

GVERNUL REPUBLICII MOLDOVA

HOTĂRÎRE nr. _____

din _____ 2022

**”Cu privire la aprobarea Conceptului Sistemului Informațional
„Programul de vânzare directă a valorilor mobiliare de stat persoanelor
fizice în Republica Moldova” și modificarea unei Hotărâri de Guvern”**

În vederea executării art.22 lit.d) din Legea nr.467/2003 ”Cu privire la informatizare și la resursele informaționale de stat” și dezvoltării pieței valorilor mobiliare de stat, sporirii educației financiare și facilitării accesului persoanelor fizice la procurarea valorilor mobiliare de stat, Guvernul

HOTĂRĂȘTE:

1. Se aprobă Conceptul Sistemului Informațional „Programul de vânzare directă a valorilor mobiliare de stat persoanelor fizice în Republica Moldova” (se anexează).

2. Conceptul Programului de vânzare directă a valorilor mobiliare de stat persoanelor fizice în Republica Moldova, aprobat prin Hotărârea Guvernului Republicii Moldova nr.192/2021 (Monitorul Oficial al Republicii Moldova, 2021, nr.249-253, art.483), se modifică după cum urmează:

- 1) la punctul 1 textul ” , fără licitații și fără aplicarea procedurii de subscriere” se substituie cu textul ”prin subscriere”;
- 2) la punctului 3, subpunctul 1) textul ” și deținător” se exclude;
- 3) la punctului 3, subpunctul 2) textul ”implementator tehnic” se substituie cu textul ”deținător”.

Prim-ministru

Natalia GAVRILIȚA

Contrasemnează:

Ministru al Finanțelor

Dumitru BUDIANSCHI

Conceptul Sistemului Informațional „Programul de vânzare directă a valorilor mobiliare de stat persoanelor fizice în Republica Moldova”

Introducere

În Republica Moldova programul „Managementul datoriei de stat pe termen mediu (2020-2022), aprobat prin Hotărârea Guvernului nr.56/2020 include obiective specifice privind gestionarea datoriei de stat în perioada 2020-2022, unul dintre care este și dezvoltarea pieței interne a valorilor mobiliare de stat (VMS). În scopul realizării obiectivului propus, a fost elaborat Programul de vânzare directă a valorilor mobiliare de stat persoanelor fizice în Republica Moldova (în continuare – Program), aprobat prin HG nr. 192/2021. Programul menționat urmărește facilitarea accesului cetățenilor Republicii Moldova la cumpărarea VMS, dar și înstrăinarea acestora până la scadență, prin intermediul unei platforme electronice.

Prezentul Concept, elaborat în conformitate cu prevederile Legii nr. 467/2003, descrie platforma electronică pentru vânzarea VMS, concepută ca un canal specific care explorează potențialul efectuării operațiunilor cu VMS prin intermediul unei pagini web, fără intermediari.

Conceptul utilizează noțiunile definite de Legea nr.419/2006 cu privire la datoria sectorului public, garanțiile de stat, recreditarea de stat și Regulamentul cu privire la plasarea, tranzacționarea și răscumpărarea valorilor mobiliare de stat în formă de înscriere în cont, aprobat prin Hotărârea Comitetului executiv al Băncii Naționale a Moldovei nr.170/2018 și Ordinul Ministerului Finanțelor nr.129/2018.

Capitolul I. Dispoziții generale

1.1 Definiția Sistemului Informațional

Sistemul Informațional al „Programului de vânzare directă a valorilor mobiliare de stat persoanelor fizice în Republica Moldova” reprezintă o platformă online (Platforma electronică pentru vânzarea VMS) destinată investitorilor retail în Republica Moldova.

Platforma electronică pentru vânzarea VMS va asigura achiziția directă a VMS de către investitorii retail și vânzarea acestora până la scadență de către investitorii retail către dealerii primari sau către Ministerul Finanțelor (în continuare – MF).

Platforma electronică pentru vânzarea VMS va fi proprietatea Republicii Moldova și va fi operată și gestionată de I.P. „Centrul de Tehnologii Informaționale în Finanțe” în comun cu MF. Aceasta se va baza pe serviciile oferite de Depozitarul Central Unic al Valorilor Mobiliare (în continuare – DCU) al cărui model de activitate este bazat pe standardele și practicile internaționale.

1.2 Noțiuni de bază și abrevieri

În sensul prezentului Concept, noțiunile și abrevierile utilizate semnifică următoarele:

AD – Active Directory;

BD – Baze de date;

DCU – Depozitarul Central Unic al Valorilor Mobiliare;

IF - Instituții Financiare;

OS – Obligațiuni de stat;

MF – Ministerul Finanțelor;

RM – Republica Moldova;

SFS – Serviciul Fiscal de Stat;

SI – Sistemul Informațional;

SIA – Sistemul Informațional Automatizat;

VMS – Valorile mobiliare de stat;

TIC – Tehnologia informatică și de comunicație.

Totalitatea noțiunilor utilizate în prezentul document sunt delimitate și explicate în tabelul de mai jos:

Active Directory - este o implementare a serviciilor de directoare LDAP, folosită de Microsoft în cadrul sistemelor de operare Windows. Astfel, Active Directory pune la dispoziția administratorilor un mediu flexibil cu efect global pentru asigurarea permisiunilor, instalarea programelor, înnoirea securității; toate aceste operațiuni pot fi aplicate atât în rețele mici, cât și la rețele complexe.

Bază de date - ansamblu de date organizate conform structurii conceptuale care descrie caracteristicile de bază și relația dintre entități.

Dealeri primari - băncile care au fost acceptate de MF, în baza unui Acord, să deruleze operațiuni cu VMS pe piața VMS.

Depozitarul Central Unic - instituție care efectuează înregistrarea, evidența și decontarea valorilor mobiliare corporative, valorile mobiliare de stat și instrumentelor Băncii Naționale a Moldovei.

Investitori retail - cetățean al RM cu vârsta minimă de 18 ani împliniți la momentul procurării VMS, având un cont de plăți valid deschis la unul din prestatorii locali de servicii de plăți și dispunând de semnătură electronică avansată calificată.

Jurnalizare - funcție de înregistrare a informației despre evenimente. În cadrul sistemelor informatice, înregistrările despre evenimente includ detalii despre data și ora, utilizatorul, acțiunea întreprinsă.

