Anexa la Ordinul SFS nr. _____ din _____

Program de dezvoltare IT al Serviciului Fiscal de Stat pentru anii 2025-2027

Anul 2024

CUPRINS

1. Abrevieri și Noțiuni

1.1. Abrevieri

IP CTIF	–	**Instituția Publică Centrul de Tehnologii Informaționale în Finanțe**
SISFS	–	Sistem informațional al Serviciului Fiscal de Stat
STISC	–	Instituția Publică Serviciul Tehnologia Informațiilor și Securității Cibernetice
TIC	–	Tehnologia informației și comunicațiilor
DWH	–	DataWareHouse
SFS	–	Serviciul Fiscal de Stat
VIES	–	VAT Information Exchange System
OSS	–	One Stop Shop
CESOP	–	Central Electronic System on Payment Information
SIEM	–	Security Information and Event Management
DLP	–	Data Loss Prevention
VPN	–	Virtual Private Network
LAN	–	Local Area Network
WAN	–	Wide Area Network
IDS/IPS	–	Intrusion Detection/Prevention Systems
DAC	–	Directives Administrative Cooperation

1.2. Noţiuni

Abundența datelor	–	este cantitatea mare și disponibilitatea unui volum vast de date. Aceasta poate include date structurate și nestructurate provenite dintr-o varietate de surse, cum ar fi dispozitive IoT (Internet of Things), rețele sociale, tranzacții online, sisteme de monitorizare a sănătății etc. Abundența datelor este caracterizată de volumul crescut, viteza mare de generare și varietatea informațiilor disponibile.
DataLake	–	este un depozit centralizat conceput pentru a stoca, procesa și securiza cantități mari de date structurate, semi structurate și nestructurate
Internet of Things	–	se referă la rețeaua interconectată de dispozitive fizice sau obiecte care sunt încorporate cu tehnologie, software, senzori și alte funcționalități pentru a colecta și schimba date.
Non-core	–	se referă la activitățile care nu sunt considerate parte esențială sau centrală a unei afaceri sau organizații. Activitățile "non-core" sunt cele care nu sunt direct legate de principalele obiective sau scopuri ale organizației și care nu contribuie direct la realizarea misiunii sau viziunii acesteia.
DataWareHouse	–	se referă la un depozit de date centralizat și organizat, utilizat pentru stocarea și analiza informațiilor din diverse surse de date ale unei organizații. Este proiectat pentru a facilita rapoartele, analizele și luarea deciziilor bazate pe date, oferind o perspectivă consolidată și coerentă asupra informațiilor de afaceri
Data Centru	–	Infrastructura care centralizează și gestionează toate resursele de stocare și calcul necesare pentru funcționarea sistemelor IT ale SFS.
Virtualizare	–	Tehnologia prin care resursele fizice, precum serverele, sunt divizate în mai multe resurse virtuale pentru eficiență și scalabilitate.
SIEM	–	Un sistem care monitorizează și analizează evenimentele de securitate din infrastructura IT, detectând și prevenind atacurile cibernetice.
DLP	–	Tehnologie care previne scurgerile de informații sensibile din cadrul organizației prin monitorizarea și controlul fluxului de date.

VPN	–	Rețea privată virtuală care asigură o conexiune securizată și criptată între două sau mai multe dispozitive pe internet.
IDS/IPS	–	Sisteme de detectare și prevenire a intruziunilor în rețeaua IT, care monitorizează traficul de rețea și aplică măsuri de securitate
DLP	–	Tehnologie care previne scurgerile de informații sensibile din cadrul organizației prin monitorizarea și controlul fluxului de date.

1.3. Aspecte cheie legate de infrastructura IT și securitate cibernetică

În contextul modernizării Serviciului Fiscal de Stat (SFS) și alinierea la cerințele Uniunii Europene, este esențial să înțelegem conceptul de **infrastructură IT** și componentele cheie ale **securității cibernetice**. Aceste concepte reprezintă pilonii pe care se va baza dezvoltarea și protecția datelor, garantând astfel eficiența, disponibilitatea și securitatea informațiilor fiscale.

Infrastructura IT se referă la totalitatea componentelor hardware, software, rețele și resurse necesare pentru funcționarea eficientă a unui sistem IT. În cadrul SFS, aceasta include:

- **Data Centru**, care este nucleul infrastructurii IT, unde se stochează și se procesează datele critice. Un centru de date modernizat va asigura scalabilitatea și redundanța necesare pentru a face față volumelor mari de informații fiscale și pentru a oferi continuitate în caz de incidente. Prin utilizarea soluțiilor de stocare redundantă (SAN/NAS) și a tehnologiilor de recuperare în caz de dezastru (DR), SFS va putea proteja datele esențiale și asigura continuitatea operațiunilor.
- **Tehnologiile de virtualizare** permit rularea mai multor sisteme și aplicații pe o singură platformă hardware, crescând astfel eficiența utilizării resurselor. Virtualizarea reduce costurile, permite un management mai flexibil al resurselor și îmbunătățește recuperarea în caz de incidente, făcând infrastructura IT mai agilă și mai rezistentă la avarii.
- **Rețelele locale LAN** conectează serverele și dispozitivele din cadrul instituției, în timp ce rețelele externe permit conectarea la alte instituții și platforme internaționale. Segmentarea rețelelor prin utilizarea VLAN-urilor și implementarea soluțiilor de optimizare a traficului asigură performanță și securitate ridicate, prevenind accesul neautorizat la resursele critice.
- **Rețele Private Virtuale (VPN)** sunt esențiale pentru accesul securizat la distanță al angajaților și partenerilor, mai ales în contextul colaborărilor internaționale. Aceste rețele folosesc criptarea pentru a proteja datele transmise și autentificarea multifactorială (MFA) pentru a preveni accesul neautorizat.

Pe măsură ce digitalizarea avansează, **securitatea cibernetică** devine o prioritate, inclusiv la nivel de stat. Protejarea datelor fiscale sensibile și a infrastructurii IT împotriva atacurilor cibernetice este esențială pentru menținerea încrederii contribuabililor și conformitatea cu standardele internaționale. Principalele componente ale securității cibernetice în cadrul SFS includ:

- **SIEM (Security Information and Event Management)**, care colectează, analizează și monitorizează în timp real evenimentele de securitate din infrastructura IT. Acesta poate detecta și răspunde rapid la atacuri cibernetice, cum ar fi încercările de acces neautorizat, și poate emite alerte

atunci când sunt detectate anomalii. Prin implementarea unui SIEM centralizat, SFS va avea o vizibilitate completă asupra incidentelor de securitate și va putea răspunde proactiv la acestea.

- **Sistemele DLP (Data Loss Prevention)** previn scurgerile de informații sensibile, asigurându-se că datele fiscale importante nu părăsesc sistemul neautorizat. Aceste sisteme monitorizează fluxurile de date și impun politici stricte de control al accesului și transferului de informații. Implementarea unui DLP va proteja SFS împotriva pierderii accidentale sau intenționate a datelor critice.
- **Firewall și IDS/IPS (Intrusion Detection/Prevention Systems)** sunt componente esențiale pentru protejarea infrastructurii de rețea. Firewall-urile controlează accesul la rețea, permițând doar traficul legitim, în timp ce sistemele IDS/IPS detectează și previn atacurile cibernetice, cum ar fi tentativele de penetrare sau exploatarea vulnerabilităților.
- **Criptarea și securizarea comunicațiilor** reprezintă un element de protecție a datelor în tranzit, importantă pentru schimburile de informații cu partenerii internaționali și contribuabilii. Criptarea end-to-end și utilizarea soluțiilor VPN asigură că datele sunt protejate împotriva interceptării neautorizate, asigurând totodată integritatea și confidențialitatea acestora.

2. Introducere

2.1. Context și necesitatea modernizării

În ultimele decenii, Serviciul Fiscal de Stat din Republica Moldova a inițiat și implementat reforme menite să îmbunătățească eficiența administrării fiscale și să consolideze relația cu contribuabilii. Totuși, în ciuda acestor eforturi, infrastructura IT a SFS nu a reușit să țină pasul cu schimbările rapide din tehnologie și cu cerințele tot mai complexe ale unui sistem fiscal modern. Pe măsură ce economia globală devine din ce în ce mai digitalizată, volumele mari de date, nevoia de automatizare și presiunile pentru integrarea cu sistemele fiscale internaționale impun o tranziție inevitabilă către o infrastructură IT mai avansată și o strategie modernă de administrare fiscală.

Un factor determinant în necesitatea modernizării SFS îl reprezintă creșterea exponențială a volumului de date fiscale pe care SFS trebuie să le gestioneze. Digitalizarea economiei, expansiunea comerțului electronic și creșterea numărului de contribuabili care își desfășoară activitățile în multiple jurisdicții creează provocări imense pentru infrastructura actuală. În acest context, procesele tradiționale, dependente de intervenția manuală și bazate pe sisteme învechite, nu mai sunt capabile să facă față acestei presiuni. Datele fiscale trebuie acum procesate rapid și cu un grad ridicat de acuratețe pentru a preveni erorile, evaziunea fiscală și alte forme de non-conformitate. Lipsa unui sistem IT eficient împiedică monitorizarea în timp real a activităților economice, limitând astfel capacitatea autorității de a detecta riscurile și fraudele în timp util.

În plus, transformările tehnologice globale și emergența noilor tehnologii, cum ar fi inteligența artificială, Big Data și analiza predictivă, oferă oportunități semnificative pentru SFS de a îmbunătăți și automatiza procesele fiscale. Aceste tehnologii permit autorităților fiscale să analizeze volume mari de date pentru a identifica tipare suspecte, comportamente de risc și pentru a îmbunătăți eficiența colectării impozitelor. Prin automatizarea proceselor repetitive și utilizarea de algoritmi avansați, se poate reduce considerabil timpul necesar pentru verificarea și administrarea impozitelor, creând în același timp o infrastructură flexibilă și scalabilă. De asemenea, utilizarea acestor soluții reduce dependența de resursele umane, eliminând erorile și asigurând o administrare fiscală mai transparentă și mai eficientă.

Un alt factor major care impune modernizarea urgentă a SFS este procesul de integrare a Republicii Moldova în Uniunea Europeană. În calitate de țară candidată la aderare, Moldova trebuie să-și alinieze politicile și sistemele fiscale la standardele și cerințele UE. Acest lucru presupune integrarea cu platformele europene de schimb de informații fiscale, cum ar fi VAT Information Exchange System (VIES), One Stop Shop (OSS) și Central Electronic System on Payment Information (CESOP). Aceste sisteme sunt esențiale pentru facilitarea tranzacțiilor economice transfrontaliere și pentru reducerea fraudei fiscale prin schimbul rapid și sigur de date fiscale între statele membre ale UE. În lipsa unei infrastructuri IT capabile să susțină aceste integrări, Republica Moldova riscă să rămână în urmă în procesul de armonizare cu politicile europene, afectându-și astfel șansele de aderare și dezvoltare economică pe termen lung.

