APROBAT:
Dumitru OBADĂ,
Președintele Consiliului
Superior al Procurorilor

Digitally signed by Obadă Dumitru
Date: 2026.06.09 14:11:34 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

CONSILIUL SUPERIOR AL PROCURORILOR

CAIET DE SARCINI

Elaborare specificațiilor tehnice pentru proiectarea, dezvoltarea, configurarea și implementarea

Sistemului Informațional „e-CSP”

INTRODUCERE

ACRONIME ȘI DEFINIȚII

Lista acronimelor utilizate în prezentul document:

#	Acronim	Descriere
1.	API	Interfața de programare a aplicațiilor (EN: Application Programming Interface)
2.	CMS	Sistem de administrare a conținutului
3.	BD	Bază de date
4.	HTTPS	Protocol de transfer hipertext securizat
5.	TIC	Tehnologia informației și comunicațiilor
6.	SI	Sistem informațional
7.	FRQ	Cerință funcțională;
8.	NFRQ	Cerințe non-funcționale
9.	SO	Sistem de operare
10.	JSON	Notarea obiectelor JavaScript
11.	SOAP	Protocol simplu de acces la obiect
12.	SQL	Limbaj de interogare structurat
13.	WSDL	Limbaj de descriere a serviciilor web
14.	XML	Limbaj de marcare extensibil
15.	e-CSP	Sistemul Informațional e-CSP
16.	RSP	Registrul de Stat al Populației
17.	CSP	Consiliul Superior al Procurorilor
18.	CSEP	Colegiul pentru selecția și evaluarea procurorilor
19.	CDE	Colegiului de Disciplină și Etică
20.	IP	Inspecția Procurorilor
21.	CNPDCP	Centrul Național pentru Protecția Datelor cu Caracter Personal
22.	STISC	Serviciul Tehnologia Informației și Securitate Cibernetică
23.	AGE	Agenția de Guvernare Electronică
24.	MUD	Modelul Unitar de Design

Tabelul de mai jos conține lista definițiilor utilizate în prezentul document:

#	Acronim	Descriere
1.	Actor	Entitate (persoană, rol instituțional sau sistem) care interacționează cu sistemul informațional pentru a iniția sau participa la realizarea unui Use Case
2.	Componentă	Orice subsistem, modul sau subset al Sistemului identificat ca parte integrantă a Sistemului.
3.	Bază de date	O colecție de date organizată în conformitate cu o structură conceptuală bine definită, care descrie caracteristicile de bază și relația dintre entități.
4.	Jurnalizare	Funcția de înregistrare a informațiilor despre evenimentele care au loc într-un sistem. În sistemele informaționale, înregistrarea evenimentelor include detalii despre data, ora, utilizatorul și acțiunea realizată.
5.	Flux de lucru	O serie de sarcini realizate cu scopul de a produce un rezultat dorit, care presupune, de regulă, mai mulți participanți și mai multe etape într-o organizație.
6.	Sistem informatic (SI)	Ansamblu de programe și echipamente care asigură prelucrarea automată a datelor.

7.	Caz de utilizare (UC – Engl. Use Case)	Scenariu de interacțiune dintre un actor și sistemul informațional, care descrie pașii necesari pentru realizarea unei funcționalități specifice din perspectiva utilizatorului.
8.	Cerință funcțională (FR – Engl. Functional Requirement)	Descriere a unei funcționalități pe care sistemul trebuie să o realizeze, exprimată în termeni de acțiuni, procese sau servicii oferite utilizatorilor.
9.	Cerință non-funcțională (NFR – Engl. Non-Functional Requirement)	Descriere a condițiilor și criteriilor de calitate pe care sistemul trebuie să le respecte în funcționare (ex. securitate, performanță, disponibilitate).
10.	Sistem informațional	Sistem de prelucrare a informațiilor, împreună cu resursele organizaționale aferente, cum ar fi resursele umane și tehnice, care furnizează și distribuie date/informații.
11.	Beneficiar	În contextul prezentului document, Beneficiarul este CSP.
12.	Log-uri (jurnale de sistem)	Înregistrări automate ale acțiunilor și evenimentelor din sistem, utilizate pentru monitorizare, trasabilitate și audit.

CONTEXT

Consiliul Superior al Procurorilor, în calitate de organ independent, reprezentativ și de autoadministrare al procurorilor, exercită atribuții esențiale în garantarea independenței și imparțialității procurorilor, precum și în administrarea proceselor de carieră, evaluare și disciplină din cadrul sistemului Procuraturii. În acest context instituțional, modernizarea infrastructurii digitale și optimizarea fluxurilor administrative reprezintă o condiție esențială pentru creșterea transparenței, eficienței operaționale și calității procesului decizional.

Proiectul „e-CSP” constituie răspunsul strategic al CSP la necesitatea digitalizării integrate a proceselor interne, prin implementarea unui sistem informațional unitar care să susțină managementul documentelor, digitalizarea dosarelor disciplinare (e-Disciplinară) și a proceselor de selecție și evaluare a performanțelor profesionale ale procurorilor (e-carieră). Sistemul informațional „e-CSP” va asigura automatizarea fluxurilor de lucru, trasabilitatea completă a operațiunilor, raportare centralizată, interoperabilitate cu registrele și platformele guvernamentale, repartizarea aleatorie a sesizărilor la nivelul Inspecției procurorilor, a cauzele disciplinare la nivelul Colegiului de disciplină și etică și a cererilor/dosarelor de evaluare și selecție la nivelul Colegiului pentru selecția și cariera procurorilor, precum și fundamentarea deciziilor pe bază de date, cu respectarea strictă a cerințelor de securitate și confidențialitate.

Inițiativa se aliniază priorităților și angajamentelor asumate de Republica Moldova în cadrul documentelor strategice și de politici publice naționale și europene, inclusiv:

- Programului Național de Aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025–2029 (HG nr. 306/2025, Cluster 1 – Valori fundamentale, Capitolul 23 „Justiție și drepturile fundamentale”), care prevede digitalizarea completă a proceselor administrative și judiciare;
- Foii de parcurs pentru Statul de Drept 2023–2025 (HG nr. 275/2025), care include dezvoltarea software-ului intern pentru digitalizarea dosarelor disciplinare și a dosarelor de selecție și evaluare ale procurorilor;
- Cadrului Bugetar pe Termen Mediu pentru anii 2026–2028, care prevede implementarea soluției informatice „e-CSP” ca măsură prioritară pentru digitalizarea proceselor administrative și operaționale ale CSP;
- Agendei de reforme aferente Planului de creștere al Republicii Moldova pentru anii 2025–2027, care subliniază necesitatea investițiilor în digitalizarea serviciilor publice și consolidarea capacității administrative;

- Strategiei de Transformare Digitală a Republicii Moldova 2023–2030 și Programului de implementare 2025–2027, care promovează dezvoltarea infrastructurilor digitale sigure, interoperabile și durabile în sectorul public.

I. SCOPUL DOCUMENTULUI

1.1. Scopul prezentului caiet de sarcini

Prezentul Caiet de Sarcini are ca scop definirea cadrului tehnic, funcțional, operațional și organizațional pentru proiectarea, dezvoltarea, implementarea și punerea în exploatare a CSP, destinat digitalizării activităților CSP și ale entităților afiliate acestuia.

Documentul stabilește cerințele obligatorii pe care trebuie să le respecte soluția informatică propusă, precum și condițiile de realizare a proiectului, în vederea asigurării conformității cu legislația aplicabilă, regulamentele interne și standardele relevante în domeniul sistemelor informaționale publice.

1.2. Scopul SI e-CSP

Scopul SI e-CSP constă în digitalizarea integrală, standardizarea și automatizarea proceselor administrative, disciplinare și de gestionare a carierei procurorilor, aflate în competența CSP și a organismelor sale din subordine.

Prin implementarea SI e-CSP se urmărește:

- Asigurarea unei gestionări unitare și trasabile a documentelor și dosarelor;
- Creșterea eficienței operaționale și reducerea dependenței de procese manuale;
- Respectarea strictă a termenelor procedurale prevăzute de legislație și regulamente;
- Consolidarea mecanismelor de transparență și responsabilitate instituțională;
- Protejarea confidențialității și integrității datelor sensibile gestionate de CSP.

1.3. Obiectivele generale ale proiectului

Obiectivele generale ale proiectului de implementare a SI e-CSP sunt:

- Crearea unei platforme informatice integrate, bazate pe module interoperabile, care să susțină activitatea CSP și a organismelor din subordine;
- Digitalizarea completă a fluxurilor de lucru aferente activităților disciplinare, de carieră și administrative;
- Implementarea unui sistem de arhivă electronică securizată, cu evidență și trasabilitate completă;
- Asigurarea unui cadru tehnic care să permită auditarea tuturor acțiunilor efectuate în sistem;
- Integrarea cu platformele guvernamentale partajate relevante precum MPass, MSign, MNotify, MLog ș.a.

Pentru atingerea acestor obiective, SI e-CSP va integra următoarele 3 module:

1. Integrarea e-CSP cu e-Management CSP existent al documentelor – modul care va institui managementul integral al documentelor și arhivarea digitală.
2. e-Disciplinară – modul care va facilita digitalizarea integrală a dosarului disciplinar de la momentul înregistrării sesizării (care va fi inițial înregistrată în e-Managementul documentelor) până la pronunțarea hotărârii finale (definitive/irevocabile).
3. e-Carieră – modulul conceput pentru a gestiona și optimiza administrarea carierei profesionale a procurorilor.

1.4. Obiective specifice

În mod specific, CSP va urmări:

- Automatizarea proceselor de înregistrare, repartizare, examinare și soluționare a sesizărilor disciplinare;
- Gestionarea digitală a dosarelor profesionale ale procurorilor și a procedurilor de selecție, evaluare și promovare;
- Asigurarea repartizării aleatorii a sesizărilor și dosarelor/cererilor, în conformitate cu prevederile legale;
- Generarea de rapoarte, statistici și indicatori de performanță pentru sprijinirea procesului decizional;
- Asigurarea unui nivel ridicat de securitate cibernetică și protecție a datelor cu caracter personal.

Astfel cele 3 module vor îndeplini următoarele funcții specifice:

1. *Integrarea e-Management CSP existent al documentelor*:
   - Gestionare a fluxurilor de lucru și nomenclatoarelor, care coordonează procesul de creare, revizuire și aprobare a documentelor și nomenclatoarelor, optimizând fluxurile de lucru și colaborarea între utilizatori;
   - Stocare digitală, care va permite arhivarea documentelor într-un format electronic, asigurând accesibilitatea și protecția acestora;
   - Căutare și acces, care oferă funcționalități avansate de căutare și acces rapid la documente, bazate pe criterii de clasificare și ierarhizarea documentelor;
   - Audit, monitorizare și executare, care permite înregistrarea, monitorizarea și executarea acțiunilor efectuate asupra documentelor, oferind trasabilitate și posibilitatea de a realiza audituri;
   - Notificarea privind actualizarea documentelor, elaborarea altora noi sau repartizarea spre executare;
   - Securitate și confidențialitate, care asigură controlul accesului în funcție de permisiuni și roluri utilizatorilor;
   - Integrare cu alte sisteme, care permite integrarea cu alte aplicații și sisteme informaționale, facilitând schimbul de informații și sincronizarea datelor între diferite platforme;
   - Generare de rapoarte și analize.

2. *e-Disciplinară*:
   - Stocarea și gestionarea digitală a informației unui dosar disciplinar;
   - Repartizarea aleatorie a sesizărilor la nivelul Inspecției procurorilor (imperativ normat de Legea nr. 3/2016 cu privire la Procuratură), măsură care se va aplica inclusiv la nivelul Colegiului de disciplină și etică și al CSP pentru desemnarea raportorilor pe cauze disciplinare;
   - Digitalizate tuturor procesele interne aferente procedurii disciplinare, inclusiv: notificări/citații, depunerea declarațiilor, solicitarea și primirea referințelor, cererile de recuzare/declarațiile de abținere; gestionarea materialelor acumulate și alte operațiuni conexe.

3. *e-Carieră*:
   - Managementul dosarelor, care centralizează și digitalizează informațiile personale și profesionale ale procurorilor, ce vizează date și materiale aferent evaluării profesionale și traseul profesional;
   - Facilitează gestionarea proceselor de evaluare și selecție ale procurorilor;
   - Repartizarea aleatorie a cererilor de evaluare și selecție a procurorilor;
   - Raportare și analiză, care furnizează rapoarte și analize detaliate despre concursuri organizate și rezultatele acestora (participanți, criteriu de gen, procuratură, ș.a.), evaluări efectuate și alte aspecte relevante pentru managementul resurselor umane;
   - Integrare cu alte sisteme pentru preluarea datelor necesare în procesul de evaluare și selecție.

1.5. Publicul-țintă al documentului

Prezentul Caiet de Sarcini este destinat următoarelor categorii de utilizatori:

- Membrilor CSP, membrilor organelor colegiale și inspectorilor din cadrul Inspecției procurorilor, pentru validarea obiectivelor și a direcției strategice;
- Structurilor operaționale ale CSP, pentru înțelegerea funcționalităților și a impactului sistemului;
- Ofertanților și furnizorilor de soluții informatice, pentru elaborarea ofertelor tehnice și financiare;
- Echipelor de implementare și administrare, pentru asigurarea conformității soluției livrate cu cerințele stabilite.

II. DOMENIUL DE APLICARE AL PROIECTULUI

2.1. Domeniul general de aplicare

Prezentul proiect vizează proiectarea, dezvoltarea, implementarea, testarea și punerea în exploatare a SI e-CSP, ca soluție informatică integrată, destinată susținerii activităților CSP și ale entităților funcționale ale acestuia.
Domeniul de aplicare al proiectului acoperă integral ciclul de viață al sistemului informatic, în conformitate cu bunele practici și standardele relevante privind dezvoltarea și exploatarea sistemelor informatice în sectorul public.

2.2. Activități incluse în proiect

În cadrul prezentului proiect sunt incluse, fără a se limita la, următoarele activități:

- Analiza detaliată a proceselor operaționale, procedurale și administrative ale CSP și ale entităților subordonate, în măsura în care acestea sunt reflectate în cerințele funcționale ale sistemului;
- Proiectarea arhitecturii logice și fizice a SI e-CSP;
- Dezvoltarea modulelor funcționale prevăzute în prezentul caiet de sarcini, inclusiv componentele comune ale sistemului;
- Implementarea mecanismelor de securitate, audit, trasabilitate și control al accesului;
- Integrarea sistemului cu platformele guvernamentale naționale relevante și cu alte sisteme informatice indicate în document;
- Testarea funcțională, de performanță și de securitate a soluției dezvoltate;
- Instalarea și configurarea sistemului în mediile stabilite (test și producție);
- Instruirea utilizatorilor desemnați și a personalului tehnic implicat;
- Asigurarea suportului post-implementare și remedierea eventualelor neconformități constatate în perioada de garanție.

2.3. Activități excluse din proiect

Următoarele activități nu fac obiectul prezentului caiet de sarcini, cu excepția cazului în care sunt explicit prevăzute în mod contrar:

- Modificarea cadrului legislativ sau a regulamentelor interne ale CSP;
- Redefinirea proceselor de fond din punct de vedere juridic sau decizional;
- Furnizarea de infrastructură hardware care nu este explicit menționată ca responsabilitate a furnizorului;
- Operarea curentă a sistemului după expirarea perioadei de suport contractual;

- Introducerea sau migrarea de date istorice, cu excepția cazurilor explicit definite în cerințele funcționale;
- Furnizarea de servicii de mentenanță pe termen lung, peste perioada contractuală stabilită.

2.4. Limite de responsabilitate instituțională

Responsabilitățile în cadrul proiectului sunt delimitate după cum urmează:

- CSP este responsabil pentru definirea cerințelor funcționale, validarea livrabilelor și acceptanța soluției informatice;
- Entitățile funcționale ale CSP **(**Colegiile, Inspecția procurorilor, Aparatul CSP) participă la validarea proceselor și la testarea funcționalităților aferente competențelor proprii;
- Structura IT a CSP, în cooperare cu entitățile desemnate (ex. STISC, după caz), asigură suportul tehnic instituțional și administrarea infrastructurii puse la dispoziție;
- Furnizorul este responsabil pentru livrarea end-to-end a soluției informatice, în conformitate cu cerințele prezentului caiet de sarcini, inclusiv pentru calitatea codului, respectarea termenelor și conformitatea tehnică.

2.5. Ipoteze și constrângeri

Implementarea proiectului se realizează în baza următoarelor ipoteze și constrângeri:

- Procesele operaționale și procedurale existente sunt considerate valide și nu fac obiectul reinterpretării sau modificării de fond;
- Soluția informatică trebuie să respecte legislația în vigoare privind protecția datelor cu caracter personal și securitatea informațională;
- Integrarea cu platformele guvernamentale se va realiza în limita interfețelor și condițiilor tehnice puse la dispoziție de administratorii acestora;
- Orice modificare semnificativă a cerințelor va fi gestionată printr-un mecanism formal de management al schimbărilor, conform prevederilor contractuale.

III. CADRUL LEGAL ȘI NORMATIV

3.1. Cadrul legislativ general

SI e-CSP va fi proiectat, dezvoltat și exploatat în strictă conformitate cu legislația în vigoare a Republicii Moldova, aplicabilă activității CSP, precum și cu actele normative care reglementează funcționarea sistemelor informaționale publice.
Implementarea soluției informatice nu trebuie să contravină și nu poate substitui prevederile legale sau regulamentare existente, sistemul având rol exclusiv de suport tehnic și operațional pentru procesele instituționale reglementate.

3.2. Acte legislative aplicabile

În cadrul proiectării și implementării SI e-CSP se va ține cont, în mod obligatoriu, de următoarele acte legislative, fără a se limita la acestea:

- Legea nr. 3/2016 cu privire la Procuratură, cu modificările și completările ulterioare;
- Legea nr. 252/2023 privind evaluarea externă a judecătorilor și procurorilor și modificarea unor acte normative;
- Legea nr. 195/2024 privind protecția datelor cu caracter personal;
- Legea nr. 467/2003 privind informatizarea și resursele informaționale de stat;
- Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere;

- Legea nr. 1069/2000 cu privire la informatică;
- Legea nr. 71/2007 cu privire la registre;
- Legea nr. 142/2018 privind schimbul de date și interoperabilitatea;
- HG nr.260/2025 privind aprobarea Agendei de reforme aferente Planului de creștere al Republicii Moldova pentru anii 2025-2027;
- HG nr.306/2025 privind aprobarea Programului Național de Aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029;
- HG nr. 308/2025 privind aprobarea Strategiei de Transformare Digitală a Republicii Moldova 2023–2030 și Programul de implementare 2025–2027 al Strategiei de Transformare Digitală;
- HG nr.1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass);
- HG nr.405/2014 privind serviciul electronic guvernamental integrat de semnătură electronică (MSign);
- HG nr.376/2020 pentru aprobarea Conceptului serviciului guvernamental de notificare electronica (MNotify) și a Regulamentului privind modul de funcționare și utilizare a serviciului guvernamental de notificare electronică (MNotify);
- HG nr.211/2019 privind platforma de interoperabilitate (MConnect);
- HG nr.708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog);
- HG nr.128/2014 privind platforma tehnologică guvernamentală comună (MCloud);
- alte acte normative incidente, aplicabile domeniului de activitate al CSP și sistemelor informaționale publice.

