**pentru aprobarea Conceptului-cadru al Sistemului informațional integrat al Ministerului Afacerilor Interne**

**------------------------------------------------------------**

În temeiul art. 22 lit. a) și b) din Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr. 6-12, art. 44), GuvernulHOTĂRĂȘTE:

**1.** Se aprobă Conceptul-cadru al Sistemului informațional integrat al Ministerului Afacerilor Interne, (se anexează).

**2.** Ministerului Afacerilor Interne:

1) va asigura implementarea Conceptului-cadru al Sistemului informațional integrat al Ministerului Afacerilor Interne la etapa elaborării cadrului normativ privind sistemele și resursele informaționale din posesia sa sau a structurilor organizaționale din sfera de competență a ministerului;

2) în comun cu structurile organizaționale din sfera de competență a ministerului, va asigura respectarea prevederilor Conceptului-cadru al Sistemului informațional integrat al Ministerului Afacerilor Interne la etapa creării, administrării, mentenanței, dezvoltării și utilizării sistemelor informaționale din sfera de competență.

**3.** Realizarea prevederilor prezentei hotărâri se va efectua din contul și în limitele mijloacelor financiare prevăzute în bugetul de stat și ale altor mijloace, conform legislației.

**Prim-ministru DORIN RECEAN**

Contrasemnează:

Viceprim-ministru,

ministrul dezvoltării

economice și digitalizării Dumitru Alaiba

Ministrul afacerilor interne Adrian Efros

Aprobat

prin Hotărârea Guvernului nr.\_\_\_\_/2023

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**CONCEPTUL-CADRU**

**al Sistemului informațional integrat al Ministerului Afacerilor Interne**

**INTRODUCERE**

Sistemului informațional integrat al Ministerului Afacerilor Interne (*în continuare – SII MAI*) are drept scop consolidarea capacităților instituționale în procesul realizării sarcinilor de prevenire şi combatere a criminalității, asigurării ordinii de drept şi a societății sigure.

În era modernă a tehnologiei și informației, eficiența, securitatea și colaborarea coerentă reprezintă baza fundamentală a fiecărei instituții guvernamentale responsabile de asigurarea ordinii publice și siguranței cetățenilor. Ministerul Afacerilor Interne, ca entitate-cheie în garantarea acestor principii, recunoaște necesitatea dezvoltării și implementării unui Sistem informațional integrat, care să permită o gestionare eficientă a resurselor, o coordonare îmbunătățită a acțiunilor și o mai bună comunicare între atât structurile interne ale Ministerului, cât şi cele externe.

Conceptul-cadru al SII MAI reprezintă un angajament al Ministerului Afacerilor Interne de a spori eficiența operațională, de a răspunde prompt la nevoile cetățenilor și de a asigura o guvernanță transparentă și responsabilă.

Conceptul-cadru definește direcțiile strategice, obiectivele și principalele componente ale SII MAI, evidențiind avantajele și beneficiile ce vor rezulta din implementarea sa.

Prin aprobarea Conceptului-cadru, Guvernul Republicii Moldova semnalează angajamentul său în modernizarea continuă a instituțiilor statului în conformitate cu standardele internaționale, contribuind astfel la o societate mai sigură, mai eficientă și mai conectată.

Conceptul-cadru al SII MAI este aliniat la Programul strategic de modernizare tehnologică a guvernării (e-Transformare), aprobat prin Hotărârea Guvernului nr. 710/2011 și urmărește asigurarea, în mod coerent, a necesităților Ministerului Afacerilor Interne din sfera respectivă pe termen mediu și lung, definind destinația, scopul și locul acestuia în spațiul informațional național, cadrul normativ aplicabil, arhitectura datelor, arhitectura de aplicații şi cea tehnologică a SII MAI.

**Capitolul I**

**DISPOZIȚII GENERALE**

**1.** SII MAI reprezintă totalitatea resurselor informaționale, a tehnologiilor informaționale și de comunicații, împreună cu structurile organizaționale asociate, ce interacționează în manieră organizată pentru colectarea, procesarea, stocarea și furnizarea informației, în scopul atingerii obiectivelor strategice ale MAI, executării funcțiilor și îndeplinirii misiunii Ministerului Afacerilor Interne (*în continuare – MAI*).

**2.** Scopul SII MAI este de a oferi o infrastructură modernă și eficientă pentru gestionarea datelor și informațiilor critice, în vederea optimizării proceselor operaționale, sporirii eficienței instituționale și consolidării capacității de a asigura siguranța cetățenilor și a ordinii publice în Republica Moldova. Acest sistem propune să îmbunătățească colaborarea și coordonarea dintre autoritățile administrative și instituțiile din subordinea MAI, precum și să faciliteze comunicarea cu alte entități de drept public sau privat.

**3.** Pentru asigurarea realizării scopului şi destinației stabilite, SII MAI este guvernat de patru categorii de principii:

1) principii generale de arhitectură;

2) principii pentru arhitectura de date;

3) principii pentru arhitectura de aplicații;

4) principii pentru arhitectura tehnologică.

**4.** Principiile generale de arhitectură sunt:

1) *prevalarea principiilor*, care presupune că principiile de arhitectură TIC se aplică tuturor subdiviziunilor MAI la gestiunea domeniului TIC;

2) *maximizarea beneficiului*, care presupune că deciziile ce țin de domeniul TIC sunt luate urmărind maximizarea beneficiului produs pentru MAI, ca o singură entitate;

3) *responsabilitatea tuturor pentru TIC* – toate părțile interesate participă la luarea deciziilor pe domeniul TIC și la implementarea acestora;

4) *continuitatea afacerii*, care presupune că MAI trebuie să-și poată continua activitățile operaționale cheie în cazul căderii sistemelor TIC;

5) *orientare spre servicii*, care implică faptul că Arhitectura TIC de scară largă a MAI trebuie să fie orientată pe prestarea serviciilor TIC către procesele de activitate ale MAI;

6) *conformitate și legalitate* – MAI va gestiona și utiliza domeniul TIC conform reglementărilor legale aplicabile, inclusiv cele ce țin de protecția proprietății intelectuale.

**5.** Principiile aplicate pentru arhitectura de date sunt:

1) *valoarea datelor MAI ca resursă*, care presupune că MAI este posesorul tuturor datelor deținute, gestionate și accesate de subdiviziunile MAI. Aceste date sunt considerate resurse de mare valoare pentru MAI și vor fi gestionate ca orice alte resurse ce prezintă valoare;

2) *partajarea datelor* – datele sunt partajate la nivel de funcții și instituții în cadrul MAI și utilizate în comun pentru îndeplinirea atribuțiilor de serviciu;

3) *accesibilitatea datelor* – datele sunt accesibile utilizatorilor pentru îndeplinirii atribuțiilor de serviciu;

4) *toate datele au un posesor responsabil primar pentru calitatea acestora* – pentru fiecare tip de date este desemnat un posesor în cadrul MAI, care va fi responsabil primar de deplinătatea şi corectitudinea acestora la nivelul MAI;

5) *o singură sursă primară de referință* – pentru orice tip de date este stabilită și utilizată o unică sursă de referință;

6) *prevalarea datelor în formă electronică* – dacă datele pot servi scopului în forma lor electronică, nu se vor reproduce și pe suport hârtie. Dacă datele vor trebui să existe și pe suport hârtie, va exista o copie a acestora și în formă electronică;

7) *vocabular comun de definire a datelor* – datele sunt definite complet la nivelul MAI, iar definițiile sunt ușor de înțeles și disponibile tuturor părților interesate;

8) *securitatea datelor* – datele sunt protejate împotriva utilizării și divulgării neautorizate, proporțional nivelului de sensibilitate a acestora.

**6.** Principiile pentru arhitectura de aplicații sunt:

1) *alinierea la arhitectura guvernamentală de scară largă* – arhitectura TIC este aliniată la arhitectura guvernamentală pe scară largă;

2) *arhitectură SOA* – arhitectura TIC este dezvoltată cu aplicarea principiilor specifice unei arhitecturi de sistem orientate pe servicii;

3) *asigurarea interoperabilității* – cadrul de interoperabilitate este stabilit și implementat la nivelul arhitecturii de aplicații MAI. Acesta este aliniat la cadrul de interoperabilitate guvernamental;

4) *orientare pe servicii autonome* – arhitectura de aplicații este orientată spre servicii TI autonome (funcțional și instituțional). Acestea pot fi combinate în scopul formării serviciilor aplicative compuse;

5) *dependențe slabe la nivelul arhitecturii de aplicații* – aplicațiile și componentele aplicative sunt dezvoltate asigurând dependența minimă a acestora de alte aplicații și componente aplicative;

6) *reutilizare aplicații și utilizare partajată* – MAI va reutiliza sau va utiliza partajat maxim posibil aplicațiile deținute de MAI și sistemele informaționale partajate instituite de către Guvern;

7) *independența de platforma tehnologică* – aplicațiile sunt independente în raport cu anumite tehnologii specifice și pot rula pe orice platformă tehnologică;

8) aplicații ușor de utilizat – aplicațiile sunt ușor și comod de utilizat pentru utilizatori, iar tehnologiile prezente sunt transparente.

