițial cu statutul **„Contestație nouă”**, urmând a fi verificate formal de către funcționarul responsabil din cadrul DTISD. După validarea completitudinii și conformității, contestația este înregistrată oficial în sistem oferindui nr. de înregistrare, iar statutul său procedural este actualizat în **„În examinare”**.

Pentru contestațiile transmise prin metode tradiționale (e-mail oficial, poștă fizică, depunere la anticameră), înregistrarea se realizează manual de către funcționarul desemnat, direct în Registrul Contestațiilor din Back Office. Și în acest caz, după completarea tuturor metadatelor necesare și validarea formală, contestația va fi integrată în fluxul procedural cu statutul **„În examinare”**, iar sistemul va genera automat dosarul digital asociat.

Fiecare înregistrare arhivată este sigilată digital și indexată pentru acces rapid și audit, contribuind la conformitatea cu normele privind păstrarea și evidența documentelor publice. Registrul Contestațiilor din componenta Back Office a SIMED va constitui sursa principală de alimentare a modulului „Contestații” din cadrul Front Office-ului platformei. Astfel, informațiile esențiale privind contestațiile aflate în examinare – inclusiv statutul procedural, data înregistrării, completul desemnat, programarea ședinței și decizia adoptată – vor fi afișate public, într-un format structurat și actualizat în timp real, asigurând transparență și acces facil pentru părțile implicate.

4.2.4. Registrul Deciziilor

Modulul „Registrul Deciziilor” este parte componentă a Back Office-ului SIMED, responsabil de gestionarea structurată și completă a tuturor deciziilor emise de Agenția Națională pentru Soluționarea

Contestațiilor (ANSC) în procesul de soluționare a contestațiilor în domeniul achizițiilor publice. Acest registru digital centralizat oferă suport operațional personalului autorizat al ANSC în vederea consultării, administrării, arhivării și monitorizării actelor decizionale, într-un cadru informatic unitar, sigur și interoperabil.
Modulul este destinat în principal membrilor completelor de soluționare a contestațiilor (CSC), structurilor de suport administrativ și funcționarilor ANSC implicați în validarea, raportarea și publicarea deciziilor finale. Toate deciziile generate în cadrul proceselor de examinare sunt înregistrate în acest modul, împreună cu metadatele esențiale care permit identificarea, căutarea și asocierea rapidă a acestora cu dosarele digitale corespunzătoare.
Totodată, modulul „Registrul Deciziilor" din Back Office SIMED alimentează în mod automat componenta publică a modulului Decizii din Front Office SIMED, printr-un mecanism de integrare bidirecțională. Această conexiune se realizează printr-un API REST securizat, care transmite în format JSON standardizat toate deciziile adoptate și semnate digital. Transferul are loc asincron, fie prin mecanisme de polling incremental, fie prin Webhooks care notifică imediat sistemul Front Office în momentul înregistrării unei noi decizii.
În plus, inițierea proiectului de decizie este declanșată direct din Modulul Registrul Contestațiilor, sistemul generează automat un proiect de decizie CSC pe baza unui șablon configurabil. Acest șablon este completat automat cu datele relevante ale contestației și compilează toate documentele procesuale asociate din dosarul digital. Draftul generat poate fi ulterior consultat și modificat de către membrii CSC, Direcția Juridică și DTISD, urmând a fi supus semnării electronice prin MSign. După semnare, decizia este înscrisă automat în Registrul Deciziilor și clasată în dosarul digital al contestației.

Arhitectura interfeței și experiența utilizatorului

Interfața grafică este concepută sub forma unui tabel interactiv inteligent, cu rânduri extensibile (expandable rows), oferind o experiență de navigare intuitivă și eficientă. Vizualizarea implicită afișează doar atributele-cheie, în timp ce detaliile suplimentare devin disponibile la acțiunea utilizatorului (click, hover sau expand), reducând aglomerarea vizuală și susținând concentrarea asupra datelor relevante.

Funcționalități UI avansate:

- **Căutare semantică completă**, cu suport pentru expresii complexe și logică booleană;
- **Sortare și filtrare pe câmpuri multiple**, cu instrumente de rafinare a rezultatelor;
- **Paginare asincronă și afișare configurabilă a rândurilor**, adaptabilă volumului de date;
- **Selector temporal asistat**, cu opțiuni rapide de intervale prestabilite;
- **Acțiuni directe din tabel**, inclusiv: descărcare decizie, acces la dosar, adăugare mențiuni, export selecție etc.

Câmpuri cheie afișate în Registrul Deciziilor (versiune extensibilă):

1. **Nr. decizie** – identificator unic, cu link către PDF-ul semnat digital;
2. **Data adoptării** – data oficială a emiterii deciziei;
3. **Contestatar** – denumirea completă a persoanei fizice sau juridice;
4. **Autoritatea contractantă** – entitatea publică vizată;
5. **Obiectul contestației** – titlul procedurii preluat din MTender;
6. **Elementele contestației** – descrierea succintă a motivelor invocate;
7. **Complet decizional** – codul CSC și denumirea, cu link către profilul completului;
8. **Nr. procedurii** – cod unic MTender, cu redirecționare către pagina aferentă;
9. **Conținutul deciziei** – rezumat al raționamentului decizional;
10. **Tip procedură** – clasificarea achiziției (licitație, negociere etc.);
11. **Obiectul achiziției** – denumire + CPV;
12. **Statut decizie** – rezultat: admisă, respinsă, parțial admisă, anulată;
13. **Document decizie** – link către fișier PDF/A semnat prin MSign;

14. **Raportare decizie** – indicator dacă decizia a fost transmisă către alte sisteme;
15. **Nr. înregistrare contestație ANSC** – codul oficial al contestației de referință.

Funcționalități avansate și interoperabilitate

- **Export individual sau în lot** al deciziilor pe baza criteriilor configurabile;
- **Clasificare automată** în funcție de metadatele contestației și ale procedurii;
- **Integrare directă cu dosarul digital al contestației**, pentru acces contextualizat;
- **Alerte și notificări automate** pentru decizii nepublicate, incomplete sau cu termen depășit;
- **Verificare automată a conformității** fișierelor deciziei (semnătură digitală, timestamp, integritate hash);
- **Audit trail detaliat** cu log de activitate complet pentru fiecare decizie (istoric modificări, acces, generare);
- **Preluare automată și afișare în modulul Decizii din Front Office**, în baza fluxului sincronizat de date între Back Office și Front Office SIMED.

La încheierea fiecărui an calendaristic, toate deciziile înregistrate în sistem pot fi arhivate automat sau la solicitarea explicită a Administratorului SIMED, în conformitate cu politicile instituționale ANSC privind ciclul de viață al documentelor digitale.
Această arhivare (An->Lună) facilitează conservarea integrității documentare, susține auditabilitatea pe termen lung și contribuie la reducerea sarcinii operaționale privind gestiunea istorică a datelor decizionale.

4.2.5. Agenda Ședințelor

Modulul „Agenda Ședințelor” este o componentă digitală specializată a Back Office-ului SIMED, concepută pentru a automatiza și structura întregul proces de planificare, validare, notificare și publicare a ședințelor Completelor de Soluționare a Contestațiilor (CSC) din cadrul Autorității Naționale pentru Soluționarea Contestațiilor (ANSC). Acest modul răspunde nevoii instituționale de a gestiona în mod coerent și trasabil activitatea deliberativă aferentă soluționării contestațiilor, eliminând dependența de instrumente fragmentare (e-mail, calendare disparate, documente Word) și înlocuindu-le cu un mecanism digital integrat și guvernat de reguli procedurale clare.
Destinația principală a modulului este utilizarea de către actorii interni ANSC implicați în procesul de examinare a contestațiilor – în special Președinții CSC, consilierii raportori, secretariatul tehnic și personalul administrativ. Aceștia vor folosi modulul pentru a iniția, configura și valida ședințele, pentru a notifica părțile implicate și pentru a asigura publicarea automată a agendelor. Totodată, modulul facilitează încărcarea documentelor rezultate în urma ședinței – precum procesele-verbale și înregistrările audio/video – și integrarea lor automată în dosarele digitale ale contestațiilor corespunzătoare.
Datele generate în cadrul acestui modul sunt stocate în baza de date centrală a SIMED, în format structurat, cu metadate standardizate și corelare directă cu registrul contestațiilor. Fiecare ședință este tratată ca o entitate procedurală distinctă, asociată în mod bidirecțional cu dosarul digital aferent contestației.
Pentru a funcționa în regim complet digital și interoperabil, Modulul „Agenda Ședințelor” este integrat direct cu următoarele componente ale sistemului SIMED și ale infrastructurii digitale guvernamentale:

- **Back Office->Modulul „ Registrul Contestațiilor”**, din care preia contestațiile aflate în stadiul „În examinare” și în care înregistrează ședințele asociate fiecărui dosar;
- **Front Office->Cabinetul Personal Digital**, prin care sunt trimise automat alertele și convocările către părțile implicate;

- **Front Office->Modulul „Ședințe”**, în care este publicată agenda ședinței, cu filtrare avansată și posibilitate de descărcare;
- **Serviciile MPass și MSign**, utilizate pentru autentificarea funcționarilor și semnarea electronică a proceselor-verbale;**1. Inițierea și configurarea ședinței**

Procesul debutează în Back Office-ul SIMED, unde un utilizator autorizat – Președintele Completului CSC sau Consilierul Raportor – accesează modulul „Agenda Ședințelor” pentru a crea o ședință nouă asociată unei contestații aflate în proces de examinare.

- **Inițiere ședință nouă**. Utilizatorul selectează opțiunea de inițiere a unei ședințe, pornind de la o contestație eligibilă, identificabilă în sistem ca fiind „în examinare”.
- **Selectare contestație activă**. Sistemul oferă o listă filtrată automat cu contestațiile în curs, din care se alege cea vizată de audiere.
- **Preluare automată a metadatelor**. La selecție, fișa ședinței este completată automat cu datele esențiale: numărul contestației, denumirea contestatarului și a autorității contractante, obiectul achiziției (cu codul CPV), membrii completului de soluționare, precum și data și ora planificată (standard UTC+2), cu validare calendaristică integrată.

2. Validare și Aprobare Instituțională

Odată completată, fișa este transmisă pentru validare formală. Acest pas este esențial pentru declanșarea automată a următoarelor procese digitale.

- **Confirmare de către Președintele CSC**. Președintele completului analizează datele introduse și confirmă electronic organizarea ședinței, utilizând autentificarea sigură MPass.
- **Înregistrare oficială în Registrul Ședințelor**. Confirmarea generează automat înscrierea ședinței în registrul oficial din SIMED, marcând începutul ciclului procedural formal.

3. Transmiterea notificărilor automatizate

Pentru a asigura o comunicare eficientă și uniformă, sistemul declanșează notificarea sincronizată a tuturor părților implicate.

- **Notificare pe e-mail instituțional**. Fiecare parte primește un e-mail personalizat, generat automat pe baza șablonului aprobat, conținând toate detaliile relevante privind ședința.
- **Alertă directă în Cabinetul Personal Digital**. Simultan, se emite o alertă în interfața Cabinetului Digital al fiecărei părți, cu posibilitate de confirmare a participării. Această metodă asigură redundanță și siguranța livrării mesajului.

4. Publicarea agendei în portalul public (Front Office)

În spiritul transparenței instituționale, agenda ședinței este publicată automat în modulul public „Ședințe” al Front Office-ului SIMED.

- **Afișare publică în Modulul Ședințe**. Agenda devine vizibilă într-o interfață cronologică intuitivă, accesibilă oricărui utilizator extern.
- **Filtrare avansată & ewxport în PDF**. Vizitatorii pot filtra ședințele după dată, autoritate contractantă, contestație sau complet și pot descărca agenda publică în format PDF, pentru uz personal sau instituțional.

5. Arhivarea în Dosarul Digital al Contestației

Fiecare ședință aprobată este înregistrată automat în dosarul digital al contestației corespunzătoare, consolidând coerența procedurală și integritatea documentară.

- **Asociere automată în Dosarul Contestației**. Corelarea se face automat, fără intervenție manuală, iar ședința devine parte a liniei temporale a procedurii.
- **Trasabilitate și audit procedural complet**. Sistemul păstrează un istoric detaliat al fiecărei acțiuni, cu marcaj temporal și identificator de utilizator, asigurând integritatea și verificabilitatea procesului.

6. Gestionarea documentelor și materialelor media

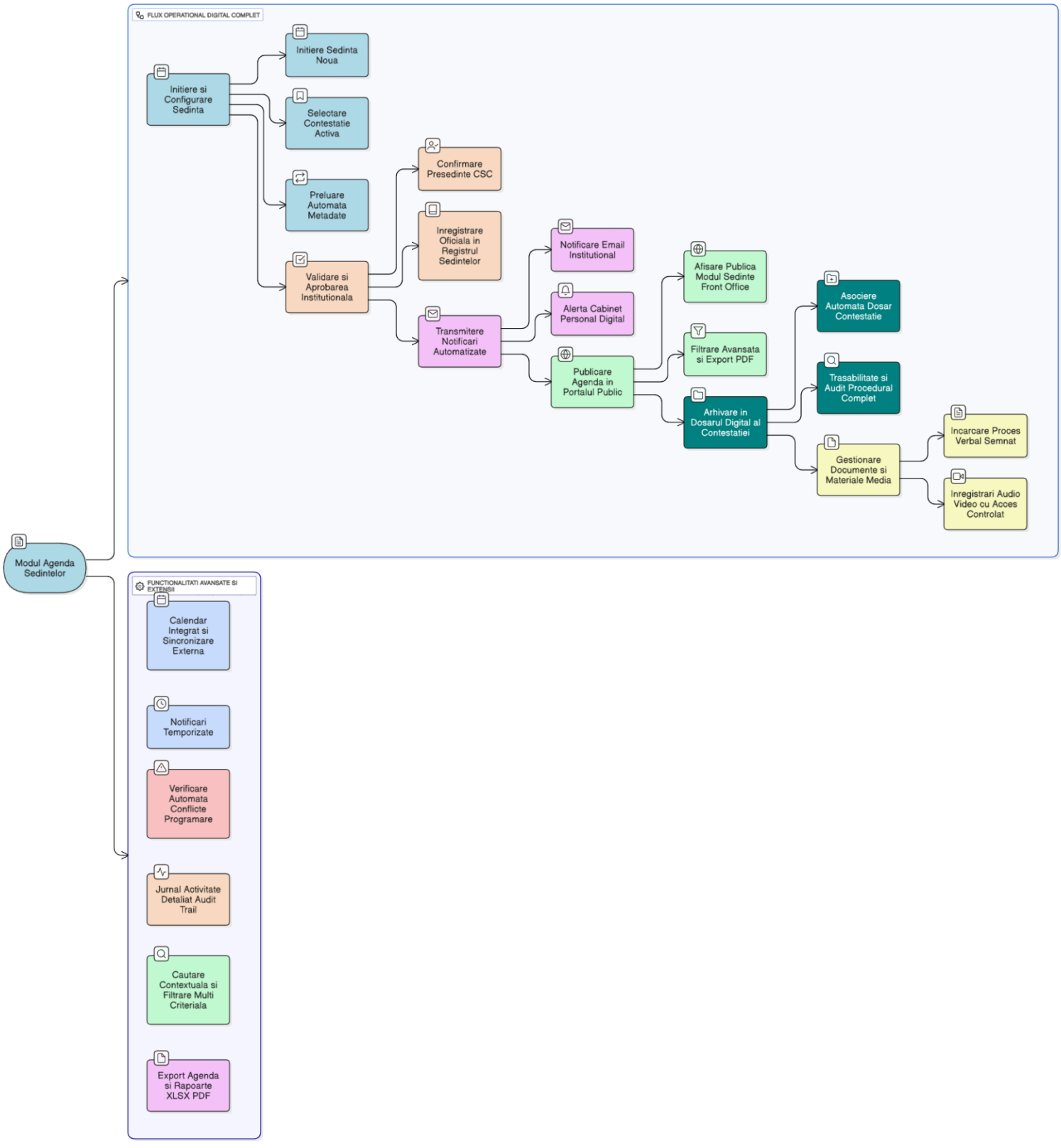
După desfășurarea ședinței, documentele generate pot fi atașate direct în fișa acesteia și în dosarul digital aferent.

- **Încărcare proces-verbal Semnat (PDF + MSign)**. Procesul-verbal al ședinței este redactat în format standardizat și semnat digital prin MSign, apoi arhivat electronic.
- **Înregistrări audio/video cu acces controlat (MP4)**. Înregistrările sunt încărcate în sistem într-un format securizat și pot fi accesate fie prin streaming intern (HTML5 player), fie prin descărcare controlată, în funcție de nivelul de autorizare al utilizatorului.

Funcționalități avansate și extensii

Modulul este completat de un set de funcționalități inteligente care sporesc performanța operațională și ușurința în utilizare:

- **Calendar integrat și sincronizare externă**. Ședințele pot fi exportate în aplicații externe de tip calendar (Outlook, Google Calendar), prin flux iCal/ICS automat.
- **Notificări temporizate (T-24h / T-1h)**. Participanții primesc remindere automate, fără intervenție umană, la intervale predefinite față de ora programată.
- **Verificare automată a conflictelor de programare**. Sistemul detectează automat suprapunerile de timp sau resurse (ex. complet deja programat) și avertizează utilizatorul.
- **Jurnal de activitate detaliat (Audit Trail)**. Fiecare modificare – de la planificare, la reprogramare sau anulare – este înregistrată cu marcaj temporal și identitate digitală, garantând control și responsabilitate.
- **Căutare contextuală și filtrare multi-criterială**. Interfața oferă funcții de căutare după cuvinte-cheie, statusuri, date, complet, părți implicate sau coduri CPV.
- **Export agendă și rapoarte în XLSX/PDF**. Utilizatorii pot genera rapid rapoarte de activitate, statistici sau agende sintetizate pentru diferite perioade sau categorii de ședințe.


FLUX OPERATIONAL DIGITAL COMPLET
Initiere si Configurare Sedinta
Initiere Sedinta Noua
Selectare Contestatie Activa
Preluare Automata Metadate
Validare si Aprobarea Institutionala
Confirmare Presedinte CSC
Inregistrare Oficiala in Registrul Sedintelor
Transmitere Notificari Automatizate
Notificare Email Institutional
Alerta Cabinet Personal Digital
Publicare Agenda in Portalul Public
Afisare Publica Modul Sedinte Front Office
Filtrare Avansata si Export PDF
Arhivare in Dosarul Digital al Contestatiei
Asociere Automata Dosar Contestatie
Trasabilitate si Audit Procedural Complet
Gestionare Documente si Materiale Media
Incarcare Proces Verbal Semnat
Inregistrari Audio Video cu Acces Controlat
Modul Agenda Sedintelor
FUNCTIONALITATI AVANSATE SI EXTENSII
Calendar Integrat si Sincronizare Externa
Notificari Temporizate
Verificare Automata Conflicte Programare
Jurnal Activitate Detaliat Audit Trail
Cautare Contextuala si Filtrare Multi Criteriala
Export Agenda si Rapoarte XLSX PDF

4.2.6. Modulul documente procesuale

Modulul „Documente procesuale” va asigura gestionarea integrată a tuturor documentelor și formularelor utilizate în cadrul procesului de examinare și soluționare a contestațiilor de către ANSC.
Toate formularele prevăzute la pct. 7 al Procedurii operaționale vor fi digitalizate, configurate și integrate în SIMED. Acestea vor fi utilizate pentru generarea documentelor procesuale aferente dosarului electronic al contestației și vor constitui parte integrantă a fluxurilor de examinare, redactare, avizare, semnare, înregistrare, comunicare și arhivare a documentelor.
Pentru fiecare tip de document procesual, sistemul va asigura existența unui șablon electronic configurabil, administrat din componenta Back Office, fără a necesita modificarea codului sursă. Șabloanele vor putea fi create, configurate, actualizate, activate, dezactivate și versionate exclusiv de către utilizatorii autorizați.
Fiecare șablon va conține cel puțin:

- codul și denumirea șablonului;
- tipul documentului procesual;
- descrierea și scopul utilizării;
- structura documentului;
- câmpurile obligatorii și opționale;
- regulile de completare și validare;
- rolurile autorizate să utilizeze șablonul;
- fluxul de redactare, avizare și semnare;
- versiunea șablonului;
- data aprobării;
- data intrării în vigoare;
- data încetării valabilității, după caz;
- statutul „Draft”, „Activ”, „Inactiv” sau „Arhivat”;
- limba sau limbile în care poate fi generat documentul.

Sistemul va permite completarea automată a câmpurilor documentelor procesuale cu datele disponibile în dosarul electronic al contestației, inclusiv, după caz:

- numărul și data înregistrării contestației;
- numărul dosarului;
- datele contestatarului;
- datele autorității contractante;
- datele operatorului economic desemnat câștigător;
- datele reprezentanților și împuternicirile acestora;
- obiectul contestației;
- datele procedurii de achiziție;
- numărul procedurii din SIA RSAP/MTender;
- componența completului de soluționare a contestației;
- numele raportorului;
- data și ora ședinței;
- termenele procedurale;
- documentele și actele asociate dosarului;

- statutul curent al contestației;
- rezultatul examinării;
- alte informații relevante disponibile în SIMED.

Datele completate automat vor putea fi modificate numai în limitele drepturilor acordate utilizatorului și ale regulilor procedurale aplicabile. Sistemul va diferenția câmpurile completate automat care nu pot fi modificate de câmpurile care permit completarea sau ajustarea manuală.

Modificarea manuală a datelor preluate automat din dosarul electronic nu va modifica informația-sursă din registrele sau modulele SIMED, cu excepția cazurilor în care utilizatorul deține drepturi explicite pentru actualizarea respectivei informații. Orice asemenea modificare va fi jurnalizată.

La generarea unui document procesual, sistemul va asocia automat documentului:

- dosarul electronic corespunzător;
- tipul documentului;
- șablonul și versiunea utilizată;
- autorul documentului;
- data și ora generării;
- starea documentului;
- fluxul de aprobare aplicabil;
- utilizatorii responsabili de redactare, avizare și semnare;
- termenul de finalizare, dacă este aplicabil.

Documentele procesuale vor parcurge, în funcție de tipul documentului, următoarele stări:

1. Draft;
2. În redactare;
3. Spre verificare;
4. Returnat pentru modificare;
5. Spre avizare;
6. Avizat;
7. Respins la avizare;
8. Spre semnare;
9. Semnat;
10. Înregistrat;
11. Expediat;
12. Comunicat;
13. Anulat;
14. Arhivat.

Documentele care necesită semnare electronică vor fi transmise către MSign numai după finalizarea etapelor obligatorii de redactare, verificare și avizare. Sistemul va verifica rezultatul semnării și va păstra documentul semnat, semnăturile aplicate, certificatele și informațiile necesare verificării autenticității și integrității documentului.

După semnarea, înregistrarea sau emiterea unui document procesual, conținutul acestuia nu va mai putea fi modificat. Orice corectare ulterioară va fi realizată prin generarea unui document nou, prin emiterea unei

versiuni corectate sau prin aplicarea unei proceduri de anulare și reemitere, conform regulilor aprobate de ANSC.
Modificarea unui șablon nu va afecta documentele deja generate, semnate, emise sau arhivate. Fiecare document va păstra legătura cu versiunea exactă a șablonului utilizată la momentul generării sale.
La activarea unei versiuni noi a unui șablon:

- versiunea anterioară va fi păstrată în sistem;
- documentele deja inițiate vor continua să utilizeze versiunea cu care au fost create, dacă ANSC nu stabilește altfel;
- documentele noi vor utiliza versiunea activă în vigoare la data generării;
- data intrării în vigoare va fi obligatorie;
- activarea va fi jurnalizată;
- nu va fi permisă existența simultană a mai multor versiuni active pentru același tip de document și același context procedural, cu excepția cazurilor configurate expres.

Șabloanele și documentele vor permite utilizarea elementelor condiționale, astfel încât anumite secțiuni, formulări sau câmpuri să fie incluse automat în funcție de:

- tipul contestației;
- obiectul contestației;
- etapa procedurală;
- deciziile intermediare;
- existența unei excepții procedurale;
- necesitatea organizării unei ședințe publice;
- măsura dispusă;
- rezultatul examinării;
- alte condiții configurate de ANSC.

Sistemul va permite inserarea în documente a unor texte standard, clauze, temeiuri juridice și formulări predefinite, administrate prin nomenclatoare sau biblioteci de conținut. Modificarea acestor elemente va fi versionată și nu va afecta documentele deja emise.
Documentele procesuale vor fi generate în formate deschise și uzuale, inclusiv DOCX, pentru editare, și PDF/PDF-A, pentru semnare, comunicare, publicare și arhivare, în funcție de etapa fluxului și de tipul documentului.
Documentele generate vor respecta identitatea vizuală și regulile instituționale aprobate de ANSC, inclusiv antetul, subsolul, numerotarea paginilor, structura, fonturile, semnăturile, mențiunile privind caracterul documentului și alte elemente obligatorii.
Sistemul va permite previzualizarea documentului înainte de transmiterea spre avizare sau semnare și va valida existența tuturor câmpurilor obligatorii. Nu va fi permisă promovarea documentului la etapa următoare dacă lipsesc date obligatorii sau dacă documentul conține neconformități de validare.
Fiecare document procesual va fi asociat automat dosarului electronic al contestației și va fi disponibil în istoricul cronologic al acestuia. Sistemul va permite căutarea, filtrarea și consultarea documentelor după tip, număr, dată, autor, statut, destinatar, dosar și alte criterii relevante.
Accesul la documentele procesuale va fi acordat în funcție de rolul utilizatorului, etapa procedurală, caracterul public sau nepublic al documentului și drepturile asupra dosarului. Documentele publice vor fi

transmise către componenta Front Office numai după aprobarea pentru publicare și, după caz, anonimizarea datelor cu caracter personal sau a altor informații protejate.

Tipuri de formulare

1. Ordin de constituire a CSC (7.1)
2. Proces-verbal privind punerea în discuție a necesității organizării ședinței publice (7.2)
3. Proces-verbal al ședinței deschise de soluţionare a contestaţiei (7.3)
4. Proces-verbal al ședinței completului de soluţionare a contestaţiei (7.4)
5. Scrisoare de completare a contestaţiei (7.5)
6. Scrisoare de expunere pe marginea excepției de tardivitate (7.6)
7. Scrisoare de expunere pe lipsa de competență (7.7)
8. Scrisoare de expunere pe lipsa de interes (7.8)
9. Scrisoare de solicitare a documentelor/explicaţiilor – rezultate procedură (7.9)
10. Scrisoare de solicitare a documentelor/explicaţiilor – documentația de atribuire (7.10)
11. Proces-verbal al deciziei de suspendare (7.11)
12. Scrisoare de însoțire a deciziei de suspendare (7.12)
13. Invitație la ședința publică de examinare a contestației (7.13)
14. Proces-verbal de retragere a contestației (7.14)
15. Scrisoare privind retragerea contestației (7.15)
16. Proces-verbal de prelungire a termenului de soluţionare a contestaţiei (7.16)
17. Scrisoare de însoțire a deciziei (7.17)
18. Decizia de soluţionare a contestaţiei (7.18)

4.2.7. Rapoarte

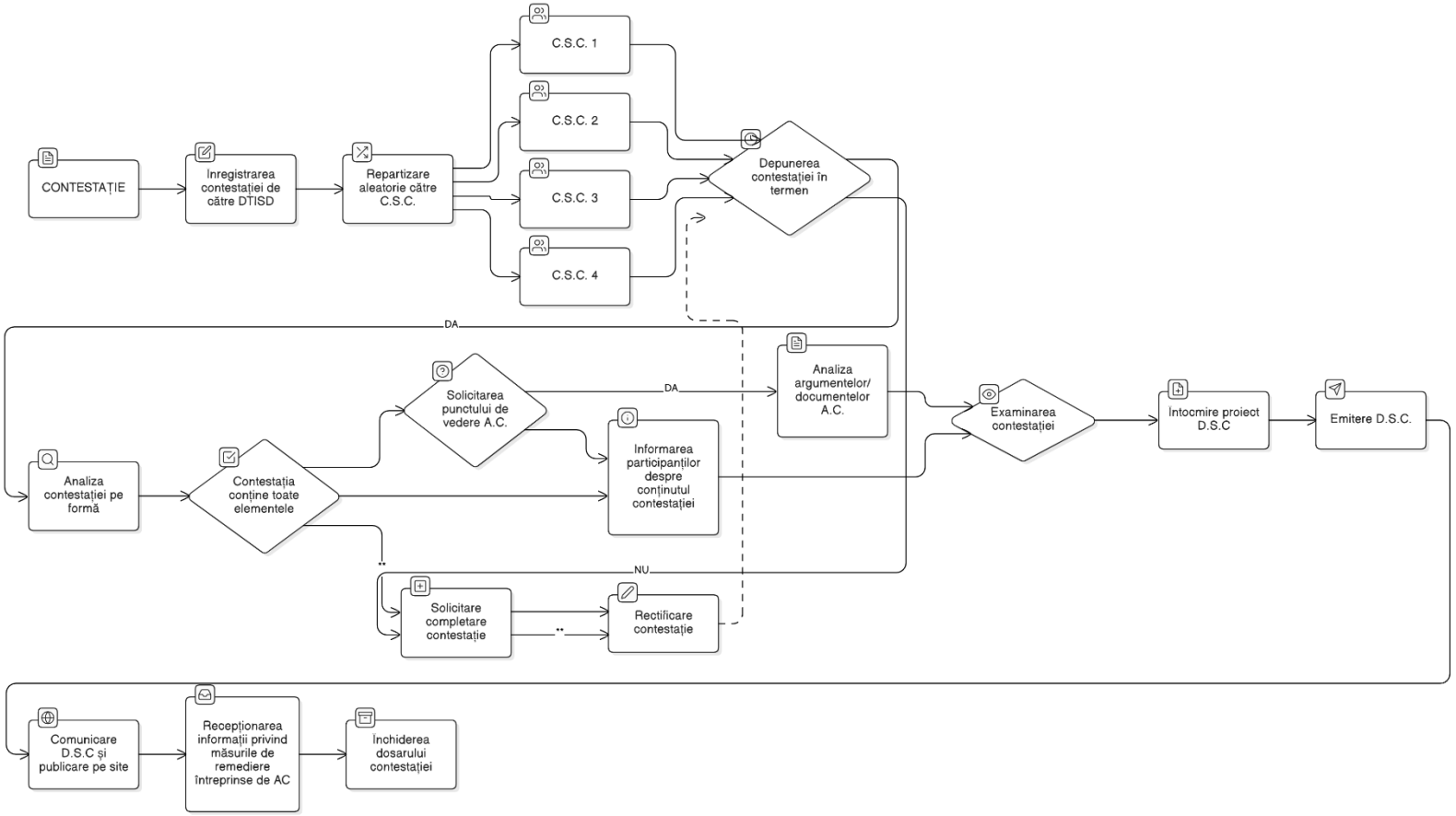
În cadrul Sistemului Informațional de Management Electronic al Documentelor (SIMED) vor fi dezvoltate și implementate o serie de rapoarte standardizate, destinate atât nivelului instituțional, cât și anumitor direcții și departamente din cadrul ANSC. Aceste rapoarte vor acoperi integral procesele de gestionare a contestațiilor și a deciziilor, indicatorii de performanță instituțională, precum și aspecte legate de transparență, cooperare interinstituțională și analiza jurisprudenței.
Forma, conținutul, structura câmpurilor și template-urile aferente fiecărui raport vor fi elaborate și validate în strictă coordonare cu ANSC, pentru a răspunde necesităților reale de raportare și monitorizare. Sistemul va permite ulterior ajustarea și personalizarea acestor rapoarte din interfața Back Office, fără intervenții în codul sursă, asigurând astfel flexibilitatea și adaptabilitatea la modificările instituționale și legislative.
Rapoartele enumerate mai jos vor constitui un instrument esențial de management, analiză și raportare, sprijinind ANSC în activitățile de planificare strategică, monitorizare a performanței, evaluare a eficienței proceselor și consolidare a transparenței instituționale.

