Componenta C7. Transformare digitală

Domeniu de intervenție: Transformare digitală

Obiectiv: O infrastructură digitală coerentă și integrată la nivelul administrației publice din România care să ofere servicii digitale de înaltă calitate atât cetățenilor, cât și companiilor. Prin realizarea acestui obiectiv sunt create condițiile pentru adoptarea tehnologiilor digitale în toate sectoarele și domeniile de activitate ale instituțiilor statului și pentru creșterea numărului de cetățeni și companii care vor putea beneficia și fructifica oportunitățile oferite de digitalizare. Implementarea pe scară largă a soluțiilor digitale va contribui, la creșterea gradului de transparentizare a activității autorităților statului și la reducerea barierelor birocratice, contribuind, de asemenea, la realizarea obiectivelor de dezvoltare durabilă.

Reforme și investiții:

A. Servicii publice digitale pentru cetățeni și firme

a) Reforma

R1. Dezvoltarea unui cadru unitar pentru definirea arhitecturii unui sistem de tip cloud guvernamental

b) Investiții

I1. Implementarea infrastructurii de cloud guvernamental

I2. Investitii pentru dezvoltarea/migrarea în cloud

I3. Realizarea sistemului de eHealth și telemedicină

I4. Digitalizarea sistemului judiciar

I5. Digitalizare în domeniul mediului

I6. Digitalizare în domeniul muncii și protecției sociale

I7. Implementarea formularelor electronice eForms în domeniul achizițiilor publice

I8. Carte de identitate electronică și semnătura digitală calificată

I9. Digitalizarea sectorului organizațiilor neguvernamentale

I10. Transformarea digitală în managementul funcției publice

Direcția Generală Management Mecanism de Redresare și Reziliență
Șos. București-Ploiești, nr. 1-1B/ Intrarea str. Menuetului, nr. 7, Victoria Office, Sector 1, București
info.pnrr@mfe.gov.ro
http://mfe.gov.ro/
https://www.facebook.com/PNRROficial

I18. Transformarea digitală și adoptarea tehnologiei de automatizare a proceselor de lucru în administrația publică

B. Conectivitate digitală

a) Reforma

R2. Tranziția către atingerea obiectivelor de conectivitate UE-2025 și stimularea investițiilor private pentru dezvoltarea rețelelor de foarte mare capacitate

b) Investiții

I11. Implementarea unei scheme de sprijinire a utilizării serviciilor de comunicații prin diferite tipuri de instrumente pentru beneficiari, cu accent pe zonele albe

C. Securitate cibernetică

a) Reforma

R3. Asigurarea securității cibernetice a entităților publice și private care dețin infrastructuri cu valențe critice

b) Investiții

I12. Asigurarea protecției cibernetice atât pentru infrastructurile TIC publice, cât și pentru cele private cu valențe critice pentru securitatea națională, prin utilizarea tehnologiilor inteligente

I13. Dezvoltarea sistemelor de securitate pentru protecția spectrului guvernamental

I14. Creșterea rezilienței și a securității cibernetice a serviciilor de infrastructură ale furnizorilor de servicii de internet pentru autoritățile publice din România

I15. Crearea de noi competențe de securitate cibernetică pentru societate și economie

D. Competențe digitale, Capital Uman și utilizarea Internetului

a) Reforma

R4. Creșterea competentelor digitale pentru exercitarea funcției publice și educație digitală pe parcursul vieții pentru cetățeni

b) Investiții

I16. Program de formare de competențe digitale avansate pentru funcționarii publici

I17. Scheme de finanțare pentru biblioteci pentru a deveni hub-uri de dezvoltare a competențelor digitale

I19. Scheme dedicate perfecționării/recalificării angajaților din firme

Buget: 1.884,96 mil. euro, din care solicitat în cadrul PNRR: 1.884,96 mil. euro. Valorile din prezenta componentă nu includ TVA.

Provocări și obiective

a) Provocări

Conform Indexului DESI (Digital Economy and Society Index) 2020, România ocupă ultimul loc în UE în ceea ce privește indexul Servicii Publice Digitale. De asemenea, România se află pe ultimul loc în ceea ce privește formularele precompletate și serviciile realizate integral online, ceea ce indică o problemă sistemică în privința calității și capacității de utilizare a serviciilor digitale oferite atât cetățenilor, cât și companiilor. În perioada 2015-2018, nu s-a înregistrat o îmbunătățire semnificativă a calității serviciilor publice digitale pentru companii, România ocupând și din acest punct de vedere ultimul loc în UE. Lipsa interoperabilității sistemelor informatice din administrația publică este un obstacol major în dezvoltarea serviciilor digitale centrate pe utilizatorul final (cetățean sau companie).

Sistemele existente sunt în general fragmentate, fiind proiectate și dezvoltate izolat de către diferite instituții ale statului, în afara unui cadru național coerent. Un accent major trebuie să cadă pe asigurarea interoperabilității la nivel de date (a regiștrilor de bază identificați și inventariați), pe principiile de reutilizare a building-blocks europene și pe principiile menționate anterior și incluse în cadrul național și european de interoperabilitate. Este prioritară, așadar, asigurarea interoperabilității bazelor de date disponibile la nivelul tuturor instituțiilor statutului român și dezvoltarea unei arhitecturi integrate a serviciilor digitale publice într-un Cloud Guvernamental.

Spre deosebire de componentele DESI2020 mai sus-menționate, România se situează mai bine la nivel european în ceea ce privește Conectivitatea. Acoperirea de bandă largă de mare viteză a crescut până la 82%, dar se situează încă sub media UE care este de 86%. Utilizarea conexiunii de bandă largă a stagnat la 66% dintre gospodării pentru al treilea an consecutiv și se situează cu mult sub media UE de 78%. O problemă majoră o reprezintă persistența decalajului digital între zonele urbane și cele rurale, acoperirea națională cu 4G (85%) fiind semnificativ mai mică decât media UE (96%). Unul dintre factorii principali care contribuie la lipsa investițiilor operatorilor telecom în construcția de rețele, îl reprezintă barierele legislative și birocratice în domeniul obținerii autorizațiilor de construire și al celorlalte avize și autorizații necesare derulării investițiilor. În același timp, aspecte precum competențele digitale scăzute ale unei părți a populației și gradul redus de digitalizare al sistemului public și al întreprinderilor contribuie la cererea scăzută pentru conectarea la servicii de Internet.

În ceea ce privește Securitatea Cibernetică, România se confruntă cu amenințări provenite din spațiul cibernetic la adresa infrastructurilor sale critice, având în vedere interdependența din ce în ce mai ridicată între infrastructurile cibernetice şi infrastructuri precum cele din sectoarele financiar-bancar, de transport, energie și apărare națională. Caracterul global al spaţiului cibernetic este de natură să amplifice riscurile la adresa infrastructurilor critice, afectând deopotrivă cetățenii, mediul de afaceri și cel guvernamental. Conform Strategiei Naționale de Apărare a Țării 2020-2024, România se confruntă cu următoarele probleme:

– nivel redus de securitate cibernetică a infrastructurilor de comunicații și tehnologia informației din domenii strategice;

– acutizarea decalajului tehnologic şi valorificarea insuficientă a beneficiilor conferite de utilizarea noilor tehnologii;

– tendința exponențială de dezvoltare a tehnologiilor emergente (5G, inteligența artificială, big data, Internet of Things, cloud şi smart computing) care vor genera, pe de o parte, nevoi de creștere și îmbunătățire a comunicațiilor, ce vor conduce la implementarea de servicii digitale inovatoare menite să sprijine cetățenii și mediul de afaceri, dar care, pe de altă parte, vor crește nevoia de colectare a unui volum din ce în ce mai mare de date și de securizare a acestora;

– concepte, instrumente și tehnologii inovatoare, precum criptomonedele, tehnologia blockchain, inteligenţa artificială, machine learning, Internet of Things, big data, tehnologia cuantică sau Internetul Ascuns (Dark Web-ul), pot fi utilizate și în planul criminalității organizate, infracționalității cibernetice, activităților de profil hacktivist, terorist sau extremist.

România este un inovator modest la nivelul UE, conform celui mai recent scoreboard pentru inovare. Conform datelor Institutului Național de Statistică, doar 14.6% dintre firmele din România au inovat în perioada 2016 – 2018 și doar 14.3% au inovat cu succes. Conform celui mai recent raport anual EIDES (Indexul European al Sistemelor de Antreprenoriat Digital) condițiile de piață și cultura și instituțiile informale erau sub-componentele unde România înregistrează cele mai scăzute scoruri.

Conform observațiilor Băncii Mondiale formulate în cadrul proiectului Romania: *Startup Ecosystem Strategy*, derulat cu sprijinul DG REFORM, printre provocările la adresa dezvoltării antreprenoriatului inovativ în România se numără:

– absența informațiilor privind nevoile și provocările specifice start-up-urilor față de alte întreprinderi mici și mijlocii;

– lipsa unor date credibile și sistematice despre ecosistemul inovativ în ansamblul său;

– insuficienta coordonare între autorități și actorii ecosistemului de start-up inovative.

În ceea ce privește adoptarea de tehnologii innovative de către mediul privat, România ocupă locul 27 din 28 de state UE în DESI 2020. Același loc este ocupat și în ceea ce privește competențele digitale. România se află mult sub media UE în ceea ce privește persoanele cu competențe digitale de bază (31% vs. 58%), a persoanelor deținând competențe digitale avansate (10% vs. 33%) și a persoanelor cu competențe elementare în domeniul software (35% vs. 61%). România se află considerabil sub media UE și în ceea ce privește procentul de specialiști IT din totalitatea persoanelor încadrate cu un loc de muncă (2.2% vs. 3.9%).

Cea mai recentă cercetare EIDES conchide că intervențiile de politică publică în formarea capitalului uman reprezintă cea mai importantă intervenție a statului pentru sprijinirea dezvoltării antreprenoriatului digital. Firmele nu pot adopta cu succes tehnologii inovative în lipsa unei forțe de muncă ce deține competențe digitale. Mai mult, o tranziție de succes a companiilor către era digitală este condiționată de deținerea unor competențe digitale avansate, cum ar fi cunoștințele

de programare (coding) sau data analytics. În plus, conform concluziilor programului România: Startup Ecosystem Strategy, dezvoltarea antreprenoriatului digital este frânată în România și de lipsa competențelor manageriale. Mai mult, serviciile digitale publice nu pot fi livrate cetățenilor și companiilor decât de funcționari publici cu un nivel ridicat de competențe digitale.

Reformele propuse a fi implementate în cadrul acestui Plan răspund următoarelor Recomandări Specifice de Țară (2019 și 2020):

- ✓ 2019_III.2 Să asigure îmbunătățirea competențelor, inclusiv a competențelor digitale, în special prin sporirea relevanței pe piața forței de muncă a educației și formării profesionale și a învățământului superior;
- ✓ 2020_III.3 Să direcționeze cu prioritate investițiile către tranziția ecologică și digitală, în special către transportul durabil și infrastructura de servicii digitale;
- ✓ 2020_IV.1 Să îmbunătățească eficacitatea și calitatea administrației publice, precum și previzibilitatea procesului decizional, inclusiv printr-o implicare adecvată a partenerilor sociali;
- ✓ 2020_II.3 Să extindă accesul la serviciile esențiale pentru toți;
- ✓ 2020_II.5 Să consolideze competențele și învățarea digitală.

b) <u>Obiective</u>

Principalul obiectiv al Pilonului II Transformare digitală este acela de a înfăptui transformarea digitală a României prin realizarea unei infrastructuri digitale coerente și integrate la nivelul administrației publice din România care să ofere posibilitatea accesării de servicii digitale de înaltă calitate atât cetățenilor, cât și companiilor, prin creșterea numărului de localități aflate în zone albe conectate la intrenet de mare viteză și în același timp prin sporirea competențelor digitale ale cetățenilor.

Viziunea și perspectivele pentru transformarea digitală a Europei până în 2030 (viziune pentru deceniul digital al UE), care se articulează în jurul celor patru puncte cardinale (digitalizarea serviciilor publice, competențe, infrastructuri digitale sigure și durabile și transformarea digitală a întreprinderilor) au servit drept punct de plecare în conceperea Pilonului II Transformare digitală.

Ca parte a eforturilor de a atinge acest obiectiv propus, Pilonul II Transformare Digitală abordează patru elemente cheie cu obiective conexe și anume:

A. Servicii publice digitale pentru cetățeni și firme
B. Conectivitate digitală
C. Securitate cibernetică
D. Competente digitale, capital uman și utilizarea Internetului

Astfel sunt propuse investiții în tehnologii digitale, infrastructură și procese care vor conduce la realizarea, pentru prima dată în România, a interoperabilității tuturor serviciilor publice digitale, sub garanția unui nivel ridicat de securitate cibernetică pentru realizarea unei transformări digitale

de succes în beneficiul cetățeanului și respectând cadrul legal privind protecția datelor cu caracter personal.

Investiții precum realizarea cloudului guvernamental prin folosirea unor tehnologii de vârf, cu un nivel înalt de securitate cibernetică și eficiente din punct de vedere energetic, dezvoltarea și migrarea aplicațiilor existente aferente serviciilor publice digitale (în principal în ceea ce privește evenimentele de viață), asigurarea interoperabilității serviciilor publice astfel încât să poate fi atins obiectivul "once-only", sunt câteva dintre tipurile de intervenții care vor facilita trecerea României către o economie bazată pe date, sigură și dinamică, aliniindu-se cu direcțiile strategice de acțiune ale UE în ceea ce privește guvernanța datelor.

Tehnologia digitală sprijină procesul de transformare a modului în care se poate facilita existența prin integrarea lor în toate sectoarele și domeniile de activitate, de către toți cetățenii și întreprinderile. Digitalizarea oferă impulsul necesar pentru dezvoltarea societății în ansamblu pe termen lung, creșterea capacității de reziliență la situații de criza și adaptarea forței de muncă la noile condiții din piață pentru a fi competitivi. Prin digitalizare se vor crea premisele de dezvoltare cu impact de durată asupra modului în care trăim, muncim și relaționăm. Digitalizarea va facilita schimbul de informații și va oferi posibilitatea reducerii timpilor de așteptare în ceea ce privește obținerea de servicii sau produse digitale.

Obiectivul contribuie la dezvoltarea și implementarea de tehnologii și capacități avansate de prelucrare a datelor ce vor spori suveranitatea tehnologică și competitivitatea UE, asigurând livrarea de servicii în timp real cetățenilor, entităților publice, partenerilor sociali și întreprinderilor.

Din aceste puncte de vedere preconizăm că odată cu implementarea măsurilor prevăzute în cadrul PII *Transformare digitală*, administrația publică va beneficia de o modificare structurală importantă, generate totodată și de schimbările structurale de la nivelul celor mai relevante politici din domeniu.

Odată cu generarea acestei modificări atât de importante și prin facilitarea acesului egal pentru toți cetățenii la serviciile administrației publice sunt puse în aplicare și principiile Pilonul european al drepturilor sociale (principiul nr. 2 *Egalitatea de gen* şi principiul nr. 5. *Locuri de muncă sigure și adaptabile*). De asemenea, digitalizarea creează premisele pentru asigurarea egalităţii de gen, în sensul participării egale a femeilor şi bărbaţilor pe piaţa forţei de muncă, precum și asigurarea unor avantaje ce țin de o mai mare flexibilitate pentru găsirea unui loc de muncă, conducând spre aplicarea principiilor nr. 3 *Egalitatea de şanse,* nr. 17. *Incluziunea persoanelor cu handicap* şi nr. 20. *Accesul la servicii esențiale*

Totodată, prin implementarea cărții de identitate electronică (eID) se va asigura accesul mai facil la serviciile publice modernizate oferite tuturor cetățenilor, independent de locație, cu costuri reduse și în timp real.

1. Descrierea reformelor și investițiilor

A. Servicii publice digitale pentru cetățeni și firme

a. Reforme

R1. Dezvoltarea unui cadru unitar pentru definirea arhitecturii unui sistem de tip cloud guvernamental (Alocare 11,89 mil. euro)

Provocări:

Conform Indexului DESI 2020, România ocupă unul dintre ultimele locuri în UE la capitolul Servicii Publice Digitale la nivelul anului 2018. De asemenea, România se află pe ultimul loc în ceea ce privește formularele precompletate și serviciile realizate integral online, ceea ce indică o problemă sistemică în privinta calitatii și capacitatii de utilizare a serviciilor digitale oferite cetățenilor și companiilor. În perioada 2015-2018, nu s-a înregistrat nicio îmbunătățire semnificativă a calității serviciilor publice digitale pentru companii, România ocupând și din acest punct de vedere ultimul loc în UE.

Unul dintre obstacolele principale pentru dezvoltarea serviciilor digitale oferite de instituțiile statului îl reprezintă nivelul redus de interoperabilitate al sistemelor informatice din administrația publică. Sistemele existente sunt, în general fragmentate, fiind proiectate și dezvoltate izolat de către diferite instituții ale statului, în afara unui cadru național coerent. În acest sens, prioritară este asigurarea interoperabilității bazelor de date existente la nivelul instituțiilor publice și realizarea unei arhitecturi integrate a serviciilor digitale publice într-un Cloud Guvernamental, așa cum este, de altfel sugerat și de Recomnadările specifice de țară 20_III.3 *Să direcționeze cu prioritate investițiile către tranziția ecologică și digitală, în special către transportul durabil și infrastructura de servicii digitale*.

Atât reformele și investițiile propuse pentru realizarea Cloud-ului Guvernamental sprijină inițiativele emblematice europene de tip **Scale-up**, având în vedere avantajele tehnice și economice care privesc procesarea, stocarea datelor și disponibilitatea serviciilor. Funcționarea în regim de cloud generează economii consistente sub aspectul investițiilor și al cheltuielilor operaționale și asigură cele mai eficiente soluții de digitalizare ale instituțiilor administrației la toate nivelurile, conform celor mentionate în „*European Commission Cloud Strategy / Cloud as an enabler for the European Commission Digital Strategy*”.

Având în vedere nivelul relativ scăzut al serviciilor publice digitalizate în România, prin investițiile propuse se urmărește consolidarea potențialului de creștere a economiei pe termen lung, prin asigurarea unor servicii publice accesibile și cu un grad ridicat de transparentizare având drept obiectiv primordial interesul cetățeanului. Investițiile în tehnologiile digitale (inovatoare) reprezintă elemente cheie într-o economie bazată pe cunoaștere, fiind deosebit de importante pentru realizarea unei creșteri echitabile, inclusive, sustenabile și care asigură, în același timp, potențial pentru crearea de locuri de muncă specializate în tehnologii avansate, permițând astfel recrutarea de specialiști în cloud și tehnologii de vârf, vizându-se astfel, în mod indirect și reducerea decalajului de competențe digitale.

Obiective:

i) Modernizarea administrației publice prin transformare digitală disruptivă și adoptarea celor mai evoluate tehnologii informatice și modele de organizare care

reorientează administrația publică spre cetățean și companii, către societate în ansamblu, asigurând premisele dezvoltării de politici publice bazate pe date, într-o societate informațională adaptată provocărilor societale și riscurilor semnificative;

ii) Dezvoltarea arhitecturii integrate a serviciilor digitale publice prin creșterea gradului de interoperabilitate al tehnologiilor digitale existente în prezent în cadrul instituțiilor publice din România.

Implementare:

Arhitectura fragmentată a administrației publice este vizibilă pe orice nivel, pornind de la o infrastructură de găzduire a sistemelor informatice bazată pe camere de date ineficiente energetic și vulnerabile operațional până la lipsa unei sistematizări și consolidări morfologice cu impact direct în valoarea de reutilizare a datelor publice. Dificultățile întâmpinate de instituțiile publice în atragerea și reținerea specialiștilor TIC, imposibilitatea coordonării investițiilor în vederea asigurării compatibilității tehnologice sunt provocări care limitează beneficiile pe care un sistem de e-guvernare funcțional și interoperabil le poate aduce cetățenilor și mediului de afaceri. Sunt necesare reforme și investiții care să asigure sinergia administrației publice prin interoperabilitate și competență.

Concentrarea marilor sisteme ITC în centre de date moderne va asigura eficiență și reziliență cu investiții și cheltuieli de operare proporțional mai mici pe baza unor echipe tehnice complete și bine specializate. Transformarea digitală succesivă prin etapele ”cloud ready” și ”cloud first” este astfel posibilă ducând rapid la servicii de cloud de tip IaaS și evolutiv la servicii de tip PaaS și SaaS. Adopția serviciilor SaaS va fi încurajată prin oferirea de către operatorul cloud-ului a unui număr în permanență creștere de servicii și building blocks. Trecerea la servicii PaaS, spre exemplu de baze de date, va oferi completă siguranță în privința respectării standardelor de date, respectiv o interoperabilitate nativă și completă.

Pentru un eficient management al schimbării serviciile publice vor fi segregate în categorii cu nevoi specifice urmând a se adresa astfel posibila rezistență instituțională. Atât utilizarea serviciilor de cloud cât și schimbul de date necesită o infrastructură de comunicații protejată și de capacitate îndestulătoare. Trecerea la conectarea instituțiilor publice, mai ales cele din teritoriu, pe baza tehnologiei fibrei optice va asigura capacitate și reziliență.

Date standardizate: Identificarea principalelor informații prelucrate de administrația publică, catalogarea acestora într-un sistem ierarhic de tip nomenclator, alegerea celor mai potrivite structuri de date pentru înregistrarea acestora. Emiterea de norme succesive cu privire la structurile de date ce vor fi utilizate în viitoarele sisteme guvernamentale.

Prioritizarea cloud ready și cloud first: Norme legale incrementale prin care orice nouă aplicație a administrației publice trebuie construită într-un cadru tehnologic care permite migrarea facilă în cloud (cloud ready) respectiv trebuie direct lansată în producție în cloud (cloud first). Orice excepție trebuie argumentată și aprobată de o autoritate publică specializată.

Date credibile: Prioritizând cele mai importante seturi de date este necesară evaluarea procedurilor istorice de colectare respectiv producere a acestora, inclusiv a gradului de conformare, evaluarea exactității datelor prin compararea unor eșantioane semnificative statistic cu alte surse de date și orice altă metodă rezonabilă care să indice un grad de încredere specific acestora. Realizarea unui catalog al surselor de date guvernamentale.

Date compatibile: Pentru datele de interes cu un grad rezonabil de credibilitate stabilit se vor proiecta și implementa modalități de transformare prin aliniere la standardul guvernamental.

Registre naționale și depozite de date certe: Va fi elaborată legislație dedicată registrelor naționale definind caracterul autentic al acestora și modalitățile de utilizare. Datele sigure și compatibile vor fi incluse în sistemul registrelor naționale. Restul datelor vor fi înregistrate în catalogul de depozite de date certe.

Interoperabilitatea dintre serviciile administrației publice este scăzută, întrucât, în general, fiecare instituție publică și-a dezvoltat propriul serviciu public digital. Prin realizarea interoperabilității serviciilor electronice se oferă soluții pentru optimizarea operațiunilor guvernamentale, consolidarea activelor IT și reutilizarea datelor din registrele de bază. Cetățenii vor beneficia de un guvern conectat și eficient. Cetățenii vor putea să ofere date cu caracter personal guvernului o singură dată, iar instituțiile publice vor putea reutiliza aceste date pentru furnizarea de servicii. Pentru a atinge un nivel al serviciilor conform cu arhitectura europeană de interoperabilitate trebuie completate lacunele care împiedică realizarea unor servicii “digital first”. Pentru aceasta este nevoie de migrarea și integrarea în structurile de date existente a tuturor datelor existente, astfel încât acestea să susțină funcționarea în timp real a serviciilor oferite. Totodată, implementarea funcționalităților implică alinierea infrastructurilor de identificare și autorizare națională cu cele ale statelor membre ale UE, într-o schemă transnațională, conform normelor europene stabilite prin regulamentul eIDAS si actualizările succesive. Interoperabilitatea bazelor de date utilizate de către administrația publica presupune că schimbul de date este sigur, certificat și criptat asigurându-se astfel securitatea datelor. Odată eliminate lacunele existente se vor realiza servicii agregate constituite prin gruparea unui număr de servicii publice de bază care pot fi accesate într-un mod sigur și controlat. Aceste funcții vor fi furnizate de autoritățile și instituțiile administrației publice de orice nivel, noile sisteme IT vor fi dezvoltate pe baza unei arhitecturi orientate pe servicii. Stimularea utilizării tehnologiilor inovative va avea un impact pozitiv asupra calității vieții cetățenilor, protejării mediului, dezvoltării mediului de afaceri și dezvoltării durabile a comunităților locale și societății, în general.

În același timp, lipsa conectivității digitale și a infrastructurii adecvate adâncește și mai mult disparitățile dintre regiuni și din interiorul acestora. În cadrul regiunilor, județele în care conectivitatea este redusă, înregistrează un nivel scăzut de creștere economică, în timp ce județele în care conectivitatea este bună, în care se investește semnificativ în infrastructură și în care ratele investițiilor străine directe sunt ridicate, nivelul creșterii economice și nivelul salariilor medii sunt ridicate.

În vederea dezvoltării arhitecturii integrate a infrastructurii serviciilor digitale este necesară adoptarea Legii Interoperabilitatii Sistemelor Informatice care stabilește cadrul național de referință pentru realizarea interoperabilității institutiilor publice în domeniul tehnologiei

informației și comunicațiilor si furnizarea serviciilor electronice urmarind principiul “once-only” și centrarea serviciilor publice în jurul utilizatorului final („user centricity”). Aceasta lege va fi aliniata cu prevederile din European Interoperability Framework si va fi implementată prin norme tehnice pe care entitățile publice le vor aplica pentru dezvoltarea aplicatiilor interoperabile, intr-un ansmablu coerent care reprezinta arhitectura sistemului de date guvernamentale, clasificate după gradele de confidențialitate și durabilitate.

Adoptarea Legii Cloudului Guvernamental impune realizarea obiectivului vizat și asigurarea unui management eficient privind gestionarea centralizată a resurselor TIC. Se impune adoptarea cu celeritate a unor responsabilități și sarcini precise cu privire la proiectarea, implementarea, dezvoltarea și administrarea infrastructurilor, tehnologiilor și serviciilor Cloudului Guvernamental.

Pentru a decide soluția optimă cu privire la dezvoltarea Cloudului Guvernamental, MCID va contracta servicii de consultanță specializate pentru a efectua o analiză detaliată a opțiunilor strategice, cu beneficii și riscuri clar specificate, care corespund, realist și ambițios, particularitățile instituționale din România și obiectivele reformei. Analiza va oferi, în special, informațiile necesare cu privire la disponibilitatea centrelor de date adecvate care sunt în prezent operaționale și care pot fi recuperate în Cloud guvernamental, în conformitate cu termenii impuși de regulamentul RRF.

Opțiunile strategice și tehnologice și pachetul legislativ și normativ, care vor sta la baza dezvoltării guvernului Cloud, care sunt în responsabilitatea MCID, Autoritatea pentru Digitalizarea României (ADR) și a instituțiilor cu atribute în acest domeniu (ADR se afla în subordinea MCID, iar roluluri distincte vor fi trasate prin Ordin de ministru). Soluția tehnologică va fi pusă în aplicare de către o autoritate națională (cum ar fi STS), pe baza unei proceduri de achiziții competitive și transparente.

Se vor avea în vedere, în mod special, soluții de cloud hibrid utilizate în funcție de nivelurile de sensibilitate și durabilitate ale datelor și de modalitățile de utilizare și ale aplicațiilor și organizarea într-o structură de încredere concentrică pe trei niveluri care evoluează progresiv din interior către exterior.

Nivelul 1. Cloud-ul Intern capitalizează soluțiile existente în prezent cu niveluri scăzute de virtualizare prin transformarea lor în solutii informatice cloudificate IaaS si PaaS accesibile instituțiilor din administrația publică. In funcție de opțiunile individuale, instituțiile publice vor putea dezvolta și livra servicii SaaS. Acest tip de cloud asigură interoperabilitatea bazelor de date și functionarea soluțiilor digitale bazate și pe consumul datelor sensibile, clasificate și catalogate corespunzator, raspunzând totodată exigentelor de control și securitate a informațiilor.

Nivelul 2. Cloud-ul Dedicat se bazează pe soluțiile de Cloud disponibile în sectorul industrial/comercial și va fi dezvoltat astfel încât să asigure funcționarea integrată cu Cloudul intern. Acesta va fi personalizat pentru a răspunde cerințelor specifice administrației publice și se va baza pe infrastructuri dedicate cu asigurarea interoperabilității și securității cibernetice. Acest tip de cloud va permite centralizarea și prelucrarea acelor aplicații și date care prezintă cel mai scăzut tip de sensibilitate, dar care necesită, în același timp un anumit nivel de durabilitate.

Nivelul 3. Cloud-ul Extern este constituit dintr-un catalog de soluții de Cloud externe, generice, accesibile în Internet ca SaaS, ușor accesibile și intuitive pentru facilitarea utilizării. Acest tip de Cloud stimulează participarea unui număr crescut de furnizori de soluții informatice în ecosistemul digital.

Securitatea cibernetică va viza atât protecția externă a Cloudului, cât și cea internă, având în vedere riscurile și vulnerabilitățile specifice, prin implementarea celor mai avansate soluții de cybersecurity disponibile și eficiente economic.

Măsuri specifice:

- Un consultant specializat contractat de MCID în urma unei proceduri standard prevăzute de legislația în domeniul achiziției publice va efectua analiza opțiunilor pentru atingerea obiectivelor reformei. Procedurile de achiziție vor respecta legislația în vigoare. Criteriile de selecție pentru fiecare contract vor respecta prevederile Legii nr. 98/2016 cu modificările și completările ulterioare. În ceea ce privește tipul procedurilor de achiziții publice și criteriile de selecție, acestea depind de valoare, respectiv de tipul contractului propus și vor fi decise de fiecare autoritate contractantă, conform specificului fiecărei proceduri. Totodată, toate procedurile de achiziții care vor fi realizate vor avea prevăzute dispoziții privind asigurarea securității cibernetice a soluțiilor TIC achiziționate/ implementate de către instituțiile publice. În cazul în care se decide că analiza va fi realizată de către o autoritatea a statului, procedura de achiziție nu va mai fi realizată.

- Analiza va prezenta:

  i) opțiunile strategice și tehnologice și pachetul legislativ și normativ pe baza cărora Guvernul, prin MCID, ADR și institutiile cu responsabilitati în domeniu, stabilește modalitatea de realizarea a Cloudului Guvernamental, cu includerea normelor de interoperabilitate și modelului de guvernanță a datelor guvernamentale;

  ii) evaluarea posibilităților de construcție, livrare, instalare și funcționare a infrastructurilor civile și tehnologice, conform termenelor prevăzute în Plan;

  iii) inventarierea și catalogarea riguroasă a aplicațiilor/serviciilor digitale publice oferite în prezent de autoritățile statului din administratia centrală și bazelor de date, designul proceselor și procedurilor implementate în producție și/sau aflate în stadii de implementare;

  iv) planul de dezvoltare/ migrare în cloud (în prezent, nivelul existent de virtualizare este estimat de ADR și STS ca fiind scăzut) a aplicațiilor catalogate.

Dezvoltarea soluțiilor cloud se va realiza pe baza principiilor once-only, interoperable-by-default, digital-by-default, disponibile inclusiv pentru persoanele cu dizabilități (în conformitate cu Directiva 2102/2016 transpusă prin OUG 112/2018). Această acțiune va fi complementară celei ce va fi realizată ca parte a asistenței tehnice oferite ADR de către DG Reform și prin care se urmărește implementarea unei metodologii de evaluare a nivelului de digitalizare în cadrul administrației publice.

În vederea realizării obiectivelor de reformă și investițiilor prevăzute pentru transformarea digitală în cadrul MCID se operaționalizează și va funcționa un *Task Force* pentru implementarea și monitorizarea reformelor și investițiilor privind digitalizarea, propuse în Planul Național de Redresare și Reziliență. Acest Task Force va fi operaționalizat până în Q4 2021 și va funcționa cu caracter temporar, doar pe durata derulării Planului Național de Redresare și Reziliență (2021-2026), având printre atributii următoarele:

- dezvoltarea componentelor sectoriale ale PNRR;
- monitorizarea implementării reformelor și investițiilor în cadrul PNRP, concentrându-se pe proiectele cheie și propunând măsuri de remediere imediată pentru blocurile critice, în strânsă colaborare cu celelalte instituții implicate;
- dezvoltarea sistemelor de management al performanței proiectelor în acoperirea obiectivelor specifice ale pilonului digital;
- dezvoltarea și reglementarea cadrului normativ, metodologic și a procedurilor funcționale, operaționale și financiare din domeniul său de activitate;
- dezvoltarea instrumentelor pentru implementarea politicilor în domeniul său de activitate;
- managementul proiectului și raportarea tuturor etapelor de realizare a obiectivelor stabilite în cadrul PNRR pentru proiectele de digitalizare;
- îndeplinirea oricăror alte atribute necesare pentru a acoperi implementarea proiectelor / reformelor de investiții care sunt finanțate din digitalizarea PNRR.

Grupul de lucru se află sub coordonarea unui director, subordonat ministrului care deține portofoliul de digitalizare.

Unitatea va fi operaționalizată și va funcționa cu un număr de 17 angajați contractuali, în perioada de implementare a PNRR, resursă umană înalt specializată în domeniul tehnologiilor digitale și managementului de proiect de specialitate, cu scopul asigurării coordonării operaționale a procesului de digitalizare prevăzut.

În ceea ce privește implementarea principiilor Pilonului european al drepturilor sociale, Task Force-ul va realiza acțiuni de monitorizare a modului de respectare a prevederilor OUG 112/2018 privind transpunerea Directivei 2102/2016 privind accesibilitatea site-urilor web și a aplicațiilor mobile ale organismelor din sectorul public, precum și respectarea prevederilor Directivei (UE) 2019/882 a Parlamentului European și a Consiliului din 17 aprilie 2019 privind cerințele de accesibilitate aplicabile produselor și serviciilor. Monitorizarea se va realiza pe baza unei grile de indicatori relevanți în conformitate cu, dar fără a se limita la, indicatorii specifici tabloului de bord social revizuit și a indicatorilor și reperelor de monitorizare ale Agenției pentru Drepturi Fundamentale a Uniunii Europene (FRA). În urma procesului de monitorizare Task-Force va elabora recomandări de remediere, pe care le va înainta operatorilor vizați în calitatea acestora de beneficiari ai acestei componente din PNRR.

În acest sens, pe baza valorificării practicilor de calitate din alte state membre desfășurate în faza de analiză, în noul cadru legal vor fi specificate principiile și abordările potrivite pentru creșterea

accesibilității la serviciile publice digitale de către utilizatori, în special de către persoanele cu dizabilități, a persoanelor cu cerințe speciale, persoanelor în vârstă sau a celor cu un nivel scăzut al competențelor digitale ș.a.

Astfel, investițiile ce vor fi realizate sub umbrela legislației dezvoltate vor trebui să respecte principiile accesibilității serviciilor digitale și pentru categoriile de cetățeni vulnerabili.

Grup Țintă: Administrația publică centrală și instituții publice de la nivel central și local.

Ajutor de stat:

Măsurile din cadrul acestei reforme nu implică elemente de ajutor de stat, vizând în general modificări legislative și/sau aspecte de natură administrativă. În ceea ce privește investițiile/serviciile necesare implementării acestor măsuri, acestea vor fi achiziționate printr-o procedură competitivă, transparentă, nediscriminatorie și necondiționată, nefiind incidente astfel prevederile legislației din domeniul ajutorului de stat.

