Anexa nr.1
la Hotărârea Consiliului Superior al Procurorilor
nr.1-143/2026 din 14 mai 2026

Conceptul Sistemului informațional „e-CSP”

Capitolul I
DISPOZIȚII GENERALE

1. Sistemul informațional „e-CSP” *(în continuare - e-CSP)* constituie un ansamblu integrat de resurse software, hardware informaționale și organizatorice destinat formării, administrării, procesării și valorificării resursei informaționale aferente activității Consiliului Superior al Procurorilor (CSP) și a entităților funcționale din subordinea acestuia.

2. Sistemul informațional „e-CSP” reprezintă platforma informatică instituțională unică, concepută pentru digitalizarea, automatizarea și gestionarea integrată a proceselor operaționale, disciplinare și administrative aflate în competența CSP și a entităților funcționale din subordinea acestuia, prin asigurarea înregistrării, evidenței, repartizării aleatorii automate, examinării, monitorizării și arhivării electronice a sesizărilor și dosarelor disciplinare, administrării documentelor electronice și gestionării proceselor aferente carierei procurorilor, precum și prin furnizarea mecanismelor necesare raportării, auditării și controlului activităților desfășurate.

3. Destinația principală a e-CSP este formarea, gestionarea și utilizarea resursei informaționale instituționale, care să conțină totalitatea datelor, documentelor și informațiilor aferente proceselor de înregistrare, repartizare, examinare și soluționare a sesizărilor disciplinare, gestionării dosarelor disciplinare și administrative, administrării documentelor electronice și gestionării proceselor aferente carierei procurorilor, asigurând evidența electronică unitară, trasabilitatea completă a acțiunilor, precum și accesul controlat la informațiile gestionate, în conformitate cu competențele legale și drepturile de acces ale utilizatorilor sistemului.

4. Sistemul informațional „e-CSP” este găzduit pe Platforma tehnologică guvernamentală comună (MCloud) și este compatibil cu infrastructuri informatice bazate pe tehnologii de tip container.

5. Implementarea e-CSP are ca obiectiv principal consolidarea capacității instituționale a CSP, prin:

a) constituirea unei resurse informaționale instituționale unice și integrate, care să asigure evidența completă și gestionarea electronică a sesizărilor disciplinare, dosarelor disciplinare, documentelor și proceselor aferente competențelor CSP și ale entităților funcționale din subordinea acestuia;

b) asigurarea repartizării aleatorii automate a sesizărilor, în conformitate cu prevederile cadrului normativ aplicabil, cu respectarea principiilor de imparțialitate, transparență și echitate în distribuirea sarcinii de muncă;

c) creșterea eficienței operaționale prin automatizarea fluxurilor de lucru, reducerea dependenței de procese manuale și optimizarea proceselor de gestionare, examinare și soluționare a sesizărilor disciplinare;

d) garantarea trasabilității complete a operațiunilor efectuate în sistem, prin jurnalizarea automată a operațiunilor și instituirea mecanismelor necesare auditării tehnice și juridice;

e) consolidarea transparenței, responsabilității instituționale și capacității de monitorizare a activităților desfășurate, prin furnizarea mecanismelor de raportare, analiză și control a performanței operaționale;

f) asigurarea unui nivel înalt de securitate, integritate și confidențialitate a datelor gestionate, în conformitate cu legislația privind protecția datelor cu caracter personal și securitatea informațională;

g) facilitarea interoperabilității cu alte sisteme informaționale de stat și utilizarea serviciilor guvernamentale partajate, în vederea eficientizării schimbului de date și a proceselor administrative.

6. Principiile care stau la baza creării e-CSP sunt:

a) principiul legalității;

b) principiul veridicității datelor;

c) principiul imparțialității;

d) principiul transparenței și trasabilității;

e) principiul controlului accesului bazat pe roluri;

f) principiul plenitudinii și integrității datelor;

g) principiul controlului asupra formării și utilizării sistemului;

h) principiul modularității și scalabilității;

i) principiul securității informaționale;

j) principiul confidențialității;

k) principiul interoperabilității;

l) principiul auditabilității;

m) principiul eficienței operaționale;

n) principiul aplicării, după caz, a Modelului Unitar de Design (MUD).

Capitolul II
CADRUL NORMATIV-JURIDIC AL SISTEMULUI INFORMAȚIONAL e-CSP

7. Dezvoltarea, administrarea și gestionarea e-CSP este reglementată, de următoarele acte normative:

a) Legea nr.467/2003 cu privire la informatizare și la resursele informaționale de stat;

b) Legea nr.71/2007 cu privire la registre;

c) Legea nr.195/2024 privind protecția datelor cu caracter personal;

d) Legea nr.148/2023 privind accesul la informațiile de interes public;

e) Legea nr.3/2016 cu privire la Procuratură, cu modificările și completările ulterioare;

f) Legea nr.124/2022 privind identificarea electronică și serviciile de încredere;

g) Hotărârea Guvernului nr.1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass);

h) Hotărârea Guvernului nr.128/2014 privind platforma tehnologică guvernamentală comună (MCloud);

i) Hotărârea Guvernului nr.708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog);

j) Hotărârea Guvernului nr.967/2016 cu privire la mecanismul de consultare publică cu societatea civilă în procesul decizional;

k) Hotărârea Guvernului nr.562/2025 cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice;

l) Hotărârea nr.737/2017 pentru aprobarea Regulamentului cu privire la normele de creare a serviciilor de rețea și termenul de implementare a acestora;

m) Hotărârea Guvernului nr.414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat;

n) Hotărârea Guvernului nr.276/2020 pentru aprobarea Conceptului serviciului guvernamental de notificare electronică (MNotify) și a Regulamentului privind modul de funcționare și utilizare a serviciului guvernamental de notificare electronică (MNotify);

o) Hotărârea Guvernului nr.386/2020 cu privire la planificarea strategică;

p) Hotărârea Guvernului nr. 650/2023 cu privire la aprobarea Strategiei de transformare digitală a Republicii Moldova pentru anii 2023-2030;

q) Hotărârea Guvernului nr. 677/2025 cu privire la consolidarea accesului la serviciile publice electronice în cadrul Portalului guvernamental integrat EVO utilizat la prestarea serviciilor publice electronice și aprobarea măsurilor necesare pentru implementarea modelului unitar de design;

r) Hotărârea Guvernului nr.260/2025 privind aprobarea Agendei de reforme aferente Planului de creștere al Republicii Moldova pentru anii 2025-2027;

s) Hotărârea Guvernului nr.306/2025 privind aprobarea Programului Național de Aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029;

t) Hotărârea Guvernului 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;

u) Reglementarea tehnică „Procesele ciclului de viață al software-ului” RT 38370656-002:2006, aprobată prin Ordinul ministrului dezvoltării informaționale nr.78/2006;

v) Regulamentul cu privire la organizarea și funcționarea Consiliului Superior al Procurorilor aprobat prin Hotărârea Consiliului Superior al Procurorilor nr.1-420/2025 din 11.12.2025.