Totodată, modernizarea infrastructurii IT a SFS este necesară și din perspectiva utilizării mai eficiente a resurselor umane și financiare. În momentul de față, multe dintre procesele administrative ale SFS sunt dependente de sisteme învechite, care nu mai sunt capabile să susțină nevoile actuale. Acest lucru duce la o utilizare ineficientă a resurselor, în special în ceea ce privește costurile de întreținere și operaționale. Prin adoptarea tehnologiilor cloud și a soluțiilor de

virtualizare, SFS poate reduce costurile asociate cu achiziționarea și întreținerea echipamentelor hardware tradiționale, permițând totodată o gestionare mai flexibilă și mai eficientă a datelor și a resurselor. Aceste tehnologii permit, de asemenea, o scalare rapidă a capacității de stocare și procesare, ceea ce este esențial pentru a face față volumelor de date în creștere, fără a investi în mod constant în infrastructuri fizice noi.

Un alt aspect important al modernizării îl reprezintă capacitatea de a răspunde rapid la schimbările globale și crizele economice sau sociale, cum a fost, de exemplu, pandemia de COVID-19. În această perioadă, s-a evidențiat necesitatea unor soluții digitale eficiente care să permită contribuabililor să interacționeze cu autoritățile fiscale de la distanță, fără a fi nevoiți să se deplaseze fizic la birourile locale. Lipsa unor astfel de soluții nu numai că afectează eficiența administrativă, dar subminează și încrederea contribuabililor în capacitatea instituției de a le oferi servicii eficiente și sigure. Modernizarea IT ar permite dezvoltarea unor platforme online robuste, capabile să susțină o gamă largă de servicii fiscale digitale, accesibile de oriunde și în orice moment.

Astfel, necesitatea modernizării infrastructurii IT a Serviciului Fiscal de Stat din Republica Moldova este determinată de o combinație de factori interni și externi, care variază de la creșterea volumului de date fiscale și oportunitățile oferite de noile tehnologii, până la cerințele de conformitate impuse de integrarea europeană. Modernizarea nu doar că va optimiza procesele fiscale, dar va asigura și o mai bună utilizare a resurselor, îmbunătățind în același timp experiența contribuabilului și întărind încrederea publicului în sistemul fiscal. În acest context, modernizarea IT reprezintă o prioritate strategică pentru dezvoltarea economică și administrativă a Republicii Moldova și o condiție esențială pentru integrarea sa reușită în Uniunea Europeană.

2.2. Misiunea și viziunea Serviciului Fiscal de Stat

MISIUNEA

SERVICIULUI FISCAL DE STAT AFERENT SISTEMULUI INFORMAȚIONAL

Facilitarea implementării proceselor de administrare fiscală prin intermediul tehnologiilor informaționale, care permite gestionarea instituției administrarea eficientă și eficace a proceselor menite întru realizarea atribuțiilor de bază a SFS și asigură un canal de comunicare cu contribuabilii operativ, interactiv și econom.

VIZIUNEA

SERVICIULUI FISCAL DE STAT AFERENT SISTEMULUI INFORMAȚIONAL

Un sistem integrat axat pe servicii digitale centrate pe utilizator, înzestrat cu date și instrumente care să permită buna administrare a proceselor interne ale instituției în vederea asigurării performanței.

VALORILE

SERVICIULUI FISCAL DE STAT AFERENT SISTEMULUI INFORMAȚIONAL

confidențialitate

integritate

disponibilitate

2.3. Alinierea la cerințele de aderare la Uniunea Europeană

Aderarea Republicii Moldova la Uniunea Europeană este un proces complex și de lungă durată, care necesită numeroase ajustări economice, politice și sociale. Un domeniu important în acest proces este alinierea administrării fiscale și infrastructurii IT ale Republicii Moldova la cerințele Uniunii Europene. Pentru SFS, această aliniere este importantă, deoarece Uniunea Europeană pune un accent deosebit pe eficiență administrativă, combaterea fraudei fiscale și facilitarea schimbului de informații între statele membre.

Un prim pas în această direcție este adoptarea și integrarea platformelor europene de schimb de informații fiscale, care sunt necesare pentru facilitarea tranzacțiilor economice și comerciale transfrontaliere. În acest sens, Republica Moldova trebuie să asigure compatibilitatea infrastructurii sale IT cu sisteme precum VIES (VAT Information Exchange System), OSS (One Stop Shop) și CESOP (Central Electronic System on Payment Information). Aceste sisteme ajută la monitorizarea și gestionarea eficientă a tranzacțiilor economice internaționale, prevenind evaziunea fiscală și consolidând controlul asupra fluxurilor financiare transfrontaliere.

Un alt aspect important al alinierii la cerințele Uniunii Europene este adoptarea și implementarea directivelor DAC (Directives Administrative Cooperation), care reglementează schimbul automat de informații fiscale între statele membre. DAC include o serie de directive care impun statelor membre obligații de a schimba automat informații cu privire la diverse domenii, inclusiv rulările fiscale (DAC3), rapoartele de țară (DAC4), proprietarii beneficiari (DAC5) și aranjamentele transfrontaliere (DAC6). Pentru a se conforma acestor cerințe, Republica Moldova trebuie să-și dezvolte capacitatea tehnologică de a colecta, procesa și transmite datele necesare conform standardelor impuse de Uniunea Europeană.

De asemenea, alinierea la cerințele europene presupune și o securizare avansată a infrastructurii IT și a schimburilor de date, în special în contextul informațiilor sensibile schimbate între autoritățile fiscale. Uniunea Europeană impune standarde ridicate de securitate cibernetică și protecția datelor, ceea ce înseamnă că SFS trebuie să implementeze soluții moderne de securitate cibernetică, precum criptarea datelor, protecția împotriva atacurilor cibernetice (IDS/IPS) și prevenirea scurgerilor de informații (DLP). Aceste măsuri sunt necesare pentru a asigura integritatea și confidențialitatea datelor fiscale transmise între autoritățile fiscale din diferite state membre ale Uniunii Europene.

Pe lângă integrarea tehnologică și securitatea informațiilor, alinierea la cerințele UE impune și o reformare a cadrului legislativ și a procedurilor administrative ale SFS. Legislația națională trebuie ajustată pentru a se conforma directivelor și reglementărilor europene, iar personalul SFS trebuie să fie instruit corespunzător pentru a aplica noile proceduri și standarde impuse de Uniunea Europeană. Acest proces va necesita investiții semnificative în formare și dezvoltare profesională, precum și colaborare strânsă cu experții europeni și autoritățile fiscale din alte state membre.

Așadar, alinierea la cerințele de aderare la Uniunea Europeană este crucială pentru modernizarea SFS și pentru integrarea Republicii Moldova în spațiul fiscal european. Adoptarea platformelor de schimb de informații fiscale, implementarea directivelor DAC și consolidarea securității cibernetice vor permite SFS să își îndeplinească obligațiile față de Uniunea Europeană și să faciliteze o tranziție lină către un sistem fiscal modern, eficient și transparent, compatibil cu standardele europene. Această aliniere va sprijini dezvoltarea economică a țării și va consolida relațiile comerciale și fiscale cu partenerii europeni.

3. Analiza situației

3.1. Starea actuală a sistemului informațional SFS (SISFS)

În prezent, SFS din Republica Moldova se confruntă cu diverse provocări legate de infrastructura sa IT și de procesele interne, care necesită îmbunătățiri semnificative pentru a se alinia la standardele moderne de eficiență și securitate.

O problemă majoră cu care se confruntă SFS este fragmentarea infrastructurii IT. Sistemele existente, deși au capacitatea de a gestiona procese importante precum declarațiile fiscale electronice și de evidență a obligațiilor fiscale, sunt dezvoltate pe platforme diferite, cu tehnologii variate. Această fragmentare creează probleme în ceea ce privește integrarea datelor și eficiența operațională. În plus, multe procese sunt încă realizate manual sau semi-manual, ceea ce duce la erori și la o performanță scăzută.

Un exemplu concret îl reprezintă dificultatea în gestionarea integrată a datelor între diferitele registre naționale și internaționale. Sistemele de înregistrare fiscală nu sunt complet compatibile între ele, ceea ce îngreunează accesul rapid și eficient la date. Deși au fost implementate soluții precum SIA „e-Cerere” și sistemul de facturare electronică SIA „eFactura”, acestea necesită extinderi și îmbunătățiri pentru a facilita o integrare completă și automatizarea proceselor.

Responsabilitatea pentru gestionarea IT și securitatea informațiilor în cadrul SFS este delegată în mare parte către IP CTIF (Instituţia Publică „Centrul de Tehnologii Informaționale în Finanțe”), ceea ce creează anumite limitări în vederea controlului direct al SFS asupra strategiei sale IT.

În plus, securitatea cibernetică a sistemelor IT necesită îmbunătățiri majore. În prezent, SFS nu dispune de un sistem robust pentru gestionarea vulnerabilităților și controlul accesului. Protocolul actual de gestionare a incidentelor nu este suficient de bine definit, iar măsurile de protecție împotriva scurgerilor de informații sau atacurilor cibernetice sunt limitate. Este necesară implementarea unor soluții mai avansate, cum ar fi criptarea end-to-end și sistemele de detectare a intruziunilor (IDS/IPS).

În ceea ce privește automatizarea proceselor de control fiscal, SFS folosește în prezent sisteme de analiză a riscurilor fiscale, însă majoritatea proceselor de control rămân dependente de intervenția manuală. Integrarea datelor și utilizarea analiticii avansate pentru operațiunile de control și conformare sunt încă în faze incipiente, ceea ce limitează capacitatea SFS de a monitoriza și detecta riscurile în timp real.

Sistemele de control și conformare trebuie îmbunătățite pentru a permite colectarea și analiza automată a datelor în timp real. Implementarea unui standard de raportare fiscală primară (SAF-T) și adoptarea de soluții avansate de analiză predictivă vor îmbunătăți capacitatea SFS de a identifica frauda fiscală și de a optimiza procesul de control și conformare.

O altă provocare majoră este capacitatea limitată a infrastructurii IT actuale de a susține volumul în creștere de date și cerințele analitice avansate. SFS nu dispune încă de un cadru robust de guvernanță a datelor, iar accesul la date în timp real este limitat. Integrarea datelor între diferitele sisteme este fragmentată, ceea ce afectează utilizarea eficientă a acestor date pentru luarea deciziilor informate și optimizarea proceselor interne.

Pentru a remedia aceste probleme, este necesară o modernizare extensivă a infrastructurii IT, inclusiv dezvoltarea unui cadru formal de guvernanță a datelor care să asigure calitatea, securitatea și integritatea datelor. De asemenea, trebuie implementate soluții de big data, inclusiv implementarea conceptului de DataWareHouse și instrumente de business intelligence, care să permită o analiză detaliată și luarea deciziilor bazate pe date, cu un accent special pe riscurile fiscale și conformitatea contribuabililor.

În ansamblu, analiza situației curente a SFS evidențiază necesitatea unei modernizări substanțiale a infrastructurii IT. Problemele de fragmentare a sistemelor, lipsa unei guvernanțe eficiente și automatizarea limitată a proceselor afectează grav eficiența și securitatea administrării fiscale. Pentru a se alinia la cerințele Uniunii Europene și pentru a îmbunătăți performanța, SFS trebuie să implementeze un cadru de guvernanță IT solid, să îmbunătățească securitatea cibernetică și să integreze soluții avansate de automatizare și analiză a datelor.