MCloud - reprezintă platforma tehnologică guvernamentală comună bazată pe conceptul „Cloud Computing”.

MConnect - reprezintă platforma tehnologică guvernamentală de interoperabilitate care facilitează schimbul de date dintre autorități pentru creșterea eficienței și calității de prestare a serviciilor.

MNotify - serviciul electronic guvernamental de expedierea notificărilor despre diferite evenimente produse în sistem.

MPass - serviciul guvernamental de autentificare și autorizare, care oferă acces securizat la serviciile electronice.

MPay - serviciul guvernamental de plăți electronice, un instrument informațional cu ajutorul căruia pot fi achitate diverse servicii online.

MLog - serviciul electronic guvernamental de jurnalizare, serviciu centralizat, reutilizabil, găzduit pe platforma tehnologică guvernamentală comună (MCloud), care are scopul de a oferi un mecanism securizat și flexibil de jurnalizare și audit, asigurând evidența evenimentelor, în contextul utilizării Sistemelor Informaționale.

MSign - serviciul guvernamental de semnare electronică, care oferă posibilitatea utilizării tuturor tipurilor de semnătură electronică și verificării semnăturilor în condiții de securitate garantată.

Sistem Informațional - sistem de prelucrare a informației, împreună cu resursele organizaționale asociate, cum ar fi resursele umane și tehnice, care furnizează și distribuie informația.

1.3 Locul SI în spațiul informațional al Republicii Moldova

Platforma electronică pentru vânzarea VMS este parte componentă a resurselor informaționale de stat și cuprinde interacțiunea cu totalitatea resurselor informaționale, proprietarii cărora, în virtutea activității sale, sunt obligați să interacționeze cu colecția de date a sistemului financiar național.

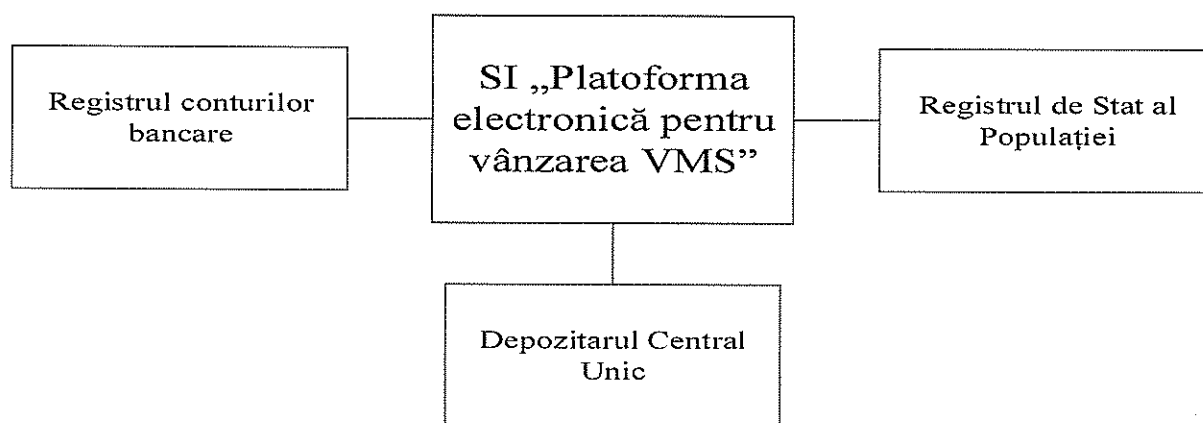


Figura 1 Locul SI „Platforma electronică pentru vânzarea VMS” în spațiul informațional al RM

SI „Platforma electronică pentru vânzarea VMS” va interacționa cu următoarele resurse informaționale:

- a) Registrul de Stat al Populației – în vederea completării și actualizării datelor aferente investitorilor retail (persoane fizice).
- b) Depozitarul Central Unic – în vederea înregistrării, evidenței și decontării VMS.
- c) Registrul conturilor bancare – în vederea recepționării informației aferente conturilor bancare ale investitorilor retail.

1.4 Scopul SI

Scopul SI constă în crearea accesului direct al investitorilor retail la cumpărarea VMS, utilizând platforma electronică.

1.5 Obiectivele de bază a SI

Obiectivele SI sunt îndreptate spre:

- a) Extinderea cercului de investitori retail și crearea condițiilor favorabile de participare directă a investitorilor retail pe piața internă a VMS;
- b) Diversificarea canalelor de vânzare a VMS;
- c) Dezvoltarea pieței secundare a VMS;
- d) Creșterea transparenței tranzacțiilor cu VMS;
- e) Creșterea nivelului de educație financiară a persoanelor fizice în instrumentele financiare oferite de către stat.

1.6 Sarcinile de bază realizate de SI

Implementarea SI va permite optimizarea și automatizarea activităților actorilor care interacționează cu componentele sistemului inclusiv, va genera o listă de beneficii așteptate ca urmare a implementării și dezvoltării soluției informatice:

- a) implementarea mecanismelor eficiente de schimb electronic de date dintre MF și terțe părți;
- b) reducerea cheltuielilor de procesare a datelor și monitorizare a proceselor;
- c) reducerea costurilor legate de prelucrarea informației pe suport material tradițional (hârtie) prin trecerea la procesarea informației exclusiv în format digital.

1.7 Principiile de bază ale SI

La proiectarea, realizarea și implementarea SI trebuie să se țină cont de următoarele principii generale:

- a) Principiul legalității: care presupune crearea și exploatarea SI în conformitate cu legislația națională în vigoare și a normelor și standardelor internaționale recunoscute în domeniu;
- b) Principiul consecutivității: care presupune dezvoltarea și implementarea etapizată a componentelor SI;
- c) Principiul respectării drepturilor omului: care prevede exploatarea SI în strictă conformitate cu documentele normative naționale, cu tratatele și convențiile internaționale privind drepturile omului la care RM este parte;
- d) Principiul independenței de platformă - interfață utilizator a SI nu va impune o anumită platformă software și hardware pentru calculatorul client al utilizatorului;
- e) Principiul datelor sigure: stipulează introducerea datelor în sistem doar prin canalele autorizate și autentificate;