3.3. Regulamente și acte normative interne

SI e-CSP trebuie să fie aliniat și să susțină aplicarea prevederilor regulamentelor interne ale CSP și ale entităților funcționale, inclusiv, dar fără a se limita la:

- Regulamentul cu privire la organizarea și funcționarea Consiliului Superior al Procurorilor;
- Regulamentul cu privire la organizarea și funcționarea Colegiului de disciplină și etică ;
- Regulamentul cu privire la procedura de selecție și evaluare a procurorilor și funcționarea Colegiului pentru selecția și evaluarea procurorilor;
- Regulamentul cu privire la organizarea și funcționarea Inspecției procurorilor;
- Regulamentul de organizare și funcționare a Aparatului CSP;
- alte regulamente, instrucțiuni sau proceduri interne aprobate de CSP, relevante pentru domeniul de aplicare al sistemului.

Aceste documente constituie baza procedurală pentru definirea fluxurilor de lucru, a rolurilor și a drepturilor de acces în cadrul sistemului informațional.

3.4. Standarde și cadre de referință

În dezvoltarea și implementarea SI e-CSP se vor respecta bunele practici și standardele recunoscute în domeniul sistemelor informaționale, inclusiv:

- Standardele internaționale privind ciclul de viață al software-ului (ex. ISO/IEC 12207);
- Principiile de securitate informațională și management al riscurilor (ex. ISO/IEC 27001 – ca referință);
- Recomandările și ghidurile naționale privind dezvoltarea sistemelor informaționale guvernamentale;
- Politicile de interoperabilitate și e-guvernare promovate la nivel național.

Aplicarea acestor standarde are rolul de a asigura calitatea, securitatea, scalabilitatea și sustenabilitatea soluției informatice.

3.5. Conformitate, audit și responsabilitate juridică

Furnizorul soluției informatice este obligat să asigure conformitatea tehnică a SI e-CSP cu cadrul legal și normativ menționat, inclusiv prin implementarea mecanismelor de:

- Trasabilitate completă a acțiunilor efectuate în sistem;
- Monitorizarea accesului și a modificărilor de date;
- Protecție a datelor cu caracter personal și a informațiilor sensibile;
- Respectare a principiilor de confidențialitate, integritate și disponibilitate a informației.

Responsabilitatea juridică asupra deciziilor de fond rămâne exclusiv în sarcina organelor competente ale CSP, sistemul informatic având un rol strict instrumental și suportiv.

IV. ROLURI ȘI RESPONSABILITĂȚI

4.1. Principii generale privind rolurile și responsabilitățile

SI e-CSP este destinat utilizării de către CSP și de către organele aflate în subordinea sau în coordonarea acestuia, în limitele competențelor stabilite prin legislația în vigoare și regulamentele interne aprobate.

Definirea rolurilor și responsabilităților în cadrul sistemului urmărește respectarea următoarelor principii:

- Separarea competențelor instituționale și funcționale;
- Utilizarea sistemului exclusiv ca instrument de suport, fără substituirea atribuțiilor legale;
- Controlul accesului bazat pe roluri și competențe legale;
- Asigurarea trasabilității și auditabilității tuturor acțiunilor efectuate;
- Protejarea confidențialității informațiilor și a datelor cu caracter personal.

4.2. Consiliul Superior al procurorilor (CSP)

CSP este autoritatea de autoadministrare a procurorilor și exercită competențele stabilite de lege și de regulamentele interne proprii.

În cadrul SI e-CSP, CSP are rol de owner funcțional global, cu următoarele responsabilități principale:

- Aprobarea cadrului funcțional general al sistemului și a politicilor de utilizare;
- Validarea cerințelor funcționale și a modificărilor majore;
- Acceptanța livrabilelor și a etapelor de implementare;
- Utilizarea sistemului pentru gestionarea documentelor, dosarelor și deciziilor aferente competențelor sale legale;
- Asigurarea guvernanței funcționale a sistemului.

Sistemul nu substituie atribuțiile decizionale ale CSP, acestea fiind exercitate exclusiv de către membrii Consiliului, conform cadrului legal.

4.3. Inspecția procurorilor

Inspecția procurorilor este organ funcțional din subordinea CSP, cu atribuții specifice în domeniul verificării și investigării sesizărilor disciplinare, conform regulamentului aprobat.

În cadrul SI e-CSP, Inspecția procurorilor are rol de owner operațional pentru modulul e-Disciplinară (descris în capitolul VII), fiind responsabil pentru:

- Înregistrarea și gestionarea sesizărilor disciplinare;
- Inițierea, formarea și administrarea dosarelor disciplinare în format electronic și a materialelor procedurale, de la înregistrarea sesizării până la transmiterea dosarului către CDE, inclusiv gestionarea dosarelor retrimise/recepționate de la CDE în aceleași condiții de evidență și procedură.
- Respectarea termenelor procedurale stabilite;
- Transmiterea dosarelor către colegiul de disciplină și etică, conform etapelor procedurale;
- Extragerea istoricului disciplinar al unui procuror, după caz;
- Asigurarea trasabilității complete a activităților desfășurate.

Inspectorul-șef, suplimentar atribuțiilor manageriale exercitate în cadrul Inspecției procurorilor, poate desfășura și activități funcționale aferente rolului de inspector, inclusiv examinarea dosarelor disciplinare și exercitarea atribuțiilor procedurale corespunzătoare. Sistemul informațional e-CSP va reflecta această particularitate prin aplicarea unor reguli diferențiate de repartizare și calcul al încărcării, conform cadrului normativ aplicabil.

4.4. Colegiul de disciplină și etică (CDE)

Colegiul de disciplină și etică este organ funcțional din subordinea CSP, care își exercită competențele stabilite de lege și își desfășoară activitatea în baza regulamentului propriu.

În cadrul SI e-CSP, CDE este owner-ul funcțional principal pentru modulul e-Disciplinară (descris în capitolul VII), având următoarele responsabilități:

- Examinarea cauzelor disciplinare și a materialelor aferente, în format electronic;
- Utilizarea sistemului pentru gestionarea ședințelor colegiului, deliberărilor și deciziilor;
- Administrarea dosarelor disciplinare electronice și a materialelor procedurale;
- Accesarea dosarelor disciplinare, a documentelor și a istoricului acțiunilor;
- Extragerea istoricului disciplinar al unui procuror, după caz;
- Respectarea cerințelor de confidențialitate și protecție a datelor.

Sistemul informatic nu intervine în procesul decizional al colegiului și nu generează automat soluții disciplinare.

4.5. Colegiul pentru selecția și evaluarea procurorilor (CSEP)

Colegiul pentru selecția și evaluarea procurorilor care își exercită competențele stabilite de lege și își desfășoară activitatea în baza regulamentului propriu.

În cadrul SI e-CSP, CSEP este owner-ul funcțional principal pentru modulul e-Carieră (descris în capitolul VII)**,** având următoarele responsabilități:

- Gestionarea procedurilor de selecție, evaluare și promovare a procurorilor;
- Utilizarea sistemului pentru examinarea dosarelor profesionale și a documentelor aferente;
- Gestionarea ședințelor colegiului și a actelor adoptate;
- Utilizarea rapoartelor și evidențelor generate de sistem în procesul decizional.

4.6. Aparatul CSP

Aparatul CSP este o subdiviziune structurală a CSP, având misiunea de a asigura asistenţă administrativă, metodică, analitică și logistică CSP și organelor din subordinea acestuia.

În cadrul SI e-CSP, Aparatul CSP are rol operațional și de suport, în special pentru:

- Gestionarea fluxurilor documentare și a registraturii electronice;
- Administrarea documentelor instituționale și a arhivei electronice;
- Pregătirea materialelor pentru ședințele CSP și ale colegiilor;
- Suport administrativ pentru utilizatorii sistemului.

4.7. Structura IT a CSP și entitățile tehnice desemnate

Structura IT a CSP, precum și entitățile tehnice desemnate, sunt responsabile pentru administrarea tehnică a SI e-CSP, în limitele mandatului acordat.

Responsabilitățile includ:

- Administrarea conturilor de utilizator și a drepturilor de acces, conform deciziilor CSP;
- Asigurarea funcționării continue a sistemului;
- Implementarea măsurilor de securitate informațională;
- Monitorizarea, backup-ul și restaurarea sistemului.

Structura IT nu are competențe asupra conținutului procedural sau decizional al datelor gestionate în sistem.

4.8. Furnizorul soluției informatice

Furnizorul soluției informatice este responsabil pentru dezvoltarea, implementarea și livrarea SI e-CSP în conformitate cu cerințele prezentului caiet de sarcini.

Furnizorul:

- Asigură calitatea soluției și respectarea termenelor contractuale;
- Remediază neconformitățile identificate în perioada de garanție;
- Furnizează documentația și instruirea necesară.

Furnizorul nu are acces la datele operaționale ale sistemului în exploatarea curentă, cu excepția situațiilor expres autorizate, documentate și limitate.

4.9. Principii de control și delimitare a responsabilităților

Pentru toate categoriile de actori se aplică următoarele principii:

- Accesul la sistem se acordă strict pe bază de rol și competență legală;
- Toate acțiunile sunt jurnalizate și auditabile;
- Drepturile de acces sunt revizuite periodic;
- Separarea rolurilor este menținută pentru prevenirea conflictelor de interese.

Detalierea responsabilităților și a relațiilor dintre actori va fi prezentată în Anexa C, parte integrantă a prezentului document.

V. ARHITECTURA SISTEMULUI ȘI FLUXURI OPERAȚIONALE A SI E-CSP

5.1. Model arhitectural general

Sistemul informațional e-CSP va fi implementat ca aplicație web instituțională, destinată gestionării electronice a procedurilor aflate în competența CSP. Arhitectura sistemului va asigura separarea clară între funcția de registratură oficială și funcția de gestionare procedurală internă.

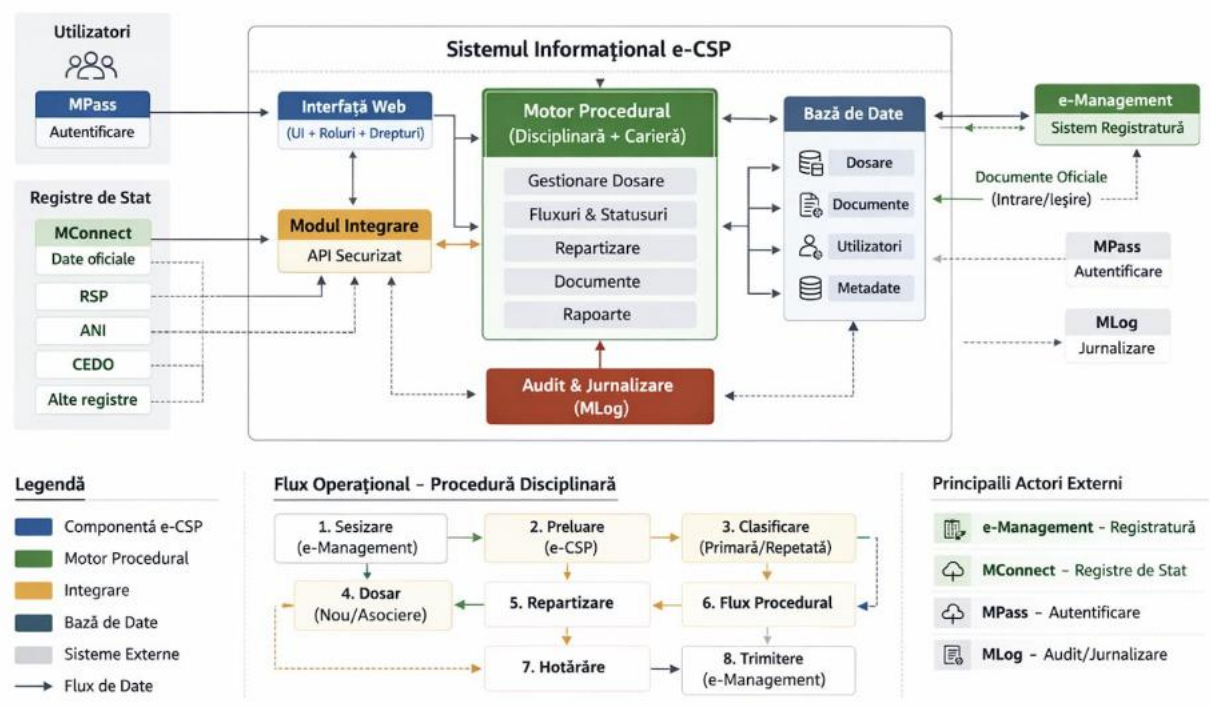
În acest model (Figură 1):

- e-Management CSP existent, rămâne sistemul oficial de evidență și numerotare a documentelor (intrare/ieșire, corespondență externă);
- e-CSP gestionează exclusiv fluxurile procedurale interne (disciplinare, carieră, evaluare), fără a replica sau substitui registratura oficială.

Sistemul e-CSP va include următoarele componente logice:

- Interfață web securizată pentru utilizatori (acces controlat prin MPass);
- Motor procedural pentru administrarea etapelor și statutelor dosarelor;
- Modul de gestionare a documentelor (atașare, versionare, integritate);
- Modul de integrare externă (e-Management, MConnect, alte registre);
- Modul de audit și jurnalizare;
- Bază de date relațională pentru stocarea informațiilor.

Această structură permite gestionarea integrală a procedurilor în format digital, cu trasabilitate completă și control instituțional asupra datelor.



Figură 1. Arhitectura Sistemului Informațional e-CSP

5.2. Flux operațional principal – Procedură disciplinară

Fluxul procedural disciplinar va funcționa după următorul model:

1. Sesizarea este înregistrată oficial în e-Management.
2. e-CSP preia sesizarea prin integrare automată.
3. Secretariatul stabilește tipul sesizării (primară / repetată / analogică).
4. Sistemul:

    - creează dosar disciplinar nou (pentru sesizare primară); sau
    - asociază sesizarea la un dosar existent (pentru repetată/analogică).
5. Se aplică mecanismul de repartizare conform regulilor stabilite.
6. Etapele procedurale sunt gestionate integral în e-CSP.
7. Hotărârea finală este generată în e-CSP.
8. Documentul este transmis către e-Management pentru înregistrare oficială și comunicare externă.

Toate acțiunile sunt înregistrate și auditabile.

5.3. Integrare și interoperabilitate

Sistemul va interopera cu infrastructura guvernamentală existentă, inclusiv:

- e-Management – pentru transmiterea și recepționarea documentelor oficiale;
- MConnect – pentru preluarea datelor din registrele de stat;
- MPass – pentru autentificare;
- MSign – pentru semnarea electronică a dosarelor, scrisorilor rezoluțiilor în cadrul e-CSP și modulele acestuia;
- MLog – pentru jurnalizare, unde este aplicabil;
- MNotify – pentru expedierea notificărilor, unde este aplicabil.

Schimburile de date se vor realiza prin mecanisme securizate, fără replicarea registrelor externe și fără duplicarea numerotării oficiale.

5.4. Principii arhitecturale obligatorii

Sistemul trebuie să respecte următoarele principii:

- Separare clară între registratură și motor procedural;
- Identificatori unici interni pentru dosare;
- Interzicerea duplicării registrelor oficiale;
- Versionare documente și control al integrității;
- Audit complet și imuabil al acțiunilor;
- Performanță maxim 3 secunde pentru operațiuni standard.

5.5. Clasificarea utilizatorilor sistemului

Sistemul e-CSP va gestiona următoarele categorii de utilizatori:

1. Utilizatori interni (CSP și structuri aferente)
    - Membrii CSP
    - Inspectori și personalul Inspecției procurorilor
    - Membrii CDE și CSEP
    - Secretariat și personal administrativ
2. Utilizatori externi
    - Procurori (în afara aparatului CSP)
    - Persoane fizice sau juridice care depun sesizări
    - Alte instituții publice prin integrare (API / MConnect)
3. Utilizatori tehnici
    - Administratori de sistem
    - Personal IT CSP / operatori tehnici
    - Furnizorul (în limite contractuale)
4. Utilizatori de audit și control
    - Auditori interni
    - Instituții de control autorizate

Principii:

- autentificare prin MPass pentru utilizatorii identificați
- acces diferențiat bazat pe roluri (RBAC)
- jurnalizare completă prin MLog
- separarea clară a accesului intern vs extern

VI. CERINȚELE FUNCȚIONALE FAȚĂ DE SI E-CSP

6.1. Modulul de integrare cu e-Management CSP existent

Modulul implementează un model hibrid în care e-Management CSP existent rămâne sistemul oficial de registratură și corespondență externă (numerotare, intrare/ieșire, expediere, arhivare), iar e-CSP gestionează exclusiv fluxurile procedurale interne, fără a replica sau substitui funcționalitățile e-Management.

Integrarea este bidirecțională și se realizează prin API securizat, fără duplicarea registrelor și fără generarea numerelor oficiale în e-CSP. În acest cadru, e-CSP:

- preia documente relevante înregistrate în e-Management CSP existent pentru inițierea/actualizarea dosarelor interne;
- transmite către e-Management documente rezultate și actualizări de status;
- inițiază scrisori oficiale din fluxurile procedurale și le transmite către e-Management CSP pentru înregistrare și expediere către destinatari externi;
- menține corelarea între numărul oficial din e-Management CSP și dosarul procedural din e-CSP (identificator unic e-CSP creat: ID-eCSP-xxx), cu trasabilitate completă.

Modulul nu permite modificarea documentelor înregistrate în e-Management CSP existent și nu interferează cu fluxurile interne ale acestuia.

6.1.1. Actorii modulului de integrare cu e-Management CSP existent

Modulul va implica următorii actori:

Sistem e-Management CSP (sistem existent în cadrul CSP) – Inițiază transmiterea documentelor înregistrate către e-CSP și primește actualizări de status sau documente rezultate din procesele interne e-CSP.

Sistem e-CSP (serviciu de integrare) – Procesează datele primite, creează corelarea cu dosarele interne și transmite actualizările relevante către e-Management CSP

Secretariat CSP – Vizualizează documentele preluate din e-Management, confirmă corelarea cu dosarele interne (dacă este necesar) și monitorizează statusurile sincronizate. Nu poate modifica datele oficiale provenite din e-Management.

Executor intern (ex. Inspector / Colegiu) – Primește documentele prin intermediul dosarului intern creat în e-CSP și poate declanșa transmiterea statusului final către e-Management.

Responsabil tehnic CSP (IT CSP) – Monitorizează funcționarea integrării, validează configurările și aprobă modificările de integrare, fără a interveni în conținutul documentelor sau fluxurile procedurale.

UC-EM01. Integrare bidirecțională cu sistemul e-Management CSP existent

FR-UC-EM01.01. Recepție și validare documente

Sistemul trebuie să recepționeze prin API documentele și metadatele transmise din e-Management, să valideze câmpurile obligatorii și să respingă mesajele incomplete, cu notificarea motivului respingerii.

FR-UC-EM01.02. Gestionare anexe și verificare fișiere

Sistemul trebuie să recepționeze anexele asociate documentului, să le coreleze automat cu documentul principal și să valideze formatul, dimensiunea și integritatea acestora, inclusiv verificare antivirus, conform parametrilor configurați.

FR-UC-EM01.03. Corelare identificatori și prevenire duplicate

Sistemul trebuie să păstreze legătura unică dintre identificatorul documentului din e-Management și identificatorul intern din e-CSP și să prevină crearea înregistrărilor duplicate pentru același document.

FR-UC-EM01.04. Procesare integrală document și anexe

Sistemul trebuie să asigure că documentul și anexele aferente sunt procesate împreună; în cazul apariției unei erori, operațiunea se anulează complet, fără a rămâne înregistrări parțiale.

FR-UC-EM01.05. Transmitere actualizări către e-Management

Sistemul trebuie să transmită către e-Management actualizările relevante generate în e-CSP, inclusiv statusuri și documente rezultate, conform regulilor stabilite.

FR-UC-EM01.06. Gestionare confirmări și erori

Sistemul trebuie să înregistreze confirmarea primirii mesajelor, să gestioneze situațiile de eroare prin mecanism de retransmitere controlată și să prevină generarea de duplicate.