Managementul contribuabililor în administrația fiscală din Republica Moldova implică o serie de procese și măsuri menite să gestioneze eficient contribuabilii și să permită furnizarea de servicii fiscale electronice. Utilizarea tehnologiilor informaționale moderne joacă un rol semnificativ în eficientizarea acestor procese și în creșterea eficienței generale a procesului de administrare fiscală a contribuabililor. De asemenea, oferă oportunitatea de a transforma serviciile digitale de la servicii de tip cerere-executare-răspuns către servicii instantanee de autoservire prin mijloace on-line.

Analiza situației actuale se va prezenta conform principalelor procese de bază (core processes).

Înregistrarea contribuabililor:

O componentă importantă a procesului de administrare fiscală a contribuabililor este sistemul informațional automatizat „e-Cerere” *(în continuare – SIA „e-Cerere”)*, care permite contribuabililor să depună diverse cereri în format electronic. SIA „e-Cerere” este o soluție informațională menită să înlocuiască procedura tradițională de depunere a cererilor de către contribuabili cu un mecanism modern, bazat pe tehnologii informaționale.

Astfel, sistemul permite procesarea electronică a cererilor depuse on-line de către contribuabili și emiterea certificatelor de către SFS cu utilizarea semnăturii electronice pentru:

1. înregistrarea/anularea în calitate de plătitor de TVA;
2. înregistrarea on-line a contribuabililor/obiectelor impozabile;
3. înregistrarea/anularea în calitate de plătitor de Accize
4. efectuarea/amânarea controalelor fiscale;
5. modificarea perioadei fiscale;
6. eliberarea confirmării veniturilor;
7. stingerea obligației fiscale prin compensare și/sau restituirea mijloacelor bănești;
8. înregistrarea contractelor de locațiune;
9. eliberarea patentei de întreprinzător.

Nr. d/o	Denumirea serviciului din cadrul SIA „e-Cerere”	Total solicitări	Total solicitări Online	Total solicitări Ghișeu
1	Certificat de atribuire a codului fiscal	163 930	20	163 910

Nr. d/o	Denumirea serviciului din cadrul SIA „e-Cerere”	Total solicitări	Total solicitări Online	Total solicitări Ghișeu
2	Înregistrarea activității de prelucrare și/sau fabricare a mărfurilor supuse accizelor	38	32	6
3	Înregistrarea on-line a contribuabililor	8 577	6	8 571
4	Înregistrarea subdiviziunilor/obiectelor impozabile	76 433	60 432	16 001
5	Confirmarea privind veniturile obținute în Republica Moldova de persoanele fizice cetățeni ai Republicii Moldova	14 722	209	14 513
6	Eliberarea/prelungirea patentei de întreprinzător	38 618	93	38 525
Total		302 318	60 792	241 526

Efectuând analiza datelor dintre numărul total de solicitări depuse în regim online și numărul de solicitări la ghișeu, se atestă că totuși contribuabilii în mare parte preferă procedura tradițională.

Declarații fiscale și raportare:

Pentru depunerea declarațiilor fiscale este utilizat sistemul informațional automatizat „Declarație electronică”. În vederea implementării mecanismului de obligativitate a utilizării metodelor automatizate de raportare, SFS a avut o abordare etapizată prin conformarea treptată a contribuabililor în vederea utilizării mecanismului de raportare electronică. Acest lucru poate fi observat prin prisma modificărilor efectuate la art. 187 alin.(2^1) din Codul fiscal, inițiate încă din anul 2011.

Astfel, în anul 2023 avem o rată de **84,49%** de prezentare a dărilor de seamă fiscală prin metode automatizate de raportare electronică (1 578 045 declarații electronice din totalul de 1 867 685 declarații prezentate).

Colectarea impozitelor și taxelor:

Sistemul informațional automatizat „Contul curent al contribuabilului” permite accesul la informațiile privind obligațiile fiscale ale contribuabililor și verificarea situației actuale a tuturor restanțelor sau sumelor plătite în plus către bugetul public național. În situația actuală se atestă o perioadă de actualizare a datelor care se desfășoară cu întârziere, în cazul plăților procesarea se desfășoară într-o perioadă de la 1 zi la 5 zile, iar calculul cu 1 zile întârziere, or acest proces ar trebui să fie unul instant.

Modulul „Contul unic”, facilitează plata obligațiilor fiscale, oferind oportunitatea achitării tuturor obligațiilor fiscale printr-o singură plată. În anul 2019, modulul „Cont unic” a fost integrat cu serviciul guvernamental MPay, care permite plata obligațiilor fiscale direct de pe interfața modulului menționat, fără necesitatea imprimării și remiterii ordinului de plată la prestatorul de servicii de plată.

Acţiuni de conformare fiscală

SFS este relativ precar în ceea ce privește abundența și disponibilitatea datelor, nu dispune de suficiente integrări de date cu părți terțe și, de fapt, nu utilizează în mod eficient instrumente de analiză generală și/sau avansată pentru a obține valoare din date.

Guvernanța datelor este centralizată și definită prin aplicarea bunelor practici de management în cadrul SFS. SFS trebuie să își îmbunătățească capacitatea de a ști ce tip de date, momentul și modul în care le gestionează, să îmbunătățească în mod sistematic calitatea datelor și să aplice bune practici de guvernanță a datelor.

În prezent, SFS nu poate îmbunătăți în mod semnificativ procesele fiscale de bază fără a consolida SISFS, sub o singură platformă standardizată. Îmbunătățirile părților separate pot aduce mici câștiguri, dar nu schimbări strategice. Principalele limitări sunt următoarele:

1. Infrastructură TIC la IP CTIF aflată la sfârșitul duratei de viață și necesită investiții de capital importante.
2. Tranziția limitată sau imposibilă, a sistemelor dezvoltate pe tehnologii învechite, către Centrul de date al STISC.
3. O mare varietate de tehnologii utilizate în trecut pentru a crea sisteme de aplicații, neactualizate și potențial vulnerabile la amenințări cibernetice.

Beneficiile exploatării unei infrastructuri TIC și a unei platforme de aplicații standardizate se vor concretiza prin reducerea riscurilor operaționale, a capacității de gestionare, a agilității și a pregătirii pentru schimbări, a costurilor de întreținere și operaționale, a posibilității de a se axa pe dezvoltarea de servicii complementare (non-core), asigurarea calității datelor și multe altele.

Guvernanța și gestionarea IT, inclusiv securitatea cibernetică, sunt delegate în mare măsură unui organism competent, dar extern, și anume IP CTIF.

Servicii pentru contribuabili:

SFS, ca instituție publică, nu poate funcționa izolată de publicul său, publicul care îi conferă, întrucâtva, legitimitate. Pentru a primi un răspuns favorabil din partea persoanelor pentru care desfășoară activități, trebuie să-și exprime intențiile, să-și creeze o imagine solidă și să se supună unui imperativ: de a se apropia de public prin adaptarea structurii organizaționale la cerințele și/sau așteptările acestuia.

Acest lucru se realizează prin intermediul canalelor existente de comunicare: pagina web oficială www.sfs.md, paginile de pe rețele de socializare (Facebook, Instagram, LikedIn, Telegram), canalul de Youtube, modulul „Mesagerie” din cadrul SIA „Cabinetul personal al contribuabilului”, seminare de instruire, ședințe cu mediul de afaceri/grupuri de contabili, etc.

Formarea opiniei publice pentru dezvoltarea unei conștiințe fiscale reprezintă o sarcină pe care organizația fiscală și-a asumat-o și va continua să o dezvolte în viitor.

3.2. Lacune tehnologice și nevoi de modernizare

SFS din Republica Moldova se confruntă cu o serie de lacune tehnologice care împiedică optimizarea activităților sale și eficiența în administrarea fiscală. Identificarea acestor lacune este necesară

pentru dezvoltarea unui plan de modernizare bine structurat, care să permită alinierea infrastructurii IT la cerințele Uniunii Europene și la standardele moderne de eficiență și securitate.

Multe dintre sistemele IT existente în cadrul SFS sunt construite pe tehnologii învechite, care nu mai răspund nevoilor actuale de procesare și gestionare a datelor. Aceste sisteme nu sunt integrate eficient, ceea ce duce la dificultăți majore în transferul și utilizarea datelor între departamentele interne și între SFS și alte instituții naționale sau internaționale. Lipsa interoperabilității între diferitele sisteme nu permite accesul eficient și rapid la informații esențiale, ceea ce afectează negativ procesele administrative și de audit.

Volumul de date gestionat de SFS crește continuu, însă capacitatea de stocare și procesare a datelor rămâne limitată. În lipsa unor soluții moderne de cloud computing și de virtualizare a resurselor, SFS se confruntă cu probleme legate de supraîncărcarea serverelor și de eficiența scăzută a procesării datelor. Această limitare îngreunează analiza datelor și implementarea de soluții avansate de monitorizare a riscurilor fiscale sau de predicție a comportamentului contribuabililor.

Securitatea cibernetică reprezintă un domeniu important în care SFS are nevoie de îmbunătățiri semnificative. Infrastructura actuală nu este pregătită să facă față provocărilor moderne legate de atacurile cibernetice, iar măsurile de protecție existente sunt insuficiente. Sistemele actuale nu beneficiază de protecție avansată împotriva intruziunilor (cum ar fi IDS/IPS), iar lipsa criptării avansate pentru comunicarea datelor sensibile expune organizația unor riscuri semnificative. În plus, procesele de gestionare a incidentelor de securitate nu sunt bine definite, ceea ce crește vulnerabilitatea la atacuri și la scurgerile de informații.

O altă lacună majoră o reprezintă lipsa unei automatizări extinse a proceselor fiscale. În multe cazuri, contribuabilii și personalul SFS trebuie să gestioneze manual procese care ar putea fi automatizate cu ajutorul tehnologiei moderne. Această dependență de proceduri manuale îngreunează activitatea, reduce eficiența și crește riscul de erori umane. Automatizarea proceselor, precum validarea și verificarea declarațiilor fiscale, ar putea reduce semnificativ sarcinile administrative și ar îmbunătăți colectarea și conformitatea fiscală.

Pentru a răspunde acestor provocări, SFS trebuie să investească în modernizarea infrastructurii sale IT. Acest lucru presupune:

- Implementarea soluțiilor de cloud computing pentru scalabilitate și acces rapid la resursele de stocare și procesare.
- Virtualizarea resurselor IT pentru a crește eficiența utilizării serverelor și pentru a reduce costurile de întreținere a echipamentelor fizice.
- Dezvoltarea unui sistem de guvernanță a datelor, care să includă proceduri clare pentru colectarea, validarea și stocarea datelor fiscale, asigurând astfel calitatea și securitatea informațiilor.
- Îmbunătățirea securității cibernetice prin implementarea de măsuri avansate de protecție, inclusiv criptare, detectarea și prevenirea intruziunilor, precum și protocoale clare de gestionare a incidentelor.
- Automatizarea proceselor fiscale pentru a reduce volumul de muncă manuală și pentru a asigura eficiența în administrarea taxelor și impozitelor.

- Aceste lacune tehnologice indică necesitatea unui plan de modernizare amplu, care să transforme SFS într-o instituție fiscală modernă, capabilă să gestioneze eficient datele și să ofere servicii digitale contribuabililor, în conformitate cu cerințele Uniunii Europene.