- f) Principiul securității informaționale: presupune asigurarea unui nivel adecvat de integritate, selectivitate, accesibilitate și eficiență pentru protecția datelor de pierderi, alterări, deteriorări și de acces nesancționat;
- g) Principiul transparenței: presupune proiectarea și realizarea conform principiului modular, cu utilizarea standardelor transparente în domeniul tehnologiilor informatice și de telecomunicații;
- h) Principiul expansibilității: stipulează posibilitatea extinderii și completării SI cu noi componente, îmbunătățirea celor existente sau integrarea cu alte sisteme informatice externe;
- i) Principiul scalabilității: presupune asigurarea unei performanțe constante a soluției informatice la creșterea volumului de date și a solicitării SI;
- j) Principiul simplității și comodității utilizării: presupune proiectarea și realizarea tuturor aplicațiilor, mijloacelor tehnice și de program accesibile utilizatorilor SI, bazate pe principii exclusiv vizuale, ergonomice și logice de concepție.
- k) Principiul orientării WEB: presupune că interfața utilizator va fi concepută doar în baza tehnologiilor WEB prin intermediul celor mai populare exploratoare WEB (Microsoft Internet Explorer, Mozilla FireFox, Google Chrome, Opera și Safari);
- l) Principiul ajutorului interactiv: presupune înzestrarea interfeței de utilizator cu un modul de ajutor contextual on-line (versiunea în limba română – obligatorie), la nivelul fiecărei interfețe WEB de utilizare;
- m) Principiul mobilității: presupune dispunerea de mecanisme de asigurare a ergonomiei în funcție de dispozitivul de conectare (PC, Notebook, tabletă, smartphone, alte dispozitive mobile).

1.8 Baza normativă a SI

Crearea și funcționarea SI este reglementată de următoarele acte normative și documente de politici:

1. Legea Nr. 91 /2004 privind semnătura electronică și documentul electronic, Monitorul Oficial Nr. 174-177 din 04.07.2014;
2. Legea Nr. 71 /2007 cu privire la registre, Monitorul Oficial Nr. 70-73 din 25.11.2007;
3. Legea Nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat, Monitorul Oficial nr. 6-12/44 din 01/01/2004;
4. Legea Nr. 982/ 2000 privind accesul la informație, Monitorul Oficial Nr. 88 art. Nr. 664 din 28.07.2000;

5. Legea Nr. 133 /2011 privind protecția datelor cu caracter personal, Monitorul Oficial Nr. 171-175 din 14.10.2011;;
6. Legea Nr. 1069/2000 cu privire la informatică, Monitorul Oficial Nr. 073 din 05.07.2001;
7. Legea Nr.142 /2018 cu privire la schimbul de date și interoperabilitate, Monitorul Oficial Nr. 295-308 din 10.08.2018;
8. Legea finanțelor publice și responsabilității bugetar-fiscale nr.181/2014, Monitorul Oficial Nr. 223-230 din 08.08.2014;
9. 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, Monitorul Oficial Nr. 254-256 din 24.12.2010;
10. Hotărârea Guvernului Nr. 945/2005 cu privire la centrele de certificare a cheilor publice, Monitorul Oficial Nr. 123-125 din 16.09.2005;
11. Hotărârea Guvernului Nr. 1032 /2006 cu privire la aprobarea Concepției sistemului informațional automatizat "Registrul resurselor și sistemelor informaționale de stat", Monitorul Oficial Nr. 150-152 din 22.09.2006;
12. Hotărârea Guvernului Nr.710 /2011 cu privire la aprobarea Programului strategic de modernizare tehnologică a guvernării (e-Transformare), Monitorul Oficial Nr. 156-159 din 23.09.2011;
13. Hotărârea Guvernului Nr. 128/2014 privind platforma tehnologică guvernamentală comună (MCloud), Monitorul Oficial Nr. 47-48 din 25.02.2014;
14. Hotărârea Guvernului Nr.1090 /2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass), Monitorul Oficial Nr. 4-8 din 10.01.2014;
15. Hotărârea Guvernului Nr.405 /2014 privind serviciul electronic guvernamental integrat de semnătură electronică (MSign), Monitorul Oficial Nr. 147-151 din 06.06.2014;
16. Hotărârea Guvernului Nr.708 /2014 privind serviciul electronic guvernamental de jurnalizare (MLog), Monitorul Oficial Nr. 261-267 05.09.2014;
17. Hotărârea Guvernului Nr.916 /2007 cu privire la Concepția Portalului guvernamental, Monitorul Oficial Nr. 127-130/952 din 17.08.2007;
18. Hotărârea Guvernului Nr.330/2012 cu privire la crearea și administrarea portalului guvernamental unic al serviciilor publice, Monitorul Oficial Nr. 104-108 din 01.06.2012;

19. Hotărârea Guvernului Nr.701 /2014 cu privire la aprobarea Metodologiei publicării datelor guvernamentale deschise, Monitorul Oficial Nr. 256-260 din 29.08.2014;
20. Hotărârea Guvernului Nr.320 /2006 pentru aprobarea Regulamentului privind ordinea de aplicarea semnăturii digitale în documentele electronice ale autorităților publice, Monitorul Oficial Nr. 51-54 din 31.03.2006;
21. 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), Monitorul Oficial Nr.149-151 din 29.06.2020;
22. Hotărârea Guvernului nr.192 /2021 „Cu privire la aprobarea Conceptului Programului de vânzare directă a valorilor mobiliare de stat persoanelor fizice în Republica Moldova”, Monitorul Oficial Nr.249-253 din 15.10.2021.
23. Hotărârea Guvernului nr.712/2020 cu privire la serviciul guvernamental de plăți electronice (Mpay), Monitorul Oficial Nr.267-271 din 16.10.2020;
24. Ordinul Ministerului Finanțelor nr.215/2015 cu privire la aprobarea Normelor metodologice privind executarea de casă a bugetelor componente ale bugetului public național și a mijloacelor extrabugetare prin Contul Unic Trezorerial (CUT) al Ministerului Finanțelor, Monitorul Oficial Nr.377-391 din 31.12.2015.