Lista tipurilor de rapoarte care urmează a fi dezvoltate în SIMED

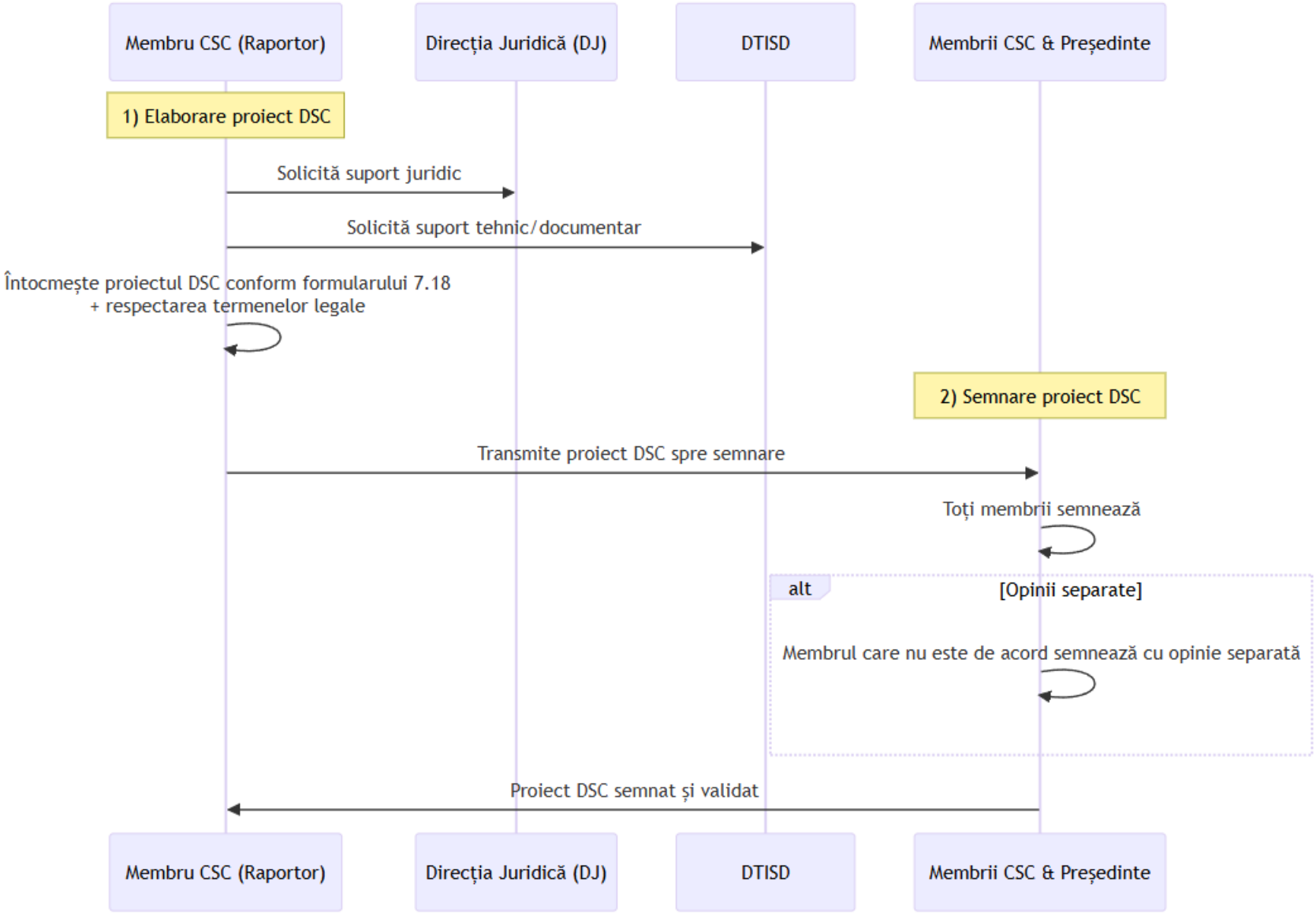
Nr.	Denumire raport	Direcția / Serviciul responsabil
1	Raport date generale contestații	Instituțional (toate direcțiile relevante)
2	Raport date generale decizii	Instituțional

Nr.	Denumire raport	Direcția / Serviciul responsabil
3	Raport date generale contestații și decizii	Instituțional
4	Raport de monitorizare a executării deciziilor ANSC	Direcția metodologie, planificare, raportare și monitorizare
5	Raport privind acțiunile în instanță împotriva deciziilor ANSC	Direcția juridică
6	Raport privind indicatorii de performanță instituțională ai ANSC	Direcția metodologie, planificare, raportare și monitorizare
7	Raport privind comunicarea și cooperarea cu organele de investigație	Direcția juridică
8	Raport privind activitatea consultantului juridic în examinarea contestațiilor	Direcția juridică
9	Raport de evaluare a eficienței procesului de gestionare a contestațiilor	Direcția metodologie, planificare, raportare și monitorizare
10	Raport privind jurisprudența comparată și tipologia contestațiilor	Direcția metodologie, planificare, raportare și monitorizare
11	Raport privind transparența și comunicarea publică a ANSC	Serviciul comunicare
12	Notă analitică privind executarea deciziei ANSC	Direcția metodologie, planificare, raportare și monitorizare

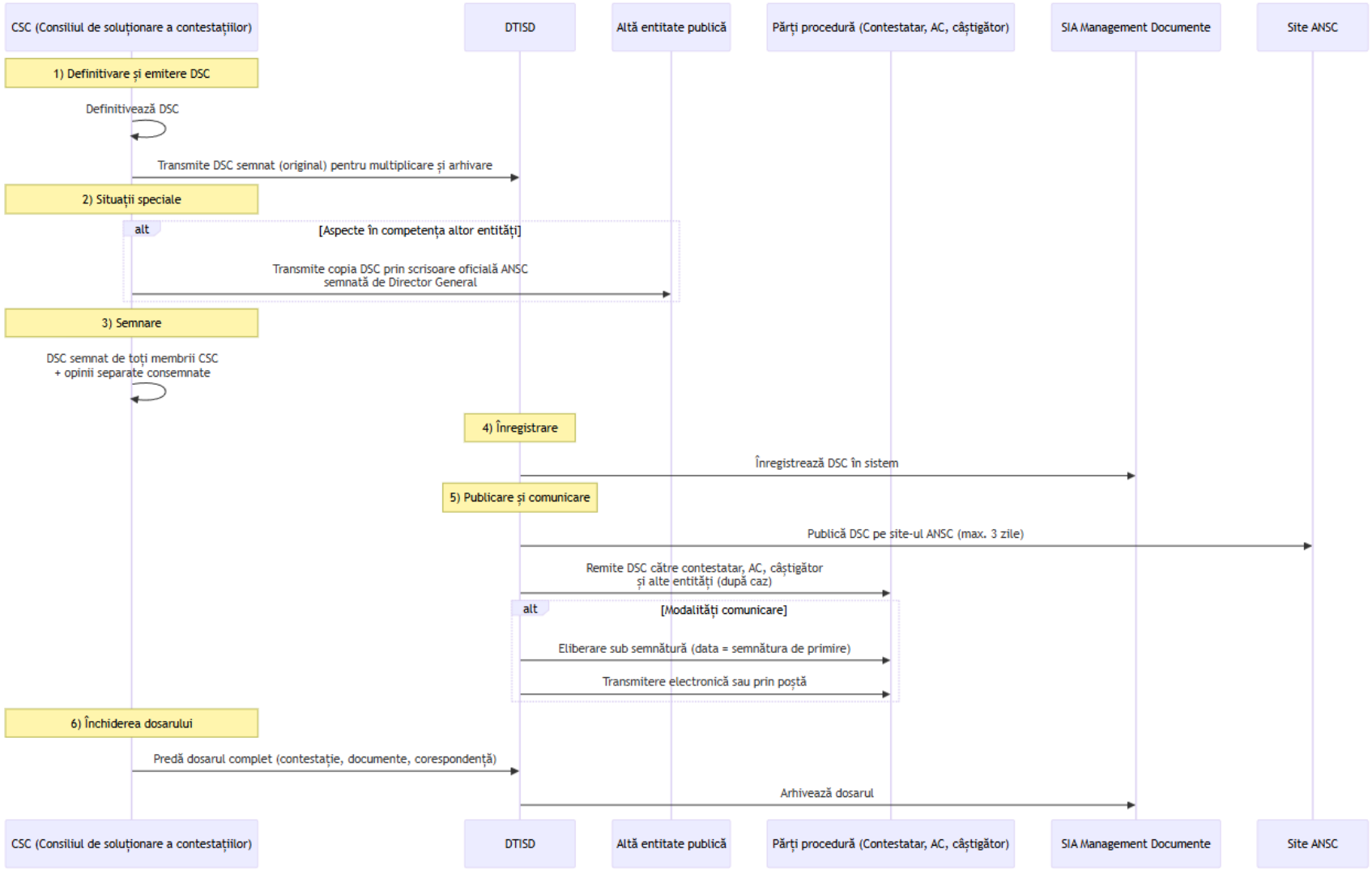
4.3. Cerințe funcționale pentru Procedura Operațională de soluționare a contestației


CONTESTAȚIE
Înregistrarea contestației de către DTISD
Repartizare aleatorie către C.S.C.
C.S.C. 1
C.S.C. 2
C.S.C. 3
C.S.C. 4
Depunerea contestației în termen
DA
Analiza contestației pe formă
Contestația conține toate elementele
Solicitarea punctului de vedere A.C.
DA
Informarea participanților despre conținutul contestației
Analiza argumentelor/ documentelor A.C.
Examinarea contestației
Întocmire proiect D.S.C
Emitere D.S.C.
NU
Solicitare completare contestație
Rectificare contestație
Comunicare D.S.C și publicare pe site
Recepționarea informații privind măsurile de remediere întreprinse de AC
Închiderea dosarului contestației

Întocmirea proiectului DSC



Emiterea, comunicarea DSC şi închiderea dosarului contestaţiei



4.4. Nomenclatoare de referință în cadrul SIMED

Nomenclatoarele reprezintă structuri de date standardizate și controlate, compuse din seturi de valori discrete, definite formal și gestionate centralizat, care servesc ca sursă unică de adevăr pentru etichetele, clasificările și opțiunile utilizate în interfața și logica aplicației SIMED. În cadrul Sistemului Informațional SIMED, nomenclatoarele sunt utilizate extensiv în următoarele scopuri:

- Precompletarea automată a câmpurilor din formulare electronice;
- Alimentarea componentelor UI dinamice, precum liste derulante, filtre, butoane de selecție sau câmpuri cu validare multiplă;
- Clasificarea documentelor și înregistrărilor în baza unor criterii uniforme, pentru asigurarea coerenței datelor în cadrul jurnalului de audit, modulelor de arhivare și generatoarelor de rapoarte;
- Filtrarea și sortarea datelor în modulele de căutare, statistici și dashboard-uri, în baza valorilor unificate ale câmpurilor procedurale;
- Validarea logică a fluxurilor de lucru (workflow), prin utilizarea statusurilor și codificărilor formale acceptate de sistem.

PRINTRE PRINCIPALELE NOMENCLATOARE ȘI CLASIFICATOARE UTILIZATE ÎN SIMED SE REGĂSESC:

STATUT CONTESTAȚIE

Retrasă
Număr anulat
În examinare
Decizie adoptată
Contestație retrasă
Examinare preliminară
În așteptarea dosarului
Restituită spre corectare
Nu ține de competența ANSC
În examinare, procedură suspendată
În așteptarea explicațiilor de la AC
Contestație retrasă – motiv neprecizat
Contestație retrasă – motivul situației excepționale din țară
Contestație retrasă – pentru a nu pereclita activitatea AC
Contestație retrasă – argumentele AC acceptate de contestatar
Contestație retrasă – procedură anulată, contestație rămasă fără obiect
Contestație retrasă – măsuri de remediere efectuate de AC, contestație rămasă fără obiect

STATUT DECIZIE

În vigoare
Anulată de instanța de judecată
Suspendată de instanța de judecată

CONȚINUT DECIZIE

Contestație admisă
Procedură anulată
Procedură parțial anulată
Măsuri de remediere
Contestație parțial admisă
Contestație respinsă
Contestație depusă tardiv
Contestație depusă neconformă / lipsită de obiect
Contestație neîntemeiată

CRITIVI/MOTIVE DE CONTESTARE

RP – Respingerea ofertei contestatorului / Acceptarea ofertei altor participanți
RP 1 Respingerea ofertei contestatorului ca neconformă sau inacceptabilă
RP 1.1 Respingerea ofertei ca inacceptabilă – ofertantul nu îndeplinește cerințele
RP 1.2 Respingerea ofertei ca inacceptabilă – depășește fondul alocat
RP 1.3 Respingerea ofertei – oferta tehnică nu corespunde cerințelor
RP 1.4 Lipsa garanției pentru ofertă
RP 1.5 Preț anormal de scăzut
RP 1.6 Lipsa clarificărilor din partea autorității
RP 1.7 Lipsa transmiterii documentelor solicitate
RP 1.8 Modificarea conținutului prin răspunsuri – tehnic
RP 1.9 Modificarea conținutului prin răspunsuri – financiar
RP 1.10 Modul de punctare/evaluare al ofertei
RP 1.11 Ofertă neadecvată față de obiectul achiziției
RP 1.12 Completarea defectuoasă a formularelor
RP 2 Acceptarea ofertelor altor participanți neconforme/inacceptabile
RP 2.1 Participanții nu îndeplinesc cerințele de calificare
RP 2.2 Ofertele tehnice nu corespund cerințelor
RP 2.3 Lipsa garanției pentru ofertă
RP 2.4 Preț anormal de scăzut
RP 2.5 Modificări prin răspunsuri – tehnic
RP 2.6 Modificări prin răspunsuri – financiar
RP 2.7 Modul de punctare al ofertelor
RP 2.8 Formulare completate defectuos de alți participanți
RP 3 Neinformarea privind rezultatul procedurii de atribuire
RP 4 Anularea fără temei legal a procedurii
RP 5 Erori tehnice privind SIA RSAP (MTender)
RP 6 Altele
DA – Deficiențe în documentația de atribuire
DA 1 Cerințe restrictive privind situația personală a ofertantului
DA 2 Cerințe restrictive privind situația economico-financiară
DA 2.1 Cerințe privind disponibilitatea de lichidități
DA 2.2 Cerințe privind cifra medie de afaceri
DA 3 Cerințe privind capacitatea tehnică/profesională
DA 3.1 Cerințe privind experiența similară
DA 4 Cerințe privind standarde de calitate / mediu
DA 5 Cerințe restrictive privind specificații tehnice
DA 6 Criterii de atribuire neclare/subiective
DA 7 Mărci/produse/tehnologii fără "sau echivalent"
DA 8 Lipsă de răspuns clar din partea autorității
DA 9 Forma de constituire a garanției pentru ofertă
DA 10 Clauze contractuale inechitabile/excesive
DA 11 Neîmpărțirea achiziției pe loturi
DA 12 Publicarea documentației incomplete
DA 12.1 Altele

OBIECTUL CONTESTAȚIEI

Documentele de atribuire/anunțul de participare
Rezultatele procedurii

TIP PROCEDURĂ

Licitație publică: LP
Cerere ofertă de prețuri: COP

5. CERINȚE NEFUNCȚIONALE

Această secțiune a specificațiilor tehnice consacră un cadru detaliat pentru definirea cerințelor nefuncționale esențiale ce guvernează proiectarea, dezvoltarea, implementarea și operarea Sistemului Informațional de Management Electronic al Documentelor (SIMED) al Autorității Naționale pentru Soluționarea Contestațiilor (ANSC). Aceste cerințe, deși nu vizează în mod direct comportamentele funcționale explicite ale sistemului, constituie fundamentul arhitectural al soluției IT și determină performanțele de ansamblu ale acesteia în mediile reale de exploatare instituțională.

Cerințele nefuncționale definesc în mod riguros parametrii de calitate, securitate, eficiență și interoperabilitate care trebuie respectați pentru a asigura un sistem robust, fiabil, scalabil și sustenabil pe termen lung. Ele transpun în termeni tehnici așteptările instituționale privind comportamentul sistemului în condiții variate de utilizare, garantând că infrastructura digitală a ANSC va fi în măsură să răspundă corespunzător provocărilor de ordin operațional, legal și strategic.

Soluția SIMED trebuie să asigure, în mod documentat și auditat, următoarele caracteristici esențiale:

- **Stabilitate operațională și reziliență sistemică**, indiferent de complexitatea cazurilor procesate, de încărcarea sistemului sau de factorii externi perturbatori;
- **Scalabilitate elastică**, atât verticală (prin extinderea resurselor hardware/software), cât și orizontală (prin creșterea capacității de procesare paralelă pentru un număr mai mare de utilizatori sau contestații);
- **Interoperabilitate avansată și nativă**, cu ecosistemul digital guvernamental din Republica Moldova, prin integrarea facilă cu servicii partajate precum MPass (autentificare), MSign (semnătură digitală), MNotify (notificări), MConnect (interfațare de date), MPay (plăți) și MCabinet (comunicare instituțională);
- **Conformitate deplină** cu legislația națională aplicabilă în domeniul protecției datelor cu caracter personal (Legea nr. 133/2011), securității cibernetice, arhivării electronice și accesului la informațiile publice, precum și cu reglementările europene (ex. GDPR, eIDAS, NIS2);
- **Ergonomie digitală superioară și experiență de utilizare intuitivă**, adaptată diversității actorilor implicați în procedura de contestații (autorități contractante, operatori economici, membri ANSC), cu interfețe moderne, responsive și orientate pe sarcini.

Pentru asigurarea unei guvernanțe tehnice coerente, fiecare cerință nefuncțională este codificată în baza unei convenții de structurare de forma X.Y, unde:

- **X** reprezintă domeniul tematic al cerinței (ex. disponibilitate, securitate, mentenanță, performanță, accesibilitate etc.);
- **Y** este un identificator unic în cadrul respectivei categorii.

În plus, cerințele sunt ierarhizate după nivelul de obligativitate, după cum urmează:

- **M – Mandatory**: cerințe obligatorii a căror implementare este critică pentru validarea soluției;
- **D – Desirable**: cerințe recomandate ce aduc plus-valoare în termeni de eficiență, utilizabilitate și adaptabilitate;

- **I – Informativ**: cerințe orientative, care reflectă bunele practici internaționale și standardele de referință în domeniul guvernanței IT.

Această structură metodologică permite o trasabilitate completă și o evaluare transparentă a conformității sistemului, facilitând etapele de proiectare, dezvoltare incrementală (DevSecOps), testare, implementare și audit post-livrare. Prin urmare, cerințele nefuncționale nu sunt accesorii, ci constituie coloana vertebrală care susține calitatea, sustenabilitatea și încrederea în SIMED ca platformă digitală națională pentru soluționarea contestațiilor în domeniul achizițiilor publice.

Tabelul 5. Categorii de cerințe nefuncționale

Acronim	Semnificație	Descriere
ARH	Cerințe de arhitectură	Cerințele vizează arhitectura logică și tehnică a sistemului, inclusiv modularitatea, separarea responsabilităților și conformitatea cu standardele guvernamentale.
CPF	Cerințe privind punerea în funcțiune	Cerințele descriu procesul de tranziție de la dezvoltare la producție, incluzând configurarea mediului operațional și validarea funcționalităților de bază.
DEL	Cerințe privind produsele livrabile	Cerințele definesc setul de produse, documente și artefacte obligatorii ce trebuie furnizate de către dezvoltator în cadrul proiectului.
DEP	Cerințe privind desfășurarea	Cerințele descriu activitățile și condițiile necesare pentru integrarea și operaționalizarea sistemului în infrastructura ANSC.
DEV	Cerințe de dezvoltare	Cerințele stabilesc principiile de proiectare, standardele de cod, controlul versiunilor și cerințele metodologice pentru procesul de dezvoltare.
FLEX	Cerințe privind flexibilitatea	Cerințele se referă la capacitatea sistemului de a se adapta rapid la modificări de legislație, procese sau volum de date, fără intervenții majore.
GMS	Cerințe privind perioada de stabilizare, mentenanță și suport post-implementare	Cerințele reglementează serviciile de asistență tehnică, mentenanță corectivă și evolutivă, precum și timpul de reacție în perioada post-livrare.
INT	Cerințe de interoperabilitate	Cerințele definesc capacitatea sistemului de a comunica cu alte sisteme publice prin API-uri, formate standard și infrastructuri interoperabile.
LPR	Cerințe privind licențele și proprietatea intelectuală	Cerințele se referă la regimul juridic al codului sursă, componentelor software, licențelor și drepturilor patrimoniale aferente sistemului livrat.
MG	Cerințe privind gestionarea proiectului	Cerințele stabilesc structura de guvernanță a proiectului, responsabilii cheie, calendarul de livrare și instrumentele de monitorizare.
MIG	Cerințe privind migrarea datelor	Cerințele vizează strategia de migrare a datelor existente în format digital sau fizic, validarea și integrarea în sistemul nou.
MR	Cerințe privind întreținerea	Cerințele detaliază acțiunile de întreținere periodică necesare pentru funcționarea optimă și durabilă a sistemului.

Acronim	Semnificație	Descriere
PIR	Cerințe postimplementare	Cerințele definesc obligațiile furnizorului după livrarea sistemului, inclusiv perioada de garanție, ajustări și menținerea performanței.
PSR	Cerințe privind performanța și scalabilitatea sistemului IT	Cerințele definesc parametrii tehnici minimi privind viteza de răspuns, volumul de procesare și extensibilitatea în funcție de nevoi viitoare.
RC	Cerințe privind reziliența și continuitatea	Cerințele stabilesc măsuri de continuitate în caz de defecțiuni, dezastre sau întreruperi, inclusiv backup și recuperare rapidă.
SEC	Cerințe de securitate	Cerințele stabilesc standarde de securitate pentru protecția datelor, accesul utilizatorilor, criptare, audit și prevenirea atacurilor informatice.
SLA	Cerințe privind nivelul serviciilor oferite de furnizor	Cerințele stabilesc parametrii minimi agreați privind disponibilitatea serviciilor, timpul de răspuns și remedierea incidentelor.
STAB	Cerințe privind perioada de stabilizare	Cerințele definesc perioada imediat următoare punerii în funcțiune, în care sistemul este monitorizat intensiv pentru corectarea anomaliilor.
TS	Stack tehnologic	Cerințele stabilesc tehnologiile, platformele și limbajele de programare permise sau recomandate pentru dezvoltarea sistemului.
UAT	Testarea acceptării utilizatorului	Cerințele descriu etapele și criteriile de validare practică a funcționalităților livrate de către utilizatori finali.
UTD	Formarea și documentația utilizatorilor	Cerințele stabilesc conținutul, durata, forma și materialele pentru instruirea utilizatorilor sistemului.
UI	Cerință privind interfața cu utilizatorul	Cerințele definesc calitatea interfeței grafice, ergonomia, accesibilitatea și experiența utilizatorului în interacțiunea cu sistemul.

5.1. Cerințe privind licențierea și proprietatea intelectuală

ANSC va beneficia, fără limită de timp, de toate drepturile necesare pentru utilizarea, operarea, administrarea, modificarea, mentenanța, extinderea și transferul SIMED. Drepturile asupra componentelor dezvoltate special în cadrul proiectului vor fi transferate integral către ANSC, cu delimitarea clară a componentelor FOD/PDSE și a produselor terțe preexistente.

Tabelul 5.1 stabilește cerințele privind licențierea, codul sursă, componentele software, datele și drepturile de proprietate intelectuală. Cerințele sunt aliniate modelului AGE, care prevede drept de utilizare perpetuă, drept de redistribuire și drepturi depline asupra datelor, precum și cerințelor privind evitarea dependenței de furnizor și inventarierea componentelor software.

Tabelul 5.1 Cerințe privind licențele și proprietatea intelectuală

ID	Obligativitate	Cerință/Descriere
LPI 001	M	Contractantul va asigura ANSC dreptul perpetuu, irevocabil și fără limitări teritoriale de a instala, rula, utiliza, administra, reproduce, configura, modifica, testa, migra, integra, menține și extinde SIMED în toate mediile necesare, inclusiv dezvoltare, testare, instruire, preproducție, producție și recuperare în caz de dezastru.

ID	Obligativitate	Cerință/Descriere
LPI 002	M	Soluția și licențele aferente nu vor impune restricții privind numărul utilizatorilor, utilizatorii simultani, tranzacțiile procesate, volumul datelor, numărul mediilor, numărul instanțelor aplicației, capacitatea de procesare sau funcționalitățile utilizate.
LPI 003	M	Soluția va utiliza cu prioritate componente open-source distribuite sub licențe permisive, precum MIT, BSD sau Apache 2.0. Utilizarea produselor comerciale sau a componentelor proprietare va fi permisă numai dacă este justificată, aprobată în prealabil de ANSC și nu generează dependență critică de un furnizor unic.
LPI 004	M	Toate costurile aferente licențelor indispensabile implementării și funcționării soluției vor fi incluse în oferta financiară. SIMED nu va depinde, după recepția finală, de abonamente, licențe recurente sau servicii comerciale neaprobate care ar împiedica funcționarea sistemului în lipsa unor plăți suplimentare.
LPI 005	M	Drepturile patrimoniale asupra codului sursă, configurațiilor, extensiilor, adaptoarelor, API-urilor, modelelor de date, scripturilor, șabloanelor și celorlalte componente dezvoltate special pentru SIMED vor fi transferate integral către ANSC, în condițiile contractului.
LPI 006	M	Drepturile transferate ANSC vor include cel puțin dreptul de utilizare, reproducere, modificare, adaptare, traducere, integrare, compilare, instalare, migrare, distribuire, reutilizare și dezvoltare ulterioară, direct sau prin intermediul unor terți desemnați de ANSC.
LPI 007	M	Codul sursă complet al componentelor dezvoltate în cadrul proiectului va fi livrat continuu în repozitoriul indicat de ANSC sau de autoritatea tehnică competentă. Livrarea exclusiv sub formă de arhive, executabile sau fișiere compilate nu va fi acceptată.
LPI 008	M	Livrarea codului sursă va include toate fișierele necesare compilării, testării, construirii imaginilor de containere, configurării, instalării, migrării bazei de date și implementării automate a sistemului, precum și documentația aferentă.
LPI 009	M	Componentele, modulele și bibliotecile FOD/PDSE existente anterior proiectului nu vor face obiectul transferului drepturilor de proprietate către ANSC. Acestea vor fi reutilizate conform regimului juridic și condițiilor stabilite pentru FOD/PDSE. Configurările, extensiile și componentele dezvoltate special pentru SIMED vor fi evidențiate separat.
LPI 010	M	Contractantul va prezenta un registru complet al componentelor software utilizate, în care va indica pentru fiecare componentă: denumirea, versiunea, furnizorul, proveniența, scopul utilizării, tipul licenței, perioada de suport, eventualele costuri și restricțiile aplicabile.
LPI 011	M	Contractantul va furniza și actualiza la fiecare livrare semnificativă un inventar al componentelor software și al dependențelor directe și tranzitive, în format SBOM, corelat cu versiunea efectiv livrată a sistemului.
LPI 012	M	Nu se admite utilizarea componentelor cu licențe copyleft, restrictive sau incompatibile care pot obliga publicarea codului sursă al SIMED, limita modificarea ori redistribuirea soluției sau crea alte obligații neacceptate de ANSC, decât în baza unei analize juridice și tehnice aprobate în prealabil.