3.3. Evaluarea riscurilor actuale și necesitățile de integrare cu UE

Evaluarea riscurilor actuale la SFS relevă o serie de vulnerabilități tehnologice și administrative care necesită o abordare strategică pentru a asigura o tranziție eficientă către cerințele impuse de integrarea cu Uniunea Europeană. Aceste riscuri sunt direct legate de starea actuală a infrastructurii IT, fragmentarea sistemelor și lipsa unui cadru clar de guvernanță a datelor, care împiedică o gestionare eficientă și sigură a informațiilor fiscale. Fără o modernizare semnificativă și o consolidare a resurselor, SFS riscă să rămână în urmă în procesul de aliniere la standardele europene.

Un prim risc major identificat este securitatea cibernetică deficitară, care expune infrastructura IT a SFS la atacuri cibernetice și scurgeri de informații sensibile. În contextul cerințelor stricte de protecție a datelor impuse de Uniunea Europeană, securitatea cibernetică reprezintă o prioritate absolută. În absența unor soluții avansate, cum ar fi criptarea end-to-end, sistemele de detectare și prevenire a intruziunilor (IDS/IPS) și protocoalele clare de gestionare a incidentelor, SFS nu poate asigura integritatea și confidențialitatea datelor fiscale gestionate. Această vulnerabilitate nu doar că amenință securitatea operațională a organizației, dar poate compromite și încrederea contribuabililor, esențială pentru eficiența administrării fiscale.

Un alt risc important este fragmentarea sistemelor IT, care afectează interoperabilitatea și schimbul rapid de informații. Pentru a se alinia cu cerințele europene, SFS trebuie să își îmbunătățească capacitatea de a integra și utiliza datele la nivel național și internațional. Lipsa de interoperabilitate între sistemele interne și cele externe limitează accesul la informații și împiedică schimburile rapide de date fiscale între Republica Moldova și statele membre ale Uniunii Europene. Această problemă devine mai critică în contextul unor platforme esențiale, precum VIES (VAT Information Exchange System) și OSS (One Stop Shop), care impun integrarea rapidă și fără erori a datelor fiscale transfrontaliere.

Un al treilea risc semnificativ este dependența de procese manuale și lipsa automatizării în procesele fiscale. Aceste deficiențe nu doar că încetinesc operațiunile, dar și cresc riscul de erori umane și reduc eficiența colectării fiscale. Automatizarea proceselor este o cerință majoră pentru conformitatea cu reglementările europene, mai ales în contextul schimburilor de informații automate și al raportărilor fiscale. Fără o integrare completă a soluțiilor digitale, SFS nu va putea răspunde cerințelor de eficiență și transparență fiscală impuse de Uniunea Europeană.

Lipsa unui cadru formal de guvernanță a datelor este un alt factor care agravează riscurile actuale. Standardele europene cer o gestionare riguroasă a datelor, care să asigure calitatea, securitatea și integritatea acestora. Fără un sistem formalizat de guvernanță a datelor, SFS riscă să gestioneze date incomplete, redundante sau inaccesibile, ceea ce afectează deciziile strategice și operaționale. Integrarea cu UE necesită un management coerent al datelor, care să permită accesul rapid și sigur la informații fiscale de înaltă calitate, pentru schimburile transfrontaliere.

Necesarul de modernizare devine evident în contextul acestor riscuri. Pentru a se alinia cerințelor Uniunii Europene, SFS trebuie să investească urgent în tehnologii moderne, să îmbunătățească securitatea cibernetică, să automatizeze procesele fiscale și să implementeze un cadru robust de

guvernanță a datelor. În caz contrar, există riscul de a nu respecta termenele impuse de procesul de integrare și de a rămâne în urmă în ceea ce privește eficiența și transparența fiscală, necesare pentru aderarea la Uniunea Europeană.

Astfel, evaluarea riscurilor actuale scoate în evidență nevoia strigentă de modernizare și integrare. Alinierea la standardele europene nu doar că va îmbunătăți eficiența operațională a SFS, dar va asigura și conformitatea cu reglementările europene, consolidând încrederea în sistemul fiscal și facilitând procesul de aderare la Uniunea Europeană.

4. Obiective generale

Această secțiune stabilește obiectivele specifice pe termen mediu, precum și măsuri/mecanisme pentru atingerea acestor obiective. În plus, stabilește indicatori de performanță și monitorizează progresul așteptat al SFS, rezultatele și efectul financiar, precum și prioritățile pentru fiecare fază a implementării Cartei în sine.

Obiectiv general nr.1 Creșterea capacității de analiză a datelor mari

Realizarea acestui obiectiv general se va asigura prin următoarele direcții prioritare:

1) Înființarea unui cadru de guvernanță a datelor cuprinzător pentru a asigura calitatea, securitatea și confidențialitatea datelor.
2) Implementarea instrumentelor de analiză și de business intelligence pentru luarea deciziilor bazate pe date, inclusiv prin valorificarea posibilitățile tehnice ale inteligenței artificiale.
3) Asigurarea îmbunătățirii continue în calitatea datelor, în abundența și disponibilitatea acestora.
4) Concentrarea pe identificarea și cuantificarea conformității și altor riscuri.
5) Dezvoltarea capacității de cercetare în analiza avansată a datelor în colaborare cu universitățile și instituțiile de cercetare.

Indicatori

1) Crearea unei subdiviziuni de business intelligence (BI).
2) Instruirea angajaților din cadrul subdiviziunii BI.
3) Elaborarea și aprobarea politicii de guvernanță a datelor și de calitate a acestora.
4) Elaborarea și aprobarea glosarului și a dicționarului de date.
5) Dezvoltarea arhitecturii inițiale DataLake.
6) Conectarea surselor de date la DataLake.
7) Numirea unui ofițer de date.
8) Extinderea volumului de date prin implementarea noilor schimburi de informații utilizând platforma guvernamentală MConnect.
9) Stabilirea parteneriatelor cu universități care dețin expertiză în domeniul matematicii și statisticii pentru dezvoltarea abordărilor bazate pe riscuri, inclusiv identificarea riscurilor asociate contribuabililor, auditului și fraudei, pe baza datelor colectate. Un indicator specific al acestui obiectiv va fi aplicarea și implementarea instrumentelor de analiză a datelor bazate pe inteligență artificială în procesul de evaluare a riscurilor.

Obiectiv general nr.2 Consolidarea și dezvoltarea competențelor de guvernanță și securitate IT internă

Realizarea acestui obiectiv general se va asigura prin următoarele direcții prioritare:

1) Consolidarea capacității TIC, arhitectură și management prin consolidarea operațiunilor și a cunoștințelor IT în cadrul SFS.
2) Implementarea cadrelor de guvernanță IT pentru alinierea inițiativelor tehnologice cu obiectivele organizaționale.

Indicatori

1) Dezvoltarea competențelor profesionale pentru implementarea serviciilor IT.
2) Instituirea unui mecanism de control ce va monitoriza implementarea cerințelor TIC.
3) Minimizarea dependenței de un singur furnizor (IP CTIF).

Obiectiv general nr.3 Securitatea IT și protecția datelor

Realizarea acestui obiectiv general se va asigura prin următoarele direcții prioritare:

1) Centrarea agendei de securitate cibernetică în cadrul SFS.
2) Consolidarea măsurilor de securitate cibernetică și de reziliență cibernetică.
3) Asigurarea conformității documentației aferente procesului în conformitate cu regulamentele și standardele de protecție a datelor.
4) Asigurarea unei infrastructuri ICT rezistentă, scalabilă și securizată.

Indicatori

1) Desemnarea unui Ofițer principal de securitate a informațiilor în cadrul SFS.
2) Definirea politicii de securitate cibernetică a SFS.
3) Implementarea măsurilor de monitorizare a securității, control al accesului, gestionare a conturilor privilegiate, monitorizare a vulnerabilităților, jurnale de audit, securitate a logicii de afaceri (piste de auditare), etc. (Implementare recomandată bazată pe Controalele CIS versiunea 8[1]).
4) Desfășurarea misiunilor de auditori IT.
5) Migrarea tuturor sistemelor informaționale pe platforma guvernamentală MCloud[2].

Obiectiv general nr.4 Servicii digitale centrate pe utilizator

Realizarea acestui obiectiv general se va asigura prin următoarele direcții prioritare:

1) Îmbunătățirea experienței utilizatorului prin dezvoltarea unor platforme online intuitive și opțiuni de autoservire, precum ghiduri automate și instrumente de verificare online a autenticității și statutului certificatelor emise de SFS. Ca indicator, se va urmări integrarea codurilor QR sau a altor elemente de identificare electronică în certificatele emise contribuabililor.

Indicatori

1) Utilizarea feedback-ului din partea contribuabililor pentru îmbunătățirea continuă a serviciilor și platformelor IT.
2) Implementarea funcționalităților rapide și prietenoase pentru utilizator, prin utilizarea declarațiilor precompletate.

Obiectiv general nr.5 Reflectarea instantă în SISFS obligațiilor fiscale ale contribuabililor

[1] https://www.cisecurity.org/controls/v8

[2] art.4 alin.(2) din HG nr.128 din 20.02.2014 privind platforma tehnologică guvernamentală comună (MCloud), Ministerele, Cancelaria de Stat, alte autorități administrative centrale subordonate Guvernului și autoritățile/instituțiile publice din sfera lor de competență, precum și entitățile publice indicate în anexa nr.2, vor găzdui sistemele informaționale existente și cele noi pe platforma tehnologică guvernamentală comună (MCloud), cu excepția cazurilor expres prevăzute în actele normative

Realizarea acestui obiectiv general se va asigura prin următoarele direcții prioritare:

1) Ajustarea proceselor core de procesare a dărilor de seamă fiscale și a notelor de plată ca să se reflecte instant sumele obligațiilor calculate și achitate.
2) Precompletarea declarațiilor privind impozitul pe venit pentru persoanele juridice și fizice care desfășoară activități de antreprenoriat urmează a fi ajustată pentru a permite procesarea automată în cadrul Sistemului Informațional al Serviciului Fiscal de Stat (SISFS), în conformitate cu standardele UE, asigurând astfel un proces fiscal digitalizat și eficient.

Indicatori

1) Reducerea timpului de procesare a dărilor de seamă fiscale la zero sau la o perioadă minimă acceptabilă, care să permită actualizarea instantanee a informațiilor.
2) Reducerea timpului de procesare a plăților către bugetul public național la zero sau la o perioadă minimă acceptabilă, astfel încât plățile să fie reflectate instantaneu în conturile contribuabililor.
3) Dezvoltarea și implementarea unui sistem informațional automatizat care să permită procesarea instantanee a dărilor de seamă fiscale și a plăților, eliminând necesitatea unei intervenții manuale și reducând riscul de erori.

4.1. Proceduri de monitorizare și raportare

Transformarea digitală este un proces de învățare socială, susținut în timp și care implică diverse părți interesate (funcționari fiscali, contribuabili, alte autorități publice).

Procesul de monitorizare a implementării Strategiei va fi organizat printr-un set de indicatori de monitorizare și evaluare a acțiunilor planificate, prin care se măsoară gradul de implementare a Cartei și prin care se stabilește nivelul de realizare a obiectivelor.

Indicatorii de rezultat vor cuantifica efectele imediate și pe termen mediu produse de implementarea Cartei asupra diferitor grupuri-țintă.