Capitolul II. Spațiul funcțional al SI

2.1 Funcțiile de bază ale SI

Reieșind din destinația sistemului, pot fi delimitate procesele generale de administrarea financiară a RM și repartizate pe funcții de bază ale SI:

1. Comunicare directă cu investitorii retail în privința VMS;
2. Administrare a contului utilizatorului retail.

Reieșind din funcțiile menționate mai sus, SI urmează să îndeplinească următoarele cerințe de bază:

- a) dezvoltarea unui mediu de colaborare sigur și protejat, care să ofere un instrument de colaborare persoanelor fizice, indiferent de locația fizică a acestora;

- b) asigurarea accesului la SI a tuturor utilizatorilor prin intermediul unui mecanism integrat: portalul WEB al sistemului, în funcție de rolurile și drepturile de care dispun utilizatorii;
- c) consolidarea și gestiunea unui depozit de date aferent activității MF și interacțiunii reciproce cu resurse informaționale externe, având rolul de a genera rapoarte și analize destinate asistenței procesului de luare a decizie la nivelul MF sau statului;
- d) asigurarea autenticității, protecției și integrității datelor în procesul colectării, stocării, procesării și utilizării în cadrul SI;
- e) automatizarea proceselor de colectare sau diseminare a datelor primare prin intermediul proceselor de interacțiune automată cu SI ale autorităților publice din RM.

Pe lângă funcțiile de bază, SI urmează să asigure realizarea unor funcții auxiliare necesare bunei funcționari a acestuia:

Funcții de administrare a infrastructurii TIC:

- a) asigurarea accesului la informație pentru utilizatorii autentificați și autorizați;
- b) menținerea, actualizarea și dezvoltarea infrastructurii tehnice și program;
- c) asigurarea suportului și asistenței în operarea componentelor SI;
- d) asigurarea conformării cu condițiile de licențiere a produselor program.

Funcții de audit și control:

- a) auditul activităților utilizatorilor autorizați;
- b) jurnalizarea activităților utilizatorilor autorizați și a proceselor automate implementate în cadrul SI;
- c) colectarea statisticilor și generarea de rapoarte relevante.

2.2 Contururile funcționale de bază ale SI

Contururile funcționale de bază ale SI sunt:

1. Gestionarea contului în sistem, care va asigura următoarele funcții:
 - a) înregistrarea și crearea în mod automat al contului;
 - b) managementul ulterior al datelor primare aferente contului;
 - c) modificarea în mod automat a datelor primare personale ale utilizatorilor.
2. Gestionarea cererilor în sistem, care va asigura următoarele funcții:
 - a) asigurarea operațiunilor de plată;

- b) gestionarea cererilor utilizatorilor.
- 3. Auditarea sistemului, care va asigura următoarele funcții:
 - a) vizualizarea evenimentelor jurnalizate;
 - b) generarea rapoartelor analitice.
- 4. Administrarea sistemului, care va asigura următoarele funcții:
 - a) gestionarea utilizatorilor și drepturile de acestora;
 - b) gestionarea copiilor de rezervă;
 - c) monitorizarea performanței sistemului;
 - d) generarea rapoartelor, statisticilor și indicatorilor de performanță;
 - e) suportul tehnic și mentenanță;
 - f) gestionarea metadatelor;
 - g) gestionarea clasificatoarelor, nomenclatoarelor.

Capitolul III. Structura organizațională a SI

Proprietarul Sistemului Informațional este Republica Moldova.

Posesorul Sistemului Informațional este Ministerul Finanțelor.

Deținătorul Sistemului Informațional este Instituția Publică „Centrul de Tehnologii Informaționale în Finanțe”, care își exercită atribuțiile în conformitate cu cadrul normativ în materie de administrare tehnică și menținere a Sistemelor Informaționale de stat, în conformitate cu HG Nr.125/2018.

Administratorul tehnic al Sistemului Informațional este Instituția Publică „Serviciul Tehnologia Informației și Securitatea Cibernetică”, care își exercită atribuțiile în conformitate cu cadrul normativ în materie de securitate cibernetică a sistemelor informaționale de stat, în conformitate cu Legea Nr.467/2003.

Registrator de date va fi posesorul, care va înregistra, actualiza, radia date din sistem.

Furnizori de date vor fi:

1. Agenția Servicii Publice, care va furniza date din Registrul de Stat al Populației.
2. Serviciul Fiscal de Stat, care va furniza date din Registrului conturilor bancare.
3. Depozitarul Central Unic, care va furniza date aferente VMS.
4. Ministerul Finanțelor, care va furniza date aferente tranzacțiilor cu VMS.

Destinatari de date vor fi MF, DCU, investitorii retail, băncile în limita dreptului de acces la sistem, acordat în conformitatea cu legislația.

Capitolul IV. Documentele SI

Documentele de bază ale SI se clasifică, după cum urmează:

1. Documentele de intrare ale SI sunt considerate:
 - a) solicitarea de procurarea a VMS;
 - b) solicitarea de vânzare a VMS înainte de scadență.
2. Documentele de ieșire ale SI sunt considerate:
 - a) Nota de plată;
 - b) Confirmarea de plată a notei;
 - c) Notificarea utilizatorului privind emisiunile VMS disponibile pentru cumpărare;
 - d) Notificarea utilizatorului privind emisiunile VMS disponibile pentru răscumpărare;
3. Documentele tehnologice ale SI sunt considerate:
 - a) Semnăturile documentelor și înregistrărilor semnate digital;
 - b) Certificatele digitale cu care au fost produse semnăturile digitale;
 - c) Șabloanele documentelor menționate mai sus;
 - d) Forme electronice;
 - e) Documentele ce conțin înregistrări de audit privind acțiunile utilizatorilor;
 - f) Rapoarte, statistici și indicatori de performanță agregate privind utilizarea sistemului.

Capitolul V. Spațiul informațional al SI

5.1. Obiectele informaționale gestionate de SI

Ca urmare a implementării SI, acesta trebuie să conțină o serie de obiecte informaționale care vor putea fi utilizate în scopul executării cerințelor așteptate, listate mai jos:

- a) Profilurile investitorului retail – reprezintă obiecte informaționale care furnizează totalitate datelor aferente investitorului retail.
- b) Obiectele VMS – reprezintă obiecte informaționale care furnizează date aferente VMS.
- c) Notificări – reprezintă obiecte informaționale care înștiințează utilizatorii sistemului despre anumite evenimente din cadrul sistemului.