FR-UC-EM01.07. Evidență stare schimburi

Sistemul trebuie să păstreze pentru fiecare schimb de date starea acestuia (acceptat, respins, eroare), împreună cu identificatorii de corelare.

FR-UC-EM01.08. Jurnalizare și audit

Sistemul trebuie să jurnalizeze toate schimburile de date între e-CSP și e-Management în MLog, inclusiv recepție, transmitere și erori, cu dată, oră și identificatori de corelare.

UC-EM02. Inițiere și expediere scrisori oficiale către instituții externe (prin e-Management). Sistemul va permite executorilor din e-CSP (ex. modul e-Disciplinară) să inițieze scrisori/interpelări oficiale către instituții externe (ex. Inspectoratul Fiscal, bănci comerciale, Procuratura Generală, Guvern, Agenții etc.), direct din dosarul intern, prin transmiterea documentului către e-Management pentru înregistrare, expediere și evidență oficială. e-CSP va recepționa numărul de ieșire și statusurile de expediere, păstrând trasabilitatea în dosarul intern.

FR-UC-EM02-01. Generare solicitare din dosar

Sistemul trebuie să permită inițierea unei solicitări oficiale din cadrul unui dosar (ex. disciplinar), cu selectarea destinatarului, completarea câmpurilor obligatorii și atașarea documentelor suport.

FR-UC-EM02-02. Transmitere către e-Management pentru înregistrare/expediere

Sistemul trebuie să transmită solicitarea și anexele către e-Management prin API, pentru înregistrare oficială ca document de ieșire și expediere prin canalele gestionate de e-Management.

FR-UC-EM02-03. Preluare număr oficial și corelare

Sistemul trebuie să recepționeze din e-Management numărul unic de ieșire și să îl asocieze solicitării din dosar, ca identificator oficial utilizat în căutare, afișare și audit.

FR-UC-EM02-04. Preluare statusuri expediere și livrare

Sistemul trebuie să recepționeze din e-Management statusurile relevante (ex. „Înregistrat”, „Expediat”, „Livrat/Confirmat”, „Eșuat”) și să le afișeze în dosarul intern.

FR-UC-EM02-05. Jurnalizare și trasabilitate

Sistemul trebuie să jurnalizeze în MLog inițierea solicitării, transmiterea către e-Management, recepția numărului oficial și actualizările de status, cu referință la dosar și identificatorii de corelare.

6.2. Modulul e-Disciplinară

Modulul e-Disciplinară asigură gestionarea integrală, în format digital, a procedurii disciplinare aflate în competența CSP, de la preluarea sesizării înregistrate în e-Management până la pronunțarea hotărârii finale (definitive/irevocabile).
Sesizarea înregistrată oficial în e-Management este preluată automat în e-CSP, unde se constituie dosarul disciplinar electronic. Toate etapele procedurale se desfășoară exclusiv în e-CSP, cu păstrarea corelării unice între numărul oficial din e-Management și identificatorul intern al dosarului.
Modulul asigură:

- constituirea și administrarea dosarului disciplinar electronic;
- repartizarea aleatorie a sesizărilor la nivelul Inspecției procurorilor și desemnarea raportorilor în cadrul Colegiului de disciplină și etică și al CSP, conform cadrului normativ aplicabil;
- gestionarea etapelor procedurale (verificare admisibilitate, examinare, audiere, deliberare, adoptare hotărâre);
- generarea și gestionarea notificărilor, citațiilor, declarațiilor, referințelor și a materialelor acumulate;
- monitorizarea termenelor procedurale și alertarea utilizatorilor responsabili;
- înregistrarea votului și a rezultatului deliberării;
- generarea hotărârilor și transmiterea acestora către e-Management pentru înregistrare și comunicare oficială.

Modulul e-Disciplinară asigură trasabilitatea completă a tuturor acțiunilor, prevenirea duplicării dosarelor și menținerea integrității datelor pe întreaga durată a procedurii disciplinare.

6.2.1. Actorii modulului e-Disciplinară

Modulul e-Disciplinară va avea următorii actori:

A-ED01. Secția de profil a Inspecției (subdiviziune a Aparatului CSP) – Secretariatul Inspecției (terminologie folosită pentru acest document)

Rol operațional de registratură specializată pentru Inspecție: înregistrează sesizarea/procesul-verbal, atribuie număr unic și creează dosarul.

A-ED02. Inspector (Inspecția procurorilor)

Executor procedural care efectuează verificarea (prealabilă/în fond), administrează probe, întocmește raport și, dacă există temei, transmite dosarul către CDE.

A-ED03. Inspector-șef (Inspecția procurorilor)

Rol managerial și de control procedural: are acces la dosarele create de secretariatul Inspecției, soluționează incompatibilități/recuzări și poate redistribui dosare.

A-ED04. Registrator / Operator registratură (Aparatul CSP)

Rol de recepție inițială: primește sesizarea și o transmite către secretariatul Inspecției în termenul procedural.

A-ED05. Membru CDE

Rol decizional colegial: examinează cauze disciplinare, deliberează și votează soluții (care se materializează prin hotărâri ale organului colegial).

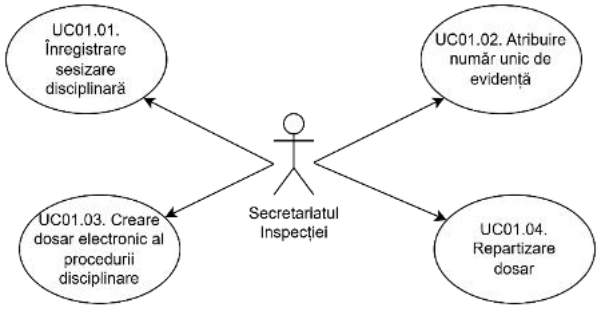
A-ED06. Președintele CDE

Rol de conducere a colegiului: aprobă/gestionează agenda, repartizează dosarele disciplinare către raportori, conduce ședințele, organizează lucrările CDE.

A-ED07. Secretar ședință CDE (funcție de secretariat, subdiviziune din cadrul Aparatului CSP)

Rol operațional pentru ședințe și documentarea lor: minute/procese-verbale, evidența corespondenței, evidența hotărârilor, publicare cu anonimizare (după reguli).

6.2.2. Funcționalitățile aferente actorului Secretariatul inspecției



Figură 2. Diagrama cazurilor de utilizare aferente Secretariatului inspecției

UC-ED01.01. Înregistrare sesizare disciplinară: Sistemul permite Secretariatului să înregistreze o sesizare/raport (inclusiv sesizare din oficiu) în registrul disciplinar, prin completarea câmpurilor obligatorii și atașarea documentelor primite (fișiere/copii scanate). La salvarea înregistrării, sistemul stabilește statusul inițial „Recepționată/Înregistrată", păstrează trasabilitatea acțiunilor și pregătește datele pentru crearea dosarului.

FR-UC-ED01.01-01. Creare înregistrare sesizare. Sistemul trebuie să permită Secretariatului să creeze o înregistrare nouă de sesizare disciplinară în registru, prin completarea unui formular electronic și inițierea unui dosar preliminar (în starea de lucru/„draft").

FR-UC-ED01.01-02. Capturare câmpuri obligatorii și validări. Sistemul trebuie să solicite și să valideze completarea câmpurilor obligatorii pentru sesizare (cel puțin: tip sesizare. petiție/raport/oficiu, data recepționării, canal recepționare, date autor sau marcaj „din oficiu", procuror vizat / entitate vizată, descriere succintă, autor), și să nu permită salvarea ca „înregistrată" dacă lipsesc câmpuri obligatorii.

FR-UC-ED01.01-03. Încărcare și gestionare anexe. Sistemul trebuie să permită Secretariatului să încarce și să atașeze la sesizare documente justificative (fișiere și/sau copii scanate), cu evidență minimă per anexă (denumire, tip document, dată încărcare, utilizator), și să asigure păstrarea acestora în dosar (fără modificare neautorizată).

FR-UC-ED01.01-04. Stabilire status inițial. La salvarea sesizării ca „înregistrată", sistemul trebuie să seteze automat statusul inițial al sesizării la „Recepționată/Înregistrată", să înregistreze data/ora și utilizatorul care a efectuat acțiunea, și să afișeze sesizarea în registrul Secretariatului cu acest status.

FR-UC-ED01.01-05. Clasificarea sesizării. Sistemul trebuie să permită clasificarea sesizării (tip/categorie). La înregistrarea unei sesizări Secretariatul va selecta tip-ul/categoria sesizării dintr-o listă de tip nomenclator.

FR-UC-ED01.01-06. Identificare procuror vizat. Sistemul trebuie să permită selectarea procurorului vizat dintr-o sursă oficială/listă, pentru a preveni erori de identificare (nume duplicat). Secretariatul va selecta procurorul dintr-o listă cu toți procurorii.

FR-UC-ED01.01-08. Validare fișiere (format/dimensiune). Sistemul trebuie să valideze tipurile de fișiere, dimensiunea și să aplice scanare antivirus pentru anexele încărcate. Tipurile și dimensiunile fișierelor acceptate vor fi parametri configurabile de către Administratorul sistemului.

FR-UC-ED01.01-09. Trasabilitate și audit pentru acțiuni. Sistemul trebuie să jurnalizeze în MLog cel puțin următoarele evenimente: crearea sesizării, modificările ulterioare înainte de „înregistrare", încărcarea/ștergerea anexelor (dacă este permisă), și acțiunea de salvare ca „Recepționată/Înregistrată", incluzând utilizator, timestamp și identificatorul intern al sesizării.

UC-ED01.02. Atribuire număr unic de evidență. La prima oficializare a sesizării (trecerea în starea „Recepționată/Înregistrată” conform fluxului), sistemul generează automat un număr unic de evidență conform schemei configurate, îl asociază definitiv sesizării/dosarului și îl utilizează ca identificator principal în căutare, afișare, export și jurnalul de audit. Numărul nu poate fi modificat sau reutilizat.

FR-UC-ED01.02-01. Generare automată la salvare „înregistrată/complet”. Sistemul trebuie să genereze automat un număr unic de evidență pentru sesizare/dosar la prima salvare în stare oficială (ex. „Recepționată/Înregistrată” sau „Complet”, conform fluxului configurat), fără intervenție manuală.

FR-UC-ED01.02-02. Unicitate și secvențialitate conform schemei. Sistemul trebuie să asigure că numărul de evidență este unic la nivelul registrului și este atribuit în ordine crescătoare, conform unei scheme de numerotare configurabile (ex.: an + contor, prefix instituție/structură etc.).

FR-UC-ED01.02-03. Imutabilitate și controlul modificărilor. Sistemul nu trebuie să permită modificarea manuală a numărului unic de evidență după atribuire și trebuie să prevină reutilizarea unui număr atribuit, inclusiv în scenarii de anulare/ștergere logică a înregistrării (numărul rămâne rezervat în audit).

FR-UC-ED01.02-04. Afișare și utilizare ca identificator principal. Sistemul trebuie să afișeze numărul unic de evidență în toate ecranele relevante (registru, detalii dosar, căutare, rapoarte) și să-l folosească drept identificator principal în documentele generate/exportate (PDF/print) și în notificări (dacă există).

FR-UC-ED01.02-05. Audit și tratarea concurenței. Sistemul trebuie să înregistreze în audit evenimentul de atribuire (număr, utilizator, timestamp, înregistrare/dosar asociat) și trebuie să gestioneze concurența (mai mulți utilizatori care salvează simultan) astfel încât să nu apară duplicate sau „sărituri” nejustificate din cauza coliziunilor.

UC-ED01.03. Creare dosar electronic al procedurii disciplinare. Sistemul creează dosarul electronic asociat sesizării înregistrate, ca un „container” unic ce include metadatele cazului, documentele (sesizare, anexe și documente generate de sistem), istoricul acțiunilor și statusurile inițiale ale dosarului până la starea „Complet”. Sistemul permite Secretariatului să vizualizeze și să descarce documentele din dosar (inclusiv fișele de repartizare generate automat), păstrând integritatea și auditul tuturor acțiunilor.

FR-UC-ED01.03-01. Reguli de creare și asociere dosar disciplinar. Sistemul trebuie să creeze automat un dosar disciplinar electronic (CaseID unic) pentru sesizările clasificate ca primare, menținând relația 1:1 între sesizare și dosar.

La etapa de înregistrare inițială a sesizării preluate din e-Management CSP, Secretariatul stabilește tipul sesizării: primară, repetată sau analogică.

Pentru sesizările clasificate ca repetate sau analogice, sistemul nu va crea dosar disciplinar nou, ci le va înregistra ca sesizări asociate unui dosar disciplinar principal existent, păstrând numărul de evidență și referința auditabilă către dosarul principal. În acest caz, relația aplicabilă este N:1 (mai multe sesizări → un dosar principal).
Sistemul trebuie să prevină crearea duplicată a dosarelor pentru același număr de evidență și să înregistreze în audit tipul sesizării stabilit, utilizatorul, data și dosarul principal asociat (dacă este cazul).
FR-UC-ED01.03-02. Metadate minime ale dosarului. Sistemul trebuie să stocheze în dosar un set minim de metadate (cel puțin: număr evidență, tip sesizare: primară, repetată sau analogică, data recepționării, autor/din oficiu, procuror vizat, status curent, termene/repere), astfel încât dosarul să poată fi căutat, filtrat și raportat.

FR-UC-ED01.03-03. Management documente în dosar. Sistemul trebuie să permită atașarea și organizarea documentelor în dosar și să includă în aceeași gestiune documentele generate de sistem (ex.: fișe de repartizare, alte acte procedurale), cu metadate minime per document (tip, denumire, dată/ora, utilizator/proces generator).

FR-UC-ED01.03-04. Istoric fișe de repartizare în dosar. Sistemul trebuie să păstreze în dosar toate fișele de repartizare generate (inițială + re-repartizări + manuală în excepție), ordonate cronologic și legate de evenimentul care le-a generat.

FR-UC-ED01.03-05. Statutele inițiale ale dosarului și tranziții până la „Complet". Sistemul trebuie să gestioneze statutele inițiale ale dosarului și regulile de tranziție (ex.: Schiță → Înregistrat → Complet), inclusiv validările necesare pentru trecerea în „Complet".

FR-UC-ED01.03-06. Istoric acțiuni și audit pe dosar. Sistemul trebuie să păstreze un istoric complet și auditabil al acțiunilor asupra dosarului în MLog (creare, modificări metadate, încărcare/ștergere documente dacă este permis), cu minim: utilizator, timestamp, acțiune și câmpuri/documente afectate.

FR-UC-ED01.03-07. Structură standard a dosarului. Sistemul trebuie să creeze dosarul pe baza unei structuri standard (secțiuni/categorii de documente), pentru a asigura consistență în gestionare și regăsire.

FR-UC-ED01.03-08. Restricții de editare după „Complet". După marcarea dosarului ca „Complet", sistemul trebuie să limiteze modificările permise (doar câmpuri autorizate) și să solicite justificare + audit pentru orice corecție ulterioară.

FR-UC-ED01.03-09. Căutare și filtrare dosare. Sistemul trebuie să permită căutarea și filtrarea dosarelor după metadate esențiale (număr evidență, procuror vizat, status, perioadă, tip sesizare ș.a.), pentru operare și control administrativ.

UC-ED01.04. Repartizare dosar. La salvarea dosarului de către Secretariat, sistemul validează datele minime, determină lista de inspectori eligibili și repartizează aleatoriu dosarul unui inspector. Inspectorul desemnat poate înregistra un refuz cu motiv legal; după fiecare refuz sistemul efectuează automat o re-repartizare aleatorie către un alt inspector eligibil, excluzând inspectorii care au refuzat deja. Dacă toți inspectorii eligibili refuză, sistemul marchează excepția și permite Inspectorului-șef să facă repartizarea manuală. După fiecare repartizare/re-repartizare (și, după caz, manuală), sistemul generează automat fișa de repartizare ca document al dosarului, cu trasabilitate și audit complet.

FR-UC-ED01.04-01. Declanșare automată la „Complet". Sistemul trebuie să execute automat repartizarea dosarului imediat după ce dosarul este salvat în starea „Complet", fără acțiune suplimentară din partea Secretariatului.

FR-UC-ED01.04-02. Repartizare aleatorie. Sistemul trebuie să repartizeze dosarul aleatoriu către un inspector eligibil, folosind un mecanism de randomizare controlat de sistem (fără intervenție manuală în alegere). Sistemul va asigura că, în condiții de utilizare simultană (mai multe dosare completate în același timp), repartizarea se face atomic și nu produce stări inconsistente (ex.: același dosar repartizat simultan la doi inspectori).

FR-UC-ED01.04-03. Determinare listă inspectori eligibili. Sistemul trebuie să determine lista de inspectori eligibili pentru repartizare pe baza regulilor configurate (ex.: activ/în funcție, disponibilitate, rol/competență, excluderi administrative), aplicate consistent pentru fiecare repartizare.

FR-UC-ED01.04-03A. Tratarea Inspectorului-șef în algoritmul de repartizare. Sistemul trebuie să includă Inspectorul-șef în lista inspectorilor eligibili pentru repartizare doar în limitele unei capacități de lucru reduse, corespunzătoare unui volum de activitate de maximum 50% comparativ cu un inspector standard, prin aplicarea unui coeficient de ponderare configurabil în algoritmul de repartizare aleatorie.

FR-UC-ED01.04-04. Excluderea inspectorilor care au refuzat dosarul. Sistemul trebuie să excludă automat din lista de eligibili pentru același dosar orice inspector care a înregistrat deja un refuz pentru acel dosar.

FR-UC-ED01.04-05. Gestionarea refuzului de către inspector (triger pentru re-repartizare). Sistemul trebuie să permită inspectorului desemnat să înregistreze un refuz al dosarului, obligatoriu

cu selectarea/introducerea unui motiv legal (și, dacă este cazul, atașarea documentelor justificative), iar după înregistrare să declanșeze automat re-repartizarea.

FR-UC-ED01.04-06. Cicluri de re-repartizare până la epuizarea eligibililor. Sistemul trebuie să repete procesul de repartizare aleatorie după fiecare refuz, până când:

- dosarul este acceptat implicit (nu există refuz în termenul definit) sau
- se epuizează lista de inspectori eligibili prin refuzuri.

FR-UC-ED01.04-07. Escaladarea dosarului către Inspectorul-șef. Dacă sistemul constată că toți inspectorii eligibili au refuzat dosarul, sistemul trebuie să:

- oprească re-repartizarea automată;
- seteze statusul dosarului la „Necesită repartizare de către Inspectorul-șef” (sau echivalent);
- notifice Inspectorul-șef (și să marcheze vizibil starea de excepție).

Sistemul nu trebuie să permită repartizarea manuală a dosarului către un inspector de către Inspectorul-șef sau alt rol decât în situație de blocaj.
Descrierea tehnică a metodologiei repartizării aleatorii este descrisă în Anexa A, a prezentului document.

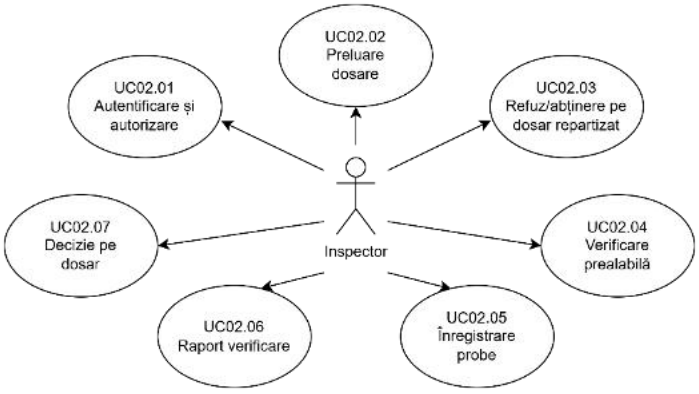
FR-UC-ED01.04-08. Actualizare statut și disponibilizare în liste. Sistemul trebuie să actualizeze automat statutul dosarului în registru (ex.: „Repartizat”, „Refuzat”, „Re-repartizat”, „Excepție – Inspector-șef”) și să reflecte imediat atribuirea în listele de lucru ale inspectorilor (task/inbox).