Indicatori de monitorizare și evaluare

Nr. crt.	Obiective generale	Indicatori	Valori de referință (2024)	Ținte pentru 2025	Ținte pentru 2027	Subdiviziunile responsabile
1	**Creșterea capacității de analiză a datelor mari**	1.1 Crearea unei subdiviziuni de business intelligence (BI)	0	1 subdiviziune nou creată, componența 3 angajați	3 noi angajați	DMRU
		1.2 Instruirea periodică a angajaților din cadrul subdiviziunii	0	0	2 instruiri desfășurate	DMRU DEF DOMIP

Nr. crt.	Obiective generale	Indicatori	Valori de referință (2024)	Ținte pentru 2025	Ținte pentru 2027	Subdiviziunile responsabile
		BI pentru dezvoltarea competențelor				
		1.3 Elaborarea și aprobarea politicii de guvernanță a datelor și de calitate a acestora	1 act intern elaborat și aprobat	1 act intern revizuit	1 act intern revizuit	DDI
		1.4 Elaborarea și aprobarea glosarului și a dicționarului de date	0	1 act intern elaborat și aprobat	1 act intern revizuit	DDI
		1.5 Dezvoltarea arhitecturii inițiale DataLake	0	1 arhitectură dezvoltată	0	DDI (IP CTIF)
		1.6 Conectarea surselor de date la DataLake	0	Surse de date conectate 50%	Surse de date conectate 100%	DDI (IP CTIF)
		1.7 Numirea unui ofițer de date	1 act intern elaborat și aprobat	1 act intern revizuit	1 act intern revizuit	DSIA
		1.8 Creșterea diversității datelor prin realizarea noilor schimburi de date prin intermediul platformei guvernamentale MConnect	3 Anexe tehnice aprobate	5 Anexe tehnice aprobate	7 Anexe tehnice aprobate	DDI (IP CTIF) DGMIT DEIF DGConformare
		1.9 Identificarea și acordul cu parteneriatele cu universitățile capabile să ofere capacități de cunoștințe matematice, statistice pentru elaborarea abordărilor bazate pe riscuri (identificarea riscului contribuabililor, identificarea riscului de audit, identificarea și gestionarea fraudei pe baza datelor colectate)	0	1 acord semnat	1 acord semnat	DMRU
2	**Consolidarea și dezvoltarea competențelor de guvernanță și**	2.1 Dezvoltarea competențelor profesionale ale angajaților din cadrul DDI pentru	2 instruiri desfășurate	2 instruiri desfășurate	2 instruiri desfășurate	DMRU DEF DOMIP

Nr. crt.	Obiective generale	Indicatori	Valori de referință (2024)	Ținte pentru 2025	Ținte pentru 2027	Subdiviziunile responsabile
	securitate IT internă	implementarea serviciilor IT				
		2.2 Instituirea unui mecanism de control ce va monitoriza implementarea cerințelor TIC	0	1 sistem identificat	1 sistem implementat	DDI
		2.3 Minimizarea dependenței de un singur furnizor (IP CTIF)	Act legislativ înaintat spre consultare publică	Act legislativ aprobat	4 noi furnizori	DGEJ
3	**Securitatea IT și protecția datelor**	3.1 Desemnarea unui Ofițer principal de securitate a informațiilor în cadrul SFS	1 act intern elaborat și aprobat	1 act intern revizuit	1 act intern revizuit	DSIA
		3.2 Definirea politicii de securitate cibernetică a SFS	1 act intern elaborat și aprobat	1 act intern revizuit	1 act intern revizuit	DSIA
		3.3 Implementarea măsurilor de monitorizare a securității, control al accesului, gestionare a conturilor privilegiate, monitorizare a vulnerabilităților, jurnale de audit, securitate a logicii de afaceri (piste de auditare), etc. (Implementare recomandată bazată pe Controalele CIS versiunea 8, 3 grupuri de implementare a măsurilor de protecție)	1 act intern elaborat și aprobat	2 instruiri desfășurate	2 instruiri desfășurate	DSIA DMRU
		3.4 Desfășurarea misiunilor de audit sau a verificărilor aferent securității IT, protecția datelor și accesul la informații din SISFS	1 misiune de audit sau verificată realizată	1 misiune de audit sau verificată realizată	1 misiune de audit sau verificată realizată	DAI
		3.5 Migrarea tuturor sistemelor	50% sisteme migrate	70% sisteme migrate	100% sisteme migrate	DDI (IP CTIF)

Nr. crt.	Obiective generale	Indicatori	Valori de referință (2024)	Ținte pentru 2025	Ținte pentru 2027	Subdiviziunile responsabile
		informaționale pe platforma guvernamentală MCloud				
4	**Servicii digitale centrate pe utilizator**	4.1 Utilizarea feedback-ului din partea contribuabililor pentru îmbunătățirea continuă a serviciilor și platformelor IT	1 sondaj de opinie efectuat	1 sondaj de opinie efectuat	1 sondaj de opinie efectuat	DDI SC
		4.2 Implementarea funcționalităților rapide și prietenoase pentru utilizator, prin utilizarea declarațiilor precompletate		2 declarații noi precompletate	2 declarații noi precompletate	DGMIT
5	**Reflectarea instantă în SISFS obligațiilor fiscale ale contribuabililor**	5.1 Reducerea timpului de procesare a dărilor de seamă fiscale la zero sau la o perioadă minimă acceptabilă, care să permită actualizarea instantanee a informațiilor.	Concept aprobat		1 proces optimizat	DDI (IP CTIF) DEIF
		5.2 Reducerea timpului de procesare a plăților către bugetul public național la zero sau la o perioadă minimă acceptabilă, astfel încât plățile să fie reflectate instantaneu în conturile contribuabililor.	Concept aprobat		1 proces optimizat	DDI (IP CTIF) DEIF
		5.3 Dezvoltarea și implementarea unui sistem informațional automatizat care să permită procesarea instantanee a dărilor de seamă fiscale și a plăților, eliminând necesitatea unei intervenții manuale și reducând riscul de erori	Concept aprobat		1 sistem informațional dezvoltat	DDI (IP CTIF) DEIF

4.2. Integrarea cu sistemele informaţionale europene

Integrarea Republicii Moldova în Uniunea Europeană reprezintă un obiectiv strategic de importanță națională, implicând transformări semnificative în multiple sectoare. Un element esențial al acestui proces îl constituie alinierea și integrarea în sistemele informaționale europene. Această strategie IT națională își propune să stabilească direcțiile și acțiunile necesare pentru a asigura interoperabilitatea, securitatea și eficiența schimbului de informații cu statele membre ale UE, contribuind astfel la dezvoltarea socio-economică a țării și la creșterea bunăstării cetățenilor.

Obiectivele strategice includ armonizarea cadrului legislativ și normativ, standardizarea și interoperabilitatea tehnologică, consolidarea securității cibernetice, dezvoltarea capitalului uman și a competențelor digitale, modernizarea infrastructurii IT și participarea activă la inițiative și programe europene. Adaptarea legislației naționale la acquis-ul comunitar în domeniul tehnologiei informației și comunicațiilor va crea un mediu legal propice integrării în sistemele informaționale ale UE. Este imperativă adoptarea și implementarea integrală a Regulamentului General privind Protecția Datelor (GDPR) pentru a asigura un nivel înalt de protecție a datelor și a facilita schimbul de informații cu statele membre. De asemenea, implementarea Directivei NIS și elaborarea unei strategii naționale de securitate cibernetică sunt cruciale pentru a răspunde provocărilor actuale în materie de securitate.

Asigurarea compatibilității tehnice cu sistemele europene se va realiza prin adoptarea standardelor și specificațiilor tehnice recunoscute la nivelul UE. Implementarea protocoalelor și a formatelor de date standardizate va facilita interoperabilitatea sistemelor și va permite un schimb de informații eficient și securizat. Obținerea certificărilor necesare pentru infrastructurile și serviciile IT, conform standardelor și normelor europene, va garanta calitatea și fiabilitatea acestora.

Dezvoltarea unui cadru robust de securitate cibernetică este esențială pentru protejarea infrastructurii IT naționale și asigurarea rezilienței în fața amenințărilor cibernetice. Aceasta implică stabilirea unui cadru legislativ și operațional care să includă politici, proceduri și mecanisme de răspuns la incidente cibernetice. Participarea la rețele și inițiative europene în domeniul securității cibernetice și colaborarea cu agenții precum ENISA vor întări capacitatea de a face față provocărilor transfrontaliere. Identificarea și securizarea infrastructurilor IT critice sunt, de asemenea, priorități pentru asigurarea funcționării continue a societății și economiei.

Investiția în educație și formare profesională este vitală pentru dezvoltarea capitalului uman și a competențelor digitale. Integrarea competențelor digitale în curricula educațională și promovarea programelor de formare continuă pentru specialiști IT vor contribui la crearea unei forțe de muncă calificate. Facilitarea participării la programe de schimb și cooperare cu instituții de învățământ și organizații din UE va încuraja transferul de cunoștințe și bune practici.

Modernizarea infrastructurii tehnologice este necesară pentru a satisface cerințele de performanță și scalabilitate impuse de integrarea europeană. Alocarea de resurse pentru modernizarea rețelelor de comunicații, a centrelor de date și a infrastructurilor cloud va asigura capacitatea tehnică necesară. Adoptarea tehnologiilor emergente, precum inteligența artificială, big data și Internet of Things (IoT), va stimula inovația și va spori competitivitatea economică.

Participarea activă la inițiative și programe europene oferă oportunități de dezvoltare și acces la resurse, expertiză și finanțare în domeniul digitalizării. Accesarea fondurilor disponibile prin programe precum Europa Digitală și Horizon Europe va sprijini implementarea proiectelor

strategice. Stabilirea de parteneriate cu entități publice și private din UE va facilita implementarea proiectelor comune și va consolida relațiile internaționale.

Implementarea strategiei va fi coordonată de un comitet interministerial responsabil cu supravegherea progresului și asigurarea coerenței între diferitele domenii de acțiune. Se vor stabili indicatori de performanță cheie pentru a monitoriza eficient evoluția și pentru a ajusta măsurile, dacă este necesar. Raportarea periodică și transparentă către Guvern și public va asigura responsabilitatea și implicarea tuturor părților interesate.