**7.** Principiile pentru arhitectura tehnologică sunt:

1) *focusare pe termen lung pentru arhitectura tehnologică* indică că infrastructura tehnologică, reprezentând fundamentul pentru dezvoltarea durabilă a domeniului TI, necesită o planificare și o arhitectură bine definită, bazată pe obiectivele strategice și planurile de business pe termen mediu și lung;

2) *utilizarea tehnologiilor deschise la nivelul arhitecturii tehnologice* – principiul presupune că tehnologiile deschise permit implementarea unei infrastructuri tehnologice eficiente și flexibile;

3) *arhitectura tehnologică orientată pe servicii* – arhitectura orientată pe servicii (SOA) reprezintă modalitatea de definire și oferire a unei infrastructuri IT pentru a permite diferitor aplicații să schimbe date și să participe la procese de dezvoltare de servicii, prin reutilizarea părților componente;

4) *scalabilitate, adaptabilitate și flexibilitate pentru platforma tehnologică* – arhitectura tehnologică trebuie să ia în calcul necesitățile de viitor a organizației în vederea asigurării continuității activității;

5) *partajarea resurselor platformei tehnologice și partiționarea logică* –MAI și instituțiile subordonate trebuie să utilizeze resurse în comun, lucru ce va permite o eficientizare a utilizării, administrării și menținerii infrastructurii tehnologice;

6) *utilizarea platformei guvernamentale comune* – platforma tehnologică guvernamentală comună (MCloud) este selectată prioritar pentru furnizarea platformei tehnologice necesare implementării sistemelor aplicative ale MAI și subdiviziunilor subordonate;

7) *interoperabilitatea la nivelul arhitecturii tehnologice* – interoperabilitatea va permite o cooperare eficientă în vederea îndeplinirii funcțiilor și misiunilor instituțiilor ministerului, lucru ce va fi posibil în condițiile similitudinii/compatibilității structurilor TI și organizatorice, procedurilor specifice, tehnicii și serviciilor utilizate, etc.;

8) *virtualizarea resurselor la nivelul arhitecturii tehnologice* – virtualizarea resurselor permite utilizarea eficientă a acestora;

9) *securitatea arhitecturii tehnologice* – reprezintă un domeniu-cheie în gestionarea domeniului TI, definirea căreia trebuie să înceapă la nivelul infrastructurii tehnologice;

10) *fiabilitatea rețelei corporative* – rețeaua corporativă a MAI asigură nivele înalte de fiabilitate, rezistență la căderi și securitate pentru transport de date, video și voce.

**8.** Sarcinile de bază ale SII MAI sunt:

1) colectarea și gestionarea datelor: SII MAI va asigura colectarea și stocarea datelor şi informațiilor relevante privind realizarea misiunii şi sarcinilor MAI într-o manieră reglementată, ordonată şi aliniată la conceptul dezvoltării domeniului tehnologiei informației al MAI, în special la arhitectura TIC pe scară largă;

2) integrarea și interoperabilitatea: SII MAI va integra datele și informațiile autorităților administrative și instituțiilor din subordinea MAI, asigurând interoperabilitatea între sistemele existente. Acest lucru va permite un schimb fluid de informații și o coordonare eficientă între diferitele entități interne.

3) comunicarea și colaborarea: SII MAI va facilita comunicarea și colaborarea între autoritățile administrative și instituțiile din subordinea MAI, dar și cu alte organe şi structuri guvernamentale și entități partenere. Acest aspect este esențial pentru o coordonare eficientă în răspunsul la situații complexe.

4) asigurarea securității datelor: SII MAI va include măsuri robuste de securitate cibernetică pentru a proteja datele sensibile și confidențiale împotriva accesului neautorizat și a atacurilor cibernetice.

5) actualizarea și menținerea sistemului: SII MAI va necesita o gestionare continuă, actualizări și întreținere pentru a se asigura că rămâne performant, sigur și adaptat la schimbările tehnologice și nevoile în evoluție ale MAI.

**Capitolul II**

**CADRUL NORMATIV al SII MAI**

**9.** Crearea și funcționarea SII MAI sunt reglementate de actele normative în domeniul implementării și exploatării sistemelor informatice, tehnologiilor informaționale și comunicațiilor, precum şi prevederile prezentului Concept-cadru.

**10.** Actele normative de reglementare a sectorul TIC, lansare și exploatare a sistemelor informatice și securitatea informației sunt:

1) Legea nr.982/2000 privind accesul la informație;

2) Legea nr.1069/2000 cu privire la informatică;

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

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

5) Legea nr. 133/2011 privind protecția datelor cu caracter personal;

6) Legea nr. 305/2012 cu privire la reutilizarea informațiilor din sectorul public;

7) Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate;

8) Legea nr. 234/2021 cu privire la serviciile publice;

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

10) Hotărârea Guvernului nr. 735/2002 cu privire la sistemele speciale de telecomunicații ale Republicii Moldova;

11) Hotărârea Guvernului nr. 840/2004 cu privire la crearea Sistemului de telecomunicații al autorităților administrației publice;

12) Hotărârea Guvernului nr. 562/2006 cu privire la crearea sistemelor și resurselor informaționale automatizate de stat;

13) Hotărârea Guvernului nr. 1123/2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal;

14) Hotărârea Guvernului nr.329/2012 cu privire la Serviciul Guvernamental de Plăți Electronice (MPay);

15) Hotărârea Guvernului nr. 656/2012 cu privire la aprobarea Programului privind Cadrul de Interoperabilitate;

16) Hotărârea Guvernului nr. 822/2012 cu privire la serviciile sistemului de poștă electronică al autorităților administrației publice;

17) Hotărârea Guvernului nr.886/2013 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 305 din 26 decembrie 2012 privind reutilizarea informațiilor din sectorul public;

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

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

20) Hotărârea Guvernului nr. 405/2014 privind serviciul electronic guvernamental integrat de semnătură electronică (MSign);

21) Hotărârea Guvernului nr. 700/2014 pentru aprobarea Concepției privind principiile datelor guvernamentale deschise;

22) Hotărârea Guvernului nr. 701/2014 cu privire la aprobarea Metodologiei publicării datelor guvernamentale deschise;

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

24) Hotărârea Guvernului nr. 201/2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică;

25) Hotărârea Guvernului nr. 1140/2017 pentru aprobarea Regulamentului privind activitatea prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice;

26) Hotărârea Guvernului nr. 1141/2017 pentru aprobarea Regulamentului privind modalitatea de aplicare a semnăturii electronice pe documentele electronice de către funcționarii persoanelor juridice de drept public în cadrul circulației electronice ale acestora;

27) 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;

28) Hotărârea Guvernului nr. 211/2019 privind platforma de interoperabilitate (MConnect);

29) Hotărârea Guvernului nr. 375/2020 pentru aprobarea Conceptului Sistemului informațional automatizat „Registrul împuternicirilor de reprezentare în baza semnăturii electronice” (MPower) și a Regulamentului privind modul de ținere a Registrului împuternicirilor de reprezentare în baza semnăturii electronice;

30) Hotărârea Guvernului nr. 376/2020 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);

31) Hotărârea Guvernului nr. 413/2020 pentru aprobarea Regulamentului privind utilizarea, administrarea și dezvoltarea Portalului guvernamental al cetățeanului;

32) Hotărârea Guvernului nr. 712/2020 cu privire la serviciul guvernamental de plăți electronice (MPay);

33) Hotărârea Guvernului nr. 153/2021 pentru aprobarea Conceptului Sistemului informațional „Registrul resurselor și sistemelor informaționale de stat” și a Regulamentului privind modul de ținere a Registrului resurselor și sistemelor informaționale de stat;

34) Hotărârea Guvernului nr. 491/2022 cu privire la aprobarea modului de recunoaștere a semnăturilor electronice calificate create utilizând un certificat calificat al cheii publice eliberat de un prestator de servicii de încredere dintr-un stat membru al Uniunii Europene;

35) Ordinul ministrului dezvoltării informaționale nr. 78/2006 cu privire la aprobarea Reglementării tehnice nr. RT 38370656 - 002:2006 „Procesele ciclului de viață al software-lui”;

36) Ordinul ministrului dezvoltării informaționale nr. 94/2009 cu privire la aprobarea unor reglementări tehnice (modul de evidentă a serviciilor publice electronice, prestarea serviciilor publice electronice, asigurarea securității informaționale la prestarea serviciilor publice electronice, determinarea costului de elaborare și implementare a sistemelor informaționale automatizate);

37) Ordinul ministrului dezvoltării informaționale nr. 195/2016 cu privire la implementarea practicilor de management centralizat al serviciilor de Tehnologia Informației și Comunicațiilor în cadrul MAI.