FR-UC-ED01.04-09. Trasabilitate completă și audit al repartizării. Sistemul trebuie să înregistreze în MLog fiecare repartizare/re-repartizare:

- dosarul, inspectorul desemnat, data/ora, tipul (inițială/re-repartizare), lista de eligibili (sau referință la setul determinat), și identificatorul evenimentului;
- și pentru fiecare refuz: inspectorul, motivul legal, data/ora, documente atașate (dacă există).

FR-UC-ED01.04-12. Actualizare fișă repartizare. După fiecare repartizare/re-repartizare, sistemul trebuie să actualizeze fișa de repartizare (identificator dosar, inspector desemnat, timestamp, tip repartizare), astfel încât fișa să poată fi generată pentru fiecare eveniment de repartizare.

6.2.3. Funcționalitățile aferente actorului Inspector



Figură 3. Diagrama cazurilor de utilizare aferente Inspectorului

UC-ED02.01. Autentificare și autorizare. Sistemul permite inspectorului să se autentifice și să inițieze o sesiune securizată, cu acces controlat la funcționalitățile e-Disciplinară conform rolului și permisiunilor.

FR-UC-ED02.01-01. Autentificare prin MPass. Sistemul trebuie să autentifice Inspectorul exclusiv prin serviciul guvernamental MPass, fără mecanisme alternative de login local (user/parolă în aplicație).

FR-UC-ED02.01-02. Preluare identitate și atribute din MPass. După autentificare, sistemul trebuie să preia din MPass identitatea utilizatorului și atributele necesare (identificator unic,

nume/prenume și atribute/roluri disponibile), pentru a crea/actualiza contextul de utilizator în e-Disciplinară.

FR-UC-ED02.01-03. Control acces pe baza atributelor/rolurilor. Sistemul trebuie să acorde acces la funcționalități și date în e-Disciplinară în baza rolului „Inspector" și a permisiunilor configurate, determinate din atributele/rolurile furnizate prin MPass (și/sau mapare internă controlată).

FR-UC-ED02.01-04. Sesiune securizată, logout și invalidare sesiune. Sistemul trebuie să inițieze o sesiune securizată după autentificare și să permită logout; la logout, sesiunea locală trebuie invalidată și, să fie inițiat fluxul de logout conform integrării cu MPass.

FR-UC-ED02.01-05. Expirare sesiune și re-autentificare. Sistemul trebuie să aplice expirarea automată a sesiunii după inactivitate (parametru configurabil de Administratorul sistemului, implicit 30 de minute) și să solicite re-autentificarea prin MPass pentru reluarea accesului.

UC-ED02.02. Preluare dosar repartizat. Sistemul permite inspectorului să vizualizeze lista dosarelor repartizate și să preia un dosar pentru lucru (acces la dosar, documente/anexe și istoric), marcând în sistem momentul preluării și inițiind etapa de examinare/verificare în cadrul dosarului.

FR-UC-ED02.02-01. Listă dosare repartizate. Sistemul trebuie să permită inspectorului să vizualizeze lista dosarelor repartizate lui, cu informații minime: număr evidență, data repartizării, status curent, procuror vizat și indicator de urgență/termen (dacă există).

FR-UC-ED02.02-02. Acces dosar și documente. Sistemul trebuie să permită inspectorului să deschidă un dosar repartizat și să acceseze toate documentele/anexele și metadatele aferente, conform drepturilor, inclusiv documentele generate de sistem (ex. fișe de repartizare, istoric).

FR-UC-ED02.02-03. Acțiune de „preluare". Sistemul trebuie să permită inspectorului să execute acțiunea explicită „Preluare dosar" asupra unui dosar repartizat, iar la această acțiune să înregistreze automat data/ora și utilizatorul și să actualizeze statutul dosarului la „În lucru".

FR-UC-ED02.02-04. Blocare preluare duplicată / consistență. Sistemul trebuie să prevină stări inconsistente în care același dosar este marcat „În lucru" simultan în contexte contradictorii (ex.: dacă dosarul a fost re-repartizat între timp sau este în excepție), afișând inspectorului starea actuală și interzicând preluarea dacă nu mai este asignat lui.

FR-UC-ED02.02-05. Trasabilitate și audit pentru preluare și acces. Sistemul trebuie să înregistreze în MLog cel puțin: deschiderea dosarului, acțiunea „preluare", și accesările/descărcările documentelor sensibile (unde politica o cere), cu utilizator și timestamp.

FR-UC-ED02.02-06. Vizibilitate termene și sarcini asociate dosarului. Sistemul trebuie să afișeze inspectorului, la preluarea dosarului, termenele/reperele procedurale relevante și sarcinile/pașii inițiali (dacă sunt definite), pentru a asigura respectarea termenelor.

UC-ED02.03. Refuz / abținere pe dosar repartizat. Sistemul permite inspectorului să înregistreze refuzul dosarului și/sau abținerea/conflictul de interese, cu motiv legal obligatoriu și, dacă este cazul, atașarea justificărilor; acțiunea declanșează fluxul de re-repartizare conform regulilor sistemului.

FR-UC-ED02.03-01. Inițiere refuz/abținere pe dosar repartizat. Sistemul trebuie să permită inspectorului să inițieze acțiunea de Refuz și/sau Abținere/Conflict pentru un dosar care îi este repartizat (și este în starea permisă pentru refuz).

FR-UC-ED02.03-02. Motiv legal obligatoriu. Sistemul trebuie să impună selectarea/introducerea unui motiv legal pentru refuz/abținere (câmp obligatoriu), fără de care acțiunea nu poate fi înregistrată.

FR-UC-ED02.03-03. Atașare justificări (după caz). Sistemul trebuie să permită atașarea documentelor justificative la refuz/abținere (fișiere/documente scanate), cu metadate minime (denumire, tip, format, dată/ora, încărcat de, referință la refuz), atunci când procedura internă o cere.

FR-UC-ED02.03-04. Notificare și declanșare re-repartizare. La înregistrarea refuzului, sistemul trebuie să:

- marcheze dosarul ca refuzat de inspectorul curent;
- notifice actorii relevanți (cel puțin Secretariat și/sau Inspectorul-șef, conform configurației);
- declanșeze automat re-repartizarea aleatorie și să excludă inspectorul care a refuzat din eligibilitate pentru acel dosar.

FR-UC-ED02.03-05. Interdicție de lucru după refuz. După înregistrarea refuzului/abținerii, sistemul nu va mai permite inspectorului să continue lucrul pe dosarul dat (editări/acte/probe), cu excepția vizualizării istoricului propriei acțiuni.

FR-UC-ED02.03-06. Trasabilitate și audit. Sistemul trebuie să înregistreze în MLog evenimentul de refuz/abținere (dosar, inspector, motiv legal, data/ora, documente atașate, rezultat/efect), astfel încât să existe trasabilitate completă a motivării și a fluxului declanșat.

FR-UC-ED02.03-07. Control stări și protecție la conflicte. Sistemul trebuie să prevină înregistrarea refuzului dacă dosarul nu mai este asignat inspectorului (ex.: a fost deja re-repartizat) sau dacă dosarul se află într-o stare în care refuzul nu este permis, afișând motivul și starea curentă.

UC-ED02.04. Verificare prealabilă. Sistemul permite inspectorului să înregistreze desfășurarea și rezultatul verificării prealabile (constatări, status, pași efectuați), cu trasabilitate în dosar.

FR-UC-ED02.04-01. Inițiere etapă de verificare. Sistemul trebuie să permită inspectorului să inițieze etapa „Verificare prealabilă” pentru un dosar preluat, setând statutul/etapa corespunzătoare și înregistrând data/ora începerii.

FR-UC-ED02.04-02. Evidență termene și alerte. Sistemul trebuie să calculeze/afișeze termenele procedurale relevante pentru verificarea prealabilă (configurabile de Administratorul sistemului) și să notifice inspectorul la apropierea/scurgerea termenelor (alertă în sistem și/sau notificare, conform politicii).

FR-UC-ED02.04-03. Rezultat verificare și tranziție de etapă. Sistemul trebuie să permită inspectorului să înregistreze rezultatul verificării prealabile (ex. „continuă examinarea” / „propune încetare” / „propune transmitere”), să actualizeze statusul dosarului conform rezultatului și să pregătească fluxul pentru raport/decizie.

FR-UC-ED02.04-04. Restricții și trasabilitate. Sistemul trebuie să aplice restricții de editare în funcție de status (ex.: după închiderea verificării prealabile) și să înregistreze în MLog toate acțiunile relevante (inițiere, modificări, atașări probe, închidere, rezultat), cu utilizator și timestamp.

UC-ED02.05. Înregistrare probe. Sistemul permite inspectorului să înregistreze probe la dosar ca urmare a solicitării de informații/probe de la entități/persoane relevante.

FR-UC-ED02.05-01. Adăugare probă în dosar. Sistemul trebuie să permită inspectorului să înregistreze o probă în dosar, inclusiv la etapa de verificare prealabilă, prin: încărcarea unui fișier (document scanat) și/sau înregistrarea unei referințe (ex. număr/act extern), asociind proba cu dosarul curent.

FR-UC-ED02.05-02. Metadate obligatorii pentru probă. Sistemul trebuie să solicite completarea metadatelor minime obligatorii pentru fiecare probă, cel puțin:

- tip probă (document, răspuns instituție, explicație, extras, aviz etc.);
- sursa probei (entitate/persoană) și data obținerii;
- descriere/rezumat;
- legătura cu etapa (ex. verificare prealabilă) și/sau cu o activitate/notă.

FR-UC-ED02.05-03. Clasificare și organizare probe. Sistemul trebuie să permită inspectorului să clasifice și să organizeze probele (categorii/etichete), astfel încât să poată fi filtrate și regăsite în dosar (după tip, sursă, dată, relevanță).

FR-UC-ED02.05-04. Integritate și versionare a probelor. Sistemul trebuie să asigure integritatea fișierelor încărcate ca probe (restricții de modificare) și, dacă se înlocuiește un document, să păstreze versiuni/istoric (fără a suprascrie proba inițială).

FR-UC-ED02.05-05. Control acces și confidențialitate probe. Sistemul trebuie să aplice reguli de acces la probe (vizualizare/descărcare), moștenite din dosar sau setate explicit, pentru a proteja datele sensibile.

FR-UC-ED02.05-06. Audit pentru probe. Sistemul trebuie să înregistreze în MLog: adăugarea probei, modificarea metadatelor, încărcarea/înlocuirea fișierelor și accesarea/descărcarea (unde politica cere), cu utilizator și timestamp.

FR-UC-ED02.05-07. Interdicții după stări "închise". Sistemul trebuie să restricționeze adăugarea/modificarea probelor după închiderea anumitor etape/statute (ex.: după emiterea deciziei), permițând doar acțiuni autorizate și auditabile (ex. anexare suplimentară prin dispoziție).

UC-ED02.07. Raport verificare. Sistemul permite inspectorului să întocmească și să salveze raportul de verificare ca document oficial al dosarului (analiză, probe, concluzii).

FR-UC-ED02.07-01. Creare raport în dosar. Sistemul trebuie să permită inspectorului să creeze un raport de verificare asociat unui dosar, ca document distinct în dosar, cu salvări iterative (schițe).

FR-UC-ED02.07-02. Structură minimă a raportului. Sistemul trebuie să asigure o structură minimă a raportului (șablon sau secțiuni obligatorii), cel puțin:

- date identificare dosar (nr. evidență, procuror vizat);
- descriere sesizare și obiect;
- activități desfășurate;
- probe analizate (referințe către probele din dosar);
- analiză/constatări;
- concluzii și propunere (orientativ pentru decizie).

FR-UC-ED02.07-03. Versionare și istoric. Sistemul trebuie să păstreze istoricul versiunilor raportului (cel puțin: versiune schiță și versiune finală), fără suprascriere, cu evidență a autorului și timestamp.

FR-UC-ED02.07-04. Finalizare raport și blocare editare. Sistemul trebuie să permită inspectorului să marcheze raportul ca „Final"; după finalizare, sistemul trebuie să blocheze editarea conținutului (cu excepții controlate și justificare).

FR-UC-ED02.07-05. Export raport (PDF) și atașare în dosar. Sistemul trebuie să permită generarea/exportul raportului în format neschimbabil (cel puțin PDF) și să îl păstreze ca document în dosar, accesibil rolurilor autorizate.

FR-UC-ED02.07-06. Jurnalizare evenimente raport. Sistemul trebuie să înregistreze în MLog: crearea raportului, modificările, finalizarea, exportul/descărcarea și orice acțiune de corecție excepțională, cu utilizator și timestamp.

UC-ED02.08. Decizie pe dosar. Sistemul permite inspectorului să emită decizia motivată (încetare / transmitere la CDE) și, când este „transmitere", să expedieze pachetul complet către CDE cu trasabilitate și confirmare în sistem.

FR-UC-ED02.08-01. Creare decizie asociată dosarului. Sistemul trebuie să permită inspectorului să creeze o decizie asociată unui dosar (document oficial), cu salvări iterative (schițe).

FR-UC-ED02.08-02. Tip decizie (opțiuni obligatorii). Sistemul trebuie să permită selectarea tipului deciziei dintr-o listă controlată, cel puțin:

- Încetare a procedurii (lipsă temei/alte cazuri prevăzute), sau
- Transmitere la CDE (există temei pentru examinare disciplinară).

FR-UC-ED02.08-03. Motivare obligatorie și structură minimă. Sistemul trebuie să impună completarea motivării (câmp obligatoriu) și să asigure o structură minimă a deciziei, cel puțin:

- date identificare dosar;
- temeiuri/argumentare;
- dispoziția (încetare / transmitere);
- referințe la raportul de verificare și probe relevante.

FR-UC-ED02.08-04. Finalizare decizie și blocare editare. Sistemul trebuie să permită marcarea deciziei ca „Finală/Emisă”; după emitere, conținutul deciziei trebuie blocat la editare, cu excepții controlate (doar cu justificare și audit).

FR-UC-ED02.08-05. Export decizie (PDF) și păstrare în dosar. Sistemul trebuie să genereze decizia în format neschimbabil (cel puțin PDF) și să o păstreze în dosar ca document oficial accesibil rolurilor autorizate.

FR-UC-ED02.08-06. Efect procedural automat în funcție de tip. Sistemul trebuie să execute efecte automate în funcție de tipul deciziei:

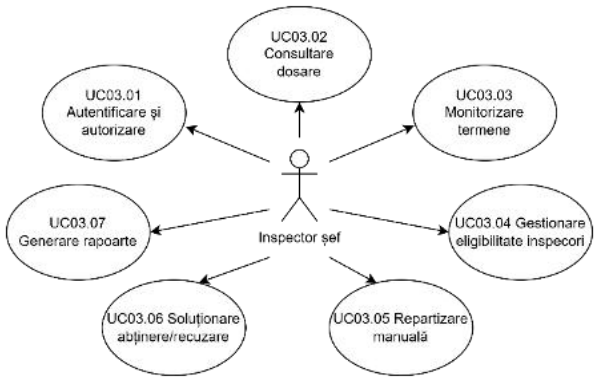
- la încetare: actualizează statusul dosarului (ex. „Încetat/Închis”);
- la transmitere la CDE: actualizează statusul (ex. „Transmis la CDE”) și inițiază procesul de transmitere a pachetului.

FR-UC-ED02.08-07. Transmitere pachet la CDE. În cazul deciziei de transmitere, sistemul trebuie să transmită către CDE pachetul minim: decizia finală, raportul final și lista/legături către probele din dosar (sau anexele exportate), cu confirmare/înregistrare a transmiterii.

FR-UC-ED02.08-08. Trasabilitate și jurnalizare. Sistemul trebuie să înregistreze în MLog: crearea, modificările, emiterea deciziei, exportul/descărcarea (unde politica cere), schimbările de status declanșate și transmiterea la CDE (dacă există), cu utilizator și timestamp.

FR-UC-ED02.08-09. Restricții după emiterea deciziei. După emiterea deciziei, sistemul trebuie să restricționeze modificările în dosar (probe, raport, cereri), permițând doar acțiuni excepționale autorizate, cu justificare și audit.

6.2.4. Funcționalitățile aferente actorului Inspector șef



Figură 4. Diagrama cazurilor de utilizare aferente Inspectorului Șef

UC-ED03.01. Autentificare și autorizare (MPass). Sistemul permite Inspectorului-șef să se autentifice prin serviciul guvernamental MPass și să inițieze o sesiune securizată, cu acces la funcționalitățile e-Disciplinară conform rolului și permisiunilor.

FR-UC-ED03.01-01. Autentificare exclusiv prin MPass. Sistemul trebuie să autentifice Inspectorul-șef exclusiv prin serviciul guvernamental MPass după principiul single sign on, fără mecanisme alternative de autentificare locală în aplicație.

FR-UC-ED03.01-02. Preluare identitate și atribute din MPass. După autentificare, sistemul trebuie să preia din MPass identitatea utilizatorului și atributele necesare (identificator unic, nume/prenume și atribute/roluri), pentru a stabili contextul de acces în e-Disciplinară.

FR-UC-ED03.01-03. Control acces pe rol Inspectorul-șef. Sistemul trebuie să acorde acces la funcționalități și date în baza rolului „Inspectorul-șef", determinat din atributele/rolurile furnizate de MPass (și/sau mapare internă), aplicând restricții de acces corespunzătoare.

FR-UC-ED03.01-04. Expirare sesiune și re-autentificare. Sistemul trebuie să aplice expirarea automată a sesiunii după o perioadă configurabilă de inactivitate (implicit 30 min) și să de-logheze utilizatorul după principiul single sign off sau să solicite re-autentificarea prin MPass pentru reluarea accesului.

FR-UC-ED03.01-05. Audit evenimente de autentificare. Sistemul trebuie să înregistreze în jurnalul de audit evenimentele relevante: autentificare reușită/eșuată, logout și expirare sesiune, cu minim: utilizator (ID), data/ora, tip eveniment și rezultat (succes/eșec), fără a expune date sensibile.

UC-ED03.02. Consultare dosare. Sistemul permite Inspectorului-șef să caute și să consulte dosarele disciplinare (liste, filtre, căutare), să deschidă un dosar și să vizualizeze documentele din dosar, inclusiv istoricul evenimentelor-cheie (repartizări, refuzuri, re-repartizări) și documentele generate de sistem (ex. fișe de repartizare).

FR-UC-ED03.02-01. Listare dosare (registru) cu câmpuri minime. Sistemul trebuie să permită Inspectorului-șef să vizualizeze lista dosarelor disciplinare, cu afișarea câmpurilor minime: număr unic de evidență, data înregistrării, starea curentă, inspector desemnat (dacă există), procuror vizat, și indicator de termen/depășire (dacă există).

FR-UC-ED03.02-02. Căutare și filtrare. Sistemul trebuie să permită căutarea și filtrarea dosarelor cel puțin după: număr evidență, interval de date, stare, inspector, procuror vizat și tip sesizare, astfel încât Inspectorul-șef să poată identifica rapid dosarele relevante.

FR-UC-ED03.02-03. Acces la detaliile dosarului. Sistemul trebuie să permită deschiderea unui dosar din listă și vizualizarea metadatelor dosarului (datele principale, stare/etapă, termene, alocare) și a legăturii cu sesizarea inițială.