Capitolul III
SPAȚIUL FUNCȚIONAL AL SISTEMULUI INFORMAȚIONAL „e-CSP”

8. Sistemul informațional e-CSP asigură realizarea unui ansamblu de funcții de bază, orientate spre gestionarea integrată a proceselor instituționale, după cum urmează:

a) formarea și gestionarea resursei informaționale aferente activității CSP și entităților funcționale din subordinea acestuia, prin asigurarea evidenței electronice a sesizărilor, dosarelor disciplinare, documentelor și altor obiecte informaționale relevante;

b) înregistrarea electronică a sesizărilor disciplinare și a altor documente aferente proceselor disciplinare, cu atribuirea automată a identificatorilor unici și formarea dosarului disciplinar electronic;

c) asigurarea repartizării aleatorii automate a sesizărilor disciplinare către inspectori, prin intermediul unui mecanism bazat pe algoritmi obiectivi, fără intervenție

umană în procesul de selecție, cu respectarea principiilor imparțialității, echității și transparenței;

d) gestionarea dosarelor disciplinare în format electronic, inclusiv crearea, completarea, actualizarea, transmiterea, monitorizarea și arhivarea acestora, precum și gestionarea materialelor și documentelor aferente;

e) gestionarea electronică a documentelor instituționale, inclusiv crearea, înregistrarea, stocarea, clasificarea, căutarea, accesarea și arhivarea acestora;

f) asigurarea evidenței și gestionării proceselor aferente carierei procurorilor, în conformitate cu competențele CSP;

g) asigurarea trasabilității complete a operațiunilor efectuate în sistem, prin jurnalizarea automată a acțiunilor utilizatorilor și a evenimentelor de sistem;

h) asigurarea controlului accesului la resursele informaționale, în funcție de rolurile și drepturile utilizatorilor, în conformitate cu competențele stabilite prin cadrul normativ;

i) generarea rapoartelor, statisticilor și analizelor necesare monitorizării activităților desfășurate și susținerii procesului decizional;

j) asigurarea interacțiunii cu alte sisteme informaționale de stat, precum și conexiunea cu platforme și servicii guvernamentale partajate;

k) asigurarea securității, integrității și protecției datelor gestionate, în conformitate cu cerințele de securitate informațională aplicabile sistemelor informaționale de stat.

9. Din punct de vedere funcțional, e-CSP este structurat pe următoarele componente:

1. Conturul *„e-Disciplinar”*, care asigură următoarele funcții:

a) înregistrarea electronică a sesizărilor disciplinare și formarea automată a dosarului disciplinar electronic;

b) repartizarea aleatorie automată a sesizărilor disciplinare către inspectori, prin intermediul mecanismului informatic, în conformitate cu prevederile cadrului normativ aplicabil;

c) gestionarea dosarului disciplinar electronic, inclusiv completarea, actualizarea, transmiterea și arhivarea acestuia;

d) gestionarea documentelor, materialelor și probelor aferente procedurii disciplinare;

e) gestionarea fluxurilor de lucru aferente procedurii disciplinare, inclusiv transmiterea dosarelor către entitățile competente;

f) evidența și monitorizarea etapelor procedurale și a statutului dosarelor disciplinare;

g) asigurarea trasabilității complete a operațiunilor efectuate în cadrul procedurii disciplinare.

2. Conturul *„e-Carieră”*, care asigură următoarele funcții:

a) gestionarea dosarelor electronice aferente carierei procurorilor;

b) gestionarea proceselor de selecție, evaluare și promovare a procurorilor;

c) repartizarea aleatorie a dosarelor și cererilor aferente proceselor de evaluare și selecție;

d) gestionarea documentelor și informațiilor aferente proceselor de carieră;

e) generarea rapoartelor și analizelor aferente proceselor gestionate.

3. Conturul *„e-Management al documentelor”*, care asigură următoarele funcții:

a) înregistrarea electronică a documentelor;

b) gestionarea fluxurilor documentare;

c) stocarea și arhivarea electronică a documentelor;

d) clasificarea, căutarea și accesarea documentelor;

e) gestionarea nomenclatoarelor și clasificatoarelor aferente documentelor;

f) asigurarea trasabilității documentelor și a operațiunilor efectuate asupra acestora.

4. Conturul *„Raportare și analiză”*, care asigură următoarele funcții:

a) generarea rapoartelor operaționale și statistice;

b) generarea rapoartelor analitice și a indicatorilor de performanță;

c) monitorizarea activităților desfășurate în sistem;

d) exportarea datelor și rapoartelor, în conformitate cu drepturile de acces ale utilizatorilor.

5. Conturul *„Gestiunea sistemului informatic”*, care asigură următoarele funcții:

a) configurarea parametrilor generali ai sistemului informatic;

b) gestiunea resurselor sistemului informatic;

c) administrarea conturilor de utilizatori și gestionarea drepturilor de acces ale acestora;

d) gestiunea nomenclatoarelor și clasificatoarelor și metadatelor utilizate;

e) gestiunea notificărilor și mesajelor generate de sistem;

f) jurnalizarea evenimentelor de sistem.