ID	Obligativitate	Cerință/Descriere
LPI 013	M	Sistemul nu va include componente, servicii sau mecanisme care depind de conturi personale, conturi ale Contractantului, chei, certificate, registre de artefacte, repozitorii private sau infrastructuri aflate exclusiv sub controlul Contractantului.
LPI 014	M	ANSC va avea dreptul de a transfera SIMED, codul sursă, configurațiile și drepturile de utilizare către o altă autoritate sau instituție publică, inclusiv în cazul reorganizării instituționale, schimbării posesorului sistemului sau desemnării unei alte entități pentru operare și mentenanță.
LPI 015	M	Contractantul va declara distinct toate componentele preexistente proprii sau ale terților pe care intenționează să le integreze în soluție. Componentele nedeclarate la etapa aprobării stivei tehnologice vor putea fi respinse de ANSC.
LPI 016	M	Contractantul garantează că deține toate drepturile și autorizările necesare pentru utilizarea și integrarea componentelor livrate și că soluția nu încalcă drepturile de proprietate intelectuală ale terților. Contractantul va răspunde pentru revendicările rezultate din utilizarea neautorizată a unor componente software.
LPI 017	M	ANSC va deține drepturi depline asupra tuturor datelor, documentelor, metadatelor, nomenclatoarelor, configurațiilor funcționale, rapoartelor și informațiilor introduse, prelucrate sau generate prin SIMED. Contractantul nu va dobândi niciun drept asupra acestora.
LPI 018	M	Contractantul va putea accesa datele SIMED numai în măsura strict necesară executării contractului, în baza drepturilor acordate și a obligațiilor de confidențialitate. Utilizarea datelor pentru alte scopuri, inclusiv analiză proprie, instruirea modelelor de inteligență artificială sau reutilizare comercială, este interzisă.
LPI 019	M	La încetarea contractului sau la solicitarea ANSC, Contractantul va restitui ori va elimina toate copiile datelor aflate în posesia sa, cu excepția celor a căror păstrare este impusă de lege, și va prezenta o confirmare privind eliminarea acestora.
LPI 020	M	Datele vor fi păstrate în formate deschise și documentate, iar SIMED va include mecanisme pentru exportul complet al datelor, documentelor și metadatelor, astfel încât migrarea către o altă soluție să poată fi realizată fără dependență critică de Contractant.
LPI 021	M	La recepția finală, Contractantul va preda ANSC toate conturile administrative, configurațiile, certificatele, cheile, tokenurile, parolele, artefactele și informațiile de acces necesare operării independente a sistemului.
LPI 022	M	Contractantul nu va putea reutiliza, distribui sau comercializa codul, configurațiile, regulile de business, șabloanele și componentele dezvoltate exclusiv pentru SIMED fără acordul scris al ANSC. Această restricție nu se aplică instrumentelor generice și componentelor preexistente declarate și acceptate înainte de utilizarea lor în proiect.

5.2. Cerințe privind arhitectura sistemului IT

Arhitectura SIMED va fi deschisă, modulară, securizată și extensibilă, compatibilă cu FOD/PDSE, tehnologia .NET și infrastructura MCloud. Front Office-ul va reutiliza componentele FOD/PDSE, iar Back Office-ul va fi configurat și adaptat conform fluxurilor operaționale și regulilor procedurale ale ANSC.

Comunicarea dintre componente se va realiza prin API-uri și mesaje documentate, fără acces direct al Front Office-ului sau al sistemelor externe la bazele de date ale Back Office-ului. Alegerea arhitecturii va respecta principiile cloud-native, container-first, API-first, secure-by-design și reuse-before-build.

Tabelul 5.2 conține cerințele tehnice detaliate referitoare la arhitectura sistemului.

ID	Obligativitate	Cerință/Descriere
ARH 001	M	Arhitectura SIMED trebuie să utilizeze standarde deschise și formate interoperabile inclusiv HTTPS, REST, JSON, XML, UTF-8 și OpenAPI 3.1. SOAP va fi utilizat numa pentru integrările în care este impus de sistemul extern.
ARH 002	M	Componenta Front Office trebuie realizată prin reutilizarea, configurarea și adaptare componentelor FOD/PDSE. Dezvoltarea unor funcționalități paralele va fi permisă numa dacă analiza de decalaj demonstrează că acestea nu pot fi acoperite prin componentel existente.
ARH 003	M	Componentele principale ale Back Office-ului, serviciile backend, API-urile și extensiil aferente FOD/PDSE trebuie dezvoltate utilizând C# și .NET/ASP.NET Core într- versiune LTS aflată în suport activ.
ARH 004	M	Arhitectura trebuie să asigure separarea clară dintre Front Office, Back Office, stratul d integrare, serviciile comune, stratul de date, managementul documentelor, raportare ș administrare.
ARH 005	M	Front Office-ul nu va accesa direct bazele de date, sistemele de stocare sau serviciil interne ale Back Office-ului. Toate operațiunile vor fi realizate prin API-uri și servici aplicaționale securizate.
ARH 006	M	Soluția trebuie să fie modulară și orientată pe servicii. Microserviciile vor fi utilizat pentru frontiere funcționale distincte și justificate, evitând fragmentarea excesivă. Pentr componentele care nu justifică separarea se admite o arhitectură de tip monolit modula cu granițe clare între module.
ARH 007	M	Modulele și serviciile trebuie proiectate astfel încât să poată fi dezvoltate, testate implementate, scalate și actualizate independent, în măsura permisă de relațiil funcționale dintre acestea.
ARH 008	M	Arhitectura trebuie să respecte principiile cloud-native și container-first și să permit rularea componentelor aplicaționale în containere construite automat și reproductibil.
ARH 009	M	SIMED trebuie să fie compatibil cu infrastructura MCloud, inclusiv cu OpenStack ș Kubernetes, în măsura în care acestea sunt puse la dispoziție în mediul tehnic țintă.
ARH 010	M	Componentele server trebuie să fie compatibile cu sistemele de operare Linux aprobat pentru infrastructura guvernamentală, inclusiv familiile Red Hat/Rocky Linux/AlmaLinux sau Debian/Ubuntu LTS.
ARH 011	M	Arhitectura nu trebuie să depindă de servicii proprietare, conturi ale Contractantului sa infrastructuri externe care nu pot fi preluate și operate independent de ANSC ori d entitatea tehnică desemnată.

ID	Obligativitate	Cerință/Descriere
ARH 012	M	Arhitectura trebuie să evite punctele unice de eșec și să permită, în funcție de nivelul d disponibilitate aprobat, redundanță, distribuirea încărcării, replicare, failover și rulare mai multor instanțe ale componentelor critice.
ARH 013	M	Componentele aplicaționale trebuie proiectate, în măsura posibilului, fără păstrarea stări sesiunii exclusiv în memoria unei singure instanțe, astfel încât să permită scalare orizontală și redistribuirea solicitărilor.
ARH 014	M	Modificarea configurațiilor și scalarea componentelor nu trebuie să determine pierdere sesiunilor active, a solicitărilor în curs sau a mesajelor neprocesate.
ARH 015	M	Arhitectura trebuie să permită actualizarea controlată a componentelor, cu impact minin asupra disponibilității, inclusiv prin strategii de tip rolling update, blue-green sa mecanisme echivalente aprobate.
ARH 016	M	Sistemul trebuie proiectat conform principiilor API-first și specification-first. Contractel API trebuie definite și aprobate înaintea implementării funcționalităților de integrare.
ARH 017	M	API-urile publice și de integrare trebuie documentate conform OpenAPI 3.1. Pentr comunicarea internă dintre servicii se poate utiliza gRPC cu Protocol Buffers, dac utilizarea este justificată.
ARH 018	M	Componentele trebuie să comunice prin interfețe bine definite, versionate și slab cuplate Nu se admite integrarea prin acces direct la tabelele sau schemele bazei de date ale altu modul.
ARH 019	M	Pentru operațiunile care nu necesită un răspuns sincron imediat, arhitectura trebuie s permită procesarea asincronă prin mesaje și evenimente, utilizând RabbitMQ, MConnec Events sau Apache Kafka, în funcție de cazul de utilizare aprobat.
ARH 020	M	Mesajele asincrone trebuie să utilizeze identificatori unici de corelare, confirmare procesării, mecanisme de retry, prevenirea duplicatelor și cozi pentru mesajele care nu po fi procesate.
ARH 021	M	Interfețele externe și interne trebuie să utilizeze canale de comunicație criptate, protocoal TLS aflate în suport activ și mecanisme de autentificare tehnică aprobate.
ARH 022	M	Parolele, cheile, certificatele, tokenurile, șirurile de conexiune și celelalte date secret trebuie păstrate în mecanisme securizate și externalizate față de codul sursă și imaginil de containere.
ARH 023	M	Stratul de prezentare nu va implementa reguli de business, cu excepția validărilo orientative necesare interacțiunii cu utilizatorul. Toate regulile obligatorii vor fi verificat și în stratul aplicațional.
ARH 024	M	Logica de business trebuie implementată în servicii și module aplicaționale distincte d interfața utilizatorului și de mecanismele de persistență a datelor.
ARH 025	M	Accesul la date trebuie realizat exclusiv prin componentele autorizate ale stratulu aplicațional și de acces la date. Utilizatorii, Front Office-ul și sistemele externe nu vo avea acces direct la baza de date.

ID	Obligativitate	Cerință/Descriere
ARH 026	M	Modelul de date trebuie să reflecte toate obiectele informaționale gestionate de SIMED inclusiv contestații, dosare, documente, părți, proceduri de achiziție, complete, ședințe sarcini, termene și decizii.
ARH 027	M	PostgreSQL va fi utilizat ca bază de date relațională principală. Utilizarea altor sistem de gestiune a datelor este permisă numai pentru clase de probleme distincte și justificat prin arhitectura aprobată.
ARH 028	M	Fișierele, documentele, imaginile și atașamentele nu vor fi stocate direct în baza de dat relațională. Acestea vor fi păstrate într-un sistem de stocare de obiecte compatibil S3 utilizând MinIO sau o alternativă acceptată.
ARH 029	M	Sistemul trebuie să permită utilizarea OpenSearch sau a unei alternative acceptate pentr indexarea și căutarea full-text în date, metadate și conținutul documentelor, dac funcționalitățile și volumele o justifică.
ARH 030	M	Obiectele bazei de date trebuie să utilizeze o convenție unitară de denumire, documentat și aplicată consecvent. Pentru PostgreSQL se va utiliza, de regulă, limba engleză ș convenția lowercase_snake_case, evitând combinarea limbilor și stilurilor.
ARH 031	M	Tipurile de date ale bazei de date trebuie selectate conform naturii datelor și capabilităților PostgreSQL. Nu se vor utiliza tipuri sau lungimi derivate artificial din reprezentări XM dacă acestea nu corespund modelului de date relațional.
ARH 032	M	Sistemul trebuie să utilizeze UTF-8 pentru toate datele textuale și să asigure stocarea căutarea, sortarea și afișarea corectă a conținutului în limbile română, rusă și engleză.
ARH 033	M	Datele multilingve trebuie modelate astfel încât versiunile lingvistice să poată f administrate și extinse fără modificarea structurii de bază a entităților și fără duplicare necontrolată a datelor.
ARH 034	M	Fiecare obiect informațional principal trebuie să dețină un identificator tehnic unic imuabil și generat de sistem, de tip UUID sau echivalent. Identificatorii oficiali d business, precum numărul contestației sau numărul deciziei, vor fi gestionați separat.
ARH 035	M	Identificatorii tehnici nu vor fi configurabili manual de utilizatori și nu vor fi reutilizaț pentru alte obiecte, inclusiv după anularea logică a unei înregistrări.
ARH 036	M	Arhitectura datelor trebuie să asigure integritatea referențială, consistența tranzacțional și controlul concurenței în scenarii cu utilizatori și procese simultane.
ARH 037	M	Mecanismele de control al concurenței trebuie să prevină suprascrierea necontrolată modificărilor și să informeze utilizatorul atunci când datele au fost modificate simulta de un alt utilizator sau proces.
ARH 038	M	Modificările structurii bazei de date trebuie gestionate prin scripturi de migrar versionate, incrementale, automatizate și reproductibile, incluse în procesul CI/CD.
ARH 039	M	Modelul de date trebuie să includă mecanisme pentru păstrarea istoricului, versionare informațiilor critice și anularea logică a înregistrărilor, fără pierderea trasabilității.
ARH 040	M	Datele de referință, nomenclatoarele și clasificatoarele preluate din alte sisteme trebui sincronizate prin MConnect sau prin mecanismele oficiale aprobate, cu păstrarea sursei versiunii și datei actualizării.

ID	Obligativitate	Cerință/Descriere
ARH 041	M	Arhitectura trebuie să permită migrarea datelor existente ale ANSC și preluarea datelo relevante din SIA RSAP/MTender, cu validarea structurii, consistenței, integrității ș trasabilității datelor migrate.
ARH 042	M	Sarcinile operaționale și sarcinile de raportare trebuie proiectate astfel încât generare rapoartelor complexe să nu afecteze nejustificat procesarea tranzacțiilor curente. Se po utiliza replici de citire, procesare asincronă sau componente analitice distincte, dacă sun justificate.
ARH 043	M	Configurațiile aplicației, parametrii operaționali, adresele serviciilor și setările specific mediilor trebuie externalizate și administrate separat pentru dezvoltare, testare preproducție și producție.
ARH 044	M	Fiecare componentă aplicațională trebuie să includă mecanisme de health check ș readiness check pentru verificarea disponibilității, conectivității și pregătirii de a proces solicitări.
ARH 045	M	Arhitectura trebuie să asigure observabilitatea componentelor prin loguri structurate metrici, identificatori de corelare și, după caz, trasare distribuită a solicitărilor.
ARH 046	M	Contractantul trebuie să elaboreze și să mențină arhitectura funcțională, aplicațională, d date, integrare, securitate, infrastructură și implementare a SIMED.
ARH 047	M	Documentația arhitecturală trebuie să includă cel puțin diagrame de context, containere ș componente, diagrame de implementare, modele de date, fluxuri de integrare, zone d securitate și relațiile Front Office–Back Office.
ARH 048	M	Deciziile arhitecturale importante trebuie documentate prin înregistrări ADR, incluzân contextul, opțiunile analizate, decizia adoptată, justificarea, riscurile și consecințele.
ARH 049	M	Utilizarea UML, C4 Model sau a unor notații echivalente este permisă, cu condiția c documentația să fie coerentă, actualizată și suficient de detaliată pentru operarea ș dezvoltarea ulterioară a sistemului.
ARH 050	M	Arhitectura propusă și orice abatere semnificativă de la arhitectura aprobată trebui prezentate ANSC și coordonate, după caz, cu AGE și STISC înainte de implementare.
ARH 051	M	Contractantul trebuie să demonstreze la recepția finală că sistemul poate fi instalat într-u mediu nou pe baza codului sursă, configurațiilor, artefactelor și documentației predate fără dependență critică față de Contractant.

5.3. Cerințe privind stiva tehnologică guvernamentală

Stiva tehnologică a SIMED reprezintă ansamblul coerent de tehnologii, platforme, framework-uri, biblioteci, sisteme de gestiune a datelor, componente middleware, mecanisme de integrare, instrumente DevSecOps și servicii tehnologice utilizate pentru dezvoltarea, testarea, implementarea, operarea, monitorizarea și mentenanța sistemului.
Stiva tehnologică va fi proiectată și implementată în conformitate cu Stiva Tehnologică Guvernamentală aplicabilă sistemelor informaționale de stat, cu cerințele infrastructurii guvernamentale MCloud și cu documentația tehnică pusă la dispoziție de AGE și STISC.
Întrucât funcționalitățile destinate interacțiunii cu utilizatorii externi ai SIMED urmează să fie realizate prin reutilizarea, configurarea și adaptarea componentelor platformei FOD/PDSE, iar aceasta este dezvoltată utilizând

tehnologia .NET, stiva tehnologică principală a SIMED va fi compatibilă cu ecosistemul .NET. Componentele Back Office, serviciile aplicaționale, API-urile și extensiile dezvoltate în cadrul proiectului vor utiliza, cu prioritate obligatorie, C# și .NET/ASP.NET Core în versiuni Long-Term Support aflate în suport activ.
Utilizarea altor limbaje sau ecosisteme tehnologice va fi permisă numai pentru componente izolate și specializate, pentru care utilizarea .NET nu este adecvată din punct de vedere tehnic, cu condiția ca:

- respectiva componentă să nu dubleze funcționalități disponibile în FOD/PDSE;
- necesitatea utilizării unei alte tehnologii să fie justificată tehnic;
- integrarea cu restul sistemului să fie realizată prin contracte și interfețe standardizate;
- tehnologia să fie prevăzută sau acceptată de Stiva Tehnologică Guvernamentală;
- abaterea să fie aprobată în prealabil de ANSC și coordonată, după caz, cu AGE și STISC.

SIMED va fi proiectat conform principiilor **cloud-native**, **container-first**, **API-first**, **secure-by-design**, **reuse-before-build** și **specification-first**. Soluția va fi compatibilă cu infrastructura MCloud și va putea fi instalată, configurată, actualizată și operată prin procese automatizate și reproductibile.
Oferta nu va include procurarea infrastructurii hardware. Cerințele privind calculul, stocarea, rețeaua, orchestrarea, backup-ul și celelalte resurse de infrastructură vor fi documentate de Contractant și coordonate cu ANSC și STISC pentru găzduirea în MCloud.
Sistemul nu va depinde nejustificat de servicii proprietare, conturi ale Contractantului, infrastructuri externe sau tehnologii care nu pot fi preluate, operate și dezvoltate independent de ANSC sau de entitatea tehnică desemnată.
Tehnologiile pentru baze de date, stocare de obiecte, căutare, cache, mesagerie, streaming și analiză vor fi selectate în funcție de clasa problemei tehnice. Contractantul nu va introduce toate tehnologiile prevăzute în Stiva Tehnologică Guvernamentală în mod automat, ci numai componentele necesare și justificate prin arhitectura aprobată.

Tabelul 5.3 prezintă cerințele funcționale și non-funcționale aferente stivei tehnologice a sistemului.

ID	Obligativitate	Cerință/Descriere
TS 001	M	Stiva tehnologică a SIMED trebuie să fie conformă cu Stiva Tehnologică Guvernamentală aplicabilă la data inițierii proiectului sau la momentul de referință stabilit prin documentația de achiziție și contract.
TS 002	M	Soluția trebuie să reutilizeze, configureze și adapteze componentele și funcționalitățile disponibile în cadrul FOD/PDSE pentru componenta de interacțiune cu utilizatorii externi. Dezvoltarea unor componente paralele este permisă numai în baza unei analize de decalaj aprobate.
TS 003	M	Componentele Back Office, serviciile backend, API-urile și extensiile aferente FOD/PDSE trebuie dezvoltate utilizând C# și .NET/ASP.NET Core într-o versiune LTS aflată în suport activ pe durata implementării, garanției și mentenanței contractuale.
TS 004	M	Utilizarea altor limbaje de programare decât C#/.NET pentru componentele principale ale SIMED nu este permisă. Pentru componente tehnice izolate și specializate se pot utiliza alte limbaje acceptate de Stiva Tehnologică Guvernamentală numai în baza unei justificări tehnice documentate și aprobate în prealabil.
TS 005	M	Arhitectura trebuie să fie modulară și orientată pe servicii. Microserviciile vor fi utilizate pentru frontiere funcționale distincte și justificate. Fragmentarea excesivă a soluției trebuie evitată; pentru componentele care nu justifică separarea în microservicii se admite un monolit modular, cu granițe funcționale clar definite.

ID	Obligativitate	Cerință/Descriere
TS 006	M	Sistemul trebuie proiectat conform principiului container-first. Componentele aplicaționale vor rula în containere, iar construcția imaginilor de containere va fi automatizată și reproductibilă.
TS 007	M	Imaginile de containere trebuie să fie minimizate, versionate, scanate din perspectiva vulnerabilităților și construite exclusiv pe baza codului și fișierelor de configurare păstrate în repozitoriul aprobat.
TS 008	M	Soluția trebuie să fie compatibilă cu infrastructura MCloud, inclusiv cu OpenStack ca nivel de infrastructură și cu Kubernetes ca nivel de orchestrare, în măsura în care aceste servicii sunt disponibile în mediul țintă pus la dispoziție de STISC.
TS 009	M	Configurarea și operarea soluției trebuie să fie compatibile cu instrumentele de administrare a orchestrării utilizate în infrastructura guvernamentală, inclusiv Rancher sau OpenShift, în funcție de mediul efectiv pus la dispoziție.
TS 010	M	Sistemul trebuie să fie compatibil cu sisteme de operare Linux utilizate în infrastructura guvernamentală, inclusiv familia Red Hat/Rocky Linux/AlmaLinux sau familia Debian/Ubuntu LTS. Componentele server nu trebuie să depindă de un sistem de operare Windows.
TS 011	M	Configurarea infrastructurii și a mediilor trebuie documentată și, acolo unde este aplicabil, definită prin mecanisme declarative și versionabile, utilizând Ansible și/sau OpenTofu ori instrumente echivalente aprobate pentru MCloud.
TS 012	M	Codul sursă, configurațiile, scripturile, documentația tehnică și definițiile infrastructurii trebuie gestionate prin Git și livrate în repozitoriul indicat de ANSC sau de autoritatea tehnică competentă.
TS 013	M	Pipeline-ul CI/CD trebuie să fie implementat utilizând infrastructura aprobată pentru sistemele informaționale de stat. Se va utiliza Gitea cu Gitea Runner ca opțiune principală sau GitLab Community Edition ca alternativă acceptată, în funcție de mediul pus la dispoziție.
TS 014	M	Pipeline-ul CI/CD nu trebuie să depindă de conturi, abonamente, runner-e, registre de artefacte sau infrastructuri controlate exclusiv de Contractant.
TS 015	M	Serverul web, reverse proxy-ul și mecanismul de ingress trebuie să fie compatibile cu Stiva Tehnologică Guvernamentală. NGINX va constitui opțiunea principală; alte soluții acceptate pot fi utilizate numai dacă sunt justificate și compatibile cu infrastructura țintă.
TS 016	M	SIMED trebuie să aplice principiile API-first și specification-first. Contractele API trebuie definite și aprobate înaintea implementării funcționalităților aferente.
TS 017	M	API-urile publice și de integrare trebuie documentate în format OpenAPI 3.1 și trebuie să utilizeze, cu prioritate, REST, HTTPS și JSON.
TS 018	M	Pentru comunicarea internă între servicii se poate utiliza gRPC cu Protocol Buffers, atunci când acest mecanism este justificat de cerințele de performanță, tipizare sau comunicare internă. gRPC nu va substitui API-urile publice REST.
TS 019	M	Schimbul de date cu registrele, platformele și sistemele informaționale de stat trebuie realizat prin MConnect, inclusiv, după caz, prin mecanismele de evenimente puse la

ID	Obligativitate	Cerință/Descriere
		dispoziție de platformă. Conexiunile directe între sisteme sunt permise numai în cazuri justificate, documentate și aprobate.
TS 020	M	Toate comunicațiile externe și interne care transportă date sensibile trebuie realizate prin canale criptate și protocoale securizate, utilizând versiuni TLS aflate în suport activ și configurații criptografice aprobate.
TS 021	M	Sistemul trebuie să utilizeze PostgreSQL ca bază de date relațională principală. Utilizarea MariaDB sau MS SQL Server este permisă numai în cazuri justificate de compatibilitatea cu componente existente, cu aprobarea ANSC și coordonarea tehnică necesară.
TS 022	M	Structura bazei de date, modificările de schemă și datele de configurare trebuie gestionate prin migrații versionate, incrementale, automatizate și reproductibile.
TS 023	M	Fișierele, documentele, imaginile și atașamentele nu vor fi stocate direct în baza de date relațională. Acestea vor fi păstrate într-un sistem de stocare de obiecte compatibil S3, utilizând MinIO sau o alternativă acceptată de Stiva Tehnologică Guvernamentală.
TS 024	M	Sistemul trebuie să permită indexarea și căutarea full-text în date și documente prin utilizarea OpenSearch sau a unei alternative acceptate, dacă această componentă este justificată prin cerințele funcționale și de volum.
TS 025	M	Pentru mecanismele de cache și stocare in-memory se va utiliza cu prioritate Valkey. Redis poate fi utilizat ca alternativă numai după analiza licenței, riscurilor de mentenanță și compatibilității cu infrastructura țintă.
TS 026	M	Pentru procesarea asincronă și schimbul fiabil de mesaje se va utiliza RabbitMQ, dacă această componentă este necesară conform arhitecturii aprobate.
TS 027	M	Apache Kafka poate fi utilizat pentru fluxuri distribuite de evenimente și volume ridicate de date. Kafka și RabbitMQ vor fi utilizate pentru cazurile distincte pentru care sunt proiectate și nu vor fi tratate ca tehnologii interschimbabile.
TS 028	M	Pentru rapoarte analitice complexe sau procesare OLAP pe volume mari de date poate fi utilizat ClickHouse sau o alternativă acceptată, numai dacă necesitatea este demonstrată prin analiza volumelor și a cerințelor de raportare.
TS 029	M	Pentru date cu schemă flexibilă poate fi utilizat MongoDB sau o alternativă acceptată numai în cazuri justificate, precum formulare dinamice, gestionarea conținutului sau structuri de date care nu pot fi administrate eficient în baza de date relațională.
TS 030	M	Interfețele utilizator trebuie să reutilizeze componentele și resursele FOD/PDSE și să respecte Modelul Unitar de Design. Contractantul nu va crea un sistem de design paralel care dublează componentele guvernamentale disponibile.
TS 031	M	Pentru componente UI noi din ecosistemul .NET se pot utiliza tehnologii compatibile precum Blazor Server, Blazor WebAssembly sau Razor Pages, dacă sunt compatibile cu arhitectura FOD/PDSE și cu Modelul Unitar de Design.
TS 032	M	În cazul utilizării ecosistemului JavaScript/TypeScript pentru extensii frontend, TypeScript este obligatoriu. JavaScript fără tipizare statică nu este acceptat pentru cod frontend nou. Se vor utiliza numai framework-uri mature și suportate, compatibile cu componentele FOD/PDSE și MUD.