- d) Fișiere de jurnalizare - reprezintă obiecte informaționale destinate auditului SI și implementării politicii de asigurare a securității informaționale. Orice modificare potențial periculoasă: creare, modificare, marcarea la ștergere, schimbarea statutului trebuie să fie înregistrată în registre speciale (fișiere de jurnalizare) arătând momentul de timp și utilizatorul care a efectuat modificarea potențial periculoasă. În caz că modificările potențial periculoase nu vor implica suprimarea fizică a datelor pentru fiecare înregistrare sau atribut va fi posibil de văzut utilizatorul care a efectuat ultima modificare.
- e) Metadate – reprezintă totalitatea nomenclatoarelor/clasificatoarelor din sistem.

Pentru obiectele informaționale preluate din SI externe se va prelua modalitatea de identificare a obiectelor informaționale respective existente în aceste sisteme informatice (pentru a asigura un mecanism eficient de sincronizare a datelor). La această categorie de obiecte informaționale se referă:

- a) Datele de identificare a investitorilor retail (conform identificatoarelor *Registrului de Stat al Populației*);
- b) Elemente de securitate personalizate ale utilizatorilor (Credentials) (conform identificatoarelor Autorității de certificare sau serviciului *M-Pass*);

Pentru celelalte obiecte informaționale vor fi utilizate principiile interne de atribuire a identificatoarelor unice.

Astfel, SI va oferi registre specializate care vor atribui și înregistra în mod automat identificatoare pentru totalitatea obiectelor informaționale create în cadrul SI .

5.2. Scenariile de bază ale SI

Scenariul de bază reprezintă lista evenimentelor sau a proceselor aferente obiectelor informaționale.

1. Scenariul procesului de vânzare directă a VMS de către MF

Din punct de vedere al utilizatorului Investitorul retail, scenariul procesului de cumpărare a VMS este descris mai jos:

- a) Persoana fizică, se autentifică pe Platforma electronică pentru vânzarea VMS prin intermediul serviciului guvernamental de autentificare și autorizare (MPass).

- b) Investitorul retail va putea accesa listele de VMS pe parcursul perioadei de subscriere anunțate de MF, și plasa ordine de procurare a instrumentelor respective la prețul afișat pe Platforma electronică pentru vânzarea VMS.
- c) Odată ce ordinul de procurare este confirmat prin semnătură electronică de către utilizator, sistemul va redirecționa utilizatorul către interfața de plăți a serviciului guvernamental MPay. Pentru a asigura execuția ordinului într-un „timp cvasi-real”, utilizatorul va avea timp limită pentru efectuarea plății. Dacă plata nu va fi efectuată în acel interval de timp, ordinul va fi respins de sistem și va trebui retrimis.
- d) După finalizarea plății, persoana va fi direcționată înapoi pe Platforma electronică pentru vânzarea VMS unde i se va afișa statutul plătit la ordinul său. Ulterior, persoana va fi notificată prin MNotify aferent statutului plății (reușit/eșuat). Această notificare se actualizează în profilul de utilizator al investitorului retail, cu indicarea clară a stării curente a decontării și confirmarea faptului că VMS procurate urmează a fi înscrise în cont în ziua de închidere a perioadei de subscriere.
- e) După procurarea VMS, la atingerea datei scadente de plată a dobânzii sau în cazul răscumpărării anticipate sau preschimbării a VMS, Platforma electronică pentru vânzarea VMS va transmite informația necesară în Registrul de conturi personale, în scopul asigurării plății dobânzii către persoana fizică și va notifica persoana prin intermediul MNotify.
- f) Plata dobânzii, precum și plata pentru VMS răscumpărate vor fi efectuate la contul de plăți indicat de utilizator și va marca eliberarea plății corespunzător în Registrul de conturi personale.

Din punct de vedere al utilizatorului Emitentul de VMS (MF), scenariul procesului de vânzare electronică al VMS este descris mai jos:

- a) Funcționarul MF, se autentifică prin intermediul serviciului guvernamental de autentificare și autorizare (MPass) în cadrul back-endului Platformei electronice de vânzarea VMS.
- b) În back-end-ul Platformei electronice de vânzarea VMS, funcționarul poate gestiona stocurile de VMS, cum ar fi: crearea, modificarea, ștergerea parametrilor principali al VMS, solicitarea înregistrării VMS în sistemul DCU, transmiterea comunicatelor către DCU privind plasarea/răscumpărarea anticipată/preschimbarea VMS, setarea perioadei de subscriere pe parcursul căreia investitorii retail pot plasa ordine de cumpărare a VMS, transmiterea către DCU la finele perioadei de subscriere a informațiilor cu privire la

cantitatea de VMS subscrisă de investitori și care necesită a fi înregistrată în contul omnibus.

2. Scenariul procesului de vânzare de către investitorii retail a VMS deținute către dealerii primari

Investitorul retail autentificat pe Platforma electronică pentru vânzarea VMS, va transmite un formular de cerere, cu privire la intenția sa de a vinde o anumită cantitate din VMS cu un anumit cod ISIN, pe care le-a procurat anterior prin intermediul Platformei. Platforma electronică pentru vânzarea VMS va transmite cererea de ofertă către dealerul sau dealerii primari selectați de către MF;

După recepționarea prețului oferit de dealerul primar, utilizatorul confirmă sau respinge formularul de vânzare.

Odată confirmată, tranzacția este expediată electronic către DCU pentru decontare. Decontarea este executată în cadrul sistemului DCU existent, conform regulilor și regulamentului acestuia.

DCU va asigura transferul mijloacelor bănești rezultate în urma tranzacției către contul IBAN al MF, care va asigura transferul ulterior al fondurilor către contul clientului vânzător.

5.3. Interacțiunea cu alte sisteme și platforme electronice guvernamentale

Va fi găzduit pe platforma tehnologică guvernamentală comună (MCloud pentru MF) care funcționează în baza tehnologiei de „cloud computing”, utilizată pentru găzduirea SI guvernamentale.

Sistemul va interacționa cu următoarele platforme și servicii electronice guvernamentale:

- a) platforma de interoperabilitate (MConnect) – pentru schimbul de date cu alte SI și registre de stat;
- b) serviciul electronic guvernamental de autentificare și control al accesului (MPass) - pentru autentificarea și controlul accesului în cadrul sistemului;
- c) serviciul electronic guvernamental de jurnalizare (MLog) - pentru asigurarea evidenței operațiunilor (evenimentelor) produse în sistem;
- d) serviciul electronic guvernamental de notificare (MNotify) – pentru notificarea utilizatorilor;
- e) serviciul electronic guvernamental de plăți (MPay) – pentru asigurarea achitărilor VMS;

- f) serviciul electronic guvernamental de semnare (MSign) – pentru asigurarea autenticității și aplicării semnăturii electronice de către investitorii retail;
- g) sistemul informațional „Registrul de Stat al Populației” – pentru accesul la datele aferente personale ale persoanei fizice.
- h) sistemul informațional „Registrul conturilor bancare” – pentru accesul la datele aferente conturilor investitorilor retail.