Notă: Contururile funcționale ale e-CSP reprezintă componente logice ale sistemului informațional și nu constituie sisteme informaționale distincte. În cazul gestionării documentelor, funcționalitățile aferente e-CSP se implementează în interoperabilitate cu sistemul instituțional e-Management utilizat pentru evidența oficială și circulația documentelor CSP. e-CSP nu substituie și nu dublează funcțiile de registratură și evidență oficială asigurate de sistemul e-Management.

10. Sistemul informațional e-CSP interacționează cu sisteme informaționale partajate și alte resurse și sisteme informaționale de stat, după cum urmează:

a) Serviciul electronic guvernamental de autentificare și control al accesului (MPass) - pentru autentificarea utilizatorilor și gestionarea controlului accesului în cadrul sistemului pe bază de roluri;

b) Platforma de interoperabilitate (MConnect) - pentru asigurarea interoperabilității și realizarea schimbului de date cu alte sisteme informaționale de stat; inclusiv serviciul MConnect Events, pentru schimbul sincron și asincron de date și evenimente între sistemele participante;

c) Serviciul electronic guvernamental de jurnalizare (MLog) – pentru asigurarea mecanismelor securizate și flexibile de jurnalizare, monitorizare și audit al evenimentelor generate în contextul utilizării sistemului informațional;

d) Serviciul guvernamental de notificare electronică (MNotify) - pentru notificarea utilizatorilor sistemului;

e) Serviciul guvernamental integrat de semnătură electronică (MSign) - pentru asigurarea semnării electronice a documentelor și validării autenticității acestora.

11. Interfața utilizator a e-CSP este proiectată astfel, încât:

a) să ofere o interfață ergonomică, intuitivă și accesibilă tuturor categoriilor de utilizatori. Interfața utilizator a platformei reprezintă un design grafic echilibrat, distinct și adaptabil pentru majoritatea dispozitivelor utilizate;

b) să asigure o interfață în limbile română (implicit), engleză și rusă;

c) să furnizeze interfețe personalizate în funcție de categoria utilizatorilor, rolurile, atribuțiile și drepturile de acces ale acestora.

Capitolul IV
STRUCTURA ORGANIZAȚIONALĂ A SISTEMULUI INFORMAȚIONAL e-CSP

12. Proprietarul Sistemului informațional „e-CSP” este statul.

13. Posesorul și deținătorul e-CSP este CSP, care asigură condițiile juridice, financiare și organizatorice necesare pentru crearea, administrarea, utilizarea, mentenanța și dezvoltarea sistemului.

14. Administratorul tehnic al infrastructurii guvernamentale utilizate pentru găzduirea e-CSP este Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică”, care își exercită atribuțiile în conformitate cu cadrul normativ privind administrarea tehnică și menținerea resurselor și sistemelor informaționale de stat.

15. Utilizatori ai Sistemului informațional e-CSP sunt:

1. utilizatori interni:

a) administratorul de sistem – persoana responsabilă de administrarea tehnică, gestionarea și menținerea operațională a sistemului informatic, precum și de efectuarea activităților necesare funcționării acestuia;

b) persoanele autorizate care, în exercitarea atribuțiilor de serviciu, utilizează sistemul în scopul îndeplinirii competențelor stabilite de legislația în vigoare și actele normative interne ale CSP;

c) membrii CSP;

d) membrii Colegiului de disciplină și etică;

e) inspectorul-șef și inspectorii din cadrul Inspecției procurorilor;

f) personalul subdiviziunilor structurale ale CSP;

g) alte persoane autorizate, în conformitate cu cadrul normativ aplicabil și actele normative interne.

2. utilizatori externi, care includ persoanele fizice sau reprezentanții autorităților și instituțiilor care interacționează cu CSP prin intermediul sistemului, în limitele competențelor stabilite, după cum urmează:

a) procurorii, în cazurile prevăzute de cadrul normativ aplicabil;

b) persoanele fizice care depun sesizări sau cereri;

c) reprezentanții autorităților publice și instituțiilor care interacționează cu CSP;

d) alte persoane autorizate, în conformitate cu cadrul normativ aplicabil.

16. Gestionarea accesului utilizatorilor în cadrul e-CSP se realizează prin intermediul serviciului guvernamental de autentificare și control al accesului MPass, în baza rolurilor și competențelor stabilite.

Capitolul V
DOCUMENTELE DE BAZĂ ALE PORTALULUI SISTEMULUI INFORMAȚIONAL e-CSP

17. Documentele gestionate în cadrul Sistemului informațional e-CSP se clasifică, în funcție de rolul și destinația acestora, în următoarele categorii:

a) documente de intrare;

b) documente de ieșire;

c) documente tehnologice.

18. Documentele de intrare reprezintă totalitatea datelor, documentelor și informațiilor introduse în sistem, după cum urmează:

a) sesizările disciplinare depuse de persoane fizice sau juridice;

b) sesizările disciplinare depuse de autorități publice sau instituții;

c) sesizările disciplinare inițiate din oficiu, în conformitate cu cadrul normativ aplicabil;

d) cererile și demersurile aferente procedurilor disciplinare;

e) documentele și materialele probatorii anexate sesizărilor sau dosarelor disciplinare;

f) actele procedurale și documentele transmise de entitățile competente în cadrul procedurilor disciplinare;

g) documentele aferente proceselor de carieră a procurorilor, în conformitate cu competențele CSP;

h) datele și documentele introduse în sistem de către utilizatorii autorizați;

i) formularele electronice și datele aferente obiectelor informaționale gestionate în sistem;

j) alte documente și date necesare funcționării e-CSP, în conformitate cu cadrul normativ aplicabil.

19. Documentele de ieșire reprezintă rezultatul procesării informațiilor în cadrul sistemului, după cum urmează:

a) dosarele disciplinare electronice generate și gestionate în sistem;

b) rapoartele și actele întocmite în cadrul procedurilor disciplinare;

c) deciziile, hotărârile și actele procedurale generate în cadrul proceselor gestionate în sistem;

d) notificările generate automat de sistem privind statutul sesizărilor și dosarelor disciplinare;

e) rapoartele operaționale, statistice și analitice generate de sistem;

f) extrasele și informațiile furnizate utilizatorilor autorizați, în conformitate cu drepturile de acces stabilite;

g) datele și informațiile utilizate pentru monitorizarea și controlul proceselor gestionate în sistem;

h) alte documente generate de Sistemul informațional e-CSP, în conformitate cu cadrul normativ aplicabil.