ID	Obligativitate	Cerință/Descriere
TS 033	M	Soluția trebuie să fie accesibilă prin browsere web și nu va necesita instalarea unei aplicații client dedicate, cu excepția componentelor oficiale impuse de serviciile guvernamentale reutilizate.
TS 034	M	Sistemul trebuie să fie compatibil cu cele mai recente două versiuni majore ale browserelor Google Chrome, Mozilla Firefox, Microsoft Edge și Safari, disponibile la momentul testării de acceptanță.
TS 035	M	Interfețele destinate publicului trebuie să fie responsive și conforme cu WCAG 2.1 nivel AA, inclusiv în ceea ce privește navigarea prin tastatură, compatibilitatea cu tehnologiile asistive, contrastul, structura semantică și mesajele de eroare.
TS 036	M	Sistemul trebuie să utilizeze codificarea UTF-8 pentru toate datele textuale și să asigure procesarea, stocarea, căutarea, sortarea și afișarea corectă a conținutului în limbile română, rusă și engleză.
TS 037	M	Textele interfeței, mesajele de eroare, notificările și formularele trebuie externalizate și administrate astfel încât să poată fi traduse sau actualizate fără modificarea codului sursă.
TS 038	M	Configurațiile aplicației, adresele serviciilor, parametrii de mediu și datele secrete trebuie externalizate. Parolele, cheile, certificatele, tokenurile și șirurile de conexiune nu vor fi incluse în codul sursă, imaginile containerelor sau fișierele publice ale repozitoriului.
TS 039	M	Sistemul trebuie să utilizeze mecanisme clare de versionare pentru cod, aplicație, API-uri, baze de date, configurații, imagini de containere și artefacte, inclusiv Semantic Versioning acolo unde este aplicabil.
TS 040	M	Toate dependențele directe și tranzitive trebuie declarate explicit, versionate și gestionate prin manageri de pachete corespunzători ecosistemului tehnologic utilizat.
TS 041	M	Contractantul trebuie să furnizeze și să actualizeze la fiecare livrare semnificativă inventarul complet al componentelor software și dependențelor, în format SBOM, incluzând versiunea, furnizorul, licența, proveniența și statutul de suport.
TS 042	M	Se vor utiliza cu prioritate componente distribuite sub licențe permisive, inclusiv MIT, BSD și Apache 2.0. Nu se admit componente a căror licență poate impune publicarea codului sursă al SIMED sau poate limita operarea și mentenanța independentă, fără o analiză juridică și tehnică aprobată în prealabil.
TS 043	M	Sistemul nu trebuie să utilizeze tehnologii experimentale, versiuni fără suport activ, componente aflate în End-of-Life, tehnologii fără roadmap clar sau componente care prezintă riscuri majore de securitate, licențiere ori mentenanță.
TS 044	M	Nu se admit tehnologii care creează dependență critică față de un furnizor unic, de conturile Contractantului, de servicii SaaS neaprobate sau de infrastructuri care nu pot fi administrate și operate independent de ANSC ori de entitatea desemnată.
TS 045	M	Componentele SIMED trebuie să utilizeze jurnalizare structurată în format JSON, cu identificatori de corelare și cu posibilitatea colectării și procesării centralizate a logurilor prin mecanismele aprobate în infrastructura guvernamentală.
TS 046	M	Evenimentele semnificative din punct de vedere juridic, operațional și de securitate trebuie transmise către MLog, fără a exclude păstrarea logurilor locale necesare operării, monitorizării și depanării.

ID	Obligativitate	Cerință/Descriere
TS 047	M	Sistemul trebuie să dispună de endpoint-uri standardizate pentru verificarea disponibilității și pregătirii componentelor, inclusiv health check și readiness check, utilizabile de platforma de orchestrare și de sistemele de monitorizare.
TS 048	M	Build-ul, testarea, scanarea de securitate, generarea SBOM, construirea imaginilor, publicarea artefactelor, instalarea și verificările post-deploy trebuie automatizate prin pipeline-ul CI/CD.
TS 049	M	Eșecul testelor obligatorii, scanărilor critice sau verificărilor de conformitate trebuie să blocheze promovarea automată a livrării către mediile următoare.
TS 050	M	Instalarea și actualizarea sistemului trebuie realizate prin mecanisme automatizate și reproductibile. Copierea manuală necontrolată a fișierelor în mediile de staging și producție nu este permisă.
TS 051	M	Sistemul trebuie să permită upgrade, downgrade și rollback controlat al aplicației, configurațiilor și bazei de date, cu păstrarea integrității datelor și cu impact minim asupra disponibilității serviciului.
TS 052	M	Contractantul trebuie să demonstreze, la recepția finală, că SIMED poate fi instalat într-un mediu nou exclusiv pe baza codului sursă, configurațiilor, scripturilor, artefactelor și documentației predate, prin realizarea unui test de deploy independent.
TS 053	M	Sistemul trebuie să reutilizeze serviciile guvernamentale aplicabile, inclusiv MPass pentru autentificare, MSign pentru semnătură, MConnect pentru schimb de date, MPower pentru împuterniciri, MNotify pentru notificări, MLog pentru jurnalizare și, după caz, MDocs, MPay și MDelivery.
TS 054	M	Nu se admite implementarea unor mecanisme paralele de autentificare, semnare, schimb de date, notificare sau jurnalizare atunci când funcționalitatea respectivă este asigurată de un serviciu guvernamental reutilizabil și aplicabil SIMED.
TS 055	M	Contractantul trebuie să furnizeze descrierea completă a stivei tehnologice propuse, incluzând limbajele, versiunile, framework-urile, bazele de date, componentele middleware, instrumentele DevSecOps, sistemele de stocare, licențele și justificarea utilizării fiecărei componente.
TS 056	M	Contractantul trebuie să prezinte o matrice de conformitate cu Stiva Tehnologică Guvernamentală, cerințele FOD/PDSE, cerințele MCloud/STISC și prezentul ToR, indicând pentru fiecare cerință soluția propusă și dovada conformității.
TS 057	M	Orice abatere de la stiva tehnologică aprobată trebuie documentată înainte de implementare și trebuie să includă motivul, alternativele analizate, impactul asupra securității, interoperabilității, portabilității, licențierii, mentenanței și costurilor de operare. Abaterea va necesita aprobarea ANSC și coordonarea cu AGE/STISC, după caz.

5.4. Cerințe privind sistemul de gestionare a bazelor de date și administrarea datelor relaționale

IMED va utiliza **PostgreSQL** ca sistem principal de gestiune a bazelor de date relaționale, în conformitate cu Stiva Tehnologică Guvernamentală și cerințele infrastructurii MCloud. Compatibilitatea cu FOD/PDSE și cu tehnologia

.NET va fi asigurată prin drivere și framework-uri de acces la date suportate activ, fără ca utilizarea .NET să impună automat Microsoft SQL Server.
Modelul de date va reflecta procesele și obiectele informaționale specifice ANSC și va asigura integritatea, trasabilitatea, securitatea, performanța și administrarea controlată a datelor pe întregul ciclu de viață al SIMED.

ID	Obligativitate	Descriere
SGBD 001		Sistemul trebuie să utilizeze un sistem de gestiune a bazelor de date relaționale matur, stabil, suportat activ și compatibil cu Stiva Tehnologică Guvernamentală, infrastructura MCloud și cerințele operaționale ale ANSC și STISC.
SGBD 002		SIMED trebuie să utilizeze PostgreSQL ca sistem principal de gestiune a bazelor de date relaționale, într-o versiune aflată în suport activ și compatibilă cu mediul tehnic pus la dispoziție în MCloud.
SGBD 003		Utilizarea unui alt sistem de gestiune a bazelor de date relaționale va fi permisă numai în cazuri excepționale, justificate tehnic și economic, aprobate de ANSC și coordonate, după caz, cu AGE și STISC.
SGBD 004		Utilizarea tehnologiei .NET/ASP.NET Core și reutilizarea componentelor FOD/PDSE nu constituie, prin ele însele, o justificare pentru utilizarea Microsoft SQL Server. Contractantul trebuie să demonstreze existența unei incompatibilități tehnice reale cu PostgreSQL și să documenteze impactul alternativei asupra licențierii, costurilor, portabilității, operării și mentenanței.
SGBD 005		Sistemul trebuie să utilizeze o versiune PostgreSQL aflată în suport activ. Nu se admite utilizarea unor versiuni End-of-Life, fără actualizări de securitate sau fără suport pentru remedierea vulnerabilităților critice.
SGBD 006		Baza de date trebuie proiectată și configurată conform proprietăților ACID, asigurând atomicitatea, consistența, izolarea și durabilitatea tranzacțiilor aferente proceselor operaționale ale ANSC.
SGBD 007		Modelul relațional trebuie documentat complet și trebuie să includă cel puțin diagrame entitate-relație, scheme, tabele, câmpuri, tipuri de date, chei primare, chei externe, constrângeri, indecși, relații, vederi și celelalte obiecte relevante ale bazei de date.
SGBD 008		Modelul de date trebuie să reflecte în mod explicit obiectele informaționale ale SIMED, inclusiv contestații, dosare electronice, documente, părți procedurale, proceduri de achiziție, complete CSC, ședințe, sarcini, termene, notificări, documente procesuale și decizii.
SGBD 009		Modelul de date trebuie să fie normalizat corespunzător pentru evitarea duplicării și inconsistenței datelor. Denormalizarea va fi permisă numai în cazuri justificate prin cerințe de performanță sau raportare și va fi documentată în arhitectura datelor.
SGBD 010		Utilizarea câmpurilor JSON/JSONB va fi permisă pentru date semistructurate și extensibile, numai atunci când această abordare este justificată. JSON/JSONB nu va substitui nejustificat modelarea relațională a entităților și relațiilor principale ale SIMED.

ID	Obligativitate	Descriere
SGBD 011		Sistemul trebuie să utilizeze mecanisme de indexare optimizate pentru interogările frecvente, filtrele, căutările, rapoartele și operațiunile critice de business, evitând totodată crearea excesivă a indecșilor.
SGBD 012		Contractantul trebuie să analizeze și să optimizeze interogările SQL și planurile de execuție, astfel încât creșterea volumului de date să nu determine degradarea necontrolată a performanței.
SGBD 013		Modificările asupra schemei bazei de date trebuie realizate prin scripturi sau migrații versionate, incrementale, automatizate și reproductibile, păstrate în repozitoriul Git al proiectului.
SGBD 014		Crearea, modificarea sau eliminarea tabelelor, coloanelor, constrângerilor, indecșilor, funcțiilor, vederilor și a altor obiecte ale bazei de date nu se va realiza prin intervenții manuale necontrolate în mediile de preproducție și producție.
SGBD 015		Migrațiile bazei de date trebuie integrate în procesul CI/CD și trebuie să permită verificarea versiunii curente a schemei, aplicarea controlată a modificărilor și, acolo unde este posibil, rollback-ul sau downgrade-ul sigur.
SGBD 016		Modificările de schemă trebuie corelate cu versiunea aplicației și a API-urilor, astfel încât să nu apară incompatibilități între codul aplicației, structura bazei de date și datele existente.
SGBD 017		Sistemul trebuie să permită separarea logică, inclusiv prin scheme distincte unde este justificat, a datelor operaționale, datelor de referință, datelor de audit, datelor temporare și datelor utilizate pentru raportare.
SGBD 018		Sistemul trebuie să asigure integritatea referențială prin chei externe, constrângeri de unicitate, reguli de validare și alte mecanisme aplicabile modelului relațional.
SGBD 019		Regulile critice privind integritatea și consistența datelor trebuie validate atât la nivelul aplicației, cât și la nivelul bazei de date, acolo unde natura regulii permite acest lucru.
SGBD 020		Sistemul trebuie să prevină pierderea, duplicarea sau coruperea datelor în scenarii de acces simultan, prin tranzacții, control al concurenței, mecanisme de blocare și/sau versionare optimistă.
SGBD 021		Baza de date trebuie să utilizeze un model de acces bazat pe roluri și principiul privilegiilor minime. Drepturile vor fi acordate numai conturilor și serviciilor care au nevoie de acestea pentru îndeplinirea funcțiilor aprobate.
SGBD 022		Aplicația nu va utiliza conturi administrative generale pentru operațiunile curente. Vor fi create conturi tehnice distincte pentru aplicații, servicii, procese automate, raportare, migrare și activități administrative.
SGBD 023		Conturile tehnice nu vor fi partajate între componente fără justificare. Fiecare cont trebuie să permită identificarea serviciului sau procesului care îl utilizează și revocarea independentă a accesului.
SGBD 024		Conexiunile dintre componentele aplicației și serverul PostgreSQL trebuie securizate prin protocoale criptate și configurații aprobate pentru mediul MCloud. Conexiunile necriptate nu vor fi permise în mediile de preproducție și producție.

ID	Obligativitate	Descriere
SGBD 026		Parolele, certificatele, cheile și șirurile de conexiune aferente bazei de date trebuie externalizate și păstrate în mecanisme securizate de gestionare a secretelor. Acestea nu vor fi incluse în codul sursă, imagini de containere sau fișiere de configurare publice.
SGBD 027		Sistemul trebuie să permită monitorizarea bazei de date, inclusiv a utilizării CPU, memoriei, spațiului de stocare, conexiunilor active, timpilor de răspuns, blocajelor, deadlock-urilor, interogărilor lente, replicării și erorilor SQL.
SGBD 028		Sistemul trebuie să permită identificarea și investigarea interogărilor lente, blocajelor, deadlock-urilor, consumului excesiv de resurse și degradării planurilor de execuție.
SGBD 029		Parametrii operaționali PostgreSQL trebuie configurați în funcție de volumul estimat de date, numărul utilizatorilor simultani, frecvența tranzacțiilor, resursele disponibile și cerințele de performanță aprobate. Configurația va fi documentată și coordonată cu STISC.
SGBD 030		Pentru datele sensibile se vor aplica mecanisme de criptare adecvate, inclusiv criptare la nivelul infrastructurii de stocare și, atunci când clasificarea datelor o impune, criptare la nivelul aplicației sau al câmpurilor. Cheile de criptare vor fi administrate separat de baza de date.
SGBD 031		Fișierele, documentele electronice, imaginile și atașamentele nu vor fi stocate direct în baza de date relațională. Acestea vor fi gestionate într-un sistem dedicat de stocare de obiecte, iar PostgreSQL va păstra metadatele, identificatorii, amprentele digitale și referințele necesare.
SGBD 031		Mecanismul de acces la date trebuie să fie compatibil cu stiva .NET/ASP.NET Core și PostgreSQL. Se poate utiliza Entity Framework Core cu furnizorul PostgreSQL suportat activ, un query builder sau un alt mecanism aprobat în arhitectura tehnică.
SGBD 033		Utilizarea unui ORM nu trebuie să împiedice optimizarea interogărilor critice, utilizarea SQL parametrizat, gestionarea eficientă a tranzacțiilor, folosirea funcționalităților PostgreSQL și aplicarea regulilor de integritate la nivelul bazei de date.
SGBD 034		Interogările SQL construite dinamic trebuie parametrizate și protejate împotriva atacurilor de tip SQL Injection. Concatenarea necontrolată a valorilor introduse de utilizatori în instrucțiuni SQL nu este permisă.
SGBD 035		Sistemul trebuie să permită exportul controlat al datelor în formate standardizate pentru raportare, audit, migrare și analiză, în conformitate cu rolurile utilizatorilor, clasificarea datelor și regulile privind protecția informațiilor.
SGBD 036		Contractantul trebuie să elaboreze proceduri de mentenanță PostgreSQL care să includă, după caz, operațiuni VACUUM, ANALYZE, REINDEX, actualizarea statisticilor, verificarea integrității, monitorizarea spațiului și gestionarea tabelelor cu creștere accelerată.
SGBD 037		Activitățile de mentenanță trebuie planificate și automatizate astfel încât impactul asupra utilizatorilor și proceselor operaționale ale ANSC să fie minim și să nu afecteze integritatea tranzacțiilor în curs.

ID	Obligativitate	Descriere
SGBD 038		Arhitectura bazei de date trebuie să permită extinderea controlată a resurselor de procesare, memorie și stocare și, dacă este justificat, utilizarea replicilor de citire sau a altor mecanisme de scalare compatibile cu MCloud.
SGBD 039		Baza de date trebuie să fie compatibilă cu mecanismele aprobate de backup, restaurare și recuperare la un moment determinat, în conformitate cu obiectivele RPO și RTO stabilite pentru SIMED. Procedurile de restaurare vor fi testate periodic.
SGBD 040		Mediile de dezvoltare, testare, preproducție, instruire și producție trebuie să utilizeze instanțe sau baze de date separate și configurații controlate. Accesul și transferul datelor între medii vor fi restricționate și jurnalizate.
SGBD 041		Datele reale de producție nu vor fi utilizate în mediile de dezvoltare, testare sau instruire, cu excepția cazurilor expres autorizate. În mediile non-producție se vor utiliza date sintetice, anonimizate sau pseudonimizate.
SGBD 042		Contractantul trebuie să furnizeze și să mențină un dicționar de date actualizat, care să descrie entitățile, câmpurile, tipurile de date, valorile admise, sursele, clasificarea, regulile de validare, relațiile și semnificația funcțională a datelor.
SGBD 043		Orice abatere de la utilizarea PostgreSQL sau de la cerințele Stivei Tehnologice Guvernamentale privind sistemele de gestiune a bazelor de date trebuie justificată și aprobată înainte de implementare. Justificarea va include impactul asupra costurilor, licențierii, securității, portabilității, interoperabilității, mentenanței și operării în MCloud.

5.5.Cerințe privind infrastructura MCloud, virtualizarea, containerizarea și operarea cloud

SIMED va fi găzduit și operat în infrastructura guvernamentală MCloud, administrată de STISC. Soluția va respecta principiile cloud-native și container-first și va fi compatibilă cu OpenStack, Kubernetes și sistemele de operare Linux aprobate pentru MCloud.
Contractantul va proiecta, configura și documenta componentele aplicaționale, iar STISC va asigura resursele infrastructurale de bază, în limita responsabilităților și capacităților aprobate. Soluția nu va depinde de infrastructura, conturile sau serviciile externe controlate exclusiv de Dezvoltator.

ID	Descriere
CLOUD 001	SIMED trebuie să fie proiectat pentru găzduire, instalare și operare în Platforma tehnologică guvernamentală comună MCloud, administrată de STISC, în conformitate cu cerințele tehnice, de securitate și operaționale aplicabile sistemelor informaționale de stat.
CLOUD 002	Soluția trebuie să fie compatibilă cu serviciile și resursele disponibile în MCloud, inclusiv resurse de calcul, stocare, rețea, echilibrare a încărcării, monitorizare, backup și administrare operațională.
CLOUD 003	Arhitectura SIMED trebuie să respecte principiile cloud-native și container-first, astfel încât componentele aplicaționale să poată fi instalate, scalate, actualizate, restaurate și operate controlat în infrastructura guvernamentală.

ID	Descriere
CLOUD 004	Componentele aplicaționale ale SIMED trebuie să ruleze în containere compatibile cu mediul MCloud. Imaginile containerelor trebuie să fie reproductibile, versionate, minimizate și construite automat din codul sursă aflat în repozitoriul aprobat.
CLOUD 005	SIMED trebuie să fie compatibil cu Kubernetes ca nivel de orchestrare a aplicațiilor și cu instrumentele de administrare utilizate în MCloud, inclusiv Rancher sau OpenShift, în măsura în care acestea sunt puse la dispoziție de STISC.
CLOUD 006	Soluția trebuie să fie compatibilă cu OpenStack ca nivel de infrastructură și virtualizare sau cu alte tehnologii aprobate și utilizate în cadrul MCloud.
CLOUD 007	Componentele server trebuie să fie compatibile cu sisteme de operare Linux aprobate pentru MCloud, inclusiv familia Red Hat, Rocky Linux sau AlmaLinux și familia Debian sau Ubuntu LTS, conform mediului pus la dispoziție de STISC.
CLOUD 008	SIMED trebuie să utilizeze medii distincte pentru dezvoltare, testare, preproducție, instruire și producție. Fiecare mediu va fi configurat, securizat, administrat și validat separat.
CLOUD 009	Parametrii specifici fiecărui mediu, inclusiv endpoint-urile, variabilele de mediu, conexiunile, certificatele și setările operaționale, trebuie externalizați și gestionați fără modificarea codului sursă.
CLOUD 010	Contractantul trebuie să prezinte necesarul estimat de resurse pentru fiecare mediu, incluzând CPU, RAM, stocare, trafic de rețea, volume persistente, stocare de obiecte, componente middleware și marja necesară pentru creșterea încărcării.
CLOUD 011	Contractantul trebuie să elaboreze arhitectura infrastructurală a SIMED, indicând componentele, relațiile dintre acestea, fluxurile de comunicație, zonele de rețea, porturile, protocoalele, volumele de stocare și dependențele tehnice.
CLOUD 012	Contractantul trebuie să transmită ANSC și STISC cerințele tehnice necesare configurării MCloud, inclusiv necesarul de resurse, segmentele de rețea, regulile de acces, DNS, certificatele, mecanismele de load balancing, stocarea și serviciile auxiliare.
CLOUD 013	STISC va asigura, în limitele responsabilităților stabilite, configurarea și administrarea infrastructurii fizice, resurselor virtuale, rețelelor, segmentelor de securitate și serviciilor de bază MCloud, în baza cerințelor aprobate de ANSC.
CLOUD 014	Contractantul va configura și instala componentele aplicaționale, containerele, serviciile middleware, conexiunile, parametrii și celelalte elemente necesare funcționării SIMED în infrastructura pusă la dispoziție de STISC.
CLOUD 015	Arhitectura trebuie să permită scalarea independentă a componentelor aplicaționale în funcție de încărcare, consumul de resurse și limitele infrastructurii aprobate.
CLOUD 016	SIMED trebuie să permită implementarea mecanismelor de disponibilitate ridicată, redundanță, load balancing, failover și reluare operațională pentru componentele critice, în măsura permisă de infrastructura MCloud și de nivelurile de serviciu aprobate.
CLOUD 017	Componentele aplicaționale trebuie să permită utilizarea mecanismelor de autoscaling și self-healing, atunci când acestea sunt susținute de platforma de orchestrare și sunt aprobate de ANSC și STISC.
CLOUD 018	SIMED trebuie să utilizeze mecanisme de stocare persistentă și stocare de obiecte compatibile cu MCloud. Volumele persistente, clasele de stocare, politicile de retenție și drepturile de acces trebuie documentate.

ID	Descriere
CLOUD 019	Soluția nu trebuie să depindă de infrastructuri externe neaprobate, servicii cloud publice neautorizate, conturi ale Contractantului sau componente care nu pot fi instalate și operate în MCloud.
CLOUD 020	SIMED trebuie să poată fi instalat și operat integral în MCloud, fără obligația utilizării unor servicii SaaS, PaaS sau IaaS externe, cu excepția serviciilor aprobate expres de ANSC, AGE și STISC.
CLOUD 021	Contractantul trebuie să verifice și să demonstreze compatibilitatea tuturor componentelor software și middleware cu politicile, restricțiile și procedurile operaționale ale MCloud înainte de instalarea în producție.
CLOUD 022	Contractantul trebuie să participe la configurarea, instalarea, integrarea, testarea și validarea SIMED în mediile furnizate de STISC până la finalizarea recepției tehnice și finale.
CLOUD 023	Instalarea SIMED trebuie să fie automatizată, reproductibilă și realizată pe baza codului sursă, imaginilor, manifestelor, configurațiilor și artefactelor versionate. Copierea manuală necontrolată a fișierelor în mediile de preproducție și producție nu este permisă.
CLOUD 024	Configurarea infrastructurii și a componentelor operaționale trebuie realizată, după caz, prin mecanisme declarative și automatizate, utilizând Ansible, OpenTofu sau alte instrumente aprobate și compatibile cu MCloud.
CLOUD 025	Contractantul trebuie să livreze toate fișierele necesare instalării și operării, inclusiv Dockerfile-uri, manifeste Kubernetes, configurații Helm sau echivalente, scripturi de instalare, definiții de infrastructură și parametri configurați pe medii.
CLOUD 026	SIMED trebuie să se integreze cu mecanismele de monitorizare, colectare a logurilor, alertare și observabilitate disponibile în infrastructura guvernamentală, conform cerințelor ANSC și STISC.
CLOUD 027	Fiecare componentă critică trebuie să includă mecanisme de health check, readiness check și, după caz, startup check, pentru verificarea stării aplicației, conexiunilor, serviciilor și dependențelor tehnice.
CLOUD 028	Resursele, configurațiile, datele secrete și drepturile de acces trebuie administrate separat pentru fiecare mediu, astfel încât modificările efectuate într-un mediu să nu afecteze necontrolat celelalte medii.
CLOUD 029	Mediile non-producție trebuie izolate logic și operațional de mediul de producție. Nu se admite utilizarea comună necontrolată a bazelor de date, conturilor tehnice, secretelor, certificatelor sau volumelor de stocare.
CLOUD 030	SIMED trebuie să permită reconstruirea, reinstalarea sau migrarea unui mediu în MCloud pe baza configurațiilor, artefactelor și procedurilor predate, fără dependență de echipamentele sau configurațiile locale ale Contractantului.
CLOUD 031	Contractantul trebuie să documenteze toate dependențele infrastructurale, inclusiv baze de date, brokeri de mesaje, cache, stocare de obiecte, servicii de căutare, DNS, certificate, load balancing, rețele și mecanisme de monitorizare.
CLOUD 032	Contractantul trebuie să elaboreze proceduri complete de instalare, configurare, actualizare, rollback, verificare și depanare, astfel încât operațiunile să poată fi executate de personalul autorizat al ANSC sau STISC.
CLOUD 033	Compatibilitatea SIMED cu MCloud trebuie verificată înainte de lansarea în producție prin instalarea în mediile non-producție, executarea testelor tehnice și confirmarea funcționării componentelor și integrărilor critice.

ID	Descriere
CLOUD 034	Contractantul trebuie să declare toate limitările tehnice, cerințele minime și dependențele care pot influența performanța, disponibilitatea, scalarea, backup-ul, restaurarea sau operarea SIMED în MCloud.
CLOUD 035	Configurațiile infrastructurale și aplicaționale trebuie să poată fi adaptate la resursele efectiv puse la dispoziție de STISC, fără modificarea nejustificată a arhitecturii funcționale sau rescrierea componentelor principale.
CLOUD 036	Toate componentele instalate în MCloud trebuie să fie declarate, documentate și incluse în inventarul tehnic al sistemului. Nu se admit servicii ascunse, componente nedeclarate, procese neautorizate sau comunicații externe neaprobate.
CLOUD 037	SIMED trebuie să poată fi operat, administrat, actualizat și menținut pe termen lung de ANSC și/sau STISC, fără dependență critică de infrastructura locală a Contractantului, conturile acestuia, servicii comerciale neaprobate sau proceduri manuale nedocumentate.

5.6. Cerințe privind DevSecOps, CI/CD și livrarea reproductibilă

Dezvoltarea, testarea și livrarea SIMED vor fi realizate prin practici DevSecOps și procese CI/CD automatizate, documentate și controlate. Pipeline-urile, configurațiile, testele, scripturile și artefactele de livrare vor fi predate ANSC și vor putea fi operate în infrastructura aprobată, fără dependență critică față de Contractant.
Procesele de livrare vor ține cont de reutilizarea componentelor FOD/PDSE, de stiva .NET și de responsabilitățile ANSC, AGE și STISC privind aprobarea, găzduirea și operarea soluției.

ID	Descriere
DEVOPS 001	Dezvoltarea și livrarea SIMED trebuie să fie organizate conform principiilor DevSecOps, prin integrarea cerințelor de securitate, calitate, testare, trasabilitate și automatizare pe întregul ciclu de viață al sistemului.
DEVOPS 002	Codul sursă, configurațiile, scripturile, testele, documentația tehnică și definițiile proceselor de livrare trebuie gestionate prin Git.
DEVOPS 003	Codul sursă și toate livrabilele tehnice trebuie păstrate în repozitoriul indicat de ANSC sau de autoritatea competentă. Livrarea exclusiv prin arhive, e-mail, suporturi fizice sau repozitorii controlate de Contractant nu este permisă.
DEVOPS 004	Platforma CI/CD trebuie să fie compatibilă cu infrastructura guvernamentală. Se va utiliza Gitea cu Gitea Runner ca opțiune principală sau GitLab Community Edition ca alternativă, în funcție de instrumentele puse la dispoziție în MCloud.
DEVOPS 005	Pipeline-ul CI/CD nu trebuie să depindă de conturi personale, abonamente, runner-e, registre de artefacte sau servicii cloud aflate exclusiv sub controlul Contractantului.
DEVOPS 006	Contractantul trebuie să definească și să documenteze strategia de gestionare a ramurilor, versiunilor, cererilor de integrare, release-urilor și remedierilor urgente.
DEVOPS 007	Ramurile principale și ramurile utilizate pentru livrări trebuie protejate împotriva modificărilor directe neautorizate. Integrarea codului se va realiza prin cereri de integrare și revizuire de cod.