**11.** Standarde TIC și cele relevante pentru SII MAI sunt:

1) SM 12207:2005 – „Procesele ciclului de viață al software-ului”;

2) SM SR ISO 15489-1:2012 – Informare și documentare. Managementul înregistrărilor. Partea 1: Generalități;

3) SM ISO/CEI/IEEE 15288:2015 – „Ingineria sistemelor și software-ului. Procesele ciclului de viață al sistemului”;

4) SM EN ISO/IEC 27001:2017 – Tehnologia informației. Tehnici de securitate. Sisteme de management al securității informației. Cerințe;

5) SM EN ISO/IEC 27002:2017 – Tehnologia informației. Tehnici de securitate. Cod de bună practică pentru managementul securității informației;

6) SM ISO 14641:2018 – Managementul documentelor electronice. Proiectarea și exploatarea sistemului informațional de stocare a documentelor electronice. Specificații;

7) SM EN ISO/IEC 15408-1:2020 – Tehnologia informației. Tehnici de securitate. Criterii de evaluare a securității IT. Partea 1. Introducere și model general;

8) SM EN ISO/IEC 15408-2:2020 – Tehnologia informației. Tehnici de securitate. Criterii de evaluare a securității IT. Partea 2. Componente funcționale de securitate;

9) SM EN ISO/IEC 15408-3:2020 – Tehnologia informației. Tehnici de securitate. Criterii de evaluare a securității IT. Partea 3. Componente de asigurare a securității;

10) Recomandările W3C (http://validator.w3.org) privind testarea paginilor WEB;

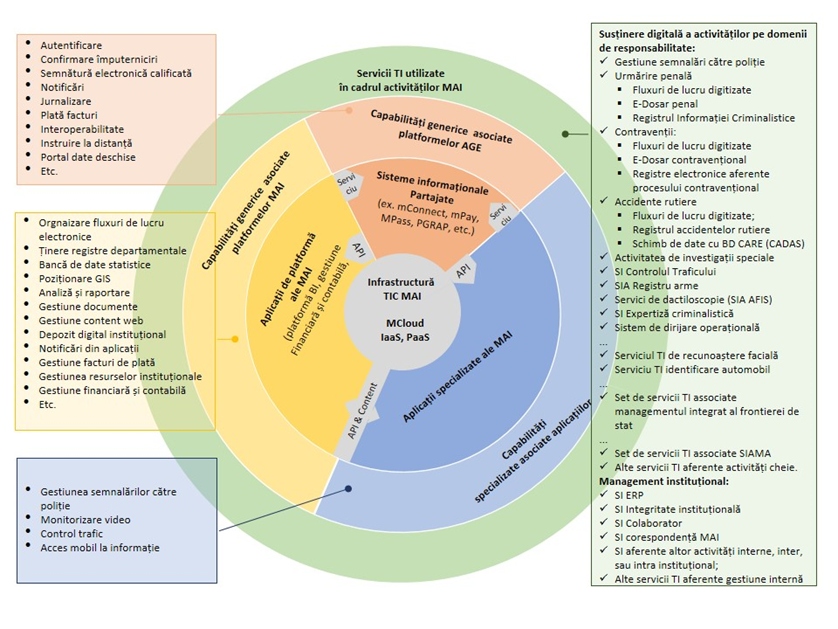
11) Standardul SDMX (*Statistical data and metadata exchange standard* - <http://sdmx.org>);

12) SM ISO/IEC 11179-1:2023 Tehnologia informației. Registre de metadate (MDR). Partea 1: Structura”.

**Capitolul III.**

**SPAȚIUL FUNCȚIONAL AL SII MAI**

**12.** SII MAI este format prin intermediul separării nivelelor funcționale distincte, prezente în figura nr. 1, în forma cercurilor concentrice. Fiecare nivel are asociate funcții specifice în cadrul SII MAI, care asigură realizarea funcțiilor de bază ale unui sistem informațional, stipulate conform legislației, precum și a funcțiilor specifice ce reies din destinația sistemului informațional.



**Figura nr. 1. Conceptul-cadrul al Sistemului Informațional Integrat al MAI**

**13.** Nivelul 1: Servicii TIC – la acest nivel funcțional sunt reprezentate serviciile TI utilizate de MAI în cadrul activităților sale sau în scopul prestării serviciilor către terțe părți. Este felul în care SII MAI este perceput din perspectiva proceselor de activitate ale MAI. Serviciile TIC pot fi grupate logic în scopul formării Sistemelor Informaționale Automatizate, relevante din perspectiva utilizatorilor și activităților MAI. Serviciile TIC susțin activitățile și procesele MAI într-o manieră flexibilă, business orientată și independentă de tehnologie.

**14.** Sunt identificate două tipuri de servicii TIC aferente SII MAI:

1) Servicii TIC pentru utilizatori, destinate salariaților MAI sau utilizatorilor externi autorizați (cetățeni, salariați ai altor instituții și terțe părți);

2) Servicii TIC pentru aplicații, destinate accesării de către alte aplicații în scopul îmbogățirii funcționalității acestora și livrării în final a unor servicii TIC pentru utilizatori. Serviciile TIC pentru aplicații pot fi accesate de aplicații din cadrul MAI sau din afara MAI.

Serviciile TIC sunt construite prin orchestrarea și agregarea de capabilități TIC accesibile în cadrul SII MAI.

**15.** Nivelul 2: Capabilități TIC reprezintă caracteristicile funcționale ale SII MAI. Capabilitățile TIC pot fi orchestrate și agregate pentru a construi servicii TIC. Una sau mai multe capabilități agregate formează un serviciu TIC din perspectiva proceselor de activitate ale MAI. Capabilitățile TIC sunt asociate aplicațiilor din arhitectura de aplicații a MAI, sau serviciilor TIC furnizate de terțe părți. Orchestrarea și agregarea capabilităților TIC se face prin configurarea, adaptarea și integrarea aplicațiilor din arhitectura de aplicații a MAI. Dezvoltarea de noi capabilități TIC implică achiziționarea și implementarea de noi aplicații sau dezvoltarea de sisteme TIC existente. Alternativ, MAI poate contracta servicii TIC externe ce vor furniza capabilitățile TIC necesare MAI. Capabilitățile cheie deținute de SII MAI sunt descrise în următoarea secțiune.

**16.** Nivelul 3: Arhitectura de aplicații include totalitatea componentelor de aplicații (platforme de aplicații, aplicații distincte și componente ale acestora) deținute de MAI sau accesibile MAI pentru a fi utilizate (ex. aplicațiile ce stau la baza serviciilor guvernamentale). Caracteristicile funcționale și non-funcționale ale aplicațiilor MAI constituie capabilități TIC în baza cărora sunt produse serviciile TIC. În contextul în care un sistem informațional al MAI prezintă o grupare logică a diferitor capabilități TIC, sistemele informaționale ale MAI pot avea la bază una sau mai multe aplicații din arhitectura de aplicații a MAI.

**17.** Arhitectura de aplicații a MAI deține o structură modulară, ce asigură flexibilitate pentru a răspunde la nevoile MAI, în același timp, facilitând reutilizarea componentelor deja existente. Toate aplicațiile susțin standarde unice pentru interoperabilitatea tehnică. Integrarea aplicațiilor este implicit asigurată prin intermediul platformei de interoperabilitate a MAI. Schimbul de date cu aplicații din afara arhitecturii de aplicații a MAI este implicit efectuat prin intermediul platformei de interoperabilitate a guvernului.

**18.** Următoarele grupe mari de aplicații formează arhitectura de aplicații a MAI:

1) aplicații de platformă ale MAI: dețin capabilități TIC ce răspund necesităților comune ale mai multor procese și activități ale MAI. Acest fapt facilitează reutilizarea aplicațiilor de platformă pentru a produce servicii TIC distincte;

2) aplicații specializate ale MAI: dețin capabilități TIC necesare susținerii în mod particular a anumitor activități și procese ale MAI. Capabilitățile specializate sunt dezvoltate atunci când nu pot fi asigurate prin orchestrarea capabilităților generice. De asemenea, sunt asociate aplicațiilor deja implementate și ce vor continua să fie utilizate;

3) sistemele informaționale partajate instituite de către Guvern și ale terților: dețin capabilități TIC caracteristice sistemelor informaționale partajate instituite de către Guvern și destinate pentru uzul comun al autorităților publice. Acestea pot răspunde și necesitățile MAI, caz în care sunt cooptate și tratate ca parte integrantă din arhitectura de aplicații a MAI.

Aplicațiile din arhitectura de aplicații a MAI (inclusiv serviciile guvernamentale) sunt interoperabile.

**19.** MAI dezvoltă, implementează și operează aplicații ca parte a SII MAI în scopul asigurării capabilităților TIC necesare producerii serviciilor TIC. Oricând MAI constată necesitatea unor capabilități TIC noi ce nu pot fi asigurate de arhitectura de aplicații curentă a MAI, va întreprinde următoarele acțiuni, în următoarea ordine:

1) va analiza posibilitatea obținerii capabilităților necesare, prin integrarea în arhitectura de aplicații a MAI a serviciilor guvernamentale disponibile;

2) va analiza posibilitatea dezvoltării aplicațiilor de platformă curente. Noi capabilități TIC pot fi asigurate prin implementarea de noi funcționalități ale aplicațiilor de platformă;

3) va analiza raționalitatea dezvoltării de noi aplicații specializate sau de platformă.