20. Documentele tehnologice sunt acele înregistrări și resurse necesare funcționării și administrării sistemului, după cum urmează:

a) înregistrările privind utilizatorii sistemului și drepturile de acces ale acestora;

b) înregistrările jurnalului de audit și ale operațiunilor efectuate în sistem;

c) înregistrările privind repartizarea aleatorie a sesizărilor și dosarelor disciplinare;

d) nomenclatoarele, clasificatoarele și parametrii utilizați în sistem;
e) formularele electronice utilizate pentru gestionarea obiectelor informaționale;
f) configurațiile și parametrii funcționali ai sistemului;
g) ghidurile și instrucțiunile de utilizare a sistemului;
h) politicile și regulile de securitate aplicabile sistemului;
i) copiile de siguranță ale datelor și mecanismele de restaurare;
j) alte documente și resurse necesare funcționării și dezvoltării e-CSP.

Capitolul VI
SPAȚIUL INFORMAȚIONAL AL SISTEMULUI INFORMAȚIONAL e-CSP

21. Totalitatea obiectelor informaționale de bază care formează resursa informațională a e-CSP se determină în funcție de destinația acestora și include următoarele categorii: sesizarea disciplinară, dosarul disciplinar, jurnalul de audit, profilul de utilizator, șabloanele și rapoartele, precum și nomenclatoarele și clasificatorii.

22. *Sesizarea disciplinară* – reprezintă obiectul informațional care conține informația înregistrată în sistem, prin care se solicită examinarea unor fapte ce pot constitui abateri disciplinare.

23. Identificatorul obiectului informațional *„sesizarea disciplinară”* este numărul de ordine generat automat de sistem, având următoarea structură:

a) ID Sesizare - identificator unic al fiecărei sesizări disciplinare, generat automat de sistem, în format numeric sau alfanumeric;

b) Tip Sesizare - tipul sesizării disciplinare, dup caz: sesizare depusă de persoană fizică, sesizare depusă de autoritate publică, autosesizare, sesizare transmisă de altă instituție, sau alt tip prevăzut de clasificatorul sistemului;

c) Categoria sesizării - categoria sau tipologia sesizării disciplinare, conform clasificatorului stabilit în sistem;

d) ID Autor - identificatorul autorului sesizării, care poate reprezenta persoana fizică, persoana juridică, instituția sau utilizatorul sistemului care a înregistrat sesizarea;

e) ID Procuror - identificatorul unic al procurorului vizat în sesizare, dacă este cazul;

f) Data înregistrării - data și ora la care sesizarea disciplinară a fost înregistrată în Sistemul informațional e-CSP;

g) Obiectul sesizării - descrierea succintă a faptelor sesizate sau a obiectului sesizării disciplinare;

h) Documente asociate - referințe sau legături către documentele electronice anexate sesizării, inclusiv fișiere PDF, imagini, alte documente relevante;

i) Statutul sesizării - starea curentă a sesizării disciplinare în cadrul sistemului (de exemplu: „înregistrată”, „repartizată”, „în examinare”, „finalizată”, „clasată”);

j) ID Inspector - identificatorul inspectorului desemnat prin mecanismul de repartizare aleatorie automată, responsabil de examinarea sesizării disciplinare;

k) Istoric sesizare - totalitatea înregistrărilor privind acțiunile efectuate asupra sesizării disciplinare, inclusiv data, ora, utilizatorul și tipul acțiunii efectuate.

l) Pentru persoanele fizice, identificatorii utilizați în cadrul obiectelor informaționale vor reutiliza identificatorii oficiali ai resurselor informaționale de stat de bază, inclusiv IDNP preluat din Registrul de Stat al Populației.

24. Scenariile de bază ale obiectului informațional *„sesizarea disciplinară”* sunt următoarele:

1. Crearea și înregistrarea sesizării disciplinare, care presupune:

a) introducerea datelor aferente sesizării disciplinare în sistem de către utilizatorii autorizați sau prin intermediul mecanismelor automatizate;

b) generarea automată de către sistem a identificatorului unic al sesizării disciplinare;

c) atribuirea statutului inițial al sesizării disciplinare;

d) formarea înregistrării electronice aferente sesizării disciplinare.

2. Validarea și completarea sesizării disciplinare, care presupune:

a) verificarea datelor introduse în sistem;

b) completarea informațiilor și anexarea documentelor relevante;

c) actualizarea statutului sesizării disciplinare, după caz.

3. Repartizarea aleatorie automată a sesizării disciplinare, care presupune:

a) inițierea automată a procesului de repartizare de către sistem;

b) aplicarea algoritmului de repartizare aleatorie, în conformitate cu regulile stabilite;

c) desemnarea automată a inspectorului responsabil;

d) înregistrarea rezultatului repartizării în sistem și în jurnalul de audit;

e) actualizarea statutului sesizării disciplinare.

4. Examinarea sesizării disciplinare, care presupune:

a) accesarea sesizării disciplinare de către inspectorul desemnat;

b) analizarea informațiilor și documentelor aferente sesizării;

c) completarea dosarului disciplinar cu informații și documente relevante;

d) actualizarea statutului sesizării disciplinare, în conformitate cu evoluția procedurii.

5. Transmiterea și utilizarea sesizării disciplinare, care presupune:

a) transmiterea electronică a sesizării sau a datelor aferente către entitățile competente, după caz;

b) utilizarea datelor în cadrul procedurilor disciplinare sau administrative;

c) asigurarea accesului controlat la sesizare, în conformitate cu drepturile de acces stabilite.

6. Finalizarea sesizării disciplinare, care presupune:

a) adoptarea deciziei aferente sesizării disciplinare, după caz;

b) actualizarea statutului sesizării disciplinare cu indicarea rezultatului procedurii;

c) marcarea sesizării disciplinare ca finalizată în sistem.