5.4. Furnizorii de date

Principalii furnizori de date pentru SI sunt :

- a) Registrul de stat al populației al Agenției Servicii Publice;
- b) Registrul conturilor bancare din cadrul SIA „Creare și circulație a documentelor electronice în SFS și IF” al Serviciului Fiscal de Stat.

Informația furnizată de fiecare registru este prezentată în tabelul de mai jos.

Instituția deținătoare	Registrul de stat	Tipul de informații
Agencia Serviciilor Publice	Registrul de stat al populației	Persoane fizice: <ul style="list-style-type: none"> • numărul de identificare de stat - IDNP • nume • prenumele • patronimicul • data nașterii • numărul, seria, valabilitatea documentului de identificare al persoanei • imaginea grafică
Serviciul Fiscal de Stat	Registrul conturilor bancare	Contul bancar al persoanei fizice: <ul style="list-style-type: none"> • IBAN • IDNP • Tip cont • Tip valută

5.5. Clasificatoarele (nomenclatoarele) SI

În scopul asigurării veridicității și reducerii volumului informației stocate în SI precum și al clasificării corecte a obiectelor sistemului, se utilizează următoarele nomenclatoare:

Locale (propriei sistemului):

1. nomenclatorul utilizatorilor;
2. nomenclatorul permisiunilor;
3. nomenclatorul tipurilor documentelor;

4. nomenclatorul stării documentelor;
5. nomenclatorul stărilor dosarelor de executare;
6. nomenclatorul documentelor executorii.

Capitolul VI. Spațiul tehnologic al SI

6.1 Nivelele infrastructurii informaționale ale SI

La dezvoltarea sistemului se va aplica arhitectura multi-nivel (având cel puțin următoarele nivele - baza de date, logica de aplicație și interfața cu utilizatorul) și principiile agile. Utilizarea unei astfel de arhitecturi și principii va permite o cuplare redusă între componente, în care responsabilitățile fiecărei componente sunt specializate, precum și implementarea iterativă, operarea modificărilor și flexibilitate în implementare.

Sistemul va utiliza standarde deschise și va fi compatibilă cu sisteme care, la fel, utilizează standarde non-proprietare, cât și cu standardele deja existente.

Infrastructura informațională a sistemului se formează din două nivele:

- a) Nivelul superior – este nivelul caracteristic infrastructurii informatice și de comunicație aferente structurii centrale, constituie totalitatea echipamentelor tehnice și infrastructurii program găzduite în centrul de date al MF, M-Cloud și I.P. „CTIF”.
- b) Nivelul inferior – este un nivel caracteristic infrastructurii informatice și de comunicație și infrastructurii program găzduite în cadrul MF.

Fiecare nivel conține unul sau câteva obiecte informaționale de telecomunicații. Nucleul informațional al SI este depozitul de date. În activitatea sa, SI interacționează cu soluțiile informatice ale altor autorități publice din RM.

6.2 Arhitectura SI

Arhitectura SI „Platforma electronică pentru vânzarea VMS” va fi creată din următoarele nivele :

- a) Infrastructura de prezentare;
- b) Infrastructura procedurilor de sistem;
- c) Infrastructura bazelor de date;
- d) Infrastructura de integrare cu SI ale autorităților publice;
- e) Infrastructura de interoperabilitate guvernamentală.