**20.** Nivelul 4: Arhitectura tehnologică include componente de infrastructură tehnologică destinate asigurării mediului TIC necesar funcționării performante și sigure a aplicațiilor din arhitectura de aplicații a MAI, precum și accesibilității acestora de către utilizatori și alte aplicații. Arhitectura tehnologică include: centre de date, echipamente de procesare și stocare date, rețele de comunicații, medii de operare și soft de sistem. Pentru asigurarea arhitecturii tehnologice potrivite, MAI va aplica următoarele principii:

1) va analiza ca primă opțiune posibilitatea obținerii componentelor de arhitectură tehnologică necesare în cadrul platformei guvernamentale MCloud;

2) va analiza posibilitatea reutilizării componentelor de arhitectură tehnologică deja existente în cadrul SII MAI;

3) va analiza posibilitatea dezvoltării arhitecturii tehnologice a MAI prin achiziționarea și implementarea de noi componente pentru arhitectura tehnologică.

**21.** MAI va integra în arhitectura tehnologică componente achiziționate sau închiriate de la alte terțe părți doar în cazul în care acestea nu pot fi oferite de platforma guvernamentală și nu este rațional a fi dezvoltate de MAI.

**22.** Pentru a corespunde necesităților, SII MAI va deține capabilitățile TIC cheie descrise în tabelul nr.1:

|  |  |  |
| --- | --- | --- |
| Nr. | CAPABILITĂȚI | descriere |
| CAPABILITĂȚI GENERICE ASOCIATE SOLUȚIILOR DE PLATFORMĂ ALE MAI  *Caracteristici funcționale dezvoltate pentru a răspunde necesităților comune în mai multe procese și activități ale mai. acest fapt facilitează reutilizarea tehnologiilor ce produc capabilitățile generice, sau utilizarea partajată în mai multe procese și activități.* | | |
|  | Organizare procese de activitate în formă electronică | Set de capabilități destinate a fi utilizate pentru organizarea proceselor și activităților MAI în baza fluxurilor de informație și documente în formă electronică. Susțin definirea și procesarea documentelor structurate. Susțin organizarea fluxurilor de circulație a documentelor și a scenariilor de operare și procesare a documentelor. Permit colaborarea în cadrul activităților, coordonarea și aprobarea documentelor. Accesul la documente și operații cu documentele este permis în bază multicriterială, inclusiv: tip document, informație conținută, rolul utilizatorului în cadrul procesului. Susțin interoperabilitatea între diferite procese, prin schimburi de informație și documente electronice structurate. Toate activitățile MAI ce țin de crearea, procesarea, distribuirea și accesarea de documente și informații structurate, pot fi susținute prin acest set de capabilități. |
|  | Depozitar de conținut digital | Set de capabilități destinate a fi utilizate în scopul stocării fișierelor de dimensiuni mari (audio, video, diferit format grafic, etc.). Permit altor sisteme informaționale, ce nu dețin capabilități potrivite de a păstra acest tip de conținut, să depoziteze fișierele și informația descriptivă asociată și să le acceseze la necesitate prin interfețe aplicative. Asigură indexarea conținutului (în baza metadatelor sau a conținutului textual) și oferă metode de căutare a informației conform criteriilor. Conținutul stocat poate fi partajat cu alte aplicații, sau nu. Utilizatorii nu dețin acces direct la informația din depozitarul de conținut. |
|  | Ținerea registrelor | Set de capabilități destinat definirii, implementării și ținerii registrelor deținute de MAI (registre de stat sau registre interne). Activitățile de luare la evidență, operare a modificărilor și radiere din registre sunt inițiate de sistemele informaționale de tip ”front end” prin accesarea interfețelor aplicative (API), ale aplicațiilor ce oferă capabilități de ținere a registrelor, specific implementate pentru fiecare registru. Aceste aplicații dețin mecanisme solide pentru controlul accesului la înregistrări și pentru asigurarea integrității și non-repudierii înregistrărilor. Asigură flexibilitate în ajustarea modelului de date, în cazul modificării legislației cu privire la registrele ținute. |
|  | Formarea băncilor de date statistice | Set de capabilități destinat să formeze băncile de date statistice pentru domeniile în responsabilitatea MAI. Băncile de date statistice conțin date depersonalizate produse în cadrul proceselor MAI sau recepționate din alte surse externe. Capabilitățile asigură definirea modelului statistic, a obiectelor de observație statistică, variabilelor statistice și indicatorilor statistici. Susține aplicarea standardului ISO 17369:2013 SDMX (Statistical Data and Metadata eXchange) și grupul de standarde SM ISO/IEC 11179:2018 Tehnologia informației - Registre de metadate (MDR). Datele statistice pot fi furnizate prin diferite metode: interfețe aplicative, fișiere de date structurate. Datele de intrare sunt validate și procesate conform regulilor stabilite. Informația statistică este furnizată în formă de rapoarte și seturi de indicatori statistici. |
|  | Analiza riscurilor | Set de capabilități destinate susținerii activităților de analiză la riscuri operaționale, tactice și strategice. Permit formarea băncii de date centralizate (warehouse) prin preluarea datelor din orice alt sistem informațional al MAI. Permite corelarea datelor din diferite surse, conform modelului de date definit. Pot fi integrate și surse de date externe. Seturile de date încărcate pot fi ajustate și îmbogățite, pentru a crește valoarea de analiză a lor. Permit formarea cuburilor de date din banca centrală de date (data marts), destinate să răspundă necesităților specifice de analiză a diferitor subdiviziuni și unități funcționale ale MAI. Deține instrumente utilizator pentru accesarea datelor și efectuarea analizelor necesare utilizatorilor. |
|  | Gestiune conținut web | Set de capabilități destinate producerii paginilor web ale MAI și subdiviziunilor MAI. Paginile web pot fi publice sau interne. Pot avea diferit conținut, inclusiv forme utilizator pentru interacțiunea cu vizitatorii paginilor web. |
|  | Geolocalizare | Set de capabilități destinate poziționării geospațiale a obiectelor și evenimentelor de interes pentru MAI. Permite încărcarea și utilizarea diferitor hărți cu destinație specifică, inclusiv a hărților oficiale furnizate de către autoritățile centrale și locale. Capabilitățile pot fi integrate prin interfețe aplicative în alte sisteme informaționale. Scenarii de utilizare: obținerea coordonatelor geospațiale prin indicarea de către utilizator a locației pe hartă; plasarea pe hartă a obiectelor și evenimentelor conform coordonatelor geospațiale ale acestora. |
|  | Gestiune facturi de plată (amenzi, servicii) | Set de capabilități destinate emiterii facturilor de plată pentru amenzile emise de MAI și pentru serviciile publice oferite de MAI cetățenilor. Permite definirea modelelor tipizate de facturi de plată pentru diferite scenarii de utilizare. Asigură urmărirea unei facturi de plată pe întreg ciclul de viață al acesteia. Furnizează informație în scopul reconcilierii facturilor achitate. |
|  | Gestiune resurse instituționale | Set de capabilități destinate gestiunii centralizate la nivel de MAI și locale la nivelul subdiviziunilor MAI, a tuturor tipurilor de resurse deținute (sedii, mijloace de transport, obiecte de inventar, consumabile, etc.). Asigură accesul la informația despre resursele deținute prin interfețe aplicative pentru alte sisteme informaționale. Gestionează resursele deținute pe întreg ciclul de viață al acestora. Asigură gestionarea angajamentelor reciproce aferente resurselor instituționale (furnizori de resurse și prestatori de servicii aferente resurselor). |
|  | Gestiune financiară și contabilă | Set de capabilități destinate gestiunii financiare și contabile centralizat la nivel de MAI și local la nivelul subdiviziunilor MAI. Susține procesele de planificare și execuție bugetară, inclusiv prin producerea de rapoarte interne și cele destinate în scop de raportare externă (către Ministerul Finanțelor și subdiviziunile subordonate). Susține ținerea evidenței contabile conform legislației și raportarea financiară și contabilă către autoritățile competente. |
|  | Interoperabilitate sisteme | Set de capabilități destinate asigurării interoperabilității centralizate, standardizate și controlate pentru sistemele informaționale ale MAI. Schimburile de date pot fi efectuate între SIA ale MAI sau între SIA ale MAI și sisteme externe. Implicit, asigură interoperabilitatea cu platforma guvernamentală de interoperabilitate, MConnect. Permite definirea și menținerea catalogului semantic pe domeniile în care sunt efectuate schimburi de date structurate în cadrul MAI și în afara MAI. |
| CAPABILITĂȚI GENERICE ASOCIATE SISTEMELOR INFORMAȚIONALE PARTAJATE INSTITUITE DE CĂTRE GUVERN ȘI SERVICIILOR EXTERNE  *Caracteristici funcționale ce pot fi accesate de mai prin intermediul serviciilor guvernamentale. complementează capabilitățile generice asociate platformelor mai.* | | |
|  | MPass | serviciu care asigură autentificarea și controlul accesului utilizatorilor în sistemele informaționale, în conformitate cu Hotărârea Guvernului nr.1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass). Serviciul oferă două mecanisme de autentificare: semnătura mobilă și certificatul electronic. Prin intermediul M-Pass, MAI obține acces la capabilități de autentificare sigură a utilizatorilor la accesarea sistemelor informaționale ale MAI. |
|  | MSign | Serviciu reutilizabil, furnizat la nivelul platformei tehnologice comune a Guvernului, care oferă un mecanism integrator, securizat şi flexibil, al diferitelor soluții de aplicare şi verificare a autenticității semnăturii electronice de către utilizatori (inclusiv în contextul utilizării sistemelor informaționale şi a serviciilor electronice), oferite de către furnizorii de semnătură electronică în conformitate cu legislația, reglementat de Hotărârea Guvernului nr.405/2014. Prin MSign, MAI obține acces la capabilități pentru semnarea documentelor cu semnătura electronică calificată (conferirea efectului juridic) și verificarea autenticității documentelor semnate. Aceste capabilități pot fi integrate în sistemele informaționale ale MAI unde integritatea, autenticitatea și non-repudierea informației este deosebit de importantă. |
|  | MNotify | Reprezintă o soluție informatică din categoria Guvern către Cetățean (G2C) și Guvern către Business (G2B) și are ca obiectiv principal asigurarea necesităților informatice și informaționale pentru realizarea procesului de notificare, reglementată de Hotărârea Guvernului nr.376/2020. Prin MNotify, MAI obține acces la capabilități de notificare a clienților în cazul producerii evenimentelor ce țin de competența MAI (ex. avertizări situații excepționale, prestare servicii solicitate, aplicare sancțiuni, etc.). |
|  | MLog | Constituie un serviciu centralizat, reutilizabil, găzduit pe platforma tehnologică guvernamentală comună (MCloud), care are scopul de a oferi un mecanism securizat şi flexibil de jurnalizare şi audit, asigurând evidența evenimentelor, fiind reglementat de Hotărârea Guvernului nr. 708/2014. Prin MLog, MAI obține acces la capabilități de înregistrare și stocare sigură a evenimentelor de securitate importante produse în sistemele sale. MLog va furniza înregistrările sale în cazul necesității investigării incidentelor sau soluționării disputelor. |
|  | MConnect | Este o soluție tehnică reglementată de Hotărârea Guvernului nr. 211/2019, destinată asigurării schimbului de date între sistemele informaționale deținute de participanții la schimbul de date, în conformitate cu Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate. MConnect furnizează pentru MAI capabilități de interoperabilitate a sistemelor sale informaționale cu sistemele informaționale ale altor autorități. Catalogul semantic guvernamental susținut prin MConnect constituie sursă de referință pentru modelul de date al MAI. |
|  | MPay | Serviciul respectiv reprezintă un sistem informațional care este utilizat în calitate de mecanism unic de încasare și de distribuire a plăților. Prin MPay, MAI obține acces la capabilități de încasare a plăților pentru amenzile aplicate și serviciile prestate cetățenilor și entităților juridice. Serviciul oferă o multitudine de opțiuni pentru alegerea instrumentelor de plată, iar MAI nu trebuie să se îngrijească de acest fapt, fiind intrinseci serviciului MPay. |
|  | Date.gov.md | Portalul guvernamental unic de date deschise (www. date.gov.md) reprezintă un punct unic de acces la datele guvernamentale cu caracter public, reglementat prin Hotărârea Guvernului nr. 701/2014. Prin date.gov.md, MAI obține acces la capabilități de publicare a seturilor de date de interes public pe domeniile de competență ale MAI. |
|  | MPower | Reprezintă un sistem informațional constituit dintr-un ansamblu de resurse și tehnologii informaționale, mijloace tehnice de program și metodologii, aflate în interconexiune, destinate consemnării împuternicirilor de reprezentare în baza semnăturii electronice, acordate de către persoane fizice sau persoane juridice altor persoane fizice sau persoane juridice, reglementat de Hotărârea Guvernului nr.375/2020. Prin utilizarea serviciului MPower MAI asigură confirmarea împuternicirilor acordate angajaților săi și asigură transparența acțiunilor acestora. |
|  | MLearn | Platforma Guvernamentală de Instruire la Distanță este un mecanism eficient și modern de instruire prin crearea, dezvoltarea, punerea la dispoziție, precum și acordarea accesului la resursele de instruire, care duc la un mod mai bun, mai practic si mai inteligent de aplicare a competențelor digitale pentru toate categoriile de utilizatori. |
|  | Alte servicii guvernamentale | Ale servicii guvernamentale accesibile MAI pot furniza capabilități ce pot fi integrate de MAI în cadrul sistemelor informaționale ale sale. Prin aceasta MAI optimizează investițiile în TIC, crește calitatea serviciilor TIC și se aliniază la strategia guvernamentală pe domeniul TIC. |
|  | Accesare informație din registre de stat | Setul de capabilități asigură accesul sistemelor informaționale ale MAI la informația din registrele de stat deținute de alte autorități publice. În acest mod, este îmbunătățită calitatea informației în SI ale MAI. De asemenea, este îmbunătățită interoperabilitatea cu alte autorități publice, toți participanții operând cu aceleași date (structură și conținut). |
|  | Accesul la servicii ale altor instituții (din RM și din afară) | Capabilitățile de acces la surse de informații externe sunt integrate în sistemele informaționale ale MAI pentru a îmbunătăți calitatea datelor procesate și utilitatea serviciilor TI pentru angajații MAI. Accesul la sursele de date externe este asigurat în baza acordurilor încheiate de MAI cu instituții din țară (ex. pentru verificare RCA) și din afara țării (ex. pentru acces la BD Interpol). |
| CAPABILITĂȚI SPECIALIZATE ASOCIATE APLICAȚIILOR MAI  *Caracteristici funcționale dezvoltate în scopul susținerii în mod particular a anumitor activități și procese ale mai. capabilitățile specializate sunt dezvoltate atunci când nu pot fi asigurate prin orchestrarea capabilităților generice. de asemenea, sunt asociate aplicațiilor deja implementate și ce vor continua să fie utilizate.* | | |
|  | Gestiunea semnalărilor | Set de capabilități destinat recepționării semnalărilor către poliție, pe toate canalele posibile, inclusiv: la sediu, telefon, poștă, email, web, viber, autosesizări, etc. Asigură gestiunea semnalărilor pe întreg ciclul de viață al acestora. Pasează rezultatul către alte sisteme informaționale în vederea continuării proceselor MAI potrivite, funcție de rezultatul procesării semnalării (ex. constatarea contravenției, infracțiunii, etc.). |
|  | Acces mobil la informație operativă | Set de capabilități destinat asigurării accesului cu utilizarea dispozitivelor mobile (aplicații, SMS) la informația operativă relevantă pentru contextul în care se află colaboratorul MAI și pentru funcția acestuia. |
|  | Gestiune informații dactiloscopice | Set de capabilități destinat colectării, procesării, stocării și accesării informației dactiloscopice. |
|  | Gestiune profile ADN | Set de capabilități destinate stocării, căutării și accesării pofilelor ADN și a datelor aferente din cadrul Registrului de stat al datelor genetice (Banca de date națională ADN) |
|  | Gestiune forțe și management operațional | Set de capabilități specializate de gestiune evenimente de ordine si securitate publica destinate subdiviziunilor de management operațional al MAI |
|  | Expertiza balistică | Set de capabilități destinate colectării, stocării și accesării informației privind rezultatele expertizei balistice a armelor de foc și a urmelor lăsate de acestea pe tub și glonț. |
|  | Monitorizare video | Set de capabilități destinate monitorizării video a traseelor naționale, a locațiilor și sediilor. Asigură depistarea automată e evenimentelor de interes pentru poliție și semnalarea acestora către poliție. |
|  | Gestiune servicii privind migrația și azilul | Set de capabilități specializate asociate serviciilor TI și sistemelor informaționale deținute de BMA. |
|  | Securitatea la frontieră | Set de capabilități specializate asociate serviciilor TI și sistemelor informaționale deținute de IGPF. |
|  | Alte capabilități specializate | Capabilități specializate asociate sistemelor informaționale și aplicațiilor utilizate de subdiviziunile MAI la moment. Alte capabilități ce vor fi dezvoltate în timp pentru a răspunde la necesități specifice ale activităților MAI, ce nu pot fi satisfăcute prin orchestrarea de capabilități generice. |