Calendar: 2021 - 30 iunie 2022

b. Investiții

I1. Implementarea infrastructurii de cloud guvernamental (Alocare 374,73 mil. euro)

Provocări:

Infrastructura IT existentă în prezent în cadrul instituțiilor care livrează servicii publice digitale este inadecvată, fragmentată, depășită din punct de vedere tehnologic, cu nivel redus de interoperabilitate și grad scăzut de securitate cibernetică.

Prin implementarea investiției vor fi asigurate infrastructura, tehnologiile și operarea Cloudului Guvernamental pentru viitoarele aplicații ale instituțiilor publice în cloud IaaS, PaaS și/sau SaaS într-un mod unitar, standardizat, eficient și adaptat cerințelor utilizatorilor finali, firme și/sau cetățeni.

De asemenea, se urmărește creșterea capacităților de colectare, stocare, analiză a datelor guvernamentale prin extinderea Cloudului Guvernamental cu noduri de Edge Computing, cu putere de procesare ridicată și latență scazută. Această capabilitate este critică pentru utilizarea tehnologiilor de Inteligență Artificială (AI), Machine Learning și Big Data și elaborarea politicilor publice pe baza datelor certe. Vor fi asigurate, de asemenea și servicii de consum și analiză a datelor prin structuri de data lakes/data marts și data warehouse, în vederea asigurării rapidității analitice și de raportare recurentă. Această categorie particulară are o importanță strategică din perspectiva utilizării datelor.

Operațional, Cloud-ul Guvernamental va funcționa cu asigurarea elasticității specifice și disponibilității ridicate prin implementarea a două centre de date principale și două secundare, de

nivel Tier III/IV by design. Realizarea celor două centre de date secundare, interoperabile cu cele două principale, este necesară pentru asigurarea cerințelor tehnice și legale de business continuity și disaster recovery.

Centrele de date vor funcționa cu consum energetic scăzut, asigurat de cele mai avansate soluții low power și răcire cu apă, cu respectarea parametrilor de eficiență energetică prevăzuți de documentul "2021 Best Practice Guidelines for the EU Code of Conduct on Data Center Energy Efficiency". De asemenea, vor fi implementate tehnologii verzi pentru asigurarea unei părți a alimentării cu energie electrică de tipul panourilor fotovoltaice. Este necesară dotarea acestor centre de date cu instalații tehnice de electroalimentare, climatizare, securitate la incendiu, redundante, cu un regim de funcționare neîntreruptă, operate de personal specializat și înalt calificat care să asigure monitorizarea continuă 24/7 și intervenția promptă în cazul unor disfuncționalități. |Astfel, pentru implementarea și operarea centrelor de date este necesară existența unei resurse umane înalt calificate, conform standardelor în domeniu care sa asigure administrarea continuă pe toată perioada de funcționare a cloud-ului guvernamental.

Următoarele aspecte importante sunt avute în vedere pentru realizarea, operarea și administrarea cloudului guvernamental:

a. existența unei resurse umane bine pregătite și cu experiență în implementarea și administrarea de infrastructuri complexe și performante IT&C, la nivel central și la nivel național;

b. existența la nivel național de infrastructură redundantă de comunicații de bandă largă;

c. asigurarea de servicii integrate de comunicații și securitate;

d. monitorizarea funcțională a tuturor parametrilor tehnici ai serviciilor de la nivel fizic, prin centre specializate de tip NOC, 24/7;

e. asigurarea de servicii de tip CERT, proactive și reactive, ce includ monitorizare de securitate, audit de securitate, răspuns la incidente de securitate;

f. asigurarea managementului integrat al securității cibernetice și al infrastructurii IT&C aferentă Cloud-ului guvernamental;

g. asigurarea periodică a auditului extern la nivel operațional și al managementului accesului și protecției datelor cu caracter personal;

h. creșterea nivelului general de securitate cibernetică și siguranță a datelor în administrația publică centrală și locală prin consolidarea capacității de prevenție și reziliență la atacuri și incidente cibernetice;

i. asigurarea de copii de rezervă pentru restaurarea infrastructurii de Cloud Guvernamental.

Obiectiv: Realizarea infrastructurii cloud-ului guvernamental, folosind tehnologii de ultimă generație, cu un înalt grad de securitate cibernetică, eficiente din punct de vedere energetic, necesare asigurării găzduirii de sisteme informatice publice centrale și interoperabilității acestora, într-un mod unitar și standardizat.

Atingerea obiectivului general va fi posibilă prin realizara următoarelor obiective specifice:

1. Amenajarea și dotarea centrelor de date cu un nivel de reziliență caracteristic nivelului Tier IV/III by design;

2. Echiparea centrelor de date cu infrastructură și tehnologii cloud specifice IT&C (hardware și software);

3. Asigurarea comunicațiilor securizate folosind infrastructurile de comunicații de bandă largă operate de autoritatea publică abilitată la nivel național.

Implementare: Conform celor prezentate în detaliu în cadrul Reformei 1, un consultant extern va efectua, la solicitarea MCID, o analiză a serviciilor digitale publice curente și a condițiilor de dezvoltare/migrare ale acestora în cloud și va propune un set de standarde tehnologice adoptate prin legislatia de cloud și interoperabilitate.

În urma analizei, Guvernul prin MCID, în colaborare cu ADR și instituțiile cu responsabilități în domeniu (SGG, STS, SRI, Cyberint, CERT-RO, MAI, MApN) stabilesc responsabilitățile privind construcția și operarea cloud-ului guvernamental optând pentru soluția optimă din punct de vedere financiar, al capabilităților tehnice și al calendarului de implementare, adecvată obiectivelor investiției.

Facilitățile propuse pentru includerea în cloudul guvernamental și care necesită amenajare/îmbunătățire/pregătire cu infrastructură și suport tehnic (alimentare cu energie electrică, aer condiționat și sisteme de securitate) și dotare cu infrastructură TIC, sunt cele care au fost special concepute cu scopul de a funcționa ca centre de date (de nivelul III și nivelul IV), aflându-se în prezent în diferite etape de implementare, respectiv la faza de execuție/elaborare studiu de fezabilitate.

Astfel, aceste facilități, aflate în diferite faze de implementare, urmează să fie selectate cu prioritate, deoarece acestea au fost special concepute pentru a funcționa ca centre de date și pentru a reduce timpul de implementare a proiectelor, asigurând astfel respectarea termenelor impuse de Regulamentul 241/2021, referitor la angajarea cheltuielilor (contractare) și la plata acestora. Utilizarea facilităților special concepute pentru a funcționa ca centre de date, asigură găzduirea infrastructurii TIC la standarde industriale ridicate.

Reziliența economică este astfel asigurată de faptul că dezvoltarea cloud-ului guvernamental (folosind fie investiții brownfield/greenfield sau ambele) va duce la o creștere a gradului de digitalizare a serviciilor oferite de autoritățile / instituțiile publice din România. Acest lucru va asigura:

- eficientizarea furnizării acestor servicii;

- reducerea costurilor necesare asigurării acestora;

- reducerea timpului în care cetățenii / operatorii economici beneficiază de aceste servicii;

- îmbunătățirea interacțiunii dintre cetățeni / mediul de afaceri cu autoritățile / instituțiile publice;

- asigurarea continuității serviciilor IT chiar și în cazul evenimentelor neașteptate cu impact major asupra dezvoltării normale a activităților din societate (de exemplu pandemia COVID-19, cutremure, inundații).

Toate aceste beneficii obținute prin dezvoltarea infrastructurii guvernamentale de cloud vor contribui la reziliența economiei prin asigurarea eficienței și continuității serviciilor publice furnizate de autoritățile / instituțiile publice cetățenilor și mediului de afaceri.

Totodată, va fi asigurată compatibilitatea funcțională (*cloud native, cloud ready*) a centrelor de date din cadrul cloudului pentru a asigura un grad ridicat de reziliență și scalabilitate în cazul unei situații de criză de lungă durată, de tipul celei pandemic. Centrele de date vor fi dotate cu infrastructură TIC care să permită oferirea de servicii de tip IaaS, PaaS și SaaS.

Implementarea cloudului guvernamental va presupune cel putin urmatoarele etape:

- construcția de centre de date Tier IV by design pentru cele doua centre principale si Tier III by design pentru cele secundare;
- furnizarea infrastructurii de comunicații şi tehnologia informației (cabluri de fibră optică şi echipamente de comunicații de mare capacitate) specifice;
- dezvoltarea/extinderea rețelei de alimentare cu energie electrică pentru fiecare centru de date în parte în vederea asigurării redundanței și a necesarului de energie electrică;
- realizarea unei infrastructuri de climatizare scalabile şi redundante, eficientă din punct de vedere energetic;
- instalarea sistemului de detecție şi stingere incendiu cu gaz inert care să asigure protecția pentru întreaga infrastructură a fiecărui Centru de Date în parte;
- implementarea sistemului de securitate fizică (control acces, monitorizare video, antiefracție etc.) pentru infrastructura dezvoltată;
- implementarea rețelei de monitorizare și management a infrastructurii în cadrul facilității realizate;
- realizarea infrastructurii IT&C scalabilă și de înaltă disponibilitate (echipamente de procesare, stocare, comunicații, software virtualizare) în cadrul fiecărui Centru de Date în parte;
- achiziţia de licenţe şi echipamente specializate pentru securitate cibernetică perimetrală. Securitatea va fi asigurată de administratorul infrastructurii de Cloud guvernamental.

Grup țintă: Administrația publică centrală și locală, ecosistemul digital guvernamental.

Ajutor de stat:

Investițiile/serviciile necesare implementării acestor măsuri vor fi achiziționate printr-o procedură competitivă, transparentă, nediscriminatorie și necondiționată, nefiind incidente astfel prevederile legislației din domeniul ajutorului de stat.

Calendar: 2021 – 2025

I2. Investitii pentru dezvoltarea/migrarea în cloud (Alocare 187,05 mil. euro)

Provocări: Tehnologiile folosite în prezent în cadrul instituțiilor publice care oferă servicii digitale au un grad redus de interoperabilitate și adesea sunt depășite din punct de vedere tehnologic.

Obiectiv: Tehnologiile folosite în prezent în cadrul instituțiilor publice vor fi upgradate și vor deveni cloud-ready. În paralel, noi aplicații, cloud-native vor fi create pentru migrarea în cloud.

Implementare:

Conform celor prezentate în cadrul Reformei 1, un consultant extern va efectua o analiză a serviciilor digitale publice curente și a condițiilor de dezvoltare și migrare ale acestora în cloud.

În prezent, nu există un inventar al aplicațiilor digitale la nivelul administrației publice. Așadar, mutarea în cloud a ecosistemului digital va presupune analiza specifică și inventarierea aplicațiilor existente cu un nivel adecvat al virtualizării cloud-ready, dar, mai ales și preponderent, ale acelor care trebuie dezvoltate cloud-native/cloud-ready. De asemenea, analiza va evidenția măsurile și soluțiile tehnice necesare creșterii gradului de accesibilitate a serviciilor digitale de către utilizatorii vulnerabili, cum ar fi, dar fără a se limita la, persoanele cu dizabilități, persoanele în vârstă sau a celor cu un nivel scăzut al competențelor digitale etc.

Analiza se va realiza la nivelul fiecărei instituții din administrația publică centrală, de către ADR, care va coordona și lansarea procedurilor de achiziții publice.

Un număr minim de aplicații cloud - ready/ virtualizate vor fi migrate în cloud. Cu toate acestea, pe baza discuțiilor cu principalii furnizori/gazde (STS, ADR), majoritatea serviciilor vor necesita refactoring /reproiectare de la zero. Migrarea /refactorizarea va necesita o analiză specifică de business (astfel cum este aceasta menționată în cadrul reformei 1), având în vedere soluțiile alternative / sistemele vechi utilizate.

Grup țintă: administrația publică, autorități publice în domentiul ITC și digitalizării, entități producătoare de aplicații informatice.

Ajutor de stat:

Investițiile/serviciile necesare implementării acestor măsuri vor fi achiziționate printr-o procedură competitivă, transparentă, nediscriminatorie și necondiționată, nefiind incidente astfel prevederile legislației din domeniul ajutorului de stat.

Calendar: 2021 -2026

I3. Realizarea sistemului de eHealth și telemedicină (Alocare 400 mil. euro)

Provocări:

Conceptul de „sănătate digitală“ care include atât m-sănătatea (sănătatea mobilă), cât și e-sănătatea, descrie utilizarea generală a TIC - Tehnologiei Informației și Comunicației (aplicații digitale, mobile, wireless, platformă cloud etc.) pentru furnizarea serviciilor de asistență medicală. De asemenea, este folosit cu accepțiunea de „domeniu al cunoașterii și practicii asociat cu dezvoltarea și utilizarea tehnologiilor digitale pentru îmbunătățirea sănătății. Sănătatea digitală extinde conceptul de e-sănătate pentru a include consumatorii digitali, cu o gamă mai largă de dispozitive inteligente și conectate. De asemenea, înglobează și alte utilizări ale tehnologiilor digitale pentru sănătate, precum internetul obiectelor, învățarea automată, inteligența artificială, tehnica avansată de calcul, analiza volumelor mari de date și robotica.“ (Organizația Mondială a Sănătății 2020).

O cercetare națională recentă realizată de UNICEF (2020) la nivelul utilizatorilor serviciilor de sănătate digitală evidențiază situația actuală a sănătății digitale din perspectiva acestora: cetățenii și comunitățile preferă să vadă un medic în persoană decât prin telemedicină; nu există o structură centrală de implementare și monitorizare a politicilor din domeniul sănătății digitale; actorii de decizie din domeniu sunt împiedicați atât de nivelurile scăzute de capacitate tehnică, cât și de lipsa de date, de dovezi și de consens pentru elaborarea politicilor eficiente; lipsesc competențele în gestionarea proceselor digitale în rândul profesioniștilor - există o mulțime de proceduri pe care medicii de familie trebuie să le respecte și în general, majoritatea folosesc doar sisteme de calcul în scopuri administrative, cu consultațiile medicale scrise doar pe hârtie. Companiile care furnizează soluțiile digitale nu permit analiza ușoară a datelor, iar în prezent majoritatea medicilor de familie folosesc doar 20% din potențialul sistemelor lor; o parte din sistemele informatice ale CNAS sunt depășite din punct de vedere tehnologic; sistemul de telemedicină în zonele rurale nu este operațional. Sectorul privat oferă niveluri de servicii „normale”, dar la un preț ridicat; nu există încredere în schimbul de date și informații și nu există tablouri de bord care să permită managerilor și planificatorilor să știe ce este nevoie, cine are nevoia și unde; fluxurile majore de date sunt către CNAS în scopuri de plată.

După cum precizează propunerea de strategie mondială pentru sănătatea digitală a Organizației Mondiale a Sănătății „Pentru a-și realiza potențialul, inițiativele privind sănătatea digitală trebuie să facă parte dintr-un ecosistem de sănătate și digital mai larg și să fie călăuzite de o strategie robustă, care integrează leadershipul și resursele financiare, organizaționale, umane și tehnologice.“

Astfel, în strânsa dinamica cu problemele cu care se confruntă în prezent sistemul de sănătate, următoarele componente de sănătate digitală sunt prezentate și propuse în cadrul acestui program:

1. Redimensionare, standardizare și optimizare a Platformei informatice din asigurările de sănătate (PIAS).
2. Digitalizarea instituțiilor cu atribuții în domeniul sanitar aflate în subordinea MS.
3. Investiții în sistemele informatice și în infrastructura digitală a unităților sanitare publice.

4. Telemedicina și sisteme mobile de monitorizare a pacienților.

În același timp, sistemul național de date medicale va fi complet interoperabil cu sistemul European Health Data Space.

1. Redimensionare, standardizare și optimizare a Platformei informatice din asigurările de sănătate (PIAS)

Activitatea Casei Naționale de Asigurări de Sănătate (CNAS) presupune îndeplinirea unor funcții specifice domeniului asigurărilor sociale de sănătate. Acestea presupun administrarea fondurilor colectate de la contribuabili precum și finanțarea serviciilor medicale necesare asiguraților. Platforma informatică din asigurările de sănătate (PIAS) gestionată de Casa Națională de Asigurări de Sănătate, cuprinde Sistemul informatic unic integrat (SIUI), Sistemul național al cardului de asigurări sociale de sănătate (CEAS), Sistemul național de prescriere electronică (SIPE) și Sistemul dosarului electronic de sănătate al pacientului (DES) și gestionează un număr de peste 18 milioane de persoane beneficiare de servicii medicale și medicamente, un număr de peste 70.000 de utilizatori reprezentând furnizori de servicii medicale și medicamente, peste 700.000 de servicii raportate și validate zilnic, din care aproximativ 200.000 sunt prescripții medicale, datele fiind structurate în peste 420.000 tabele format Oracle. CNAS are în subordine 43 de case de asigurări de sănătate județene și cea a municipiului București.

Informațiile administrative despre asigurați provin din diverse surse externe CNAS, astfel, există un număr de aproximativ 22 instituții cu care CNAS schimbă date într-un mod nestandardizat și ineficient.

Echipamentele (hardware) din PIAS au fost achiziționate începând cu 2002 şi majoritatea sunt perimate, „end of production", „end of life" nu se mai produc piese de schimb pentru înlocuirea celor defecte și nu se mai poate asigura atingerea obiectivelor funcționale, având în vedere creșterile importante ale numărului de furnizori şi de servicii medicale de la cele de la nivelul anului 2002 la cele din prezent.

În plus, operațiile cu datele din PIAS se fac direct pe baza de producție, datele sunt accesate simultan de foarte mulți utilizatori iar volumul acestor date fiind mare, procesul este îngreunat, ajungându-se des la blocaje și chiar la necesitatea reinițializării proceselor.

La momentul actual, în comparaţie cu evoluţia tehnologică hardware şi software, cu creşterea exponenţială a numărului de contracte şi a serviciilor medicale oferite, precum şi cu continuele cerinţe de interoperabilitate cu alte sisteme la nivel naţional şi european, tehnologiile PIAS sunt perimate şi grav subdimensionate. Din aceste motive, funcţionarea PIAS este deficitară iar operarea la nivelul furnizorilor de servicii medicale se face cu timpi mari de întârziere, în deficitul asiguratului. Acest lucru este ușor de constatat chiar și în perioade normale când accesul și interacțiunea cu sistemul din partea celor care oferă servicii medicale este extrem de lentă și anevoioasă, creând blocaje și făcând se piardă timp prețios de către personalul medical și cetățeni. Având în vedere magnitudinea problemelor și disfuncționalităților, singura soluție posibilă este reprezentată de redimensionarea PIAS, standardizarea și actualizarea acesteia la necesitățile actuale impuse de numărul efectiv al conexiunilor și de cerințele de prelucrare a datelor.

Obiectiv:

Obiectivele acestei investiții sunt următoarele:

- reducerea timpilor de lucru atât pentru furnizorii de servicii medicale cât și pentru angajații CNAS/CAS, în interesul direct al cetățeanului;
- asigurarea unei funcționări optime și performante;
- asigurarea securității cibernetice a sistemelor din cadrul PIAS cu implementarea normelor GDPR;
- consolidarea capacității instituțiilor centrale, regionale și locale din domeniul sănătății de a gestiona digital datele din sistemul de sănătate;
- îmbunătățirea integrării verticale și orizontale a instituțiilor sanitare din România prin intermediul infrastructurii digitale;
- accelerarea adoptării soluțiilor de telemedicină și eficientizarea proceselor implicate;
- creșterea gradului de accesibilitate a serviciilor digitale ale PIAS pentru utilizatorii vulnerabili, cum ar fi persoanele cu dizabilități sau cerințe speciale, vârstnicii, persoanele cu un nivel limitat de competențe digitale etc.

Deficiențele tehnologice ale PIAS fac ca CNAS să nu reușească integrarea corectă cu sistemele informatice ale furnizorilor de servicii medicale aflați în contract. De asemenea, vechimea tehnologiilor și soluțiilor arhitecturale ale PIAS fac ca platforma să nu poată opera cu modulele recomandate la nivel european (building blocks europene) făcând sistemul ilizibil și deseori inaccesibil pentru furnizorii sau asiguratorii transfrontalieri din UE. Singura soluţie este refacerea pe bază de soluţii noi şi pe baza unei reproiectări complete, rezultată şi din viziunea europeană asupra domeniului sănătăţii (building blocks).

În concluzie, PIAS gestionează un volum enorm de date pentru procese de lucru și funcționalități care se bazează pe o platformă informatică perimată moral și fizic, a fost completată la diverse momente de timp cu funcționalități în diverse tehnologii prin proiecte adiacente, a devenit subdimensionată și perimată tehnologic, fiind absolut necesar să fie redimensionată și standardizată, motiv pentru care se justifică proiectul „Redimensionare și standardizare sistem informatic CNAS.

Rezultatele proiectului vor fi concretizate în instrumente informatice flexibile, reutilizabile și interoperabile. Pentru a atinge un nivel al serviciilor conform cu arhitectura europeană de interoperabilitate va fi asigurată migrarea și integrarea în structurile de date existente a tuturor datelor disponibile, astfel încât acestea să susțină funcționarea în timp real a serviciilor oferite. Totodată implementarea funcționalităților va implica alinierea infrastructurilor de identificare și autorizare națională cu cele ale statelor membre ale UE, într-o schemă transnațională, conform regulamentului EIDAS. În realizarea proiectului se vor respecta prevederile Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, aprobat prin Hotărârea nr. 271/2013.

Proiectul își propune realizarea unui proces complex de integrare, standardizare, planificare, coordonare, sincronizare, armonizare şi desfăşurare a acţiunilor în spaţiul cibernetic pentru protecţia, controlul şi utilizarea reţelelor de calculatore în scopul obţinerii superiorităţii informaţionale, concomitent cu neutralizarea amenințărilor.

Pentru asigurarea securităţii cibernetice se vor stabili şi aplica profile şi cerinţe de securitate adaptate și conforme cu infrastructurile cibernetice naţionale și europene, relevante din punct de vedere al funcţionării corecte a infrastructurilor critice cu asigurarea rezilienţei infrastructurilor cibernetice. Prin proiect se va asigura starea de securitate prin cunoaşterea, prevenirea şi contracararea vulnerabilităţilor, riscurilor şi ameninţărilor la adresa securităţii cibernetice, prin definirea, stabilirea și aplicarea unui set de măsuri specifice la standarde internaționale privind utilizarea spaţiului cibernetic.

În cadrul proiectului se va dezvolta un ansamblu de măsuri proactive şi reactive prin care se va asigura confidenţialitatea, integritatea, disponibilitatea, autenticitatea şi nonrepudierea informaţiilor în format electronic, a resurselor şi serviciilor publice sau private, din spaţiul cibernetic. Măsurile proactive şi reactive vor include politici, concepte, standarde şi ghiduri de securitate, managementul riscului, activităţi de instruire şi conştientizare a utilizatorilor sistemului, implementarea de soluţii tehnice de protejare a infrastructurilor cibernetice, managementul identităţii, managementul consecinţelor. Aceste măsuri vor asigura apărarea cibernetică prin monitorizare, analiză, detectare, contracarare a agresiunilor şi asigurare a răspunsului oportun împotriva ameninţărilor cibernetice specifice.

Implementare:

Un prim pas în implementarea acestei investiții este evaluarea sistemului PIAS funcțional în prezent, în vederea cartografierii infrastructurii disponibile (hardware, software), identificarea vulnerabilităților tehnice, problemelor de capacitate și oportunităților de integrare cu alte sisteme din domeniul medical din România. În funcție de nevoile identificate la acest nivel, echipamentele care susțin PIAS la nivel național și județean vor fi adaptate la exigențele tehnice ale prezentului, atât la nivel de performanță, cât și în ceea ce privește siguranța informațiilor. Acest demers va remedia problemele existente privind fiabilitatea sistemului, crescând în același timp capacitatea acestuia, în pregătirea elementelor noi la nivel de funcționalitate.

În detrimentul înlocuirii integrale a PIAS cu alt sistem, operațiune asociată invariabil limitarea accesului la servicii medicale în perioada de tranziție de la un sistem la altul, CNAS va lucra împreună cu Casele de Asigurări de Sănătate la nivel județean și cu Casa Asigurărilor de Sănătate a Apărării, Ordinii Publice, Siguranței Naționale și Autorității Judecătorești (CASA OPSNAJ) pentru a schimba sistemul în mod incremental, fără a perturba funcționarea acestuia.

La nivel de dezvoltare a soluției software, investiția va urmări transformarea PIAS dintr-un sistem aparent modular, cu funcționalitate fragmentată, într-un sistem e-health ce funcționează ca un tot unitar, deservind în timp real nu doar plătitorul din sistemul de sănătate (CNAS), ci și mai ales nevoile pacienților. Pentru a atinge acest obiectiv, interfața modulelor PIAS (SIUI, CEAS, DES, SIPE) va suferi modificări pentru:

- a asigura un mediu prietenos și accesibil pentru utilizatori, inclusiv cei cu dizabilități;
- a îmbunătăți interconectarea și interoperabilitatea acestor sisteme;
- a permite funcționalități noi (ex. digitalizarea unor documente conexe actului medical);
- a optimiza fluxurile de date, monitorizarea electronică a obiectivelor generale, obiectivelor specifice, activităților și indicatorilor de performanță asumați la nivelul CNAS/CAS/furnizor de servicii medicale;
- permite interoperabilitatea sistemelor informatice la nivelul administrației publice inter instituțional, utilizarea datelor organizaționale încrucișate și a resurselor existente la nivel național (în linie cu celelalte investiții planificate la acest nivel).

2. Digitalizarea instituțiilor cu atribuții în domeniul sanitar aflate în subordinea MS

Analiza datelor de sănătate la nivel național este incompletă și ineficientă. Datele sunt incomplete, fragmentate, nesigure, nestructurate, nestandardizate și de multe ori non-electronice. Nu există un cadru sistemic de guvernanță a datelor pentru a aborda calitatea datelor și schimbul eficient al acestora in cadrul diferitelor institutii administrative, furnizori de servicii, pacienți. Deși mari volume de date colectate există, acestea nu sunt vizibile pentru toate instituțiile din sistemul de sănătate. Bazele de date CNAS, deși bogate în conținut de informații, sunt în mare parte legate de activitatea de bază a asigurărilor și nu sunt ușor accesibile pentru Ministerul Sănătății și pentru alte părți interesate. Calitatea datelor colectate de la furnizori și instituții este scăzută deoarece sunt furnizate aceeasi tipuri de date în template-uri diferite, făcând dificilă corelarea și interpretarea lor. Ministerului Sănătății îi lipsește capacitatea de administrare pentru a face față fragmentării informațiilor despre sănătate și pentru a se coordona între agenții. Nu există un serviciu centralizat de schimb de date medicale făcând dificilă coordonarea multiplelor sisteme de informații însoțită și de bariere instituționale și tehnice semnificative. Deși majoritatea furnizorilor au un fel de sisteme informatice computerizate, lipsa unei platforme de standardizare a guvernanței datelor nu permite introducerea eficientă a indicatorilor de performanță și a mecanismelor de asigurare a calității necesare pentru metodele de plată bazate pe performanță. De aceea, instituțiile cu atribuții în domeniul sanitar aflate în subordinea MS vor trebui să conlucreze cu o baza de date informatică comună.

Având în vedere cele menționate mai sus, dezvoltarea unor module informatice noi care să deservească activitatea Ministerului Sănătății și a instituțiilor din subordinea sa, se impune. Astfel, va fi demarat un proces de digitalizare, prin achiziționarea și instalarea echipamentelor necesare (echipamente IT, echipamente pentru comunicații, și echipamente conexe, inclusiv licențe), dezvoltare de aplicații informatice aferente, dar și prin instruirea personalului tehnic la nivel local.

Instituțiile în subordinea Ministerului Sănătății pentru care se urmărește această digitalizare vor include în principal direcţiile de sănătate publică judeţene (inclusiv cea a municipiului Bucureşti, Serviciile de ambulanţă judeţene (inclusiv Serviciul de Ambulanţă Bucureşti - Ilfov), Institutul

Naţional de Sănătate Publică, Institutul Naţional de Medicină Sportivă, Institutul Naţional de Hematologie Transfuzională "Prof. Dr. C.T. Nicolau", Agenţia Naţională de Transplant, Oficiul Central de Stocare pentru Situaţii Speciale, Registrul Naţional al Donatorilor Voluntari de Celule Stem Hematopoietice, Agenţia Naţională a Medicamentului şi a Dispozitivelor Medicale, institutele de medicina legala, Centrul Naţional de Sănătate Mintală şi Luptă Antidrog Bucureşti, Şcoala Naţională de Sănătate Publică, Management şi Perfecţionare în Domeniul Sanitar Bucureşti.

Lista finală a instituțiilor și gradul de digitalizare ce vor fi atinse în cadrul proiectului va depinde de bugetul final necesar, având în vedere suma alocată pentru această sub-componentă.

Pentru fiecare investiție în parte se va realiza procedura de licitație deschisă urmând ca criteriile de selecție să aibă la bază cel mai bun raport calitate-pret cu proceduri de atribuire care oferă posibilitatea de a alege cea mai avantajoasă ofertă din punct de vedere al calității și expertizei tehnice și totodată încadrarea în limitele bugetului alocat.

3. Investiții în sistemele informatice și în infrastructura digitală a unităților sanitare publice

Dificultățile de colaborare dintre spitale și Ministerul Sănătății (inclusiv serviciile furnizate prin contractul cu CNAS dar și programele naționale de sănătate) îngreunează revizuirea cheltuielilor de sănătate și a modelelor de utilizare a bugetelor alocate. Lipsa unei platforme de standardizare a guvernanței datelor limitează comunicarea între sisteme și împiedică introducerea unor mecanisme de asigurare a calității pentru a responsabiliza furnizorii pentru performanță.

Aceste investiții au ca scop:

- contribuția directă la îmbunătăţirea calităţii serviciilor şi a coerenţei episodului de îngrijire medicală;
- îmbunătățirea comunicaţiilor dintre toate părţile implicate în serviciile de sănătate
- contribuția la accesul rapid şi sigur al cetăţenilor şi sau al pacienţilor la propriul dosar de sănătate şi de asemenea la informaţii privind serviciile şi calitatea îngrijirilor medicale
- o mai bună administrare şi management al serviciilor de sănătate;

Se urmărește înlocuirea, acolo unde este cazul, infrastructurii IT a spitalelor publice din România, dar și migrarea de date către noile sisteme de date și infrastructură.

Îmbunătățirea rețelelor de comunicare la un număr de spitale aflate în subordinea MS va sprijini eforturile de a construi sisteme IT care să permită identificarea și reducerea cheltuielilor de sănătate ineficiente și să promoveze managementul performanței în furnizarea de servicii. De asemenea va îmbunătăți supravegherea epidemiologică, care poate oferi detectarea exactă la timp a modificărilor incidenței, mortalității în anumite boli cu impact major epidemiologic.

În principal, se dorește achiziția și implementarea de sisteme informatice spitalicești integrate (SIS) pentru conectarea tuturor sistemelor de înregistrare și administrare digitale, și care ar permite completarea computerizată a comenzii medicului (CPCM) - un proces de introducere electronică a instrucțiunilor medicului pentru tratamentul pacienților (în special pacienților spitalizați) aflați sub îngrijirea sa, astfel ca medicii să acceseze elementele SIS de la pat.

Luarea de decizii bazate pe date va facilita MS în introducerea unei platforme centralizate de schimb de date interoperabile, aplicarea algoritmilor adaptivi care identifică cheltuielile ineficiente în sectorul sănătății și consolidarea rolului de administrare a MS în traducerea datelor disponibile în responsabilitate pentru furnizorii de servicii medicale și instituțiile implicate în furnizarea de servicii, promovarea eficienței cheltuielilor publice pentru sănătate.

4. Telemedicina și sisteme mobile de monitorizare a pacienților

Telemedicina reprezintă furnizarea de servicii medicale și îngrijiri pentru pacienți la distanță sau cu personal instruit folosind echipamente moderne de investigații imagistice și de laborator avansate conectate la tehnologiile de telecomunicații și calculatoare. Acesta include întregul spectru de livrare de îngrijiri medicale: de la screening-ul medical de prevenție și monitorizarea bolilor cronice la îngrijirea cazurilor acute și la îngrijirea și reabilitarea post spitalicească.

Telemedicina se conturează tot mai pregnant ca unul dintre cele mai importante domenii de dezvoltare ale activităţii medicale la nivel mondial.

Tocmai de aceea, extinderea sistemelor de telemedicină în România a cunoscut în ultimii ani o dinamică remarcabilă, cuplată în special cu dezvoltarea sistemului de medicină de urgenţă, astfel încât există în acest moment 3 reţele inter-spitaliceşti majore şi o reţea integrată în asistenţa de urgenţă prespitalicească.

Având în vedere că ameliorarea accesibilităţii populaţiei la servicii de sănătate în zonele rurale sau greu accesibile reprezintă, de asemenea, o prioritate esenţială a politicilor de sănătate la nivel naţional, este necesară o nouă direcţie de dezvoltare a sistemelor de telemedicină, prin constuirea de astfel de reţele şi în mediul rural, care să asigure rezolvarea mai rapidă a problemelor medicale ale populaţiei şi care să fie mai puţin costisitoare, atât pentru pacient cât şi pentru sistemul de sănătate.

Spre deosebire de reţelele deja existente în România, care fac legături între spitale sau între spitale şi serviciile de urgenţă prespitalicească şi care se concentrează pe rezolvarea extrem de rapidă a urgenţelor medicale pentru pacienţii critici, sistemul informatic de telemedicina pentru zonele rurale propune realizarea unei conexiuni între cabinetele de medici de familie şi spitalele judeţene (medicii specialisti) şi vor fi axate în special pe consultatii de specialitate la distanţă pentru patologii cronice. Acest sistem are la bază ideea de ajutor a pacienților greu deplasabili sau care se află în zone greu accesibile, ajutând prin acest deziderat la creșterea calității serviciilor medicale oferite acestor pacienți.

Prin intermediul prezentului proiect se asigură premisele pentru realizarea unor servicii electronice de o calitate sporită, care au drept scop final un acces facil și eficient al părților interesate la aceste tipuri de servicii.

Nu în ultimul rând, telemedicina este una din componentele strategiei de e-Health a Comunităţii Europene, enunțate încă din anul 2004, potrivit căreia, până la sfârşitul anului 2008, ţările europene ar fi trebuit să fie capabile să asigure sisteme de tele-consultaţie, prescriere electronică, telemonitoring şi teleCare.

Totodată, implementarea sistemului de telemedicină va asigura un important progres către alinierea cu realităţile existente în prezent în Uniunea Europeană.

Obiectivul general al proiectului de telemedicina este reprezentat de creșterea calității actului medical și îmbunătățirea gradului de sănătate socială prin diversificarea serviciilor de sănătate ocazionate de implementarea Sistemului Informatic de Telemedicină, oferite comunităților și cetățenilor, care nu au acces la îngrijire medicală din zona rurală și urbanul mic.