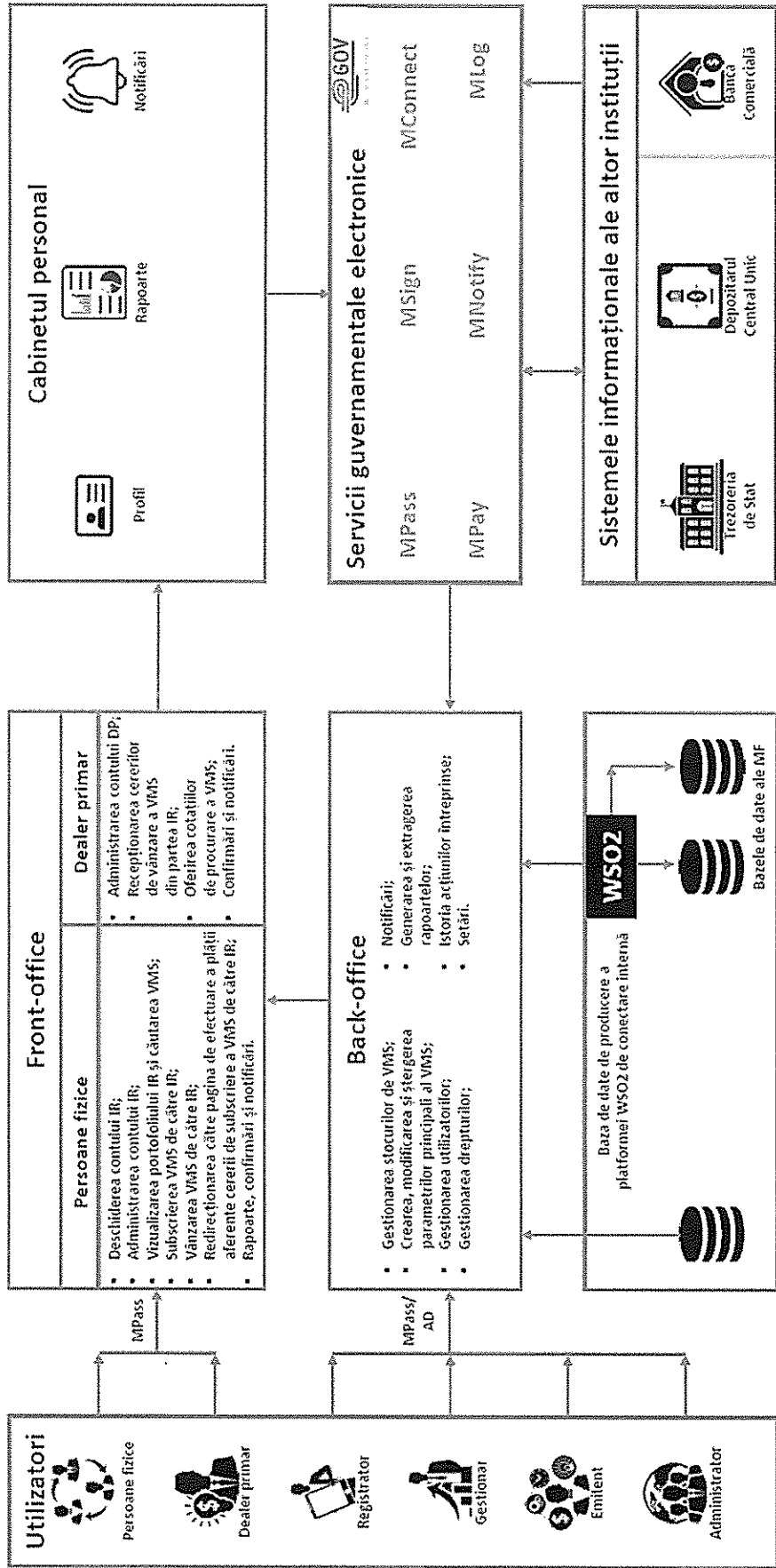


Figura 2 Arhitectura SI „Platforma electronică pentru vânzarea VMS”

Infrastructura de prezentare – reprezintă setul de portaluri ce asigură interacțiunea utilizatorilor cu SI.

Infrastructura procedurilor de sistem – reprezintă totalitatea fluxurilor de lucru, acțiunilor ce asigură funcționalitatea sistemului.

Infrastructura bazelor de date – reprezintă totalitatea bazelor de date care interacționează pentru schimbul de date, pentru stocarea datelor.

Infrastructura de integrare cu sistemele informaționale ale autorităților publice – reprezintă totalitatea SI ale autorităților publice care furnizează, consumă date aferente VMS.

Infrastructura de interoperabilitate guvernamentală – reprezintă serviciile guvernamentale de platformă (MConnect, Mpay, MPass, MNotify, MLog) destinate schimbului de date între instituțiile participante la procesele sistemului.

6.3 Complexe tehnice de program ale SI

Platforma tehnologică a SI constă din ansamblul produselor de program și a echipamentului care furnizează realizarea „materială” a SI. Pot fi delimitate următoarele cerințe față de platforma tehnologică a SI:

- a) asigurarea și suportul formatelor unice de prezentare a datelor și a protocoalelor comune de schimb de date;
- b) protecția informație contra accesului nesancționat la orice etapă de transfer și/sau prelucrare a acesteia;
- c) asigurarea accesului permanent la date;
- d) asigurarea funcționării fiabile a rețelei și prevenirea posibilității de supraîncărcare a acesteia;
- e) compatibilitatea interfețelor de sistem, a tehnicilor de prelucrare a informației.

Capitolul VII. Asigurarea securității informaționale

Sistemul complex al securității informaționale reprezintă totalitatea măsurilor legislative, normative, organizatorice și economice, precum și a mijloacelor software-hardware, care sunt orientate spre asigurarea unui nivel necesar al integrității, confidențialității și accesibilității resurselor informaționale ale sistemului, pentru minimizarea prejudiciilor care ar putea fi suportate de utilizator și proprietar.

Obiectivele principale ale securității trebuie să fie:

- a) Asigurarea integrității informației - protecția împotriva modificării și distrugerii datelor;
- b) Asigurarea confidențialității - protecția împotriva accesării neautorizate a datelor;

- c) Asigurarea disponibilității - protecția împotriva blocării accesului utilizatorilor autorizați la resursele informaționale;
- d) Asigurarea funcționării fără deficiențe în procesul realizării unor operațiuni concrete;
- e) Asigurarea monitorizării proceselor - capacitatea proceselor IT de a fixa orice activitate a utilizatorilor sau a proceselor, precum și ținerea evidenței evenimentelor legate de informație.

Cerințele principale ale securității trebuie să fie:

- a) Complexitate;
- b) Obiective orientate;
- c) Continuitate;
- d) Fiabilitate, durabilitate;
- e) Gestionare centralizată;
- f) Suficiență rezonabilă.

Etapetele creării sistemului complex de securitate informațională:

- a) Determinarea profilurilor de securitate;
- b) Clasificarea resurselor protejate;
- c) Analiza riscurilor;
- d) Dezvoltarea politicii de securitate;
- e) Dezvoltarea arhitecturii de securitate;
- f) Crearea și implementarea sistemului din punct de vedere a securității informaționale;
- g) Certificarea sistemului informațional automatizat.

Componentele de bază ale sistemului securității informaționale:

- a) Protecția informației și a infrastructurii de mentenanță la conectare la rețelele externe;
- b) Protecția informației în procesul interacțiunii dintre rețele;
- c) Protecția fluxurilor de date;
- d) Protecția serviciilor sistemului informațional automatizat;
- e) Protecția antivirus;
- f) Asigurarea securității mediului de program;
- g) Accesul autentificat și monitorizat;
- h) Protocolare și auditul.

Principalele mecanisme tehnologice de asigurare a protecției și securității informaționale în cadrul SI sunt:

- a) Permisunile utilizatorilor și semnătura electronică. Semnătura electronică și permisunile utilizatorilor sunt modalități de securitate care asigură autorizarea, confidențialitatea, autenticitatea și non-repudierea. Aceste servicii se bazează pe infrastructura de semnătură electronică

MSign și pe directoarele de sistem pentru a gestiona permisiunile utilizatorilor și autorizarea la nivelul blocurilor funcționale.