7. Arhivarea sesizării disciplinare, care presupune:

a) stocarea sesizării disciplinare și a datelor aferente în sistem, în conformitate cu cerințele privind păstrarea și arhivarea datelor;

b) asigurarea integrității, securității și accesului controlat la sesizarea disciplinară arhivată.

8. Jurnalizarea operațiunilor aferente sesizării disciplinare, care presupune:

a) înregistrarea automată în jurnalul de audit a tuturor acțiunilor efectuate asupra sesizării disciplinare;

b) asigurarea trasabilității complete a ciclului de viață al sesizării disciplinare.

25. Dosarul disciplinar reprezintă obiectul informațional care include totalitatea datelor, documentelor electronice, actelor procedurale și materialelor aferente unei

proceduri disciplinare inițiate în privința unui procuror, gestionate și stocate în cadrul Sistemului informațional e-CSP, pe întreaga durată a ciclului de viață al procedurii disciplinare.

26. Identificatorul obiectului informațional *„dosarul disciplinar”* este numărul unic generat automat de sistem, care asigură evidența, trasabilitatea și auditabilitatea procesului de repartizare automată a sesizărilor și dosarelor disciplinare, având următoarea structură:

a) ID Repartizare - identificator unic al fiecărei operațiuni de repartizare aleatorie, generat automat de sistem, în format numeric sau alfanumeric;

b) ID Sesizare/ID Dosar - identificatorul unic al sesizării disciplinare sau al dosarului disciplinar care face obiectul repartizării;

c) Tip obiect repartizat - tipul obiectului supus repartizării (de exemplu: sesizare disciplinară, dosar disciplinar, cerere, alt tip de obiect informațional);

d) ID Procuror - identificatorul unic al procurorului vizat în procedura disciplinară;

e) ID Inspector - identificatorul unic al inspectorului desemnat automat de sistem în urma procesului de repartizare aleatorie;

f) Lista inspectorilor eligibili - referință către lista inspectorilor eligibili pentru repartizare la momentul efectuării acesteia, conform criteriilor stabilite în sistem;

g) Algoritm de repartizare - identificatorul sau versiunea algoritmului utilizat pentru efectuarea repartizării aleatorii;

h) Valoare aleatorie generată - valoarea numerică sau alfanumerică generată automat de sistem, utilizată pentru determinarea rezultatului repartizării;

i) Data și ora repartizării - data și ora la care a fost efectuată repartizarea aleatorie în sistem;

j) Statut repartizare - starea repartizării (de exemplu: „efectuată”, „anulată”, „repetată”, „invalidată”);

k) Motiv redistribuire – motivul redistribuirii, în cazul în care repartizarea a fost anulată sau efectuată din nou (de exemplu: incompatibilitate, recuzare, eroare tehnică);

27. Scenarii de bază ale obiectului informațional *„dosar disciplinar”* sunt următoarele:

1. Crearea dosarului disciplinar, care presupune:

a) generarea automată a dosarului disciplinar în e-CSP, în baza unei sesizări disciplinare înregistrate sau în urma inițierii procedurii disciplinare din oficiu;

b) atribuirea automată a identificatorului unic al dosarului disciplinar;

c) asocierea dosarului disciplinar cu sesizarea disciplinară corespunzătoare;

d) atribuirea statutului inițial al dosarului disciplinar.

2. Repartizarea aleatorie automată a dosarului disciplinar, care presupune:

a) inițierea procesului de repartizare automată de către sistem, în conformitate cu regulile stabilite;

b) aplicarea algoritmului de repartizare aleatorie;

c) desemnarea automată a inspectorului responsabil de gestionarea dosarului disciplinar;

d) înregistrarea rezultatului repartizării în sistem și în jurnalul de audit;

e) actualizarea statutului dosarului disciplinar.

3. Gestionarea și completarea dosarului disciplinar, care presupune:

a) introducerea, actualizarea și gestionarea datelor aferente dosarului disciplinar;

b) anexarea documentelor, probelor și altor materiale relevante;

c) înregistrarea actelor procedurale și a acțiunilor efectuate în cadrul dosarului;

d) actualizarea statutului dosarului disciplinar, în funcție de evoluția procedurii.

3. Examinarea dosarului disciplinar, care presupune:

a) analizarea datelor și documentelor aferente dosarului disciplinar de către inspectorul desemnat;

b) efectuarea acțiunilor procedurale necesare, în conformitate cu cadrul normativ aplicabil;

c) completarea dosarului disciplinar cu actele și informațiile aferente examinării;

d) transmiterea dosarului disciplinar către entitățile competente, după caz.

5. Transmiterea și utilizarea dosarului disciplinar, care presupune:

a) transmiterea electronică a dosarului disciplinar către Colegiul de disciplină și etică sau alte entități competente, în conformitate cu cadrul normativ aplicabil;

b) utilizarea datelor și documentelor aferente dosarului disciplinar în procesul decizional;

c) asigurarea accesului controlat la dosarul disciplinar, în conformitate cu drepturile de acces stabilite.

6. Finalizarea dosarului disciplinar, care presupune:

a) înregistrarea deciziei finale aferente dosarului disciplinar;

b) actualizarea statutului dosarului disciplinar, în funcție de rezultatul procedurii;

c) marcarea dosarului disciplinar ca finalizat în sistem.

7. Arhivarea dosarului disciplinar, care presupune:

a) stocarea dosarului disciplinar și a datelor aferente în Sistemul informațional e-CSP, în conformitate cu cerințele privind păstrarea și arhivarea datelor;

b) asigurarea integrității, securității și accesului controlat la dosarul disciplinar arhivat.

8. Jurnalizarea operațiunilor aferente dosarului disciplinar, care presupune:

a) înregistrarea automată în jurnalul de audit a tuturor acțiunilor efectuate asupra dosarului disciplinar;

b) asigurarea trasabilității complete a ciclului de viață al dosarului disciplinar.

28. Jurnalul de audit reprezintă totalitatea înregistrărilor generate automat de Sistemul informațional „e-CSP”, cu privire la acțiunile utilizatorilor, operațiunile efectuate și evenimentele de sistem, în scopul asigurării trasabilității, securității, monitorizării și auditării funcționării sistemului.