**Tabelul nr. 1: Capabilitățile TIC cheie ale SII MAI**

**23.** SII MAI este parte din arhitectura guvernamentală de scară largă. Este integrat și interoperabil cu sistemele informaționale ale altor autorități publice și terțe părți. De asemenea, deține componente ce sunt parte a Sistemului Informațional Integrat al Organelor de Drept, conform Hotărârii Guvernului nr. 1202/2006. Relația SII MAI în raport cu sistemele informaționale externe este următoarea:

1) SII al Organelor de drept. Conceptul SIIOD pornește de la premisa că fiecare organ de drept deține propriile sisteme informaționale automatizate. Acestea sunt gestionate individual de fiecare organ de drept. În același timp, sunt integrate și dirijate într-o manieră coordonată, pentru a susține informațional activitatea organelor de drept. MAI trebuie să asigure capabilitățile TIC necesare partajării informației respective în cadrul SIIOD. SII MAI este parte din SIIOD prin intermediul acestor capabilități TIC. Există alte capabilități TIC ale MAI, parte din SII MAI și care nu sunt parte din SIIOD (ex. dirijare operațională MAI);

2) sistemele informaționale ale altor autorități publice. Conform Legii nr. 142/2018, cu privire la schimbul de date și interoperabilitate, schimbul de date între MAI și alte autorități și instituții publice se va face prin intermediul platformei de interoperabilitate guvernamentală (MConnect). MAI poate avea schimburi de date în afara platformei MConnect, dacă legea specială stabilește acest fapt. Schimburi directe de date pot exista, în acest context, cu alte organe de drept;

3) sistemele informaționale ale altor terțe părți din RM. SII MAI poate face schimburi de date sistemele informaționale și ale altor terțe părți decât autorități și instituții publice, în baza acordurilor semnate cu acestea. În acest caz integrarea între sistemele TIC ale MAI și sistemele TIC ale terțelor părți se poate face direct sau prin intermediul platformei MConnect;

4) sistemele informaționale cu instituții corespondente din afara Republicii Moldova. MAI are semnate acorduri de schimburi de date cu autorități și instituții corespondente din afara țării. Natura informației ține de domenii specifice de activitate ale subdiviziunilor MAI. Schimbul de informații se face între sistemele TIC ale MAI și sistemele partenerilor MAI, prin integrare directă.