- b) Înregistrarea și accesul utilizatorilor. Sistemul este capabil de a determina univoc dacă utilizatorul este cel care pretinde că este. Procesul de înregistrare este asigurat de administratorul sistemului, iar contul de utilizator al persoanei care accesează informațiile din cadrul sistemului se va activa către sistem în momentul autentificării utilizatorului prin intermediul serviciului guvernamental MPass, cu semnătura electronică.
- c) Autentificare. Utilizatorii care accesează informațiile și funcționalitățile sistemului sunt autentificați înainte de a li se permite accesul.
- d) Autorizare bazată pe roluri. Sistemul restricționează drepturile de acces ale utilizatorului la funcționalitățile sistemului pe baza rolului desemnat acestuia. Fiecare utilizator are asociat unul sau mai multe roluri. Fiecare rol are asociat un set de drepturi. Drepturile reprezintă prerogativele acordate unui utilizator de a efectua anumite activități în cadrul unui sistem informatic. Sistemul poate limita sau permite accesul unui utilizator la anumite date și funcționalități pe baza apartenenței la un rol.
- e) Control acces. Sistemul include mecanisme de prevenire a utilizării neautorizate sau de manieră neautorizată a resurselor. Fiecărui utilizator autorizat i se asociază o autorizare. Controlul accesului constă în restricționarea capacității unui subiect de a folosi un sistem sau un obiect în acel sistem, precum și jurnalizarea activităților efectuate. Utilizatorii sistemului sunt autorizați să lucreze doar asupra elementelor informaționale pentru care au permisiunile necesare. Cererea de motivare a accesului este realizată în cadrul unui sistem de control al accesului, în care este stabilit: cine, cui, în conformitate cu care împuterniciri, pentru care acțiuni sau care tip de acces poate fi permis și în care condiții, și care presupune determinarea pentru toți utilizatorii, a resurselor informaționale și program la care au acces pentru operații concrete de accesare (citire, scriere, modificare, ștergere, execuție) folosind resursele tehnice și program de accesare.
- f) Infrastructura de semnătură electronică. Sistem de semnătură electronică ce permite utilizatorilor să semneze documente cu putere juridică. În calitate de mecanism de implementare a semnăturii electronice în cadrul sistemelor este folosit serviciul guvernamental MSign. Semnătura electronică și controlul accesului constituie măsurile de control de securitate, care asigură integritatea, confidențialitatea, disponibilitatea, autenticitatea și non-repudierea.
- g) Administrare (configurare). Sistemul permite aplicarea politicilor de securitate încorporate în arhitectura și funcționalitățile lui. Definirea utilizatorilor și grupurilor sau rolurilor, precum și atribuirea de drepturi se realizează de către utilizatori cu drepturi de deținător, doar în urma

coordonării și oferirii acceptului de către posesor. Sistemul permite delegarea administrării drepturilor complet sau limitat la anumite operații (de exemplu, adăugare utilizator, modificare clasificatoare) către alți utilizatori dintr-o organizație. Sistemul oferă posibilitatea ca deținătorul să poată configura restricții legate de adresele de IP sau domeniile de la care conectarea va fi permisă, pentru fiecare utilizator/grupuri de utilizatori în parte.

- h) Securitatea împotriva accesului neautorizat. Sistemul informatic este protejat împotriva încercărilor deliberate sau accidentale de acces neautorizat la datele pe care acesta le stochează. SI include următoarele facilități:
- controlul accesului utilizatorilor la sistemele de aplicații și fișierele de date;
 - ierarhizarea în clase a utilizatorilor finali;
 - permiterea accesului direct la bazele de date numai administratorilor de baze de date autorizați;
 - asigurarea securității tuturor interfețelor sistemului;
 - raportarea pe baze periodice a detaliilor privitoare la accesul în sistem al utilizatorilor.
- i) Efectuarea auditului. Activitățile derulate în sistem sunt înregistrate, fiind posibilă ulterior efectuarea auditului. O necesitate importantă legată de securitate este necesitatea păstrării tuturor înregistrărilor, tranzacțiilor, incidentelor de sistem, în scopul identificării modului de funcționare, pentru analiza integrității sistemului, pentru monitorizarea activității utilizatorilor. Sistemul se bazează pe un mecanism de înregistrări de audit ce urmează practicile mondiale curente. Pentru garantarea securității la nivelul infrastructurii tehnico-logice este implementat auditul activ al securității informaționale.
- j) Disponibilitatea sistemului. Utilizatorii depind într-o măsură considerabilă de disponibilitatea sistemului pentru a-și putea îndeplini sarcinile. Acest lucru ridică cerințe semnificative față de infrastructura SI pentru ca aceasta să fie rezistentă la erori de hardware și software. Pentru a preveni aceste probleme, infrastructura include un set de circuite redundante care consistă din noduri de rezervă ce vor prelua încărcătura sistemului pe timpul cât sistemul principal se află în proces de mentenanță sau restaurare.
- k) Integritatea datelor. Asigurarea protecției, exactității și completitudinii datelor și a soluțiilor furnizate pentru stocarea și gestionarea acestora, dar și asigurarea împotriva manipulării frauduloase a datelor/informațiilor. Datele stocate și procesate în sistem urmează a fi corecte și complete. Protecția împotriva dezastrelor este realizată prin crearea copiilor de rezervă incrementale și depline. Sistemul permite implementarea unor mecanisme

care să verifice și să valideze datele din punctul de vedere al corectitudinii și completitudinii.

- l) Securitatea informației. La transmiterea informațiilor confidențiale sau protejate de stat, se va ține cont de transmiterea informației prin canale de comunicații securizate pentru a preveni falsificarea, scurgerea informației.
- m) Pentru gestiunea riscurilor de securitate va fi implementată o politică generală de securitate. Politica de securitate va include prevederi referitoare la organizarea auditurilor periodice de securitate pentru a verifica politica și conformitatea cu regulile de securitate, precum și a stabili domeniile care necesită îmbunătățiri.
- n) Securitatea informațională se menține pe parcursul întregului ciclu de viață a SI și se perfecționează continuu, pentru prevenirea noilor pericole.
- o) Asigurarea securității informației se va realiza de către I.P. CTIF în conformitate cu cerințele standardelor internaționale în domeniu.

Capitolul VIII. Dispoziții finale

Prezentul Concept reprezintă viziunea privind procesele ce urmează a fi dezvoltate în vederea elaborării SI. Implementarea SI va conduce la optimizarea proceselor punând la dispoziția utilizatorilor un set de instrumente, tehnici moderne și ușor de utilizat, totodată asigurând o performanță a întregului sistem de gestionare a VMS și acțiunile aferente acestora în conformitate cu standardele internaționale de eficiență, stabilitate și securitate. Crearea noului sistem va avea drept rezultat principal alinierea capacității MF la tehnologiile informaționale și comunicaționale moderne.

În urma aprobării prezentului Concept va fi elaborat Sistemului Informațional și Regulamentul privind utilizarea și administrarea Sistemului Informațional.