29. Identificatorul obiectului informațional *„jurnalul de audit”* este numărul unic generat automat de sistem, care asigură evidența, monitorizarea și trasabilitatea tuturor acțiunilor și evenimentelor înregistrate în sistem, având următoarea structură:

a) ID Audit - identificator unic al fiecărei înregistrări din jurnalul de audit, generat automat de sistem, în format numeric sau alfanumeric;

b) ID Utilizator - identificatorul unic al utilizatorului care a efectuat acțiunea în sistem, dacă este cazul;

c) Rol utilizator - rolul utilizatorului care a efectuat acțiunea (de exemplu: inspector, administrator, membru CSP, utilizator extern);

d) Tip acțiune - tipul acțiunii efectuate (de exemplu: autentificare, creare sesizare, repartizare aleatorie, modificare dosar, vizualizare document, semnare document);

e) ID Obiect - identificatorul unic al obiectului informațional asupra căruia a fost efectuată acțiunea (de exemplu: Sesizare ID, Dosar ID, Utilizator ID);

f) Tip obiect - tipul obiectului informațional asupra căruia a fost efectuată acțiunea (de exemplu: sesizare disciplinară, dosar disciplinar, utilizator, document);

g) Data și ora acțiunii - data și ora la care a fost efectuată acțiunea, generate automat de sistem;

h) Rezultatul acțiunii - rezultatul acțiunii efectuate (de exemplu: succes, eșec, respins, anulat);

i) Adresa IP - adresa IP a dispozitivului de la care a fost efectuată acțiunea, dacă este cazul;

j) ID Sistem - identificatorul sistemului informațional care a înregistrat acțiunea;

k) Detalii acțiune - informații suplimentare privind acțiunea efectuată, inclusiv parametrii relevanți ai operațiunii;

l) Hash integritate - cod generat automat de sistem pentru asigurarea integrității și protecției înregistrării din jurnalul de audit împotriva modificării neautorizate.

30. Scenarii de bază ale obiectului informațional *„jurnalul de audit”*:

1. Generarea automată a înregistrărilor în jurnalul de audit, care presupune:

a) crearea automată a unei înregistrări în jurnalul de audit la fiecare acțiune efectuată de utilizatori sau la producerea unui eveniment de sistem;

b) atribuirea automată a identificatorului unic al înregistrării din jurnalul de audit;

c) înregistrarea datelor privind utilizatorul, acțiunea efectuată, obiectul vizat, data și ora acțiunii și rezultatul acesteia.

2. Înregistrarea operațiunilor efectuate asupra obiectelor informaționale, care presupune:

a) înregistrarea automată a operațiunilor de creare, modificare, vizualizare, transmitere, repartizare, semnare și ștergere a obiectelor informaționale;

b) înregistrarea automată a operațiunilor de repartizare aleatorie, inclusiv parametrii utilizați și rezultatul repartizării;

c) înregistrarea automată a operațiunilor de autentificare și acces în sistem.

3. Stocarea și păstrarea înregistrărilor din jurnalul de audit, care presupune:

a) stocarea automată a înregistrărilor în condiții care asigură integritatea, securitatea și disponibilitatea acestora;

b) protejarea înregistrărilor împotriva modificării, ștergerii sau accesului neautorizat;

c) păstrarea înregistrărilor în conformitate cu cerințele cadrului normativ aplicabil.

4. Accesarea și utilizarea jurnalului de audit, care presupune:

a) accesarea înregistrărilor din jurnalul de audit de către utilizatorii autorizați, în conformitate cu drepturile de acces stabilite;

b) utilizarea jurnalului de audit în scopuri de monitorizare, control și analiză a activităților desfășurate în sistem;

c) utilizarea jurnalului de audit în cadrul procedurilor de verificare, control și audit.

5. Monitorizarea și controlul funcționării sistemului, care presupune:

a) utilizarea jurnalului de audit pentru identificarea și analiza incidentelor de securitate sau a utilizării neautorizate a sistemului;

b) utilizarea jurnalului de audit pentru verificarea corectitudinii funcționării mecanismelor sistemului, inclusiv a mecanismului de repartizare aleatorie;

c) utilizarea jurnalului de audit pentru asigurarea responsabilității utilizatorilor sistemului.

6. Asigurarea trasabilității și auditabilității, care presupune:

a) menținerea istoricului complet al acțiunilor și evenimentelor din sistem;

b) asigurarea posibilității de reconstituire a operațiunilor efectuate asupra obiectelor informaționale;

c) asigurarea suportului informațional necesar desfășurării auditului tehnic, funcțional și juridic.

31. Profilul de utilizator reprezintă obiectul informațional care cuprinde totalitatea datele referitoare la utilizatorii autorizați ai e-CSP, inclusiv datele de identificare, funcția, rolurile atribuite, drepturile de acces și funcționalitățile sistemului disponibile utilizatorului.

32. Profilul de utilizator este o entitate de sistem și conține înregistrările tuturor rolurilor de sistem pe care le poate deține utilizatorul, având următoarea structură:

a) ID Utilizator - identificatorul înregistrării;

b) Nume - numele și prenumele utilizatorului;

c) Funcția - funcția utilizatorului;

d) Titlu - denumirea rolului;

e) Tip - descrierea rolului, nivelul de acces;

f) Data - data creării, data revocării;

g) Contacte - datele de contact ale utilizatorului (telefon, adresă de email).

33. Scenarii de bază ale obiectului informațional *„profilul de utilizator”*:

1. Înregistrarea unui nou utilizator cu un rol specific în sistem, care presupune:

a) accesarea, de către administratorul de sistem, a modulului de administrare a utilizatorilor;

b) inițierea procesului de creare prin selectarea opțiunii „Creare profil nou”;

c) completarea formularului de profil cu următoarele date: nume, funcție, date de contact, rol atribuit, nivel de acces;

d) validarea datelor - sistemul verifică dacă toate câmpurile obligatorii sunt completate.

e) salvarea profilului;

f) acordarea accesului utilizatorului conform rolului atribuit.