Obiectivele specifice sunt următoarele:

- Realizarea la nivelul medicului de familie a managementului bolilor cronice cu impact major în populație, cu sprijinul medicilor specialiști prin sistemul de telemedicină;
- Furnizarea de servicii medicale de specialitate ambulatorii postspitalizare pacienților externați din spitale prin intermediul telemedicinei;
- Facilitarea accesului populației din zona rurală și urbanul mic la servicii ambulatorii de specialitate cu ajutorul soluțiilor de telemedicină;
- Expertiză medicală disponibilă în mod egal, independent de locul unde trăiește pacientul;
- Creșterea gradului de accesibilitate a serviciilor de telemedicina și sisteme mobile de monitorizare a pacienților pentru utilizatorii vulnerabili, cum ar fi persoanele cu dizabilități, vârstnicii, persoanele cu un nivel limitat de competențe digitale etc.
- Reducerea timpului de accesare și așteptare pentru anumite servicii medicale
- Creșterea accesului gravidelor la informații, educație prenatală, la consultații și la a doua părere cu ajutorul soluțiilor de telemedicină, în special pentru gravidele din zone cu un procent mare de sarcini neurmărite.
- Creșterea informării și a educației pentru prevenirea sarcinilor în rândul adolescenților și a femeilor care nu își doresc o sarcină. Acces la planning familial pentru populația vulnerabilă, care nu ajunge la consultații în cabinet de obicei.
- Oferirea de informații și servicii de calitate către pacienți;
- Îmbunătățirea calității deciziilor medicale prin asigurarea unei mai mari disponibilități a informațiilor existente în format electronic;

- Îmbunătățirea eficienței și productivității serviciilor de sănătate prin reducerea muncii administrative de rutină, datorită informațiilor existente în format electronic;
- Asigurarea unei pregătiri continue a personalului medical;
- Asigurarea utilizării adecvate a resurselor locale și regionale.

Proiectul de față propune o serie de activități care au ca finalitate implementarea soluțiilor de telemedicină: tele-consultația între pacient și medicul de familie, tele-consultația între medicul specialist și pacient, direct sau indirect prin medicul de familie, tele investigații, tele monitorizare la domiciliu. Aceste soluții de telemedicină sunt menite să rezolve problemele de acces identificate în sistemul furnizării serviciilor de sănătate din zona rurală și urbanul-mic, ținând cont că medicii specialiști au cea mai mare concentrate pe centrele universitare. Astfel se preconizează ca un număr de 200 000 de consultații de telemedicină vor avea loc până la finalizarea perioadei de implemenatre a investiției (Q2 2025). De asemenea, prin interoperabilitatea între soluțiile de telemedicină și dosarul electronic al pacientului se va reduce costul cu anumite investigații medicale.

Telemedicina curentă și activitățile de e-sănătate (TM & eS) pot fi clasificate în funcție de tehnologia utilizată, de tipul de activitate, sau grupul țintă. Una dintre cele mai importante aspecte ale clasificării este distincția între timp real și înmagazinează și dă mai departe.

Există două tipuri majore de activități TM & eS:

- sincrone, sau în timp real implică contactul în timp real direct între furnizorul de servicii de TM (de exemplu, un medic specialist de la distanță) și utilizatorul final (cum ar fi un pacient sau un medic de familie), prin videoconferinte, sau transmisie de date în timp real (ecografie, EKG, analize de laborator, radiologie, informații de la sistemele de monitorizare pacienți etc).

În acest tip de serviciu, exemplu clasic este video consultația, unde interacțiunea dintre participanți este "vie", și ei pot interacționa imediat, monitorizarea afecțiunilor cronice cu ajutorul dispozitivelor inteligente cu senzori, BT și WIFI. Avantajul acestei abordări este acela că permite un transfer optim de informații între participanți.

- asincrone, sau stochează și dă mai departe - presupune colectarea datelor pacientului (cum ar fi imagini sau clipuri video, diagrame EKG, rapoartele de laborator, imagini radiologie sau diapozitive patologie) și le trimite mai târziu la un site la distanță pentru analizarea, diagnosticarea și planificarea tratamentului.

Stocarea și transmiterea datelor medicale sunt mai puțin costisitoare și mai ușor de gestionat deoarece nu există nici o interacțiune "în direct". Un participant adună informații (texte, date, imagini, etc), în format electronic și îl trimite la alt participant, care le analizează la un moment convenabil ulterior și transmite înapoi. Exemplul clasic este aici a doua opinie.

Sistemul de telemedicină propus va trebui să permită lucrul în ambele variante funcție de complexitatea bolii, gradul de acutizare a acesteia și disponibilitatea medicilor specialiști.

Sistemul va fi proiectat ca un sistem de sine stătător care va pune la dispoziția utilizatorilor funcționalități de telemedicină și care se va interfața și cu alte sisteme informatice în scopul realizării acestor funcționalități.

În conformitate cu Regulamentul Parlamentului European și al Consiliului de Instituire a Mecanismului de Redresare și Reziliență, toate soluțiile digitale dezvoltate sau contractate prin Planul Național de Redresare și Reziliență vor fi implementate în concordanță cu articolul 12 al acestui regulament, care indică utilizarea de soluții cu sursă deschisă. De asemenea, programele, aplicațiile și platformele dezvoltate vor fi aliniate cu prevederile Cadrului European de Interoperabilitate care indică, cu precădere la nivelul administrației locale, utilizarea tehnologiilor și a produselor software cu sursă deschisă ca un element esențial pentru reducerea costurilor de dezvoltare, a timpului și efortului de implementare, pentru standardizare și încurajarea cooperării între instituții, respectând principiul fundamental al EIF (European Interoperability Framework) privind reutilizabilitatea. Acestor măsuri li se adaugă și programul ISA2 al Uniunii Europene care cuprinde Cadrul de Partajare și Reutilizare a soluțiilor informatice dezvoltate de către și/sau pentru administrația publică și care are ca obiective" reducerea costurilor, creșterea eficienței acestora și promovarea interoperabilității prin reutilizarea, partajarea sau dezvoltarea în comun a soluțiilor informatice care îndeplinesc cerințele comune". În vederea creșterii gradului de accesibilitate a serviciilor de telemedicină soluțiile digitale implementate vor respecta legislația și cadrul normativ al UE privind accesibilitatea la serviciile digitale a diverselor categorii de utilizatori vulnerabili.

Pentru toate aceste reforme și investiții mai sus menționate, calendarul detaliat de implementare este următorul:

Activități	*2021*	*2022*		*2023*		*2024*		*2025*		*2026*	
	S2	*S 1*	*S 2*	*S 1*	*S 2*	*S 1*	*S 2*	*S 1*	*S 2*	*S 1*	*S 2*
Realizarea unei analize complete a nevoilor sistemului e-health (Platforma Informatică a Asigurărilor de Sănătate + module noii), realizată de Ministerul Sănătății: · Evaluare Platforma Informatică a Asigurărilor de Sănătate · Analiză nevoi telemedicină · Strategie registre de boală											
Redimensionarea Platformei Informatice a Asigurărilor de Sănătate și standardizarea Platformei Informatice a Asigurărilor de Sănătate în conformitate cu soluția aleasă și cu											

standardele europene;											
Optimizarea fluxurilor de date, monitorizarea electronică a obiectivelor generale, obiectivelor specifice, activităților și indicatorilor de performanță asumați la nivelul CNAS/CAS/furnizor de servicii medicale;											
Interoperabilitatea sistemelor informatice la nivelul administrației publice, inter-instituțional											
Digitalizarea instituțiilor cu atribuții în domeniul sanitar aflate în subordinea Ministerului Sănătății											
Realizarea de investiții în sistemele informatice și în infrastructura digitală a unităților sanitare publice;											
Asistență tehnică pentru dezvoltarea și integrarea soluțiilor de sănătate digitală în sistemul de sănătate.											
Monitorizare & evaluare											

Grup țintă: MS, personal medical, populația generală

Ajutor de stat: Investițiile/serviciile necesare implementării acestor măsuri vor fi achiziționate printr-o procedură competitivă, transparentă, nediscriminatorie și necondiționată, nefiind incidente astfel prevederile legislației din domeniul ajutorului de stat.

Calendar: 2021 - 30 iunie 2025.

I4. Digitalizarea sistemului judiciar (Alocare 162,31 mil. euro)

Provocări: Provocările pe care sistemul judiciar trebuie să le depășească vizează aspecte precum: procese de lucru birocratice, utilizarea documentelor preponderent pe hârtie, sisteme IT fragmentate/insulare, multe camere tehnice (data rooms) instalate în diverse autorități publice, dar nici un centru de date/data center. Totodată, resursele tehnice și umane sunt limitate. La nivel de guvernare IT sunt carențe de coordonare între diversele entități ale sistemului judiciar, iar interoperabilitatea este limitată infra-sector. Pe de altă parte, capabilitățile de raportare, generarea de analize complexe și statistice sunt reduse, inclusiv pentru publicarea de date deschise. Această situație generează riscuri inerente de securitate cibernetică și în continuitatea operațională/business continuity.

Obiectiv: In cadrul Componentei 14 *Buna guvernanță*, reforma 5 vizează *Asigurarea independenței sistemului judiciar, îmbunătățirea calității și eficienței acestuia* prin pregătirea unei noi strategii pe baza analizelor interne și a propunerilor primite în timpul procesului de consultare publică. În cadrul celui de-al doilea pilon al strategiei, vor fi incluse politici de consolidare a capacității instituționale cu privire la resurse, procese și gestionare precum utilizarea eficientă a resurselor umane, politica de optimizare a infrastructurii instanțelor judecătorești și transformare digitală.

Investiția propusă pentru transformarea digitală a sistemului judiciar vizează trecerea la documente electronice simultan cu accelerarea utilizării semnăturilor și sigiliilor electronice, modernizarea registrelor naționale, creșterea interoperabilității cu autorități publice naționale și din UE, întărirea securității cibernetice și a guvernanței IT, pentru îmbunătățirea accesului la informație și eficientizarea proceselor în tot sistemul judiciar.

Transformarea digitală cuprinde mai multe măsuri integratoare și de suport prin care se urmărește generalizarea utilizării documentelor electronice, inclusiv a probelor în format digital, simultan cu accelerarea utilizării semnaturilor și sigiliilor electronice. Atingerea acestui obiectiv este condiționată și de o întărire a interoperabilității și securității cibernetice. Odată atins acest obiectiv crește schimbul de date pe plan național, precum și cooperarea transfrontalieră în materie civilă și penală. Accesul la justiție este urmărit și prin alte politici precum optimizarea infrastructurii judiciare.

Implementare: Transformarea digitală în cadrul sistemului juridic se va face etapizat, cu respectarea principiilor EU de „sharing and reuse", „once only" și „user centric", prin adoptarea urmatoarelor măsuri:

Etapa I (2021-2022)

Ministerul Justitiei se află deja în prima etapa de implementare a sistemului RMS (management financiar, resurse umane etc.) și de utilizare a unui document management system. Se urmărește ca aceste sisteme să fie folosite în întreg sistemul judiciar. În perioada 2021-2022, va fi necesară aplicarea unor politici de întărire a capacității institutionale, respectiv de dezvoltare a guvernanței IT, prin care să se asigure coordonarea strategică pentru sectorul justiției și eficientizarea aspectelor de administrare IT de zi cu zi prin echipe operaționale, inclusiv pentru securitate cibernetică și protecție a datelor personale. Separat, va fi dezvoltată capacitatea de analiză și de realizare a unor statistici complexe, precum și de publicare de date deschise (open data). Se va face tranziția către utilizarea semnăturii electronice și a sigiliului electronic în întreg sistemul

judiciar. Se va întocmi un plan de acțiune pentru preluarea bunelor practici, naționale și internaționale și unde este posibil, sistemele IT tip dosar electronic existente în sistemul judiciar se vor generaliza la nivel național.

Etapa II (2022-2023)

În faza a doua, vor fi demarate majoritatea investițiilor. Astfel, spre exemplu, se va face up-gradarea sistemului ECRIS 4 prin tranziția de la severe locale (instalate în peste 200 de locații) la servere centrale, utilizate în comun prin virtualizare și utilizarea unitară a soluțiilor (extensiilor ECRIS) pentru administrarea dosarelor elecronice, precum și modernizarea infrastructurii (servere, storage, echipamente LAN/WAN) și dotarea cu stații de lucru și alte echipamente de tip birou pentru eficientizarea activității și reducerea riscurilor operaționale.

Tot în această etapă, raportat la tehnicile și tehnologiile utilizate pentru fiecare investiție în parte și aliniat la impactul acestora asupra politicilor de guvernanță IT, de securitate cibernetică pentru protecția datelor personale (GDPR) și de resurse umane pentru specialiștii IT din sectorul justiție, se va face actualizarea acestora. De asemenea, se va trece la generalizarea utilizării semnăturilor și sigiliilor electronice de către judecători, procurori, grefieri și parteneri majori (avocați, notari, executori judecatoresti).

Etapa III (2023 – 2026)

Această etapă se va focaliza pe finalizarea implementării și operaționalizării proiectelor angajate și se va urmări tranziția la ECRIS 5 și operaționalizarea acestuia. Simultan, se vor definitiva politicile care au suferit ajustări în etapele anterioare ceea ce va conduce la o abordare unitara IT cross sector justitie. Astfel, se va urmări întărirea politiciilor de securitate cibernetică (inclusiv continuitate operațională business continuity), protecției datelor personale și se vor extinde schimburile de date – interoperabilitate atât la nivel național, cât și cross EU, inclusiv cu sistemele e-Evidence Digital Exchange System (eEDES), eCODEX.

Toate investițiile și măsurile din etapele enumerate anterior privind transformarea digitală vizează instanțele, inclusiv Înalta Curte de Casație și Justitie, CSM, Ministerul Public, Ministerul Justiției și autoritătile publice subordonate.

Investițiile urmăresc:

• Pentru ECRIS 4 (versiunea curenta în exploatare de management de dosare), tranziția de la servere locale la servere centrale utilizate în comun prin virtualizare și, pe cât posibil, extinderea capabilităților de dosar electronic într-o abordare națională (acum există mai multe versiuni locale, la nivel de curți de apel, în exploatare). Totodată, se vor realiza achiziții de servicii pentru creșterea capacității de raportare, statistici și extragere de open data, inclusiv în ceea ce privește sistemul actual ECRIS 4;

• Modernizarea infrastructurii IT de la nivel local (instanțe, parchete, birouri etc): servere de management/administrare LAN, scanner, laptopuri, soluții de comunicații unificate (VoIP pentru Ministerul Justiției și instituții subordonate) și alte echipamente specializate pentru persoane cu dizabilități, inclusiv pentru asigurarea desfășurării activității în regim de telemuncă;

• Pornind de la situația actuală cu foarte multe camere de date (data rooms), pentru micșorarea riscurilor operaționale și a costurilor administrative, se construiește un centru de date integrat pentru sistemul judiciar;

• Îmbunătățirea capacităților privind securitatea cibernetică atât la nivel central, cât și la nivel local (în special instanțe, dar și parchete). Sunt incluse achiziția de echipamente, software, instruire și alte servicii pentru cyber security;

• Modernizarea dotării tehnice pentru supraveghere video, audio și alte echipamente specializate pentru alte procese critice (de ex., upgrade tehnologic pentru creșterea calității serviciilor de expertiză criminalistică, echipamente specializate de urmărire video și audio);

• Pentru trecerea de la arhive fizice la cele digitale, se va face un studiu și un proiect pilot la nivel de sistem judiciar și se va planifica detaliat digitizarea fondului arhivistic existent;

• Dezvoltarea de sisteme integrate pentru înregistrarea audio-video în sălile de judecată, transcrierea automată (speech2text) și programare videoconferințe (inclusiv integrare cu ECRIS V), având în vedere și rezultatele unei analize privind soluțiile de realizare a transmisiunilor live a ședințelor de judecată, pe Portalul Instanțelor.

Concomitent, pentru a reduce riscul operațional al sistemului existent de gestionare a cazurilor (Sistemul electronic de informare a înregistrărilor judiciare, versiunea ECRIS IV) și pentru a introduce o alternativă modernă pentru accesul electronic al dosarelor de caz se va proceda la următoarele:

- reducerea numărului de servere de la aproximativ 270 de locații la 60 de locații „virtualizarea” (dar nu centralizarea completă, imposibil de realizat din cauza limitării comunicării datelor pe termen scurt și a tehnologiei vechi pentru ECRIS IV);

- „centralizarea” celor 4 extensii existente ale fișierului electronic într-un singur „fișier electronic” național prin care justițiabilii vor putea accesa cu ușurință și în siguranță documentele din dosarele instanței.

Față de acestea, accelerarea și asigurarea unei tranziții ușoare la următoarea versiune a ECRIS (ECRIS V) devine un obiectiv strategic major. Astfel, scopul concret al „virtualizării și centralizării” propus în PNRR este îmbunătățirea tehnologică a infrastructurii IT a sistemului judiciar prin:

- creșterea capacității de transmisie a datelor în WAN (creșterea lățimii de bandă), necesară pentru buna funcționare a sistemului electronic de gestionare a cazurilor într-o configurație centralizată;
- asigurarea și capacitatea adecvată de procesare și stocare la nivelul tribunalelor și curților de apel pentru a centraliza cererile de justiție și a realiza o gestionare eficientă a resurselor IT în instanțe;
- creșterea securității și disponibilității serviciilor oferite publicului larg prin implementarea fișierului electronic național (fișier electronic).

Investițiile enumerate anterior vor crea premisele derulării facile și tranziției la nivel cross-sector și pentru o serie de aplicații precum:

• Generalizarea aplicațiilor/platformelor de tip document management în tot sistemul judiciar

• Generalizarea unei soluții tehnice destinate anonimizării hotărârilor judecătorești

Grup țintă: cetățenii care se adresează sistemului judiciar (pentru actul de justitie și informații din registrele naționale și alte date deschise), practicienii din sistemul judiciar: avocați, notari, executori, jurişti/consilieri juridici, personalul autorităților din sistemul judiciar: Consiliului Superior al Magistraturii, Înalta Curte de Casație și Justiție, instanțele de judecată, Ministerului Public și parchetele, Ministerul Justiției și autoritățile publice subordonate.

Ajutor de stat: Investițiile/serviciile necesare implementării acestor măsuri vor fi achiziționate printr-o procedură competitivă, transparentă, nediscriminatorie și necondiționată, nefiind incidente astfel prevederile legislației din domeniul ajutorului de stat.

Complementaritate cu alte surse de finanțare:

Prin Programul Operațional Capacitate Administrativă 2014-2020 se finanțează dezvoltarea efectivă a noului sistem electronic de management al cauzelor (ECRIS V), concomitent cu achiziționarea de software aferent și hardware pentru susținerea acestuia (parțial), precum și servicii de instruire a utilizatorilor. ECRIS V reprezintă elementul central al transformării digitale a sistemului judiciar. Prin PNRR se vor finanța măsuri suplimentare și complementare care să faciliteze tranziția la noul sistem și utilizarea eficientă a acestuia.

Calendar: 2021- 30 iunie 2026.

I5. Digitalizare în domeniul mediului (Alocare 52 mil. euro)

Provocări: România suferă, în mod sistemic și persistent, conform Comisiei Europene, de acces deficitar la informațiile legate de mediu, cum ar fi managementul deșeurilor, calitatea aerului, calitatea apei potabile, suprafața de spațiu verde în zonele urbane etc. Această situație este generată, pe de o parte, de evidența, colectarea și agregarea deficitară a datelor la nivel local și național, ceea ce se reflectă în calitatea scăzută a statisticilor, în discrepanțele mari dintre diferite baze de date care se referă la aceleași raportări (ex. date diferite la nivelul Min. Mediului, ANPM, AFM, GNM), precum și în accesibilitatea limitată sau inexistentă a acestor date de către public, pe site-uri ale diferitelor instituții, în formate diferite, care nu pot fi agregate sau a căror agregare relevă discepanțe majore.

Utilizarea raportărilor necorespunzătoare ca punct de referință pentru implementarea unor proiecte și planuri de acțiune concrete implică riscuri de eroare materială, cheltuieli supra sau subdimensionate, îngreunează și întârzie îmbunătățirea indicatorilor de performanță de mediu a României în ceea ce privește obiectivele asumate prin aderarea la UE.

Proiectul promovează politicile publice bazate pe dovezi, transparenţa guvernamentală, utilizarea de noi tehnologii în administraţie şi încurajarea participării civile la viaţa publică, prin colaborarea cu membrii comunității (cetățeni, ONG-uri, mediul academic, mediul privat) și cu

alte autorități și instituții publice. De asemenea, va asigura cadrul procedural pentru implementarea acțiunilor necesare respectării principiilor de guvernare deschisă, așa cum sunt acestea descrise în Open Data Partnership.

Obiectiv:

Implementarea unui sistem informatic integrat pentru susținerea dezvoltării durabile, îmbunătățirea infrastructurii și calității mediului, protecția naturii și conservarea biodiversității.

Dezvoltarea infrastructurii hardware și software prin extinderea serviciilor electronice în sistem informatic integrat de supraveghere, control și asigurare a integrității fondului forestier care va fi implementat utilizând soluții tehnologice mature, de tip enterprise, recunoscute pe plan intern și internațional.

Digitalizarea a 32 de servicii publice din domeniul mediului; monitorizarea și colectarea datelor de mediu, dezvoltarea sistemului online de depunere a documentelor, atât de persoane fizice cât și de persoane juridice.

Elaborarea unui serviciu informatic integrat de supraveghere, control, monitorizare a fondului forestier, utilizarea de solutii tehnologice pentru paduri si monitorizarea transportului de masa lemnoasa integrate prin utilizarea sistemelor de monitorizare video.

Implementare:

Sistemele informatice vor fi implementate de către Autoritatea publică centrală de mediu prin structurile aflate în coodonare și subordonare ale acesteia, respectiv Agenția Națională pentru Protecția Mediului la nivel central și prin structurile descentralizate, Garda Națională de Mediu, Regia Națională a Pădurilor, Garda Forestieră, precum și a structurilor regionale și județene.

Obiectivul sistemului informatic integrat de supraveghere, control și asigurare a integrității fondului forestier va utiliza sisteme și echipamente moderne de supraveghere și control.
Sistemul va avea o arhitectură distribuită, astfel:
• componenta centrală, în două centre de date de complexitate deosebită
Componenta informatică locală oferă abilitatea de a recepționa cantități mari de date dintr-o varietate de surse:

- sisteme de tip drone - aeronave fără pilot (UAV)
- sisteme satelitare
- sisteme video monitorizare a fondului forestier de a le analiza rapid și de a oferi rezultate semnificative într-o formă ușor de înțeles.

Sistemul informatic integrat de supraveghere, control și asigurare a integrității fondului forestier va fi implementat utilizând soluții tehnologice mature, de tip enterprise, recunoscute pe plan intern și internațional. Sistemul va putea fi implementat etapizat astfel:

Etapa I (30 luni):

- Livrarea, instalarea și configurarea Sistemului informatic integrat de supraveghere, control și asigurare a integritatii fondului forestier

Etapa II (8 luni):

• Implementarea de soluții/instrumente de securitate ce vor asigura confidențialitatea, disponibilitatea și integritatea datelor/documentelor
• Instruirea utilizatorilor aplicației
• Digitalizarea serviciilor publice în domeniul mediului vor fi implementate în trei etape :
• Dezvoltare infrastructură hardware și software de bază pentru dezvoltarea și extinderea serviciilor electronice existente în cadrul ANPM
• Dezvoltare/extindere servicii electronice
• Implementarea unei platforme integrate pentru investigații și alertare în ceea ce privește evenimentele de securitate

Intervenția pornește de la premisa implicării a cât mai mulți din stakeholderii care colectează, raportează, utilizează sau doar vizualizează în scop informativ datele de mediu ce fac obiectul intervenției propuse. Abordarea participativă (prin grupuri tehnice de lucru, focus grupuri, consultare publică prin chestionare și sondaje de opinie) va asigura transparentizarea procesului și va crește gradul de încredere în noua sursă unitară de acces date de mediu.

Scopul principal al investiției este de a avea un sistem digital, inovator, pentru combaterea exploatării forestiere ilegale. Acesta va fi integrat cu SUMAL 2.0 (Sistemul de Urmărire a Materialului Lemnos), sistemul românesc de trasabilitate a lemnului în curs de dezvoltare.

În timpul implementării SUMAL 1.0 au fost identificate mai multe lacune, inclusiv lipsa sistemelor de monitorizare pentru a evita transportul dublu al lemnului, precum și utilizarea imaginilor din satelit pentru a monitoriza integritatea zonei forestiere și starea de sănătate. În același timp, sistemul actual de măsurare a arborilor (bazat pe evaluarea vizuală a calității arborelui) aduce multă subiectivitate și uneori subevaluarea intenționată a lemnului. Măsurarea LIDAR (Light Detection and Ranging) a materialului lemnos care urmează să fie colectat este cea mai precisă soluție disponibilă și aceasta va înlocui sistemul actual care este supus unei posibile fraude. Scanerele LIDAR pot fi utilizate pentru măsurarea rapidă a camioanelor cu lemn, precum și a grămezilor de lemn din depozitele de lemn și pentru identificarea eventualelor înregistrări false ale stocurilor. Monitorizarea video a transporturilor de lemn atât pe drumurile forestiere, dar și pe drumurile publice va reduce drastic posibilitatea de transporturi multiple, dar și evaluări / încărcări false ale lemnului.

Această investiție face parte din reforma sistemului de control și monitorizare prezentat pe larg în cadrul componentei Păduri și biodiversitate. Imaginile prin satelit vor fi incluse ca un nivel distinct în sistemul SUMAL 2.0 împreună cu hărți de gestionare a pădurilor, hărți Natura 2000 și, de asemenea, seturi de date GIS relevante. Sistemul va fi utilizat pentru a monitoriza obligațiile legale legate de recoltarea lemnului, regenerarea pădurilor la timp, sănătatea pădurilor, dar și starea conservării habitatului forestier, impactul schimbărilor climatice și adaptarea la schimbările climatice a diferitelor ecosisteme forestiere.

Toate agențiile naționale, operatorii autorizați și forțele de ordine vor avea acces la sistem pe baza diferitelor roluri pe care le au în implementarea diferitelor reglementări sau monitorizare și control. Sistemul va fi capabil să includă date din Inventarul Național al Pădurilor și să servească drept cel mai bun instrument cartografic pentru planificarea colectării și prelevării de date din Inventarul Național.

Grup țintă: Autoritatea publică centrală de mediu, populația generală, mediul antreprenorial.

Ajutor de stat: Investițiile/serviciile necesare implementării acestor măsuri vor fi achiziționate printr-o procedură competitivă, transparentă, nediscriminatorie și necondiționată, nefiind incidente astfel prevederile legislației din domeniul ajutorului de stat.

Calendar: 2021 - 30 iunie 2026.

I6. Digitalizare în domeniul muncii și protecției sociale (Alocare 85 mil. euro)

Provocări: Lipsa unor instrumente digitale adecvate pentru oferirea acestor măsuri a însemnat o mare provocare pentru ANOFM. Aplicarea acestor măsuri a condus la necesitatea regândirii modalităților de transmitere a documentelor necesare stabilirii drepturilor luând in considerare si restricțiile impuse pentru prevenirea și combaterea efectelor pandemiei de COVID-19. Tehnologia digitală este esențială și va contribui la o redresare mai solidă a societăților și a economiilor. Măsurile recente de distanțare fizică au scos în evidență importanța unei infrastructuri digitale moderne care să garanteze accesul pe scară largă la internet și disponibilitatea serviciilor digitale, indispensabile pentru activitățile de zi cu zi. Investițiile în digitalizarea întreprinderilor și a sectorului public și dezvoltarea serviciilor digitale de date în sectorul public și în cel privat pot favoriza telemuncă, învățarea în mediul virtual și școlarizarea la domiciliu. Pe lângă efectul de creștere a rezilienței și a productivității, această tranziție poate contribui, de asemenea, la transformarea verde a economiilor noastre și la integrarea grupurilor vulnerabile în viața economică.

Consecințele muncii nedeclarate se reflectă negativ și prin distorsionarea mediului concurențial. Angajatorii care utilizează munca nedeclarată au mai puține obligații financiare și se află în concurență neloială cu angajatorii care depun eforturi reale pentru respectarea obligațiilor legale ce le revin.

In prezent, în cadrul Inspecției Muncii și al Inspectoratelor Teritoriale de Muncă, nivelul de digitalizare este redus, mare parte dintre activitățile care s-ar putea realiza digital fiind încă realizate pe suport de hârtie. Neimplementarea semnăturii electronice și inexistența unor programe informatice adecvate, au ca efect îngreunarea activității, generarea și circuitul documentelor specifice activității neputându-se realiza exclusiv în format electronic.

Întocmirea documentelor de control se realizează pe suport de hârtie, prin completarea documentelor cu regim special (proces verbal de control și proces verbal de constatare și sancționare a contravenților) și a anexelor, care chiar dacă pot fi întocmite electronic trebuie printate, neexistând posibilitatea întocmirii semnării și comunicării electronice, fapt care îngreunează activitatea de control și procedura ulterioară de comunicare către contravenient și către organele fiscale.

Lipsa digitalizarii proceselor de prelucrare a cererilor de beneficii sociale,in vederea punerii in plata,iar pe de altă parte, relaționarea greoaie cu cetățenii,care se realizează fragmentat,pe suport de hârtie,cu timpi mari de soluționare etc. In prezent, o parte dintre plăți se efectuează, pentru anumite beneficii sociale, printr-un sistem de plata conceput la nivelul anului 2006, cu risc major

de nefunctionare, pe echipamente din 2009-2010, iar alta parte dintre plăți se procesează neunitar, în Excell.

Obiectiv:

- Implementarea unor procese de digitalizare a serviciilor pentru clienții SPO și oferirea de măsuri personalizate
- adaptarea resurselor umane SPO la noile procese digitale prin dezvoltarea competențelor în TIC
- dezvoltarea sistemului informatic al instituției astfel încât să faciliteze adoptarea unor decizii eficiente privind identificarea şi combaterea cazurilor de muncă nedeclarată;
- mediatizarea modificărilor legislative în domeniul relaţiilor de muncă și a cazurilor grave de încălcare a legislației;
- perfecționarea profesională a inspectorilor de muncă și eficientizarea activității acestora.
- utilizarea mai eficientă a timpului alocat controlului, diminuarea timpului alocat aspectelor procedurale și creșterea timpului alocat verificărilor, utilizarea mai eficientă a resurselor umane și materiale disponibile.
- accesarea de pe teren a datelor necesare efectuării controlului, existente în baza de date a Inspecției Muncii precum și a altor instituții (ANF, ONRC, Evidența Populației, etc) precum și prin comunicarea în timp util a tuturor situațiilor deosebite/incidentelor/ dificultăților, întâmpinate în timpul controlului, pentru a primi informațiile, îndrumarea și sprijinul necesare.
- facilitarea procedurii de comunicare a documentelor de control către entitatea controlată, care nu trebuie să se mai deplaseze (atunci când documentele nu sunt încheiate la sediul social al acesteia), la sediul inspectoratului teritorial de muncă sau în altă locație, în vederea primirii procesului verbal de control. Eliminarea procedurii de afișare la sediul angajatorului a procesului verbal de contravenție, și, pe cale de consecință, a dificultăților procedurale pe care le implică, constând inclusiv găsirea unui martor, precum și a prejudiciului de imagine pe care îl poate genera angajatorului, documentul fiind vizibil pentru orice persoană aflată la locația respectivă și nu doar pentru acesta.
- facilitarea verificării plății și, după caz, a executării amenzilor contravenționale de către organele fiscale.
- îmbunătățirea calității serviciilor oferite cetățenilor și mediului de afaceri, printr-o utilizare mai eficientă a resurselor și scurtarea timpilor de răspuns la solicitările primite.
- creșterea capacității administrative a ANPIS prin digitalizarea si gestionarea proceselor de acordare a tuturor beneficiilor de asistență socială, precum si a capacitatii de reactie rapida in situatii de criza.
- dezvoltarea unui sistem informatic, unitar si integrat la nivelul ANPIS, adecvat și adaptabil la dinamica schimbărilor specifice reformelor în domeniul asistenței sociale.
- modificarea legislatiei referitoare la modul de acordare a beneficiilor sociale, din perspectiva digitalizarii.
- dobândirea competențelor digitale de către personalul implicat în procesul de acordare a beneficiilor de asistență socială de la nivelul administrației locale și centrale

- creșterea gradului de informare și constientizare a cetățenilor cu privire la acordarea beneficililor de asistență sociala utilizând mijloace moderne de digitalizare.

- creșterea gradului de accesibilitate a serviciilor digitale în domeniul muncii și protecției sociale pentru utilizatorii vulnerabili, cum ar fi persoanele cu dizabilități, vârstnicii, persoanele cu un nivel limitat de competențe digitale etc.

Implementare:

a) Plecând de la obiectivul propus de digitalizare a serviciilor pentru clienții Agenției Naționale pentru Ocuparea Forței de Muncă (ANOFM) şi oferirea de măsuri personalizate, propunerile de reformă din cadrul proiectului sunt un pas important din două perspective: trăim într-o eră digitală unde orice serviciu trebuie furnizat și digital, iar pe de altă parte digitalizarea serviciilor presupune investiții în infrastructură și formarea resurselor umane și nu în ultimul rând în concept.

În prezent, ANOFM realizează interoperabilitatea cu bazele de date ITM și ANPIS, prin propriul sistem IT. Această activitate va continua prin proiectul PNRR. În ceea ce privește modul în care se va realiza integrarea diferitelor instrumente / baze de date utilizate în prezent la nivel național și / sau regional al acestor servicii, acest urmează a fi stabilit la nivelul Ministerului Muncii și Protecției Sociale.

Maturitatea proiectului este conferită de faptul că atât obiectivele cât și rezultatele propuse duc spre:

• Transferul prin digitalizare a proceselor/activităților desfășurate de Serviciul Public de ocupare (SPO). La momentul de față ANOFM oferă un singur serviciu online - medierea muncii. Ne propunem ca serviciile ANOFM să fie mai accesibile prin digitalizare. O componentă importantă a proiectului o reprezintă înlocuirea infrastructurii hardware care la momentul de față nu poate asigura acordarea online a serviciilor.

Echipamentele hardware ale ANOFM din centrul de date din STS au fost puse în funcțiune în anul 2009 ceea ce înseamnă că, echipamentele au ieșit din perioada de garanţie, având peste 10 ani de utilizare neîntreruptă, fiind uzate fizic și moral.

La nivelul Agențiilor județene din subordinea ANOFM serviciile informatice sunt instalate pe servere ce au fost achiziţionate şi instalate în anul 2009.

• Adaptarea resurselor umane SPO la noile procese digitale prin dezvoltarea competențelor în TIC. Din cele 2175 de posturi sunt ocupate aproximativ 1800 de posturi personalul având nevoie de dezvoltarea unor competențe digitale. Ținta propusă în acest proiect este de 1200 de persoane formate ceea ce reprezintă peste 65% din personalul existent. Sub acest aspect considerăm că țintele propuse în acest proiect sunt unele de amploare pentru SPO.

Reforma vizează transformarea SPO într-un actor competitiv în domeniul plasării forței de muncă, oferind posibilitatea clienților să acceseze serviciile fără a se deplasa la sediul AJOFM/AMOFM.

Serviciile care pot fi introduse, ca urmare a investițiilor realizate, pentru solicitanții de locuri de muncă sunt:

- trimiterea online a documentelor necesare pentru: înregistrarea beneficiarului / CAE, inclusiv pentru acordarea prestațiilor - de exemplu: concedii medicale, suspendare / reintegrare / încetarea indemnizației de șomaj etc.