În acest sens, urmează să fie asigurată interoperabilitatea cu următoarele sisteme/aplicaţii:

- **TVA**
    - **VIES – VAT Information Exchange System**
      VIES (Sistemul de Schimb de Informații privind TVA) este un sistem electronic al Uniunii Europene care permite verificarea numerelor de înregistrare în scopuri de TVA ale companiilor înregistrate în statele membre. Acesta facilitează schimbul de informații privind TVA între autoritățile fiscale ale țărilor UE pentru a combate frauda fiscală și a asigura conformitatea.
    - **OSS – One Stop Shop**
      OSS (Punct Unic de Contact) este un sistem implementat de UE pentru a simplifica obligațiile de TVA ale companiilor care furnizează servicii și bunuri transfrontaliere. Prin OSS, companiile pot declara și plăti TVA într-un singur stat membru, evitând necesitatea de a se înregistra fiscal în fiecare țară în care au clienți.
    - **CESOP – Central electronic system on payment information**
      CESOP (Sistemul Electronic Central privind Informațiile de Plată) este o platformă centralizată creată de UE pentru colectarea și schimbul de informații privind plățile transfrontaliere. Scopul principal al CESOP este de a combate frauda în domeniul TVA, în special în contextul comerțului electronic, prin monitorizarea fluxurilor financiare între statele membre.
    - **ViDA – Vat in the digital age**
      ViDA (TVA în Epoca Digitală) este o inițiativă a Uniunii Europene care vizează modernizarea sistemului de TVA pentru a se adapta provocărilor și oportunităților aduse de economia digitală. Aceasta include propuneri legislative și măsuri menite să îmbunătățească colectarea TVA și să reducă frauda fiscală în contextul comerțului electronic și al serviciilor digitale.
    - **Alte sisteme ()**

- **Accize**
    - EMCS – Excise movement and control system

Pe lângă sistemele informaționale ale UE, la care autoritatea competentă din Republica Moldova urmează să se conecteze la platformele de conectare, este necesar de implementat următoarele schimburi de date:

- DAC1 (Standard Transmission Format) - stabilește cadrul general pentru cooperarea administrativă în domeniul fiscal și prevede schimbul de informații la cerere, facilitând investigarea cazurilor specifice de evaziune fiscală.
- DAC2 (Common reporting standard) - Introduce schimbul automat de informații privind conturile financiare ale nerezidenților, conform Standardului Comun de Raportare (CRS) al OCDE, permițând depistarea veniturilor ascunse în străinătate.
- DAC3 (Exchange of tax rulings) - Prevede schimbul automat de informații referitoare la deciziile fiscale anticipate și acordurile de preț în avans, sporind transparența în practicile fiscale ale companiilor multinaționale.
- DAC4 (Country by country reporting) - Introduce raportarea țară cu țară pentru grupurile multinaționale, oferind autorităților fiscale o imagine de ansamblu asupra distribuției profiturilor și impozitelor plătite.
- DAC5 (beneficial ownership information as collected under Anti-Money Laundering rules (AML)) - Extinde accesul autorităților fiscale la informațiile privind beneficiarii reali ai entităților juridice, contribuind la combaterea spălării banilor și a finanțării terorismului.
- DAC6 (Cross-border tax arrangements) - Impune intermediarilor fiscali obligația de a raporta aranjamentele fiscale transfrontaliere care prezintă semne distinctive de planificare fiscală agresivă, prevenind astfel evitarea obligațiilor fiscale.
- DAC7 (Model Reporting for Digital Platforms) - Extinde schimbul automat de informații la platformele digitale, obligând operatorii să raporteze veniturile obținute de vânzători și prestatorii de servicii, abordând provocările economiei digitale.
- DAC8 (Crypto Asset Reporting Framework) - Include cripto-activele și monedele electronice în sfera de aplicare a schimbului automat de informații, prevenind utilizarea acestora în scopuri de evaziune fiscală și spălare de bani.
- DAC9 (Global Anti-Base Erosion Model Rules) - Vizează îmbunătățirea și actualizarea cadrului existent de cooperare administrativă, sporind eficiența și eficacitatea schimbului de informații fiscale între statele membre.

Întru realizarea schimburilor de date cu UE, utilizînd aplicaţii, sistemle şi prin intermediul Directivelor UE, este necesar de conectat la platforme de comunicare, inclusiv

- CCN/CSI – Common Communication Network/Common System Interface. Care este o infrastructură securizată destinată schimbului de informații între administrațiile naționale și instituțiile Uniunii Europene, în special în domeniile vamal și fiscal. CCN/CSI facilitează interoperabilitatea între diferitele sisteme informatice ale statelor membre, permițând un flux eficient și securizat de date.

  Acesta asigură fluxul de date pentru următoarele sisteme:
  - VIES - VAT Information Exchange System
  - OSS – One Stop Shop
  - DAC1
  - DAC2
  - DAC4
  - altele

- CCN Mail, care este un serviciu de mesagerie electronică securizată integrat în cadrul CCN/CSI. Acesta permite transmiterea de mesaje și documente sensibile între autoritățile naționale și instituțiile europene, asigurând confidențialitatea și integritatea informațiilor schimbate. CCN Mail este esențial pentru comunicarea rapidă și sigură în cadrul Uniunii Europene

  Acesta asigură fluxul de date pentru următoarele sisteme:
  - EOIR (Exchange of information on request)
- CCN2 - Common Communication Network (v.2), reprezintă evoluția de nouă generație a infrastructurii CCN. Această versiune îmbunătățită oferă performanțe superioare, scalabilitate și securitate sporită, răspunzând cerințelor crescute de comunicare și integrare ale statelor membre și ale instituțiilor UE. CCN2 suportă un număr mai mare de aplicații și servicii, facilitând o cooperare și mai strânsă la nivel europea

  Acesta asigură fluxul de date pentru următoarele sisteme:
  - SME (Small and medium-sized enterprises)
  - altele
- eDelivery, care este o inițiativă a Comisiei Europene care furnizează specificații tehnice și standarde pentru schimbul securizat și fiabil de date între administrațiile publice, companii și cetățeni. Bazându-se pe un model descentralizat și pe standarde deschise, eDelivery asigură interoperabilitatea și compatibilitatea între diferitele sisteme și platforme la nivel european, facilitând comunicarea transfrontalieră.

  Acesta asigură fluxul de date pentru următoarele sisteme:
  - CESOP – System on Payment Data
  - altele
- Central Directory, care este un component central al infrastructurii CCN/CSI care stochează informații esențiale despre participanții la rețea, inclusiv date de contact și rutare. Acesta permite gestionarea eficientă a informațiilor despre entitățile conectate, asigurând o comunicare fluentă și securizată între diferitele sisteme și platforme implicate:

  Acesta asigură fluxul de date pentru următoarele sisteme:
  - DAC7
  - altele
- eFCA (Electronic Forms Carrier Application) este o platformă electronică destinată gestionării și schimbului de formulare și documente oficiale în format digital între statele membre și instituțiile UE. Prin intermediul eFCA, se facilitează procesarea rapidă și eficientă a documentelor, reducând sarcinile administrative și îmbunătățind transparența și colaborarea între diferitele entități.

  Acesta asigură fluxul de date pentru următoarele sisteme:
  - EOIR (Exchange of information on request)
  - altele

5. Modernizarea infrastructurii IT și de comunicații

5.1. Extinderea și modernizarea centrului de date (Data Centru)

Pentru a face față cerințelor moderne, centrul de date al SFS trebuie extins și modernizat. Echipamentele existente sunt învechite, iar volumul de date gestionat crește constant. Prin urmare, se propune achiziția de servere noi și soluții moderne de stocare, precum și implementarea de tehnologii de redundanță și backup (*Tabelul 1*).

Tabelul 1. Specificații tehnice recomandate pentru centrul de date

Nr.	Echipament	Specificații	Cantitate	Cost aproximativ (EUR)
1	Servere rackmount	Procesor 40 nuclee, 768 GB RAM, SSD 2 TB	10	400000
2	Storage SAN/NAS	100 TB SSD, conectivitate Fiber Channel 16 Gbps	2	200000
3	Switchuri de rețea	48 porturi 10 Gbps	4	80000
4	UPS (alimentare de rezervă)	Putere 60 kVA	2	50000
5	Sisteme de climatizare	Sisteme HVAC pentru centre de date	2	30000
6	Software de gestionare	Software de monitorizare și management IT	-	20000
-	**Total**			**780000**

5.2. Optimizarea infrastructurii serverelor și soluțiilor eficiente de virtualizare

Virtualizarea infrastructurii IT va permite SFS să utilizeze mai eficient resursele disponibile și să reducă costurile operaționale. Soluțiile de virtualizare, cum ar fi VMware sau Hyper-V, vor asigura scalabilitatea și flexibilitatea infrastructurii, permițând gestionarea mai eficientă a cerințelor variabile ale utilizatorilor și aplicațiilor fiscale (*Tabelul 2*).

Tabelul 2. Specificații tehnice recomandate pentru virtualizare

Nr.	Echipament	Specificații	Cantitate	Cost aproximativ (EUR)
1	Servere de virtualizare	4 x CPU 32 nuclee, 1.5 TB RAM, 25 Gbps Ethernet	15	1500000

Nr.	Echipament	Specificații	Cantitate	Cost aproximativ (EUR)
2	Licențe VMware/Hyper-V	Licențe pentru 400 mașini virtuale	-	200000
3	Storage virtualizat	500 TB stocare dedicată pentru mașini virtuale	2	500000
4	Software de management	Monitorizare și management resurse virtuale	-	50000
-	**Total**			**2250000**

6. Securitatea Cibernetică și Informațională

6.1. Implementarea sistemului de management al securității informaționale (SIEM)

Implementarea unui sistem integrat de management al securității informaționale (SIEM) este necesară pentru consolidarea securității cibernetice la nivel național, asigurând o monitorizare proactivă și detectarea rapidă a amenințărilor. SIEM va oferi capabilități avansate de colectare, analiză și corelare a datelor din diverse surse pentru a preveni, detecta și răspunde incidentelor de securitate într-un mod eficient și coordonat.

În contextul amenințărilor cibernetice tot mai sofisticate și a volumului din ce în ce mai mare de date critice gestionate la nivel național, implementarea unui SIEM devine foarte importantă pentru a monitoriza în timp real infrastructurile IT esențiale. Acest sistem va permite detectarea și gestionarea incidentelor de securitate înainte ca acestea să provoace daune majore, asigurând astfel continuitatea operațiunilor și protecția datelor sensibile.

Funcționalități de bază ale SIEM:

- **Colectarea centralizată a datelor** – SIEM va agrega în mod automat evenimentele și jurnalele de la diverse componente IT (servere, rețele, aplicații) și sisteme de securitate (firewall, IDS/IPS, DLP), facilitând monitorizarea centralizată și integrată a întregii infrastructuri.
- **Analiza în timp real** – SIEM va analiza evenimentele în timp real, detectând comportamente anormale și generând alerte pentru incidentele de securitate. Această capacitate va permite o reacție rapidă la posibilele amenințări, reducând timpul de răspuns și impactul asupra sistemelor.
- **Corelarea datelor** – Sistemul va corela date din surse multiple pentru a identifica tipare de atac complexe, care nu ar fi evidente prin monitorizarea individuală a componentelor. Astfel, va îmbunătăți capacitatea de a detecta atacuri avansate, cum ar fi atacurile cu persistență avansată (APT).
- **Rapoarte și auditare** – SIEM va genera rapoarte detaliate pentru a satisface cerințele de conformitate cu standardele naționale și internaționale de securitate (ex. GDPR, ISO 27001). Aceste rapoarte vor oferi o imagine clară asupra stării securității infrastructurii și a incidentelor gestionate.
- **Automatizarea răspunsului la incidente** – SIEM va permite automatizarea unor acțiuni de răspuns la incidente, precum izolarea rețelelor compromise, blocarea adreselor IP suspecte și declanșarea măsurilor de protecție suplimentare. Automatizarea va accelera procesele de răspuns și va minimiza erorile umane.

Implementarea soluției SIEM se propune a fi realizată în următoarele 4 etape:

- **Evaluarea infrastructurii existente**. Se va face o analiză detaliată a infrastructurii IT curente pentru a identifica sursele de date relevante pentru SIEM și compatibilitatea acestora cu soluțiile disponibile.

- **Selectarea soluției SIEM**. Va fi organizat un proces de achiziție pentru selectarea soluției SIEM care să îndeplinească cerințele naționale și să se integreze cu infrastructura existentă. Acesta va include o analiză comparativă a opțiunilor disponibile și a costurilor aferente.
- **Implementare pilot**. Implementarea soluției într-un mediu de testare pentru validarea funcționalităților și integrarea sistemelor IT existente.
- **Implementarea completă și extinderea**. După validarea soluției pilot, implementarea va fi extinsă la nivel național în toate instituțiile relevante.