ID	Descriere
DEVOPS 008	Modificările codului sursă trebuie revizuite de cel puțin o altă persoană autorizată înainte de integrarea în ramura principală, cu excepția situațiilor urgente aprobate și documentate.
DEVOPS 009	Fiecare modificare a codului trebuie să poată fi corelată cu o cerință, sarcină, incident, neconformitate sau solicitare de modificare aprobată.
DEVOPS 010	Componentele FOD/PDSE reutilizate, configurațiile specifice SIMED și extensiile dezvoltate pentru ANSC trebuie evidențiate și versionate distinct, astfel încât să poată fi identificate modificările realizate asupra fiecărei categorii de componente.
DEVOPS 011	Modificarea componentelor comune FOD/PDSE nu va fi realizată fără analiza impactului și coordonarea cu ANSC și AGE, conform responsabilităților și procedurilor aplicabile.
DEVOPS 012	Pentru toate componentele SIMED trebuie configurate pipeline-uri automatizate de compilare, testare, verificare, construire a artefactelor, publicare și implementare.
DEVOPS 013	Pipeline-ul CI/CD trebuie să includă, după caz, cel puțin următoarele etape: preluarea codului, restaurarea dependențelor, compilare, teste automate, analiză statică, verificarea dependențelor, generarea SBOM, construirea imaginilor, scanarea artefactelor, publicarea, instalarea și verificările post-deploy.
DEVOPS 014	Compilarea componentelor .NET trebuie realizată utilizând versiuni LTS aprobate ale SDK-ului și runtime-ului .NET, compatibile cu platforma FOD/PDSE și cu stiva tehnologică SIMED.
DEVOPS 015	Procesul de compilare trebuie să fie automatizat și reproductibil, astfel încât același cod sursă, aceleași dependențe și aceleași configurații să genereze artefacte echivalente.
DEVOPS 016	Toate dependențele software trebuie declarate explicit și gestionate prin managerii de pachete corespunzători. Versiunile nespecificate, instabile sau preluate din surse nedeclarate nu sunt permise.
DEVOPS 017	Contractantul trebuie să utilizeze fișiere de blocare a versiunilor sau mecanisme echivalente, acolo unde ecosistemul tehnologic le permite, pentru reproducerea exactă a dependențelor utilizate la fiecare livrare.
DEVOPS 018	Fiecare artefact software trebuie să fie versionat și corelat cu versiunea codului sursă, commit-ul, pipeline-ul, configurația, rezultatele testelor și inventarul componentelor software.
DEVOPS 019	Imaginile de containere și celelalte artefacte aprobate trebuie publicate într-un registru controlat de ANSC, STISC sau de autoritatea tehnică desemnată.
DEVOPS 020	Artefactele publicate nu vor fi suprascrise. Orice modificare va genera o versiune nouă, identificabilă și trasabilă.
DEVOPS 021	Contractantul trebuie să genereze și să actualizeze un inventar SBOM pentru fiecare livrare semnificativă, incluzând componentele, dependențele directe și tranzitive, versiunile, licențele și proveniența acestora.
DEVOPS 022	Pipeline-ul trebuie să verifice automat licențele componentelor terțe și să semnaleze dependențele cu licențe neaprobate, restrictive sau incompatibile cu cerințele SIMED.
DEVOPS 023	Pipeline-ul trebuie să includă analiza statică a codului sursă pentru identificarea defectelor, vulnerabilităților, practicilor nesigure și neconformităților de calitate.
DEVOPS 024	Dependențele software trebuie scanate automat pentru vulnerabilități cunoscute, versiuni retrase, componente End-of-Life și riscuri aferente lanțului de aprovizionare software.

ID	Descriere
DEVOPS 025	Imaginile de containere trebuie scanate automat înainte de publicare și înainte de promovarea către mediile de preproducție și producție.
DEVOPS 026	Pentru interfețele și serviciile expuse public trebuie efectuate teste dinamice de securitate în mediile non-producție, înainte de lansarea în producție și după modificările majore.
DEVOPS 027	Vulnerabilitățile critice și majore, testele obligatorii eșuate și neconformitățile de securitate care afectează funcționarea sistemului trebuie să blocheze automat promovarea livrării către etapa următoare.
DEVOPS 028	Acceptarea temporară a unei vulnerabilități sau neconformități trebuie justificată, aprobată de ANSC, limitată în timp și însoțită de măsuri compensatorii și termen de remediere.
DEVOPS 029	Pipeline-ul trebuie să execute automat testele unitare aferente logicii de business. Pentru logica de business critică a SIMED se va asigura o acoperire de minimum 80%, dacă planul de testare aprobat nu stabilește un prag superior.
DEVOPS 030	Testele unitare trebuie să acopere în special regulile privind înregistrarea contestațiilor, termenele procedurale, repartizarea dosarelor, statuturile, validarea documentelor și emiterea deciziilor.
DEVOPS 031	Pipeline-ul trebuie să execute teste de integrare pentru bazele de date, API-uri, mesagerie, Front Office–Back Office, FOD/PDSE și serviciile guvernamentale integrate.
DEVOPS 032	Trebuie implementate teste funcționale sau end-to-end pentru fluxurile critice ale ANSC, inclusiv depunerea contestației, înregistrarea documentelor, repartizarea, examinarea, ședința, elaborarea și comunicarea deciziei.
DEVOPS 033	Procesul de livrare trebuie să includă teste de regresie pentru a confirma că modificările nu afectează funcționalitățile existente și componentele FOD/PDSE reutilizate.
DEVOPS 034	Testele de performanță și încărcare trebuie executate înainte de lansarea în producție și după modificările care pot afecta capacitatea, scalabilitatea sau timpii de răspuns.
DEVOPS 035	Rezultatele testelor, acoperirea codului, scanările de securitate și celelalte verificări automate trebuie păstrate ca dovezi de conformitate și incluse în dosarul de acceptanță al livrării.
DEVOPS 036	Configurațiile trebuie separate de codul sursă și administrate distinct pentru mediile de dezvoltare, testare, preproducție, instruire și producție.
DEVOPS 037	Parolele, cheile, certificatele, tokenurile și celelalte date secrete nu vor fi stocate în cod, imagini de containere, scripturi sau fișiere de configurare neprotejate.
DEVOPS 038	Datele secrete trebuie gestionate prin mecanisme securizate aprobate pentru infrastructura MCloud și trebuie injectate în componente numai la momentul execuției.
DEVOPS 039	Conturile tehnice utilizate de pipeline-uri și runner-e trebuie să respecte principiul privilegiilor minime și să aibă drepturi distincte pentru fiecare mediu.
DEVOPS 040	Mediul de producție nu trebuie să fie accesibil direct din mediile de dezvoltare și nici prin conturile personale sau infrastructura locală a Contractantului.
DEVOPS 041	Același artefact aprobat trebuie promovat succesiv între mediile de testare, preproducție și producție. Recompilarea necontrolată a codului separat pentru fiecare mediu nu este permisă.
DEVOPS 042	Promovarea unei versiuni în producție trebuie să necesite aprobarea explicită a persoanelor autorizate de ANSC și, după caz, validarea tehnică a STISC.

ID	Descriere
DEVOPS 043	Pipeline-ul trebuie să permită livrarea etapizată și independentă a componentelor SIMED, fără afectarea nejustificată a celorlalte module sau servicii operaționale.
DEVOPS 044	Implementarea în mediile de preproducție și producție trebuie realizată automatizat. Copierea manuală de fișiere, executarea scripturilor locale nedocumentate sau configurarea directă necontrolată nu sunt permise.
DEVOPS 045	Modificările schemei bazei de date trebuie realizate prin migrații versionate, testate și integrate în pipeline-ul de livrare.
DEVOPS 046	Migrațiile bazei de date trebuie proiectate, în măsura posibilului, astfel încât să fie compatibile cu versiunea precedentă a aplicației pe durata procesului de actualizare.
DEVOPS 047	Procesul de livrare trebuie să includă o procedură documentată de rollback pentru aplicație, configurații și, în limitele tehnic posibile, pentru modificările bazei de date.
DEVOPS 048	Înainte de instalarea unei versiuni în producție trebuie verificată existența backup-urilor, capacitatea de restaurare și condițiile necesare revenirii la versiunea precedentă.
DEVOPS 049	După fiecare deploy trebuie executate automat verificări privind disponibilitatea componentelor, conectivitatea, migrațiile bazei de date, integrarea cu serviciile externe și funcționarea fluxurilor critice.
DEVOPS 050	Componentele trebuie să furnizeze health check, readiness check și, după caz, startup check, utilizabile de platforma de orchestrare și de procesul de verificare post-deploy.
DEVOPS 051	Eșecul verificărilor post-deploy trebuie să determine oprirea promovării, inițierea procedurii de rollback sau intervenția controlată a persoanelor autorizate.
DEVOPS 052	Pipeline-ul trebuie să păstreze jurnalul execuțiilor, identitatea persoanelor care au inițiat și aprobat livrarea, etapele executate, artefactele utilizate, rezultatele și eventualele erori.
DEVOPS 053	Pentru fiecare versiune livrată, Contractantul trebuie să furnizeze note de versiune care să includă funcționalitățile noi, modificările, defectele remediate, migrațiile, incompatibilitățile cunoscute și instrucțiunile operaționale.
DEVOPS 054	Contractantul trebuie să documenteze procedura de remediere urgentă a incidentelor și vulnerabilităților, inclusiv regulile de creare, testare, aprobare, livrare și integrare ulterioară a remedierilor în ramura principală.
DEVOPS 055	Modificarea directă a codului, configurațiilor sau bazei de date în mediul de producție este interzisă, cu excepția intervențiilor urgente aprobate, documentate, jurnalizate și reflectate ulterior în repozitoriu.
DEVOPS 056	Contractantul trebuie să livreze ANSC toate pipeline-urile, fișierele de build, Dockerfile-urile, manifestele, scripturile de migrare, testele, configurațiile și documentația necesară operării procesului CI/CD.
DEVOPS 057	Documentația procesului CI/CD trebuie să descrie etapele pipeline-ului, regulile de promovare, responsabilitățile, mecanismele de securitate, gestionarea secretelor, structura artefactelor, rollback-ul și tratarea eșecurilor.
DEVOPS 058	Contractantul trebuie să asigure instruirea personalului desemnat de ANSC și/sau STISC privind utilizarea, administrarea, monitorizarea și modificarea controlată a pipeline-urilor.

ID	Descriere
DEVOPS 059	Pipeline-urile și instrumentele livrate trebuie să permită operarea și dezvoltarea ulterioară a SIMED de către ANSC, STISC sau un alt furnizor desemnat, fără intervenția obligatorie a Contractantului inițial.
DEVOPS 060	La recepția finală, Contractantul trebuie să demonstreze printr-un test de deploy independent că SIMED poate fi compilat, testat, instalat și verificat într-un mediu nou pe baza codului, configurațiilor, artefactelor și documentației predate.
DEVOPS 061	Orice fișier, configurație, dependență sau intervenție manuală disponibilă exclusiv pe echipamentele ori în conturile Contractantului și necesară livrării SIMED va constitui neconformitate la recepție.
DEVOPS 062	Dosarul de acceptanță al fiecărei versiuni majore trebuie să includă cel puțin referința la codul sursă, versiunea artefactelor, SBOM, rezultatele testelor, rezultatele scanărilor, notele de versiune, dovada instalării și lista neconformităților.
DEVOPS 063	Contractantul trebuie să mențină pipeline-urile, testele și configurațiile actualizate pe întreaga perioadă de implementare, garanție și mentenanță, în corelare cu evoluția codului și a infrastructurii SIMED.
DEVOPS 064	Utilizarea instrumentelor de inteligență artificială pentru generarea codului este permisă numai dacă rezultatul respectă aceleași cerințe de securitate, licențiere, revizuire, testare și trasabilitate aplicabile codului scris manual. Contractantul rămâne integral responsabil pentru codul livrat.

5.7. Cerințe privind interoperabilitatea sistemului IT

Interoperabilitatea SIMED reprezintă capacitatea sistemului de a comunica, schimba, valida și procesa date și documente împreună cu platformele guvernamentale, registrele de stat și celelalte sisteme informaționale relevante, prin mecanisme securizate, standardizate, documentate și auditabile.

SIMED va fi proiectat conform principiilor API-first, specification-first, reuse-before-build și loose coupling, astfel încât componentele sale și sistemele externe să poată evolua independent, fără dependențe tehnice rigide și fără acces direct necontrolat la bazele de date.

Schimbul de date cu registrele, platformele și sistemele informaționale deținute de autorități și instituții publice se va realiza, cu prioritate obligatorie, prin Platforma de interoperabilitate MConnect. Conexiunile directe între SIMED și alte sisteme vor fi permise numai atunci când serviciile necesare nu sunt disponibile prin MConnect și numai în baza unei justificări tehnice și juridice documentate, aprobate de ANSC și coordonate cu AGE și cu posesorul sistemului extern, după caz.

Pentru scenariile care presupun notificarea sistemelor despre producerea unor evenimente, modificarea statutului unui dosar, emiterea unei decizii sau actualizarea unor entități informaționale, se va utiliza, după caz, componenta de evenimente MConnect. SIMED va putea avea rol de producător, consumator sau ambele, în funcție de fluxurile aprobate.

Integrarea Front Office-ului bazat pe FOD/PDSE cu Back Office-ul SIMED se va realiza exclusiv prin API-uri securizate, documentate și versionate și, pentru procesele asincrone, prin mesaje și evenimente. Front Office-ul nu va accesa direct bazele de date, sistemele de stocare sau serviciile interne ale Back Office-ului.

Tabelul 5.4. Cerințe privind interoperabilitatea sistemului IT

ID	Obligativitate	Cerință/Descriere
INT 001	M	SIMED trebuie să fie proiectat conform principiilor API-first și specification-first. Contractele API și modelele de date aferente vor fi definite, documentate și aprobate înaintea implementării funcționalităților de integrare.
INT 002	M	API-urile publice și API-urile utilizate pentru integrarea dintre Front Office și Back Office trebuie să utilizeze REST, HTTPS și JSON și să fie documentate conform OpenAPI 3.1. XML și SOAP vor fi utilizate numai atunci când sunt impuse de un sistem extern sau de un serviciu guvernamental existent.
INT 003	M	Comunicarea internă dintre servicii poate utiliza gRPC cu Protocol Buffers atunci când această soluție este justificată de cerințele de performanță, tipizare sau comunicare internă. gRPC nu va înlocui API-urile REST destinate integrării externe.
INT 004	M	Schimbul de date cu registrele, platformele și sistemele informaționale de stat trebuie realizat prin MConnect. Conexiunile directe între sisteme sunt permise numai în cazuri justificate, documentate și aprobate conform procedurilor aplicabile.
INT 005	M	Pentru schimburile bazate pe evenimente, SIMED trebuie să utilizeze, după caz, componenta MConnect Events, documentând rolul de producător și/sau consumator, structura evenimentului, condițiile de publicare, confirmarea procesării și mecanismele de reluare.
INT 006	M	Integrarea dintre Front Office-ul bazat pe FOD/PDSE și Back Office-ul SIMED se va realiza exclusiv prin API-uri și mesaje securizate. Front Office-ul nu va avea acces direct la bazele de date, sistemele de fișiere sau alte resurse interne ale Back Office-ului.
INT 007	M	API-urile Back Office trebuie să permită, în limitele drepturilor acordate, transmiterea contestațiilor și documentelor, consultarea statutului dosarelor, preluarea solicitărilor ANSC, transmiterea completărilor, consultarea ședințelor și accesarea deciziilor și comunicărilor.
INT 008	M	Interfețele trebuie să fie slab cuplate și să permită evoluția independentă a sistemelor integrate. Modelele interne ale bazei de date nu vor fi expuse direct ca modele API, iar sistemele externe nu vor depinde de structura internă a tabelelor SIMED.
INT 009	M	Pentru procesele asincrone, SIMED trebuie să utilizeze mecanisme fiabile de mesagerie compatibile cu Stiva Tehnologică Guvernamentală, inclusiv RabbitMQ și, pentru fluxuri distribuite de evenimente cu volum ridicat, Apache Kafka, dacă utilizarea este justificată prin arhitectura aprobată.
INT 010	M	Mesajele și operațiunile asincrone trebuie să includă identificatori unici de corelare și mecanisme pentru prevenirea procesării duplicate, confirmarea procesării, reluarea controlată a operațiunilor și gestionarea mesajelor care nu pot fi procesate.
INT 011	M	Operațiunile de integrare care creează sau modifică date trebuie proiectate, în măsura posibilului, ca operațiuni idempotente, astfel încât repetarea aceleiași solicitări să nu genereze înregistrări sau efecte duplicate.
INT 012	M	Toate API-urile expuse și consumate trebuie să fie versionate. Modificările incompatibile trebuie introduse prin versiuni noi, cu o perioadă documentată de tranziție și cu menținerea compatibilității pentru sistemele consumatoare, conform politicii aprobate.

ID	Obligativitate	Cerință/Descriere
INT 013	M	Documentația API trebuie să includă cel puțin descrierea operațiunilor, endpoint-urile, parametrii, modelele de date, câmpurile obligatorii, codurile de răspuns, codurile de eroare, exemplele de cereri și răspunsuri, mecanismele de autentificare și autorizare și politica de versionare.
INT 014	M	Documentația API trebuie să fie disponibilă atât într-un format citibil de mașină, conform OpenAPI 3.1, cât și printr-o interfață destinată utilizatorilor tehnici, de tip Swagger UI sau instrument echivalent aprobat.
INT 015	M	Autentificarea utilizatorilor SIMED trebuie realizată exclusiv prin MPass, potrivit documentației oficiale de integrare. Sistemul nu va implementa baze locale de parole sau mecanisme paralele de autentificare pentru utilizatorii care trebuie autentificați prin MPass.
INT 016	M	Autentificarea și autorizarea tehnică dintre SIMED și sistemele externe se vor realiza conform documentației oficiale a platformei integrate, utilizând certificate, tokenuri, semnarea mesajelor sau alte mecanisme aprobate. Mecanismele de autentificare tehnică nu vor fi confundate cu autentificarea utilizatorilor prin MPass.
INT 017	M	SIMED trebuie să integreze MSign pentru aplicarea și verificarea semnăturilor electronice asupra contestațiilor, punctelor de vedere, documentelor procesuale, proceselor-verbale, deciziilor și altor documente pentru care semnarea este obligatorie.
INT 018	M	SIMED trebuie să integreze MPower pentru verificarea dreptului unei persoane de a acționa în numele unei persoane fizice sau juridice, atunci când fluxul presupune reprezentare. MPower nu va înlocui modelul intern de roluri și drepturi al SIMED.
INT 019	M	SIMED trebuie să integreze MNotify pentru transmiterea notificărilor către contestatari, autorități contractante, operatori economici și utilizatori interni, conform evenimentelor și șabloanelor aprobate de ANSC.
INT 020	M	Evenimentele semnificative din punct de vedere juridic, operațional și de securitate trebuie transmise către MLog, inclusiv accesarea datelor cu caracter personal, modificarea datelor critice, semnarea documentelor, emiterea deciziilor și alte evenimente stabilite împreună cu AGE.
INT 021	M	Integrarea cu MLog nu exclude jurnalizarea locală. SIMED trebuie să păstreze loguri locale structurate, corelate și suficiente pentru monitorizare, depanare și investigarea incidentelor, fără expunerea nejustificată a datelor cu caracter personal.
INT 022	D	SIMED trebuie să permită integrarea cu MDocs pentru păstrarea, partajarea și accesarea securizată a documentelor electronice, dacă analiza arhitecturală și funcțională confirmă aplicabilitatea serviciului pentru dosarele și documentele ANSC.
INT 023	D	SIMED trebuie să permită integrarea cu MPay numai dacă legislația și fluxurile aprobate prevăd efectuarea unei plăți. Integrarea va asigura generarea solicitării, identificarea tranzacției, verificarea statutului și asocierea plății cu contestația.
INT 024	D	SIMED trebuie să permită integrarea cu MDelivery numai pentru scenariile de livrare fizică a documentelor sau rezultatelor pe suport de hârtie, dacă această funcționalitate este aplicabilă proceselor ANSC.

ID	Obligativitate	Cerință/Descriere
INT 025	M	SIMED trebuie să se integreze cu SIA RSAP/MTender pentru preluarea și sincronizarea datelor relevante privind procedurile de achiziție, autoritățile contractante, operatorii economici, loturile, obiectele achiziției, statuturile și rezultatele procedurii.
INT 026	M	Integrarea cu SIA RSAP/MTender se va realiza prin serviciile publicate în MConnect sau prin interfețele oficiale puse la dispoziție de posesorul sistemului. O conexiune directă va fi utilizată numai dacă serviciul necesar nu este disponibil prin MConnect și există aprobările necesare.
INT 027	M	Contractantul nu va presupune existența unor endpoint-uri, câmpuri, webhook-uri sau operațiuni MTender care nu sunt confirmate prin documentația oficială. Specificația integrării va fi coordonată cu ANSC, Ministerul Finanțelor și posesorul sau administratorul tehnic al SIA RSAP/MTender.
INT 028	M	Pentru fiecare integrare, Contractantul trebuie să elaboreze o matrice de schimb de date care să includă sistemul furnizor, sistemul consumator, scopul schimbului, temeiul juridic, entitățile și câmpurile transmise, frecvența, direcția, responsabilitățile, perioada de păstrare și regulile de actualizare.
INT 029	M	Modelele de date, clasificatoarele, nomenclatoarele, identificatorii și celelalte active semantice utilizate în schimburile informaționale trebuie documentate, versionate și corelate cu activele semantice guvernamentale aplicabile.
INT 030	M	Datele preluate din alte sisteme trebuie validate din punct de vedere structural, semantic și al integrității înainte de procesare. Sistemul va respinge sau izola mesajele neconforme și va păstra informațiile necesare investigării erorilor.
INT 031	M	SIMED trebuie să aplice principiul minimizării datelor. Prin integrări vor fi solicitate și transmise numai datele strict necesare realizării fluxului procedural și pentru care există temei juridic și drept de acces.
INT 032	M	Toate schimburile de date trebuie realizate prin canale criptate, utilizând protocoale și configurații de securitate aflate în suport activ și aprobate pentru infrastructura guvernamentală.
INT 033	M	Sistemul trebuie să asigure trasabilitatea schimburilor informaționale prin înregistrarea cel puțin a identificatorului de corelare, sistemului sursă și destinație, operațiunii, datei și orei, rezultatului, codului de răspuns și duratei procesării.
INT 034	M	Jurnalele integrărilor nu vor stoca integral parole, tokenuri, chei, certificate private, documente, date personale sau conținut sensibil. Datele necesare depanării vor fi mascate, pseudonimizate sau limitate corespunzător.
INT 035	M	Sistemul trebuie să permită configurarea profilurilor de integrare pentru fiecare sistem extern, incluzând endpoint-urile, certificatele, politicile de securitate, timeout-urile, limitele de utilizare, mecanismele de retry și parametrii specifici mediilor.
INT 036	M	Configurațiile integrărilor și adresele serviciilor externe trebuie externalizate și administrate separat pentru mediile de dezvoltare, testare, preproducție și producție, fără modificarea codului sursă.

ID	Obligativitate	Cerință/Descriere
INT 037	M	Sistemul trebuie să implementeze mecanisme configurabile de timeout, retry cu interval progresiv, circuit breaker și izolare a erorilor, astfel încât indisponibilitatea unui sistem extern să nu determine blocarea întregului SIMED.
INT 038	M	În cazul indisponibilității temporare a unui serviciu extern, operațiunile care pot fi procesate ulterior vor fi păstrate într-o coadă controlată și reluate fără pierderea datelor, fără procesare duplicată și cu păstrarea ordinii atunci când aceasta este relevantă.
INT 039	M	Sistemul trebuie să asigure monitorizarea continuă a integrărilor, inclusiv disponibilitatea endpoint-urilor, timpul de răspuns, rata erorilor, mesajele neprocesate, lungimea cozilor și starea certificatelor utilizate.
INT 040	M	Componentele de integrare trebuie să expună endpoint-uri de health check și readiness check, fără a divulga utilizatorilor neautorizați informații sensibile despre infrastructură sau configurație.
INT 041	M	SIMED trebuie să permită transmiterea evenimentelor către sisteme externe prin MConnect Events sau prin mecanismele oficiale aprobate. Webhook-urile directe vor fi utilizate numai dacă nu există o alternativă guvernamentală și dacă utilizarea lor este justificată și aprobată.
INT 042	M	Sistemul trebuie să permită exportul controlat al datelor pentru raportare și analiză în formate deschise precum CSV, JSON și, după caz, Parquet, fără a crea o dependență obligatorie față de un produs BI comercial concret.
INT 043	M	Exporturile și integrările cu instrumente analitice trebuie să respecte regulile privind protecția datelor, anonimizarea, clasificarea informațiilor și drepturile de acces. Datele publice și datele instituționale interne vor fi furnizate prin fluxuri separate.
INT 044	M	Toate integrările trebuie testate în medii separate de producție, utilizând date sintetice, anonimizate sau pseudonimizate. Utilizarea datelor reale de producție în mediile de dezvoltare și testare nu este permisă decât în cazuri expres autorizate.
INT 045	M	Testarea integrărilor va include cel puțin scenarii pozitive, date nevalide, indisponibilitatea serviciului extern, timeout, răspuns duplicat, reluarea procesării, eroare de autorizare, expirarea certificatelor și volum ridicat de mesaje.
INT 046	M	Contractantul trebuie să furnizeze simulatoare, mock-uri sau servicii de test pentru sistemele externe atunci când mediile oficiale de testare nu sunt disponibile sau nu pot fi utilizate continuu în procesul de dezvoltare.
INT 047	M	Contractantul trebuie să livreze codul sursă al adaptoarelor, configurațiile, schemele, contractele API, exemplele de mesaje, scripturile de test și documentația integrărilor, astfel încât acestea să poată fi operate și dezvoltate independent de Contractant.
INT 048	M	Orice modificare a contractelor API, modelelor de date, schemelor mesajelor sau mecanismelor de securitate trebuie evaluată, versionată, testată și comunicată sistemelor consumatoare înainte de implementarea în producție.
INT 049	M	Contractantul trebuie să elaboreze un catalog al tuturor API-urilor, evenimentelor și integrărilor SIMED, indicând proprietarul, consumatorii, versiunea, starea, nivelul de criticitate și documentația aferentă.

ID	Obligativitate	Cerință/Descriere
INT 050	M	Contractantul trebuie să prezinte o matrice de conformitate privind interoperabilitatea și reutilizarea serviciilor guvernamentale, indicând pentru fiecare funcție serviciul reutilizat, modul de integrare, documentația aplicată, starea implementării și dovezile de testare.

5.8. Cerințe privind performanța și scalabilitatea sistemului IT

Sistemul Informațional de Management Electronic al Documentelor al ANSC trebuie să asigure un nivel ridicat de performanță operațională, care să permită procesarea în timp real și cu latență minimă a cererilor, deciziilor și altor acțiuni critice efectuate de utilizatori, în condițiile unui volum crescut de contestații și documente administrative. Tabelul 6.5 definește cerințele esențiale de performanță care trebuie respectate de sistem pentru a garanta disponibilitate, scalabilitate și timp de răspuns optim în cadrul misiunii instituționale a ANSC.

Tabelul 5.5. Cerințe privind performanța sistemului IT

ID	Obligativitate	Descriere
PSR 001	M	Sistemul trebuie să asigure un timp de răspuns de maximum **3 secunde pentru operați standard**, în condiții normale de funcționare și la nivelul de încărcare stabilit prin cerințe capacitate și performanță. Valorile de performanță vor fi măsurate pe baza percentililor P90 și P99, după cum urmea • pentru interogările simple: o maximum **1 secundă pentru cel puțin 90%** dintre solicitări; o maximum **3 secunde pentru cel puțin 99%** dintre solicitări; • pentru interogările complexe: o maximum **3 secunde pentru cel puțin 90%** dintre solicitări; o maximum **10 secunde pentru cel puțin 99%** dintre solicitări; • pentru generarea rapoartelor standard: o maximum **3 secunde pentru cel puțin 90%** dintre solicitări; o maximum **10 secunde pentru cel puțin 99%** dintre solicitări; • pentru operațiunile de procesare documentară, inclusiv generarea, conv verificarea, asocierea sau înregistrarea documentelor: o maximum **3 secunde pentru cel puțin 90%** dintre operațiuni; o
PSR 002	M	Sistemul trebuie să susțină simultan până la 500 de sesiuni active, inclusiv utilizatori inte ANSC și conexiuni externe. Perioadele de vârf includ orele de program standard (08:00–1 și lunile cu activitate intensificată (noiembrie–decembrie).
PSR 003	M	Contractantul va include în documentația tehnică descrierea proceselor cu impact negativ as performanței, împreună cu recomandări de execuție secvențială sau în afara orelor de vâr raportare masivă vs backup).
PSR 004	M	Activitățile de business intelligence și extragere de date pentru analiză nu trebuie să compro performanțele operaționale în procesarea tranzacțiilor.
PSR 005	M	Documentația sistemului trebuie să evidențieze operațiunile cu impact semnificativ as performanței și să propună bune practici pentru utilizatori în vederea menținerii indicatoril performanță.

ID	Obligativitate	Descriere
PSR 006	M	Contractantul trebuie să detalieze în propunerea tehnică valorile minime garantate performanței sistemului, în corelație cu stiva tehnologică propusă.
PSR 007	M	Sistemul trebuie să permită procesarea tranzacțiilor atât în regim real-time (online), c asincron (batch sau joburi planificate).
PSR 008	M	Sistemul trebuie să deservească simultan: • până la 5 administratori de sistem; • până la 50 utilizatori autorizați (interni și externi); • până la 500.000 de utilizatori anonimi (acces pub anumite date).
PSR 009	M	Sistemul trebuie să stocheze date provenite de la: • până la 5.000 autorități contractante; • la 40.000 operatori economici; • până la 60.000 contestații anuale.
PSR 010	M	Sistemul trebuie să fie proiectat pentru scalabilitate orizontală fără downtime – adăugare noduri noi și echilibrarea automată a sarcinilor.
PSR 011	D	Sistemul ar trebui să suporte autoscalare dinamică pentru componentele sensibile la latenț volum, adaptându-se automat la încărcarea de lucru.
PSR 012	M	Sistemul trebuie să fie capabil să gestioneze un număr nelimitat de tranzacții, condițion disponibilitatea și configurarea resurselor de infrastructură (CPU, memorie, stocare).
PSR 013	M	Contractantul trebuie să implementeze o soluție avansată de monitorizare a performanțe suport pentru metrice în timp real, alertare automată și instrumente vizuale (ex: Gra Kibana).