FR-UC-ED03.02-04. Vizualizare documente din dosar. Sistemul trebuie să permită Inspectorului-șef să vizualizeze și să descarce documentele din dosar, inclusiv: sesizare, anexe, probe, raport, decizie și documentele generate de sistem (ex. fișe de repartizare), conform regulilor de confidențialitate și drepturilor de acces.

FR-UC-ED03.02-05. Vizualizare istoric evenimente-cheie. Sistemul trebuie să permită Inspectorului-șef să consulte istoricul evenimentelor-cheie pe dosar (înregistrare, marcarea ca „Complet", repartizări/re-repartizări, refuzuri, preluare, raport final, decizie, transmitere), cu data/ora și actorul aferent.

FR-UC-ED03.02-06. Acces controlat și confidențialitate. Sistemul trebuie să aplice control de acces la nivel de dosar și document (vizualizare/descărcare) pentru Inspectorul-șef, conform politicilor de confidențialitate, inclusiv pentru documente/probe cu acces restricționat.

FR-UC-ED03.02-07. Jurnalizare. Sistemul trebuie să înregistreze în MLog accesările relevante efectuate de Inspectorul-șef (deschiderea dosarului și accesarea/descărcarea documentelor sensibile, unde politica o cere), cu utilizator și timestamp.

UC-ED03.03. Monitorizare termene. Sistemul permite Inspectorului-șef să monitorizeze termenele procedurale pe dosare și pe inspectori, să vizualizeze alerte pentru termene apropiate/depășite și să acceseze lista dosarelor cu risc de întârziere (cu detalii și filtrare).

FR-UC-ED03.03-01. Calcul și afișare termene pe dosar. Sistemul trebuie să calculeze și să afișeze pentru fiecare dosar termenele procedurale relevante (data-limită și zile rămase/depășite), pe baza

regulilor de termen configurate și a dăților acțiunilor aplicate (ex.: data înregistrării, data preluării, data începerii verificării etc.).

FR-UC-ED03.03-02. Listă dosare cu termene apropiate/depășite. Sistemul trebuie să permită Inspectorului-șef să vizualizeze liste dedicate:

- „Termene apropiate” (dosare cu termen în următoarele N zile),
- „Termene depășite” (dosare cu termen depășit),
- cu filtrare cel puțin după: inspector, stare/etapă, perioadă, tip sesizare.

FR-UC-ED03.03-03. Praguri de alertă configurabile. Sistemul trebuie să permită configurarea pragului N (zile înainte de termen) pentru lista/alerta „Termene apropiate” și a altor praguri operaționale (ex. categorii de termen), de către rol autorizat (administrare).

FR-UC-ED03.03-04. Alerte pentru Inspectorul-șef. Sistemul trebuie să genereze alerte în aplicație (ex. notificare internă / indicator pe dashboard) pentru dosarele care intră în zona „Termene apropiate” și pentru dosarele care devin „Termene depășite”, astfel încât Inspectorul-șef să le poată identifica fără căutare manuală.

FR-UC-ED03.03-05. Detaliere cauză și istoric termen. Sistemul trebuie să permită Inspectorului-șef să vadă pentru un dosar: termenul vizat, data-limită, evenimentul de la care a fost calculat termenul (ex. „preluare dosar”) și starea/etapa curentă, pentru a înțelege cauza întârzierii.

UC-ED03.04. Gestionare eligibilitate inspectori. Sistemul permite Inspectorului-șef să gestioneze eligibilitatea inspectorilor pentru repartizarea aleatorie (activ/inactiv, indisponibil temporar, excluderi), astfel încât lista inspectorilor eligibili folosită de mecanismul automat de repartizare să includă doar inspectori eligibili. Această acțiune nu repartizează dosare și nu permite selectarea manuală a inspectorului în repartizarea aleatorie; ea doar controlează cine poate fi luat în calcul de mecanismul automat.

FR-UC-ED03.04-01. Listă inspectori și stare eligibilitate. Sistemul trebuie să permită Inspectorului-șef să vizualizeze lista inspectorilor, cu afișarea stării curente de eligibilitate pentru repartizare (eligibil/neeligibil) și a motivului (dacă este neeligibil).

FR-UC-ED03.04-02. Setare eligibil / neeligibil. Sistemul trebuie să permită Inspectorului-șef să marcheze un inspector ca neeligibil pentru repartizare și să revină la eligibil. La marcarea ca neeligibil, sistemul trebuie să impună completarea unui motiv obligatoriu (selectat dintr-o listă controlată și/sau text justificativ) și să nu permită salvarea fără acest motiv.

FR-UC-ED03.04-03. Neeligibilitate temporară cu perioadă. Sistemul trebuie să permită setarea neeligibilității temporare prin indicarea unei perioade (data început – data sfârșit). La expirarea perioadei, sistemul trebuie să reactiveze automat eligibilitatea inspectorului.

FR-UC-ED03.04-04. Excludere din repartizarea aleatorie. Sistemul trebuie să excludă automat inspectorii marcați neeligibili din lista inspectorilor eligibili folosită la repartizarea aleatorie a dosarelor, fără a afecta dosarele deja repartizate anterior.

FR-UC-ED03.04-05. Restricții la modificare dacă există dosare active (opțional, dar util). Dacă un inspector are dosare în lucru/preluate, sistemul trebuie să permită marcarea ca neeligibil pentru repartizări viitoare, dar să nu retragă automat dosarele deja repartizate (redistribuirea se face prin flux dedicat, dacă există).

FR-UC-ED03.04-06. Jurnalizare. Sistemul trebuie să înregistreze în MLog orice schimbare a eligibilității (cine, când, inspector afectat, valoare veche/nouă, motiv, perioadă), pentru trasabilitate.

UC-ED03.05. Repartizare manuală. În situația în care sistemul confirmă excepția „toți inspectorii eligibili au refuzat dosarul”, sistemul permite Inspectorului-șef să repartizeze manual dosarul unui inspector, cu înregistrarea motivului/actului și audit complet. Funcționalitatea este disponibilă doar în această condiție de excepție determinată de sistem.

FR-UC-ED03.05-01. Precondiție obligatorie "toți au refuzat". Sistemul trebuie să permită inițierea repartizării manuale de către Inspectorul-șef doar pentru dosarele aflate în starea „Necesită repartizare de către Inspectorul-șef" (sau echivalent), setată automat de sistem după constatarea că toți inspectorii eligibili au refuzat.

FR-UC-ED03.05-02. Afișare motiv excepție și istoric refuzuri. Înainte de repartizarea manuală, sistemul trebuie să afișeze Inspectorului-șef lista refuzurilor pentru dosar (inspector, motiv legal, data/ora) și faptul că lista eligibililor a fost epuizată, pentru justificarea deciziei.

FR-UC-ED03.05-03. Selectare inspector destinatar (din listă controlată). Sistemul trebuie să permită Inspectorului-șef să selecteze inspectorul destinatar din lista inspectorilor activi (listă controlată), chiar dacă aceștia au refuzat anterior (deoarece este situație de excepție).

FR-UC-ED03.05-04. Motiv/act obligatoriu pentru repartizare manuală. Sistemul trebuie să impună completarea unui motiv/act (câmp obligatoriu) pentru repartizarea manuală (ex.: referință la dispoziție internă / justificare), fără de care repartizarea nu poate fi confirmată.

FR-UC-ED03.05-05. Efect: actualizare alocare și stare dosar. La confirmarea repartizării manuale, sistemul trebuie să actualizeze alocarea dosarului către inspectorul selectat și să schimbe starea dosarului la „Repartizat" (sau echivalent), astfel încât noul inspector să poată prelua dosarul în lucru.

FR-UC-ED03.05-06. Generare fișă de repartizare. Sistemul trebuie să genereze automat fișa de repartizare pentru repartizarea manuală (marcată ca „manuală – excepție") și să o atașeze în dosar în istoricul fișelor de repartizare.

FR-UC-ED03.05-07. Notificare către inspectorul desemnat. Sistemul trebuie să notifice inspectorul desemnat despre atribuirea dosarului (notificare internă și/sau MNotify).

FR-UC-ED03.05-08. Jurnalizare. Sistemul trebuie să înregistreze în MLog: dosarul, inspectorul desemnat, Inspectorul-șef (autor), data/ora, motivul/actul, tipul repartizării („manuală – excepție") și referința la condiția declanșatoare („toți eligibili au refuzat").

UC-ED03.06. Soluționare abținere/recuzare. Sistemul permite Inspectorului-șef să examineze cererile de abținere/recuzare și să adopte o soluție motivată (admitere/respingere). La admitere, sistemul aplică efectele asupra alocării dosarului (ex. eliberarea dosarului de la inspectorul curent și declanșarea re-repartizării conform regulilor sistemului); la respingere, dosarul rămâne la inspectorul desemnat, cu trasabilitate și audit.

FR-UC-ED03.06-01. Acces la cererile de abținere/recuzare. Sistemul trebuie să permită Inspectorului-șef să vizualizeze lista cererilor de abținere/recuzare înregistrate în sistem, cu câmpuri minime: dosar, inspector vizat, data depunerii, tip cerere și stare cererii (nouă/în examinare/soluționată).

FR-UC-ED03.06-01A. Tratarea cererilor privind Inspectorul-șef. În cazul în care declarația de abținere sau cererea de recuzare vizează Inspectorul-șef, sistemul trebuie să redirecționeze automat examinarea cererii către Președintele Consiliului Superior al Procurorilor sau către rolul desemnat conform cadrului normativ aplicabil, restricționând Inspectorului-șef accesul la acțiunile de examinare și soluționare aferente propriei cereri.

FR-UC-ED03.06-02. Vizualizare conținut și anexele cererii. Sistemul trebuie să permită deschiderea unei cereri și vizualizarea motivării și a documentelor anexate, precum și a contextului dosarului (alocare curentă, istoric refuzuri/redistribuiri relevante).

FR-UC-ED03.06-03. Soluție controlată: admitere sau respingere. Sistemul trebuie să permită Inspectorului-șef să soluționeze cererea prin selectarea uneia dintre opțiuni: Admitere sau Respingere (listă controlată).

FR-UC-ED03.06-04. Motivare obligatorie a soluției. La soluționarea cererii, sistemul trebuie să impună completarea unei motivări obligatorii (câmp obligatoriu) și să nu permită confirmarea fără motivare.

FR-UC-ED03.06-04A. Separarea competențelor în cazul Inspectorului-șef. Sistemul trebuie să asigure separarea funcțională a competențelor astfel încât Inspectorul-șef să nu poată examina, aproba, respinge sau influența procedural cererile de abținere sau recuzare care îl vizează direct.

FR-UC-ED03.06-05. Efect automat la admitere. La admiterea cererii, sistemul trebuie să:

- marcheze cererea ca „Admisă”;
- elibereze dosarul de la inspectorul curent (anularea alocării active);
- declanșeze re-repartizarea conform regulilor sistemului (repartizare aleatorie către inspectori eligibili, cu excluderile aplicabile, inclusiv inspectorul vizat).

FR-UC-ED03.06-06. Efect automat la respingere. La respingerea cererii, sistemul trebuie să marcheze cererea ca „Respinsă” și să mențină alocarea dosarului la inspectorul curent (fără schimbarea alocării).

FR-UC-ED03.06-07. Notificare părți relevante. Sistemul trebuie să notifice intern și/sau prin MNotify actorii relevanți despre soluția cererii (cel puțin inspectorul vizat și, dacă este cazul, secretariatul), prin mecanismul de notificare al sistemului.

FR-UC-ED03.06-08. Jurnalizare. Sistemul trebuie să înregistreze în audit: cererea, dosarul, soluția (admis/respins), motivarea, autorul (Inspectorul-șef), data/ora, și efectele produse (schimbare alocare/re-repartizare), inclusiv identificatorul evenimentului de alocare rezultat.

UC-ED03.07. Generare rapoarte. Sistemul permite Inspectorului-șef să genereze rapoarte privind volumul de dosare, distribuția pe inspectori, refuzuri, stoc și vechime, timpi pe etape, cu filtre și export (PDF/Excel) pentru analiză și control operațional.

FR-UC-ED03.07-01. Listă rapoarte disponibile (catalog). Sistemul trebuie să pună la dispoziția Inspectorului-șef o listă de rapoarte manageriale standard, cel puțin:

- volum dosare (înregistrate / repartizate / închise) pe perioadă;
- distribuție dosare pe inspectori;
- refuzuri (număr și distribuție) pe perioadă/inspector;
- stoc și vechime (dosare deschise, pe intervale de vechime);
- termene depășite (număr și listă, pe inspector).

FR-UC-ED03.07-02. Parametrizare rapoarte (filtre). Sistemul trebuie să permită parametrizarea rapoartelor cel puțin prin: interval de timp, inspector, stare/etapă, tip sesizare (și, dacă este cazul, unitatea/procuratura), cu posibilitatea combinării filtrelor.

FR-UC-ED03.07-03. Generare raport și afișare rezultate. Sistemul trebuie să genereze raportul selectat pe baza parametrilor aleși și să afișeze rezultatele în interfață (tabel/listă), incluzând totaluri/numărări relevante pentru raportul respectiv.

FR-UC-ED03.07-04. Export raport. Sistemul trebuie să permită exportul rapoartelor generate cel puțin în Excel/CSV și PDF (unde e aplicabil), păstrând parametrii folosiți la generare în antet/metadate.

FR-UC-ED03.07-05. Acces din raport la dosare (drill-down). Pentru rapoartele care includ liste de dosare (ex. termene depășite, stoc/vechime), sistemul trebuie să permită deschiderea directă a dosarului din raport.

FR-UC-ED03.07-06. Control acces și limitare la datele rolului. Sistemul trebuie să permită Inspectorului-șef generarea rapoartelor pe întregul set de dosare (conform drepturilor de vizualizare ale rolului) și să nu permită editarea datelor prin intermediul rapoartelor (rapoartele sunt doar pentru consultare/export).

FR-UC-ED03.07-07. Jurnalizare. Sistemul trebuie să înregistreze în MLog generarea și exportul rapoartelor: utilizator, data/ora, tip raport, parametrii principali (interval, filtre) și tipul acțiunii (vizualizare/export).

6.3. Modulul e-Carieră

Modulul e-Carieră este utilizat de Operator HR CSP, Membrii CSP și Conducerea CSP pentru gestionarea dosarelor profesionale ale procurorilor și personalului relevant. În funcție de decizia instituțională, poate permite acces limitat de tip self-service persoanei vizate (consultare/încărcare documente).

Modulul gestionează următoarele procese operaționale:

A. Crearea și administrarea dosarului profesional unic, identificat prin IDNP, cu structură standard și secțiuni predefinite.
B. Actualizarea datelor profesionale, inclusiv:
    - angajări și funcții deținute,
    - delegări/detașări,
    - studii și instruiri,
    - atestări și evaluări,
    - stimulări, sancțiuni, distincții,
    - grade/ranguri.
C. Gestionarea documentelor suport, cu atașare, versionare și control al accesului.
D. Gestionarea concursurilor de recrutare și promovare, inclusiv:
    - inițiere concurs,
    - înregistrare candidați,
    - verificare eligibilitate,
    - evaluare și consemnare rezultate,
    - comunicare rezultate.
E. Gestionarea ciclurilor de evaluare a performanței, cu agregare automată a datelor din dosar și urmărirea planurilor de îmbunătățire.
F. Gestionarea acțiunilor de carieră, precum numiri, transferuri, promovări, detașări, cu actualizare automată a istoricului profesional.
G. Raportare și analiză, prin căutare transversală, rapoarte standard, indicatori și export controlat.

Integrare cu alte sisteme:
Modulul e-Carieră se integrează cu:

- MConnect / Registre de stat, pentru preluarea și actualizarea automată a datelor personale (read-only);
- Sistemul e-Management CSP existent, pentru corelarea documentelor oficiale (acolo unde o acțiune de carieră este inițiată prin document înregistrat);
- Alte module e-CSP (ex. e-Disciplinară), prin interfețe API pentru consultarea controlată a datelor de carieră;
- Sistemul e-Personal PG, pentru import inițial/migrare date istorice a procurorilor.
- Sistemul informațional de instruire al Institutului Național al Justiției, după caz, precum și alte sisteme informaționale relevante din domeniul învățământului superior, inclusiv cele gestionate de Ministerul Educației și Cercetării prin API-uri securizate și/sau MConnect.

Modulul nu gestionează corespondența externă și nu atribuie numere oficiale de înregistrare – aceste funcții rămân în sistemul e-Management CSP existent.

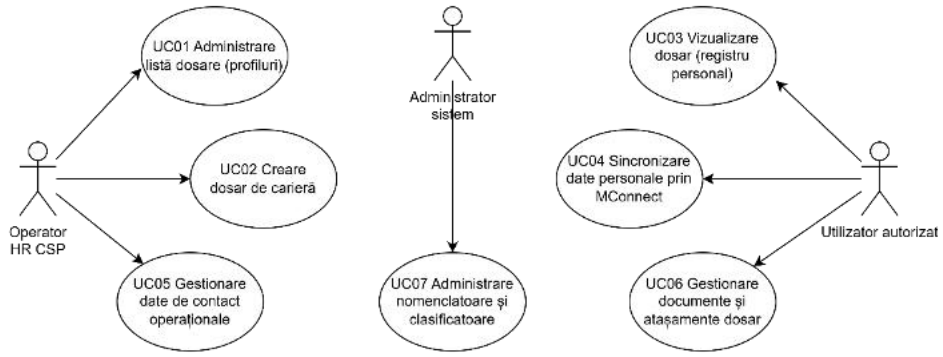
6.3.1. Actorii modulului e-Carieră

Modulul e-Carieră va avea următorii actori:

A-EC01. Operator HR CSP – introduce și actualizează datele profesionale ale procurorilor; gestionează dosarele de carieră; verifică completitudinea documentelor și menține evidența administrativă a proceselor.
A-EC02. Membru CSP – consultă dosarele și rapoartele aferente; participă la procesul de evaluare, deliberare și adoptare a deciziilor în cadrul concursurilor sau altor proceduri de carieră.
A-EC03. Conducere CSP / Management – accesează informații agregate și rapoarte; utilizează datele pentru planificarea funcțiilor, analiza resurselor și luarea deciziilor strategice.

A-EC04. Angajat CSP / Procuror (opțional, în cazul implementării accesului self-service) – consultă propriul dosar profesional și poate depune sau actualiza documente, în limitele stabilite prin drepturile de acces configurate.

A-EC05. Administrator sistem (IT CSP) – gestionează rolurile și drepturile de acces, nomenclatoarele, parametrii tehnici și integrarea cu sisteme externe; asigură mentenanța și monitorizarea tehnică a modulului, fără a interveni în conținutul deciziilor procedurale.



Figură 5. Diagrama cazurilor de utilizare aferente componentei de managementul dosarelor

6.3.2. Managementul dosarelor (centralizare & digitalizare)

UC-EC01. Administrare listă dosare (profiluri): Modulul permite Operatorului HR CSP și Membrilor CSP să vizualizeze lista dosarelor de carieră (procurori, membri CSP, angajați ai aparatului CSP), cu funcții de filtrare/sortare/căutare, afișarea câmpurilor cheie (statut, funcție curentă, instituție) și accesarea rapidă a dosarului selectat, păstrând trasabilitatea accesărilor conform drepturilor.

UC-EC02. Creare dosar de carieră: Modulul permite Operatorului HR CSP să inițieze crearea unui dosar de carieră pentru o persoană (pe baza unui identificator unic, ex. IDNP), verificând existența unui dosar anterior pentru a evita duplicarea; la salvare, sistemul creează dosarul cu status inițial „Activ/Inițializat", declanșează preluarea datelor personale prin MConnect și pregătește structura completă a dosarului pentru completarea datelor profesionale.