- formare profesională online, secțiune pentru înregistrarea intenției de a participa la un curs (pre-înregistrare), suport pentru curs online / secțiune pentru simularea evaluării competențelor teoretice profesionale, platformă pentru participarea la un program de formare profesională în funcție de tipul de curs (dacă se poate livrate online), secțiunea pentru comunicarea / programarea interacțiunilor necesare pentru procesul de formare / evaluare a competențelor, un mecanism de monitorizare a programelor de formare profesională: în faza de livrare (de exemplu, prezență), formare post-profesională;

- revizuirea procedurii și implementarea unui instrument de organizare a evenimentelor de angajare / târg de locuri de muncă și online, pentru a le face interactive;

- platforme pentru programarea și desfășurarea sesiunilor de consiliere online (programarea poate fi realizată atât de beneficiar, cât și de funcționarul public), monitorizarea participanților la sesiuni de informare și consiliere în ceea ce privește evoluția acestora pe parcursul perioadei de consiliere și post-consiliere (instrumente specifice pentru beneficiari cu ocupabilitate redusă și foarte scăzută), posibilitatea beneficiarului de a actualiza informațiile trimise consilierului;

Serviciile digitale introduse în domeniul SPO vor respecta legislația și cadrul normativ al UE privind accesibilitatea la serviciile digitale a diverselor categorii de utilizatori vulnerabili, persoane cu dizabilități și cerințe speciale, persoane cu un nivel scăzut al competențelor digitale ș.a.

b) Pentru Inspecția Teritorială a Muncii (ITM) sunt propuse două proiecte de digitalizare, astfel:

> b1. Proiectul REGES-ONLINE își propune să digitalizeze relația Inspecției Muncii / ITM cu angajatorii, respectiv transmiterea datelor despre angajați și contractele lor individuale de muncă.
>
> b2. Al doilea proiect își propune să digitalizeze activitatea de control a inspectorilor ITM, activitate care se desfășoară în prezent exclusiv în format scrisoare.

Digitalizarea activității de control, prin implementarea unui sistem informatic adecvat și a semnăturilor electronice, de la întocmirea documentelor specifice până la comunicarea acestora atât entității controlate cât și organelor fiscale, în cazul aplicării amenzii, are ca efect diminuarea timpului alocat controlului, respectiv, alocat aspectelor procedurale aferente și, implicit, creșterea timpului alocat verificărilor, fapt care conduce la îmbunătățirea activității de control.

Simplificarea procedurii de comunicare este atât în beneficiul instituției cât și în beneficiul destinatarului, respectiv angajatorul controlat și organele fiscale care verifică plata amenzii, sau, după caz, procedează la executarea obligației fiscale.

Accesarea de pe teren, prin utilizarea unor dispozitive mobile, respectiv, laptopuri și telefoane, a datelor necesare efectuării controlului, existente în baza de date a Inspecției Muncii precum și a altor instituții (ANAF, ONRC, Evidența Populației, etc) conduce la efectuarea unor verificări mai

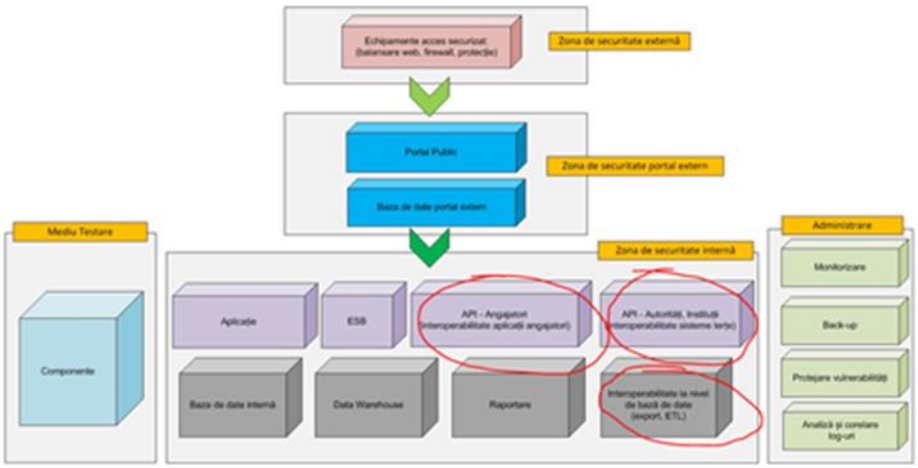
complete. De exemplu, se va putea verifica dacă salariatul a fost declarat și autorităților fiscale, sau dacă datele declarate sunt aceleași cu cele din contractul individual de muncă.

Eliminarea procedurii de afișare a documentelor de control către entitatea controlată, facilitează procedura de comunicare a acestora, renunțând la o procedură anacronică de „*lipire pe ușa infractorului*" în favoarea unei modalități adaptate secolului XXI, nivelul tehnologic evoluția și relația de entitate controlată de administrație. Acest lucru este atât în beneficiul instituției, prin scurtarea timpului alocat problemelor procedurale ca o consecință a eliminării dificultăților procedurale implicate, prin deplasarea la sediul angajatorului și găsirea unui martor și a entității controlate prin eliminarea prejudiciului de imagine pe care îl poate genera faptul că documentul este vizibil pentru oricine din acea locație și nu doar pentru ei.

În același timp, comunicarea electronică elimină necesitatea comunicării documentelor direct contravenientului, ceea ce necesită deplasarea acestuia (atunci când documentele nu sunt încheiate la sediul social), la inspectoratul teritorial de muncă sau în altă parte, pentru a primi raportul de control .

Implementarea sistemului informatic REGES-ONLINE poate fi realizată etapizat pe durata a doi ani, 2023-2024. Scopul final este implementarea și punerea în funcțiune a sistemului informatic REGES-ONLINE.

Implementarea sistemului informatic REGES-ONLINE se va face la nivel de interoperabilitate – accesul autorităților și instituțiilor publice la datele din registru la nivel de interfață de programare a aplicațiilor (API - Application Programming Interface), conform diagramei de principiu a sistemului propus:



c) Digitalizarea ANPIS include :

- ✓ Analiza serviciilor de acordare a beneficiilor de asistență social și a proceselor interne în vederea digitalizarii
- ✓ Revizuirea legislației în sensul actualizării, unificării și simplificării procedurilor de lucru
- ✓ Proiectarea sistemului informatic si a instrumentelor de digitalizare de la nivelul autorității administrației

- ✓ Achiziționarea echipamentelor(software, hardware, comunicații) pentru digitalizarea seviciilor si a echipamentelor necesare susținerii activității/asigurarea securității datelor
- ✓ Dezvoltarea sistemului informatic (software si hardware)
- ✓ Dezvoltarea instrumentelor pentru managementul documentelor si informatiilor (OCR, arhiva electronica, secretariat electronic)
- ✓ Dezvoltare unui canal de comunicare in timp real cu cetatenii
- ✓ Livrarea si conectarea echipamentelor necesare sustinerii activitatilor/asigurarea securitatii datelor
- ✓ Dezvoltarea instrumentelor de digitalizare si procesare
- ✓ Pregatirea stakeholders implicați în procesul de acordare a beneficiilor sociale in sistem digital
- ✓ Campanie de informare si constientizare despre procesul de acordare si administrare a beneficiilor sociale
- ✓ Măsurarea impactului procesului de digitalizare a serviciilor de acordare a beneficiilor de asistență socială gestionate de ANPIS, prin studii comparative.

- ✓ Îmbunătățirea nivelului de accesibilitate la serviciile digitale ale ANPIS de către persoanele vulnerabile din perspectiva competențelor digitale.

Dezvoltarea sistemului IT este o piesă cheie în procesul de digitalizare al ANPIS. Acesta creează cadrul tehnic pentru un sistem de beneficii integrat, fără erori și fără fraude. Chiar dacă sistemul IT în vigoare a suferit mai multe transformări și îmbunătățiri de-a lungul anilor, acesta are încă nevoie de lucrări suplimentare care să-i permită să se adapteze la schimbările și dinamica legislativă și la întregul concept de sistem digital de asistență socială. Mai mult, având în vedere că SII MMPS este planificat să devină operațional pe termen scurt, sunt necesare câteva module suplimentare pentru procesarea cererilor, verificarea încrucișată a diferitelor baze de date naționale și plata beneficiilor.

Ideea creării unui canal de comunicare în timp real cu cetățenii este direct legată de conceptul de a avea cetățenii în centrul sistemului de asistență socială. Podurile de comunicare sunt importante nu numai din punctul de vedere al oferirii de informații exacte cu privire la accesul la beneficii, ci și pentru crearea unei imagini clare a nevoilor reale ale cetățenilor cei mai vulnerabili. Acest lucru va oferi autorităților posibilitatea de a ajusta cadrul legal și de a adapta măsurile de protecție la nevoile specifice ale comunităților.

Instrumentele de digitalizare și procesare se referă în principal la întregul pachet de sisteme și subsisteme IT care vor fi utilizate în transformarea platformei de acces la beneficiile de la una clasică pe hârtie la una rapidă, fiabilă și digitală. Instrumentele de procesare, cum ar fi instrumentele OCR și dispozitivele compatibile hardware, vor asigura o tranziție lină către noul sistem digital.

În timp ce ANPIS și agențiile regionale joacă un rol important în întreaga schemă de beneficii sociale, pregătirea părților interesate implicate în procesul de acordare a beneficiilor sociale în sistemul digital este la fel de importantă. Digitalizarea sistemului de beneficii sociale și a ANPIS nu implică un proces de îndepărtare de cei care au nevoie de asistență, ci mai degrabă crearea de

modalități pentru un proces mai ușor și mai rapid. Ca atare, municipalitățile - un factor important - vor juca în continuare un rol semnificativ, în special pentru beneficiarii cu abilități digitale mai scăzute. Prin urmare, este obligatoriu ca astfel de părți interesate să aibă cât mai multe informații posibil și să fie instruiți în mod specific pentru transformarea digitală.

Noul sistem IT prevăzut a fi utilizat de ANPIS în procesarea cererii de beneficii va fi capabil să extragă și să verifice datele din toate bazele de date relevante utilizate și la nivel național și regional. În timp ce municipalitățile vor efectua o verificare a eligibilității la primul nivel pe baza informațiilor din bazele de date locale, Agențiile Regionale pentru beneficii și inspecție socială vor extrage și prelucra toate datele necesare pentru a acorda sau respinge beneficiul solicitat.

ANPIS efectuează două tipuri de verificări privind acuratețea acordării prestațiilor sociale:

- Verificarea ex-post, prin intermediul campaniilor de inspecție socială
- Verificare ex-ante, în momentul procesării cererilor.

Ambele tipuri vor fi mai exacte odată cu îmbunătățirea capacității sistemului IT utilizat de ANPIS de a controla informațiile din alte baze de date relevante.

Capacitatea sistemului IT al ANPIS de integrare cu alte baze de date va fi menționată și solicitată în mod specific în descrierea tehnică a proiectului, în momentul achiziționării serviciilor de dezvoltare IT. Soluțiile tehnice necesare în acest scop vor fi detaliate în documentația specifică

Digitalizarea ANPIS (Agenția Națională pentru Plățile și Inspecțiile Sociale) este complementară cu alte proiecte în curs de implementare pentru tranziția digitală și e-guvernare, cum ar fi MMPS Service Hub - SII MMPS. Proiectul, finanțat în cadrul Programului Operațional Competitivitate își propune să digitalizeze corespondentul serviciilor publice la 5 evenimente de viață, care, în schimb, corespund cu 5 beneficii sociale. SII MMP reprezintă doar o mică parte din totalul serviciilor publice furnizate de ANPIS, restul fiind abordate prin intermediul PNRR.

Adițional dezvoltării sistemului IT utilizat de ANPIS pentru procesarea și plata beneficiilor de asistență socială, operaționalizarea Venitului Minim de Incluziune (VMI) presupune dezvoltarea Sistemului National Integrat de Asistenta Sociala- SNIAS. Acesta va asigura suportul logistic și tehnic pentru introducerea cererilor de acordare a beneficiului prin mijloace electronice, și va ușura astfel povara administrativă pentru potențialii beneficiari. Pentru contracararea unor eventuale bariere impuse de lipsa infrastructurii IT în anumite comunități sau competențe digitale reduse, SNIAS va păstra funcționalități care vor permite introducerea solicitărilor la primării.

Pentru a răspunde nevoii de asigurare a unui punct de contact în cadrul autorităților locale, SNIAS va dispune de o interfață simplificată, care urmează a fi utilizată de personalul din cadrul primăriilor la introducerea cererilor depuse personal de beneficiari. Totodată, pentru asigurarea acurateței datelor înscrise în solicitările depuse de potențialii beneficiari, anterior transmiterii cererilor către agențiile județene pentru plăți și inspecției socială, funcționarii din cadrul primăriilor vor efectua verificări *ex-ante* în bazele de date proprii dar și prin încrucișarea cu alte baze de date relevante ale altor autorități locale.

SNIAS va cuprinde inclusiv un modul interoperabil care va permite o abordare integrată a procesului de evaluare a nevoilor beneficiarilor și, implicit, adoptarea unor măsuri reziliente și

țintite. Serviciile de asistență socială din primării vor efectua analize comprehensive privind situația familială a beneficiarilor și vor putea determina cel mai potrivit nivel de protecție socială în baza unor indicatori cuantificabili și măsurabili. Analizele vor fi ulterior încărcate în SNIAS și vor fi disponibile și la nivelul ANPIS și agențiilor teritoriale din subordine.

În vederea asigurării unui proces de management unitar al tuturor beneficiilor de asistență socială, SNIAS va fi integrat în totalitate cu sistemele informatice deja existente în cadrul ANPIS. În acest sens, dezvoltarea se va realiza prin utilizarea unor parametrii tehnici compatibili. De asemenea, pentru a răspunde provocărilor generate de dinamica cadrului legislativ, SNIAS va putea fi actualizat fără eforturi tehnice și financiare majore.

Grup țintă:

Ministerul Muncii și Protecției Sociale, Agenția Națională de Ocupare a Forței de Muncă, Agențiile Județene de Ocupare a Forței de Muncă, Inspecția Muncii, Inspectoratele Teritoriale de Muncă, Agenția Națională de Plăți și Inspecție Socială, Agențiile Județene de Plăți și Inspecție Socială și beneficiarii serviciilor acestor instituții publice.

Ajutor de stat: Investițiile/serviciile necesare implementării acestor măsuri vor fi achiziționate printr-o procedură competitivă, transparentă, nediscriminatorie și necondiționată, nefiind incidente astfel prevederile legislației din domeniul ajutorului de stat.

Calendar: 2021- 30 iunie 2026.

I7. Implementarea formularelor electronice eForms în domeniul achizițiilor publice (Alocare 0,85 mil. euro)

Provocări: În conformitate cu prevederile legislației din domeniul achizițiilor publice, în vederea respectării regulilor de publicitate și transparență, autoritățile/entitățile contractante au obligația de a transmite spre publicare prin mijloace electronice, la nivel național (SEAP) și după caz, în Jurnalul Oficial al Uniunii Europene, anunţuri privind procedurile de atribuire a contractelor de achiziție publică, sectoriale și de concesiune de lucrări și servicii, cu respectarea formatelor-standard stabilite de Comisia Europeană, în temeiul dispoziţiilor art. 51 din Directiva 2014/24/UE a Parlamentului European şi a Consiliului din 26 februarie 2014, a dispoziţiilor art. 71 din Directiva 2014/25/UE a Parlamentului European şi a Consiliului din 26 februarie 2014 și a dispoziţiilor art. 33 din Directiva 2014/23/UE a Parlamentului European şi a Consiliului.

În contextul adoptării, la data de 23 septembrie 2019 a Regulamentului de punere în aplicare (UE) 2019/1780 de stabilire a formularelor standard pentru publicarea anunțurilor în domeniul achizițiilor publice și de abrogare a Regulamentului de punere în aplicare (UE) 2015/1986, utilizarea noilor formulare standard electronice aferente anunțurilor în domeniul achizițiilor publice publicate la nivel european va deveni obligatorie începând cu data de 14 noiembrie 2023.

În situația în care până la data menționată în Regulament noile formulare electronice nu vor fi implementate la nivel național, există riscul să fie lansată o procedură de infringement împotriva României și să fie afectate toate proiectele cu finanțare din fonduri ale Uniunii Europene.

Obiectiv:

Instituite în temeiul Regulamentului de punere în aplicare (UE) 2019/1780 al Comisiei, publicat la 25 octombrie 2019, formularele electronice standard care urmează să fie utilizate pentru publicarea anunțurilor de achiziții publice începând cu 14 noiembrie 2023 se află în centrul transformării digitale a achizițiilor publice în UE, fiind primele formulare standard concepute pentru implementarea digitală. Utilizarea acestora va eficientiza în mod semnificativ practicile de achiziții publice atât la nivel european, cât și la nivel național. Implementarea formularelor electronice la nivel național reprezintă o nouă acțiune de modernizare a sistemului național de achiziții publice, atât din perspectiva asigurării eficienței, transparenței și integrității acestuia, cât și în vederea facilitării colectării, consolidării, gestionării și analizei datelor privind achizițiile publice.

Scopul principal al investiției îl reprezintă implementarea formularelor electronice - eForms la nivel național.

Investiția vizează următoarelor obiective:

1 - creșterea transparenței în procedurile de achiziții publice prin furnizarea de instrumente digitale care să prevină neregulile în cadrul procedurilor de achiziții publice și, prin urmare, să contribuie la reducerea corupției și fraudei în sectorul public;

2 - armonizarea interfețelor și a proceselor, precum și a îmbunătățirii accesului operatorilor economici la procedurile de achiziții publice prin asigurarea unei utilizări transparente și previzibile în cadrul sistemului național de licitații electronice;

3 - îmbunătățirea eficienței administrației naționale, simplificarea procedurilor și reducerea birocrației atât pentru autoritățile contractante, cât și pentru operatorii economici;

4 - pentru a realiza o guvernanță a achizițiilor publice bazată pe dovezi.

Implementare:

Pentru realizarea Investiției, Agenția Națională pentru Achiziții Publice (ANAP), împreună cu ADR, vor derula următoarele activități :

1. *Analiză reglementări eForms*

Aceasta este activitatea de analiză a Regulamentului de punere în aplicare al Comisiei (UE)2019/1780 din 23 septembrie 2019. Scopul acestei activități este de a înțelege toate cerințele de punere în aplicare a Regulamentului 2019/1780.

2. *Analiza formularelor electronice în comparație cu formularele anterioare*

Aceasta este o analiză comparativă a formularelor electronice față de formularele actuale implementate în sistemul electronic. Scopul acestei activități este de a înțelege care sunt principalele domenii de schimbare.

3. Analiza eForms a schemelor, listelor de coduri, regulilor de business și de validare, și a etichetelor

Această activitate este necesară pentru a înțelege detaliile de implementare la nivel scăzut ale Regulamentului 2019/1780. Rezultatul acestei analize va constitui baza de referință pentru activitățile ulterioare, cum ar fi definirea modelului de date, implementarea formularelor electronice și integrarea cu alte sisteme. Această activitate este susținută de documentația privind schema eForms.

4. Analiza integrărilor de sistem solicitate de UE

Pe baza deciziilor arhitecturale luate în ca urmare a activităților descries anterior, această activitate va defini necesitățile și cerințele de integrare pentru implementarea integrării formularelor electronice cu.sistemele UE - TED, TED eSenders, eNotices etc.

5. Adaptare formulare electronice

Această activitate se bazează pe deciziile arhitecturale luate. Această activitate este implementată în conformitate cu Manualul de implementare a politicii eForms și este susținută de documentația privind schema eForms.

6. Definirea și implementarea modelului de date eForms

Această activitate va defini și va implementa în modelul de date pentru formuarele electronice baza de date existentă a sistemului național de achiziții publice.

7. Implementarea formularelor și notificărilor electronice

Aceasta este principala activitate a proiectului și presupune implementarea formularelor electronice în Sistemul național de achiziții publice. Aceasta cuprinde toate formularele și anunțurile electronice.

8. Implementarea integrării utilizând Building Blocks

Această activitate va implementa infrastructura hardware și software pentru eDelivery, eSignature și eArchiving. Această activitate include desfășurarea sistemului eDelivery, implementarea punctului de acces eDelivery, implementarea editorului de metadate de servicii, a aplicațiilor de semnătură electronică și de arhivare electronică. De asemenea, include analiza, proiectarea, implementarea și testarea codului pentru extinderea funcționalităților sistemului național de achiziții publice cu capacitățile blocurilor de construcție.

9. Integrarea eForms cu eNotices

Bazându-se pe rezultatele analizei realizate in cadrul activității nr. 3, se va realiza integrarea eForms cu eNotices.

10. Integrarea eForms cu TED eSenders

Bazându-se pe rezultatele analizei realizate in cadrul activității nr. 3, se va realiza integrarea eForms cu eSenders.

11. Integrarea cu instrumentele operate de o organizație care trimite notificări către TED eSender

Bazându-se pe rezultatele analizei realizate in cadrul activității nr. 3, prin intermediul acestei activități se va realiza integrarea eForms cu instrumente operate de alte organizații care trimit notificări către TED eSender.

12. Integrarea formularelor electronice cu serviciile existente de Business Intelligence pentru raportare consolidate

Această activitate este necesară pentru integrarea formularelor electronice cu sistemul Business Intelligence disponibil în Sistemul național de achiziții publice pentru o raportare consolidată.

13. Integrarea eForms cu serviciile de raportare existente pentru raportarea datelor istorice

Această activitate este necesară pentru integrarea formularelor electronice cu serviciul de raportare existent și disponibil în sistemul național de achiziții publice pentru raportarea datelor colectate din formularele și notificările electronice, cât și din bazinul de date istorice.

14. Cursuri de instruire

Vor fi oferite cursuri de instruire pentru părțile interesate și pentru utilizatorii externi care doresc să utilizeze formularele electronice.

15. Suport

Sprijin operațional pentru implementarea formularelor electronice, timp de un an după implementare

Grup țintă: ANAP, ADR și beneficiarii sistemului electronic al achizițiilor publice

Ajutor de stat:

Investițiile/serviciile necesare implementării acestor măsuri vor fi achiziționate printr-o procedură competitivă, transparentă, nediscriminatorie și necondiționată, nefiind incidente astfel prevederile legislației din domeniul ajutorului de stat.

Calendar: 2021- 30 iunie 2023.

I8. Carte de identitate electronică și semnătură digitală calificată (Alocare 200 mil. euro)

Provocări: Prin raportare la nevoile actuale, impuse în mod special de procesul de digitalizare este necesar o transformare a capacităților existente dar și o transformare a modului în care funcționează autoritățile naționale și modul în care siguranța cetățenilor și drepturile la anumite informații sunt mai bine asigurate.

Cartea electronică de identitate (CEI) este un facilitator cheie pentru adoptarea serviciilor digitale guvernamentale si va permite titularului autentificarea în sistemele informatice ale Ministerului Afacerilor Interne și în sistemele informatice ale altor instituții publice sau private, precum şi utilizarea semnăturii electronice, în condițiile legii. CEI va facilita astfel accesul cetățeanului la

diverse servicii electronice (bancare, fiscale, sociale, financiare etc.), cu efecte majore privind simplificarea relației cu autoritățile publice, creșterea calității şi accesibilității serviciilor publice.

Noua CEI va respecta cerințele Comisiei Europene privind securizarea documentelor în contextul combaterii terorismului, al migrației ilegale, al traficului de droguri și de persoane, cărțile de identitate actuale fiind realizate cu tehnologie din anii '90, totodată fiind urmărită şi atingerea obiectiveleor Regulamentului (UE) 1157/2019 care impune cerințe superioare ale elementelor de securitate ale cărților de identitate. În legislația românească, în luna august 2020 a fost creat cadrul legal pentru asigurarea aplicarii directe a dispozitiilor acestui regulament prin Legea nr. 162, însoțită de normele de aplicare (aprobate prin HG nr. 295/2021).

Obiectiv: Investiția urmărește stimularea adoptării voluntare a cărții de identitate electronice cu semnătură digitală calificată

Implementare:

Noul format al cărții electronice de identitate (CEI) este de tipul ID1 (ICAO 9303), cu termen de emitere a primei CEI 2 august 2021, în condițiile impuse de dispoziţiile Regulamentului (UE) 1157/2019.

Semnatura Electronica (certificat calificat)

De asemenea, avand in vedere că CEI prezintă partitii rezervate stocarii securizate a unui certificat digital de semnatura electronica calificată, programul de investitie subventioneaza achizitia certificatului digital de catre populatie. Unul dintre beneficiile adoptării pe scară largă a semnăturii electronice îl reprezintă reducerea interacțiunii la ghișeu a cetățeanului cu administrația publică, debirocratizarea procedurilor administrative, reducerea timpului necesar pentru accesarea serviciilor publice, creșterea nivelului de sofisticare a serviciilor electronice la nivel minim 4. De asemenea, în acest fel se creează premisele unei reforme necesare sistemului judiciar.

Conform legislației naționale (Legea 162/2020) noua carte electronică de identitate va stoca 2 (două) certificate digitale astfel:

a. *Obligatoriu*: Un certificat digital pentru semnătură electronica avansată, emis de MAI. Acest certificat se va înscrie pe toate cărțile electronice de identitate și va permite autentificarea (accesarea) serviciilor electronice expuse de administraţia publică în mediul online și totodată aplicarea semnăturii electronice extinse (având aceeași valoare juridică cu cea a unei semnături olografe, aspect valid cel puțin pe teritoriul României). Costul emiterii acestui tip de certificat va fi inclus în costul CEI (cf. legislației naționale în vigoare).

b. *Optional*: Un certificat digital pentru semnătură electronică calificată, emis de furnizorii de servicii de certificare calificată (naționali sau din afara țării). Acest certificat se va înscrie OPȚIONAL de către cetățean, contra cost, și va permite autentificarea (accesarea) serviciilor electronice expuse de terți în mediul online și totodată aplicarea semnăturii electronice calificate (având aceeași valoare juridică cu cea a unei semnături olografe, atât în România cât și spațiul comunitar).

Se elaborează o procedură prin care este finanțată emiterea CEI însoțită în mod obligatoriu de un document cu certificatul digital integrat. Astfel, în condițiile finantării prin PNRR, cel de-al doilea

certificat digital (pentru semnătură electronica calificată) devine obligatoriu, pentru stimularea adoptării la scara largă a proceselor si procedurilor digitale în contextul transformării digitale. Cartea electronica de identitate (CEI) și semnătura electronică bazată pe certificatul calificat (CC) sunt key-enablers (facilitatori-cheie) ai adoptarii pe scară largă de către populație a procedurilor digitale, atât în relație cu instituțiile publice, cât și în economie în general.
Ca atare, investiția de 200 milioane EUR asigurată prin PNRR țînteste oferirea gratuită către populație a unui CEI pe care este stocat și un CC (suplimentar celui avansat emis de MAI si stocat pe o partitie a CEI, dar care nu asigură opozabilitatea juridică a semnăturii digitale în contextul legii semnăturii electronice în vigoare).

Datele MAI arată că anual expiră aproximativ 2 milioane de cărți de identitate (CI). La începutul programului de adoptare a CEI, este de așteptat să se înregistreze o cerere mare în primii 2 ani de la generalizarea implementării , astfel că pentru estimarea numărului de CEI care vor fi eliberate s-a pornit de la cerere inițială estimatăe de 3 mil. CEI/an. Începând din anul al 3-lea, se estimează reducerea cuantumului anual cu 30%,

În prezent, în medie, se preiau la nivel national 8.800 cereri/zi pentru eliberare CI și că, la nivel national, există aproximativ 610 Servicii Publice Comunitare de Evidenta a Persoanalor (SPCEP) active (și inca aprox. 25 SPCEP in procedura de avizare / deschidere), numărul maxim de cereri care au fost preluate prin intermediul serviciilor de evidență a persoanelor a fost de 20.000 cereri preluate/zi. În baza optimizărilor care vor fi realizate pentru realizarea CEI, va exista posibilitatea de a prelua un maxim de 25.000 cereri/zi.

Pentru implementarea proiectului CEI, MAI va conlucra cu Compania Națională Imprimeria Națională, care realizează producţia blanchetelor (material utilizat pentru producerea CEI) și cu prestatorii de servicii de încredere, selectați de MCID/ADR printr-o procedură de licitație deschisă la nivel european.

În baza unei evaluări realizate în anul 2018, folosind infrastructura actuală pot fi produse 30.000 blanchete/zi. În ceea ce privește personalizarea, aceasta se va realiza folosind infrastructura pentru pașapoarte a Directiei Generale de Pașapoarte, care poate personaliza la capacitate maximă aprox. 20.000 CEI /zi.

Pe baza experienței acumulate în anii anteriori, se propune următorul calendar de implementare a CEI:

	cost eID	Număr populație
2021	7,5	5.000
2022	7,5	1.000.000
2023	10	3.000.000
2024	10	2.000.000

2025	10	1.700.000
2026 (Q2)	10	800.000

Costurile estimate pentru emiterea CEI cuprind costurile necesare retehnologizarii infrastructurii informatice existente, costurile necesare pentru achiziționarea stațiilor de lucru pentru preluarea datelor biometrice, costurile infrastructurii utilizate pentru înscrierea certificatelor digitale de semnatură electronică, precum și costurile necesare pentru dezvoltarea infrastructurii MAI necesare pentru asigurarea condițiilor interacțiunii cetățenilor cu sistemele informatice din administrația publică română, context în care se urmărește pe lângă emiterea unui document de identitate cu un înalt nivel de securitate, dar și crearea infrastructurii necesare interacțiunii cetățenilor cu autoritățile administrației publice în scopul debirocratizării serviciilor prestate pentru populație și reducerii timpilor de așteptare.

Totodată, ADR și MAI vor analiza perspectiva notificării Comisiei Europene în ceea ce privește implementarea *portofelului electronic*.

Grup țintă: MAI, Imprimeria Națională, populația

Ajutor de stat:

Investițiile/serviciile necesare implementării acestor măsuri vor fi achiziționate printr-o procedură competitivă, transparentă, nediscriminatorie și necondiționată, nefiind incidente astfel prevederile legislației din domeniul ajutorului de stat.

Calendar: 2021- 30 iunie 2026

I9. Digitalizarea sectorului organizațiilor neguvernamentale (Alocare 10,30 mil. euro)

Provocări:

Sectorul ONG prezintă un nivelul scăzut de digitalizare a, precum și existenta unor decalaje de performanta si profesionalizare in domeniul digital dintre sectorul ONG și sectorul de afaceri, capacitatea scăzută de intervenție datorată lipsei eficientizarii activității lor prin tehnologie.

Obiectiv:

a) Investiția are ca **obiectiv** transformarea digitală a sectorului ONG și creșterea nivelului de alfabetizare digitală a lucrătorilor din cadrul organizațiilor.

Această investiție vizează 2 direcții strategice:

- crearea de strategii de digitalizare sustenabile pe termen lung organizaționale și crearea de resurse digitale pentru sectorul ONG.
- accesibilizarea serviciilor către beneficiari la distanță.

- contribuția la creșterea nivelului de accesibilizare a serviciilor digitale furnizate de către cel de-al treilea sector către persoanele vulnerabile din perspectiva competențelor digitale (persoane cu dizabilități sau cerințe speciale, persoane vârstnice ș.a.).

Metode de realizare a strategiei:

- prin investiții în infrastructură digitală (infrastructură cloud și servicii digitale operaționale, dezvoltarea de aplicatii software dedicate sectorului ONG (soluții de management financiar, administrarea resurselor umane, managementul voluntarilor, managementul și retenția donatorilor etc)
- creșterea competentelor digitale ale personalului și voluntarilor in furnizarea de servicii la distanta catre beneficiari
- dezvoltarea de platforme si solutii tip CRM (customer relationship management) dedicate managementului beneficiarilor)
- achiziția de echipamente (hardware) în valoare maximă de 1/3 din bugetul proiectului
- aplicarea cadrului normativ și procedural privind cerințele de accesibilitate aplicabile produselor și serviciilor, inclusiv a site-urilor web și a aplicațiilor mobile ale organismelor din sectorul public.

Tinta: 200 de granturi acordate

Mecanism implementare: Apel de proiecte - cu depunere continuă și termene succesive de evaluare și selectie a proiectelor, care să permită angajarea resurselor în țintele anuale planificate. Durata maximă de implementare a unui proiect: 30 luni cu o valoare a grantului de maxim 70.000 Euro

Perioada de derulare: 2022-2024

Grup țintă: organizații neguvernamentale din România

b) Se propune și *crearea unui centru de resurse pentru transformarea digitala* a celui de al treilea sector cu rolul de a stabili mecanisme și proceduri pentru digitalizarea sectorului ONG.

In conformitate cu Comunicarea CE privind noțiunea de ajutor de stat astfel cum este menționată la articolul 107 alineatul (1) din Tratatul privind funcționarea Uniunii Europene (2016/C 262/01), clasificarea unei entități ca întreprindere se face întotdeauna în raport cu o activitate specifică. O entitate care desfășoară atât activități economice, cât și activități neeconomice trebuie considerată ca fiind o întreprindere numai în ceea ce privește prima categorie de activități. Crearea centrului pentru transformarea digitală a celui de al treilea sector se axează pe sprijinirea activității non-economice ale ONG, activitate ce derivă din diverse prevederi legale legate de rolul celul de-al treilea sector în accesibilizarea, monitorizarea și asigurarea transparenței serviciilor publice derulate la nivelul comunității.

Astfel, investiția are ca scop dezvoltarea unui mecanism de monitorizare a serviciilor publice de gospodărire comunală și serviciilor publice sociale oferite de către stat la nivelul comunităților. În

conformitate cu prevederile Legii 236/2001 statul are atributii de monitorizare a funcţionării serviciilor publice de gospodărie comunală în judeţe, oraşe şi comune, fiind garantat tuturor persoanelor dreptul de a utiliza serviciile publice de gospodărie comunală, prin: accesibilitate egală la servicii publice, prin accesul la informaţiile privind serviciile publice, prin dreptul de asociere în organizaţii neguvernamentale pentru apărarea, promovarea şi susţinerea intereselor utilizatorilor; prin dreptul de a fi consultate direct sau prin intermediul organizaţiilor neguvernamentale ale utilizatorilor în procesul de elaborare şi adoptare a deciziilor, strategiilor şi reglementărilor privind activităţile prin dreptul de a se adresa, direct sau prin intermediul unor organizaţii neguvernamentale, autorităţilor administraţiei publice ori instanţelor judecătoreşti în vederea prevenirii sau reparării unui prejudiciu direct ori indirect. În ceea ce privește Legea asistenței sociale nr. 292/2011, sistemul naţional de asistenţă socială reprezintă ansamblul de instituţii, măsuri şi acţiuni prin care statul, reprezentat de autorităţile administraţiei publice centrale şi locale, precum şi societatea civilă intervin pentru prevenirea, limitarea sau înlăturarea efectelor temporare ori permanente ale situaţiilor care pot genera marginalizarea sau excluziunea socială a persoanei, familiei, grupurilor ori comunităţilor. Sistemul naţional de asistenţă socială se se întemeiază, printre altele, pe următoarele valori şi principii generale :

- ✓ parteneriatul, potrivit căruia autorităţile publice centrale şi locale, instituţiile publice şi private, organizaţiile neguvernamentale, instituţiile de cult recunoscute de lege, precum şi membrii comunităţii stabilesc obiective comune, conlucrează şi mobilizează toate resursele necesare pentru asigurarea unor condiţii de viaţă decente şi demne pentru persoanele vulnerabile.
- ✓ participarea beneficiarilor, potrivit căreia beneficiarii participă la formularea şi implementarea politicilor cu impact direct asupra lor, la realizarea programelor individualizate de suport social şi se implică activ în viaţa comunităţii, prin intermediul formelor de asociere sau direct, prin activităţi voluntare desfăşurate în folosul persoanelor vulnerabile;

Pentru intărirea rolului conferit de lege pentru sectorul terțiar la nivelul accesibilizării și monitorizării serviciilor publice la nivelul comunitatilor, prin mijloace digitale se are în vedere crearea centrului *de resurse pentru transformarea digitala* a celui de al treilea sector, care va pune la dispozitia ONG pentru activitatea lor non-economică, gratuit toate serviciile și dotările necesare îndeplinirii rolului acestora conferit de lege în monitorizarea serviciilor publice la nivelul comunităților.