5.9. Cerințe privind flexibilitatea sistemului IT

Sistemul Informațional de Management Electronic al Documentelor (SIMED) al ANSC trebuie să dispună de un grad înalt de adaptabilitate funcțională și arhitecturală, capabil să acomodeze modificări legislative, procedurale și operaționale fără a necesita intervenții directe asupra codului sursă sau reimplementări costisitoare. Această lflexibilitate evolutivă este esențială pentru a asigura sustenabilitatea sistemului pe termen lung, reducerea costurilor de mentenanță și accelerarea răspunsului instituțional la modificările de reglementare sau la evoluția cerințelor instituționale. Este preferabil ca personalul autorizat al ANSC să poată efectua modificări relevante (ex. actualizarea fluxurilor procedurale, parametrii de notificare, modele de documente, reguli de validare etc.) prin interfețe de configurare dedicate, fără a necesita recompilarea aplicației sau intervenția dezvoltatorilor. Un asemenea nivel de configurabilitate declarativă reduce timpul de implementare al schimbărilor, limitează riscurile operaționale și crește autonomia instituțională.

Tabelul 5.6. prezintă cerințele de flexibilitate aplicabile sistemului.

ID	Obligativitate	Descriere
FLEX 001	M	Sistemul trebuie să permită configurarea și personalizarea interfeței utilizatorului (formulare, câmpuri, controale vizuale), în funcție de rolurile și procesele operaționale ale ANSC, fără modificarea codului sursă.
FLEX 002	M	Sistemul ar trebui să permită adăugarea de formulare noi, complet funcționale, pentru inițierea de acțiuni administrative, configurabile prin interfața administratorului funcțional.
FLEX 003	M	Sistemul trebuie să permită crearea, modificarea și configurarea rapoartelor operative și strategice (ex: seturi de date, câmpuri derivate, grupări dinamice), cu salvare și reutilizare a șabloanelor.

ID	Obligativitate	Descriere
FLEX 004	D	Sistemul ar trebui să permită definirea și afișarea indicatorilor cheie de performanță (KPI) în tablouri de bord configurabile, accesibile utilizatorilor autorizați.
FLEX 005	M	Sistemul trebuie să permită programarea generării automate a rapoartelor (pe bază de evenimente sau cron), cu livrare către utilizatorii desemnați sau publicare în tabloul de bord.
FLEX 006	D	Sistemul ar trebui să permită extinderea modelului de date prin adăugarea de proprietăți noi pentru entitățile gestionate (ex: contestații, decizii, ofertanți), fără restructurarea bazei de date.
FLEX 007	M	Sistemul trebuie să permită definirea și programarea execuției procedurilor automate, pe bază de evenimente sau condiții temporale, utilizând un mecanism configurabil declarativ sau grafic.
FLEX 008	M	Sistemul trebuie să permită configurarea completă a fluxurilor de lucru (workflow): stări, tranziții, reguli, alerte, documente generate, roluri implicate și drepturi asociate.
FLEX 009	M	Sistemul trebuie să permită gestionarea nomenclatoarelor și metadatelor interne și externe (ex: baze de date, fișiere sau servicii web), configurabile din interfață.
FLEX 010	M	Parametrii operaționali (ex: căi fișiere, conexiuni externe, clasificatori) trebuie să fie configurabili fără recompilarea codului sau intervenții directe în baza de date.
FLEX 011	D	Interfața de configurare trebuie să fie disponibilă pentru administratorii funcționali ANSC, cu auditarea completă a modificărilor realizate.
FLEX 012	M	Sistemul trebuie să permită integrarea componentelor dezvoltate de alte entități publice (AGE, ITCSS etc.), asigurând interoperabilitate la nivel de API și compatibilitate arhitecturală.
FLEX 013	M	Sistemul trebuie să permită definirea de reguli dinamice de validare a datelor, configurabile de ANSC printr-un editor de reguli logic-declarative.
FLEX 014	D	Sistemul ar trebui să permită rutine automate configurabile (post hooks) declanșate la evenimente (ex: arhivare, notificare, agregare), fără dezvoltări suplimentare.
FLEX 015	M	Sistemul trebuie să includă un motor de reguli configurabil pentru adaptarea comportamentului aplicației la modificări legislative, cu activare/dezactivare în funcție de scenariu procedural.

5.10. Cerințe privind interfața cu utilizatorul și ergonomia sistemului IT

Interfața utilizator a sistemului trebuie să respecte principii moderne de ergonomie digitală, accesibilitate și design centrat pe utilizator, astfel încât personalul ANSC să poată opera eficient și intuitiv în cadrul proceselor instituționale. Interacțiunea cu sistemul trebuie să minimizeze curba de învățare, permițând inclusiv utilizatorilor cu competențe digitale de bază să acceseze și să gestioneze funcționalitățile sistemului fără efort semnificativ de instruire.

Sistemul trebuie să asigure o experiență de utilizare unitară și coerentă, printr-o interfață grafică intuitivă, ușor de navigat, cu elemente vizuale standardizate și contextualizare a opțiunilor în funcție de rolul și sarcinile utilizatorului. Este esențial ca utilizatorii sistemului să aibă acces permanent la mecanisme de asistență (tooltips, ghiduri contextuale, notificări proactive, validări în timp real) pentru a preveni erorile de operare și a garanta calitatea datelor introduse sau procesate.

În vederea creșterii autonomiei instituționale și a reducerii necesităților de suport tehnic repetitiv, sistemul trebuie să integreze componente de tip *self-help*, asistență contextuală, precum și funcționalități pentru instruire interactivă.

Tabelul 5.7. Cerințele privind interfața cu utilizatorul a sistemului IT

ID	Obligativitate	Descriere
UI 001	M	Sistemul trebuie să pună la dispoziție toate funcțiile critice prin interfețe grafice intuitive, compatibile cu standardele UX moderne.
UI 002	M	Interfața sistemului trebuie să fie ergonomică și ușor de utilizat atât pentru utilizatorii tehnici, cât și non-tehnici, asigurând acces rapid la informații esențiale.
UI 003	M	Interfața utilizator trebuie să fie disponibilă în limbile română, engleză și rusă, cu posibilitatea selectării și salvării limbii preferate la nivel de cont utilizator.
UI 004	M	Componentele grafice ale interfeței trebuie să respecte nivelul A de conformitate din WCAG 2.1, pentru a garanta accesibilitatea tuturor categoriilor de utilizatori.
UI 005	M	Interfața trebuie optimizată pentru dispozitive desktop și notebook, cu rezoluție minimă suportată de 1360x768 px.
UI 006	M	Interfața trebuie să fie responsive, adaptându-se automat la dimensiunea și specificul dispozitivului utilizat (desktop, tabletă, smartphone).
UI 007	M	Sistemul trebuie să includă un mecanism centralizat de gestionare a localizării (i18n), pentru traducerea completă a tuturor etichetelor, mesajelor și elementelor UI.
UI 008	M	Sistemul trebuie să implementeze mecanisme de salvare automată și manuală a datelor introduse de utilizator, pentru prevenirea pierderii informațiilor.
UI 009	M	Sistemul trebuie să includă un modul de căutare avansată, capabil să opereze căutări full-text, filtrări logice și interogări complexe, aplicabile uniform în întreg sistemul.
UI 010	M	Căutarea full-text trebuie să fie susținută de un motor de indexare performant (ex. Elasticsearch, Apache Solr), pentru rezultate rapide și precise.
UI 011	M	Interfața trebuie să permită filtrarea avansată a rezultatelor prin metode de rafinare interactivă (faceted search) și prin formulare QBE (Query By Example).
UI 012	M	Clasificatorii și nomenclatoarele utilizate în UI trebuie să permită filtrarea pe valori discrete și pe intervale (numerice, temporale, logice).
UI 013	M	Interfața trebuie să susțină filtrarea rezultatelor pe baza expresiilor cu wildcard pentru ID-uri, denumiri, sau alte identificatoare (ex. 123*, *ABC, *public*).
UI 014	M	Sistemul trebuie să permită exportul datelor vizualizate în UI în formate deschise și standardizate (CSV, XLSX).
UI 015	M	Obiectele informatice gestionate în sistem trebuie să suporte atașarea de fișiere cu metadate (tip, dimensiune, autor, dată creare, modificare etc.).
UI 016	M	Sistemul trebuie să furnizeze funcționalitate de ajutor contextual pentru utilizatori, disponibilă în toate modulele principale.
UI 017	M	Utilizatorii trebuie să aibă acces la dicționarele de date ale sistemului atunci când configurează rapoarte, câmpuri sau interfețe personalizate.
UI 018	M	Interfața SIMED trebuie să respecte Modelul Unitar de Design aprobat la nivel guvernamental pentru serviciile publice electronice, conform HG nr. 677/2025.
UI 019	M	Contractantul va elabora prototipuri interactive de înaltă fidelitate pentru Front Office și Back Office, aliniate la cerințele MUD și prezentate spre aprobare înainte de dezvoltare.

ID	Obligativitate	Descriere
UI 020	M	Componentele UI reutilizabile ale SIMED vor fi documentate într-un design system sau component library, de preferință în Figma și/sau Storybook.
UI 021	M	Designul interfețelor publice va fi coordonat cu ANSC și, după caz, cu AGE, înainte de trecerea la etapa de dezvoltare finală.

5.11. Cerințe privind facilitățile de întreținere a sistemului IT

Pentru a asigura un nivel înalt de disponibilitate, fiabilitate și continuitate operațională a sistemului, este esențial ca acesta să dispună de mecanisme robuste de mentenanță proactivă, atât la nivel de infrastructură tehnologică, cât și la nivel de aplicație. Sistemul trebuie să permită monitorizarea continuă a performanței, diagnosticarea timpurie a disfuncționalităților, precum și aplicarea rapidă a actualizărilor corective și evolutive fără impact negativ asupra utilizatorilor sau întreruperi neplanificate ale serviciului.

Pentru a răspunde cerințelor instituționale ale ANSC, sistemul trebuie să ofere un cadru tehnologic scalabil pentru întreținerea facilă a tuturor componentelor (hardware, software, baze de date, servicii de integrare), inclusiv prin instrumente automate de alertare, auditare, jurnalizare și restaurare. De asemenea, trebuie să fie prevăzută o arhitectură care să permită desfășurarea activităților de întreținere cu intervenții minime din partea personalului tehnic și fără afectarea serviciilor publice furnizate

Tabelul 5.8. definește cerințele esențiale privind caracteristicile de întreținere ale sistemului.

ID	Obligativitate	Descriere
MR 001	M	Sistemul trebuie să includă un mecanism unificat de monitorizare a tuturor componentelor critice (strat aplicație, strat date, servicii externe), cu tablouri de bord centralizate pentru evaluarea încărcării, disponibilității și performanței.
MR 002	D	Sistemul trebuie să emită alerte configurabile în timp real în cazul degradării performanței componentelor, integrabile cu sisteme de notificare (e-mail, webhook, etc.).
MR 003	M	Sistemul trebuie să implementeze un serviciu de tip heartbeat care transmite periodic starea operațională și parametrii de sănătate a componentelor.
MR 004	M	Sistemul trebuie să dispună de un mecanism configurabil pentru jurnalizare tehnică granulară pe module și tipuri de evenimente.
MR 005	M	Logurile trebuie să includă niveluri de severitate standardizate: info, warning, error, critical, și să permită integrarea cu soluții de analiză.
MR 006	M	Toate erorile și excepțiile critice trebuie să fie înregistrate pentru analiză ulterioară, auditabilitate și îmbunătățirea sistemului.
MR 007	M	Antreprenorul trebuie să specifice metodele și instrumentele utilizate pentru depanarea sistemului (profilare, debugging, analiză performanță).
MR 008	M	Sistemul trebuie să integreze funcționalități administrative pentru operarea componentelor: pornire, oprire, restart, backup, restaurare, golire cache.
MR 009	M	Codul sursă trebuie să respecte bune practici de dezvoltare (ex: Clean Code), să fie modular, comentat și ușor de întreținut.
MR 010	M	Arhitectura sistemului trebuie să permită aplicarea de modificări localizate cu impact minim, și identificarea clară a componentelor afectate.

ID	Obligativitate	Descriere
MR 011	M	Sistemul trebuie să permită programarea și execuția automată a sarcinilor de mentenanță (ex: arhivare, agregare date, generare rapoarte).
MR 012	M	Sistemul trebuie să susțină upgrade-uri fără afectarea configurațiilor existente sau a API-urilor definite pentru terți.
MR 013	M	Trebuie să fie posibilă migrarea sistemului între medii (producție/test/dezvoltare) cu export/import de configurări și proceduri documentate.

5.12. Cerințe privind securitatea și protecția sistemului IT

Pentru a garanta confidențialitatea, integritatea și disponibilitatea informațiilor gestionate prin intermediul sistemului, **sistemul** trebuie să integreze un set complet de măsuri de securitate cibernetică, aliniate la politicile interne ANSC și la standardele internaționale în domeniu (inclusiv seria ISO/IEC 27000 și reglementările europene privind protecția datelor și identitatea digitală).

Sistemul trebuie să fie proiectat conform principiului de **securitate stratificată (defense-in-depth)**, acoperind toate nivelurile arhitecturii informatice – de la infrastructura fizică și rețea, la stratul de aplicații și gestionarea accesului utilizatorilor. Mecanismele de control al securității trebuie să permită prevenirea, detecția, izolarea și remedierea promptă a incidentelor, precum și auditarea și trasabilitatea completă a evenimentelor de securitate.

De asemenea, este esențial ca **sistemul** să fie interoperabil cu mecanismele instituționale existente la nivelul ANSC privind **managementul riscurilor IT**, astfel încât procesele de guvernanță și conformitate să poată fi automatizate și monitorizate continuu.

Tabelul 5.9. prezintă cerințele funcționale și nefuncționale esențiale pentru arhitectura de securitate a sistemului.

ID	Obligativitate	Cerință
SEC 001	M	Arhitectura sistemului trebuie proiectată conform principiilor „Secure by Design” și „Security by Default”, asigurând controlul continuu al riscurilor.
SEC 002	M	Documentația tehnică a arhitecturii de securitate trebuie să includă modelul de securitate, componentele critice și rolurile acestora în protecția sistemului.
SEC 003	M	Documentația de securitate trebuie să includă topologia rețelei și recomandări privind politicile de acces și matricea de comunicație între componente.
SEC 004	M	Toate procesele și serviciile interne trebuie să ruleze cu privilegii minime, conform principiului „least privilege”.
SEC 005	M	Gestionarea acreditărilor trebuie realizată exclusiv prin interfețe administrative securizate; credentialele hard-coded sunt interzise.
SEC 006	M	Credentialele nu trebuie stocate în formă necriptată în fișiere, baze de date sau alte componente ale sistemului.
SEC 007	M	Toate interfețele expuse extern trebuie protejate cu autentificare robustă, ex. certificate X.509.
SEC 008	M	Interfața publică trebuie protejată cu mecanisme anti-bot (ex. CAPTCHA, reCAPTCHA).
SEC 009	M	Validarea inputurilor trebuie aplicată la nivel de client și server, conform principiilor „zero trust input processing”.
SEC 010	M	Sistemul trebuie să fie protejat împotriva celor mai critice 10 vulnerabilități OWASP 2021.

ID	Obligativitate	Cerință
SEC 011	M	Datele transmise trebuie să fie criptate (ex. TLS 1.3), asigurând confidențialitatea la nivel de transport și aplicație.
SEC 012	M	Toate acțiunile utilizatorilor trebuie înregistrate în jurnale de audit imutabile, semnate digital.
SEC 013	D	Sistemul trebuie să emită semnale de stare operațională (heartbeat), cu notificări automate în caz de anomalii.

Tabelul 5.10. Cerințe pentru mecanismul de autentificare

ID	Obligativitate	Cerință
SEC 014	M	Sistemul trebuie să permită accesul utilizatorilor exclusiv prin autentificare federată, utilizând serviciul guvernamental MPass și mecanisme de autentificare forte.
SEC 015	M	Sistemul trebuie să dispună de funcționalități pentru gestionarea identităților digitale, inclusiv crearea, actualizarea și validarea profilurilor de utilizator (IDNP, email, roluri etc.).
SEC 016	M	Sistemul trebuie să implementeze politici automatizate de suspendare și blocare a conturilor, configurabile pe baza evenimentelor de securitate sau abateri de la reguli.
SEC 017	M	Sistemul trebuie să permită parametrizarea numărului maxim de sesiuni concurente per utilizator, pentru prevenirea utilizării abuzive a acreditărilor.
SEC 018	M	Sistemul trebuie să implementeze timeouts configurabile pentru sesiuni inactive, cu valoare implicită de 15 minute și notificare anticipată înainte de expirare.
SEC 019	M	Sistemul trebuie să integreze funcții anti-hijacking care protejează sesiunile active împotriva preluării neautorizate (ex. tokenuri nonce, binding IP).
SEC 020	M	Sesiunea utilizatorului trebuie să poată fi întreruptă manual de utilizator sau automat, în funcție de politicile definite, cu blocarea imediată a accesului la resurse.

Tabelul. 5.11. Cerințe privind mecanismul de înregistrare și auditare.

ID	Nivel	Cerință
SEC 021	M	Sistemul trebuie să integreze un subsistem de audit centralizat, capabil să capteze, stocheze și coreleze evenimente relevante din toate componentele aplicației, infrastructurii și interfeței utilizator.
SEC 022	M	Subcomponenta de audit trebuie să susțină configurarea granulară a politicilor de înregistrare, permițând definirea tipurilor de evenimente și nivelul de severitate aferent acestora.
SEC 023	M	Politicile de audit trebuie să fie configurabile la nivel de strat funcțional, interfață utilizator, operațiuni asupra datelor și categorii de evenimente sistemice sau de afaceri.

ID	Nivel	Cerință
SEC 024	M	Sistemul trebuie să permită definirea parametrilor dinamici pentru evenimentele înregistrabile, inclusiv filtre contextuale (perioadă, stare, tip obiect, tranzacție etc.).
SEC 025	M	Mecanismul de auditare trebuie să permită instrumentarea oricărui obiect sau acțiune din cadrul aplicației – până la nivel de câmp sau acțiune individuală.
SEC 026	M	Fiecare înregistrare de audit trebuie să includă: timestamp sincronizat, identificatorul utilizatorului, entitatea afectată, natura exactă a acțiunii și metadate relevante (ex: IP, sesiune, modul).
SEC 027	M	Logurile de audit trebuie să excludă în mod explicit informații sensibile în clar (de ex., parole, tokenuri, chei secrete), respectând principiile de confidențialitate și minimizare a datelor.
SEC 028	M	Mecanismul de audit trebuie să fie fail-safe – erorile de scriere a logurilor nu trebuie să perturbe funcționarea sistemului principal.
SEC 029	M	Toate înregistrările de audit trebuie să utilizeze un ceas de sistem sincronizat NTP, standardizat la nivelul sistemului de operare al serverului principal.
SEC 030	M	Sistemul trebuie să asigure arhivarea automată a logurilor istorice, configurabilă după frecvență, format, durată de retenție și destinație, conform politicii de retenție aprobată.
SEC 031	M	Pentru evenimente de securitate marcate ca critice, sistemul trebuie să emită notificări automate către utilizatorii/rolurile desemnate, prin canale preconfigurate (email, SMS, webhook etc.).
SEC 032	D	Sistemul trebuie să ofere suport pentru integrarea cu soluții SIEM (ex. Splunk, ArcSight, ELK) prin standarde deschise (ex. syslog, JSON, CEF), pentru corelarea și analiza evenimentelor.
SEC 033	M	Sistemul trebuie să mențină versiuni istorice ale entităților critice, cu jurnalizare completă a modificărilor, pentru asigurarea trasabilității datelor sensibile.
SEC 034	M	Orice modificare de stare, responsabil, sau statut în cadrul obiectelor de afaceri (ex: contestații, rapoarte) trebuie înregistrată cu identificatorul utilizatorului și momentul exact.
SEC 035	M	Sistemul trebuie să ofere instrumente avansate de query și export al înregistrărilor de audit în formate uzuale (CSV, JSON, XLSX), cu filtre personalizabile pe orice atribut sau câmp.
SEC 036	M	Sistemul trebuie să utilizeze mecanisme de protecție criptografică și semnătură digitală pentru a asigura integritatea și non-repudierea înregistrărilor de audit.
SEC 037	M	Evenimentele critice de afaceri trebuie să fie raportate în paralel prin intermediul serviciului guvernamental unificat MLog, cu o latență de maximum 5 secunde.
SEC 038	M	Sistemul trebuie să includă o interfață de configurare a tipurilor de evenimente ce necesită înregistrare paralelă în MLog, cu posibilitate de actualizare fără întreruperea serviciilor active.

6. CERINȚE PENTRU IMPLEMENTAREA SISTEMULUI IT

Această secțiune stabilește cerințele esențiale privind etapele de realizare și produsele livrabile aferente proiectului de dezvoltare și implementare a Sistemului Informațional de Management Electronic al Documentelor, cu funcționalitate extinsă asupra Registrului Contestațiilor gestionat de ANSC. Scopul acestor cerințe este de a asigura livrarea unei soluții informatice moderne, scalabile și securizate, care răspunde în mod adecvat atribuțiilor legale și operaționale ale Autorității în procesul de soluționare a contestațiilor din domeniul achizițiilor publice.

Cerințele formulate vizează controlul integral al ciclului de viață al sistemului, de la faza de analiză și proiectare funcțională până la dezvoltare, testare, instruire, migrare de date, lansare în producție și suport post-implementare. Prin urmare, aceste cerințe sunt obligatorii și reflectă nevoia ANSC de a beneficia de un sistem digital integrat, care să permită trasabilitatea, auditabilitatea și eficiența proceselor interne, în deplină conformitate cu cadrul normativ în vigoare, inclusiv Legea nr. 131/2015 și Codul administrativ.

Antreprenorul selectat va trebui să descrie în mod clar și argumentat, pentru fiecare cerință, modul de realizare propus, metodele și instrumentele utilizate, precum și măsurile tehnice și organizaționale ce vor fi adoptate în vederea respectării termenelor, standardelor de calitate și indicatorilor de performanță.

În cazul cerințelor care vizează perioada post-contractuală, ofertantul va detalia planul de acțiune și garanțiile oferite privind întreținerea, suportul tehnic și actualizările sistemului. Pentru cerințele aplicabile în etapa de depunere a ofertelor, ofertantul va furniza dovezi concludente privind capacitatea sa tehnică, resursele umane implicate, experiența relevantă în proiecte similare și abordarea metodologică propusă.

Această abordare permite ANSC să dispună de un cadru solid de monitorizare și control al livrabilelor, reducând riscurile de neconformitate, întârzieri sau implementare deficitară și contribuind la consolidarea capacităților instituționale prin digitalizarea sustenabilă a proceselor operaționale.

6.2. Plan de implementare la nivel înalt pentru sistemul IT

Tabelul 7.1 detaliază etapele cheie ale implementării sistemului, alături de termenele de finalizare estimate și livrabilele aferente fiecărei faze. O etapă este considerată încheiată doar în momentul în care toate livrabilele asociate au fost realizate integral și validate de către Autoritatea Contractantă.

Etapa 1: Pregatirea proiectului

Nr.	Activitate / Sarcină	Descriere tehnică și obiective	Livrabile asociate
1.1	Elaborarea planului integrat de management al proiectului.	Elaborarea unui plan operațional ce include diagrama Gantt detaliată, matricea RACI, procedura de change management și stakeholder map.	*Livrabil 1.1:* • Plan de management al proiectului (inclusiv planuri de comunicare, riscuri și QA).
1.2	Analiza contextuală a proceselor operaționale și arhitecturii funcționale existente.	Efectuarea unei analize „as-is” privind fluxurile instituționale, sistemele interoperabile și constrângerile IT actuale.	*Livrabil 1.2:* • Raport de analiză operațională și context tehnic (AS-IS).
1.3	Definirea portofoliului funcțional și tehnologic al sistemului.	Stabilirea granițelor funcționale, a componentelor sistemului și a specificațiilor de interoperabilitate.	*Livrabil 1.3:* • Portofoliu de produse și funcționalități planificate (TO-BE).
1.4	Elaborarea specificațiilor funcționale (SRS) și de proiectare tehnică (SDD).	Redactarea cerințelor funcționale, modelelor de date, use-case-urilor, prototipurilor UI/UX și arhitecturii logice și fizice.	*Livrabil 1.4:* • Documentația tehnico-funcțională (SRS și SDD).

Nr.	Activitate / Sarcină	Descriere tehnică și obiective	Livrabile asociate
1.5	Definirea cerințelor tehnice pentru infrastructura de hosting și securitate.	Determinarea cerințelor pentru medii de dezvoltare, staging, QA/UAT și producție, inclusiv cerințe de rețea, storage și securitate.	*Livrabil 1.5:* • Specificații pentru infrastructura IT (inclusiv cloud/hybrid).
1.6	Implementarea mediilor de dezvoltare și testare/formare (Dev și UAT).	Instalarea și configurarea inițială a containerelor, orchestratorului (ex: Docker, Kubernetes) și a serviciilor suport (DB, CI/CD).	*Livrabil 1.6:* • Medii operaționale funcționale (Dev și UAT), cu validare de conformitate inițială.
DURATA IMPLEMENTĂRII: 1 lună de la data semnării contractului			

Etapa 2: Proiectarea și dezvoltarea sistemului

Nr.	Activitate / Sarcină	Descriere tehnică și obiective	Livrabile asociate
2.1	Implementarea incrementală a sistemului conform metodologiei Agile și CI/CD.	Se vor derula iterații (sprinturi) în cadrul cărora componentele sistemului vor fi proiectate, dezvoltate, testate și documentate progresiv. Se va aplica integrarea continuă (CI) și livrarea continuă (CD).	*Livrabil 2.1*: • Cod sursă funcțional dezvoltat incremental; • Documentația tehnică actualizată iterativ (SRS, SDD)Funcționalități testate și integrate în medii dedicate (dev/test).
2.2	Elaborarea și actualizarea documentației tehnice.	Documentația de sistem (SRS/SDD) va fi actualizată continuu pentru a reflecta cerințele funcționale, arhitectura logică și tehnică, scenariile de utilizare, și structura componentelor software.	*Livrabil 2.2*: • Documentație tehnică completă și actualizată la fiecare sprintProiect detaliat revizuit.
2.3	Testare funcțională, testare automată și testare a performanței sistemului.	Se vor realiza testări funcționale (black-box), testare automată (unit/integration) și testări de performanță (load/stress testing) pentru fiecare modul, utilizând instrumente precum JMeter, Selenium, Postman, JUnit.	*Livrabil 2.3*: • Rapoarte de testare funcțională: • Rapoarte de testare automată; • Rapoarte de testare performanță; • Defecte și îmbunătățiri documentate.
2.4	Organizarea atelierelor de validare și proiectare cu părțile interesate.	Sprint review-uri pentru validarea livrabilelor. Consultări interactive cu utilizatorii finali pentru validarea interfețelor, logicii aplicației și fluxurilor operaționale.	*Livrabil 2.4*: • Procese-verbale ale sesiunilor; • Feedback documentat și integratLista cerințelor validate;
2.5	Prezentări demonstrative și instruiri continue.	Demonstrarea funcționalităților livrate la sfârșitul fiecărui sprint și instruirea echipelor funcționale și tehnice.	*Livrabil 2.5*: • Prezentări (slide-uri) și ghiduri de utilizare; • Sesiuni de instruire înregistrate și documentate.

Nr.	Activitate / Sarcină	Descriere tehnică și obiective	Livrabile asociate
2.6	Integrarea cu platforma națională de achiziții publice (MTender/RSAP).	Stabilirea interfețelor de comunicație API între SIA „RSAP” și platforma națională de achiziții pentru importul/exportul informațiilor aferente procedurilor, dosarelor, etapelor și deciziilor.	*Livrabil 2.6*: • Specificații API pentru integrare; • Fluxuri documentate de interoperabilitateTestele de integrare.
2.7	Integrarea cu Registrul de Stat al Unităților de Drept (RSUD).	Integrarea sistemului cu serviciul RSUD al ASP prin MConnect pentru identificarea automată și validarea entităților juridice implicate.	*Livrabil 2.7*: • Documentația fluxurilor de interoperabilitate; • Descrierea cerințelor funcționale și tehniceRaport de testare a integrării.
2.8	Integrarea cu platformele guvernamentale (MPass, MSign, MConnect, MLog, MPay, MCabinet).	Asigurarea interoperabilității cu serviciile guvernamentale comune pentru autentificare, semnătură digitală, plată electronică, jurnalizare evenimente și interacțiune cu Cabinetul Digital al Contestatarilor.	*Livrabil 2.8*: • Servicii integrate și funcționale; • Documentație de integrareProtocoale și scheme de conectare.
2.9	Elaborarea documentației finale a interfețelor de programare (API) și validarea completă a integrărilor.	Finalizarea și transmiterea documentației tehnice privind interfețele API expuse de sistem pentru interoperabilitate. Validarea schimburilor de date și conformitatea cu cerințele de securitate și performanță.	*Livrabil 2.9*: • Documentație API publicabilă; • Raport de testare finalAcorduri de integrare semnate (acolo unde este necesar).
DURATA IMPLEMENTĂRII: 6 luni de la realizarea: **Etapei 1 – Pregatirea proiectului**			

Etapa 3: Migrarea datelor

Nr.	Activitate / Sarcină	Descriere tehnică și obiective	Livrabile asociate
3.1	Elaborarea planului de migrare a datelor.	Dezvoltatorul va elabora o strategie detaliată de migrare, care va include proceduri, responsabilități, validări, metode de testare și rollback. Planul va fi aliniat cerințelor ANSC și va include coordonarea cu administratorii platformei ELO pentru extragerea structurată a arhivei electronice.	*Livrabil 3.1:* • Plan de migrare aprobat; • Metodologie detaliată de migrare și reconciliere a datelor.
3.2	Maparea metadatelor și adaptarea structurii arhivei ELO.	Se va realiza maparea completă a structurii de metadate a arhivei ELO la modelul de date al noului sistem dezvoltat. Acest proces va asigura compatibilitatea terminologică, logică	*Livrabil 3.2:* • Matrice de mapare a metadatelor; • Documentația schemei de transformare.