**Capitolul IV**

**STRUCTURA ARHITECTURII DE APLICAŢII A SII MAI**

**24.** Din perspectiva proceselor de activitate ale MAI, un Sistem Informațional Automatizat este reprezentat prin setul de servicii TIC ce servesc un scop comun relevant pentru activitățile și funcțiile MAI. În răspuns la necesitățile și nevoile specifice proceselor de activitate ale MAI, ca regulă sunt lansate inițiative de implementare a noilor SIA sau dezvoltarea unor SIA existente. Pentru a se alinia la Conceptul-cadru al SII MAI, toate SIA ce urmează a fi implementate, vor realiza arhitectura de referință prezentată în figura nr.2:



**Figura nr. 2. Arhitectura de referință pentru implementarea/dezvoltarea SIA în cadrul MAI**

**25.** Serviciile TIC din cadrul unui Sistem Informațional Automatizat în cadrul MAI trebuie să corespundă unui set de cerințe obligatorii, divizate în 4 niveluri:

1) Nivelul 1: implementează orchestrarea capabilităților şi serviciilor TIC existente în vederea realizării necesităților funcționale ale MAI atribuite la SIA. Serviciile TIC se conformează cu aceiași cerință de orientare pe servicii și corespunzător oferă servicii TIC automatizate (de nivel înalt). Acestea la rândul lor sunt conectate la magistrală și devin disponibile atât pentru consumatorii SIA externi, cât și pentru aplicațiile client oferite utilizatorilor finali ai SIA;

2) Nivelul 2: dezvoltă sau reutilizează capabilități TIC sub forma de servicii elementare. De notat că aceste capabilități sunt integrate în soluția de magistrală (ESB). Acest fapt facilitează re-utilizarea capabilităților atât de către serviciul TIC curent, cât și de către alte servicii TIC și consumatorii SIA externi;

3) Nivelul 3: dezvoltă componentele de aplicații cu reutilizează aplicațiile și serviciilor de platformă atât din MCloud cat și deținute de MAI. În lipsa unor aplicații de platformă (MCloud sau MAI) vor fi achiziționate și implementate aplicații noi (specializate sau de platformă);

4) Nivelul 4: are la baza o soluție 'Cloud First' ce poate rula în MCloud.

**26.** Arhitectura de aplicații MAI este concepută ca o arhitectură orientată pe servicii (SOA), pornește de la modelul business și utilizează tehnologia pentru a proiecta, dezvolta și furniza servicii TI bazate pe standarde deschise, îmbunătățind astfel reutilizarea componentelor TI furnizate și creând agilitate pentru a răspunde la provocări sau schimbări.

**27.** Arhitectura de aplicații MAI reprezintă un set de servicii și microservicii încorporate, destinate pentru a explora diverse tipuri de conținut digital, indiferent locul și metoda prin care a fost creat și stocat, prin numeroase cazuri de utilizare, de către diferite grupe de utilizatori MAI și externi, realizate printr-o suită de programe de platformă integrate, aplicații separate care partajează API-uri și depozite de date comune, și componente de servicii de conținut cooptate și reutilizate, conform figurii nr. 3.

**Figura nr. 3. Figura Arhitecturii de aplicații a MAI de scară largă**



**28.** Pentru a asigura crearea Serviciilor TI, arhitectura de aplicații MAI utilizează capabilitățile furnizate de componentele aplicative ale SII MAI, după cum urmează:

1) aplicații de platformă – reprezintă soluții aplicative integrate care sunt folosite ca bază pentru a dezvolta servicii TI și automatiza procesele de activitate ale MAI. Oferă seturi integrate de servicii legate de conținut, microservicii, depozite și instrumente care sprijină cazurile comune de utilizare a conținutului informațional gestionat de MAI. Permit integrarea depozitelor de date distribuite pentru a asigura gestiunea, accesul și guvernarea centralizată a informației, la nivel de MAI, pe întreg ciclu de viață a acesteia. Oferă instrumentar pentru dezvoltarea serviciilor TI fără necesitatea dezvoltării codului program;

2) aplicații specializate: aplicațiile oferă capabilități bazate pe soluții de afaceri. Sunt aplicații specifice activităților MAI (asigurării ordinii de drept) sau a cazurilor specifice de utilizare și oferă o soluție pentru o problemă distinctă (ex. soluția AFIS (evidența dactiloscopică), soluția FRS (Face Recognition System), IBM i2 Analyst's Notebook etc.);

3) sistemele informaționale partajate instituite de către Guvern și ale terților: sunt servicii TI bazate pe utilități care adaugă capabilități suplimentare aplicațiilor și platformelor existente. Includ servicii SII MAI reutilizate, sistemele informaționale partajate instituite de către Guvern (PaaS, SaaS) și alte servicii externe cooptate (ex. servici oferite de Google).

**29.** Pentru a asigura crearea Serviciilor TI, arhitectura de aplicații MAI utilizează capabilitățile furnizate de sistemele externe:

1) SI surse de date oficiale utilizate în cadrul activităților MAI, iar principalele surse de date oficiale sunt sistemele și resursele informaționale de stat, în special Registrul de stat al populației și Registrul de stat al unităților de drept, care reprezintă resursele informaționale de bază de date veridice oficiale cu privire la obiectele informaționale luate la evidență. La fel sunt considerate în calitate de surse de date administrative orice alte sisteme deținute de persoane de drept privat și organizații internaționale al căror grad de veridicitate este cunoscut. În acest scop MAI urmează să dispune de acorduri de schimb date dacă veridicitatea sursei nu este stabilită printr-un act legislativ;

2) SI ale partenerelor de proces sunt sistemele informaționale care susțin procese de activitate comună ale MAI și partenerului de proces. În scopul asigurării interoperabilității semantice MAI urmează a conveni cu partenerii de proces asupra interoperabilității semantice. Accesul la date cu caracter personal din cadrul sistemelor partenere are la bază temeiul procesului comun.

**30.** În vederea realizării prevederilor prezentului Concept-cadru, MAI va aproba şi va întreține Catalogul componentelor arhitecturii de aplicații a SII MAI, care va conține informații despre:

1) denumirea completă a componentei de arhitectură (SIA gestionat de MAI, serviciu de platformă, aplicația specializată sau alte componente aplicative);

2) rolul componentei la nivelul arhitecturii de aplicații de scara largă;

3) funcționalități-cheie preconizate să fie asigurate de componenta de arhitectură;

4) interoperabilitatea cu alte componente ale arhitecturii de aplicații sau externe;

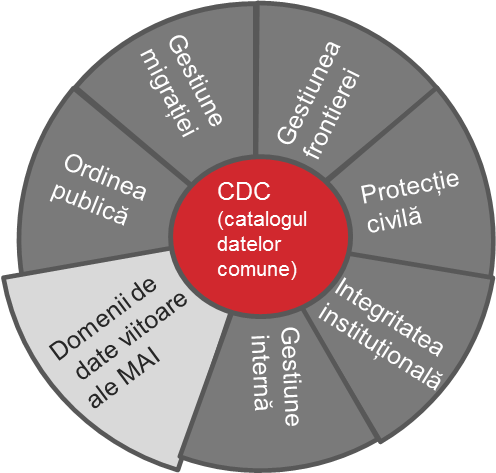
5) autoritățile administrative și instituțiile din subordinea MAI care vor beneficia de soluția implementată pentru componenta de arhitectură.