Centru se va axa pe următoarele caracteristici:

- dezvoltarea de proceduri și mecanisme relavante pentru integrarea serviciilor IT și soluțiilor software open-source pentru sectorul ONG și oferirea de asistență în implementarea strategiilor de transformare digitală pentru sectorul terțiar pentru monitorizarea accesibilității serviciilor publice la nivelul comunitatilor și pentru garantarea tuturor persoanelor a dreptului de a participa prin intermediul ONG în procesul de elaborare şi adoptare a deciziilor, strategiilor şi reglementărilor in domeniul serviciilor publice crearea unor baze centralizate de resurse digitale existente în cadrul unei librarii digitale deschise tururor, inclusiv furnizarea de asistență, e-learning și training ca resurse educaționale asincron descrise voluntarilor și persoanelor care activează în sectorul terțiar

pentru monitorizarea accesibilității serviciilor publice la nivelul comunităților și pentru garantarea tuturor persoanelor a dreptului de a participa prin intermediul ONG în procesul de elaborare şi adoptare a deciziilor, strategiilor şi reglementărilor în domeniul serviciilor publice

- crearea unor comunități de practică în domeniul digitalizării sectorului terțiar cu accent în special pe monitorizarea transparenței serviciilor publice oferite la nivelul comunităților
- atragerea de voluntari specializați în IT (ux/ui design, programare, devops, product managers, digital strategists) care să acorde sprijin pentru monitorizarea transparenței serviciilor publice oferite la nivelul comunităților, în procesele de transformare digitală.
- crearea de standarde de implementare, de accesibilizare, de securitate și de utilizare a tehnologiei in procesele de monitorizare a transparentei serviciilor publice oferite la nivelul comunitatilor (sociale, educationale, sanatate, voluntariat, culturale etc),inclusiv în relație cu legislația în vigoare în domeniul accesibilizării serviciilor publice
- gazduirea de replici ale soluțiilor dezvoltate prin granturile acordate prin program pentru a incuraja reutilizarea, scalarea și replicarea acestora la nivel sectorial unde este cazul
- training si asistenta pentru ONG pentru creșterea capacității de monitorizare digitală a serviciilor publice la nivelul comunităților

Buget: 1 grant in valoare maxima de 1.300.000 euro

Target: 2000 de organizatii neguvernamentale asistate

Grup tinta: organizatii neguvernamentale din Romania

Mecanismul de implementare pentru toate investițiile: selecție de proiecte

Ajutor de stat:

Pentru investiția de la punctul a) se are în vedere realizarea unei scheme de ajutor de minimis cu respectarea prevederilor Regulamentului (UE) nr. 1407/2013 din 18 decembrie 2013 pentru aplicarea art. 107 și 108 din Tratatul privind funcţionarea Uniunii Europene ajutoarelor de minimis, publicat în Jurnalul Oficial al Uniunii Europene L nr. 352/ 1 din 24 decembrie 2013. Schema de ajutor de minimis nu intră sub incidența obligației de notificare către Comisia Europeană în conformitate cu prevederile Regulamentului (UE) nr. 1407/2013. Valoarea maximă totală a ajutoarelor de minimis de care poate beneficia o persoana juridică ce deține spații cu altă destinație în clădirile multifamiliale pentru care se realizează lucrări de renovare, nu va depăși echivalentul în lei a 200.000 Euro pe întreprindere unică, în trei ani consecutiv.

Pentru investiția de la punctul b), pentru crearea centrului de resurse pentru transformarea digitală, se va derula o procedură de selecție deschisă, competitivă, transparentă, nediscriminatorie, având la bază inclusiv ca și criteriul prețul serviciilor furnizate. Pentru sprijinirea 2.000 de ONG-urilor, prin acordarea acestora de consultanţă și training prin intermediul centrului de resurse pentru transformarea digitală, in funcție de desfășurarea unor activități economice de către respectivele

ONG-uri și de ținerea unei evidențe contabile separate de către acestea cu privire la finanțarea și costurile activităților economice, finanțarea respectivelor ONG-uri poate să nu intre sub incidența legislației din domeniul ajutorului de stat sau ar putea fi realizată prin intermediul unei scheme de ajutor de minimis în conformitate cu prevederile Regulamentului (UE) nr. 1407/2013. Proprietarul infrastructurii, este reprezentat de entitatea care va crea și opera Centrul de resurse, iar infrastructura respectivă nu va fi utilizată în scop economic decât în limita a 20% din capacitatea globală a infrastructurii, fiind o activitate pur accesorie. Nivelul de importanță al centrului este unul național, activitatea desfășurată în cadrul acestuia nefiind considerată ca având un impact asupra comerțului dintre statele membre.

Calendar*:* 2021 – 30 iunie 2025

I10. Transformare digitală în managementul funcției publice (Alocare 10 mil. euro)

Provocări:

Pilonul V al PNRR, își propune realizarea unor obiective specifice pentru îmbunătățirea guvernanței în condițiile unui sistem de luare a deciziei predictibil, fundamentat și participativ, asigurarea de servicii publice de calitate, bazat pe existența unui corp de funcționari publici profesioniști si bine pregătiți, consolidând rezistența și, acolo unde este necesar, adaptate la tranziția verde și digitală.

Reforma 2.1 *Reforma funcției publice prin digitalizare și managementul parcursului de carieră,* din cadrul acestui pilon V, adresează o serie de provocări, care, de-a lungul timpului au condus la dezvoltarea unei birocrații excesive, într-un cadru în care, capacitatea insuficientă de a furniza servicii publice de calitate, inclusiv digitale, au un impact negativ asupra cetățenilor și a mediului de afaceri.

Pentru susținerea realizării acestei reforme, în cadrul Componentei 7 *Transformare digitală,* vor fi finanțate acele proiecte de investiții ce vizează soluționarea provocărilor specifice precum:

- Lipsa alinierii datelor și integrarea tehnică între principalii actori MRU din administrația publică (ANFP, MMPS, ministerele cu statute speciale și Ministerul Finanțelor Publice), induse de raportările reduse și fiabilitatea datelor

- Fragmentarea și lipsa standardizării principalelor date MRU (structură organizatorică, evidența personalului și salarii) pentru sectorul public din România, inexistența de metode moderne de analiză de date și, prin extenso, împiedicarea realizării unui sector public bazat mai mult pe meritocrație și performanță. Module mai avansate de MRU, cum ar fi serviciile de tip “self-service”, analiză, managementul performanțelor, managementul carierei etc., lipsesc cu desăvârșire, iar calculul salarial este de asemenea complet descentralizat.

- Lipsa unui sistem centralizat de SIMRU, construit pe “nucleul” unui registru centralizat de personal corelat cu sistemul de state de plată.

Investiții propuse de către ANFP sunt două platforme distincte, cu funcționalități diferite dar interoperabile, astfel:

I. **E-ANFP** - Dezvoltarea și extinderea platformei de gestiune a funcționarilor publici (nivel central, teritorial, local) pentru toate procesele aferente parcursului de carieră și pentru interconectarea cu instituțiile colaboratoare

E-ANFP va fi un instrument de evidență şi management integrat care va fi gestionat de către ANFP, reprezentând actualizarea/dezvoltarea progresivă a sistemelor informatice existente la nivelul Agenției cu privire la managementul carierei funcționarilor publici de la nivelul administrației publice centrale, teritoriale și locale. Va permite monitorizarea, colectarea de date, o gestiune a informațiilor din dosarul profesional la nivel complex (date actualizate de către departamentele de resurse umane de la nivelul autorităților şi instituțiilor publice, inclusiv cele locale, copii scanate ale actelor administrative emise de conducătorii acestora etc.).

Obiectiv: E-ANFP vizează transformarea digitală a serviciilor oferite de ANFP beneficiarilor interni și externi, prin crearea unei platforme interactive și colaborative de gestiune standardizată și unificată a funcționarilor publici (nivel central, teritorial, local) pentru toate procesele aferente parcursului de carieră și pentru interconectarea cu instituțiile colaboratoare, prin extinderea/dezvoltarea sistemelor existente și asigurarea interoperabilității cu alte registre naționale și europene.

Sistemul informatic va cuprinde toate procesele de la on-boarding-recrutare până la evaluare, promovare, ieșirea din sistemul public, având la bază modelul cadrelor de competență și fișe de post standardizate, devenind o platformă de gestiune a funcționarilor publici (nivel central, teritorial, local) pentru toate procesele aferente parcursului de carieră

Prin E-ANFP se urmărește alinierea Agenției la dezideratele unei administrații inteligente care să aibă în vedere îndeplinirea atribuțiilor prin sisteme inovative care să ofere servicii de calitate sigure și rapide, de tipul:

- *Arhitectură Business Intelligence pentru ANFP* (management funcție publică/angajați administrația publică dosar profesional, cazier administrativ) - soluții pentru procesele de HR pentru administrația publică centrală, work force planning, talent management, etc).

- *Asistenți RPA (Robotic Process Automation)* ce vor asista beneficiarii interni și externi (persoane fizice și structurile de RU) prin oferirea de asistență directă în gestiunea carierei, verificarea diplomelor/certificărilor, generarea de mesaje predefinite, prioritizarea solicitărilor și direcționarea acestora către Call center/operator/Info center după caz, formulare inteligente, consolidarea proceselor de management gen SCIM, SMC și management de proiect, elaborarea raportărilor majore ale Agenției (acordare asistență și suport destinat cetățenilor, funcționarilor publici și instituțiilor publice).

Implementare:

Următoarele activități vor fi realizate:

- Angajarea de experți cooptați
- Analiza situației actuale

- Derularea procedurilor de achiziții publice (externalizarea serviciilor pentru dezvoltarea sistemelor IT, achiziția de hardware/software, servicii de formare, alte tipuri de servicii)
- Încheierea de parteneriate care să conducă la interoperabilitate între bazele de date și sistemele informatice disponibile la nivelul diferitelor instituții, în corelare cu strategiile naționale
- Dezvoltarea /extinderea sistemelor informatice
- Operaționalizarea platformei
- Elaborarea unei metodologii de utilizare a platformei ce va conține proceduri și instrumente de lucru
- Pilotare /Testare și operaționalizare sisteme informatice
- Instruire
- Promovare /diseminare

Grup țintă: E-ANFP va conține date și informații privitoare doar la funcționarii publici din administrația publică centrală, teritorială și locală, grupul țintă fiind personalul ANFP, personal din cadrul instituțiilor publice centrale

II. SIMRU - sistem integrat și unitar de management a serviciilor de resurse umane pentru administrația publică centrală

SIMRU reprezintă o platformă de gestiune internă aprofundată, utilizată intern de către autorități și instituții publice pentru a realiza procesele de management al resurselor umane, de tipul platformei de HR utilizată la nivelul Comisiei Europene, SYSPER, care va include procese interne de MRU automatizate/standardizate de tip: date administrare personal, management organizațional, management al timpului - pontaj, cereri concediu, evidență formare, setare obiective, raportare etc.

Obiectiv: Crearea și operaționalizarea SIMRU - sistem integrat de management al resurselor umane și asigurarea interoperabilității sistemelor informatice.

Valorifică sistemele informatice dezvoltate în cadrul proiectului SIPOCA 870 și contribuie major la reforma serviciului public, fundamentată pe modele și tendințe europene.

Prin acest sistem se va asigura:

- livrarea de servicii integrate de management al resurselor umane pentru administrația publică centrală, cu o platformă integrată de gestiune a documentelor și a datelor referitoare la angajați și angajatori, elemente colaborative - de tip self service (acces dosar profesional digital pentru angajat, generare adeverințe - automatizat, cazier administrativ, validare acte de studii etc.) și self management (actualizarea directă de către funcționar a propriului dosar profesional),

- servicii de raportare evidență bugetari, gestiune personal administrație publică, venituri salariale, elemente de carieră/ în vederea fundamentării politicilor publice guvernamentale (Open Government Data),

- analiză privind extinderea SIMRU cu un modul de servicii financiare integrate (SFI) asociate resurselor umane pentru administrația publică centrală (managementul prezenței/gestiunea și plata drepturilor salariale pentru administrația centrală - cel puțin pentru funcționarii publici, cu aderarea în mod voluntar a administrației locale.)

Implementare:

Următoarele activități vor fi realizate:

- Angajarea de experți cooptați
- Analiza situației actuale
- Derularea procedurilor de achiziții publice (externalizarea serviciilor pentru dezvoltarea sistemelor IT, achiziția de hardware/software, servicii de formare, alte tipuri de servicii)
- Încheierea de parteneriate care să conducă la interoperabilitate între bazele de date și sistemele informatice disponibile la nivelul diferitelor instituții, în corelare cu strategiile naționale
- Dezvoltarea /extinderea sistemelor informatice
- Operaționalizarea platformei (servicii integrate de management al resurselor umane)
- Analiză privind servicii financiare integrate asociate resurselor umane pentru administrația publică centrală
- Elaborarea unei metodologii de utilizare a platformei
- Pilotare /Testare și operaționalizare platformă
- Instruire
- Promovare /diseminare

Grup țintă: SIMRU se va adresa întregului personal din administrația publică centrală, inclusiv personal ANFP, personal din cadrul instituțiilor publice centrale

Ajutor de stat:

Investițiile/serviciile necesare implementării acestor măsuri vor fi achiziționate printr-o procedură competitivă, transparentă, nediscriminatorie și necondiționată, nefiind incidente astfel prevederile legislației din domeniul ajutorului de stat.

Calendar: 2022 - 31 decembrie 2025

I18. Transformarea digitală și adoptarea tehnologiei de automatizare a proceselor de lucru în administrația publică (Alocare 21,90 mil. euro)

Provocări:

Pe baza datelor înregistrate anterior izbucnirii pandemiei, performanța României a fost identică în patru din cele cinci dimensiuni DESI 2020 măsurate. În ceea ce privește serviciile publice digitale

și utilizarea serviciilor de internet, performanța României este cea mai scăzută înrândul statelor membre ale UE, această situație finnd cauzată de progresele lente înregistrate în general, dar și de evoluțiile politice și schimbarea mai multor guverne în ultimii patru ani.

În contextul actual, generat de pandemia de Covid19, au fost accentuate și mai mult deficiențele serviciilor publice din educație, sănătate, finanțe publice și justiție, respectiv rigiditatea acestora și lipsa de adaptare la cerințele actuale în materie de digitalizare a serviciilor oferite.

În general, administrația publică este nevoită să depășească aspecte precum: procese de lucru birocratice, utilizarea documentelor preponderent pe hârtie, sisteme IT fragmentate/insulare, multe camere tehnice (data rooms) instalate în diverse autorități publice.

Totodată, resursele tehnice și umane sunt limitate. La nivel de guvernare IT există carențe de coordonare cross-sector, iar interoperabilitatea este limitată. Pe de alta parte, capabilitățile de raportare, generarea de analize complexe și statistice sunt reduse, inclusiv pentru publicarea de date deschise. Această situație generează riscuri inerente de securitate cibernetică și în continuitatea operațională/business continuity.

Prin orchestrarea proceselor de automatizare se pot depăși obstacolele birocratice cross-sectoriale și evoluția proceselor operaționale din administrație într-o maniera agilă, care va duce la debirocratizare într-un mod organic și natural, prin implicarea tuturor actorilor. Acțiunile de modelare a proceselor de business vor fi în același timp un instrument de creștere al interoperabilității organizaționale definite de EIF (modul în care administrațiile publice își aliniază procesele de afaceri, responsabilitățile și așteptările pentru a atinge obiective convenite în mod comun și benefice reciproc, menținând în același timp utilizatorii în focus.)

Automatizarea proceselor robotizate (RPA), reprezintă o nouă categorie de software pentru întreprinderi utilizată în mediul digital, replicând modul în care angajații folosesc un computer pentru a desfășura procese operationale Există multe avantaje în adoptarea RPA, așa cum este ilustrat de Studiul Centrului Comun de Cercetare (JRC) al Comisiei Europene privind explorarea transformării guvernului digital în UE(Exploring Digital Government transformation in the EU). Soluțile de tip RPA sunt suficient dezvoltate, scalabile și reziliente pentru a putea fi utilizate de administrația centrală, într-o varietate de domenii, de la administrarea fondurilor, până la poliție, asistență medicală sau educație, deoarece poate sprijini calculele fiscale, controalele antifraudă, contractele managementul, raportarea criminalității, diagnosticarea asistenței medicale și gestionarea bazelor de date pentru studenți. Studiul menționat afirmă, de asemenea, că APR este capabil „să reducă erorile umane, să reducă costurile operaționale și să permită personalului să se concentreze asupra unor sarcini mai valoroase”.

Digitalizarea, alături de adoptarea tehnologiei de automatizare a proceselor de lucru/Robotic Process Automation (RPA) și a celor bazate pe inteligență artificială de către sectorul public, pot asigura creșterea productivității și implicit a rezilienței aparatului administrativ, sprijinind astfel o relansare economică mai rapidă.

Redefinirea design-ului de procese (Business Process Reeingineering), va conduce în mod implicit la o mai mare transparență și predictibilitate a serviciilor publice oferite cetățenilor.

Există trei piloni care contribuie la realizarea creșterii economice și recuperării post pandemice prin automatizare:

1. standardizarea proceselor, ca parte a continuității operaționale cu avantajul asigurării transparenței și predictibilității serviciului public pentru cetățean
2. creșterea eficienței prin centralizarea datelor și asigurarea unui format standardizat al acestora.
3. creșterea productivității, permise prin automatizarea proceselor.

Un recent raport McKinsey arată, de asemenea, că recuperarea post-pandemică va propulsa adoptarea rapidă a automatizării pentru a reproiecta procesele de lucru și pentru a face față unei cereri crescute de furnizare de servicii sau de îndeplinire a sarcinilor, deoarece automatizarea și-a dovedit eficiența în timpul pandemiei în soluționarea controlului costurilor și reducerea interacțiuni interumane, pentru a permite operațiunilor să continue fără a expune angajații la virus.

Obiectiv: Inițiativa europeană comună Digital Compass îndeamnă guvernele să-și consolideze canalele digitale și să reproiecteze furnizarea de servicii publice pentru a „oferi un acces holistic și ușor la serviciile publice cu o interacțiune facilă pentru cetățean utilizând în acelasi timp capabilități avansate, precum prelucrarea datelor, AI și realitatea virtuală". Un pas necesar îl reprezintă creșterea capacităților de infrastructură digitală, creștere esențială pentru a contribui la realizarea unei prelucrări masive a datelor în siguranță și cu o viteză de prelucrare adecvată astfel încât să existe un spațiu optim pentru operațiuni de automatizare scalabile.

UE a aprobat deja rolul RPA în îmbunătățirea proceselor publice în cadrul politicii sale industriale europene privind inteligența artificială (IA) și robotică. Deși sectorul privat are grade de adopție diferite ale tehnologiei, există deja exemple notabile de proiecte de automatizare bazate pe AI în sectorul public care ajută la îmbunătățirea rezilienței, reducerea inexactității, îmbunătățirea experienței angajaților și a cetățenilor, furnizarea de servicii și productivitatea internă. În același timp, automatizarea poate contribui la reducerea sarcinii administrative, deoarece procesele și operațiunile necesită mai puțin timp și necesită mai puține documente, ceea ce permite sectorului public să ofere cetățenilor servicii publice mai rapide, fără erori și mai centrate pe clienți.

Investițiile urmăresc susținerea transformării digitale la nivelul întregii administrații publice, precum și modernizarea acesteia prin finanțarea infrastructurilor digitale și implementarea tehnologiilor avansate adecvate workflourilor și proceselor specifice, redefinirea design-ului de procese (Business Process Reeingineering), îmbunătățirea serviciilor publice și a procesului decizional utilizând tehnologii digitale avansate. Pe lângă beneficiile obținute privind modernizare, eficientizare și consolidarea capacității de prevenție și reziliență a serviciilor publice se obține și o reducere a sarcinii costurilor derivate din toate investițiile tehnologice utilizând noi instrumente TIC flexibile, reutilizabile și interoperabile. Totodată timpul alocat de cetățean și firme pentru obținerea serviciilor necesare se va diminua considerabil.

Cu ajutorul acestor noi tehnologii, organizațiile din sectorul public vor putea servi cetățenii mai bine și mai rapid, reduce birocrația, obține mai multă productivitate și eficiență internă și vor ajuta angajații din sectorul public să gestioneze volume de muncă considerabile sau vârfuri de cereri

venite din partea cetățenilor. Spre deosebire de roboții fizici tradiționali, RPA implementează o forță de muncă virtuală - asistenți digitali - care sprijină angajații în activitățile lor zilnice, repetitive, mecanice, fără valoare de decizie sau creativitate umană.

RPA poate fi utilizat pentru a implementa o varietate de sarcini, unul din scenariile de implementare este utilizarea unor chat-boti pentru socializare și conversație care să înlocuiască canalele tradiționale de servicii guvernamentale. Acestea includ roboții de chat (agenți software care se concentrează pe limbajul scris / text), roboții conversaționali (concentrându-se pe limbajul vorbit și oferind o alternativă la interacțiunile telefonice) și agenții inteligenți (integrarea chaturilor și roboților conversaționali într-un singur sistem). Astfel de aplicații, potrivit unor autori, vor duce la reduceri semnificative de costuri și îmbunătățiri ale serviciilor dar si la asigurarea unor canele clasice de interacțiune(de ex - telefon voce) pentru interacțiunea cu cetățenii.

Reducerea implicării umane. Prin combinarea algoritmilor de inteligența artificială cu RPA se obține un instrument puternic pentru a înțelege, monitoriza, raționa, prezice, interacționa, precum și pentru a învăța și îmbunătăți răspunsurile - înlocuind potențial sau îmbunătățind multe sarcini îndeplinite de oameni. RPA este de așteptat să preia sarcinile obositoare, permițând personalului să se concentreze asupra celor mai importante. De exemplu verificarea unor documente scanate în format imagine ar putea fi realizată în mod automat fără implicarea factorului uman într-o activitate care nu necesită o calificare deosebită. Din punctul de vedere al utilizării serviciilor publice există trei beneficii care pot fi sumarizate astfel: „Mai multă transparență și responsabilitate, mai puțină corupție."

Tehnologiile digitale din administrațiile publice sunt, de asemenea, legate de transparență sporită și echitate în cel puțin trei aspecte. În primul rând, se referă la transparența deciziilor luate de funcționarii publici, în mare parte legată de deschiderea datelor către public. În al doilea rând, implicarea umană redusă menționată mai sus și prejudecățile umane (dez-intermediere). În al treilea rând, transparența sporită ar trebui să rezulte și din implementarea mai eficientă a politicilor și furnizarea de servicii, în special în domeniul impozitării și plăților.

Implementare:

Investiția vizează implementarea soluțiilor RPA în domeniul administrației publice centrale pentru a asigura o productivitate sporită, îmbunătățiri operaționale și fluxuri de lucru slabe. RPA este un dispozitiv de digitalizare utilizat din ce în ce mai mult de organizațiile din întreaga lume, atât în zonele private, cât și în cele publice. Creșterea gradului de conștientizare a RPA ca un motor rapid pentru digitalizare este recunoscută pe scară largă la nivel mondial.

MCID organizează o procedură de achiziție publică pentru selectarea unei firme de consultanță care să analizeze fluxurile de lucru existente în cadrul instituțiilor publice solicitante și care să propună utilizarea de soluții tehnologice de tip RPA adecvate pentru automatizarea sarcinilor laborioase, repetitive, bazate pe reguli. Ulterior, MCID organizează apeluri adresate instituțiilor publice care doresc să implementeze soluții RPA ca soluții la cheie oferite de consultantul selectat. Consultantul gestionează proiectul end-to-end, de la inițierea proiectului până la pregătirea operațională, inclusiv managementul performanței de bază.

Digitalizarea, împreună cu adoptarea proceselor robotizate (RPA) și a tehnologiei bazate pe inteligență artificială de către sectorul public, pot crește productivitatea și, astfel, reziliența aparatului administrativ, sprijinind astfel o redresare economică mai rapidă.

Prin tehnologia RPA, roboții software pot efectua sarcini computerizate și repetitive, rapide și fără erori, 24/7. Astfel, RPA permite organizațiilor să automatizeze sarcini manuale, laborioase, repetitive și bazate pe reguli, creând economii de timp pentru angajați, astfel încât aceștia să se poată concentra pe activități valoroase precum: mai mult timp pentru interacțiunile cetățenilor, activități care implică management și gândire strategică, luarea deciziilor sau activități în care sunt necesare creativitate și empatie. Instituțiile publice care au implementat RPA au beneficiat de: costuri administrative de operare reduse, productivitate crescută, erori reduse, conformitate și capacitate crescută de a gestiona volume mai mari de sarcini, reducere semnificativă a timpului de execuție și de răspuns pentru cetățeni. Timpul de implementare a proiectelor de automatizare RPA este scurt, tehnologia fiind un instrument de reacție rapidă la situații critice (pentru benchmarks poate fi accesat linkul https://digital.gov/pdf/rpa-playbook.pdf).

Deoarece RPA automatizează sarcinile, nu joburile, reprezintă în primul rând un instrument pentru creșterea capacității și reducerea volumului de muncă organizațional. Acest lucru permite angajaților să se concentreze pe sarcini cu valoare adăugată mai mare, în timp ce „asistenții lor digitali" efectuează sarcinile standard / repetitive. Cu toate acestea, RPA nu este doar o tehnologie de reducere a volumului de muncă. RPA fi implementat pentru a crește calitatea, a reduce erorile umane, a crește conformitatea, a consolida mediile de control și pentru a adăuga noi servicii în portofoliul unei organizații. De exemplu, dacă un angajat are capacitatea de a audita un eșantion de 10% din tranzacții, o automatizare RPA, care rulează 24/7, poate fi capabilă să auditeze întregul set de date și să trimită înregistrări neconforme pentru adjudecare. Din perspectivă guvernamentală, impactul adoptării pe scară largă a RPA este astfel important.

RPA diferă de soluțiile IT tradiționale prin capacitatea sa de a fi proiectat și implementat rapid. Automatizările RPA sunt soluții direcționate de domeniu și complexitate limitate. Deoarece imită interacțiunile umane, nu este necesară analiza costisitoare a cerințelor de afaceri. Mai mult, pentru că sunt soluții „cu cod redus" sau „fără cod" necesită puține resurse tehnologice. Managerii pot obține rezultate semnificative în câteva săptămâni sau luni.

Automatizările RPA măresc calitatea muncii angajaților prin eliminarea sarcinilor repetitive și permițându-le să se concentreze asupra activităților critice.

Implementarea RPA contribuie la o serie de beneficii calitative, inclusiv:

1) precizie sporită;

2) creșterea conformității;

3) standardizare și auditabilitate îmbunătățite;

4) timpi de răspuns mai mici și o satisfacție crescută a clienților;

5) timpi de ciclu de proces reduși;

6) nivel ridicat de transparență și măsurabilitate.

Grup țintă: Administrația publică, instituțiile publice, angajații din sistemul public, respectiv cetățenii.

Ajutor de stat:

Investițiile/serviciile necesare implementării acestor măsuri vor fi achiziționate printr-o procedură competitivă, transparentă, nediscriminatorie și necondiționată, nefiind incidente astfel prevederile legislației din domeniul ajutorului de stat.

Calendar: 2021- 31 decembrie 2025.

B. Conectivitate digitală

a. Reforme

R2. Tranziția către atingerea obiectivelor de conectivitate UE 2025 și stimularea investițiilor private pentru dezvoltarea rețelelor de foarte mare capacitate

Comparativ cu celelalte componente ale Indexului DESI, România se situează mai bine la nivel european în ceea ce privește conectivitatea. Acoperirea de bandă largă de mare viteză a crescut până la 82%, dar se situează încă în urma majorității statelor membre (media UE este de 86%). Utilizarea benzii largi a stagnat la 66% dintre gospodării pentru al treilea an consecutiv și se situează cu mult sub media UE de 78%.

Provocări: Problema majoră o reprezintă persistența decalajului digital între zonele urbane și cele rurale, acoperirea cu 4G (85%) semnificativ mai mică decât media UE (96%). Unul dintre factorii principali care contribuie la lipsa investițiilor operatorilor telecom pentru construcția de rețele îl reprezintă barierele legislative în domeniul autorizațiilor de construire și al utilizării infrastructurilor fizice existente, care majorează necesarul investițiilor și reduce atractivitatea comercială a acoperirii anumitor zone geografice. Alți factori care contribuie la o cerere scăzută de internet îl reprezintă competențele digitale insuficiente, precum și gradul scăzut de digitalizare al sistemului public și al întreprinderilor.

Obiective: Obiectivele principale ale Reformei propuse le reprezintă adoptarea Legii de transpunere a Codului European al Comunicațiilor Electronice cu prevederi care să faciliteze autorizarea lucrărilor de construcții și realizarea investițiilor în infrastructuri și rețele telecom, Legii 5G, accelerarea introducerii pe scara larga, la nivel național a rețelelor 5G, în conformitate cu reglementările de securitate, și acoperirea în bandă largă a zonelor albe (localități rurale mărginașe, localități izolate, zone locuite defavorizate etc.).

Din perspectiva implementării Pilonului european al drepturilor sociale, această reformă urmărește să contribuie la îmbunătățirea situației privind dimensiunea „conectivitate” a indicelui economiei și societății digitale în conformitate cu Tabloul de bord social revizuit. Atât reforma cât și investiția propusă contribuie la flagship-ul european „CONNECT”, sprijinind accesul la servicii rapide în bandă largă pentru toate regiunile și gospodăriile.

Totodată, prin investițiile preconizate pentru acoperirea cu rețele de mare capacitate a zonelor albe se vor realiza premisele pentru eliminarea obstacolelor administrative inutile, eficientizarea procedurilor și a taxelor de acordare a permiselor, precum și facilitarea accesului la infrastructura

fizică pentru desfășurarea rețelelor de comunicații electronice, creând premisele accesului egal la servicii digitale și acces la internet.

Acest lucru va favoriza reducerea decalajelor urban/rural, astfel încât, atât întreprinderile cât și gospodăriile vor putea profita de transformarea digitală, având un impact pozitiv asupra accesului echitabil la educație de calitate, oportunități privind accesarea locurilor de muncă .

Prin îmbunăţirea accesibilităţii la serviciile digitale, sunt susținute inclusiv măsurile inițiativei Garanția pentru tineret, de ocupare a forței de muncă în rândul tinerilor, mai ales din zonele rurale, din regiunile mai slab conectate şi din grupurile sociale cele mai vulnerabile.

Prin asigurarea accesului la tehnologie de comunicații de foarte mare capacitate, mobilă si/sau fixa, se permite accesul universal la infrastructura si serviciile digitale publice, accelerând astfel dezvoltarea economica si tehnologica a României și adresând în același timp și Recomandarea Specifica de Țară (RST) 20_III.3 ce indrumă la direcționarea investițiilor către tranziția digitală și infrastructura de servicii digitale, cu prioritate, dar și RST 20_II.6 pentru asigurarea accesului egal la educație.

Implementare: MCID, Autoritatea Națională pentru Administrare și Reglementare în Comunicații si Autoritatea pentru Digitalizarea României vor colabora pentru facilitarea investițiilor operatorilor privați în construirea/upgradarea de rețele de comunicații de foarte mare capacitate menite să asigure acoperirea unor părți cât mai extinse din cadrul teritoriului national. Concret, instituțiile mai sus menționate vor propune actualizarea cadrului legislativ relevant pentru autorizarea lucrărilor de construcții și realizarea investițiilor, transpunerea Codului European al Comunicațiilor, aplicarea Recomandării CE 2020/1307 prevăzute în Connectivity Toolbox în acord cu foaia de parcurs națională și adoptarea legislației secundare în aplicarea Codului Comunicațiilor.

Autoritatea Națională pentru Administrare și Reglementare în Comunicații va organiza o procedură de selecție competitivă (licitație) pentru acordarea așa-numitelor „licențe 5G” (adică în benzile de 700 MHz, 1500 MHz și 3,4 - 3,8 GHz), bazându-se pe lecțiile învățate din licitații de spectru organizate în România (2012 și 2015) și cu proceduri similare recente în UE și va încorpora garanții competitive, mecanisme de formare a pieței și condiții atașate licențelor, toate potrivite pentru Specificitățile și dinamica pieței românești.

Pentru acordarea licențelor pe termen lung sunt avute în vedere criteriile Codului european al comunicațiilor electronice, pentru a stimula în mod eficient 5G, pentru a promova concurența și drepturile utilizatorilor finali.

Nivelul necesar de securitate a rețelelor și serviciilor 5G este asigurat odată cu intrarea în vigoare a legii securității rețelei 5G (Q2 2021). Principalele prevederi ale actul normativ sunt adoptarea unor măsuri referitoare la autorizarea producătorilor de tehnologii, echipamente şi programe software utilizate în cadrul infrastructurilor informatice şi de comunicaţii de interes naţional, precum şi în reţelele de comunicaţii electronice prin intermediul cărora se asigură servicii de comunicaţii electronice de tip 5G - reţele 5G, în vederea prevenirii, contractării şi eliminării riscurilor, ameninţărilor şi vulnerabilităţilor la adresa securităţii naţionale şi apărării ţării.

Furnizorii de comunicații vor putea utiliza tehnologii, echipamente și software numai în rețelele 5G de la producători autorizați în prealabil prin decizie a prim-ministrului, pe baza avizului Consiliului Suprem de Apărare Națională. Fiecare producător de echipamente și software 5G va trebui să solicite această autorizație, care va fi înaintată Ministerului responsabil pentru comunicații (MCID). Acordarea licentelor de utilizare a frecventelor radio ”5G” vor fi atribuite pe baza rezultatelor procedurii de selecție competitivă/licitației.

Implementarea foii de parcurs a României în aplicarea Toolbox-ului de conectivitate este un efort comun multipartit. Conform draftului, România va pune în aplicare pentru 12 din 39 de recomandări.

Până la finalul anului 2021 vor fi finalizate recomandările:

24 - Promovarea prețurilor de rezervă adecvate
25- Disponibilitatea la timp a benzilor armonizate 5G
28 - Regim de autorizare individuală pentru banda de frecvență 24,25-27,5 GHz
31 - Structura tarifelor de spectru recurente pentru a stimula implementarea
38 - Comunicare coordonată și direcționată pentru informarea și educarea cu privire la implementarea 5G
39 – Informarea publicului cu privire la conformitatea instalațiilor stațiilor de bază radio cu limitele de siguranță aplicabile EMF.