UC-EC03. Vizualizare dosar (registru personal): Sistemul permite utilizatorilor autorizați să deschidă dosarul de carieră și să navigheze pe secțiuni (Fișa personală, CV, Angajări, Delegări, Studii, Instruiri, Atestări, Stimulări, Sancțiuni, Distincții, Grade), afișând datele structurat și permițând accesul la documentele atașate, cu respectarea drepturilor și jurnalizarea acțiunilor.

UC-EC04. Sincronizare date personale prin MConnect: Sistemul permite preluarea și actualizarea automată a datelor personale (nume, prenume, sex, adresă, stare civilă, date despre soț/soție – dacă sunt disponibile în registrele sursă), prin integrare cu platforma MConnect; la sincronizare, sistemul marchează aceste date ca „Date din registre (read-only)", păstrează istoricul sincronizărilor și tratează erorile de integrare fără a bloca administrarea datelor profesionale.

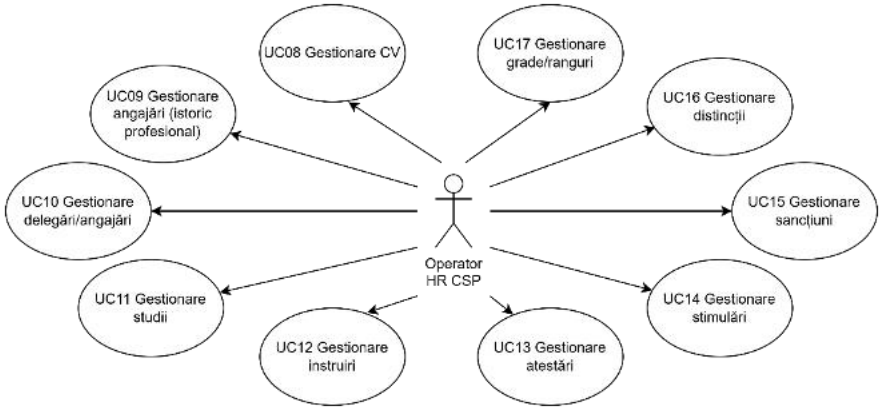
UC-EC05. Gestionare date de contact operaționale: Sistemul permite Operatorului HR CSP să completeze și să actualizeze date de contact operaționale (ex. email instituțional, telefon de serviciu, unitate/compartiment), distinct de datele de domiciliu preluate din registre, păstrând istoricul modificărilor și permițând validări de format (email/telefon).

UC-EC06. Gestionare documente și atașamente dosar: Sistemul permite utilizatorilor autorizați să încarce, vizualizeze, descarce și versioneze documente aferente dosarului (ordine/decizii, certificate, diplome, evaluări etc.), prin completarea metadatelor obligatorii (tip document, dată, emitent) și

aplicarea regulilor de acces; la salvare, sistemul păstrează integritatea fișierelor, jurnalizează operațiile și asigură trasabilitatea.

UC-EC07. Administrare nomenclatoare și clasificatoare: Sistemul permite Administratorului/ Operatorului autorizat să gestioneze nomenclatoare utilizate în dosare (instituții, funcții, tipuri documente, tipuri instruiri, calificative etc.), astfel încât utilizatorii să introducă date consistente; la publicarea modificărilor, sistemul păstrează versiuni și istoricul schimbărilor.

6.3.3. Carieră profesională



Figură 6. Diagrama cazurilor de utilizare aferente componentei Carieră profesională

UC-EC08. Gestionare CV: Sistemul permite Operatorului HR CSP (și opțional persoanei vizate, dacă se decide self-service) să înregistreze și să actualizeze CV-ul prin încărcarea fișierului și/sau completarea câmpurilor structurate, păstrând versiuni, data/autorul modificării și punând CV-ul la dispoziție pentru procesele de concurs și evaluare.

UC-EC09. Gestionare angajări (istoric profesional): Sistemul permite Operatorului HR CSP să înregistreze, actualizeze și consulte istoricul angajărilor/funcțiilor unei persoane (instituție, funcție, perioadă, temei/act), efectuând validări de cronologie (ex. suprapuneri) și atașând documentele justificative; la salvare, sistemul actualizează funcția curentă (după reguli) și păstrează trasabilitatea.

UC-EC10. Gestionare delegări/detașări: Sistemul permite Operatorului HR CSP să gestioneze delegările și detașările (tip, perioadă, destinație, temei), cu atașarea actelor și validări de perioadă; la salvare, sistemul reflectă impactul în istoricul profesional și jurnalizează acțiunile.

UC-EC11. Gestionare studii: Sistemul permite Operatorului HR CSP să introducă și să actualizeze studiile (instituție, program, calificare, perioadă), să atașeze diplome/certificate și să marcheze statusul de verificare (ex. „Neverificat/Verificat”), păstrând istoricul modificărilor.

UC-EC12. Gestionare instruiri (formare continuă): Sistemul permite Operatorului HR CSP să înregistreze instruiri/cursuri (furnizor, tematică, durată/ore, perioadă), să atașeze certificate și să calculeze totaluri pe perioade (unde e cazul), astfel încât datele să fie utilizabile în evaluarea performanței și raportare.

UC-EC13. Gestionare atestări: Sistemul permite Operatorului HR CSP să înregistreze atestări/evaluări formale (tip, dată, rezultat/calificativ, documente), păstrând istoricul și permițând consultarea lor în procesele de promovare și evaluare.

UC-EC14. Gestionare stimulări: Sistemul permite Operatorului HR CSP să înregistreze stimulări/premii (tip, motiv, dată, emitent), cu atașarea documentelor justificative; la salvare, sistemul păstrează trasabilitatea și include datele în rapoarte.

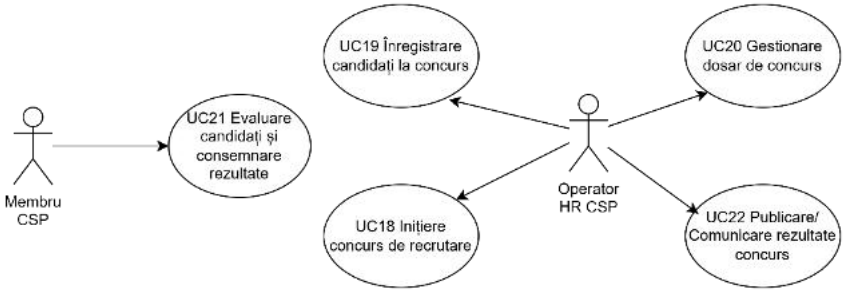
UC-EC15. Gestionare sancțiuni: Sistemul permite Operatorului HR CSP să înregistreze sancțiuni (tip, motiv, perioadă, efect, temei), cu atașarea actelor și restricționarea accesului unde e necesar; la salvare,

sistemul jurnalizează operațiile și face sancțiunile disponibile pentru analize/evaluări conform drepturilor.

UC-EC16. Gestionare distincții: Sistemul permite Operatorului HR CSP să înregistreze distincții (tip, emitent, dată, motiv), cu atașarea documentelor și includerea lor în profilul de carieră și raportare.

UC-EC17. Gestionare grade/ranguri: Sistemul permite Operatorului HR CSP să înregistreze și să actualizeze gradele/rangurile (tip, dată acordare, temei, efect), cu validări de succesiune cronologică și atașarea actelor, păstrând istoricul complet.

6.3.4. Recrutare și selecție (concursuri)



Figură 7. Diagrama cazurilor de utilizare aferente componentei Recrutare și selecție

UC-EC18. Inițiere concurs de recrutare: Sistemul permite Operatorului HR CSP să inițieze un concurs prin definirea postului/funcției, condițiilor, calendarului și componenței comisiei, stabilind statusul inițial „În pregătire” și pregătind spațiul de lucru pentru dosarele candidaților și evaluare.

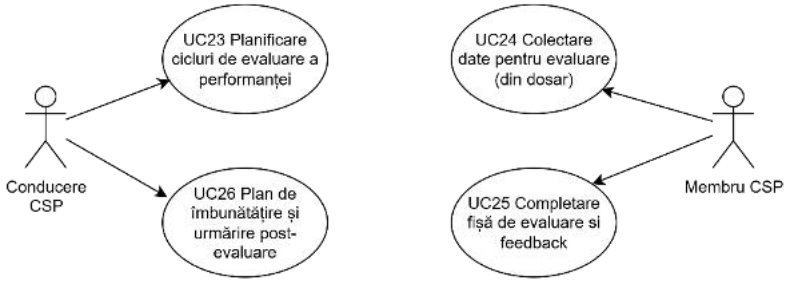
UC-EC19. Înregistrare candidați la concurs: Sistemul permite Operatorului HR CSP să înregistreze candidați (interni sau externi) în cadrul unui concurs, asociind candidații cu dosarele existente sau inițiind crearea unui dosar, colectând documentele obligatorii și stabilind statusul inițial al candidaturii „Depusă/Înregistrată”, cu trasabilitate.

UC-EC20. Gestionare dosar de concurs (verificare eligibilitate): Sistemul permite Operatorului HR CSP să verifice eligibilitatea candidaților pe baza criteriilor concursului, să completeze checklist-uri, să solicite clarificări și să gestioneze statusuri (ex. „În verificare/Eligibil/Neeligibil”), păstrând justificări și documente suport.

UC-EC21. Evaluare candidați și consemnare rezultate: Sistemul permite Membrilor CSP/comisiei să evalueze candidații prin completarea grilelor și acordarea punctajelor, să atașeze procese-verbale și să genereze decizii/rezultate, păstrând versiuni, semnături (unde e cazul) și jurnalizarea acțiunilor.

UC-EC22. Publicare/Comunicare rezultate concurs: Sistemul permite Operatorului HR CSP să comunice rezultatele către actorii autorizați (intern și/sau public, conform politicilor), inclusiv prin export și notificări, păstrând istoricul publicărilor și evidența accesărilor.

6.3.5. Evaluarea performanței



Figură 8. Diagrama cazurilor de utilizare aferente componentei Evaluarea performanței

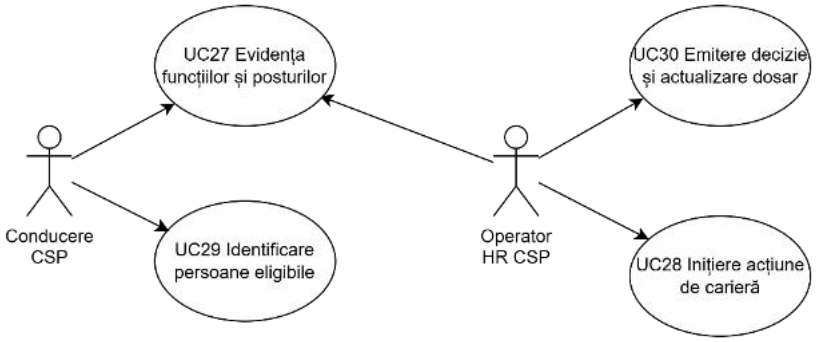
UC-EC23. Planificare cicluri de evaluare a performanței: Sistemul permite Conducerii CSP să inițieze un ciclu de evaluare prin definirea perioadei, criteriilor, evaluatorilor și populației evaluate, stabilind statusul inițial „Planificat” și generând automat listele de evaluare.

UC-EC24. Colectare date pentru evaluare (din dosar): Sistemul permite Membrilor CSP (evaluatorii) agregarea automată a datelor relevante din dosar (istoric profesional, instruiri, atestări, sancțiuni, stimulări etc.) pentru fiecare persoană evaluată, astfel încât evaluatorii să aibă un tablou complet, cu trasabilitate a surselor de date.

UC-EC25. Completare fișă de evaluare și feedback: Sistemul permite Membrilor CSP (evaluatorilor) să completeze fișele de evaluare, să înregistreze feedback și concluzii, să atașeze documente suport și să finalizeze evaluarea cu un status (ex. „În lucru/Finalizată”), păstrând audit și versiuni.

UC-EC26. Plan de îmbunătățire și urmărire post-evaluare: Sistemul permite Conducerii CSP stabilirea unui plan de îmbunătățire (măsuri, termene, responsabili) în urma evaluării, urmărirea progresului și închiderea planului cu evidența acțiunilor întreprinse.

6.3.6. Planificare și gestionarea funcțiilor (succesiune, numiri, transferuri, promovări, detașări)



Figură 9. Diagrama cazurilor de utilizare aferente componentei Planificare și gestionare funcții

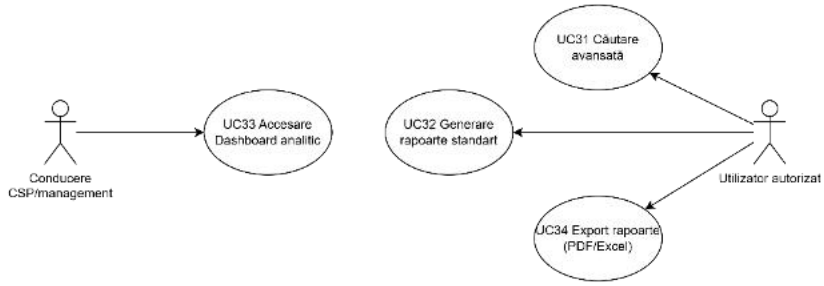
UC-EC27. Evidența funcțiilor și posturilor: Sistemul permite Conducerii CSP și Operatorilor HR CSP să gestioneze catalogul funcțiilor și posturilor (ocupat/vacant, cerințe, structură), astfel încât să susțină planificarea resurselor și procesele de recrutare.

UC-EC28. Inițiere acțiune de carieră (numire/transfer/promovare/detașare): Sistemul permite Operatorului HR CSP să inițieze o acțiune de carieră prin completarea datelor obligatorii, selectarea persoanei vizate și atașarea actelor, stabilind statusul inițial „În avizare” și declanșând circuitul intern de aprobare (unde e cazul).

UC-EC29. Identificare persoane eligibile (succesiune/shortlist): Sistemul permite Conducerii CSP să identifice persoane eligibile pentru posturi vacante sau promovare, prin aplicarea criteriilor (vechime, instruiri, sancțiuni, rezultate evaluări etc.), generând o listă scurtă și păstrând justificarea selecției.

UC-EC30. Emitere decizie și actualizare dosar: Sistemul permite Operatorului HR CSP finalizarea acțiunii de carieră prin înregistrarea deciziei și atașarea documentelor semnate; la finalizare, sistemul actualizează automat secțiunile relevante din dosar (angajări/delegări/grade), marchează statusul „Executată” și păstrează audit complet.

6.3.7. Raportare și analiză



Figură 10. Diagrama cazurilor de utilizare aferente componentei Raportare și analiză

UC-EC31. Căutare avansată în dosare și evenimente de carieră: Sistemul permite utilizatorilor autorizați să caute transversal în dosare și înregistrări (angajări, instruiri, sancțiuni etc.) pe criterii multiple, cu filtrare/sortare și acces direct la rezultatele relevante, jurnalizând interogările sensibile unde este cazul.

UC-EC32. Generare rapoarte standard: Sistemul permite utilizatorilor autorizați să genereze rapoarte predefinite (ex. recrutare, formare, sancțiuni, distribuție grade, evoluție personal), cu selectarea perioadei și parametrilor, păstrând istoricul execuțiilor de raport.

UC-EC33. Accesare Dashboard analitic (KPI și trenduri): Sistemul permite Conducerii și utilizatorilor autorizați să vizualizeze indicatori și trenduri (KPI) privind resursa umană și cariera, cu posibilitatea de filtrare pe instituții/perioade, utilizând datele din dosare și păstrând trasabilitatea datelor afișate.

UC-EC34. Export rapoarte (PDF/Excel) cu control de acces: Sistemul permite utilizatorilor autorizați exportarea rapoartelor în formate standard (PDF/Excel), aplicând reguli de confidențialitate (ex. mascarea câmpurilor, watermark), și păstrând evidența exporturilor (cine/când/ce).

6.3.8. Integrare cu alte sisteme

UC-EC38. Integrare cu MConnect (preluare și reconciliere): Sistemul va fi integrat prin MConnect cu registrele de stat relevante (ex.: Registrul de Stat al Populației, registre educaționale gestionate de Ministerul Educației și Cercetării și alte registre guvernamentale aplicabile), pentru preluarea automată a datelor oficiale necesare funcționării e-CSP, pe baza identificatorilor unici, cu actualizarea și reconcilierea diferențelor apărute, menținerea jurnalizării tranzacțiilor, logarea erorilor și reluarea sincronizării în mod controlat, fără pierderi de date sau inconsistențe.

UC-EC39. Import inițial/migrare date profesionale din e-Personal PG: Sistemul permite importarea inițială a datelor profesionale istorice existente în e-Personal PG (angajări, instruiri, sancțiuni etc.), mapând câmpurile și atașamentele, stabilind statusul „Importat” și păstrând trasabilitatea sursei.

UC-EC40. Interfețe de schimb de date cu alte module e-CSP: Sistemul permite expunerea controlată (API) a datelor de carieră către alte module existente sau ulterior în dezvoltare (ex. e-Disciplinară, e-Personal din cadrul CSP), cu validarea drepturilor și jurnalizarea accesului.

VII. CERINȚELE NON-FUNCȚIONALE FAȚĂ DE SI E-CSP

În această secțiune sunt prezentate cerințele non-funcționale ale platformei e-CSP.

7.1. Cerințe de arhitectură

Cerință	Descriere
NFRQ001	**Standarde deschise** Arhitectura soluției se va baza pe standardele deschise corespunzătoare. Arhitectura soluției nu va utiliza standarde proprietare.
NFRQ002	**Arhitectura bazată pe microservicii**

	Soluția va avea o arhitectură bazată pe microservicii.
NFRQ003	**Mediul de execuție** Platforma va rula pe motorul de containere Docker și nu va depinde de vreo anumită instanță a sistemului de operare gazdă. Construcția imaginilor de containere va fi automatizată. (pentru detalii, accesați următorul link: https://docs.docker.com/develop) Rulând într-un mediu bazat pe containere, aplicația va fi elastică, inclusiv la adăugarea/eliminarea instanțelor de containere ale aplicației (peste numărul minim necesar de instanțe pentru disponibilitate ridicată), iar modificarea configurațiilor și a parametrilor soluției nu trebuie să afecteze activitățile în desfășurare, cum ar fi sesiunile active, cereri etc.
NFRQ004	**Site-uri multiple** Arhitectura soluției va asigura o disponibilitate ridicată, inclusiv în timpul implementării noilor versiuni, și posibilitatea de a rula simultan pe mai multe site-uri.
NFRQ005	**Cerințe de compatibilitate cu browser** Soluția va fi compatibilă cu cele mai recente două versiuni majore (de care se va ține cont la acceptarea sistemului) ale următoarelor browsere web: Chrome, Safari, FireFox și Edge.
NFRQ006	**Model de date detaliat** Modelul de date detaliat al soluției va fi descris complet printr-o schemă de date care poate fi citită automat, de exemplu, utilizând un limbaj DDL pentru baze de date relaționale. Dezvoltatorul va coordona în prealabil cu CSP formatul schemei modelului de date detaliat.

7.2. Cerințe de integrare

Cerință	Descriere
NFRQ007	**Serviciul de autentificare, autorizare și gestionare a utilizatorilor** Toate funcționalitățile de autentificare, autorizare și gestionare a utilizatorilor vor fi reutilizate din MPass prin integrarea cu acesta în conformitate cu documentația furnizată. Pentru mai multe informații despre MPass a se vedea Anexa care descrie ecosistemul digital sistemului.
NFRQ008	**Serviciul de jurnalizare** Toate funcționalitățile de jurnalizare și evidență a evenimentelor importante vor fi implementate prin integrarea cu MLog în conformitate cu documentația furnizată. Această cerință nu exclude necesitatea ca soluția să înregistreze diverse evenimente legate de sistem în propria infrastructură de jurnalizare. Pentru mai multe informații despre MLog a se vedea Anexa care descrie ecosistemul digital al sistemului.
NFRQ009	**Serviciul de notificare** Toate funcționalitățile de notificare vor fi implementate prin integrarea cu MNotify în conformitate cu documentația furnizată. Pentru mai multe informații despre MNotify a se vedea Anexa care descrie ecosistemul digital al sistemului.
NFRQ0010	**Integrare prin MConnect Events** Soluția va permite utilizarea serviciului guvernamental MConnect Events pentru publicarea și consumarea evenimentelor în timp real, în măsura în care sistemele externe și scenariile operaționale necesită acest mecanism de interoperabilitate.