**Capitolul V**

**ARHITECTURA DATELOR SII MAI**

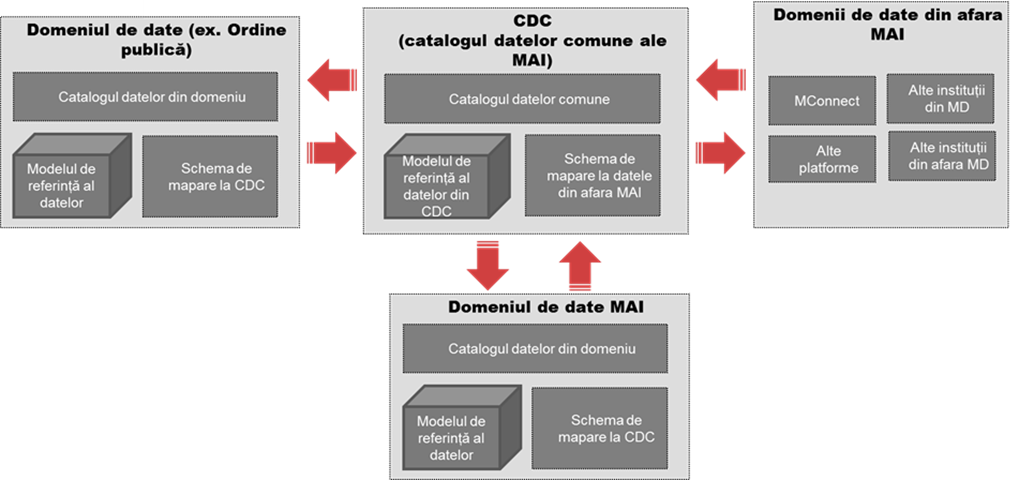
**31.** Arhitectura de date de referință are obiectivul de a servi drept reper pentru a fi stabilit cadrul instituțional pentru managementul arhitecturii de date.

**32.** Conceptul modelului de date al SII MAI este prezentat în figura nr. 4 şi nr. 5.



**Figura nr. 4. Arhitectura modelului de date al SII MAI**

**Figura nr. 5. Arhitectura modelului de date al SII MAI**



**33.** Toate datele utilizate în activitatea MAI sunt atribuite la un set de domenii convenționale. Datele pot fi gestionate relativ simplu la nivelul unui domeniu. Însă, în cadrul activităților MAI, datele circulă între domenii. Înțelegerea univocă a acestor date este asigurată prin definirea unui domeniu comun al datelor MAI. Convențional, acesta este numit Catalogul Datelor Comune ale MAI (*în continuare – CDC*) și conține date care fac parte din două sau mai multe domenii specifice.

**34.** Fiecare domeniu, atât specific, cât și CDC, conține trei elemente de bază, precum este indicat în figura nr. 5, după cum urmează:

1) catalogul datelor din domeniu – conține informație despre tipurile de date din domeniu. Acestea pot fi grupate. Pentru fiecare tip de date este stabilită semnificația semantică, atribute, domeniul de valori admisibile pentru atribute (pot fi alte tipuri de date);

2) modelul de referință al datelor – conține informație despre relațiile între tipurile de date din domeniu. Conform modelului NIEM, aceste relații pot fi simplificate la două tipuri: „ESTE UN”; „ARE UN”;

3) schema de mapare al datelor – pentru domeniile specifice, este stabilită schema de mapare a datelor din domeniul specific, la datele din CDC. Acest fapt este necesar în scopul implementării interoperabilității semantice între domeniile specifice. Schema de mapare a adatelor pentru CDC stabilește corespondența datelor din CDC cu alte domenii din afara MAI (ex.: Catalogul semantic necesar interoperabilității semantice din cadrul platformei MConnect).

**35.** În vederea realizării prevederilor prezentului Concept-cadru, MAI va aproba şi va întreține Catalogul datelor utilizate în activitatea MAI, cu indicarea categoriei, subcategoriei datelor şi a descrierii detaliate a acestora.

În scopul asigurării interoperabilității și a schimbului de date cu alte sisteme și resurse informaționale de stat, Ministerul Afacerilor Interne va înregistra activele semantice din cadrul Catalogului datelor utilizate în Sistemul informațional „Catalogul semantic”.

**36.** În scopul sistematizării informației MAI utilizează registre. În raport cu scopul și modul ținerii, registrele MAI pot fi:

1) Registre de stat – sunt instituite și ținute în scopul formării resurselor informaționale documentate de stat. Instituirea și ținerea acestora este reglementată prin Legea nr. 71/2007. Registrele de stat reprezintă sursa unică centralizate de date despre obiectul evidenței. Înregistrările acestora nu pot fi utilizate în alte scopuri decât cele definite de actul normativ ce reglementează ținerea registrului. Registrele de stat pot fi ținute doar în formă electronică. MAI este deținător de registre de stat departamentale;

2) Sub-registre – reprezintă subseturi de date aferente unui registru de stat departamental MAI ce sunt gestionate sau/și ținute într-un mod distinct. Sub-registrele sunt părți componente logic integrate ale registrului din care fac parte;

3) Registre operaționale – sunt utilizate pentru sistematizarea informației operaționale gestionate în cadrul proceselor activitate. Registrele operaționale nu se atribuie la registrele de stat. Ciclul de viață a înregistrărilor acestora este similar datelor operaționale, este determinat de procesul ce le-a creat și nu depășește durata de viață a acestuia. Registrele operaționale pot include seturi de date extrase din registrele de stat în scopul procesării operaționale sau date ce urmează a fi înscrise în registrele de stat. În ambele cazuri acestea sunt tratate în calitate de date operaționale ale procesului care le gestionează.

**37.** În scopul alinierii la cerințele legislației în vigoare cu privire la ținerea registrelor de stat, fiecare registru de stat deținut de MAI urmează a fi instituit printr-un act normativ și ținut în conformitate cu Regulamentul cu privire la ținerea registrului aprobat prin hotărârea Guvernului. Regulamentul resursei informaționale/a registrului de stat cuprinde reglementări privind drepturile și obligațiile subiecților raporturilor juridice aferente creării și ținerii resursei informaționale; modalitatea de ținere a resursei informaționale; procedura de înregistrare, modificare, completare și radiere a datelor; procedura de interacțiune cu furnizorii de date; măsuri privind asigurarea securității resursei informaționale.

**38.** În scopul ținerii registrelor de stat MAI utilizează capabilitățile componentelor arhitecturii de aplicații. Sistemul informațional automatizat poate fi creat dedicat în scopul ținerii registrului sau poate include ținerea acestuia prin automatizarea activităților aferente ținerii registrului.

Conceptele sistemelor informaționale destinate ținerii resurselor informaționale ale MAI se aprobă prin acte normative al Guvernului. Conceptul sistemului informațional definește spațiul funcțional, structura organizatorică, spațiul informațional, spațiul tehnologic, securitatea sistemului informațional și protecția informației.

**39.** SII MAI este format din următoarele sisteme/resurse informaționale, care au fost deja instituite de către Guvern şi se află în posesia MAI și a structurilor organizaționale din sfera de competență a MAI:

1) Sistemul informațional automatizat „Registrul Informației Criminalistice si Criminologice”;

2) Sistemul informațional automatizat de evidență a contravențiilor, a cauzelor contravenționale și a persoanelor care au săvârșit contravenții;

3) Sistemul informațional automatizat „Registrul de stat al armelor” ;

4) Registrul Accidentelor Rutiere;

5) Sistemul informațional integrat al Poliției de Frontieră;

6) Sistemul informațional „Migrație” (Subsistemul Biroului Migratie si Azil) ;

7) Sistemul informațional automatizat „Registrul de stat dactiloscopic” ;

8) Sistemul informațional automatizat ,,Registrul Rezervelor Materiale ale Statului”;

9) Sistemul informațional automatizat „Registrul rezervelor de stat și de mobilizare” ;

10) Sistemul informațional automatizat „e-Cazier”;

11) Sistemul informațional de supraveghere video portabil „Camera de corp”;

12) Sistemul informațional de Localizare Automatizată al Parcului Auto al MAI;

13) Sistemul automatizat de supraveghere a circulației rutiere „Controlul traficului”;

14) Sistemul informațional unic de circulație a documentelor electronice pentru necesitățile MAI;

15) Sistemul informațional „Recrutarea și evaluarea resurselor umane în sistemul afacerilor interne;

16) Sistemul informațional Colaborator;

17) Sistemul informațional Protecția Copiilor (CCCI, INI, IGP);

18) Sistemul informațional „Evidența semnalărilor și evenimentelor de ordine publică”;

19) Sistemul informațional e-Dosar Contravențional;

20) Sistemul informațional e-Dosar Penal;

21) Sistemul informațional „Registrul de stat al datelor genetice”.

**40.** Ministerul Afacerilor Interne asigură înregistrarea resurselor și sistemelor informaționale din posesia sa sau a structurilor organizaționale din sfera de competență în cadrul Registrului resurselor și sistemelor informaționale.

**Capitolul VI**

**ARHITECTURA TEHNOLOGICĂ A SII MAI**

**41.** Arhitectura tehnologică a SII MAI determină realizarea soluțiilor tehnice de infrastructură și program necesare pentru funcționarea componentelor arhitecturii de aplicații, astfel încât să fie îndeplinite obiectivele și respectate regulile care le guvernează.