Iar următoarele recomandări vor fi finalizate până la finele anului 2022:

2 – Furnizarea de reglementări model privind desfășurarea rețelei de comunicații electronice
3 - Furnizarea de materiale informative și ateliere pentru municipalități și alte autorități competente
11 - Asigurarea disponibilității informațiilor din diferite surse și sporiți transparența lucrărilor civile planificate
26 - Revizuirea periodică a planurilor naționale de spectru
32 - Folosirea ajutorului financiar ca o completare pentru a stimula investițiile
35 - Uz de condițiile tehnice armonizate elaborate de Conferința europeană a administrațiilor poștale și de telecomunicații (CEPT) / Comitetul pentru comunicații electronice (ECC), dacă sunt considerate necesare intervale de frecvență dedicate comune.

În legislația ce va fi elaborată în cadrul acestei Reforme, vor fi prevăzute măsuri pentru:

- Analiza acoperirii infrastructurii telecom și a altor infrastructuri fizice care pot fi utilizate de rețelele telecom
- Identificarea lucrărilor publice planificate în zona de interes (utilități publice și alți furnizori de infrastructură)
- Identificarea potențialilor alți actori din zona de interes care ar putea sprijini proiectul de implementare de bandă largă ultra-rapidă
- Proiectarea, autorizarea și realizarea lucrărilor de construcții pentru șosele, autostrăzi și căi ferate, cu prevederea de trasee sistematizate pentru rețele de comunicații electronice

- Definirea unor standarde tehnice naționale în acord cu cele europene și internaționale, în comunicații și alte sectoare
- Asigurarea unor mecanisme optime (sub aspect tehnic, concurențial și al securității pentru schimbul de trafic de date între rețele (peering)
- Crearea unui plan coordonat pentru dezvoltarea infrastructurii de bandă largă, unui set de terminologie universală în vederea standardizării lucrărilor, unui cadru și a unor principii conexe pentru proiectarea rețelelor

Grup țintă: Reforma are caracter național (nu regional), se adresează nediscriminatoriu tuturor furnizorilor de rețele și servicii de comunicații electronice, în beneficiul tuturor utilizatorilor finali: persoane fizice, entități publice sau private.

Ajutor de stat:

Această componentă nu are buget alocat, în consecință nu este necesară achiziționarea de servicii de asistență/expertiză etc. pentru realizarea modificărilor legislative și prin urmare, nu implică acordarea de ajutoare de stat.

Calendar: 2021 – 30 septembrie 2023

b. Investiții

I11. Implementarea unei scheme de sprijinire a utilizării serviciilor de comunicații prin diferite tipuri de instrumente pentru beneficiari, cu accent pe zonele albe (Alocare 94 mil. euro)

Provocări: Chiar și în condițiile menținerii unei dinamici concurențiale sănătoase pe termen lung, precum și a implementării reformelor asumate, piața nu poate livra conectivitate în toate localitățile din România, conform obiectivelor UE 2025.

Lipsește actualmente un plan și a un cadru integrat pentru sprijinirea conectivității și a digitalizării sistemelor publice și a actorilor din sectorul privat, prin care aceștia să poată beneficia de conectarea la infrastructura de comunicații

Obiectiv: Acoperirea cu servicii de acces la internet de mare viteză, la punct fix a aproximativ 945 de localități (sate, inclusiv zonele locuite defavorizate precum cartierele mărginașe urbane sau rurale neacoperite de servicii de date sau așezările informale) în care, conform datelor ANCOM, piața nu poate livra astfel de servicii prin forțe proprii, în limita a 80 milioane de Euro, la nivel national .

Din perspectiva implementării Pilonului european al drepturilor sociale, această investiție urmărește să contribuie la îmbunătățirea situației privind dimensiunea „conectivitate” a indicelui economiei și societății digitale în conformitate cu Tabloul de bord social revizuit.

Implementare:

Au fost identificate două măsuri de investiții prioritare:

1. Prioritate absolută (P1), localități rurale complet albe, nedeservite cu rețele fixe, dar în care există cerere latentă și/sau inductori socio-economici (școală, grădiniăa, dispensar, instituție publică etc.). Este vorba în principal de localități rurale de mici dimensiuni (min. 50 locuitori/20 gospodării), în condiții geografice deosebite (de exemplu, rural îndepărtat, enclavizat, geografie atipică etc.). Prezența în aceste localități a unor inductori socio-economici nedeserviți de internet, reprezintă o mare pierdere de bunăstare socială/pentru perspectivele de dezvoltare a respectivei comunități, precum și indicii rezonabile privind relevanța și consistența cererii de internet de mare viteză. Estimăm minim 200-250 de astfel de localități.
2. Prioritate subiacentă (P2), localități rurale insuficient deservite cu rețele fixe, în care vitezele nu pot fi îmbunătățite prin forțele pieței, conform datelor ANCOM și pe baza angajamentelor rezonabile de investiții ale operatorilor. Estimăm minim 540 - 590 de astfel de localități.

Nu vor fi eligibile pentru finanțare localitățile pentru care vor exista planuri credibile de dezvoltare a unei rețele fixe de mare viteză în următorii 3 ani.

Din experiențele avute anterior a rezultat că succesul implementării unui proiect de ajutor de stat pentru creșterea gradului de conectivitate depinde foarte mult de implicarea autorităților locale care cunosc nevoile comunității și sunt în măsură să înlăture anumite bariere administrative. Prin urmare, localitățile eligibile pentru finanțarea publică se vor stabili, în ordinea solicitărilor primite din partea autorităților locale care se angajează să emită, în condiții facile și cu celeritate, autorizațiile de construire necesare și să perceapă tarife reduse sau chiar 0 pentru accesul tuturor operatorilor de comunicații electronice pe proprietatea publică a unității administrativ teritoriale în cauză.

Vor fi finanțate următoarele:

- infrastructură pasivă (stâlpi, canalizație subterană etc.) + elemente de rețea activă
- segment de distribuție (backhaul) + segment de acces (last mile)
- realizarea unei rețele noi sau modernizarea unei rețele existente

Investiția vizează următoarele:

- acoperirea cu internet de mare viteză a aprox. 30.000 – 40.000 de gospodării rurale îndepărtate, precum și a 200 - 250 de inductori socio-economici, care ar fi rămas neacoperite cu niciun fel de rețele în absența intervenției
- îmbunătățirea acoperirii la internet pentru aproximativ 80.000 – 90.000 de gospodarii rurale, precum și a 500 - 600 de inductori socio-economici, care nu ar putea beneficia de upgrade în absența intervenției
- conectarea la internet de mare viteză a 600 de inductori socio-economici suplimentari și a 60.000 de gospodării (estimare take-up)
- va fi realizată conectare la internet de mare viteză (viteza minimă de cel puțin 100 Mbps actualizabilă, în rețelele de tip FTTB / H și / sau 5G).

Grup țintă:

Utilizatorii de servicii de comunicații în desfășurarea activităților lor, operatori din industria telecomunicațiilor, Ministerul Cercetării, Inovării și Digitalizării, Direcția Generală Comunicații și Tehnologia Informației, alți actori relevanți identificați.

Ajutor de stat*:* Investiție se va implementa prin intermediul unei scheme de ajutor stat în temeiul GBER (actualul art.52 sau art.52 și art.52a din propunerea de modificare a GBER) sau, al unei scheme de ajutor de stat notificată la CE.

Calendar: 2021 – 31 decembrie 2025

- 2021 – planificare strategică Romania Gigabit 2025
- 2022 – organizare (stabilire localități eligibile, definire criterii de selecție, întocmire documentație licitație publică, selectare câștigători licitație publică)
- 2023 – 2025 – realizarea și punerea în funcțiune a investițiilor

C. Securitate Cibernetica

a. Reforme

R3. Asigurarea securității cibernetice a entităților publice și private care dețin infrastructuri cu valențe critice

Context: În ceea ce privește *Securitatea Cibernetică*, România se confruntă cu amenințări provenite din spațiul cibernetic la adresa infrastructurilor critice, având în vedere interdependența din ce în ce mai ridicată între infrastructuri cibernetice şi infrastructuri precum cele din sectoarele financiar-bancar, transport, energie și apărare națională. Globalitatea spaţiului cibernetic este de natură să amplifice riscurile la adresa acestora, afectând deopotrivă cetățenii, mediul de afaceri și cel guvernamental. Pentru România, securitatea cibernetică reprezintă o prioritate națională orizontală, acoperind domeniile economice și de apărare, inclusiv educația și formarea, exercițiile cibernetice specifice, activitățile de sensibilizare și apărarea cibernetică.

Pentru contracararea acestor amenințări, România a stabilit un număr unic de urgență pentru incidentele de securitate cibernetică (1911) care este operațional 24/7, devenind astfel prima țară din Europa și a doua din lume cu un astfel de sistem. Informațiile obținute au contribuit la lansarea mai multor campanii de prevenire și conștientizare, ar fi "Campania Ransomware în sistemul medical" și "Microsoft Tech Support Fraud".

Strategia de Securitate Cibernetică a României prezintă obiectivele, principiile și direcțiile majore de acțiune pentru cunoașterea, prevenirea și contracararea amenințărilor, vulnerabilităților și riscurilor la adresa securității cibernetice a României și pentru promovarea intereselor, valorilor și obiectivelor naționale în spațiul cibernetic și are ca obiectiv crearea unui sistem național integrat - Sistemul Național de Securitate Cibernetică (SNSC). În vederea realizării SNCS, au fost finalizate actele normative subsecvente implementării Directivei NIS, respectiv a Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice. Conform angajamentelor asumate, România a întreprins măsuri pentru a elabora cadrul normativ național în domeniul securității cibernetice armonizat cu prevederile legislației internaționale, care să

răspundă cerințelor internaționale și care să faciliteze, pe baze voluntare, cooperarea bilaterală și schimbul prompt și eficient de informații între autoritățile competente pentru combaterea utilizării infrastructurilor critice ICT în scopuri teroriste sau criminale.

Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cu modificările și completările ulterioare, stabilește cadrul juridic și instituțional, măsurile și mecanismele necesare în vederea asigurării unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice și a stimulării cooperării în domeniu, fiind (în linie cu scopul de creștere a încrederii în Piața Digitală Unică pe care Directiva 1148/2016 îl are) adresată în mod exclusiv operatorilor economici (publici sau privați) din două categorii mari:

- Operatorii de servicii esențiale din 7 categorii economice importante (Energie, Transporturi, Medical, Bancar, Piețe financiare, Furnizare de apă potabilă, Infrastructuri Digitale);
- Furnizorii de servicii digitale din 3 categorii: Motoare de căutare, Piețe online, Servicii cloud.

Legea creează un ecosistem național de prevenire și răspuns la incidente, prin stabilirea de cerințe de asigurare a securității informatice a serviciilor furnizate, cerințe de notificare a incidentelor survenite, mecanisme de răspuns la nivel național și de participare la răspunsul comun în cadrul ecosistemului european creat de Directiva NIS.

Centrul Național Cyberint (CNC - înființat în 2013) constituit ca unitate centrală fără personalitate juridică a Serviciului Român de Informații (SRI) are atribuții în domenii operaționale de securitate cibernetică (conform Regulamentului de Funcționare a Serviciului Român de Informații, aprobat prin Hotărârea Consiliului Suprem de Apărare a Ţării) și acționează pentru cunoaşterea, prevenirea şi contracararea vulnerabilităţilor, riscurilor şi ameninţărilor la adresa securităţii cibernetice a României. În baza atribuțiilor legale, CNC are în vedere asigurarea securității cibernetice a rețelelor și sistemelor informatice aparținând instituțiilor publice, precum și a infrastructurilor critice din domeniul IT&C, a căror afectare prin atacuri cibernetice poate genera impact negativ la adresa securității naționale.

Prin utilizarea soluțiilor de securitate cibernetică, CNC furnizează beneficiarilor legali informațiile necesare prevenirii, limitării sau stopării consecințelor unor atacuri cibernetice asupra sistemelor IT&C care reprezintă infrastructuri critice.

Prin Hotărârea Guvernului nr. 494/2011 s-a înființat Centrul Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO, cu atribuții atât în cadrul sectorului public, cât și în sectorul privat, structură independentă de expertiză și cercetare-dezvoltare în domeniul protecției infrastructurilor cibernetice care poate emite alerte și atenționări cu privire la activități premergătoare atacurilor cibernetice.

Prin intrarea în vigoare la 1 ianuarie 2019 a legii nr. 362/2018 prin care este transpusă, în totalitate, Directiva (UE) 2016/1148 a Parlamentului European și Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, CERT-RO a primit noi atribuții, devenind Autoritate Competentă la Nivel Național

pentru Securitatea Rețelelor și Sistemelor Informatice, Punct Național de Contact și CSIRT Național în domeniul de aplicare a Directivei NIS.

Provocări: În privința amenințărilor, atacurile cibernetice lansate de entități statale și non-statale (grupări de criminalitate cibernetică, grupări de hackeri cu sau fără motivație ideologică, politică sau extremist-teroristă) asupra infrastructurilor informatice și de comunicații cu valente critice, reprezintă o amenințare consistentă la adresa securității naționale, intensitatea, complexitatea și diversitatea acestora plasându-se pe o tendință evolutivă, în continuă creștere.

Din perspectiva riscurilor și amenințărilor conexe mediului virtual, digitalizarea României reprezintă atât un obiectiv major de interes social, cât și un obiectiv de securitate cibernetică națională, obiectiv identificat ca prioritar în cadrul mai multor documente strategice precum: Strategia Națională de Apărare a Țării 2020-2024, Strategia Națională de Securitate Cibernetică a României, Raportul de țară pentru România 2020, Strategia Națională pentru Dezvoltare Durabilă.

Conform Strategiei Naționale de Apărare a Țării 2020-2024, România se confruntă cu următoarele probleme: nivel redus de securitate cibernetică a infrastructurilor de comunicații și tehnologia informației din domenii strategice; acutizarea decalajului tehnologic şi valorificarea insuficientă a beneficiilor conferite de utilizarea noilor tehnologii; tendința exponențială de dezvoltare a tehnologiilor emergente (5G, inteligența artificială, big data, Internet of Things, cloud şi smart computing) generează, pe de o parte, nevoi de creștere și îmbunătățire a comunicațiilor care vor susține servicii digitale inovatoare menite să sprijine cetățenii și mediul de afaceri, iar, pe de altă parte, necesități de colectare și securizare a datelor şi informațiilor; potențialele vulnerabilități tehnologice ale rețelelor 5G; criptomonedele, tehnologia blockchain, inteligenţa artificială, machine learning, Internet of Things, Big Data, tehnologia cuantică sau Internetul Ascuns (Dark Web-ul) conturează perspective de utilizare a acestora în planul criminalității organizate, infracționalității cibernetice, activităților de profil hacktivist, terorist sau extremist.

Obiectiv: Creșterea arealului de protecție, prin valorificarea know-how-ului deținut, precum și prin promovarea de modele de bune practici în demersurile de asigurare a securității cibernetice, concomitent cu creșterea nivelului de securitate cibernetică a entităților publice și private care dețin infrastructuri cu valențe critice.

Sunt necesare stabilirea unor măsuri tehnice și organizatorice adecvate și proporționale pentru a gestiona riscurile la adresa securității cibernetice și rezilienței rețelelor, a sistemelor informatice și interoperabilității acestora.

Prioritatea acordată la nivel național securității cibernetice se reflectă, de asemenea, în sistemul educațional, care plasează drept unul dintre principalele sale domenii de interes programele educaționale digitale și cibernetice. La nivel național, peste 15 programe de securitate cibernetică au fost dezvoltate în peste 11 universități și licee, pe teme variind de la securitatea cibernetică a sistemelor informatice militare, criptografie, investigații digitale la învățarea automată și securitatea rețelelor. Astfel, se constată necesitatea dezvoltării de noi competențe de securitate cibernetică prin crearea unui „set de instrumente” cu aplicabilitate în domeniile prioritare și a unui

portofoliu de servicii de pregătire profesională pentru absolvenți și studenți pe tematici precum: igienă cibernetică, control si protecția datelor, siguranța utilizării noilor tehnologii.

În perspectiva operaționalizării Centrului European Cyber de la București, Centrul Național Cyberint va contribui, alături de celelalte instituții cu competențe în domeniul securității naționale, la:

- dezvoltarea unei platforme transparente de schimb de informații în domeniul securității cibernetice, la nivel european;

- dezvoltarea și permanentizarea unui dialog la nivel european, în domeniul securității cibernetice (best practices, lessons learned);

- cooperarea în planul cercetării și inovării în domeniul securității cibernetice (în special pe componenta ce vizează infrastructurile critce din domeniul IT&C);

- cooperarea în planul susținerii și sprijinirii experților în domeniul securității cibernetice.

La nivel național, Centrul Național Cyberint coordonează, în cooperare cu toate instituțiile cu responsabilități/atribuții în domeniul securității cibernetice, elaborarea *Proiectului Strategiei Naționale de Securitate Cibernetică 2021-2026,* care include viziunea strategică privind eforturile României pentru:

- protecția rețelelor și sistemelor de calculatoare prin menținerea în parametri normali a disponibilității, continuității, integrității și pentru asigurarea rezilienței acestora;

- evaluarea și actualizarea periodică a cadrului normativ și instituțional în domeniul securității cibernetice;

- consolidarea parteneriatului public-privat-academic pentru creșterea nivelului de reziliență cibernetică a întregii societăți;

- asigurarea măsurilor reactive și proactive pentru a dezvolta capacitatea de a răspunde atacurilor cibernetice și rezilienței sistemelor, rețelelor și serviciilor;

- consolidarea rolului României în arhitectura de securitate cibernetică la nivel internațional.

În acest moment, proiectul Strategiei Naționale de Securitate Cibernetică 2021-2026 (document de politici publice referitor la protecția rețelelor IT și OT) este finalizat, aflându-se în procedura de aprobare.

De asemenea, Centrul Național Cyberint a contribuit activ la elaborarea *Legii apărării și securității cibernetice a României*, care va stabili cadrul legal și instituțional pentru organizarea și desfășurarea activităților în domeniile securității cibernetice și apărării cibernetice, mecanismelor de cooperare și responsabilităților instituții din domeniile menționate. Se preconizează intrarea în vigoare a acesteia în Q4 2022.

Implementare: Centrul Național Cyberint are rol central în cadrul *Sistemului național de protecție a infrastructurilor TIC de interes național împotriva amenințărilor provenite din spațiul*

cibernetic, prin intermediul căruia este asigurată securitatea cibernetică a infrastructurilor TIC cu valențe critice.

Reforma C *Creşterea arealului de protecție și asigurarea securității cibernetice a entităților publice și private care dețin infrastructuri cu valențe critice* va asigura securitatea cibernetică și reziliența pentru sistemele de tehnologie operațională (OT), care deservesc infrastructurile atât în sectoare cheie (reglementate prin Directiva NIS: aprovizionarea cu apă, energie și transport), cât și în sectoare noi, elemente esențiale stabilite în proiectul Directivei NIS 2 (administrație publică, spațiu, apă uzată).

Până la operaționalizarea Centrului Cibernetic European din București, Centrul Național Cyberint va contribui activ la identificarea oportunităților și demararea proiectelor cu finanțare europeană și guvernamentală, privind consolidarea securității cibernetice și a rezilienței la nivel european, cu impact pozitiv, inclusiv la nivel național. Astfel, prin cooperarea cu Centrul Cibernetic European din București, sunt avute în vedere promovarea tehnologiilor care vor sprijini consolidarea securității cibernetice și a rezilienței, precum și dezvoltarea unui cadru legislativ pentru promovarea unui spațiu cibernetic deschis, liber, stabil și sigur.

De asemenea, având în vedere misiunile și atribuțiile Serviciului Român de Informații - Centrul Cibernetic Național, acesta va contribui la identificarea și reducerea factorilor de risc pentru Centrul Cibernetic European din București din perspectiva securității naționale, cu accent pe securitatea cibernetică.

Prin implementarea prezentei reforme, Centrul National Cyberint ***va deveni un nod central*** în domeniul securizării infrastructurilor IT[1] și OT[2], a căror afectare poate aduce atingere securității nationale.

În vederea asigurării securității cibernetice a infrastructurilor IT&C cu valențe critice, CNC colaborează cu Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO), autoritate competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice care asigură furnizarea serviciilor esențiale.

Totodată, structura de tip CERT din cadrul CNC îndeplinește rolul de Centru Operațional de Răspuns la Incidente de Securitate Cibernetică, având misiunea de a preveni și de a răspunde la incidente de securitate cibernetică. Ulterior adoptării HG nr. 584/2019 de modificare și completare a HG nr. 494/2011, CERT a fost reorganizat pentru operaționalizarea celor trei piloni stabiliți prin Legea nr. 362/2018. Urmare aprobării regulamentului de organizare și funcționare a CERT-RO, au fost elaborate proiectele de documente pentru demararea procesului de introducere în Clasificarea Ocupațiilor din România (COR) a noilor ocupații specifice domeniului securității cibernetice.

Centrul Național Cyberint va încheia acorduri de parteneriat cu entități publice și private care dețin infrastructuri TIC cu valențe critice pentru securitatea națională.

[1] Tehnologia informației - rețelele de calculatoare și de date

[2] Tehnologia Operațiilor - operațiuni ale sistemelor de control industrial - ICS și grupurilor de control al proceselor

Vor fi stabilite măsuri tehnice și organizatorice adecvate și proporționale pentru a gestiona riscurile la adresa securității cibernetice și rezilienței rețelelor, a sistemelor informatice și interoperabilității acestora prin:

- evaluarea stării de securitate și a vulnerabilităților rețelelor și sistemelor informatice;
- elaborarea de politici și proceduri de securitate cibernetică în conformitate cu standarde internaționale de securitate a informației și sistemelor informaționale, de management al riscului, sau cu cerințele legale aplicabile;
- folosirea de soluții care utilizează inteligența artificială;
- asigurarea interoperabilității între componentele informatice de securitate;
- protecția sistemelor informatice și a informațiilor vehiculate la nivelul instituțiilor, autorităților publice şi operatorilor privaţi;
- asigurarea de condiții optime de securitate cibernetică pentru facilitarea desfășurării de la distanță a activității angajaților;
- eficientizarea și crearea de premise pentru a continua modernizarea infrastructurilor TIC cu valențe critice pentru securitatea națională, inclusiv prin minimizarea timpului dedicat activităților de recuperare și restaurare ca urmare a incidentelor sau atacurilor cibernetice.
- cursuri de pregătire profesională în materie de securitate cibernetică specific pentru absolvenți și studenți (igienă cibernetică, control și protecția datelor, siguranța utilizării noilor tehnologii).

După dezvoltarea acestuia la nivel național, va fi pus la dispoziția tuturor operatorilor economici și administrațiilor publice centrale și locale, în mod gratuit.

Potrivit dispozițiilor Legii nr. 92/1996 *privind organizarea şi funcţionarea Serviciului de Telecomunicaţii Speciale* (STS), cu modificările şi completările ulterioare, STS este organul central de specialitate, cu personalitate juridică, ce organizează, conduce, desfăşoară, controlează şi coordonează activităţile în domeniul telecomunicaţiilor speciale pentru autorităţile publice din România şi pentru alţi utilizatori prevăzuţi în anexa nr. 1 la Lege. Conform anexei nr. 2 la actul normativ mai sus mentionat, STS administreaza inclusiv rețele, infrastructuri, sisteme, servicii și aplicații în diferite tehnologii informatice și de comunicații, cu soluții de securitate asociate.

Prin planul de măsuri stabilit în Strategia 5G pentru România, aprobată prin Hotărârea Guvernului României nr. 429/2019, Serviciul de Telecomunicații Speciale este desemnată instituția responsabilă privind lansarea serviciilor BB-PPDR (Broadband – Public Protection and Disaster Relief).

Prin Ordonanța de urgență a Guvernului nr. 73/2020, STS a fost desemnat *Integrator de servicii de comunicaţii critice în vederea asigurării continuităţii comunicaţiilor destinate autorităţilor publice cu atribuţii în managementul situaţiilor de urgenţă pentru asigurarea continuităţii actului de comandă şi control, atât la nivel strategic, cât și la nivelul echipajelor de intervenţie, în vederea gestionării situaţiilor de urgenţă cu potenţial de afectare a securităţii naţionale.*

Prin Hotărârea Guvernului nr. 245/2015 s-a aprobat cadrul strategic pentru dezvoltarea digitală, respectiv Strategia Națională privind Agenda Digitală pentru România (SNADR).

SPP este organ de stat cu atribuţii în domeniul siguranţei naționale, specializat în asigurarea protecției demnitarilor români, a demnitarilor străini pe timpul șederii lor în România, a familiilor acestora, în limitele competențelor legale, precum şi în asigurarea pazei sediilor de lucru şi a reședințelor acestora, potrivit hotărârilor Consiliului Suprem de Apărare a Țării.

În conformitate cu prevederile Legii nr. 191/1998 *privind organizarea şi funcţionarea Serviciului de Protecţie şi Pază (SPP)*, cu modificările și completările ulterioare, pentru îndeplinirea atribuțiilor ce îi revin, SPP colaborează cu Ministerul Apărării Naţionale, Ministerul de Interne, Serviciul Român de Informaţii, Serviciul de Informaţii Externe, Serviciul de Telecomunicaţii Speciale, cu celelalte ministere şi organe de specialitate ale administrației publice centrale şi locale. Instituțiile menționate sunt obligate să acorde SPP, în limita competențelor legale, sprijinul necesar îndeplinirii atribuțiilor prevăzute de lege.

Totodată, potrivit dispozițiilor Legii nr. 191/1998, cu modificările și completările ulterioare, pentru îndeplinirea atribuțiilor legale și exercitarea actului de conducere a tuturor forțelor participante, la nivelul SPP este necesară asigurarea schimburilor de date și cooperarea cu entități din țară și străinătate, aspect ce conduce la necesitatea implementării unui sistem de comunicații sigure, cu un grad ridicat de disponibilitate (fiabilitate).

STS și SPP vor asigura, în mod colaborativ, în funcție de atribuțiile legale ale fiecărei instituții, securizarea comunicațiilor destinate asigurării serviciilor de date, transmisii video și voce pentru autoritățile statului, printr-un concept integrat ce cuprinde și măsuri de protecție a comunicațiilor, protecție medicală și securitate cibernetică și analiză a informațiilor, transport și securitate a traseelor de deplasare, intervenție etc.

În vederea asigurării securității cibernetice a sistemelor IT&C și a rețelelor informatice este în curs de contractare proiectul Consolidarea capabilităților de prevenire, identificare, analiză și reacție la incidentele cibernetice, la nivelul Serviciului de Protecție și Pază şi sunt în curs de implementare două proiecte destinate creșterii capacității operaționale a SRI (Serviciul Român de Informații) și STS (Serviciul Telecomunicații Speciale): Actualizarea și dezvoltarea sistemului național de protecție a infrastructurilor TIC cu valențe critice pentru securitatea națională împotriva amenințărilor provenite din spațiul cibernetic (proiect dezvoltat de SRI, în parteneriat cu STS) și proiectul Sistem de protecție a terminalelor operaționalizate la nivelul SRI împotriva amenințărilor provenite din spațiul cibernetic (proiect dezvoltat de SRI).

Se află în implementare proiectul Sistem de alertă timpurie și informare în timp real RO-SAT, (dezvoltat de CERT-RO în parteneriat cu STS), prin care se urmărește creșterea nivelului de securitate a spațiului cibernetic național (instituții publice, companii private, utilizatori individuali), precum și creșterea capacității de răspuns la incidente de securitate cibernetică a CERT-RO. Ulterior adoptării, la 31 iulie 2020, a Hotărârii de Guvern privind aprobarea Notei de fundamentare referitoare la necesitatea și oportunitatea efectuării cheltuielilor aferente proiectului, au fost demarate procedurile de achiziții, care sunt în diverse stadii de realizare.

De asemenea, pentru creșterea capacității administrative în vederea implementării unui sistem unitar de management al calității și performanței, a unui sistem de coordonare și consultare cu factorii interesați precum și pentru sistematizarea legislației cu incidență și impact asupra investițiilor în dezvoltarea rețelelor de acces la NGN, este în curs de finalizare implementarea proiectului Sistem integrat de management pentru o societate informațională performantă (SIMSIP).

Grup țintă: Centrul Național Cyberint, CERT – RO, STS si SPP

Ajutor de stat:

Măsurile din cadrul acestei reforme nu implică elemente de ajutor de stat, fiind în general aspecte de natură administrativă, care nu implică un buget asociat

Calendar: 2021 – 31 decembrie 2022

b. Investiții

I12. Asigurarea protecției cibernetice atât pentru infrastructurile TIC publice, cât și pentru cele private cu valențe critice pentru securitatea națională, prin utilizarea tehnologiilor inteligente (Alocare 100 mil. euro)

Provocări: În contextul crizei COVID-19, la nivel global s-au intensificat și diversificat activitățile ostile din spațiul cibernetic. Actorii cibernetici utilizează contextul social actual pentru derularea de atacuri cibernetice, care au la bază tehnici de inginerie socială, inclusiv cu scopul de a afecta servicii din domenii cheie (producție, transport și distributie gaze naturale și energie electrică, sănătate; administrație publică; educație, transporturi etc.) cu impact ridicat la buna desfășurare a activităților curente de la nivel național.

Pentru respectarea restricțiilor impuse de pandemia COVID-19, majoritatea instituțiilor publice și companiilor private au adoptat, în regim de urgență, modelul work from home (telemuncă), accesarea de la distanță a rețelelor acestor entități devenind o necesitate pentru desfășurarea activităților curente. Astfel, prin eliminarea interacțiunilor dintre angajați a fost diminuat riscul răspândirii excesive a virusului SARS-CoV2, însă a crescut riscul expunerii infrastructurilor TIC folosite la atacuri cibernetice.

Sistemele informatice, care gestionează majoritatea infrastructurilor critice, reprezintă o ţintă predilectă a atacurilor cibernetice. Atacurile asupra sistemelor informatice, aparţinând unor instituţii ale statului sau aflate în proprietate privată, devin cu atât mai periculoase şi mai dificil de prevenit. Ele pot fi iniţiate atat de grupări de criminalitate organizată care vizează, în cele mai multe cazuri, obţinerea de resurse financiare, cat şi de către state ostile pentru obtinerea unor avantaje strategice. În acest context, principalele provocări au fost reprezentate de securitatea informațiilor vehiculate și a canalelor de comunicații, precum și de adoptarea și aplicarea măsurilor necesare menținerii unui nivel optim de securitate cibernetică.

Pe de altă parte, având în vedere că la nivelul Uniunii Europene a fost demarat Programul Europa Digitală, care urmărește creșterea capacităților digitale prin implementarea de tehnologii de ultimă

generație, la nivelul României se dorește alinierea la standardele impuse de la nivel UE prin creșterea gradului de digitalizare și interconectarea propriilor servicii digitale cu cele europene.

Având în vedere cele menționate anterior, este necesară extinderea și dezvoltarea la nivel național a mecanismelor de protecție impotriva atacurilor cibernetice în continuă evoluție, prin adoptarea de tehnologii de ultimă generație (artificial intelligence, machine learning, etc.) care să asigure mijloacele defensive optime pentru toate domeniile de interes național.

Obiectiv: creșterea arealului de protecție, prin valorificarea know-how-ului deținut, precum și prin promovarea de modele de bune practici în demersurile de asigurare a securității cibernetice, precum și creşterea rezilienţei, o condiție esențială pentru succesul activităţilor de protecţie a infrastructurilor critice. Reziliența infrastructurii este strâns legată de modul în care organizaţiile îşi gestionează riscurile strategice, operaţionale şi financiare. Astfel, proiectul vizează creșterea gradului de securitate cibernetică a sistemelor de securitate deja implementate în cadrul instituțiilor publice/entităților beneficiare, precum și a interoperabilității sistemelor de securitate care urmează să fie implementate și integrate cu sistemul informatic existent, în ceea ce privește coroborarea informațiilor, colaborarea, analiză și reacție prin intermediul mecanismului computerizat pentru alertarea rapidă și diseminarea informațiilor în timp real.

Din punct de vedere al securității cibernetice, Centrul Național Cyberint (CNC) operează un SOC (Security Operation Center), prin care oferă deja, încă din anul 2015, servicii de securitate cibernetică pentru instituții publice (*ex. din domeniul administrației publice, energetic, sănătății, finanțelor, educației şi cercetării*), în scopul securizării, modernizării și eficientizării activităților proprii, circumscrise domeniului TIC.

Acest SOC asigură securizarea rețelelor instituțiilor publice și protejarea datelor prelucrate și stocate. Rolul SOC-ului Centrului National Cyberint este de a detecta, analiza și răspunde la incidentele de securitate cibernetică detectate în cadrul infrastructurilor cu valențe critice prin exploatarea soluțiilor de securitate cibernetică. Pentru derularea de investigații cât mai aprofundate și mitigarea riscurilor de securitate cibernetică, Centrului National Cyberint derulează activități specifice, precum: analiză forensics, analiză malware, audituri de securitate cibernetică și management al incidentelor de securitate cibernetică. În cadrul acestui SOC sunt analizate evenimentele de securitate generate de la nivelul serverelor, stațiilor de lucru, bazelor de date, aplicațiilor, site-urilor web sau de la nivelul echipamentelor de comunicație și securitate, în scopul identificarii activităților anormale, precursoare ale incidentelor cibernetice, prin implementarea la nivel naţional a unui sistem de management centralizat (SIEM).

Personalul SOC cooperează cu echipele din cadrul infrastructurilor protejate pentru soluționarea rapidă a incidentelor de securitate.

În derularea activității, structura CERT - CNC cooperează cu CERT-RO, instituție ce deține rolul de autoritate națională cu competențe la nivel național în transpunerea măsurilor și cerințelor de securitate din Directiva NIS, în vederea creșterii securității rețelelor și sistemelor informatice ce susțin servicii esențiale.

Menționăm că legislația privind Directiva NIS nu acoperă momentan, în plan național, toate domeniile esențiale de interes, anumite domenii rămânând în afara spectrului de adresabilitate al

actualei directive. În acest context, proiectul propus de către Centrului National Cyberint are în vedere și acoperirea unor infrastructuri TIC cu valențe critice din domenii care nu se regăsesc actualmente în sfera de competență a CERT-RO, dar care prin rolul lor sunt importante pentru securitatea națională.

Având în vedere faptul că Centrul National Cyberint desfăşoară activităţi în scopul cunoaşterii, anticipării, prevenirii şi contracarării ameninţărilor la adresa infrastructurilor critice, proiectul propus cuprinde și infrastructuri OT, care deservesc sau reprezintă sisteme de control industrial ICS/SCADA.

Infrastructurile OT susțin domenii cheie din energie și industrie, un rol important în securizarea acestora constând în gestionarea riscurilor și vulnerabilităților de securitate cibernetică precum:

- posibilitatea de accesare în mod neautorizat a echipamentelor/sistemelor de comandă și control din cadrul unor infrastructuri critice;

- afectarea serviciilor de utilitate publică vitale (de ex. furnizare energie electrică, energie termică, apă, etc.) în urma unor atacuri cibernetice;

- perimarea tehnologiilor utilizate în cadrul infrastructurilor (uzură tehnologică);

- factorul uman care operează infrastructurile.

Din perspectiva securității cibernetice, prezintă relevanță riscurile ce se manifestă la nivelul infrastructurilor OT care sunt, în general, determinate sau conexe unor: deficiențe în monitorizarea acestora sau probleme apărute în depanarea și identificarea anomaliilor (ex. dacă sunt incidente sau configurări greșite ale echipamentelor), probleme ce țin de arhitectura infrastructurii (din teren, cele de control și de proces, din zona de business sau de management etc), disfuncții pe zona fluxurilor de comunicație, DMZ[3] etc.