Costurile estimative şi resursele umane necesare a fi implicate întru realizarea soluției SIEM sunt reflectate în *Tabelul 3.*

Tabelul 3. Plan de implementare SIEM

Nr.	Indicator	Termeni de realizare	Resurse umane	Resurse financiare (EUR)
1	Evaluarea infrastructurii existente	3-6 luni	-	
2	Selectarea soluției SIEM	6-9 luni	-	
3	Implementare pilot	9-12 luni	3-4 specialiști în securitate IT	
4	Implementarea completă și extinderea	12-18 luni	Coordonator de proiect, specialiști IT	
5	Licențe software SIEM	-	-	500000
6	Infrastructură hardware	-	-	300000
7	Costuri de implementare și mentenanță	-	Echipa de suport și mentenanță	200000
-	**Total**	**-**	**-**	**1000000**

6.2. Prevenirea scurgerilor de informații (DLP)

Implementarea unei soluții de prevenire a scurgerilor de informații (Data Loss Prevention - DLP) are ca scop protejarea datelor sensibile împotriva accesului neautorizat, scurgerilor accidentale sau intenționate și asigurarea conformității cu reglementările naționale și internaționale privind protecția datelor. Soluția DLP va monitoriza și controla fluxul de date în cadrul infrastructurii IT, prevenind expunerea neautorizată a informațiilor confidențiale.

Într-o lume din ce în ce mai conectată, protejarea datelor sensibile reprezintă o prioritate. Implementarea unui sistem DLP este esențială pentru prevenirea pierderii de informații critice, fie prin canale de comunicare neautorizate, fie prin erori umane. DLP va contribui la asigurarea

conformității cu legislația națională și europeană privind protecția datelor, cum ar fi GDPR, și va ajuta la prevenirea riscurilor asociate scurgerilor de informații.

Funcționalități de bază ale DLP:

- **Monitorizarea fluxurilor de date** – Soluția DLP va monitoriza toate fluxurile de date interne și externe, detectând transferurile neautorizate sau nesecurizate de informații sensibile.
- **Politici de control al accesului** – DLP va permite definirea și implementarea unor politici stricte de control al accesului la date sensibile, prevenind accesul neautorizat la acestea de către utilizatori sau sisteme.
- **Detecția și prevenirea transferurilor de date nesecurizate** – Sistemul va detecta și bloca tentativele de transfer al datelor sensibile prin canale nesigure, cum ar fi e-mailurile necriptate sau transferurile prin dispozitive de stocare externă.
- **Audit și raportare** – Soluția DLP va genera rapoarte detaliate privind incidentele de securitate și tentativele de scurgere de date, permițând efectuarea de audituri periodice și luarea măsurilor necesare pentru a îmbunătăți protecția datelor.
- **Integrare cu alte soluții de securitate** – DLP va fi integrat cu soluțiile existente de securitate, cum ar fi SIEM și firewall-uri, pentru a oferi o protecție completă și a asigura o monitorizare continuă a rețelei și a sistemelor.

Implementarea soluției DLP se propune a fi realizată în următoarele 4 etape:

- **Evaluarea datelor și a riscurilor**. Identificarea tipurilor de date sensibile și a canalelor de transmitere a informațiilor care necesită protecție.
- **Selectarea soluției DLP**. Alegerea soluției care să răspundă cerințelor specifice de securitate și conformitate, pe baza evaluării efectuate.
- **Pilotarea soluției**. Testarea soluției într-un mediu controlat pentru a valida capacitățile de detecție, prevenire și raportare.
- **Implementarea completă**. Integrarea soluției DLP în infrastructura IT națională și asigurarea conformității cu reglementările privind protecția datelor.

Costurile estimative şi resursele umane necesare a fi implicate întru realizarea soluției SIEM sunt reflectate în *Tabelul 4*Tabelul 3.

Tabelul 4. Plan de implementare DLP

Nr.	Indicator	Termeni de realizare	Resurse umane	Resurse financiare (EUR)
1	Evaluarea datelor și a riscurilor	3-6 luni	-	-
2	Selectarea soluției DLP	6-9 luni	-	-
3	Pilotarea soluției	9-12 luni	2-3 specialiști în securitate IT	-

4	Implementarea completă și extinderea	12-18 luni	Coordonator de proiect, specialiști IT	-
5	Licențe software DLP	-	-	300,000
6	Infrastructură hardware	-	-	150,000
7	Costuri de implementare și mentenanță	-	Echipa de suport și mentenanță	100,000
-	Total			**550,000**

6.3. Fortificarea protecției împotriva atacurilor cibernetice (firewall, IDS/IPS)

Fortificarea protecției împotriva atacurilor cibernetice prin implementarea și modernizarea soluțiilor de tip firewall și sisteme de detecție și prevenire a intruziunilor (IDS/IPS) este necesară pentru a proteja infrastructura IT națională de atacuri externe și interne. Soluțiile moderne de firewall și IDS/IPS vor asigura o monitorizare continuă a traficului de rețea, identificând și blocând activitățile rău intenționate înainte ca acestea să producă daune semnificative.

Atacurile cibernetice sunt din ce în ce mai sofisticate, iar protejarea infrastructurii critice necesită soluții avansate de securitate. Implementarea unor soluții de firewall moderne, împreună cu sisteme IDS/IPS, va crește capacitatea de detectare și prevenire a atacurilor cibernetice, asigurând o protecție sporită împotriva amenințărilor. Aceste sisteme vor permite monitorizarea traficului de rețea și detectarea activităților anormale, precum tentativele de acces neautorizat sau exploatarea vulnerabilităților.

Funcționalități de bază ale soluțiilor firewall și IDS/IPS

- **Monitorizarea traficului de rețea** – Soluțiile de firewall și IDS/IPS vor monitoriza constant traficul de rețea, identificând anomalii și încercări de atac, cum ar fi scanările de porturi sau tentativele de atac prin exploatarea vulnerabilităților.
- **Controlul accesului la rețea** – Firewall-ul va controla accesul la rețea, permițând doar traficul legitim și blocând conexiunile suspecte sau neautorizate.
- **Detecția și prevenirea intruziunilor** – IDS/IPS va analiza traficul și va identifica tipare de atacuri cunoscute (atacuri DDoS, exploatarea vulnerabilităților etc.), blocând automat încercările de intruziune și alertând echipa de securitate.
- **Politici de securitate personalizabile** – Soluțiile vor permite definirea unor politici stricte de securitate, adaptate la specificul infrastructurii IT naționale, pentru a preveni accesul neautorizat și a minimiza riscurile.
- **Integrarea cu alte soluții de securitate** – Firewall-ul și IDS/IPS vor fi integrate cu alte soluții de securitate (SIEM, DLP) pentru a asigura o protecție unitară și eficientă a infrastructurii IT, oferind o monitorizare continuă și un răspuns rapid la incidente.

Fortificarea protecției împotriva atacurilor cibernetice se propune a fi realizată în următoarele 4 etape:

- **Evaluarea infrastructurii de rețea și a vulnerabilităților**. Identificarea punctelor vulnerabile și a zonelor critice de rețea care necesită protecție suplimentară.
- **Selectarea soluțiilor firewall și IDS/IPS**. Alegerea soluțiilor care să răspundă cerințelor specifice infrastructurii IT și să asigure protecția necesară împotriva atacurilor cibernetice.
- **Pilotarea soluțiilor în medii controlate**. Testarea soluțiilor firewall și IDS/IPS într-un mediu controlat pentru a valida eficiența acestora în detectarea și prevenirea atacurilor.
- **Implementarea completă și integrarea soluțiilor**. Extinderea implementării la nivel național și integrarea soluțiilor cu sistemele existente de securitate IT pentru a asigura o protecție unitară.

Costurile estimative şi resursele umane necesare a fi implicate întru fortificarea protecției împotriva atacurilor cibernetice în *Tabelul 5*Tabelul 3.

Tabelul 5. Plan de fortificare a protecției împotriva atacurilor cibernetice

Nr.	Indicator	Termeni de realizare	Resurse umane	Resurse financiare (EUR)
1	Evaluarea infrastructurii și a vulnerabilităților	3-6 luni	-	-
2	Selectarea soluțiilor firewall și IDS/IPS	6-9 luni	-	-
3	Pilotarea soluțiilor	9-12 luni	3-4 specialiști în securitate IT	-
4	Implementarea completă și integrarea	12-18 luni	Coordonator de proiect, specialiști în rețea	-
5	Achiziționarea soluțiilor firewall și IDS/IPS	-	-	400,000
6	Infrastructură hardware	-	-	200,000
7	Costuri de implementare și mentenanță	-	Echipa de suport și mentenanță	150,000
-	Total			**750,000**

6.4. Securizarea comunicațiilor și a schimburilor de date

Securizarea comunicațiilor și a schimburilor de date este esențială pentru protejarea integrității și confidențialității informațiilor transmise prin rețele interne și externe. Implementarea unor soluții de criptare end-to-end și utilizarea de rețele private virtuale (VPN) vor garanta că datele sunt protejate împotriva accesului neautorizat pe durata transmisiei și vor asigura conformitatea cu reglementările internaționale de protecție a datelor.

Într-un context digital din ce în ce mai complex, unde schimbul de date între organizații și utilizatori este constant, asigurarea unei comunicații sigure este de o importanță crucială. Criptarea comunicațiilor și utilizarea soluțiilor VPN vor proteja datele sensibile împotriva interceptărilor, asigurând astfel că informațiile rămân confidențiale pe tot parcursul transmisiei. Aceasta este esențială atât pentru asigurarea integrității datelor, cât și pentru respectarea reglementărilor legale.

Funcționalități esențiale ale soluțiilor de securizare a comunicațiilor:

- **Criptarea end-to-end** – Soluțiile de criptare vor proteja datele transmise între punctele finale ale rețelei, asigurând că doar destinatarul autorizat poate accesa informațiile transmise.
- **Utilizarea VPN-urilor securizate** – Rețelele private virtuale (VPN) vor fi utilizate pentru a asigura o conexiune criptată și securizată între dispozitivele utilizatorilor și infrastructura centrală, prevenind interceptarea datelor.
- **Autentificare multifactorială (MFA)** – Pentru a spori securitatea accesului la rețelele de comunicații, va fi implementată autentificarea multifactorială, care va solicita utilizatorilor să furnizeze mai multe forme de verificare a identității înainte de a accesa sistemele.
- **Monitorizarea și controlul schimburilor de date** – Soluțiile de monitorizare vor supraveghea schimburile de date și vor bloca orice încercare de transmitere neautorizată sau nesigură a informațiilor sensibile.
- **Integrarea cu alte soluții de securitate** – Sistemele de criptare și VPN vor fi integrate cu soluțiile existente (firewall, IDS/IPS, SIEM) pentru a oferi o protecție unitară și eficientă a schimburilor de date.