**42.** Arhitectura tehnologică a SII MAI este capabilă de a face față unor exigențe sporite față de performanță și securitate, în special în condițiile unor situații de criză. În acest sens, aceasta urmează a fi proiectată aliniat la principiile și cadrul de arhitectură guvernamentală de scară largă, după cum urmează:

|  |  |  |
| --- | --- | --- |
| **Nr.** | **Denumirea măsurii** | **Specificații** |
| 1. | Arhitectura tehnologică proiectată aliniat la principiile și cadrul de arhitectură guvernamentală de scară largă | * Consolidarea centrelor de date utilizate de MAI:   - un număr mai mic de Data centre cu o dotare mai bună;  - o deservire mai bună prin concentrarea eforturilor și resurselor necesare deservirii data centrelor;  - o securitate mai înaltă prin micșorarea numărului de locații critice la care trebuie limitat accesul;  - toate centrele de date MAI urmează să se conformeze la cerințele TIER 4.   * Infrastructură bazată pe resursele guvernamentale. MAI aliniat pentru a dezvolta componentele de infrastructură în cazul unor exigențe avansate:   - WAN MAI construit ca parte a rețelei transport date guvernamentale. Segmentele de rețea MAI transmise pentru formarea rețelei guvernamentale;  - Rețeaua data-voce TETRA construită și partajată cu alte organe de drept. Rețeaua TETRA este concepută ca rețea back-up pentru MAI și organele de drept;  - MCloud utilizat de câte ori este posibil pentru asigurarea capacităților de procesare necesare MAI. |
| 2. | Arhitectură redundantă la nivel de centre de date *(rezervare la nivel de centru de date)* | * Centre de date redundante și implementate:   - centrele de date dispersate geografic;  - centrele de date operează independent unul față de celălalt;  - centrele de date interconectate prin canale DCI (*data center interconnect*) de mare capacitate;  - centrele de date construite conform standardelor aplicabile din domeniu; |
| 3. | Arhitectură active-standby | * Arhitectură dual-site de tip active-standby   - centrul de date principal operează: (i) conexiunile de date/rețea externe de bază; (ii) instanțele active ale serviciilor de bază de date/aplicații;  - centrul de date secundar operează: (i) conexiunile de date/rețea externe de rezervă;(ii) instanțele standby ale serviciilor bază de date/aplicații.   * Afinitate între instanțele active ale serviciilor bază de date, aplicații și de rețea, prin care se va asigura:   a) disponibilitate independentă de disponibilitatea simultană a ambelor centre de date;  b) performanță îmbunătățită prin localizarea traficului de date la nivelul unui singur centru de date (*intr-site*) fără tranziții multiple prin circuitul de interconnect între centrele de date. |
| 4. | Redundanță N+1 pentru centrul de date principal și 1N pentru centrul de date secundar | * Rezervare de nivel N+1 pentru serviciile aferente centrului de date principal:   a) servicii de infrastructură centru de date;  b) servicii de rețea - implementare perechi de switch-uri in nucleul rețelei, perechi de dispozitive firewall (failover cluster) în modulul comunicațiilor externe a rețelei;  c) funcții HA la nivelul platformei de virtualizare servere; d) failover cluster for non-virtualized workload, application/DB layer;   * Rezervare de nivel 1N (no redundancy) pentru serviciile aferente centrului de date secundar; |
| 5. | Capabilități și capacități centru de date secundar comparabile cu cele ale centrului de date principal (doar că fără redundanță) | * Capabilitățile centrului de date secundar pe dimensiunea serviciilor de rețea, computing și storage SAN sunt comparabile cu cele ale centrului de date principal. În caz de pierdere a centrului de date principal, situații de incident sau downtime planificat , centrul de date secundar asigură funcționarea serviciilor de aplicații și conectivitate către acestea in limitele de performanță și disponibilitate stabilite; * La nivelul centrului de date secundar sunt realizate următoarele conexiuni de date externe de rezervă: (i) conexiuni cu terțe părți (S2S VPN); (ii) conexiunea la rețeaua WAN MAI; (iii) conexiunea la rețeaua S/RTAAP; (iv) conexiuni de la distanță prin VPN pentru angajați (remote access VPN). |
| 6. | DCI de mare capacitate, tip L3 | * Legătură de date intre centrele de date principal și secundar; * De capacitate înaltă (n x 1Gbps, 10Gbps); * Realizat printr-un circuite de fibră optică (*dark fiber*) proprie sau închiriată; * Nu sunt folosite VLAN-uri extinse (L2 extention/stretched VLANs) intre centrele de date principal și secundar (*segregated failure domain/improved stability; optimized network*); * Trafic inter-data center protejat criptografic (L3/IPSEC sau L2/MACSEC). |
| 7. | Replicare între centre de date organizată la nivel de aplicații/bază de date | * Între centrele de date principal și cel secundar sunt organizate sesiuni automate de replicare; * La nivel de servicii bază de date (Database Mirroring (SQL Server)/Oracle redo log replication); * La nivel de servicii de aplicații (de ex.: Active Directory multi-master replication); |
| 8. | Arhitectură aplicații pe mai multe nivele | * Se evită utilizarea aplicațiilor in două nivele (client-to-bază da date); * Sunt utilizate aplicații pe mai multe nivele, tradițional: client/dmz (WFE)/front-end (APP)/back-end (DB). |
| 9. | Utilizare tehnologii virtualizare servere | * Sunt folosite tehnologii de virtualizare servere pentru majoritatea aplicațiilor interne. Nu sunt virtualizate soluțiile livrate la pachet (DACTO, AFIS, Video .. etc) și acele servere pentru care nu este fezabilă migrarea pe mediul de virtualizare (servere cu sarcină mare sau/și dificultăți legate de licențele software, de ex. produse Oracle aferent SIA RICC); *Candidați pentru P2V: Vitrina RICC, INTERDICTII.* |
| 10. | Conexiuni la rețele publice sau private (dar străine) protejate prin funcții firewall | * Comunicațiile prin rețele externe - rețele publice/Internet sau private (conexiuni cu terțe părți) - sunt restricționate prin funcții firewall. Nu sunt admise conexiuni externe realizate direct in nucleul rețelei. Toate conexiunile externe sunt separate prin firewall de nucleul rețelei. Sunt implementate servicii de securitate complementare, cum ar fi IDS/IPS, AMP s.a. * Se evită implementarea politicilor de acces la nivel de rețea exclusiv prin liste de access stateless. Listele de acces stateless sunt insuficiente, ineficiente și greu de gestionat. |
| 11. | Servicii expuse către terțe părți sau accesului public accesate printr-un segment de DMZ a rețele | * Arhitectura rețelei presupune un segment de rețea dedicat DMZ pentru prezentarea serviciilor de aplicații interne către terțe părți, accesului prin conexiuni VPN de la distanță sau a accesului din rețele publice. Sunt stabilite politici de acces restrictive, prin firewall, către/dinspre segmentul de DMZ a rețelei. * Accesul la aplicații prin DMZ are loc fie prin servicii Web Front End ale aplicațiilor (dacă aplicația este construită după o arhitectură pe mai multe nivele) fie prin servicii reverse-proxy. |
| 12. | Tehnologii și configurații VPN securizate | * Conexiunile VPN de la distanță sunt organizate printr-un singur echipament de rețea (VPN gateway), folosesc aceeași tehnologie și sunt realizate după un singur standard de configurație; * Conexiunile VPN de la distanță sunt rezervate prin echipamentul de rețea din centrul de date de rezervă, fie prin liste de servere backup (failover automat) fie prin definiții de conexiuni distincte (failover manual); * Credențialele utilizatori și politicile de autorizare pentru conexiunile VPN de la distanță sunt gestionate și păstrate centralizat in baza unui serviciu AAA centralizat (server RADIUS); * Sunt utilizate tehnologii și configurații sigure pentru realizarea sesiunilor de acces prin VPN de la distanță (de ex. acces de la distanță prin SSL VPN sau IPSEC/IKEv2 cu Cisco AnyConnect). Accesul prin conexiunile VPN de la distanță este controlat prin liste de acces restrictive (tunnel filters/local sau DACL). Autentificare in baza certificatelor digitale (rsa-sig) pentru VPN gateway. Sunt utilizați algoritmi criptografici considerați siguri (preferabil NGE/suite-B); |
| 13. | Failover automat atunci când e posibil | * În caz de indisponibilitate a serviciilor în centrul de date principal, tranzițiile pe instanțele de rezervă in centrul de date secundar are loc automat, transparent pentru utilizator. Excepție fac sistemele ce nu susțin tehnologii de failover automat (de ex. tranziția pe instanța de rezervă SIA RICC). * La nivel de rețea sunt implementate conexiuni VPN/S2S și RA-VPN de rezervă (AnyConnect DPD/backup servers). Failover automat susținut prin utilizarea protocoalelor dinamice de rutare. |
| 14. | Copii de backup păstrate offsite *(cross site backup storage)* | * Copiile de backup sunt păstrate într-un alt centru de date decât cel la nivelul căruia au fost realizate. |
| 15. | Echipament & soft de generații și versiuni susținute de furnizori, contracte active de suport pentru acestea | * Toate produsele software (inclusiv medii de operare) și hardware (rețea, servere, sisteme storage SAN) sunt susținute de furnizori (inclusiv prin fereastra de suport activ); * Sunt stabilite contracte de suport și licențe active pentru produsele hardware și software utilizate. |
| 16. | Continous security, performance and availability monitoring | * Este stabilit un proces de monitorizare a nivelului de performanță și disponibilitate pentru serviciile de infrastructură centru de date, rețea, aplicații și bază de date. |
| 17. | Transparență prin documentare | * Platforma tehnologică este documentată corespunzător. Sunt documentate aspecte ce țin de arhitectura rețelei, servere de aplicații și baze de date, conexiunile de date externe, interoperabilitate. Este menținut un inventar al activelor informatice. |