Aducerea acestor infrastructuri OT în stare de funcționare în afara parametrilor optimi poate genera un impact considerabil la adresa securității naționale, care se poate traduce în pierderi sau prejudicii economice, afectarea vieții sociale sau chiar pierderea de vieți omenești.

Prin investiția curentă se urmărește creșterea nivelului de securitate cibernetică a entităților publice și private care deţin infrastructuri cu valenţe critice, prin:

- evaluarea stării de securitate și a vulnerabilităților rețelelor și sistemelor informatice;
- elaborarea de politici și proceduri de securitate cibernetică în conformitate cu standarde internaționale de securitate a informației și sistemelor informaționale, de management al riscului, sau cu cerințele legale aplicabile;
- folosirea soluțiilor care utilizează inteligența artificială;
- asigurarea interoperabilității între componentele informatice de securitate;
- protecția sistemelor informatice și a informațiilor vehiculate la nivelul instituțiilor, autorităților publice şi operatorilor privaţi;

[3] Demilitarized Zone

- întărirea securității cibernetice și a guvernantei IT, pentru îmbunătățirea accesului la informație și eficientizarea proceselor în tot sistemul judiciar (Ministerul Justiției și instituțiile subordonate, Consiliului Superior al Magistraturii, instanțele de judecată, Ministerului Public și parchetele, alte organizații din sectorul judiciar (ANABI, DNP, ONRC)

- asigurarea de condiții optime de securitate cibernetică pentru facilitarea desfășurării de la distanță a activității angajaților;

- eficientizarea și crearea de premise pentru a continua modernizarea infrastructurilor IT&C cu valențe critice pentru securitatea națională, inclusiv prin minimizarea timpului dedicat activităților de recuperare și restaurare ca urmare a incidentelor sau atacurilor cibernetice.

Implementare:

Proiectul va fi implementat de Unitatea Militară (U.M.) 0929 București prin Centrul Național Cyberint- Serviciului Român de Informaţii (CNC). Din punct de vedere tehnic, Centrul Național Cyberint administrează sistemul național de securitate cibernetică și care deține resursa umană specializată și know-how în domeniu și va administra infrastructura finanțată prin intermediul proiectului PNRR.

Serviciul Român de Informații (SRI) , cu statut de instituţie publică (Conform art. 1 din Legea nr. 14/1992) a desemnat U.M. 0929 pentru planificarea, programarea, coordonarea, asigurarea și controlul componentei de înzestrare a Serviciului Român de Informaţii. Centrul Național Cyberint va fi reprezentat în relația cu celelalte instituții și cu organismele finanțatoare de către Unitatea Militară (U.M.) 0929 București pentru implementarea proiectului în calitate de reprezentant legal

Deoarece UM 0929 București va avea calitatea de autoritate contractantă în cadrul procedurilor de achiziție publică a soluțiilor de securitate cibernetică, acestea vor intra în patrimoniul acestei instituții și vor fi puse la dispoziția beneficiarilor cu titlu gratuit. În acest sens, SRI prin U.M. 0929 București în calitate de deținător legal al bunurilor își asumă toate costurile legate de asigurarea garanțiilor și mentenanței sistemului pe durata de exploatare a acestuia (inclusiv asigurarea licențelor informatice necesare funcționării).

Pentru atingerea obiectivelor investiției este necesară dezvoltarea facilității dedicate Centrului Național Cyberint, respectiv de soluții de securitate cibernetică acoperind infrastructuri de tip IT și OT.

Următoarele activități vor fi derulate:

- Dezvoltarea capacității de protecție integrată a securității cibernetice a infrastructurilor TIC de tip IT și OT.

- Auditarea infrastructurilor TIC cu valențe critice în vederea identificării vulnerabilităților de securitate cibernetică, respectiv a dezvoltării și implementării de politici și proceduri de securitate și evaluare a riscului, în conformitate cu standardele internaționale sau cu legislația autohtonă în vigoare.

- Dezvoltarea unei infrastructuri tehnice cu rolul de identificare, monitorizare, management și reacție la incidente de securitate cibernetică destinat protejării infrastructurilor TIC cu

valențe critice pentru securitatea națională care nu/nu mai beneficiază de protecția oferită de Sistemul național de protecție a infrastructurilor TIC de interes național împotriva amenințărilor provenite din spațiul cibernetic, cu rol complementar acestuia.

- Implementarea unui program național de pregătire a operatorilor economici și a autorităților competente pentru situații de criză cibernetică și hibride, prin organizarea de exerciții și elaborarea planurilor de management a crizei.

- Stabilirea unei platforme naționale de evaluare și gestionare a riscurilor de securitate cibernetică ale noilor tehnologii.

- Implementarea unei infrastructuri destinată securității comunicatiilor radio, care va conduce la creșterea nivelului de protectie și a gradului de disponibilitate a serviciilor de comunicatii furnizare autorităților publice care oferă servicii digitale cetățenilor.

Prin realizarea activităților prezentate, se vor obține următoarele beneficii:

- Implementarea de metode, tehnici și procedee de control și gestionare a riscurilor și amenințărilor la adresa securității rețelelor de comunicații;

- Creșterea rezilienței infrastructurilor de comunicații wireless prin realizarea protecției spectrului de radiofrecvențe, în concordanță cu noile tehnologii 5G, IoT, care stau la baza implementării de proiecte de tip Smart City și Smart Village;

- Automatizarea proceselor de colectare, interpretare și decizie aferente activităților de goniometrie și monitorizarea a spectrului de radiofrecvențe;

- Implementarea de măsuri active în vederea creșterii disponibilităților serviciilor wireless, prin identificarea factorilor perturbatori și a interferențelor prejudiciabile ale spectrului de radiofrecvențe;

- Eficientizarea intervenției pentru neutralizarea factorilor perturbatori și interferențelor prejudiciabile ale spectrului de radiofrecvențe;

- Creșterea capacității de analiză și prelucrare a datelor colectate pentru îmbunătățirea serviciilor de wireless;

- Îmbunătățirea indicatorilor de conectivitatea și acces la serviciile publice digitale.

Proiectul propune asigurarea securității infrastructurilor a minim 101 instituții și entități, care au infrastructuri TIC de importanță critică pentru securitatea națională (IVC). Aceste entități vor include instituții din arcul guvernamental (ministere, agenții, autorități etc.) precum și entități din domeniul energetic (ex. furnizori/distribuitori de gaze, curent electric), domeniul serviciilor esențiale, domeniul sănătății, domeniul transporturilor (ex. aeroporturi, porturi) și domeniul alimentării cu apă și canalizării.

Entitățile nu au fost selectate până în acest moment, iar criteriile de selecție vizează următoarele:

- grad de vulnerabilitate la atacuri cibernetice
- impactul unui atac cibernetic asupra serviciilor prestate de către entități
- probabilitatea de a fi ținte ale unor atacuri cibernetice majore

- acoperire la nivel național/regional
- nr de beneficiari ai serviciilor prestate de către entități

Dupa selectarea entităților (entități din domeniul guvernamental, din domeniul energiei: de exemplu, furnizori/distribuitori de gaze sau electricitate; alimentarea cu apă și canalizare, servicii esențiale, sănătate și transport: de exemplu: aeroporturi, porturi etc.), luând în considerare cele de mai sus, vor fi incheiate cu acestea acorduri de parteneriat, însoțite de contracte de depozit în momentul recepției echipamentelor și soluțiilor, bază legală pentru a le pune la dispoziția beneficiarilor.

Entitățile vizate de proiect se împart în două categorii astfel:

- 59 de entități sunt incluse în lista beneficiarilor proiectului „*Actualizarea și dezvoltarea sistemului național de protecție a infrastructurii IT&C cu valori critice pentru securitatea națională împotriva amenințărilor cibernetice*" (codul SMIS 127221), fiind necesare asigurare de upgraduri.

Propunerea de implementare presupune crearea a două categorii de IVC-uri din punctul de vedere al probabilității cu care acestea pot fi vizate de atacuri cibernetice de tip APT, respectiv al impactului pe care un astfel de atac l-ar avea asupra infrastructurii și implicit asupra securității naționale și a statului român. Astfel, cele 59 de entități au fost împărțite în două categorii cu grade diferite de asigurare a securității cibernetice (motivat de constrângeri bugetare): 23 IVC-uri de categoria 1 și 36 IVC-uri de categoria 2, în cadrul cărora se vor realiza următoarele activități:

- Pentru IVC-urile de categoria 1, se vor îmbunătăți capacitățile soluțiilor cu rol de protecție a fluxurilor de web, mail și trafic de rețea și se vor implementa tehnologii de securitate la nivelul end-point-urilor (EDR) și de identificare a atacurilor avansate de tip APT. De asemenea, va fi crescută capacitatea de procesare a soluției de tip SIEM (sistem de management al incidentelor de securitate);

- Pentru IVC-urile de categoria 2 se vor îmbunătăți punctual capacitățile soluțiilor cu rol de protecție a fluxurilor de web, mail și trafic de rețea, precum și a sistemului de management al incidentelor de securitate. Beneficiarii de categoria 2 vor beneficia de soluții suplimentare față de cele incluse în proiectul menționat, pentru a fi aduse la același nivel de securitate cibernetică.

Având în vedere că UM 0929 București este autoritate contractantă și CNC este administratorul tehnic al sistemului, cel care va administra infrastructura pentru cele 59 IVC existente, practic va cunoaște soluția necesara upgradarii acestora, astfel încât se va evita dubla finanțare, precum și redundanțele în arhitectura soluțiilor și dotarea beneficiarilor finali. De asemenea, celor 59 de beneficiari le vor fi instalate și alte tipuri de echipamente și soluții, pe baza nevoilor constatate în cadrul site-survey-urilor efectuate.

Complementaritatea cu proiectul SMIS 127221, mai sus menționat, se realizează din rațiuni ce țin de valoarea totală a bugetului proiectului, prin care nu s-a putut asigura același pachet de

tehnologii de securitate cibernetică pentru toate cele 59 IVC-urile beneficiare. Acestea au fost grupate în două categorii:

1. Categoria 1 - 23 de IVC-uri au fost dotate cu pachetul întreg de tehnologii (Soluție de tip UTM/NGFW, Soluție Web Gateway, Soluție Email Gateway, Soluție de tip Endpoint Security, Soluție de tip detecție APT 1, Soluție de tip detecție APT 2, Soluție de tip Security Information and Event Management, Soluție de detecție IoC)

2. Categoria 2 – 36 de IVC-uri au fost dotate cu pachetul parțial de tehnologii (Soluție de tip UTM/NGFW, Soluție Web Gateway, Soluție Email Gateway, Soluție de tip Endpoint Security, Soluție de tip detecție APT 1 fără componenta EDR, Soluție de tip Security Information and Event Management)

Prin proiectul inclus în PNRR, se urmărește actualizarea pachetului de tehnologii pentru IVC-urile din Categoria 2 la Categoria 1 și integrarea a 42 de IVC-uri noi dotate cu pachetul de tehnologii din Categoria 1.

Suplimentar, pentru toate cele 101 IVC-uri definite, vor fi incluse costuri aferente operaționalizării unor tehnologii avansate de protecție cibernetică ce utilizează un spectru complex de măsuri ce permit identificarea amenințărilor cibernetice, inclusiv a celor ce nu sunt detectate prin echipamentele convenționale de securitate. Menționăm că aceste soluții tehnice sunt diferite față de cele incluse în proiectul SMIS127221, astfel încât se asigură evitarea dublei finanțări.

Totodată, 9 dintre cele 101 IVC-uri dețin infrastructuri de tip control industrial (ICS) și vor beneficia de o soluție de protecție dedicata, costuri care, de asemenea, sunt incluse în PNRR.

Deși 59 de infrastructuri sunt beneficiare ale ambelor proiecte, nu se creează situația dublei finanțări întrucât prin investiția din PNRR (investiția C1 Cybersecurity) pentru fiecare IVC se vor achiziționa exclusiv soluții de securitate cibernetică suplimentare celor existente.

- 42 dintre entități necesită infrastructuri noi vor fi dotate cu aceleași tipuri de soluții și tehnologii ca în proiectul menționat, precum și de soluțiile suplimentare, astfel încât beneficiarii finali - entități publice/private vor utiliza soluții de securitate cibernetică unitare.

Pentru un număr de 9 entități, din cele 101 entități beneficiare, sunt necesare soluții de securitate cibernetică de tip control industrial (ICS), care au infrastructuri de tip OT.

Astfel, la implementarea investiției sunt luate în considerare următoarele componente:

Securizarea noilor IVC (sunt luate în considerare 42 de IVC), cu operaționalizarea a cel puțin următoarelor soluții:

- ✓ Soluție de tip UTM / NGFW;
- ✓ Soluție Web Gateway;
- ✓ Soluție Gateway Email;
- ✓ Soluție Endpoint Security;
- ✓ Soluție de tip detecție APT (APT 1);

- ✓ Sistem complementar pentru detectarea și analiza atacurilor de tip APT (APT 2);
- ✓ Informații de securitate și soluție de gestionare a evenimentelor (SIEM);
- ✓ Soluție de detectare a COI;

Standardizarea nivelului de securitate cibernetică a infrastructurilor în cadrul sistemului național de protecție cibernetică (36 din cele 59 IVC sunt luate în considerare), cu operaționalizarea a cel puțin următoarelor soluții:

- ✓ soluție APT2;
- ✓ soluție de detectare și răspuns a punctului final APT Detection - (EDR);
- ✓ soluție de detectare a COI;

Securizarea infrastructurilor de control industrial (ICS) (se iau în considerare 9 IVC), cu operaționalizarea unei soluții de protecție APT (APT 3) a infrastructurilor de control industrial;

Activități de formare și activități legate de gestionarea resurselor umane:

- ✓ Servicii de instruire în domeniul securității cibernetice (pentru cel puțin 350 de studenți);

- ✓ Costuri asociate activității echipei de proiect / PIU (sondaj la fața locului la sediul IVC, arhitectura soluției, definirea specificațiilor și dezvoltarea procedurilor de achiziții, recepția, configurarea și integrarea soluțiilor, audit tehnic și de securitate online și la fața locului : echipă - consultanți experți IT, experți în formare, management de proiect)

Dezvoltarea capabilităților Centrului Național Cyberint, cu operaționalizarea a cel puțin următoarelor soluții:

- ✓ Platformă pentru securitatea și canalizarea datelor pentru transfer între rețele cu diferite grade de încredere, care include: hardware, licențe software, echipamente de comunicații;

- ✓ Creșterea capacității de investigare a CNC (soluții software și hardware);

Implementarea tehnologiilor concepute pentru a anticipa dezvoltarea atacurilor cibernetice (sunt luate în considerare 101 IVC), cu operaționalizarea a cel puțin următoarelor componente:

o Sistem avansat de detectare a vulnerabilităților în sistemele informatice și echipamentele de comunicații (soluții software și hardware);

o Sistem integrat de identificare a TTP-urilor asociate atacurilor cibernetice asupra rețelelor și sistemelor informatice (soluții software și hardware);

o Platforma complexă de securitate pentru analiza și procesarea automată a incidentelor cibernetice (soluții software și hardware).

Prin proiect vor fi achiziționate echipamente, soft-uri, programe care vor fi puse la dispoziția beneficiarilor indirecți.

Aceștia vor oferi date privind rețelele care urmează a fi securizate (de ex. arhitectura, număr de utilizatori, echipamente etc.) și vor permite accesul în vederea efectuării unor site-survey pentru a

stabili în detaliu nevoile de securitate, informatii care se vor regăsi în arhitectura sistemului și specificațiile tehnice din caietele de sarcini necesare procedurilor de achizitii. De asemenea, vor pune la dispoziție spațiile tehnice necesare amplasării echipamentelor, vor stabili de comun acord mecanismele de reacție și persoanele de contact și responsabile, precum și categoriile de informații care vor fi transmise de echipamente și soluții către nodul central/SOC (date vizând incidentele/alertele de securitate).

Totodată, beneficiarii indirecți vor permite instalarea echipamentelor de securitate cibernetică în cadrul rețelelor proprii, precum și colectarea, analiza și interpretarea evenimentelor de securitate în vederea identificării și blocării amenințărilor cibernetice.

Actualizarea soluțiilor de securitate implementate în cadrul infrastructurilor beneficiare trebuie luată în considerare, atât din punctul de vedere al necesității creșterii capacității echipamentelor de securitate, cât și din punctul de vedere al achiziționării de soluții complementare, prin intermediul cărora să fie detectate noi tipuri de amenințări cibernetice. Având în vedere că atacurile la nivel avansat (APT) sunt din ce în ce mai prezente și afectează echilibrul social, este esențial să fie implementate noi tehnologii de detectare a APT, complementare celor existente, pentru a crește șansele de identificare și blocare a acestor tipuri de atacuri. Acest lucru se poate face numai printr-o abordare integrată, necesitând implementarea de IVC-uri și soluții complexe de detectare APT la stațiile de lucru.

În plus, față de investițiile care vizează aceste entități, se are în vedere dezvoltarea infrastructurii aparținând Centrului Național Cyberint, investiția acoperând următoarele categorii de cheltuieli:

- Costuri pentru asigurarea noilor IVC (sunt luate în considerare 42 IVC);
- Costuri pentru standardizarea nivelului de securitate cibernetică a infrastructurilor în cadrul sistemului național de protecție cibernetică (36 din cele 59 IVC sunt luate în considerare);
- Costuri pentru securizarea infrastructurilor de control industrial (ICS) (sunt luate în considerare 9 IVC);
- Costuri cu formarea și resursele umane;
- Costuri pentru dezvoltarea capacităților Centrului Național de Cyberint;
- Costurile pentru implementarea tehnologiilor concepute pentru a anticipa desfășurarea atacurilor cibernetice (sunt luate în considerare 101 IVC).

În acest moment, România se află în proces de identificare a operatorilor de servicii esențiale legate de sectoarele prevăzute de Directiva INS (aprovizionare cu apă, transport, administrație publică, energie). Astfel, această inițiativă este anticipativă și propune includerea atât a operatorilor de servicii esențiali, în sectoarele stabilite prin Directiva NIS 1 (transpusă în legislația națională prin legea 362/2018), cât și a celor prevăzute în Directiva NIS 2, precum și alte infrastructuri din domenii considerate a avea valențe critice pentru securitatea națională (neacoperite de cele 2 directive NIS).

Grup țintă: Centrul Național Cyberint, UM 0929 București –SRI

Ajutor de stat:

Deoarece UM 0929 București -SRI, instituție publică centrală, va avea calitatea de autoritate contractantă în cadrul procedurilor de achiziție publică a soluțiilor de securitate cibernetică, acestea vor intra în patrimoniul acestei instituții și vor fi puse la dispoziția beneficiarilor indirecți cu titlu gratuit. Astfel, echipamentele și soluțiile finanțate prin proiect nu vor intra în patrimoniul beneficiarilor indirecți, astfel încât proiectul nu va avea un impact asupra capitalului social, cifrei de afaceri al acestora, ci vizează mecanismul necesar protejării entităților de atacurile cibernetice.

Investițiile/serviciile necesare implementării acestor măsuri vor fi achiziționate printr-o procedură competitivă, transparentă, nediscriminatorie și necondiționată, nefiind incidente astfel prevederile legislației din domeniul ajutorului de stat.

Calendar: 2021- 30 septembrie 2025

I13. Dezvoltarea sistemelor de securitate pentru protecția spectrului guvernamental (Alocare 38,53 mil. euro)

Provocări:

În vederea asigurării unui răspuns prompt și eficient la criza generată de COVID-19, STS a participat alături de autoritățile statului (Guvern, Secretariatul General al Guvernului, Ministerul Sănătății, Ministerul Investițiilor și Proiectelor Europene, Ministerul Economiei, Antreprenoriatului și Turismului, Ministerul Energiei) la asigurarea infrastructurii TIC necesare pentru asigurarea consolidării răspunsului la această criză și a bunei desfășurări a activităților de conducere.

De asemenea, Serviciul de Protecție și Pază (SPP) participă alături de Serviciul de Telecomunicații Speciale (STS) la asigurarea disponibilității și securității comunicațiilor necesare activităților de conducere de la nivelul autorităților publice.

Proiectul contribuie în mod esențial la securizarea comunicațiilor wireless de la nivelul instituțiilor și autorităților publice centrale și locale, prin asigurarea securității infrastructurii pe suport radio și a celorlalte infrastructuri ale STS, precum și la securizarea comunicațiilor destinate demnitarilor și obiectivelor cărora SPP le asigură protecția fizică.

Prin acest proiect se va susține transformarea digitală a serviciilor publice în servicii de calitate, sigure și rapide, în interesul cetățenilor, cu scopul de a crește satisfacția beneficiarilor de servicii publice și de a eficientiza resursele utilizate în procesele derulate de stat.

Astfel, având în vedere că în acest moment nu există această infrastructură de asigurare a securității comunicațiilor de bandă largă la nivelul autorităților statului, destinată protejării soluțiilor de comunicații radio de bandă largă, care să permită asigurarea disponibilității spectrului de radiofrecvențe, utilizat pentru transferul de date, transmiterea în timp real a imaginilor sau accesarea bazelor de date/utilizarea de servicii de date mobile de mare viteză, în scopul facilitării interacțiunii autorităților statului cu cetățeanul, este necesară realizarea unor sisteme de securitate pentru protecția spectrului guvernamental, pentru protejarea comunicațiilor radio, în vederea furnizării de servicii moderne de comunicații de bandă largă, inclusiv de tip *Mission Critical* în standard 3GPP, cum ar fi: Push-To-Video, Push-To-Data, Push-To-Talk.

Implementarea acestui proiect reprezintă o reformare foarte importantă a sistemelor de protecție a comunicațiilor radio destinate autorităților publice, prin introducerea, cu titlu de noutate, a soluțiilor tehnologice noi, prin intermediul cărora se va putea proteja transmiterea de imagini statice și dinamice și volume ridicate de date, aspecte ce nu sunt posibile în acest moment. Practic, forțele de intervenție vor beneficia de facilități tehnice suplimentare ce vor avea un impact major privind modalitatea de interacționare a autorităților publice cu cetățeanul.

Un alt avantaj important al asigurării protecției rețelelor este reprezentat de implementarea soluțiilor de securitate în conformitate cu standardele comerciale 3GPP cu aplicarea facilităților specifice de tip mission critical.

De asemenea, merită menționat faptul că, în contextul în care, la nivel european și internațional există o permanentă preocupare pentru implementarea de servicii de comunicații critice de bandă largă destinate autorităților publice ale statului, este necesară asigurarea de soluții de securizare corespunzătoare.

Pentru dezvoltarea și extinderea sistemelor de securitate pentru protecția spectrului guvernamental sunt necesare următoarele premise:

- existența resurselor umane bine pregătite și cu experiență, în implementarea și administrarea de infrastructuri complexe și performante IT&C, la nivel central și național;
- existența la nivel național a unei infrastructuri redundante proprii de comunicații și servicii;
- experiența de 25 ani în asigurarea serviciilor de asigurare a disponibilității spectrului radio pentru autoritățile publice din România;
- capacitatea asigurării de servicii integrate de comunicații și securitate;
- capacitatea de monitorizare a parametrilor tehnici ai serviciilor de la nivel fizic până la nivel aplicație, prin centre specializate de tip NOC (Network Operation Center), 24/7;
- capacitatea de monitorizare și tratare a evenimentelor/incidentelor de securitate prin centre specializate de tip SOC (Security Operation Center).

Obiective: creșterea nivelului de protecție și a gradului de disponibilitate al serviciilor de comunicații furnizate autorităților publice care oferă servicii digitale cetățenilor.

Obiectivul poate fi îndeplinit prin următoarele obiective specifice:

1. Implementarea unor mecanisme de prevenție a vulnerabilităților wireless în sistemele de comunicații;
2. Dezvoltarea unor soluții de detecție a vulnerabilităților wireless în sistemele de comunicații;
3. Crearea unui sistem unitar de management al vulnerabilităților wireless în sistemele de comunicații.

Implementare:

Având în vedere necesitatea asigurării continuității comunicaţiilor destinate autorităților publice centrale și locale din România, STS trebuie să mențină un grad ridicat de disponibilitate, reziliență și securitate a serviciilor de comunicații și tehnologia informației pentru furnizarea și digitalizarea continuă a statului român.

În acest sens, va crește nivelul de protecție și gradul de disponibilitate al serviciilor de comunicații furnizate autorităților publice care oferă servicii digitale cetățenilor.

Pentru îndeplinirea atribuțiilor sale legale vizând protecția fizică a demnitarilor, sediilor de lucru și reședințelor acestora, SPP va utiliza sisteme de protecție a comunicațiilor unitare și adaptate la noile tehnologii.

Acestea vor trebui să funcționeze atât în benzile de frecvențe radio, în care STS asigură protecția comunicațiilor, cât și în benzile de frecvențe radio în care SPP are atribuții legale să asigure acest tip de servicii.

Pentru aceste benzi de frecvențe radio SPP va asigura, ulterior implementării prezentului proiect, atât identificarea, monitorizarea și neutralizarea amenințărilor de tip UAV, cât și identificarea și blocarea amenințărilor din spectrul de frecvențe wireless (IED), în care funcționează acest tip de echipamente.

Pe cale de consecință, este necesară realizarea colaborativă, de către ambele instituții, în funcție de atribuțiile legale ale fiecăreia, a sistemelor de securitate pentru protecția spectrului guvernamental care fac obiectul prezentului proiect.

Proiectul presupune realizarea și implementarea unor sisteme de securitate pentru asigurarea protecției comunicațiilor wireless și creșterea gradului de disponibilitate al serviciilor de comunicații furnizate autorităților publice care oferă servicii digitale cetățenilor.

Autoritățile guvernamentale vor beneficia de următoarele facilități:

- implementarea de metode, tehnici și procedee de control și gestionare a riscurilor și amenințărilor la adresa securității rețelelor de comunicații;
- creșterea rezilienței infrastructurilor de comunicații wireless prin realizarea protecției spectrului de radiofrecvențe în concordanță cu noile tehnologii 5G, IoT, care stau la baza implementării de proiecte de tip Smart City și Smart Village;
- automatizarea proceselor de colectare, interpretare și decizie, aferente activităților de goniometrie și monitorizare a spectrului de radiofrecvențe;
- implementarea de măsuri active în vederea creșterii disponibilității serviciilor wireless, prin identificarea factorilor perturbatori și a interferențelor prejudiciabile ale spectrului de radiofrecvențe;
- eficientizarea intervenției pentru neutralizarea factorilor perturbatori și a interferențelor prejudiciabile ale spectrului de radiofrecvențe;
- creșterea capacității de analiză și prelucrare a datelor colectate, pentru îmbunătățirea disponibilității serviciilor wireless;

- îmbunătățirea indicatorilor de conectivitate și acces la serviciile publice digitale;

- creșterea capacității de protecție fizică a demnitarilor și obiectivelor prin identificarea, monitorizarea și neutralizarea amenințărilor de tip UAV și prin identificarea și blocarea amenințărilor din spectrul de frecvențe wireless (IED), în care funcționează acest tip de echipamente.

Pentru asigurarea unui nivel adecvat de securitate cibernetică, este necesară asigurarea securității rețelelor, care pot fi vulnerabilizate prin: compromiterea interfetelor de management, configurarea greșită a comunicatiilor intre centrele de date, expunerea la atacuri de tip DDoS sau lipsa masurilor de protecție privind atacurile care pot fi generate de resursele interne. Măsurile necesare pentru remedierea acestor posibilelor deficiente sunt realizate de Serviciul de Telecomunicații Speciale. Astfel, prin realizarea proiectului se realizează transformarea digitală a proceselor prin care se verifică automat dacă echipamentele funcționează în parametrii și la standardele necesare pentru buna funcționare a acestora, asigurând disponibilitatea serviciilor pentru autoritățile publice centrale și locale, asigurandu-se următoarele tipuri de servicii:

- Generarea automată de rapoarte de ocupare pentru a asigura o mai bună gestionare a resurselor guvernamentale de spectru radio pentru a asigura disponibilitatea și securitatea comunicațiilor radio în diverse tehnologii, inclusiv 3GPP, pentru autoritățile publice centrale și locale.

- Localizarea la nivel național a perturbatorilor de spectru guvernamentali și eliminarea acestora ducând la minimizarea timpului de intervenție pentru a crește disponibilitatea serviciilor radio furnizate.

- Optimizarea activității de gestionare a spectrului radio guvernamental, ceea ce duce la creșterea numărului de beneficiari care pot utiliza serviciile radio guvernamentale în același timp.

- Identificarea zonelor cu acoperire radio limitată pentru a extinde serviciile radio critice, în special pentru situații de urgență.

- Vor fi implementate mecanisme de prevenție a vulnerabilităților wireless în sistemele de comunicații;

- Vor fi dezvoltate soluții de detecție a vulnerabilităților wireless în sistemele de comunicații;

- Se va crea un sistem unitar de management al vulnerabilităților wireless în sistemele de comunicații.

Toate componentele sistemului, care constă din 18 puncte fixe, 65 de puncte de recepție și 10 vehicule speciale, oferă aceleași funcționalități enumerate mai sus, cu grade diferite de granularitate și contribuie la creșterea nivelului de protecție și disponibilitate a serviciilor radio furnizate autorităților care oferă servicii digitale cetățenilor și mediului de afaceri.

Rezultate:

- se vor asigura un număr de amplasamente fixe de localizare operaționalizate la nivel național (nr.): țintă - minim 18 (actual 0);

- se vor asigura un număr de amplasamente de recepție operaționalizate la nivel național (nr.): țintă minim 65 (actual 0) STS (Serviciul de telecomunicații speciale) conform Legii 92/96 este

autoritatea care gestionează spectrul radio cu utilizarea guvernamentală în România. Pentru a asigura disponibilitatea întregului spectru guvernamental, STS propune să se dezvolte o nouă rețea de senzori distribuiți la nivel național, care va fi plasat pe site-uri de recepție dedicate. Toți acești senzori amplasați în locațiile de recepție vor fi răspândiți în toată țara pentru a detecta și avertiza automat în caz de perturbări în spectrul radio-guvernamental. În acest fel, se va asigura disponibilitatea spectrului guvernamental și se va asigura continuitatea serviciilor radio guvernamentale furnizate cetățenilor și entităților publice, pe baza modelului G2G / G2B / G2C;

- se vor asigura un număr de autospeciale mobile destinate protecției rețelelor de comunicații: țintă minim 10 (actual 0).

Grup țintă:

STS asigură disponibilitatea spectrului de frecvențe guvernamentale pentru nevoile autorităților publice din România. Dintre acestea putem aminti instituțiile și autoritățile publice cu atribuții în gestionarea situațiilor de urgență, precum și Parlamentul României, Administrația Prezidențială, Guvernul României, autoritatea judecătorească, administrația publică centrală și locală și/sau unitățile aflate în subordine, Curtea de Conturi, Curtea Constituțională, organele de conducere din cadrul organismelor guvernamentale.

Ajutor de stat:

Beneficiarii acestei reforme sunt autorităţi publice. În plus, investițiile/serviciile necesare implementării acestor măsuri vor fi achiziționate printr-o procedură competitivă, transparentă, nediscriminatorie și necondiționată, nefiind incidente astfel prevederile legislației din domeniul ajutorului de stat.

Calendar: 2021 – 31 martie 2026

I14. Creșterea rezilienței și a securității cibernetice a serviciilor de infrastructură ale furnizorilor de servicii de internet pentru autoritățile publice din România (Alocare 18,39 mil. euro)

Provocări:

Orice reformă de digitalizare a serviciilor publice digitale la nivel central implică existența unei infrastructuri moderne de tip ISP (Internet Service Provider).

Conform anexei nr. 2 la Legea nr. 92/1996, cu modificările și completările ulterioare, Serviciul de Telecomunicații Speciale (STS) este desemnat să administreze rețele, infrastructuri, sisteme, servicii şi aplicaţii în diferite tehnologii informatice și de comunicații, cu soluții de securitate asociate și să ofere servicii de încredere calificată.

Astfel, STS asigură, prin intermediul sistemelor informatice și al rețelelor de comunicații pe care le administrează, accesul cetățenilor la serviciile publice de tip e-guvernare puse la dispoziție de autoritățile publice din România.

Având în vedere evoluția tehnologică este necesară creșterea numărului de puncte de acces la servicii de tip ISP, creșterea capacității de prelucrare, transfer, stocare a datelor, corelat cu

modernizarea mecanismelor de securitate și asigurarea unei disponibilități ridicate a serviciilor furnizate.

Pe de altă parte, dată fiind creșterea numărului de solicitări de servicii de tip ISP ca urmare a pandemiei COVID-19, precum și necesitatea de digitalizare a autorităților publice din România, pentru care STS asigură servicii de tip ISP, este necesară extinderea, modernizarea și securizarea infrastructurii existente prin creșterea capacității serviciilor de procesare, stocare, prelucrare si monitorizare, mărirea capacității de distribuție prin asigurarea unor legături de comunicații de mare capacitate (10G/25G/40G/100G), precum și prin introducerea unor mecanisme noi de securitate bazate pe noi tehnologii. Pentru serviciile menționate este necesară creșterea capacității de protecție cibernetică prin implementarea unor capabilități superioare de protecție împotriva amenințărilor provenite din spațiul cibernetic.

Pentru creșterea rezilienței și securității cibernetice a infrastructurii de servicii de tip ISP asigurate pentru autoritățile publice din România sunt necesare următoarele premise:

- existența resurselor umane bine pregătite și cu experiență, în implementarea și administrarea de infrastructuri complexe și performante IT&C, la nivel central și național;
- existența la nivel național a unei infrastructuri redundante proprii de comunicații și servicii;
- experiența de peste 15 ani în asigurarea serviciilor de tip ISP pentru autoritățile publice din România;
- capacitatea asigurării de servicii integrate de comunicații și securitate;
- capacitatea de monitorizare a parametrilor tehnici ai serviciilor de la nivel fizic până la nivel aplicație, prin centre specializate de tip NOC, 24/7;
- capacitatea de monitorizare și tratare a evenimentelor/incidentelor de securitate prin centre specializate de tip SOC/CERT.

Obiectiv: creșterea rezilienței și securității cibernetice a infrastructurii de servicii de tip ISP asigurate pentru autoritățile publice din România, prin îmbunătățirea accesului și creșterea capacității de furnizare a unor servicii publice digitale eficiente, implementarea capacităților digitale și asigurarea rezilienței cibernetice.

Obiectivul va fi îndeplinit prin următoarele obiective specifice:

- Modernizarea și extinderea rețelei de acces Internet de tip Gigabit pentru administrația publică și pentru serviciile publice asigurate;
- Modernizarea capabilităților de securitate cibernetică pentru serviciile asigurate de către STS;
- Securizarea serviciilor de tip ISP (DNS, WEB, EMAIL, HOSTING) furnizate autorităților publice;
- Creșterea calității serviciilor oferite de administrația publică prin asigurarea unor servicii de calitate, disponibilitate și securitate ridicată.

Prin modernizarea și securizarea serviciilor ISP ale STS, prin creșterea capacităților de furnizare de servicii de tip Internet si servicii asociate Internetului se va asigura diversificarea si funcționarea continuă a serviciilor puse la dispoziția cetățenilor de către autoritățile publice din România și se va atinge obiectivul general asumat prin proiect.