2. Actualizarea datelor unui profil.

a) accesarea, de către administratorul de sistem, a modulului de administrare a utilizatorilor;

b) selectarea profilului care urmează a fi modificat;

c) inițierea procesului de actualizare - se accesează formularul de editare a profilului;

d) modificarea câmpurilor relevante;

e) validarea datelor - sistemul validează formatul datelor;

f) salvarea modificărilor;

g) confirmarea modificărilor;

3. Revocarea unui utilizator sau a drepturilor de acces ale acestuia, care presupune:

a) accesarea, de către administratorul de sistem, a modulului de administrare a utilizatorilor;

b) selectarea profilului care urmează a fi revocat;

c) inițierea procesului de revocare;

d) confirmarea deciziei.

34. Șabloanele și rapoartele reprezintă obiectul informațional care include totalitatea funcționalităților necesare pentru generarea, salvarea și exportarea

rapoartelor, statisticilor și analizelor în baza datelor gestionate de e-CSP, inclusiv în formate DOCX, XLSX și PDF.

35. Obiectul informațional *„șabloane și rapoarte”* include următoarele elemente:

a) Template ID - identificator unic intern al fiecărui șablon;

b) Denumire - numele clar și concis al șablonului;

c) Descriere - obiectivul;

d) Indicatori incluși - listă/colecție de indicatori;

e) Frecvență raport - periodicitatea raportării;

f) Unitate măsură/cantitatea;

g) Format fișier - fișier atașat;

h) Responsabil rol (utilizatori).

36. Scenariile de bază ale obiectului informațional *„șabloane și rapoarte”*sunt:

a) crearea șablonului nou;

b) propunerea, de către operatorul sau proiectantul autorizat, a unui șablon care include anumite câmpuri, atribute și indicatori;

c) atribuirea unui Template ID, a versiunii și salvarea șablonului în registru, cu statutul „propus”;

d) validarea și publicarea șablonului, cu modificarea statutului în „activ”.

e) generarea de rapoarte analitice, rapoarte privind indicatori de performanță (set de indicatori KPI), rapoarte de monitorizare destinate utilizatorilor cu rol administrator, utilizate pentru aprecierea modalității de interacțiune a utilizatorilor autorizați cu e-CSP.

f) organizarea și afișarea conținutului fișierelor jurnalizate în vederea analizării și anticipării eventualelor vulnerabilități ale sistemului informatic.

37. Nomenclatoarele și clasificatorii reprezintă o categorie de obiecte de informații care cuprinde totalitatea metadatelor utilizate în cadrul e-CSP. Componenta de gestiune a nomenclatoarelor și clasificatoarelor (metadatelor) constă dintr-un mecanism care permite administrarea structurii și conținutului sistemului complex de nomenclatoare ale sistemului informațional, în vederea referențierii informației conținute în baza de date și adaptării conținutului bazei de date. Nomenclatoarele și clasificatoarele utilizate în cadrul sistemului pot fi documentate și înregistrate în Sistemul informațional „Catalogul Semantic”, conform cadrului guvernamental de interoperabilitate.

38. Identificatorul obiectului informațional *„nomenclatoare și clasificatori”* este numărul de ordine generat de sistem, având următoarea structură:

a) Nomenclator ID - identificator unic pentru fiecare nomenclator sau clasificator;

b) Denumire nomenclator - denumirea explicită a nomenclatorului;

c) Versiune - versiunea actuală a nomenclatorului;

d) Data validare - data aprobării/activării ultimei versiuni;

e) Statut - activ, revizuit.

39. Scenariile de bază ale obiectului informațional *„nomenclatoare și clasificatori”* sunt:

1. Importarea sau crearea nomenclatorului, care presupune:

a) importarea de către administratorul sistemului a nomenclatoarelor în formate standard, precum XML, JSON sau CSV, ori crearea acestora direct în sistem;

b) salvarea fiecărui cod cu metadatele aferente, inclusiv versiunea, sursa și descrierea;

2. Validarea nomenclatoarelor și clasificatorilor de către sistem.

3. Revizuirea nomenclatoarelor, care presupune:

a) lansarea unei noi versiuni a nomenclatorului sau clasificatorului;

b) adăugarea codurilor noi și marcarea codurilor învechite ca „expirate”;

c) păstrarea versiunilor anterioare în sistem, în scopuri de audit, verificare și trasabilitate.

Capitolul VII
SPAȚIUL TEHNOLOGIC AL SISTEMULUI INFORMAȚIONAL e-CSP

40. La dezvoltarea e-CSP se va aplica arhitectura multi-nivel (care include cel puțin următoarele nivele - baza de date, subsistem de păstrare fișiere, logica de aplicație și interfața cu utilizatorul), precum și o dezvoltare bazată pe livrări succesive și validare etapizată. Dezvoltarea sistemului va urma etape distincte, începând cu analiza și proiectarea detaliată, urmate de implementare, testare și livrare. Această abordare asigură o structură clară și predictibilă, o planificare riguroasă și o delimitare clară a fiecărei faze de dezvoltare. Arhitectura multi-nivel permite separarea clară a responsabilităților fiecărei componente, asigurând coerență și stabilitate în implementare.

41. Spațiul informațional al e-CSP utilizează standarde deschise și este compatibil cu sisteme care, la fel, utilizează standarde non-proprietare, cât și cu standardele deja existente.

42. Arhitectura complexului software-hardware, lista produselor software și a mijloacelor tehnice utilizate la crearea infrastructurii informaționale se determină de către posesor în etapele ulterioare de dezvoltare a Sistemului informațional e-CSP, ținând cont de:

a) implementarea unei soluții bazate pe SOA (Service-Oriented Arhitecture – arhitectură software bazată pe servicii), care oferă posibilitatea reutilizării unor funcții ale e-CSP cu noi funcționalități, fără a afecta funcționarea acestuia;

b) implementarea funcționalităților de arhivare (backup) și restabilire a datelor în caz de incidente.

43. Sistemul informațional „e-CSP” este proiectat astfel încât să poată fi scalat, prin extinderea resurselor hardware utilizate, pentru a acomoda numărul necesar de utilizatori, atât în regim normal de lucru, cât și în perioadele de vârf.