7.3. Cerințe de performanță

Cerință	Descriere
NFRQ0011	**Procesare asincronă** Pentru generarea intrărilor – ieșirilor, ori de câte ori este posibil soluția va utiliza procesarea asincronă.
NFRQ0012	**Utilizatori simultani**

	Sarcina și performanța standard a soluției vor fi garantate pentru 100 de utilizatori simultani.
NFRQ0013	**Timpul de reacție** Timpul de reacție al funcționalităților soluției va fi până la 3 (trei) secunde. Excepțiile (ex.: transfer fișier, generare raport complex) se vor defini și agrea la etapa de analiză și proiectare Dezvoltatorul va enumera excepțiile și le va coordona/agrea cu Consiliul Superior al Procurorilor, la etapa de analiză și proiectare.
NFRQ0014	**Performanță independentă de fișiere.** Încărcarea, validarea (format/dimensiune), scanarea antivirus și indexarea fișierelor/anexelor vor fi executate asincron (în fundal), astfel încât să nu afecteze performanța interfeței web și a operațiunilor curente (navigare, căutare, deschidere dosar, salvare metadate). Pentru operațiunile de front-end și back-end (cu excepția transferului efectiv al fișierului), timpul de răspuns va rămâne ≤ 3 (trei) secunde, indiferent de numărul și dimensiunea fișierelor încărcate în sistem, în limitele parametrilor configurați de Administrator (dimensiuni/ tipuri acceptate).
NFRQ0015	**Control al încărcării sistemului.** Control încărcare și protecție resurse (front-end / back-end / bază de date). Soluția va implementa mecanisme de control al încărcării (coadă de procesare, limitare concurență, prioritizare) pentru operațiunile de scanare antivirus și indexare, astfel încât să nu satureze resursele aplicației sau ale bazei de date. Sistemul va preveni degradarea performanței prin limitarea consumului de CPU/RAM/IO al proceselor de procesare fișiere și va asigura menținerea timpului de răspuns ≤ 3 (trei) secunde pentru operațiunile uzuale ale aplicației.
NFRQ0016	**Indicatori cheie de performanță** Cadrul va măsura și va expune indicatorii cheie de performanță. Dezvoltatorul va propune lista indicatorilor și îi va coordona/agrea cu Consiliul Superior al Procurorilor, la etapa de dezvoltare.

7.4. Cerințe pentru interfața utilizatorului

Cerință	Descriere
NFRQ0017	**Interfață multilingvă** Soluția va susține o interfață utilizator multilingvă, prin formate specifice tipului de date (de ex., data, ora, intervale de timp, valuta etc.). Interfața front-end a soluției va fi livrată cel puțin în limba română, rusă și engleză. Back-end-ul va fi cel puțin în limba română. Versiunea implicită pentru utilizatorul final va fi limba română.
NFRQ0018	**Accesibilitate interfață utilizator** Interfața utilizatorului va fi conformă cu cel puțin Nivelul A din Ghidul privind accesibilitatea conținutului web 2.0. https://www.w3.org/TR/WCAG20/ Interfața utilizator va ține cont, în măsura aplicabilității, de principiile Modelului Unitar de Design (MUD) promovate de Agenția de Guvernare Electronică.
NFRQ0019	**Design receptiv / adaptiv** Interfața utilizatorului se va adapta automat la diferite rezoluții de afișare. Lățimea minimă a zonei de afișare va fi de 480px.
NFRQ0020	**Suport contextual** Componentele Interfeței utilizator vor include Sfaturi și Sugestii pentru elementele interfeței utilizator.
NFRQ0021	**Suport clienți** Toate paginile vor include contactele de asistență.
NFRQ0022	**Marcaje** Toate interfețele serviciilor trebuie să poată fi marcate, iar Utilizatorul să poată accesa mai târziu paginile marcate.
NFRQ0023	**URL prietenoase** Cadrul va utiliza URL prietenoase pentru accesarea paginilor serviciilor.

7.5. Cerințe de mentenanță

Cerință	Descriere
NFRQ0024	**Jurnalizare** Soluția va înregistra acțiunile și evenimentele într-o manieră structurată. Jurnalizarea va fi configurabilă și bazată pe un cadru de jurnalizare extensibil (cum ar fi log4net, nlog etc.). Cadrul de jurnalizare va susține, cel puțin, formatul JSON și următoarele ținte: consolă, fișiere de rulare, UDP și HTTP POST.
NFRQ0025	**Nivele de jurnalizare și înregistrările jurnalului de evenimente** Soluția va diferenția evenimentele și acțiunile pe care le înregistrează după cel puțin următoarele nivele: Critic, Eroare, Avertizare, Info, Depanare. Evenimentele de nivel Critic și Eroare vor fi înregistrate doar pentru erorile nerecuperabile care necesită intervenția umană. Înregistrările din jurnalul evenimentelor vor include cel puțin: • tipul evenimentului • timestamp-ul (marca de timp) când evenimentul a avut loc • nivelul evenimentului • componenta cadrului care a generat evenimentul • utilizatorul/agentul utilizatorului, IP care a declanșat evenimentul • identificatorul obiectului informațional afectat • detalii textuale despre evenimentul produs
NFRQ0026	**Închidere grațioasă** Soluția va implementa închiderea grațioasă și anume închiderea unei instanțe de container a aplicației nu va afecta activitățile în derulare, cum ar fi sesiunile active, cererile, jurnalele evenimentelor etc.
NFRQ0027	**Codul sursa** Dezvoltatorul va livra codul sursă pentru componentele soluției care nu sunt disponibile ca produse comerciale autonome de la părți terțe. Codul sursă va utiliza managerii de pachete pentru dependențele de bibliotecile terțe. Toate soft-urile necesare vor fi incluse în definiția imaginii containerului și bazate pe repozitoriul public de containere.
NFRQ0028	**Implementare** Dezvoltatorul va aplica procedura de implementare și instrumentele necesare. Procedura de implementare va îndeplini toate precondițiile înainte de inițierea instalării soluției. Implementarea va fi automatizată și va include inițializarea și alimentarea bazei de date.
NFRQ0029	**Actualizări de sistem** Actualizările de sistem vor fi automatizate, inclusiv scripturile de upgrade/downgrade a bazei de date sau codul. Pentru a permite rularea actualizărilor în mediul de producție, se recomandă operarea unor modificări incrementale în baza de date.

7.6. Cerințe de securitate

Cerință	Descriere
NFRQ0030	**Arhitectură securizată** Cadrul va avea un design securizat și se va conforma cu toate cerințele relevante specificate în HG 201/2017[1]. Dezvoltatorul va prezenta documentația de design și dovezile confirmative privind securizarea acestuia. Dezvoltatorul va coordona cu CSP formatul documentației, al documentelor confirmative și lista cerințelor cu care urmează să se conformeze.
NFRQ0031	**Principiul privilegiilor minime**

[1] https://www.legis.md/cautare/getResults?doc_id=98644&lang=ro

	Componentele cadrului se vor baza pe principiul privilegiilor minime și vor rula în regim de privilegii limitate în cadrul modelului drepturilor sistemului de operare. Documentația va arăta nivelul necesar de privilegiu pentru fiecare componentă a cadrului și raționamentele nivelului de acces propus
NFRQ0032	**Datele secrete și adrese** Datele secrete (parole, cheile și certificatele private, șirurile de conexiune etc.) și adresele serviciilor externe vor fi delimitate clar în documentația de configurare și ușor modificabile prin scripturi automatizate.
NFRQ0033	**Canale de comunicare securizate** Toată comunicarea platformei cu sistemele sau utilizatorii externi va avea loc prin canale de comunicare criptate.
NFRQ0034	**Autentificare utilizator/prin parolă** Platforma va utiliza doar MPass în calitate de mecanism de autentificare. Nici o altă formă de autentificare utilizator nu va fi utilizată.
NFRQ0035	**Minimizarea stocării datelor cu caracter personal** Platforma va minimiza cantitatea datelor identificabile personal stocate. De exemplu, nu este necesară stocarea numelui și prenumelui, deoarece acestea vor fi furnizate după autentificarea prin MPass. Platforma va respecta prevederile cu privire la prelucrarea datelor cu caracter personal din HG 1123/2010[2]. Dezvoltatorul va coordona cu CSP lista cerințelor cu care urmează să se conformeze.
NFRQ0036	**Securizare împotriva Top 10 vulnerabilități OWASP** Platforma va include controale de securitate pentru toate componentele sale pentru cel puțin Top 10 vulnerabilități OWASP[3].
NFRQ0037	**API health-check** Platforma va expune pregătirea și API-ul health-check prin solicitări HTTP GET. Health-checkul va verifica starea a cât mai multor componente ale platformei posibil. În cazul identificării unei erori, va fi trimis un mesaj de eroare lizibil pentru om.
NFRQ0038	**Gestiune roluri** Utilizatorii și rolurile acestora vor fi gestionate în MPass. Platforma va prelua rolurile utilizatorilor din MPass.
NFRQ0039	**Expirare sesiune** Platforma va include un mecanism de expirare a sesiunilor care îi va cere utilizatorului să se autentifice din nou după o perioadă de inactivitate. Perioada de inactivitate va fi configurabilă, iar cea implicită va fi de 30 minute.
NFRQ0040	**Validare intrări** Toate datele de intrare vor fi validate atât de client, cât și de server.
NFRQ0041	**Conținutul utilizatorului** Conținutul utilizatorului poate fi captat doar în format text. Platforma va interzice înserarea caracterelor speciale utilizate pentru formatarea și marcarea conținutului web special. Toate caracterele UNICODE vor putea fi inserate/vizualizate de componentele platformei.
NFRQ0042	**Accesare neautorizată** În cazul unor încercări de accesare neautorizată, platforma: • va înregistra astfel de încercări, atribuind acestora cel puțin nivelul EROARE; • va transmite utilizatorilor un mesaj de avertizare că accesul nu este autorizat, iar orice abuz va fi investigat.
NFRQ0043	**Integritate date**

[2] https://www.legis.md/cautare/getResults?doc_id=16012&lang=ro
[3] https://owasp.org/www-project-top-ten/

	Dezvoltatorul va asigura integritatea datelor prin oferirea unei soluții adecvate pentru prevenirea activităților interne neautorizate (de ex., ștergerea datelor de autorizare direct din baza de date). O soluție ar putea fi înlănțuirea declarațiilor semnate într-un blockchain.

7.7. Cerințe de garanție

Cerință	Descriere
NFRQ0044	**Perioada de garanție** Perioada de garanție va fi de 9 luni și va începe imediat după punerea în producție finală a soluției.
NFRQ0045	**Acțiuni de realizare a garanției** În perioada de garanție Dezvoltatorul: • va elimina toate defectele raportate de Client; • va soluționa toate incidentele raportate de Client în conformitate cu SLA convenite. Notă: Timpul de răspuns și soluționare nu va depăși 60 minute pentru erorile non-critice și 15 min pentru erorile critice. Incidentele vor fi soluționate în termen de 2 zile lucrătoare pentru erorile non-critice și de 4 zile pentru erorile critice. În cazul erorilor critice, la fiecare oră va fi furnizat un raport de progres.

7.8. Cerințe față de documentație

Cerință	Descriere
NFRQ0046	**Documente destinate utilizatorilor finali** Dezvoltatorul va elabora și prezenta următoarele documente destinate utilizatorilor finali: 1. Ghid interactiv ajustat la rolul utilizatorului (Solicitant, Solicitant autorizat, Administratorul prestatorului de serviciu, Operatorul prestatorului de serviciu, Administrator); 2. Manualele utilizatorului descărcabile în format PDF pentru Administratorul prestatorului de serviciu, Operatorul prestatorului de serviciu, Administrator etc. Toată documentația destinată utilizatorului final va fi perfectată în limba română.
NFRQ0047	**Tutoriale video** Dezvoltatorul va pregăti tutoriale video pentru principalele funcții de comun agreate cu CSP la etapa de dezvoltare. Tutorialele vor fi în limba română.
NFRQ0048	**Documentația tehnică** Dezvoltatorul va elabora și prezenta următoarele documente tehnice: 1. Documentația pentru arhitectura platformei (inclusiv descrierea modelelor în limbaj UML, cu un nivel suficient de detaliere a arhitecturii platformei); 2. Strategia testării; 3. Codul sursă compilabil și documentat pentru aplicațiile, componentele și testele unitare dezvoltate în cadrul Proiectului; 4. Manualul de instalare și configurare a platformei (inclusiv compilarea codului, scripturile de construcție a imaginii containerului, instalarea platformei, cerințele hardware și software, descrierea și configurarea platformei, procedurile de backup și de recuperare în caz de dezastru). Toată documentația tehnică poate fi în limba engleză.
NFRQ0049	**Documentația API** Dezvoltatorul va elabora și prezenta: 1. Ghidul de integrare API; 2. Descriere într-un limbaj standard, citibil atât de om, cât și de mașină (de ex. WSDL sau Swagger).

	Toată documentația API va fi în limba engleză.

7.9. Cerințe de instruire

Cerință	Descriere
NFRQ0050	**Sesiuni de instruire** Dezvoltatorul va realiza sesiuni de instruire online cu utilizarea modulelor de e-învățare bazate pe Moodle LMS pentru grupuri țintă, precum Administratorii, Administratorii prestatorilor de servicii, Operatorii prestatorilor de servicii.
NFRQ0051	**Materiale de instruire** Materialele de instruire – curricula, suporturile de curs (manual, tutoriale video, quiz-uri) pentru administratori, prestatori de servicii, managerii portalurilor și utilizatorii finali (persoane fizice și juridice) elaborate pe platforma e-învățare în baza Moodle LMS. Toate materialele/conținutul de instruire vor fi în limba română.

7.10. Drepturi de proprietate

Cerință	Descriere
NFRQ0052	**Licență software perpetuă** Dezvoltatorul va oferi CSP-ului dreptul de a rula și utiliza întreaga soluție cu toate componentele software incluse, fără limitări de timp, spațiu și funcționalități.
NFRQ0053	**Drepturi depline asupra datelor** CSP păstrează drepturile depline asupra datelor create cu ajutorul acestei soluții.
NFRQ0054	**Formatul open data** Soluția va păstra datele în format deschis sau va implementa mecanisme de extragere a datelor în format deschis, astfel permițând transferul/migrarea datelor într-un alt sistem.

7.11. Cerințe de acceptanță

Cerință	Descriere
NFRQ0055	**Acceptanță funcțională.** Sistemul va fi considerat acceptat doar dacă toate cerințele funcționale (FR) sunt implementate integral și validate prin scenarii de testare documentate și aprobate de CSP.
NFRQ0056	**Acceptanță performanță.** Sistemul va respecta timpul de răspuns de maximum 3 secunde pentru operațiunile uzuale, în condiții de încărcare definite, fără degradare cauzată de volum de date sau fișiere încărcate.
NFRQ0057	**Teste de performanță obligatorii.** Dezvoltatorul va executa teste de performanță și va prezenta raport tehnic detaliat (metodologie, scenarii, parametri, rezultate) înainte de punerea în producție.
NFRQ0058	**Dreptul la testare independentă.** CSP poate efectua, direct sau prin expertiză terță, testări suplimentare de performanță, securitate și stabilitate înainte de acceptanța finală.
NFRQ0059	**Remedierea neconformităților.** În cazul identificării neconformităților, dezvoltatorul va remedia deficiențele și va relua testarea până la atingerea parametrilor stabiliți, fără costuri suplimentare pentru CSP.
NFRQ0060	**Acceptanță securitate.** Sistemul va fi supus testelor de securitate (scanare vulnerabilități și, dacă este cazul, test de penetrare). Vulnerabilitățile critice și majore trebuie remediate înainte de acceptanță
NFRQ0061	**Remedierea neconformităților.** În cazul identificării neconformităților, dezvoltatorul va remedia deficiențele și va relua testarea până la atingerea parametrilor stabiliți, fără costuri suplimentare pentru CSP.
NFRQ0062	**Acceptanță integrare și interoperabilitate.** Integrarea cu sistemele/interne externe (ex. e-Management, MConnect, MLog etc.) va fi validată prin teste end-

	to-end care demonstrează transmiterea corectă, completă și fără duplicări a datelor.
NFRQ0063	**Predare cod sursă și drepturi de proprietate.** Acceptanța finală este condiționată de predarea integrală a codului sursă, inclusiv repository actualizat, istoric versiuni, documentație tehnică, scripturi de instalare și configurare, precum și transferul drepturilor patrimoniale conform contractului. Codul va fi livrat într-un sistem de versionare agreat (ex. GIT).
NFRQ0064	**Acceptanță DevOps și instalare replicabilă.** Dezvoltatorul va livra pipeline-urile și procedurile DevOps (build, testare, deploy), precum și documentația de instalare astfel încât CSP să poată reproduce independent mediile de dezvoltare, test și producție. Opțional, la solicitarea CSP, Dezvoltatorul va demonstra reinstalarea completă a sistemului într-un mediu controlat.
NFRQ0065	**Documentație și perioadă de stabilizare.** Acceptanța finală este condiționată de livrarea documentației complete (manual utilizator, administrator, arhitectură, API, backup/restore) și de funcționarea stabilă a sistemului într-o perioadă de stabilizare agreată contractual, fără incidente critice.

ANEXE

la Caietul de Sarcini pentru elaborarea Sistemului Informațional e-CSP

ANEXA „A”

Anexa „A”- MODUL DE REPARTIZARE ALEATORIE A SESIZĂRILOR DISCIPLINARE

1. Context

În cadrul procedurilor disciplinare, repartizarea sesizărilor către inspectori trebuie să se realizeze în mod aleatoriu, cu respectarea principiilor de imparțialitate, transparență și echitate în distribuirea sarcinii de muncă. Pentru a reduce riscurile asociate intervenției umane și pentru a asigura trasabilitatea completă a procesului, se impune digitalizarea acestei etape.

În acest scop, în cadrul Sistemului informațional e-CSP va fi dezvoltat un modul de repartizare aleatorie automată a sesizărilor disciplinare. Modulul va elimina factorul uman din procesul de selecție a inspectorului, va contribui la distribuirea echilibrată a volumului de lucru și va asigura posibilitatea auditării tehnice și juridice a fiecărei repartizări.

2. Obiect

Obiectul prezentei inițiative îl constituie dezvoltarea și implementarea unui modul software specializat, integrat în cadrul Sistemului informațional e-CSP, destinat automatizării procesului de repartizare a sesizărilor disciplinare. Modulul va asigura distribuirea automată, aleatorie și ponderată a sesizărilor către inspectori, în baza unor reguli prestabilite și verificabile, fără intervenție manuală în procesul de selecție.

Soluția informatică va garanta înregistrarea și păstrarea unei evidențe complete pentru fiecare operațiune de repartizare, astfel încât întregul proces să fie pe deplin trasabil și auditabil din punct de vedere tehnic și juridic.

3. Scop

Scopul dezvoltării modulului de repartizare aleatorie în cadrul Sistemului informațional e-CSP este de a asigura un mecanism automatizat, imparțial și verificabil de distribuire a sesizărilor disciplinare către inspectori. Modulul va garanta realizarea unei repartizări aleatorii echitabile, contribuind la echilibrarea volumului de muncă între inspectori și la utilizarea eficientă a resurselor instituționale.