Nr.	Activitate / Sarcină	Descriere tehnică și obiective	Livrabile asociate
		și structurală între documentele existente și noile entități digitale din sistem.	
3.3	Elaborarea scenariilor de migrare și populare.	Vor fi dezvoltate scenarii tehnice și de business pentru migrarea incrementală a arhivei contestațiilor. Se vor defini reguli de curățare, deduplicare, validare și asigurare a integrității logice și cronologice a documentelor procesuale.	*Livrabil 3.3:* • Scenarii de migrare și populare; • Fișe de validare și control.
3.4	Executarea migrației complete a arhivei și dosarelor electronice.	Dezvoltatorul va efectua importul efectiv al arhivei contestațiilor din sistemul ELO în noul registru digital al al sistemului, incluzând: cereri, decizii, avize, înscrisuri, fișiere asociate, semnături, loguri, într-o structură trasabilă, conform cerințelor ANSC.	*Livrabil 3.4:* • Scripturi ETLArhivă importată și încărcată în mediul de producție; • Rapoarte de completitudine și conformitate.
3.5	Validarea și testarea datelor migrate.	Se va efectua testarea datelor importate, validarea încrucișată cu arhiva sursă, verificarea trasabilității și consistenței dosarelor migrate. Se vor genera rapoarte de reconciliere și se va obține aprobarea finală de la ANSC pentru tranziția oficială.	*Livrabil 3.5:* • Raport de testare a datelor migrate; • Rapoarte de reconciliereProces-verbal de aprobare finală de către ANSC.
DURATA IMPLEMENTĂRII: 2 luni de la realizarea: **Etapei 2 – Proiectarea și dezvoltarea sistemului**			

Etapa 4: Formarea utilizatorilor

Nr.	Activitate / Sarcină	Descriere tehnică și obiective	Livrabile asociate
4.1	Elaborarea planului de formare și amaterialelor de instruire.	Se va elabora un plan detaliat de formare, care va include programarea sesiunilor, structura pe categorii de utilizatori (CSC, DJ, DTISD), și tematicile pentru atelierele de lucru. Materialele vor include prezentări, ghiduri interactive, tutoriale video și simulări. Planul va asigura acoperirea integrală a tuturor funcționalităților critice ale sistemului.	*Livrabil 4.1:* • Planul de instruire și calendarul de formare; • Materiale suport (manuale, fișe de lucru, tutoriale video, prezentări etc.).
4.2	Instruirea administratorilor tehnici și funcționali.	Administratorii de sistem (din cadrul DTISD) vor fi instruiți cu privire la configurarea sistemului, gestiunea utilizatorilor, monitorizarea	*Livrabil 4.2:* • Raport de instruire a administratorilor;

Nr.	Activitate / Sarcină	Descriere tehnică și obiective	Livrabile asociate
		operațională, jurnalizarea și mecanismele de audit. Vor fi prezentate și mecanismele de suport și remediere în caz de erori sau incidente tehnice.	• Fișe de participareFeedback privind funcționalitățile critice.
4.3	Formarea formatorilor interni pentru ANSC.	Se vor selecta și instrui formatori interni din rândul personalului ANSC care vor putea ulterior asigura instruirea continuă a noilor angajați sau a autorităților contractante. Aceștia vor primi materiale dedicate și vor participa la sesiuni practice de predare.	*Livrabil 4.3:* • Certificare formatori interni ANSCKit de formare (scenarii, ghiduri de instruire, exerciții de simulare).
4.4	Formarea utilizatorilor operaționali (CSC, DJ, DTISD).	Vor fi organizate sesiuni dedicate pentru toți utilizatorii interni, adaptate specificului funcțional al fiecărui compartiment (gestionarea dosarului contestației, atribuirea completelor, procesare documente, emitere decizii etc.).	*Livrabil 4.4:* • Raport de participare ANSC; • Fișe de instruire completate; • Evaluări post-formare.
4.5	Atelier de lucru cu autoritățile contractante și agenții economici contestatari.	Se va organiza cel puțin un atelier de instruire practică pentru utilizatorii externi (autorități contractante și operatori economici), cu accent pe depunerea și urmărirea contestațiilor prin interfața publică, autentificare, atașare documente, primirea notificărilor etc.	*Livrabil 4.5:* • Raport atelier externListe de participanți; • Feedback pentru îmbunătățirea interfeței publice și a comunicării sistemului cu utilizatorii externi.
4.6	Asigurarea accesului la sistemul de suport și documentație.	Contractantul va furniza acces la platforma de suport tehnic și funcțional (ticketing, ghiduri online, FAQ), accesibilă tuturor utilizatorilor autorizați, pentru a facilita asistența post-livrare și clarificările suplimentare.	*Livrabil 4.6:* • Acces funcțional la sistemul de suport; • Documentație interactivă publicată pe platforma tehnică.
DURATA IMPLEMENTĂRII: 1 luna de la realizarea: **Etapei 3 – Migrarea datelor**			

Etapa 5: Stabilizarea, acceptarea și livrarea finală

Nr.	Activitate / Sarcină	Descriere tehnică și obiective	Livrabile asociate
5.1	Ajustări post-formare și îmbunătățiri ale interfeței.	Implementarea modificărilor de fine-tuning pe baza sugestiilor primite în timpul instruirii și testării cu utilizatorii ANSC (CSC, DJ, DTISD), inclusiv îmbunătățiri privind navigabilitatea,	*Livrabil 5.1:* • Raport privind îmbunătățirile funcționale; • Lista modificărilor aplicateCod sursă actualizat.

Nr.	Activitate / Sarcină	Descriere tehnică și obiective	Livrabile asociate
		mesaje de eroare, optimizarea fluxurilor și corectarea defectelor minore raportate.	
5.2	Actualizarea documentației tehnice și de utilizare.	Revizuirea și finalizarea documentației tehnice (SRS, SDD, manuale API), precum și a ghidurilor de utilizare (pentru administratori, membri CSC și contestatari), reflectând ultimele modificări aplicate în faza de stabilizare.	*Livrabil 5.2:* • Documentație tehnică revizuită; • Manuale și ghiduri de utilizare finale.
5.3	Suport pentru activitățile de informare ANSC și promovare în rândul utilizatorilor.	Oferirea de suport logistic și tehnic pentru diseminarea funcționalităților cheie ale sistemului în cadrul ANSC, autorităților contractante și agenților economici. Pot include webinarii, sesiuni de întrebări și răspunsuri sau materiale informative.	*Livrabil 5.3:* • Raport privind activitățile de comunicare și informare; • Materiale informative livrate.
5.4	Elaborarea planului de continuitate și a procedurilor de securitate.	Furnizarea documentelor strategice obligatorii: Plan de Continuitate a Activității (BCP), Plan de Recuperare în caz de Dezastru (DRP), Plan de Backup, planuri de restaurare și proceduri aferente în conformitate cu ISO/IEC 27001 și cerințele Cibernetice naționale.	*Livrabil 5.4:* • Plan BCP, DRP, backup și politici de restaurare validate.
5.5	Suport operațional și stabilizare tehnică.	Remedierea problemelor funcționale și tehnice identificate în mediul de producție, aplicarea actualizărilor necesare și suport continuu în perioada de stabilizare (post-livrare).	*Livrabil 5.5:* • Raport privind suportul oferit și acțiunile de stabilizare; • Log de remediere a erorilor.
5.6	Testarea finală de acceptare a sistemului.	Desfășurarea testelor finale de acceptanță a utilizatorului (UAT), pe baza scenariilor aprobate, cu implicarea tuturor actorilor interni (CSC, DJ, DTISD) și semnarea procesului-verbal de acceptanță.	*Livrabil 5.6:* • Raport final de testare și Proces-verbal de acceptare.
5.7	Predarea oficială a sistemului către ANSC.	Predarea codului sursă, a documentației tehnice și funcționale finale, a configurațiilor, mediilor și scripturilor, conform pachetului de livrare prevăzut în contract.	*Livrabil 5.7:* • Proces-verbal de predarePachet complet de livrare (cod sursă, documentație, configurații); • Arhivă tehnică completă.
DURATA IMPLEMENTĂRII: 2 luni de la realizarea: **Etapei 4 – Formarea utilizatorilor**			

Etapa 6: Asistență și întreținere postimplementare

Nr.	Activitate / Sarcină	Descriere tehnică și obiective	Livrabile asociate
6.1	Furnizarea serviciilor de suport tehnic și operațional postimplementare.	Prestarea serviciilor de suport tehnic de nivel 2 și 3 pentru utilizatorii sistemului (CSC, DJ, DTISD, DIRECTOR) prin mecanisme digitale de raportare incidente (ticketing), telefonic sau e-mail. Menținerea funcționalității continue a sistemului, în conformitate cu indicatorii de performanță și timpii de reacție/rezolvare stabiliți în SLA.	*Livrabil 6.1:* • Rapoarte lunare de suport (incident tickets, status, SLA indicatori).
6.2	Corectarea deficiențelor și actualizarea sistemului și documentației.	Intervenții corective pentru remedierea erorilor semnalate de ANSC, precum și livrarea de patch-uri și actualizări evolutive. Versiunile actualizate ale codului sursă și documentației (tehnice și de utilizare) vor reflecta modificările aprobate.	*Livrabil 6.1:* • Raport actualizat al corecțiilor aplicate; • Documentație tehnică și de utilizare actualizatăCod sursă versiune curentă actualizată.
DURATA IMPLEMENTĂRII: 12 luni de la realizarea: **Etapei 5 – Stabilizarea, acceptarea și livrarea finală**			

6.3. Cerințe pentru gestionarea proiectului

În cadrul procesului de implementare a sistemului, activitățile de management trebuie să asigure o coordonare eficientă a livrabilelor, transparență în comunicarea cu părțile interesate și controlul calității în toate etapele ciclului de viață al proiectului. Aceste cerințe sunt esențiale pentru garantarea implementării predictibile și conforme cu standardele asumate de ANSC.

Tabelul 6.3 Cerințe pentru managementul proiectului

ID	Obligativitate	Cerință
MG 001	M	Dezvoltatorul va gestiona implementarea în conformitate cu planul de lucru și metodologia convenită împreună cu ANSC.
MG 002	M	Sistemul va fi dezvoltat utilizând o abordare hibridă de management de proiect: analiză detaliată inițială, urmată de dezvoltare iterativă în sprinturi Agile.
MG 003	M	Antreprenorul va fi responsabil pentru alocarea și mobilizarea resurselor necesare pentru realizarea sarcinilor la standardul de calitate agreat.
MG 004	M	ANSC va gestiona aspectele instituționale, va asigura echipa proprie de proiect și va furniza infrastructura necesară desfășurării activităților.
MG 005	M	Proiectul va fi guvernat de o metodologie de management recunoscută la nivel internațional, precum PRINCE2, PMBOK sau echivalent.
MG 006	M	Antreprenorul va furniza un plan de proiect detaliat care va include: structura organizațională, roluri, calendarul activităților, planuri de comunicare, gestiunea riscurilor, controlul calității și al modificărilor.

ID	Obligativitate	Cerință
MG 007	M	Atât ANSC, cât și antreprenorul vor desemna câte un manager de proiect pentru coordonarea activităților respective.
MG 008	M	Managerul de proiect desemnat de antreprenor va deține autoritatea necesară și responsabilitatea pentru realizarea și livrarea tuturor rezultatelor proiectului.
MG 009	D	Antreprenorul poate desemna șefi de echipă pentru modulele tehnice și funcționale, pentru a facilita colaborarea cu părțile interesate.
MG 010	M	Antreprenorul va desfășura cel puțin următoarele activități: inițierea proiectului, actualizarea planurilor, managementul sprinturilor, coordonarea echipelor, comunicare periodică, menținerea registrelor (riscuri, livrabile, modificări), organizarea reuniunilor de proiect, închiderea etapelor și predarea livrabilelor.
MG 011	M	Toate documentele și comunicările oficiale aferente proiectului vor fi elaborate în limba română. ANSC poate solicita traducerea în limba engleză, dacă este necesar.
MG 012	M	Antreprenorul va livra următoarele documente esențiale de management al proiectului: carta proiectului, planul de proiect, planuri detaliate (sprinturi), prezentări, rapoarte bisăptămânale de progres, registre de proiect, rapoarte de închidere a etapelor și rapoarte de derogare.

6.4. Calificările dezvoltatorului

Compania selectată pentru implementarea proiectului trebuie să demonstreze îndeplinirea următoarelor cerințe minime de calificare, experiență și capacitate tehnică.

1. Experiență și capacitate tehnică

- Cel puțin 5 ani de experiență în proiectarea, dezvoltarea, implementarea și mentenanța sistemelor informaționale complexe;
- Experiență demonstrată în dezvoltarea și implementarea sistemelor informatice bazate pe arhitecturi distribuite, arhitectură de microservicii și infrastructuri de tip cloud;
- Experiență demonstrată în cel puțin 3 proiecte similare, finalizate și recepționate sau puse în exploatare în ultimii 5 ani;
- Prin proiect similar se înțelege un proiect care a inclus dezvoltarea și implementarea unui sistem informațional complex, a unei platforme de servicii electronice, a unui sistem de gestionare a beneficiarilor sau dosarelor, a unei platforme de management instituțional ori a unei soluții informatice cu integrări multiple și fluxuri operaționale automatizate;
- Experiență în implementarea soluțiilor informatice pentru instituții publice, autorități publice, organizații internaționale sau entități care gestionează servicii și procese cu un nivel comparabil de complexitate;
- Experiență în integrarea cu platforme guvernamentale de interoperabilitate și servicii electronice comune, precum MConnect, MPass, MSign, MNotify, MLog și MPay, sau cu platforme și servicii echivalente utilizate în alte jurisdicții;
- Experiență în proiectarea, dezvoltarea, documentarea, securizarea și integrarea API-urilor utilizând REST, SOAP, JSON, XML, OpenAPI/Swagger sau standarde și tehnologii echivalente;
- Experiență în implementarea mecanismelor de autentificare, autorizare, Single Sign-On, control al accesului bazat pe roluri și jurnalizare a activităților utilizatorilor;
- Capacitate demonstrată de aplicare a metodologiilor Agile, Scrum, Waterfall sau hibride în gestionarea și implementarea proiectelor IT;

- Experiență în organizarea proceselor de analiză, proiectare, dezvoltare, testare, migrare a datelor, implementare, instruire, suport și mentenanță post-implementare.

Îndeplinirea cerințelor privind experiența similară poate fi demonstrată prin contracte, procese-verbale de recepție, certificate de acceptanță, scrisori de recomandare, testimoniale sau alte documente relevante care confirmă executarea corespunzătoare a proiectelor declarate.

2. Sisteme de management și certificări organizaționale

Ofertantul trebuie să dețină certificate valabile care confirmă implementarea următoarelor sisteme de management:

- **ISO 9001:2015** – sistem de management al calității;
- **ISO/IEC 27001:2022** – sistem de management al securității informației;
- **ISO/IEC 20000-1:2018** – sistem de management al serviciilor de tehnologia informației;
- **ISO 37001:2025** – sistem de management anti-mită.

Se vor accepta edițiile ulterioare valabile ale standardelor menționate, precum și standarde sau sisteme de management echivalente, cu condiția demonstrării unui nivel comparabil de conformitate.

Certificatele trebuie:

- să fie valabile la data-limită de depunere a ofertelor;
- să fie emise de organisme de certificare acreditate sau recunoscute;
- să acopere activități relevante pentru obiectul contractului, precum dezvoltarea software, implementarea sistemelor informatice, securitatea informației, furnizarea și gestionarea serviciilor IT;
- să fie prezentate în copie, împreună cu informații care permit verificarea valabilității acestora.

3. Conformitate juridică și eligibilitate

Ofertantul trebuie:

- să fie o persoană juridică înregistrată legal și să desfășoare activitatea în conformitate cu legislația aplicabilă;
- să dețină toate autorizațiile, înregistrările și drepturile necesare prestării serviciilor solicitate;
- să nu se afle în stare de faliment, insolvabilitate, lichidare sau reorganizare judiciară și să nu facă obiectul unor proceduri care ar putea afecta semnificativ capacitatea de executare a contractului;
- să nu fi fost suspendat, exclus, sancționat sau declarat neeligibil de către o organizație din sistemul Organizației Națiunilor Unite, Banca Mondială sau o altă organizație internațională;
- să nu facă obiectul unei interdicții sau sancțiuni aplicate în baza listelor de sancțiuni ale Consiliului de Securitate al Organizației Națiunilor Unite;
- să nu se afle într-o situație de conflict de interese actual, potențial sau perceput în legătură cu procedura de achiziție sau executarea contractului;
- să informeze imediat autoritatea contractantă despre orice conflict de interese care apare pe parcursul procedurii sau al executării contractului;
- să respecte cerințele aplicabile privind protecția datelor cu caracter personal, confidențialitatea, securitatea informației și păstrarea datelor;

4. Documente justificative

Pentru demonstrarea îndeplinirii cerințelor, ofertantul va prezenta:

- documente de înregistrare a companiei;
- descrierea experienței generale și specifice;
- lista proiectelor similare;
- ***după caz , copii ale contractelor sau ale paginilor relevante din contracte***;

- procese-verbale de recepție, certificate de acceptanță sau documente echivalente;
- scrisori de recomandare sau datele de contact ale beneficiarilor anteriori;
- copii ale certificatelor ISO și informații privind valabilitatea acestora;
- CV-urile și certificările experților-cheie;
- structura echipei și planul de alocare;
- descrierea infrastructurii, instrumentelor și procedurilor de lucru;
- declarații privind eligibilitatea, conflictul de interese, sancțiunile, insolvența și conformitatea juridică.

6.5. Cerințe pentru dezvoltarea sistemului IT

Sistemul va fi dezvoltat utilizând o abordare iterativă și incrementală, bazată pe principiile Agile și pe practicile de integrare și livrare continuă. Înainte de inițierea ciclurilor de dezvoltare, va fi realizată o analiză de business detaliată, conform metodologiei Waterfall, pentru a asigura o înțelegere completă a cerințelor instituționale și funcționale.

Tabelul 6.5 conține cerințele specifice pentru faza de proiectare și dezvoltare.

ID	Obligativitate	Descrierea cerinței
DEV 001	M	Sistemul trebuie să fie dezvoltat utilizând o abordare hibridă de gestionare a proiectelor. În acest context, înainte de inițierea fazei de proiectare și dezvoltare, se va desfășura o etapă de analiză detaliată a proceselor instituționale și a nevoilor ANSC, în conformitate cu metodologia Waterfall. Pe baza acestei analize se va construi Product Backlog-ul necesar pentru faza iterativă de dezvoltare.
DEV 002	M	Proiectarea și dezvoltarea sistemului trebuie realizate în baza unei abordări Agile, prin iterații incrementale și utilizarea practicilor de integrare și livrare continuă (CI/CD), asigurând adaptabilitatea și testarea constantă a funcționalităților.
DEV 003	M	Sprinturile de dezvoltare vor avea o durată standard de două (2) săptămâni. În funcție de complexitatea activităților sau dinamica proiectului, durata sprintului poate fi extinsă la trei (3) săptămâni, cu acordul ANSC.
DEV 004	M	În cadrul fiecărui sprint, contractantul va executa următoarele activități: • selectarea și/sau actualizarea elementelor din Product Backlog; • analiza detaliată a cerințelor pentru elementele selectate; • redactarea și revizuirea user stories; • dezvoltarea funcționalităților planificate; • testarea internă a funcționalităților; • elaborarea/actualizarea documentației tehnice aferente (ex. SRS, SDD, ghiduri); • actualizarea portofoliului de livrabile.
DEV 005	M	Contractantul va elabora și transmite ANSC rapoarte de progres bisăptămânale care vor include: • sarcinile realizate; • sarcinile planificate; • impedimente apărute; • riscuri identificate și măsuri de atenuare propuse.

ID	Obligativitate	Descrierea cerinței
DEV 006	M	Contractantul va susține sesiuni periodice de prezentare a funcționalităților livrate, cu implicarea echipei ANSC și a altor părți interesate, documentând observațiile și sugestiile acestora pentru ajustări în sprinturile următoare.
DEV 007	M	Contractantul trebuie să fie capabil să asigure lansarea în producție, în mod parțial sau modular, a componentelor sistemului, în funcție de deciziile ANSC privind oportunitatea operaționalizării etapizate a funcționalităților livrate.

6.6. Cerințe pentru implementarea sistemului IT

Sistemul trebuie să respecte cerințele actualizate ale Agenției de Guvernare Electronică din Republica Moldova privind dezvoltarea și funcționarea sistemelor informaționale publice, inclusiv principiile de echilibrare a sarcinii și scalabilitate tehnologică. Tabelul 7.5 prezintă cerințele esențiale de implementare ce trebuie respectate în cadrul dezvoltării sistemului destinat ANSC.

Tabelul 6.6. Cerințe pentru implementarea sistemului

ID	Obligativitate	Descrierea cerințelor de desfășurare
DEP 001	M	Sistemul trebuie să poată fi instalat atât pe servere dedicate, cât și în medii virtualizate conforme arhitecturii ANSC.
DEP 002	M	Sistemul trebuie să ofere suport complet pentru infrastructură containerizată (Docker, Kubernetes etc.).
DEP 003	M	Sistemul trebuie să poată fi instanțiat în paralel în medii distincte: dezvoltare, testare/formare și producție.
DEP 004	M	Implementarea sistemului trebuie realizată prin DevOps și instrumente specializate (CI/CD, Ansible, GitLab CI etc.).
DEP 005	M	Mecanismul de livrare trebuie să permită actualizarea modulară (per container/serviciu) fără afectarea sistemului general.
DEP 006	M	Mecanismul de livrare trebuie să permită extensia containerelor existente cu noi module sau funcționalități.
DEP 007	M	Trebuie să existe posibilitatea definirii mediului țintă (cluster dedicat/local/cloud) pentru fiecare implementare.
DEP 008	M	Mecanismul de implementare trebuie să includă fluxuri automate de build, testare și generare de pachete instalabile.
DEP 009	M	Procesul de livrare trebuie să suporte acțiuni post-deployment (ex: configurări suplimentare, integrarea notificărilor).
DEP 010	M	Implementarea în mediu de producție va fi automatizată, cu opțiuni de intervenție manuală (ex: aprobare, build manual).
DEP 011	M	Trebuie să existe mecanisme de propagare a datelor de configurare din medii de testare/formare către producție.
DEP 012	M	Contractantul va livra către ANSC toate scripturile, instrumentele și instrucțiunile necesare pentru implementare automatizată.

6.7. Cerințe pentru migrarea și popularea datelor

Tabelul 7.6 include cerințele esențiale privind migrarea și popularea datelor, proces care va preceda testarea și acceptarea Sistemului de către ANSC, pe baza seturilor de date furnizate de autoritățile competente.

Tabelul 6.7 Cerințe pentru migrarea și popularea datelor.

ID	Obligativitate	Descrierea cerinței de migrare
MIG 001	M	ANSC va pune la dispoziția contractantului seturile de date inițiale și metadatele relevante pentru popularea bazei de date a sistemului. Formatul și structura datelor vor fi convenite de comun acord.
MIG 002	M	Contractantul va efectua conversia valorilor metadatelor provenite din surse externe în conformitate cu taxonomiile și clasificatoarele oficiale ale ANSC.
MIG 003	M	Oferta tehnică va include o metodologie clară privind migrarea datelor, inclusiv migrarea seturilor istorice relevante din registrele sau aplicațiile anterioare (ex. MTender, baze interne ANSC).
MIG 004	M	Contractantul va implementa un mecanism automatizat și configurabil de populare a bazei de date cu nomenclatoare, clasificatori, parametri inițiali și alte seturi de date obținute din surse externe (ASP, MF, AGE etc.).
MIG 005	M	Contractantul este responsabil pentru: definirea metodologiei de migrare, planificarea procesului, dezvoltarea scripturilor, validarea datelor, reconcilierea valorilor și soluționarea erorilor de mapare.
MIG 006	M	Se va propune o metodologie completă ce va include: cartografierea datelor, validarea și completarea câmpurilor lipsă, reconcilieri de date, curățare și îmbogățire, precum și un plan de recuperare în caz de eșec.
MIG 007	M	Contractantul va livra un plan detaliat de migrare și populare, corelat cu planul general de dezvoltare a sistemului, cu etape, livrabile și instrumente prevăzute clar.
MIG 008	M	Vor fi furnizate toate scripturile, uneltele și instrumentele software utilizate pentru popularea bazei de date, însoțite de documentație tehnică completă.
MIG 009	M	Contractantul va respecta politicile de securitate cibernetică, protecția datelor și accesul controlat la informațiile sensibile conform normelor în vigoare.
MIG 010	M	La finalul procesului de migrare, contractantul va demonstra corectitudinea și integritatea datelor migrate, iar rezultatele vor fi documentate printr-un proces-verbal de acceptanță semnat cu ANSC.

6.8. Cerințe pentru instruirea utilizatorilor

Acest compartiment descrie cerințele privind instruirea utilizatorilor sistemului informatic de management electronic al documentelor utilizat de ANSC, precum și documentația necesară pentru susținerea procesului de instruire. Tabelul 7.7 prezintă cerințele operaționale ce trebuie îndeplinite pentru planificarea, organizarea și desfășurarea sesiunilor de instruire dedicate personalului ANSC, reprezentanților autorităților contractante și operatorilor economici în calitate de contestatari.

Tabelul 6.8 Cerințe pentru formarea utilizatorilor

ID	Obligativitate	Descrierea cerinței
UTD 001	M	Antreprenorul va asigura mediul de instruire preconfigurat, accesibil prin interfață web securizată, care să reproducă funcționalitățile principale ale sistemului informațional.

ID	Obligativitate	Descrierea cerinței
UTD 002	M	Antreprenorul va elabora și livra materiale suport pentru instruire, teste de evaluare și ghiduri interactive (în limba română), adaptate pe categorii de utilizatori (operatori economici, autorități contractante, personal ANSC).
UTD 003	M	Antreprenorul va dezvolta programe de formare specializate pentru utilizatorii Front Office, Back Office și administratori, în conformitate cu specificul funcțional al sistemului.
UTD 004	M	Planificarea detaliată a sesiunilor de instruire se va realiza în colaborare cu ANSC, în baza unui calendar agreat și a conținutului instruirii aprobat.
UTD 005	M	Sesiunile de instruire vor fi susținute în limba română și vor include prezentări teoretice, exerciții practice și sesiuni de întrebări-răspunsuri.
UTD 006	M	Antreprenorul va furniza instruire specializată pentru minimum 2 administratori de sistem ANSC, incluzând configurare, securitate, restaurare și întreținere. Durata minimă: 24 ore.
UTD 007	M	Va fi asigurată formarea a minimum 2 formatori ANSC, capabili să susțină instruiri ulterioare. Durata minimă: 16 ore.
UTD 008	M	Antreprenorul va elabora și livra următoarele livrabile în format electronic, accesibil și navigabil: • Documentație tehnică: Arhitectura sistemului, Ghid administrare; • Documentație funcțională: Ghiduri utilizator pentru fiecare tip de actor; • Materiale de instruire interactive (video, tutoriale, prezentări multimedia).
UTD 009	M	Ghidurile pentru administratori vor fi furnizate în limbile română și engleză. Restul documentației este obligatoriu în limba română.
UTD 010	M	Antreprenorul va furniza următoarele ghiduri operaționale tehnice și funcționale: • Ghiduri pentru administrare, mentenanță, depanare, restaurare, securitate, dezvoltare ulterioară; • Proceduri standard pentru managementul incidentelor și actualizărilor.
UTD 011	M	La finalizarea instruirii, va fi livrat pachetul complet de documentație tehnică, incluzând codul sursă complet al componentelor dezvoltate, structurat și documentat corespunzător pentru mentenanță și extindere ulterioară.

6.9. Cerințe pentru testarea acceptării de către utilizatori

Acest compartiment definește cerințele tehnice pentru testarea formală de acceptanță a sistemului din perspectiva utilizatorului final, precum și criteriile minime necesare pentru validarea funcțională, tehnică și operațională a soluției livrate.