44. Sistemul de comunicații se bazează pe infrastructura și echipamentul rețelelor guvernamentale, care includ posibilitatea conectării redundante la internet. Infrastructura existentă este planificată în mod corespunzător, astfel încât să asigure nivelurile adecvate de performanță, capacitate, disponibilitate și securitate.

45. Interfețele de utilizare ale e-CSP este construit astfel încât să fie disponibil pentru înregistrare și pentru asigurare a accesului la informație prin servicii de rețea cu un regim de disponibilitate înaltă (24 de ore, 7 zile pe săptămână).

Capitolul VIII
ASIGURAREA SECURITĂȚII INFORMAȚIONALE

46. Asigurarea securității informaționale include totalitatea măsurilor juridice, organizatorice, economice și tehnologice, orientate spre prevenirea pericolelor securității resurselor și infrastructurii informaționale.

47. Securitatea informațională presupune protecția e-CSP, la toate etapele proceselor de creare, procesare, stocare și transmitere a datelor, împotriva acțiunilor accidentale sau intenționate, de natură artificială sau naturală, care pot cauza prejudicii posesorului, utilizatorilor resurselor informaționale sau infrastructurii informaționale.

48. Asigurarea securității informației se realizează în conformitate cu Cerințele minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr.201/2017.

49. Principalele pericole pentru securitatea informațională a Sistemului informațional e-CSP sunt:

a) colectarea și utilizarea ilegală a datelor;

b) încălcarea tehnologiei de selectare și prelucrare a datelor;

c) implementarea în produsele software și hardware a componentelor care realizează funcții neprevăzute în documentația aferentă acestor produse;

d) elaborarea și distribuirea programelor care afectează funcționarea normală a sistemelor informaționale geografice de stat și de comunicații electronice, precum și a sistemelor informaționale de securitate;

e) influența asupra sistemului cu parolă-cheie de protecție a sistemelor automatizate de prelucrare și transmitere a datelor spațiale;

f) scurgerea informației prin canalele tehnice;

g) implementarea dispozitivelor electronice pentru interceptarea informației în mijloacele tehnice de prelucrare, păstrare și transmitere a datelor, utilizând sistemele de comunicații, precum și în încăperile de serviciu ale autorităților administrației publice centrale și locale;

h) nimicirea, deteriorarea, distrugerea sau sustragerea suporturilor de informație mecanice sau de alt tip;

i) interceptarea informației în rețelele de transmitere a datelor și în liniile de comunicații, decodificarea acestei informații și impunerea informației false;

j) utilizarea, la crearea și dezvoltarea infrastructurii informaționale de comunicații electronice, a tehnologiilor informaționale naționale și internaționale, a mijloacelor de protecție a informației și a mijloacelor de informatizare care nu sunt certificate;

k) accesul neautorizat la resursele informaționale din băncile și bazele de date spațiale;

l) încălcarea prevederilor Legii nr.195/2024 privind protecția datelor cu caracter personal.

50. Sistemul informațional e-CSP asigură următoarele obiective de securitate:

a) *autentificarea* - garantează că zonele restricționate ale e-CSP vor fi accesibile doar persoanelor autorizate, cu o identitate verificată prin serviciul electronic guvernamental de autentificare și control al accesului (MPass), precum și prin alte modalități de autentificare, care permit autorizarea accesului la date cu caracter public din Sistem informațional;

b) *confidențialitatea* - garantează că datele înregistrate nu pot fi accesate de o parte terță neautorizată;

c) *integritatea* - garantează că datele înregistrate în nu au fost modificate sau alterate de o parte terță neautorizată;

d) *non-repudierea* - garantează că datele înregistrate nu pot fi negate ulterior de către utilizatorii care le-au realizat.

51. În vederea asigurării unui nivel adecvat al securității informaționale a sistemului informatic, posesorul e-CSP elaborează și implementează politica de asigurare a securității informaționale, care detaliază totalitatea compartimentelor de securitate, rolurile, drepturile și obligațiile fiecărui actor al sistemului informatic.

52. O cerință esențială pentru asigurarea securității informaționale o constituie păstrarea înregistrărilor de audit necesare pentru analiza integrității e-CSP și monitorizarea activităților desfășurate în cadrul acestuia. În acest scop, e-CSP se bazează pe un mecanism dublu de jurnalizare și audit, realizat atât intern, cât și prin utilizarea Serviciului electronic guvernamental de jurnalizare (MLog), în conformitate cu bunele practici internaționale în domeniu.

Capitolul IX
ÎNCHEIERE (DISPOZIȚII FINALE)

53. Sistemul informațional e-CSP reprezintă soluția digitală instituțională dezvoltată pentru susținerea activității CSP și a entităților funcționale din subordinea acestuia, în vederea asigurării gestionării electronice a sesizărilor disciplinare, dosarelor disciplinare, documentelor și proceselor aferente competențelor legale ale acestora, inclusiv prin implementarea mecanismului de repartizare aleatorie automată, în conformitate cu cerințele cadrului normativ aplicabil.

54. Prezentul Concept conține descrierea elementelor organizaționale, funcționale, informaționale și tehnologice principale, în baza cărora este conceput și implementat Sistemul informațional e-CSP, în scopul instituirii unui mecanism informatizat integrat care să permită evidența electronică, gestionarea, repartizarea automată, examinarea și arhivarea sesizărilor disciplinare și a dosarelor aferente, precum și asigurarea trasabilității complete și auditabilității proceselor gestionate în sistem.

55. Implementarea Sistemului informațional „e-CSP” și valorificarea potențialului tehnologiilor informației și comunicațiilor contribuie la modernizarea proceselor instituționale ale CSP, la creșterea eficienței operaționale, reducerea dependenței de procese manuale și minimizarea riscurilor asociate intervenției umane în procesele tehnice, inclusiv în procesul de repartizare a sesizărilor și dosarelor disciplinare.

56. Sistemul informațional „e-CSP” asigură un nivel înalt de transparență, securitate, integritate și trasabilitate a datelor și operațiunilor efectuate, facilitează monitorizarea și controlul proceselor disciplinare și administrative și contribuie la consolidarea capacității instituționale a CSP, în contextul procesului de digitalizare și transformare digitală a sectorului public din Republica Moldova.