Totodată, soluția va asigura trasabilitatea integrală a fiecărei etape din procesul de repartizare, cu respectarea situațiilor de incompatibilitate, recuzare sau abținere, și va reduce semnificativ riscul de influență umană în selectarea inspectorului responsabil de examinarea sesizării.

4. Domeniul de aplicare

Modulul de repartizare aleatorie integrat în Sistemul informațional e-CSP va fi utilizat exclusiv pentru distribuirea sesizărilor disciplinare privind procurorii, precum și a procedurilor disciplinare inițiate din oficiu. Acesta va acoperi doar procesele aferente răspunderii disciplinare și mecanismului de desemnare a inspectorului responsabil de examinarea acestor cauze.

Nu intră în domeniul de aplicare al modulului repartizarea altor tipuri de verificări sau activități desfășurate de Inspecție, cum ar fi controalele organizatorice sau alte proceduri cu caracter administrativ.

5. Principii funcționale obligatorii

Sistemul trebuie să respecte următoarele principii:

Principiu	**Descriere**
Aleatoriu	Selecția se face prin algoritm de generare aleatorie
Ponderat	Probabilitatea de selecție depinde de încărcarea inspectorului
Automat	Nicio persoană nu poate selecta manual inspectorul
Transparent	Toate etapele sunt logate și verificabile
Reproductibil	Procesul poate fi auditat și verificat ulterior

6. Fluxul funcțional al repartizării

6.1. Înregistrarea sesizării

- Sesizarea primește ID unic
- Status inițial: „În așteptare repartizare automată”

6.2. Generarea listei inspectorilor eligibili

Sistemul va exclude automat inspectorii care:

- sunt în concediu / suspendați
- au conflict de interese declarat
- au fost recuzați/abținuți în cauze conexe
- au atins pragul maxim de încărcare (configurabil)

6.3. Calcularea încărcării fiecărui inspector

Pentru fiecare inspector se calculează:
Încărcare = suma coeficienților de complexitate ai dosarelor active
Coeficientul de complexitate al unui dosar va fi configurabil (ex. 1–5).
Pentru Inspectorul-șef, sistemul va aplica suplimentar un coeficient distinct de capacitate operațională, configurat implicit la maximum 50% din capacitatea standard a unui inspector, în vederea reflectării atribuțiilor manageriale exercitate conform cadrului normativ aplicabil.

6.4. Determinarea ponderii de repartizare

Sistemul va transforma încărcarea într-o pondere invers proporțională:
Pondere = 1 / (Încărcare + 1)
Ponderile vor fi scalate într-un interval total numeric (ex. 1–1000).
În cazul Inspectorului-șef, ponderea de repartizare va fi ajustată automat prin aplicarea coeficientului de capacitate operațională, astfel încât probabilitatea de atribuire a dosarelor să fie proporțional redusă comparativ cu inspectorii standard.

6.5. Generarea intervalelor individuale

Fiecare inspector primește un sub-interval numeric proporțional cu ponderea sa.

Exemplu:

Inspector	**Interval**
A	1–250
B	251–600
C	601–1000

6.6. Generarea numărului aleatoriu

- Sistemul generează un număr aleatoriu între 1 și 1000
- Se utilizează generator de numere pseudo-aleatoare criptografic sigur (CSPRNG)

6.7. Atribuirea automată

- Sesizarea este atribuită inspectorului al cărui interval conține numărul generat.
- Statusul devine: „Repartizat automat”

7. Funcționalități obligatorii

7.1 Repartizare automată

- Declanșată automat la înregistrarea sesizării
- Fără buton de aprobare manuală

7.2 Redistribuire automată

În caz de:

- Recuzare
- incompatibilitate ulterioară
- suspendare inspector

Sistemul rulează din nou algoritmul, excluzând inspectorul inițial.

7.3 Jurnal de audit (obligatoriu)

Pentru fiecare repartizare sistemul va salva:

- lista inspectorilor eligibili
- încărcarea fiecăruia
- ponderile calculate
- intervalele generate
- numărul aleatoriu extras
- inspectorul selectat
- timestamp
- hash criptografic al operațiunii
- tipul inspectorului și coeficientul de capacitate aplicat la momentul repartizării

Jurnalul trebuie să fie nemodificabil.

8. Drepturi de acces

Rol	**Drepturi**
Inspector	vizualizare dosare proprii
Inspector-Șef	vizualizare rezultate + audit, fără modificare
Administrator sistem	mentenanță tehnică, fără posibilitate de influențare a repartizării
Auditor	acces read-only(citire) la evenimentele de logging (loguri)

9. Cerințe de securitate

- Generator aleatoriu criptografic
- Loguri semnate digital
- Istoric nemodificabil
- Control al accesului bazat pe roluri
- Toate operațiunile sunt jurnalizate

10. Cerințe tehnice

- API pentru interogarea statusului repartizărilor și preluarea datelor
- Interfață de vizualizare a încărcării inspectorilor
- Posibilitate de configurare a coeficienților de complexitate
- Scalabilitate pentru minimum 50.000 dosare

Anexa B. Ecosistemul digital al Sistemului Informațional e-CSP

2.1. Poziționarea sistemului în ecosistemul guvernamental

Sistemul informațional e-CSP este conceput ca o platformă procedurală internă (back-office), destinată gestionării proceselor operaționale ale Consiliului Superior al Procurorilor (CSP).
Sistemul e-CSP acoperă, la nivel funcțional, principalele domenii operaționale ale CSP, inclusiv gestionarea procedurilor disciplinare (modulul e-Disciplinară), gestionarea carierei (modulul e-Carieră), evaluarea și alte procese interne instituționale. Aceste module operează ca componente procedurale interne, fără a substitui rolul sistemelor oficiale de registratură și evidență.
e-CSP nu include funcționalități de registratură oficială și nu dublează sisteme existente, fiind integrat într-un model arhitectural hibrid, în care:

- **e-CSP (inclusiv modulele e-Disciplinară și e-Carieră)** asigură gestionarea fluxurilor procedurale, dosarelor electronice, deciziilor și proceselor interne;
- **e-Management CSP** reprezintă sistemul oficial de înregistrare, numerotare și gestionare a corespondenței oficiale.

Integrarea între aceste componente este realizată bidirecțional, prin interfețe API securizate.

2.2. Principii generale de arhitectură și integrare

Sistemul e-CSP va fi dezvoltat și operat în baza următoarelor principii:

- separarea clară a responsabilităților între sistemele procedurale interne (e-CSP) și sistemele oficiale de evidență (e-Management);
- evitarea duplicării registrelor și funcționalităților existente;
- arhitectură de tip API-first;
- interoperabilitate prin platforma guvernamentală MConnect, inclusiv suport pentru schimbul asincron de evenimente prin serviciul MConnect Events, acolo unde acesta este disponibil și aplicabil;
- trasabilitate completă a acțiunilor și evenimentelor;
- reutilizarea serviciilor și componentelor guvernamentale partajate disponibile prin ecosistemul digital guvernamental administrat de Agenția de Guvernare Electronică;
- conformitate cu standardele naționale de securitate și interoperabilitate.
- aplicarea, după caz, a principiilor Modelului Unitar de Design (MUD) pentru interfețele dezvoltate în cadrul sistemului;
- utilizarea și înregistrarea activelor semantice relevante în Sistemul informațional „Catalogul semantic”, conform cadrului guvernamental de interoperabilitate, pentru asigurarea interoperabilității, reutilizării și standardizării datelor la nivelul ecosistemului guvernamental digital;
- reutilizarea identificatorilor oficiali ai resurselor informaționale de stat de bază, inclusiv utilizarea IDNP ca identificator unic pentru persoanele fizice, fără crearea identificatorilor interni paraleli.

2.3. Integrarea cu platformele guvernamentale

e-CSP va asigura integrarea cu următoarele servicii guvernamentale, în funcție de necesitățile funcționale:

- MPass – pentru autentificare și autorizare (Single Sign-On);
- MSign – pentru semnarea electronică a documentelor generate în cadrul proceselor (inclusiv disciplinare și de carieră);
- MConnect – pentru schimbul de date cu sisteme informaționale și registre de stat;
- MLog – pentru jurnalizarea și auditarea acțiunilor și evenimentelor;
- MNotify – pentru transmiterea notificărilor către utilizatori;
    - MConnect Events – pentru sincronizarea evenimentelor și schimbul asincron de date între sisteme informaționale;

Integrarea cu aceste servicii se va realiza prin mecanisme standardizate, conform ghidurilor tehnice furnizate de autoritățile competente.

2.4. Integrarea cu sistemul e-Management CSP

e-Management reprezintă componenta critică a ecosistemului, responsabilă de:

- înregistrarea oficială a documentelor;
- atribuirea numerelor de evidență;
- gestionarea corespondenței oficiale interne și externe.

În acest context, integrarea dintre e-CSP și e-Management este bidirecțională și asigură schimbul continuu de documente, metadate și statusuri, după cum urmează:

- documentele oficiale generate în e-CSP (inclusiv cele aferente modulelor e-Disciplinară și e-Carieră) vor fi transmise către e-Management pentru înregistrare oficială, numerotare și expediere;
- documentele înregistrate în e-Management (inclusiv cele de intrare sau corespondență externă) vor fi transmise către e-CSP pentru procesare în cadrul fluxurilor procedurale;
- sistemele vor sincroniza în mod bidirecțional statusurile documentelor și metadatele asociate, asigurând consistența informației între procesele interne și evidența oficială;
- e-CSP poate iniția fluxuri de corespondență oficială prin e-Management, iar e-Management poate furniza actualizări relevante pentru procesele active din e-CSP.

Sistemele vor menține o relație unică și coerentă între documentele procedurale și înregistrările oficiale aferente, fără duplicarea registrelor.
e-CSP nu va implementa registre paralele sau mecanisme proprii de evidență oficială.

2.5. Fluxuri operaționale principale

Funcționarea sistemului se bazează pe următoarele fluxuri operaționale de bază:

Flux de intrare
Documentele sunt înregistrate în e-Management și transmise către e-CSP pentru procesare.
Flux de procesare
e-CSP (inclusiv modulele e-Disciplinară și e-Carieră) asigură:

- crearea și gestionarea dosarelor electronice;
- execuția fluxurilor procedurale specifice;
- interogarea registrelor externe prin MConnect;
- înregistrarea acțiunilor prin MLog.

Flux de decizie
Sistemul generează documente și permite semnarea acestora prin MSign.

Flux de ieșire
Documentele sunt transmise către e-Management pentru înregistrare și expediere, iar utilizatorii sunt informați prin MNotify și, după caz, prin mecanisme de livrare electronică (MDelivery, MCabinet).

2.6. Infrastructură și găzduire

Sistemul e-CSP va fi găzduit în infrastructura guvernamentală MCloud, administrată de STISC.
Arhitectura tehnică va include:

- utilizarea containerelor (ex. Docker);
- orchestrare prin Kubernetes (KaaS);
- separarea mediilor de dezvoltare, testare și producție;
- mecanisme de monitorizare și logging centralizat;
- măsuri de backup și recuperare în caz de dezastru.

2.7. Interacțiunea cu utilizatorii externi

e-CSP nu va expune direct interfețe de tip front-office pentru utilizatori externi.
Interacțiunea cu persoane fizice sau juridice se va realiza prin:

- sistemul e-Management (corespondență oficială);

- platforme guvernamentale dedicate (ex. MCabinet), în funcție de mecanismele existente.

2.8. Dispoziții finale

Ecosistemul digital al e-CSP este definit pentru a asigura:

- integrarea completă a modulelor funcționale (inclusiv e-Disciplinară și e-Carieră) în arhitectura guvernamentală existentă;
- utilizarea eficientă a serviciilor comune;
- evitarea suprapunerilor funcționale;
- separarea clară între procesele procedurale interne și evidența oficială a documentelor;
- scalabilitate și extensibilitate pentru dezvoltări ulterioare.

Această anexă stabilește cadrul de referință pentru proiectarea, dezvoltarea și integrarea sistemului e-CSP în ecosistemul digital al administrației publice.

Anexa „C” – Atribuire responsabilităților instituționale și definirea controlului accesului la funcționalități și date în cadrul sistemului informațional e-CSP
(modelele RACI și RBAC a SI e-CSP)

1. Scopul anexei

Prezenta anexă stabilește cadrul de referință privind:

- Atribuirea responsabilităților instituționale în procesele operaționale ale sistemului e-CSP (model RACI);
- Controlul accesului la funcționalități și date în cadrul sistemului (model RBAC).

Anexa are rolul de a asigura coerența între structura instituțională, procesele operaționale și mecanismele tehnice de autorizare implementate în sistem.

Modelele RACI și RBAC pot fi ajustate în faza de analiză detaliată, în comun cu Beneficiarul, în scopul alinierii la procesele operaționale reale, cu condiția respectării principiilor arhitecturale și de securitate definite în prezentul Caiet de Sarcini.

2. Matrice orientativă RACI a SI e-CSP

Sistemul informațional e-CSP va utiliza un model de atribuire a responsabilităților de tip RACI (Responsabil, Aprobă, Consultă, Informat) pentru delimitarea clară a rolurilor implicate în procesele operaționale.

Definirea responsabilităților

- R – execută activitatea (Responsabil)
- A – responsabil final pentru rezultat și **A**probă/Aprobare
- C – este consultat (Consultă)
- I – este informat (Informat)

Principii de aplicare

- fiecare activitate trebuie să aibă un singur rol „Aprobă”;
- rolurile „Responsabil” pot fi multiple, dar clar delimitate;
- separarea responsabilităților operaționale de cele decizionale este obligatorie;
- responsabilitățile tehnice (administrare, mentenanță, securitate) sunt distincte de cele operaționale;
- modelul RACI trebuie să reflecte structura instituțională și cadrul legal aplicabil CSP;
- matricea RACI va fi utilizată ca bază pentru definirea fluxurilor operaționale și a regulilor de business.

Cerințe de implementare

- sistemul trebuie să permită configurarea fluxurilor operaționale în conformitate cu modelul RACI;
- sistemul trebuie să asigure trasabilitatea responsabilităților pentru fiecare activitate;
- sistemul trebuie să permită evidențierea clară a rolurilor implicate în fiecare etapă a procesului;
- sistemul trebuie să asigure auditarea deciziilor și acțiunilor în conformitate cu rolurile definite;
- modificările în atribuirea responsabilităților trebuie să fie controlate și auditabile.

2.1. Integrare e-Management

Activitate / Proces (Use-Case)	Secretariat CSP	Inspector	Inspector-Șef	CDE / IT CSP	STISC
UC-EM-01 – Înregistrare document în e-Management	R	I	I	I	C	I
UC-EM-02 – Preluare document în e-CSP	R	I	I	I	C	I
UC-EM-03 – Transmitere document oficial din e-CSP	R	I	I	I	C	I

2.2. Modul e-Disciplinară

Activitate / Proces (Use Case)	Secretariat CSP	Inspector	Inspector-Șef	CDE	IT CSP	STISC
UC-ED01.01 – Înregistrare sesizare	R	I	I	I	C	I
UC-ED01.03 – Creare dosar disciplinar	R	I	I	I	C	I
UC-ED01.04 – Repartizare aleatorie	R	I	A	I	C	I
UC-ED02.01 – Investigare disciplinară	I	R	A	I	I	I
UC-ED02.02 – Elaborare raport	I	R	A	I	I	I
UC-ED03.01 – Examinare în CDE	I	C	C	A/R	I	I
UC-ED03.02 – Emitere decizie disciplinară	I	C	C	A/R	I	I
UC-ED03.03 – Transmitere decizie prin e-Management	R	I	I	I	C	I
UC-ED03.06A – Soluționare recuzare/abținere Inspector-șef	I	I	C	A/R	I	I

2.3. Modul e-Carieră

Activitate / Proces (Use Case)	Secretariat CSP	Utilizator (procuror)	CSEP / IT CSP	STISC
UC-EC01.01 – Creare dosar profesional	R	I	I	C	I
UC-EC01.02 – Actualizare dosar profesional	R	R	I	I	I
UC-EC02.01 – Inițiere concurs / procedură	R	I	A	I	I
UC-EC02.02 – Evaluare candidat / procuror	I	I	A/R	I	I
UC-EC02.03 – Emitere decizie carieră	I	I	A/R	I	I
UC-EC02.04 – Publicare / comunicare rezultat	R	I	I	C	I

2.4. Funcții tehnice și suport

Activitate / Proces	Secretariat CSP	Actori operaționali	IT CSP	STISC
Administrare aplicație e-CSP	I	I	R/A	I
Configurare roluri și drepturi (RBAC)	I	I	R/A	I
Monitorizare aplicație	I	I	R	A
Hosting, infrastructură, DevOps	I	I	C	R/A
Backup și continuitate	I	I	C	R/A

3. Modelul orientativ de control al accesului (RBAC)

Sistemul e-CSP va implementa un mecanism de control al accesului bazat pe roluri (Role-Based Access Control – RBAC), prin care accesul la funcționalități și date este acordat utilizatorilor în funcție de rolurile și atribuțiile instituționale ale acestora.

3.1. Matrice RBAC – roluri și permisiuni

Rol	Vizualizare dosare	Creare dosare	Modificare dosare	Gestionare documente	Aprobare / Decizie	Semnare electronică	Acces audit / loguri	Administrare sistem
Secretariat CSP	Da	Da	Da (limitat)	Da	Nu	Nu	Nu	Nu
Inspector	Da (proprii)	Da	Da (proprii)	Da	Nu	Nu	Nu	Nu
Inspector-Șef	Da (toate)	Da	Da	Da	Da (validare)	Da	Da (limitat)	Nu
Membru CDE / CSP / CSEP	Da	Nu	Nu	Da (limită procedurală)	Da (decizie finală)	Da	Da (limitat)	Nu
Utilizator extern	Da (proprii)	Da (depunere cereri/sesizări)	Nu	Nu	Nu	Nu	Nu	Nu
Auditor	Da (read-only)	Nu	Nu	Nu	Nu	Nu	Da (complet)	Nu
Administrator sistem (IT CSP)	Da	Da	Da	Da	Nu	Nu	Da	Da

Unde, „Da” indică drept de acces acordat, „Nu” indică lipsa dreptului de acces, iar mențiunea „limitat” indică restricționarea accesului în funcție de context (ex. dosare proprii, starea procesului sau alte reguli configurabile).

3.2. Principii de control al accesului

- accesul este acordat exclusiv pe baza rolurilor definite;
- rolurile reflectă atribuțiile instituționale ale utilizatorilor;
- un utilizator poate avea unul sau mai multe roluri;
- accesul la date este restricționat conform principiului „need-to-know”;
- separarea rolurilor operaționale, decizionale, administrative și de audit este obligatorie.
- rolul „Inspector-șef” include atât atribuții manageriale, cât și atribuții operaționale limitate. În cadrul mecanismului de repartizare aleatorie, sistemul va trata Inspectorul-șef ca participant eligibil cu capacitate redusă de încărcare, conform regulilor configurate și cadrului normativ aplicabil.

3.3. Autentificare și autorizare

- autentificarea utilizatorilor se realizează prin serviciul guvernamental MPass;
- autorizarea utilizatorilor se realizează la nivelul aplicației e-CSP, în baza rolurilor;
- sistemul trebuie să permită gestionarea rolurilor fără modificarea codului sursă.

3.4. Audit și trasabilitate

- toate acțiunile utilizatorilor sunt jurnalizate prin MLog;
- sistemul trebuie să asigure trasabilitatea completă a accesului și modificărilor;
- accesul la loguri este limitat la roluri autorizate.