Securizarea comunicațiilor și a schimburilor de date se propune a fi realizată în următoarele 4 etape:

- **Evaluarea cerințelor de securitate a comunicațiilor.** Identificarea tipurilor de comunicații și schimburi de date care necesită protecție și evaluarea soluțiilor disponibile pentru criptare și VPN.
- **Selectarea soluțiilor de criptare și VPN**. Alegerea soluțiilor care să răspundă nevoilor specifice de securitate și să asigure protecția necesară a comunicațiilor.
- **Pilotarea soluțiilor în medii controlate**. Testarea soluțiilor de criptare și VPN într-un mediu controlat pentru a valida eficiența acestora în protejarea comunicațiilor și datelor.
- **Implementarea completă și extinderea soluțiilor**. Implementarea soluțiilor la nivel național și integrarea acestora în infrastructura IT existentă.

Costurile estimative şi resursele umane necesare a fi implicate întru securizarea comunicațiilor și a schimburilor de date în *Tabelul 6*Tabelul 5Tabelul 3.

Tabelul 6, Plan întru securizarea comunicațiilor și a schimburilor de date

Nr.	Indicator	Termeni de realizare	Resurse umane	Resurse financiare (EUR)
1	Evaluarea cerințelor de securitate a comunicațiilor	3-6 luni	-	-

2	Selectarea soluțiilor de criptare și VPN	6-9 luni	-	-
3	Pilotarea soluțiilor	9-12 luni	3-4 specialiști în securitate IT	-
4	Implementarea completă și extinderea soluțiilor	12-18 luni	Coordonator de proiect, specialiști IT	-
5	Licențe software pentru criptare și VPN	-	-	250,000
6	Infrastructură hardware	-	-	150,000
7	Costuri de implementare și mentenanță	-	Echipa de suport și mentenanță	100,000
-	Total			**500,000**

7. Costurile de integrarea cu sistemele informaţioanle și platformele Europene

Integrarea cu sistemele informaționale și platformele europene reprezintă un pas esențial în consolidarea interoperabilității și eficienței serviciilor oferite la nivel național și continental. Aceasta facilitează schimbul de date și informații între diferite instituții și organizații, contribuind la îmbunătățirea cooperării transfrontaliere și la creșterea transparenței în gestionarea proceselor administrative. Prin adoptarea standardelor și tehnologiilor comune, se asigură alinierea la practicile europene, ceea ce permite accesul la resurse și instrumente avansate, precum și participarea activă la inițiativele de dezvoltare digitală în cadrul Uniunii Europene.

Conectarea la sistemele informaționale şi platformele UE se efectuează într-u efectuarea schimburilor de date, inclusiv în baza directivelor DAC1 – DAC9, prin intermediul canalelor de schimb dedicate şi prin intermediul unor aplicaţii puse la dispoziție în modul stabilit de către UE

7.1. Conectarea la platformele europene de schimb de informații (VIES, CESOP, OSS, etc.)

Întru conectarea la sistemele informaționale ale UE se propune următorul plan de acțiune de implementare general (*Tabelul 7*):

Tabelul 7. Plan de implementare general

Nr.	Activitate	Timp de Implementare	Data de Începere	Costuri Aproximative (EUR)
1	Evaluare Internă	2 săptămâni	01.01.2025	1000
2	Planificare și Alocare Resurse	3 săptămâni	15.01.2025	2000
3	Integrare VIES	4 săptămâni	05.02.2025	3000
4	Automatizare Rambursare TVA	6 săptămâni	01.03.2025	4000
5	Înregistrare în OSS	2 săptămâni	15.04.2025	1.500
6	Adaptare Sisteme OSS	8 săptămâni	01.05.2025	7000
7	Implementare CESOP	12 luni	01.07.2025	5000
8	Accesarea Finanțărilor IMM	3 luni	01.07.2025	3000
9	Pregătire pentru ViDA	6 luni	01.10.2025	1000
10	Stabilire Proceduri EOIR	1 lună	01.01.2026	2500

Nr.	Activitate	Timp de Implementare	Data de Începere	Costuri Aproximative (EUR)
11	Formare Personal	4 săptămâni	01.02.2026	3000
12	Monitorizare și Îmbunătățire Continuă	Continuă	01.04.2026	5000/an
-	**Total**			**92,000**

7.2. Implementarea standardelor și reglementărilor DAC

Implementarea schimburilor de date cu țările membre ale Uniunii Europene, în conformitate cu directivele DAC1 până la DAC9, are o importanță majoră pentru Republica Moldova în contextul integrării europene și al cooperării fiscale internaționale. Aceste directive, cunoscute sub denumirea de Directive privind Cooperarea Administrativă (DAC), stabilesc cadrul legal pentru schimbul automat de informații între autoritățile fiscale ale statelor membre, având ca obiectiv principal combaterea evaziunii fiscale și a planificării fiscale agresive.

Implementarea acestor directive aduce multiple beneficii Republicii Moldova, contribuind la:

- **Combaterea Evaziunii Fiscale și a Fraudei**. Schimbul automat de informații financiare și fiscale permite autorităților să identifice și să investigheze mai eficient cazurile de evaziune fiscală, asigurând astfel colectarea corectă a impozitelor și protejarea veniturilor bugetare.
- **Promovarea Transparenței și Conformității Fiscale**. Adoptarea directivelor DAC încurajează transparența în raportarea fiscală și stimulează contribuabilii să respecte obligațiile fiscale, reducând riscul practicilor fiscale neloiale.
- **Armonizarea Legislativă și Integrarea Europeană**. Adaptarea legislației naționale la standardele și cerințele UE facilitează procesul de integrare europeană și consolidează relațiile cu statele membre, recunoscând Republica Moldova ca un partener de încredere.
- **Îmbunătățirea Cooperării Internaționale**. Schimbul de informații întărește colaborarea între autoritățile fiscale la nivel internațional, permițând un răspuns coordonat la provocările globale în domeniul fiscalității și prevenirea practicilor dăunătoare.
- **Protejarea Integrității SISFS**. Monitorizarea tranzacțiilor transfrontaliere și a activităților multinaționale previne erodarea bazei impozabile și transferul profiturilor către jurisdicții cu impozitare redusă sau nulă.
- **Adaptarea la Evoluțiile Tehnologice și Economice**. Directivele mai recente, precum DAC7 și DAC8, abordează noile modele de afaceri digitale și cripto-activele, asigurând că sistemul fiscal ține pasul cu inovațiile tehnologice și economice.

Implementarea directivelor DAC în cadrul strategiei IT naționale este esențială pentru asigurarea compatibilității tehnice și operaționale cu sistemele informatice ale UE. Aceasta implică:

- Dezvoltarea Infrastructurii IT: Adaptarea sistemelor informatice pentru a putea efectua schimburi automate de informații în conformitate cu standardele tehnice ale UE, asigurând securitatea și integritatea datelor transmise.
- Formarea Resurselor Umane: Instruirea personalului din administrația fiscală pentru a gestiona noile proceduri și tehnologii asociate schimbului automat de informații, consolidând capacitatea instituțională.
- Armonizarea Legislativă: Actualizarea cadrului legal național pentru a reflecta prevederile directivelor DAC, asigurând baza juridică necesară pentru colectarea și schimbul de informații fiscale.
- Securitatea Cibernetică: Implementarea măsurilor de securitate cibernetică pentru a proteja informațiile sensibile și a preveni accesul neautorizat sau breșele de securitate.
- Impactul Strategic asupra Republicii Moldova
- Prin alinierea la directivele DAC și implementarea schimburilor de date cu țările membre ale UE, Republica Moldova își consolidează poziția în comunitatea europeană și internațională, demonstrând angajamentul față de transparență și cooperare. Această integrare contribuie la:
- Eficientizarea Administrării Fiscale: Accesul la informații detaliate despre tranzacțiile transfrontaliere îmbunătățește capacitatea autorităților fiscale de a detecta și corecta neconformitățile.
- Creșterea Încrederii Investitorilor: Un sistem fiscal transparent și aliniat la standardele internaționale creează un mediu favorabil pentru investiții și dezvoltare economică.
- Protejarea Economiei Naționale: Combaterea eficientă a evaziunii fiscale și a fluxurilor financiare ilicite contribuie la stabilitatea financiară și la protecția resurselor economice ale țării.
- Consolidarea Relațiilor Internaționale: Participarea activă în schimburile de informații fiscale întărește relațiile cu partenerii internaționali și facilitează cooperarea în alte domenii de interes comun.

Integrarea directivelor DAC în strategia IT națională nu reprezintă doar o conformare la cerințele UE, ci și un pas important către modernizarea și eficientizarea administrației fiscale a Republicii Moldova. Prin adoptarea acestor măsuri, țara își îmbunătățește infrastructura tehnologică, își dezvoltă capitalul uman și își consolidează poziția pe plan internațional, contribuind la creșterea bunăstării cetățenilor și la dezvoltarea durabilă.

Costurile estimative şi resursele umane necesare a fi implicate întru implementarea directivelor DAC1-9 sunt reflectate în *Tabelul 8*Tabelul 6Tabelul 5Tabelul 3.

Tabelul 8. Plan de implementare a directivelor DAC1-9

Nr.	Directivă	Implementare Tehnologică	Resurse Umane	Costuri Estimative (EUR)
1	**DAC1**	Dezvoltarea unui sistem informatic securizat pentru schimbul de informații fiscale la cerere.	Programatori specializați, experți în protecția datelor, personal fiscal instruit.	100.000 - 200.000

2	**DAC2**	Crearea unei platforme naționale pentru colectarea și transmiterea automată a informațiilor financiare conform CRS.	Specialiști în integrarea sistemelor IT, experți în securitate cibernetică, personal pentru gestionarea relațiilor cu instituțiile financiare.	500.000 - 1.000.000
3	**DAC3**	Adaptarea sistemelor existente pentru raportarea automată a deciziilor fiscale anticipate și a acordurilor de preț în avans.	Dezvoltatori software, experți fiscali, personal pentru gestionarea și validarea datelor.	150.000 - 300.000
4	**DAC4**	Dezvoltarea unui sistem pentru colectarea, stocarea și transmiterea rapoartelor financiare detaliate ale grupurilor multinaționale (CbCR).	Specialiști în baze de date, analiști financiari, experți în securitatea informației.	400.000 - 800.000
5	**DAC5**	Integrarea sistemelor fiscale cu registrele beneficiarilor reali și dezvoltarea unei interfețe pentru schimbul de informații.	Specialiști IT, experți juridici, personal pentru actualizarea bazelor de date.	200.000 - 400.000
6	**DAC6**	Crearea unei platforme digitale pentru raportarea aranjamentelor fiscale transfrontaliere de către intermediarii fiscali.	Dezvoltatori de aplicații web securizate, experți în criptarea datelor, personal pentru analizarea rapoartelor.	300.000 - 600.000
7	**DAC7**	Dezvoltarea unui sistem pentru colectarea și transmiterea informațiilor de la operatorii platformelor digitale.	Specialiști în integrarea API-urilor, experți în economia digitală, personal pentru gestionarea datelor colectate.	600.000 - 1.200.000
8	**DAC8**	Dezvoltarea soluțiilor tehnologice pentru monitorizarea și raportarea tranzacțiilor cu cripto-active.	Experți în blockchain, specialiști în securitate cibernetică, analiști în cripto-active.	800.000 - 1.500.000
9	**DAC9**	Actualizarea și optimizarea sistemelor existente pentru eficientizarea schimbului de informații fiscale.	Specialiști IT pentru actualizări, experți în politici fiscale, personal pentru formare.	250.000 - 500.000