Tabelul 6.9. Cerințe pentru testarea acceptării utilizatorului

ID	Obligativitate	Descrierea cerinței
UAT 01	I	În etapa de testare a acceptării de utilizator (UAT), toate modulele și componentele sistemului trebuie să fie complet implementate și configurate în strictă conformitate cu specificațiile funcționale și nefuncționale ale proiectului.
UAT 02	M	Contractantul va organiza și desfășura procesul de UAT, incluzând următoarele activități: • elaborarea strategiei și procedurilor de testare;

ID	Obligativitate	Descrierea cerinței
		• redactarea și livrarea planurilor și scenariilor de testare spre aprobare ANSC; • identificarea și documentarea defectelor; • remedierea erorilor identificate; • redactarea raportului final de testare și transmiterea acestuia către ANSC pentru aprobare.
UAT 03	M	Înainte de punerea în producție, trebuie realizate și validate următoarele categorii de teste: • Testare unitară (unit testing); • Testare de integrare; • Testare de performanță (încărcare și stres); • Testare de recuperare în caz de incident; • estare de securitate (inclusiv scanări de vulnerabilitate, evaluări OWASP Top 10).
UAT 04	M	ANSC, cu suportul contractantului, va derula următoarele teste suplimentare: • Testare de utilizabilitate (UX/UI); • Testare funcțională end-to-end a proceselor operaționale; • Testare de acceptanță formală în baza cerințelor ANSC și scenariilor de utilizare validate.
UAT 05	M	Acoperirea prin teste unitare (code coverage) trebuie să fie de minimum 90% din codul sursă al componentelor software dezvoltate.
UAT 06	M	Toate testele definite în planul de testare aprobat trebuie executate integral. Acceptanța soluției va avea loc în cazul în care nu se identifică neconformități critice și se înregistrează maximum două deviații majore restante.
UAT 07	M	Acceptarea finală a sistemului va fi formalizată la data la care toate erorile și nealinierile identificate în timpul testării UAT au fost complet remediate, conform procesului de management al defectelor.

6.10. Cerințe pentru punerea în funcțiune a sistemului IT

Această secțiune definește cerințele tehnice, metodologice și operaționale asociate fazei de *go-live* a sistemului de management electronic al documentelor din cadrul ANSC. Punerea în funcțiune reprezintă tranziția controlată de la medii de testare și validare către mediul operațional de producție. Tabelul de mai jos detaliază responsabilitățile contractantului în această fază critică.

Tabelul 6.10. Cerințe pentru punerea în funcțiune a sistemului IT

ID	Obligativitate	Descrierea cerinței
COM 01	M	Contractantul trebuie să propună și să justifice metodologic strategia de punere în funcțiune a sistemului. Strategia poate include opțiuni precum: tranziție graduală (rollout incremental), lansare pilot, execuție paralelă (*parallel run*), migrare tip *big bang*, în funcție de complexitatea arhitecturii și riscurile operaționale identificate. Abordarea trebuie să fie agreată cu ANSC.
COM 02	M	Contractantul va asigura asistență tehnică completă în toate etapele punerii în funcțiune, incluzând următoarele activități: • Elaborarea planului de punere în funcțiune (*cut-over plan*) detaliat

ID	Obligativitate	Descrierea cerinței
		• Elaborarea planului de revenire (*rollback plan*) în caz de eșec; • Validarea și actualizarea dataseturilor preexistente în sistemele conexe ANSC, acolo unde este aplicabil; • Asigurarea suportului tehnic în timp real în timpul tranziției; • Intervenții rapide pentru diagnosticarea și remedierea erorilor critice apărute în perioada inițială de operare.
COM 03	M	Contractantul are obligația de a redacta și de a livra către ANSC un Plan complet de punere în funcțiune, care va include: • Activități și termene pentru tranziția către producție; • Responsabilități alocate per rol (echipa dezvoltatorilor, administratorii de sistem ANSC, DTISD etc.); • Criterii de control al calității și mecanisme de validare post-implementare; • Proceduri de notificare și comunicare între echipele implicate. Planul va fi aprobat de echipa de management de proiect ANSC.
COM 04	M	Sistemul va fi declarat operațional și pus în producție doar în condițiile în care: • toate funcționalitățile esențiale sunt complet disponibile pentru utilizatorii autorizați din cadrul ANSC (CSC, DTISD, DJ); • Nu există erori critice deschise; • este semnat Protocolul de acceptare a punerii în funcțiune, ca document oficial între ANSC și contractant, în baza validărilor finale din testarea de acceptanță.

6.11. Cerințe pentru stabilizarea sistemului IT

Această secțiune definește cerințele esențiale privind perioada de stabilizare a sistemului de management electronic al documentelor al ANSC, imediat după punerea în funcțiune a sistemului. Perioada de stabilizare are rolul de a permite verificarea funcționării sistemului în condiții reale de producție, remedierea defectelor reziduale, optimizarea performanței și confirmarea interoperabilității cu infrastructura digitală guvernamentală.

Tabelul 6.11. Cerințe pentru stabilizarea sistemului IT

ID	Obligativitate	Descrierea cerinței
STAB 01	M	Perioada oficială de stabilizare a sistemului IT al ANSC are o durată minimă de 3 luni calendaristice și demarează imediat după finalizarea etapelor de implementare și semnarea Protocolului de punere în funcțiune. Această perioadă este considerată parte a fazei post-implementare controlată.
STAB 02	M	Pe durata celor 3 luni de stabilizare, contractantul are obligația de a furniza suport tehnic on-site și remote, inclusiv intervenție reactivă pentru eliminarea erorilor critice și a comportamentelor neconforme ale sistemului. În această fază, sistemul este evaluat în regim de producție, iar incident managementul trebuie să fie complet operaționalizat.
STAB 03	M	Contractantul trebuie să desfășoare activități de monitorizare avansată, analiză proactivă a logurilor, remediere a erorilor funcționale și optimizare a componentelor aplicației, în special a interfeței utilizator și modulelor cu grad ridicat de utilizare. Intervențiile trebuie să respecte bunele practici DevOps și să fie înregistrate în sistemul de ticketing stabilit cu ANSC.

ID	Obligativitate	Descrierea cerinței
STAB 04	M	Acceptarea finală a sistemului este condiționată de semnarea unui Protocol de recepție finală, care se va întocmi doar în baza următoarelor condiții cumulative: • perioada de stabilizare este încheiată; • toate erorile de nivel 1 (critice, blocante) au fost eliminate; • numărul total de erori de nivel 2 (majore) este mai mic de 10; • niciuna dintre erorile identificate în scenariile de testare nu afectează integritatea, disponibilitatea sau confidențialitatea datelor procesate.
STAB 05	I	O eroare de nivel 1 este definită ca orice defect care: • compromite funcționalitățile esențiale ale sistemului; • afectează capacitatea ANSC de a-și îndeplini obligațiile legale; • blochează accesul la datele critice; • împiedică operarea sistemului în parametri normali de disponibilitate sau performanță.
STAB 06	I	O eroare de nivel 2 este considerată ca fiind una care afectează funcționalități secundare sau complementare, dar pentru care există workaround-uri funcționale temporare, fără impact asupra componentelor critice sau a calității serviciului oferit de ANSC.

7. CERINȚE PENTRU PERIOADA DE GARANȚIE A SISTEMULUI IT

Serviciile de întreținere și suport aferente sistemului informațional, furnizate pe durata perioadei de garanție contractuală, au ca scop asigurarea continuității operaționale și optimizarea nivelului de serviciu, în conformitate cu cerințele Autorității Naționale pentru Soluționarea Contestațiilor În acest context, obiectivele strategice urmărite sunt următoarele:

- Alinierea continuă a funcționalităților sistemului la dinamica cerințelor operaționale și legislative ale ANSC și altor instituții implicate, prin actualizări funcționale prompte și eficiente;
- Gestionarea incidentelor tehnice și operaționale într-un interval de timp predictibil și prestabilit, cu minimizarea impactului asupra proceselor critice ale ANSC, în conformitate cu nivelurile de serviciu definite (SLA);
- Remedierea proactivă și corectă a disfuncționalităților sistemului, inclusiv prin analiză cauzală și intervenții structurale, fără întreruperea disponibilității platformei.

În vederea atingerii acestor obiective, Dezvoltatorul sistemului are obligația de a asigura un pachet complet de servicii de mentenanță și suport tehnic pe întreaga durată a perioadei de garanție, în strictă conformitate cu cerințele specificate în prezentul document. Aceste servicii trebuie să includă activități preventive, corective și adaptative, executate conform unui cadru metodologic bine definit.

Oferta tehnică prezentată de Dezvoltator va trebui să detalieze explicit:

- setul de activități și procese de suport ce vor fi implementate;
- metodologia de răspuns și intervenție în cazul incidentelor și solicitărilor de suport;
- nivelurile garantate de disponibilitate și performanță;
- capabilitățile tehnice, resursele umane specializate și capacitatea organizațională a prestatorului;
- instrumentele și tehnologiile suport utilizate pentru managementul solicitărilor, actualizărilor și remedierilor.

Se așteaptă ca livrabilele și activitățile propuse să respecte cele mai bune practici internaționale în managementul serviciilor IT – în special cele definite de standardele ISO/IEC 20000, ITIL v4 sau modele echivalente, care asigură trasabilitatea, calitatea și eficiența operațională a serviciilor.

Tabelul 7.0. din secțiunea următoare prezintă în mod detaliat cerințele generale pentru livrarea serviciilor de întreținere și suport tehnic în perioada de garanție.

Tabelul 7.0 - Cerințe generale pentru serviciile furnizate în timpul perioadei de garanție

ID	Obligativitate	Cerință detaliată
PIR 01	M	Dezvoltatorul are obligația de a furniza, pe întreaga durată a perioadei de garanție, servicii complete de întreținere și suport tehnic pentru sistem. Perioada de garanție va avea o durată de 12 luni, calculată de la data finalizării perioadei de stabilizare operațională.
PIR 02	M	Oferta financiară a Dezvoltatorului trebuie să includă o estimare detaliată a costurilor aferente furnizării serviciilor de mentenanță și suport în perioada de garanție, excluzând costurile asociate eventualelor cerințe suplimentare de dezvoltare ce depășesc limitele specificațiilor din SRS și SDD.
PIR 03	M	Orice defect de funcționare, eroare sau incident raportat în perioada de garanție trebuie remediat integral de către Dezvoltator, fără costuri suplimentare pentru ANSC.
PIR 04	M	La finalizarea perioadei de garanție de 12 luni, ANSC își rezervă dreptul de a solicita extinderea furnizării serviciilor de suport și mentenanță, pentru o perioadă de minimum 12 luni. Dezvoltatorul va asigura continuitatea serviciilor conform condițiilor contractuale și specificațiilor tehnice stabilite (inclusiv niveluri de serviciu – SLA și prețuri agreate).

7.2. Cerințe pentru serviciile de asistență tehnică în perioada de garanție

Serviciile de asistență tehnică trebuie furnizate de către Antreprenor în scopul gestionării eficiente a incidentelor apărute în perioada de exploatare a sistemului, remediind cauzele care afectează performanța, funcționalitatea sau disponibilitatea acestuia, precum și pentru a asigura o utilizare continuă, corectă și eficientă de către utilizatorii autorizați ai ANSC și alte entități relevante din ecosistemul sistemului.

În contextul prezentului proiect, se definesc următoarele concepte operaționale:

- **Incident** – orice eveniment care perturbă sau poate perturba funcționarea normală a sistemului, afectând disponibilitatea, performanța sau accesibilitatea acestuia;
- **Problemă** – cauza subiacentă a unuia sau mai multor incidente, care necesită analiză și remediere tehnică în profunzime;
- **Solicitare de consultanță** – o cerere formală din partea utilizatorilor autorizați pentru suport tehnico-funcțional în procesul de utilizare, configurare sau întreținere a sistemului, în afara cazurilor de incident sau defecțiune.
- Scopul acestor servicii este de a garanta funcționarea sistemului în parametrii de calitate prevăzuți contractual și de a susține ANSC în operarea continuă a proceselor digitale. Serviciile vor contribui la menținerea unui nivel operațional optim prin următoarele dimensiuni esențiale de calitate:
- **Disponibilitate** – capacitatea sistemului și a componentelor sale de a răspunde prompt și fiabil solicitărilor utilizatorilor autorizați, în conformitate cu nivelurile de serviciu (SLA);
- **Adecvarea pentru utilizare** – abilitatea sistemului de a furniza servicii corecte și complete, în conformitate cu specificațiile funcționale și așteptările instituționale;

- **Performanță** – timpul de răspuns și capacitatea sistemului de a procesa solicitări multiple, în regim continuu, fără degradarea calității serviciului;
- **Securitate** – asigurarea caracteristicilor de confidențialitate, integritate și disponibilitate a datelor, conform normelor naționale și europene privind securitatea cibernetică și protecția datelor. Tabelul 8.1 detaliază cerințele specifice privind serviciile de asistență tehnică ce urmează a fi prestate de Antreprenor în perioada de garanție a sistemului.

Cerințe privind serviciile de asistență tehnică pentru sistemul IT

ID	Obligativitate	Cerință tehnică detaliată
PIR 005	M	Dezvoltatorul este obligat să furnizeze servicii de suport tehnic complet pentru utilizatorii autorizați ai sistemului, în vederea tratării incidentelor apărute în timpul exploatării acestuia, indiferent de cauza care le-a generat (de exemplu: erori de aplicație, defecțiuni software, disfuncționalități la nivelul aplicațiilor terțe sau infrastructurii interconectate). Suportul va include, fără a se limita la următoarele acțiuni: • Recepționarea detaliilor despre incident de la utilizatorii autorizați; • Localizarea exactă a incidentului și aplicarea de măsuri imediate pentru diminuarea impactului; • Analiza cauzală a incidentului și definirea soluțiilor tehnice pentru remediere; • Oferirea de ghidaj tehnic utilizatorilor ANSC pentru implementarea soluțiilor de atenuare; • Raportarea documentată a cauzei incidenteului, acțiunilor corective aplicate și măsurilor preventive; • Integrarea incidentului într-un ciclu de gestionare a problemelor, acolo unde este cazul.
PIR 006	M	Dezvoltatorul trebuie să furnizeze servicii de suport pentru remedierea problemelor identificate la nivelul stratului aplicativ al sistemului. Aceste servicii includ următoarele activități: • Colectarea detaliilor relevante despre simptomatologia problemei, condițiile de apariție și impactul asupra funcționării; • Analiza profundă a componentei afectate și a relațiilor de dependență funcțională dintre modulele sistemului; • dentificarea și aplicarea soluțiilor temporare de limitare a impactului și asistență acordată ANSC pentru implementarea acestora; • Stabilirea și implementarea soluției tehnice definitive, cu informarea periodică a ANSC privind progresul; • Asistență pentru aplicarea soluțiilor de configurare (dacă sunt necesare); • Aplicarea și livrarea corecțiilor de cod aferente, în conformitate cu cerințele SLA și în cadrul serviciilor de mentenanță.
PIR 007	M	Dezvoltatorul va furniza servicii de consultanță tehnico-funcțională în sprijinul operării eficiente și conforme a sistemului de către ANSC. Aceste servicii vor presupune următoarele: • Procesarea solicitărilor de consultanță venite din partea utilizatorilor relevanți și înțelegerea contextului operațional;

ID	Obligativitate	Cerință tehnică detaliată
		• dentificarea și validarea soluțiilor tehnice în medii de test controlate și sigure; • Furnizarea de răspunsuri complete, documentate și precise privind modul de acțiune recomandat în cadrul proceselor de operare, configurare sau întreținere a sistemului.

7.3. Cerințe privind nivelul serviciilor

Această secțiune stabilește parametrii esențiali privind serviciile de întreținere și asistență tehnică ce urmează a fi furnizate de către contractant pe durata perioadei de garanție aferente sistemului. Cerințele sunt aliniate cu cele mai bune practici din domeniul ITSM (Information Technology Service Management), incluzând orientări conforme standardelor **ITIL**, **ISO/IEC 20000**, și sunt concepute pentru a asigura:

- continuitatea operațională a sistemului;
- intervenția rapidă și eficientă asupra incidentelor și problemelor tehnice;
- aplicarea unui management predictiv al modificărilor și actualizărilor;
- relație contractuală bazată pe indicatori de performanță clari (SLAs) și clasificarea solicitărilor în funcție de impact.

Toate cererile de suport tehnic vor fi tratate conform unei clasificări a priorității, iar nivelul serviciilor se va reflecta în timpii de răspuns, timpii de soluționare și disponibilitatea resurselor contractantului în intervalul **08:00–18:00 (EET), în zilele lucrătoare**. Solicitările ANSC vor fi reanalizate și, la nevoie, reclasificate în funcție de contextul evolutiv al cererii.

Cerințe esențiale privind serviciile în perioada de garanție

ID	Obligativitate	Descrierea cerinței tehnice
PIR 001	M	Contractantul va furniza servicii complete de suport tehnic și întreținere pe perioada de garanție de 9 luni.
PIR 002	M	Contractantul va asigura suport pentru incidente operaționale, indiferent de cauza: software, rețea sau terțe părți.
PIR 003	M	Contractantul va remedia problemele la nivel de aplicație, prin identificare, diagnostic și patch-uri corective.
PIR 004	M	Contractantul va furniza consultanță tehnico-funcțională pentru operarea eficientă a sistemului de către ANSC.
PIR 005	M	Pentru incidente critice, timpul maxim de răspuns este 5 minute; remedierea completă: 60 minute.
PIR 006	M	Pentru incidente majore: timp de răspuns 60 minute, rezolvare până la sfârșitul zilei lucrătoare.
PIR 007	M	Pentru incidente comune: timp de răspuns 24h, remediere în maxim 3 zile lucrătoare.
PIR 008	M	Contractantul va aplica o politică de actualizare lunară, cu excepția cazurilor critice sau actualizărilor de securitate.
PIR 009	M	Calendarul actualizărilor va fi comunicat cu minim 1 lună înainte; versiunile majore – cu minim 6 luni înainte.
PIR 010	M	Contractantul va notifica și coordona cu ANSC toate tipurile de lucrări de întreținere, conform clasificărilor definite.
PIR 011	M	Timpul maxim de reacție la o solicitare de dezvoltare: 3 zile lucrătoare.

ID	Obligativitate	Descrierea cerinței tehnice
PIR 012	M	Estimările de cost și soluțiile tehnice trebuie furnizate în maxim 10 zile lucrătoare.
PIR 013	M	Soluțiile de dezvoltare trebuie livrate conform termenelor agreate, aplicând principiul „best effort”.
PIR 014	M	ANSC va stabili prioritățile pentru cererile de dezvoltare, iar contractantul va ajusta livrările în consecință.
PIR 015	M	Pentru solicitările de prioritate scăzută, se aplică principiul „best effort”; termenul va fi agreat bilateral.

7.4. Cerințe pentru procedura de gestionare a modificărilor

Toate modificările aduse sistemului pe parcursul perioadei de garanție, în contextul furnizării serviciilor de întreținere și asistență tehnică, trebuie gestionate conform unui **proces formalizat, matur și trasabil de Change Management**, în concordanță cu cele mai bune practici din domeniul ITSM (ex. ITIL). Scopul acestui proces este de a asigura că orice modificare asupra componentelor tehnice sau funcționale ale sistemului este:
planificată riguros,

- testată corespunzător în medii controlate,
- implementată fără întreruperi majore asupra serviciilor critice,
- documentată complet și auditabilă,
- reversibilă în cazul unui eșec.

Contractantul este responsabil de aplicarea unei politici de guvernanță a modificărilor care să asigure **continuitatea operațională, securitatea, conformitatea și calitatea serviciului IT**.

Cerințe privind procedura de gestionare a modificărilor

ID	Obligativitate	Cerință tehnică
PIR 016	M	Contractantul va include în ofertă abordarea sa privind procesul de gestionare a modificărilor, cu indicarea instrumentelor, responsabilităților și fluxurilor.
PIR 017	M	Contractantul va propune o procedură formală de gestionare a modificărilor, care va fi coordonată și validată de ANSC înainte de punerea în aplicare.
PIR 018	M	Procedura de schimbare va acoperi următoarele activități minime: testare în mediu de test, plan de implementare, plan de roll-back, documentare tehnică completă, versionare și livrare software.
PIR 019	M	Pe durata serviciilor de mentenanță și dezvoltare, contractantul va efectua modificări controlate asupra componentelor sistemului (aplicație, baze de date, interfețe).
PIR 020	M	Orice modificare cu impact semnificativ asupra calității serviciilor va fi autorizată de ANSC. Contractantul va respecta: testarea completă, plan de revenire, evaluare post-implementare.
PIR 021	M	Toate modificările vor fi înregistrate într-un **Registru al Modificărilor**, menținut electronic. ANSC va avea acces permanent în regim de citire la acest registru.
PIR 022	M	Orice pachet software rezultat dintr-o modificare va include fișierele de cod sursă și executabil, semnate digital (code-signing) pentru validarea integrității și autenticității.
PIR 023	M	Contractantul va furniza documentația actualizată pentru fiecare modificare (manual de instalare, ghid de utilizare, plan de testare și plan de revenire).
PIR 024	M	În cazul în care sunt detectate erori critice post-implementare, contractantul va interveni **imediat**, aplicând măsuri corective în regim de urgență.

7.5. Cerințe pentru încheierea contractului

În eventualitatea în care părțile contractuale decid să nu prelungească acordul privind serviciile de suport tehnic și mentenanță postimplementare, se impune asigurarea unui proces de închidere contractuală controlat, care să nu afecteze continuitatea operațională a sistemului. ANSC va păstra dreptul de a contracta un furnizor alternativ sau de a prelua intern aceste servicii, în baza unui transfer complet de cunoștințe, artefacte tehnice și documentație operațională.

Contractantul are obligația să furnizeze toate componentele esențiale pentru a permite această tranziție într-o manieră transparentă și nedisruptivă, în conformitate cu cele mai bune practici din domeniul IT Governance (ex. COBIT, ITIL Transition Management). Tabelul de mai jos definește cerințele minimale care trebuie respectate la încetarea relațiilor contractuale.

ID	Obligativitate	Cerință tehnică calificată
PIR 024	M	La finalizarea contractului, contractantul va furniza către ANSC: • Codul sursă complet și actualizat al sistemului, în forma rulată în mediul de producție; • Documentația tehnică și operațională, revizuită până la data încetării; • Exportul integral al înregistrărilor privind incidentele, problemele, solicitările de consultanță, modificările și dezvoltările, în format convenit (ex. CSV, XLSX, XML).
PIR 025	M	Contractantul va arhiva și păstra, pe o durată de minimum 12 luni de la data încetării contractului, toate înregistrările generate în perioada contractuală, inclusiv codul sursă și documentația asociată.
PIR 026	M	Pe parcursul a cel puțin 12 luni postcontractuale, contractantul se obligă să colaboreze cu orice terță parte autorizată de ANSC în vederea facilitării tranziției serviciilor. Aceasta include livrarea de informații relevante și suport punctual pentru optimizarea serviciilor viitoare.
PIR 027	M	Oferta tehnică va conține o descriere detaliată a strategiei de închidere contractuală, incluzând procesul de transfer de responsabilitate, livrabilele finale și planul de tranziție către un nou operator.
PIR 028	M	Durata contractuală a SLA-ului aferent perioadei de garanție este de 9 luni. Rezilierea anticipată poate fi inițiată de oricare parte, cu condiția transmiterii unei notificări scrise cu minimum 6 luni înainte.
PIR 029	M	Toate datele stocate în bazele de date aferente sistemului sunt proprietatea exclusivă a ANSC. La încetarea contractului, contractantul este obligat să pună la dispoziția beneficiarului o procedură completă de export și livrare a datelor într-un format standardizabil și reutilizabil, care să asigure importul integral într-un sistem alternativ.

8. CERINȚE PRIVIND LIVRABILELE SISTEMULUI INFORMAȚIONAL

Produsul final aferent dezvoltării sistemului va constitui un set complet de livrabile tehnice și funcționale, care acoperă integral componentele software, artefactele documentare, precum și transferul formal de cunoștințe către ANSC, în calitate de proprietar, deținător și administrator al sistemului. Fiecare livrabil va fi furnizat în format digital, semnat electronic, cu trasabilitate completă a versiunilor și a ciclului de aprobare.

Livrabilele de referință prezentate mai jos sunt esențiale pentru configurarea, operarea, întreținerea și extinderea ulterioară a sistemului și trebuie livrate în conformitate cu cerințele de calitate, interoperabilitate și securitate stabilite de ANSC.

Tabel 8.0 Produse livrabile esențiale pentru SIA „RSAP”

ID	Obligativitate	Descriere tehnică a livrabilului
DEL 001	M	**Livrabile de management al proiectului**: •Document de inițiere a proiectului; • Plan de management al proiectului; • Rapoarte periodice privind progresul (bisăptămânale); • Rapoarte de etapă și raportul de închidere a proiectului; • Rapoarte privind deviațiile sau excepțiile identificate.
DEL 002	M	**Documentație tehnică a sistemului**: • Product Backlog complet; • Arhitectura logică și fizică a sistemului; • Documentele SRS și SDD; • Specificații tehnice pentru integrarea cu platforme partajate (MConnect, MPass, MPay etc.); • Documentația API-urilor publice și interne; • Codul sursă integral documentat și comentat; • Pachetul de instalare configurabil pentru mediul ANSC (inclusiv scripturi automate de deployment).
DEL 003	M	**Ghiduri de utilizare, întreținere și dezvoltare**: • Ghidul administratorului; • Ghid de instalare, configurare și update; • Manual de mentenanță corectivă și preventivă; • Ghid de remediere a erorilor funcționale; • Manualul utilizatorului final; • Ghid pentru dezvoltatori (extensibilitate și scalabilitate); • Ghiduri video (multimedia) pentru fluxurile critice; • Documentație privind securitatea informațională (plan de continuitate, plan DR, politici backup și failover).
DEL 004	M	**Livrabile aferente instruirii utilizatorilor**: • Planul de instruire per tip de utilizator (admin, utilizator general, supervizor); • Materiale de instruire (prezentări, fișe de exerciții, tutoriale video); • Raport de instruire cu analiza feedback-ului și propunerile de optimizare.
DEL 005	M	**Livrabile pentru asigurarea calității și testare**: • Strategia de testare (funcțională, non-funcțională); • Planuri de testare; • Seturi de scenarii și cazuri de test (unit, integrat, acceptanță); • Rapoarte de testare și indicatori de performanță; • Raportul final de acceptanță semnat de ANSC.
DEL 006	M	**Acordul privind nivelul serviciilor (SLA)** aferent perioadei de garanție, întreținere și suport tehnic postimplementare, agreat între ANSC și contractant.
DEL 007	M	**Suport digital al tuturor livrabilelor**: • Toate artefactele vor fi livrate în format electronic (ex. suport fizic DVD, medii de stocare externe criptate, și transfer securizat prin infrastructura ANSC); • Fiecare livrabil va fi însoțit de fișă de livrare și proces-verbal de recepție.

Tabelul 8.1 Servicii de transfer de cunoștințe și suport post-implementare

ID	Obligativitate	Descriere tehnică a serviciului
DEL 008	M	Formare pentru formatori („Train-the-Trainers”): Contractantul are obligația de a desfășura sesiuni de instruire intensivă pentru personalul desemnat de ANSC în calitate de formatori interni. Aceștia trebuie să dobândească competențele necesare pentru a instrui ulterior toate categoriile de utilizatori ai sistemului.
DEL 009	M	Instruirea utilizatorilor și a administratorilor de sistem: Contractantul va livra sesiuni de instruire practică și teoretică pentru toate tipurile de utilizatori autorizați (inclusiv operatori, responsabili de proces, supervizori) și pentru administratorii tehnici ai sistemului, în format fizic și/sau digital.
DEL 010	M	Suport tehnic pe durata perioadei de stabilizare: Contractantul trebuie să furnizeze servicii de suport tehnic intensiv pentru toate incidentele operaționale care pot apărea în perioada de stabilizare post-livrare a sistemului, până la finalizarea testului de acceptanță definitivă.
DEL 011	M	Asistență în testarea de acceptanță: Contractantul va asigura suport activ pentru ANSC în cadrul fazei de testare UAT (User Acceptance Testing), inclusiv remedierea în timp real a disfuncționalităților și sprijin pentru validarea finală a funcționalităților critice.
DEL 012	M	Asistență în migrarea sistemului în mediu de producție: Contractantul este responsabil de asistarea ANSC în procesul de lansare în producție, inclusiv prin verificări finale, tuning de performanță, validarea configurărilor și sprijin în transmiterea proceselor către sistemul live.
DEL 013	M	Corectarea deficiențelor identificate post-livrare: Contractantul trebuie să remedieze toate erorile și neconformitățile semnalate în perioada de stabilizare și în perioada de garanție contractuală, cu respectarea SLA-ului stabilit și a standardelor în vigoare.
DEL 014	M	Servicii de suport post-implementare timp de 9 luni: După punerea în producție, contractantul va furniza asistență tehnică completă (mentenanță corectivă, adaptivă și preventivă), în conformitate cu standardul SM ISO/IEC 14764:2015 – *Software Engineering. Software Life Cycle Processes – Maintenance*.