Implementare:

Implementarea proiectului presupune următoarele premise:

- STS asigură o arhitectură internet de tip ISP atât pentru nevoile proprii, cât şi pentru cele ale autorităţilor publice din România: Administraţia Prezidenţială, Guvernul României, Autoritatea Judecătorească, administraţia publică centrală şi locală;

- STS asigură facilităţi de găzduire şi distribuţie de servicii DNS, web, acces Internet, precum şi găzduire şi suport pentru aplicaţii de e-guvernare, găzduire şi hosting web, găzduire de conturi de email, în mod securizat;

- distribuţia serviciilor se realizează pe suport de comunicaţii rezilient, asigurat de către STS şi /sau contractat de la operatori economici de pe piaţa liberă;

- pentru toate serviciile furnizate, se asigură măsuri proactive şi reactive de securitate cibernetică prin structurile de tip CERT şi SOC (Security Operation Center) organizate la nivelul STS;

- schimbul informațional pentru asigurarea securității cibernetice va fi asigurat pe canale de comunicații dedicate cu celelalte instituții conform atribuțiilor legale;

- STS asigură, prin intermediul sistemelor informatice şi al reţelelor de comunicaţii, accesul cetăţenilor la serviciile publice de tip e-guvernare puse la dispoziţie de către autorităţile publice din România;

- s-a constatat o creştere extrem de mare de solicitări de servicii de tip ISP, ca urmare a efectelor pandemiei COVID-19, precum şi necesitatea de digitalizare a autorităţilor publice din România pentru care STS asigură servicii ISP şi de aceea este necesară extinderea, modernizarea şi securizarea infrastructurii existente, prin creşterea capacităţii de distribuţie și asigurarea unor legături de mare capacitate, precum şi prin introducerea unor mecanisme noi de securitate, bazate pe noi tehnologii, care să asigure un grad ridicat de protecţie cibernetică şi prin implementarea unor capacităţi superioare de protecţie împotriva ameniţărilor provenite din spaţiul cibernetic;

- având în vedere faptul că aplicaţiile de e-guvernare devin din ce în ce mai complexe, necesitând mai multe surse de procesare şi prelucrare, precum şi accesul simultan a mai multor utilizatori la aplicaţiile de tip e-guvernare, este necesară modernizarea sistemului de servicii şi comunicaţii de tip Internet Service Provider (ISP) STS, care să aibă un impact pozitiv asupra dezvoltării capacităţii digitale a statului roman în vederea asigurării unui acces facil, sigur şi rapid pentru cetăţeni şi mediul de afaceri la serviciile de e-guvernare;

- implementarea proiectului va genera un impact pozitiv asupra digitalizării statului român, asigurând bazele dezvoltării ulterioare de noi servicii publice digitale care vor putea fi oferite autorităţilor publice din România şi implict cetăţeanului, ca beneficiar final, bazele actualizării

aplicaţiilor existente de e-guvernare şi nu în ultimul rând bazele implementării cloudului guvernamental.

Prin modernizarea și securizarea serviciilor STS de tip ISP, prin creșterea capacității de furnizare a serviciilor bazate pe internet și conexiuni la internet se va asigura diversificarea și funcționarea continuă a serviciilor puse la dispoziția cetățenilor de către autoritățile publice române și atingerea obiectivului general al proiectului.

România este împărțită la nivel administrativ în 41 de județe. Astfel, rezultatele vor fi 41 de HUB-uri securizate de mare capacitate (care corespund celor 41 de județe la nivel național), conectate la o rețea națională de distribuție a Internetului, cu mai mulți furnizori de nivel I și mecanisme de securitate asociate, care asigură accesul autorităților publice centrale și locale la internet și servicii asociate internetului, pe baza modelului G2G / G2B / G2C.

- vor fi modernizate capabilitățile de securitate cibernetică pentru serviciile asigurate de către STS;

- vor fi disponibile legături de comunicații de tip Gigabit sau de capacitate superioară: 42;

- vor fi asigurate, suplimentar față de cele existente: 100 zone DNS, și 15.000 căsuțe email;

- instituțiile și entitățile de interes public vor avea posibilități de acces la servicii, la nivel central și local, în toate cele 41 de Hub-uri asigurate în urma implementării proiectului;

Servicii de securitate furnizate:

- Protecție anti-dos la multipli de 10Gbps

- Servicii CERT asociate (audituri de securitate, monitorizarea evenimentelor de securitate în întreaga rețea, răspuns la incidente de securitate)

- Servicii SOC asociate (mecanisme de notificare și escaladare pentru beneficiari)

- Mecanisme de reputație și filtrare pentru traficul rău intenționat bazat pe reputație și domenii rău intenționate la nivelul serviciilor DNS furnizate beneficiarilor

- Analiza sandbox pentru serviciile furnizate

- Mecanisme de detectare automată a traficului nelegitim pe baza mecanismelor furnizate de inteligența artificială

Grup țintă:

STS operează o infrastructură internet de tip ISP (Internet Service Provider) pentru nevoile autorităților publice din România, precum: Parlamentul României, Administrația Prezidențială, Guvernul României, autoritatea judecătorească, administrația publică centrală și locală și/sau unitățile aflate în subordine, Curtea de Conturi, Curtea Constituțională, organele de conducere din cadrul organismelor guvernamentale.

Ajutor de stat:

Beneficiarii acestei reforme sunt autorităţi publice. În plus, investițiile/serviciile necesare implementării acestor măsuri vor fi achiziționate printr-o procedură competitivă, transparentă,

nediscriminatorie și necondiționată, nefiind incidente astfel prevederile legislației din domeniul ajutorului de stat.

Calendar: 2021 – 31 decembrie 2024

I15. Crearea de noi competențe de securitate cibernetică pentru societate și economie (Alocare 25 mil. euro)

Provocări: Raportul DESI 2020 evidențiază faptul că ”*România a rămas în urmă în ceea ce privește indicatorii referitori la competențele digitale și are o performanță slabă în ceea ce privește digitalizarea întreprinderilor și serviciile publice digitale*”, iar prin Recomandările specifice de țară, atat cele din 2019_(III.2) cât și 2020_(II.5) se evidențiază necesitatea îmbunătățirii competențelor digitale Securitatea cibernetică reprezintă o prioritate națională orizontală, acoperind domeniile economice și de apărare, inclusiv aspecte ce țin educație și formare, exercițiile cibernetice specifice, activitățile de sensibilizare și apărarea cibernetică.

Obiective:

a) Crearea unui "set de instrumente" pentru creșterea competențelor în materie de securitate cibernetică cu aplicabilitate în domeniile prioritare ale economiei și societății.

b) Dezvoltarea unui portofoliu de servicii de pregătire profesională în materie de securitate cibernetică specific pentru absolvenți și studenți

Implementare:

In cadrul acestei investiții, pentru atingerea obiectivului propus, CERT-RO are în vedere doua sub-activități și anume:

I. Dezvoltarea unui portofoliu de servicii de pregătire profesională în materie de securitate cibernetică specific pentru absolvenți și studenți

Programul va fi implementat de MCID prin Unitatea de Transformare Digtală și va consta în următoarele activități ce vor conduce la dezvoltarea unui portofoliu de servicii de pregătire profesională în materie de securitate cibernetică specific pentru absolvenți și studenți (e.g. cursuri de igienă cibernetică, de un control mai riguros al protecției datelor și al securității utilizării noilor tehnologii).

a. Dezvoltarea și evaluarea unui curriculum național de securitate cibernetică de către CERT-RO la nivel pre-universitar și universitar.

Procesul urmat si ținte intermediare

- Termen 31.12.2021 – Identificarea și organizarea unui grup de formatori de curriculum (20 experți incluzând experți la nivel național și din UE).
- Termen 30.06.2022 – Elaborarea de către grupul de formatori de curriculum de orientări curriculare cuprinzătoare și flexibile în domeniul educației în domeniul securității

cibernetice, care să sprijine dezvoltarea viitoare a programelor și eforturile educaționale asociate la nivel pre-universitar și universitar.

- Termen 31.12.2022 – Elaborarea de către grupul de formatori de curriculum a unui volum curricular care structurează disciplina de securitate cibernetică și oferă îndrumare organizațiilor (academice, guvernamentale, business) care doresc să dezvolte sau să ofere servicii de pregătire profesională în materie de securitate cibernetică specific pentru absolvenți și studenți.
- Termen 31.12.2023 – Transfer de cunoștințe de la grupul de formatori de curriculum din România, către un grup pilot de 30 organizații din UE (academice, guvernamentale, business) care doresc să dezvolte sau să ofere servicii de pregătire profesională în materie de securitate cibernetică specific pentru absolvenți și studenți, in cooperare cu ENISA și cu Comisia Europeană.
- Termen 30.06.2026 – Transfer de cunoștințe de la grupul de formatori de curriculum către organizațiile din România (academice, guvernamentale, business) care doresc să dezvolte sau să ofere servicii de pregătire profesională în materie de securitate cibernetică specific pentru absolvenți și studenți.

b. Pregătirea în materie de securitate cibernetică a unui grup de 1.000 profesori anual, la nivel pre-universitar si universitar (train the trainer) cu organizarea unui laborator specializat dedicat in fiecare județ, inclusiv în sectoarele Bucureștiului).

Procesul urmat si ținte intermediare

- Termen 30.06.2022 – Identificarea si pregătirea unui nucleu de 25 de formatori specializați în livrarea unui curriculum pilot compact de cunoștințe de securitate cibernetică adresat profesorilor la nivel pre-universitar si universitar.
- Termen 31.03.2023 – Definirea cerințelor funcționale și a specificațiilor tehnice, avizarea indicatorilor tehnico-economici, achiziția și implementarea platformei tehnice ce va fi implementata de Romania (ca platformă Open-Source Software (OSS) / Software cu sursă deschisă) pentru sprijinirea laboratoarelor specializate din fiecare județ, inclusiv în sectoarele Bucureștiului.
- Termen 31.03.2023 – Definirea un model de livrare durabilă pentru implementarea programului de pregătire în materie de securitate cibernetică a unui grup de 1.000 profesori anual.
- Termen 31.12.2023 – Pilot la nivel European, livrat de România, incluzând pregătirea a 25 de profesori din UE pe curriculum-ul pilot compact de cunoștințe de securitate cibernetică adresat profesorilor la nivel pre-universitar si universitar.
- Termen 31.12.2023 – Faza 1, incluzând pregătirea a 1.000 de profesori din România.
- Termen 30.12.2024 – Faza 2, incluzând pregătirea a 1.000 de profesori din România.
- Termen 30.12.2025 – Faza 3, incluzând pregătirea a 1.000 de profesori din România.

- Termen 31.05.2026 – Evaluarea eficienței programului și a beneficiilor generate la nivelul României și la nivel UE.
- Termen 30.06.2026 – Faza 4, incluzând pregătirea a 1.000 de profesori din România.

c. Acreditarea de furnizori de servicii de formare și pregătire profesională în materie de securitate cibernetică specific pentru absolvenți și studenți (din Romania si din UE), inclusiv derularea de programe pilot

- Termen 30.06.2023 – Pilot.
- Termen 30.06.2026 – Acreditare anuală (perioada 2024 – 2026) a 10 de furnizori anual, de servicii de formare și pregătire profesională în materie de securitate cibernetică specific pentru absolvenți și studenți (furnizori din Romania si din UE)

Creșterea, diversificarea și o mai bună pregătire a studenților și absolvenților care intră în forța de muncă în domeniul securității cibernetice în România aduce beneficii societății. Astfel, prin creșterea nivelului educației pe această temă este sprijinită îmbunătățirea semnificativă a conștientizării necesității de asigurare a securității cibernetice pentru utilizatori, personalul operațional și factorii de decizie de la nivelul operatorilor economici, organismelor publice, și întreprinderilor. Prin urmare, formarea anuală a 1.000 de profesori va da un impuls semnificativ abilităților de securitate cibernetică la nivel național prin generarea unui efect pozitiv în cascadă.

II. Crearea unui set de instrumente pentru creșterea competențelor în materie de securitate cibernetică cu aplicabilitate în domeniile prioritare ale economiei și societății

Un alt program dezvoltat pentru atingere obiectivului investitiei îl constituie crearea si livrarea unui "set de instrumente si servicii guvernamentale" pentru creșterea nivelului de maturitate în materie de securitate cibernetică al celor 1.000 de actori cheie identificați. Criteriile pentru selectarea celor 1.000 de actori cheie ai administrației publice și economice vor fi similare celor pentru identificarea operatorilor de servicii esențiale și furnizori de servicii digitale, indiferent de dimensiunea acestora, în conformitate cu transpunerea Directivei NIS (și NIS 2) în dreptul românesc.

Acest set de instrumente va putea fi dezvoltat la nivel național și apoi pus la dispoziție gratuit către operatorii economici (mai ales întreprinderile mici și mijlocii) sau organele administrației publice centrale si locale.

a. Program național pentru analiza, revizuirea și documentarea nevoilor de competențe cibernetice și a consecințelor acestora asupra domeniilor prioritare ale economiei și societății.

Proces și ținte intermediare:

- Termen 30.06.2023 - Executarea unui inventar național și analize detaliate a cerințelor și nevoilor statului român, al economiei și societății românești de resurse umane, aptitudini și cunoștințe de securitate cibernetică.

- Termen 31.12.2023 - Consultarea actorilor cheie din învățământ, industrie, instituții publice pentru introducerea în programele și acțiunile prioritare ale acestora a unui set de masuri menite a reduce decalajul existent.
- Termen 31.12.2023 - Corelarea rezultatelor inventarului si analizei cu inițiativele la nivel european derulate în contextul implementării noii strategii de securitate cibernetică a UE pentru Deceniul Digital de către: European Union Agency for Cybersecurity (ENISA), European Defence Agency (EDA), European Security and Defence College (ESDC).

b. Evaluarea, documentarea și monitorizarea nivelului de maturitate în materie de securitate cibernetică (operațional, tehnologie, competențe) pentru 1.000 de actori cheie economici și din administrația publică (inclusiv companii, IMM-uri, școli, spitale, organisme ale administrației publice centrale și locale)

Procesul urmat și de ținte intermediare:

- Termen 30.06.2022 – Definirea și documentarea în cooperare cu European Union Agency for Cybersecurity (ENISA) a indicatorilor cheie privind maturitatea securității cibernetice a actorilor cheie economici și din administrația publică, pentru a fi măsurați efectiv.
- Termen 31.12.2022 – Validarea indicatorilor cheie privind maturitatea securității cibernetice a actorilor cheie economici și din administrația publică, împreună cu un grup de State Membre ale UE și în cooperare cu ENISA, și transferul de know-how dinspre Romania către acestea.
- Termen 31.12.2022 – Definirea cerințelor funcționale și a specificațiilor tehnice, avizarea indicatorilor tehnico-economici, achiziția și implementarea platformei tehnice ce va fi implementata de Romania (ca platformă Open-Source Software (OSS) / Software cu sursă deschisă).
- Termen 30.09.2022 – Identificarea si formarea/pregătirea unui nucleu de 100 experți pentru evaluarea, documentarea și monitorizarea nivelului de maturitate în materie de securitate cibernetică, prin utilizarea platformei tehnice.
- Termen 30.06.2023 – Evaluarea și documentarea nivelului de maturitate în materie de securitate cibernetică, prin utilizarea platformei tehnice.
- Termen 30.09.2026 – Monitorizarea continuă a nivelului de maturitate în materie de securitate cibernetică, prin utilizarea platformei tehnice. Raportare la nivel național și către instituțiile UE.

c. Crearea si livrarea unui "set de instrumente si servicii guvernamentale" pentru creșterea nivelului de maturitate în materie de securitate cibernetică al celor 1.000 de actori cheie identificați

Procesul urmat și ținte intermediare

- Termen 30.09.2022 - Identificarea și pregătirea unui nucleu de 50 de formatori specializați în livrarea setului de instrumente si servicii guvernamentale pentru creșterea

nivelului de maturitate în materie de securitate cibernetică al celor 1.000 de 1.000 de actori cheie identificați la nivel național.

- Termen 31.12.2023 – Pilot de livrare a setului de instrumente si servicii guvernamentale pentru creșterea nivelului de maturitate către primii 100 de actori cheie identificați.
- Termen 30.06.2024 – Faza 1, incluzând 300 de actori cheie identificați.
- Termen 30.06.2025 – Faza 2, incluzând 300 de actori cheie identificați.
- Termen 31.03.2026 – Faza 3, incluzând 300 de actori cheie identificați.
- Termen 31.05.2026 – Evaluarea eficienței programului și a beneficiilor generate la nivelul actorilor cheie implicati la nivel național, inclusiv impactul asupra întăririi securității și rezilienței cibernetice a sectoarelor publice și private critice românești, și la nivel UE.

Grup țintă*:* specialisti în securitate cibernetică, absolvenți, studenți, administrația publică

Ajutor de stat:
Pentru entităţile care desfăşoară activitate economică şi care vor beneficia de serviciile finanţate prin intermediul acestei reforme, se va realiza o schemă de ajutor de minimis, cu respectarea prevederilor Regulamentului (UE) nr. 1407/2013. Valoarea totală maximă a ajutoarelor de minimis de care poate beneficia o întreprindere unică este de 200.000 de euro pentru o perioadă de trei ani fiscali consecutivi.

Calendar: 2021-30 iunie 2026

D. Competențe digitale, Capital Uman și utilizarea Internetului

a. Reforme

R4. Creșterea competentelor digitale pentru exercitarea funcției publice și educație digitală pe parcursul vieții pentru cetățeni

Provocări:

Transformările rapide survenite în domeniul digitalizării din ultimul deceniu au condus către modificări ale vieții și muncii de zi cu zi, iar evoluția tehnologică bazată pe inovare remodelează atât societatea în ansamblul ei cât și piața muncii și viitorul forței de muncă. Una dintre principalele probleme apărute în acest interval de timp și cu care angajatorii se confruntă o reprezintă dificultatea în recrutarea lucrătorilor cu înaltă calificare într-o serie de sectoare economice, inclusiv în sectorul digital. Prea puțini adulți sunt pregătiți corespunzător sau recalificați pentru a ocupa astfel de posturi vacante, adesea pentru că instruirea nu este disponibilă la momentul și locul potrivit.

În ceea ce privește competențele digitale, România se situează pe locul 27 din cele 28 de țări ale UE în clasamentul Indexului DESI . România se află mult sub media UE în ceea ce privește persoanele cu competențe digitale de bază (31% vs. 58%), a persoanelor deținând competențe digitale avansate (10% vs. 33%) și a persoanelor cu competențe elementare software (35% vs. 61%). România se află considerabil în urmă și în ceea ce privește procentul de specialiști IT, din totalitatea persoanelor încadrate în muncă (2.2% vs. 3.9%).

Raportul DESI 2020 evidențiază faptul că ”*România a rămas în urmă în ceea ce privește indicatorii referitori la competențele digitale și are o performanță slabă în ceea ce privește digitalizarea întreprinderilor și serviciile publice digitale*”. Principalele bariere în calea realizării serviciilor publice digitale în România, identificate în acest raport, sunt:

- Lipsa de coordonare dintre instituțiile publice în ceea ce privește instituirea unor astfel de servicii;

- Migrarea specialiștilor IT din sectorul public înspre sectorul privat sau în străinătate;

- Lipsa generală de competențe digitale - nivelurile competențelor digitale de bază și avansate rămân cele mai scăzute în rândul statelor membre ale UE. Doar 31% dintre persoanele cu vârsta cuprinsă între 16 și 74 de ani au competențe digitale de bază (58% la nivelul UE în ansamblu), iar 10% au competențe digitale avansate (față de o medie a UE de 33%);

- Lipsa investițiilor în dezvoltarea competențelor digitale în rândul angajaților din sectorul public au condus la crearea de carențe cu impact ridicat, atât la nivel de front-office în dialog direct cu catățenii, cât și în back-office, pentru realizarea sarcinilor administrative.

De asemenea, ultima cercetare EIDES[4] conchide că intervențiile de politică publică în formarea capitalului uman reprezintă cea mai importantă intervenție în sprijinul dezvoltării antreprenoriatului digital. Firmele nu pot adopta cu succes tehnologii în lipsa unei forțe de muncă deținând competențe digitale. Mai mult, o tranziție de succes a companiilor către paradigma 4.0 este condiționată de deținerea unor competențe digitale avansate, precum cunoștințe de programare (coding) sau data analytics. În plus, conform observațiilor Băncii Mondiale în cadrul unui proiect de asistență tehnică România: Startup Ecosystem Strategy derulat împreună cu DG REFORM, dezvoltarea antreprenoriatului digital este frânată și de lipsa competențelor manageriale. De asemenea, pentru dezvoltarea și livrarea cu succes a serviciilor publice, este nevoie de funcționari publici având un nivel ridicat de competențe digitale.

Pe de altă parte, România oferă un bazin larg de specialiști TIC datorită sistemului său educațional în acest domeniu. România se situează pe locul 6 în rândul statelor membre ale UE în ceea ce privește numărul de absolvenți TIC (4,9% din totalul absolvenților). În anul universitar 2019-2020, România a avut peste 27.000 de studenți TIC înscriși în învățământul superior la toate nivelurile, atât în instituțiile publice, cât și în cele private. În aceeași perioadă, numărul absolvenților a ajuns la 5.365 la nivel național. În statisticile UE, România se află pe locul 3 la număr de femei specializate în domeniul TIC, cu mult peste media UE. Nu mai puțin de 24%

[4] The European Index of Digital Entrepreneurship Systems https://ec.europa.eu/jrc/sites/jrcsh/files/eides_2020.pdf

dintre absolvenții TIC din România sunt femei, oferind unul dintre cele mai favorabile medii incluziunii muncii.

Obiective:

Astfel cum s-a anunțat în cadrul Agendei pentru competențe în Europa și al Comunicării privind Spațiul european al educației, noul Plan de acțiune al UE pentru educația digitală 2021-2027 *Resetarea educației și formării pentru era digitală* prezintă o viziune pentru îmbunătățirea alfabetizării digitale, a competențelor și a capacității digitale la toate nivelurile de educație și formare și pentru toate nivelurile de competențe digitale (de la nivel de bază la nivel avansat). Acest Plan de acțiune susține obiectivul *Agendei pentru competențe* și prevede că 70 % dintre persoanele cu vârsta cuprinsă între 16 și 74 de ani vor avea cel puțin competențe digitale de bază până în 2025.

Prin investițiile direcționate spre dezvoltarea competențelor digitale, atât cele de nivel general, cât și în ceea ce privește competențele digitale avansate, se urmărește creșterea orizontului de posibilități pentru accesarea de noi locuri de muncă atât pentru populația generală, cât și pentru angajații din sectorul public, adresând totodată și inițiativa emblematică a UE ***Reskill and upskill.*** Creșterea competențelor digitale contribuie la crearea unei piețe interne funcționale, asigurând totodată o bază de recrutare de forță de muncă specializată care poate contribui la dezvoltarea sustenabilă a întreprinderilor din mediul privat și asigurarea competitivității ridicate a acestora.

Propunerile de investiții sunt destinate intregului teritoriu national, inclusiv pentru zonele rurale și regiuni mai isolate, pentru a fi mai competitive pe piața muncii, asigurându-se astfel premisele pentru îmbunătățirea condițiilor de viața, disparitatilor regionale, sociale si economice. Ele se adresează întregii populații a țării și pentru categorii diferite: de la cetățeni, la funcționari publici, administrație și mediul de afaceri, sprijinindu-se astfel accesul pe piața muncii pentru populație, cu precădere către locuri de muncă care necesită competențe digitale, cu respectarea principiului egalitatii de șanse și incluziunii sociale (prin accesul populației generale la programe de dezvoltare de competențe digitale).

Digitalizarea creează premisele și pentru asigurarea egalităţii de gen, în sensul participării egale a femeilor şi bărbaţilor pe piaţa forţei de muncă, precum și asigurarea unor avantaje ce țin de o mai mare flexibilitate pentru găsirea unui loc de muncă.

Atât Pilonul II *Transformare Digitală* cât și Pilonul VI *România Educată* al acestui Plan Național de Redresare și Reziliență tratează sinergic aspectele menționate mai sus.

În cadrul acestei componente a Pilonului II, este vizată realizarea Reformei clasificațiilor ocupațiilor în România și a câtorva investiții în vederea:

1. dezvoltării competențelor digitale specifice pentru funcționarii publici (măsură care va contribui, de asemenea, la digitalizarea administrației publice, venind în completarea Componentei 1 a acestui pilon),

2. dezvoltării competențelor digitale și a competențelor software ale forței de muncă (măsură care va contribui și la adoptarea tehnologiilor digitale de către mediul privat în completarea Componentei 4 a acestui pilon și a Pilonului III)
3. dezvoltării competențelor digitale ale cetățenilor României în general prin crearea unei rețele naționale a bibliotecilor ca hub-uri de învățare digitală.

- Se va efectua un studiu analiză diagnostic și prognozare pe următorii cinci ani a nevoilor forței de muncă în contextul transformării digitale a economiei și tranziției la paradigma 4.0 incluzând recomandări pentru definirea unor ocupații noi în nomenclatorul oficial al ocupațiilor. Analiza va fi realizată de către MCID Digital Transformation Task Force pentru a evita posibile întârzieri generate de lansarea procedurilor de achiziții, cu termen de realizare Q3 2022.
- Se va transmite o propunere către Ministerul Muncii și Protecției Sociale de introducere a unor meserii noi la nivelul Clasificării Ocupațiilor din România (COR) echivalente cu cele existente în țările Uniunii Europene cu bune practici în digitalizare;
- Se va proceda la ajustarea Ordinului nr. 1168 din 14 decembrie 2017 privind încadrarea în activitatea de creare de programe pentru calculator pentru includerea noilor meserii în rândul meseriilor de IT care beneficiază de scutire de la plata impozitului pe profit;
- Vor fi definite noile meserii în Clasificarea Ocupațiilor din România și inițiat un dialog cu universitățile din țară pentru deschiderea de materii noi în facultățile de profil, pentru crearea unor programe post-universitare dedicate calificării unor cadre universitare.

Implementare:

Într-o primă etapă MCID va realiza prin intermediul Task Force-ului propriu creat, o analiză diagnostic cu privire la situația curentă din perspectiva nevoilor și disponibilității competențelor digitale pe piața forței de muncă, precum și o anticipare a evoluțiilor mediului de afaceri românesc în implementarea *paradigmei 4.0*, a profesiilor viitoare și a nevoilor de competențe digitale pentru exercitarea acestora. Documentul va sta la baza elaborării unei politici publice de dezvoltare a competențelor pentru pregătirea forței de muncă pentru tranziția la *Industria 4.0*.

De asemenea, pe termen scurt, va fi creat un grup de lucru inter-instituțional format din MCID, Ministerul Muncii, Ministerul Finanțelor, Ministerul Economiei, Antreprenoriatului și Turismului, Ministerul Educației, Autoritatea pentru Digitalizarea României, Agenția Națională pentru Ocuparea Forței de Muncă, Comisia Națională de Prognoză, Secretariatul General al Guvernului/Direcția de Coordonare Politici și Priorități pentru revizuirea cadrului normativ de mai sus.

Ajutor de Stat :

Măsurile din cadrul acestei reforme nu implică elemente de ajutor de stat, vizând aspecte de natură administrativă/legislativă și nu implică realizarea de investiții, achiziționarea de servicii sau acordarea de resurse financiare.

Grup țintă: Operatori economici, angajați, șomeri.

Calendar: 2021 – 30 septembrie 2022

Investiții

I16. Program de formare competențe digitale avansate pentru funcționarii publici (Alocare 20 mil. euro)

Provocări:

Prezentul Program Național de Reziliență și Redresare își propune o intervenție amplă de digitalizare a serviciilor publice pentru cetățeni și companii și de digitalizare a operațiunilor interne ale administrației publice în scopul creșterii eficienței, transparenței și rezilienței instituționale.

Conform analizelor efectuate în contextul fundamentării și elaborării politicii publice în domeniul e-guvernării, *competențele digitale ale funcționarilor publici sunt insuficiente* pentru digitalizarea serviciilor publice și a operațiunilor interne din administrație, dezvoltarea competențelor acestora reprezentând una dintre măsurile complementare pentru implementarea e-guvernării.[5]

Obiectiv: Instruirea personalului din administrația publică va asigura creșterea nivelului competențelor digitale în administrația publică din România contribuind astfel la succesul măsurilor de digitalizare a serviciilor publice pentru și a operațiunilor interne ale administrației și va permite creșterea eficienței și rezilienței instituționale.

Implementare: În pregătirea programelor de formare se va realiza o analiză a nevoilor de formare pe competențe digitale (evaluare a nivelului actual de cunoștințe ECDL/ ICDL și competențe digitale existente, elaborare recomandări pentru instruire corelate cu profilul administrației publice) cu asistență tehnică (experți /servicii de formare /consultanță).

Până în prezent nu a fost efectuată nicio diagnosticare a nivelului actual al competențelor digitale ale funcționarilor publici. Această investiție va umple acest gol și va permite o intervenție adecvată, bazată pe dovezi și direcționată corespunzător.

Dezvoltarea competențelor digitale avansate se va realiza pentru un număr de 30.000 persoane (reprezentând aprox.20% din corpul funcționarilor publici, întrucât beneficiarii selectați necesită anumite competențe pentru o participare semnificativă și de succes), asumate de ANFP de tip ICDL și specializări IT&C (administrator baze de date (SQL, MySQL etc); Administrator de sistem; Analiști de business; Data analist; Programatori pe diverse platforme).

Totodată, vor fi derulate programe de formare de leadership și talent management în contextul digitalizării pentru 2.500 funcționari publici de conducere, reprezentând aproximativ 25% din totalul acestora. Competențele și specializările astfel obținute vor contribui la atragerea și retenția de specialiști IT și specialiști cu competențe digitale avansate. ANFP își propune ca minimum 80% dintre participanții la cursuri să obțină certificare. Cursurile vor fi desfășurate etapizat între 2022 și 2026.

[5] e-government public policy

Tehnologiile digitale au schimbat fundamental economia, societatea și modul în care se desfășoară afacerile. Managementul a fost transformat și prin apariția noilor tehnologii. Considerăm că managerii din sectorul public trebuie să țină pasul cu noile provocări, oportunități, abordări și instrumente aduse în era digitală.

Ne așteptăm ca managerii instruiți să acționeze ca agenți de schimbare în mediul lor de lucru și să transmită cunoștințele și abilitățile dobândite către colegii și colegii lor.

Această investiție începe în 2021 cu analiza necesității formării competențelor digitale. Ulterior, vor avea loc sesiunile de antrenament.

Pentru toate programele de formare se va asigura respectarea egalității de gen prin impunerea pragurilor minime stabilite prin legislația în vigoare referitoare la egalitatea de gen și asigurarea participării acestora la cursuri conform cotelor prevăzute în legislație.

Programele de formare vor fi livrate de furnizori specializați și acreditați ale căror servicii vor fi contractate în conformitate cu legislația de achiziții publice în vigoare.

Totodată, vor fi realizate analize impact al formării în domeniul TIC asupra activităților specifice derulate.

Analiza ex-ante se va baza pe un test inițial de competență și va determina ce tipuri de programe vor fi necesare, ce niveluri de certificare sunt necesare pentru fiecare beneficiar, precum și o analiză a capacității / competenței digitale actuale a fiecărui participant; se va elabora un profil general aplicabil tuturor participanților (un număr prestabilit de module), nivelul competențelor digitale vizate; analiza va pregăti harta pregătirii viitoare, pe județe, regiune, după nivelul de competență inițial și vizat, pe categorii de funcții publice (nivel executiv, management sau dacă este identificată o cerere / nevoie mai mare de formare pentru un anumit domeniu de serviciu public).

Recomandările specifice de țară din 2019 subliniază nevoi clare privind îmbunătățirea competențelor, în special a competențelor digitale, în special prin creșterea relevanței pe piața muncii, într-un context în care digitalizarea este văzută ca un factor cheie în îmbunătățirea inovației și competitivității țării. Abilitățile digitale de bază și utilizarea software-ului la nivel de bază sunt printre cele mai scăzute din Uniunea Europeană din România. Infrastructura digitală inegală și abilitățile digitale insuficiente au făcut dificilă trecerea la formarea profesională / educația la distanță în actuala pandemie. Una dintre recomandări este consolidarea abilităților digitale (recalificare și perfecționare) și învățarea digitală.

Indicele economiei și societății digitale (DESI) plasează capitalul uman din România pe locul 27 în UE în ceea ce privește competențele digitale, cu mult sub medie. Astfel, cel mai recent raport DESI indică:

• doar 29% dintre persoanele cu vârste cuprinse între 16 și 74 de ani au competențe digitale de bază (57% la nivelul UE în ansamblu);

• doar 10% au competențe digitale avansate (comparativ cu media UE de 31%).

În ceea ce privește certificatele obținute de participanții la instruiri, acestea au în vedere următoarele:

- *Pentru programele de instruire ICDL*: certificatul ICDL este recunoscut la nivel internațional și este valabil pentru o perioadă nedeterminată; în plus, competențele digitale dobândite sunt recunoscute pe tot parcursul vieții, în conformitate cu programele analitice aferente fiecărui modul în vigoare la momentul examinării. Module ICDL: nivel de bază (utilizare computer, instrumente online, editare text, foaie de calcul), nivel intermediar (prezentări, baze de date, editare web, editare imagini, securitate IT, CAD 2D, calcul, colaborare online, marketing digital, utilizarea informațiilor online), nivel avansat (editare text avansată, foaie de calcul avansată, baze de date avansate, prezentări avansate); se va utiliza un program de profil ICDL pentru a satisface nevoile și profilurile identificate în analiza ex-ante.
- *Programe de formare în conducere și gestionarea talentelor* - programe în parteneriat cu Institutul Național de Administrație (în temeiul articolului 458 alineatul (3) din Codul administrativ: programe de formare specializate care vizează dezvoltarea abilităților necesare exercitării unei funcții de management public sunt organizate de Institutul Național de Administrație) și/sau un furnizor de formare autorizat/acreditat conform legii; un program personalizat pentru leadership și managementul talentelor în contextul noilor tehnologii și al transformărilor digitale, completat cu certificate de participare, care certifică abilitățile de leadership în contextul noilor abordări tehnologice, noi provocări și instrumente ale erei digitale.
- *Programe TIC* - în funcție de tehnologia pe care o găzduiește instituția: Cisco, Microsoft, IBM, Linux, Oracle; certificate de participare sau certificate de absolvire

Grup țintă: ANFP, instituții ale administrației publice centrale, teritoriale și locale, INA, furnizori de formare Funcționarii publici din administrație, la nivel de execuție și conducere, specialiști IT&C, personal din cadrul structurilor de resurse umane, tineri profesioniști

Ajutor de stat:

Serviciile de formare profesională necesare implementării acestor măsuri vor fi achiziționate printr-o procedură competitivă, transparentă, nediscriminatorie și necondiționată, nefiind incidente astfel prevederile legislației din domeniul ajutorului de stat.

Calendar: 2021-30 iunie 2026

I17. Scheme de finanțare pentru biblioteci pentru a deveni hub-uri de dezvoltare a competențelor digitale (Alocare 37 mil. euro)

Provocari: Conform Eurostat, numai 21% din populația rurală din România și 32% din populația din orașe mici și suburbii au competențe digitale de bază (față de 39% din mediul urban mare) (Sursa https://ec.europa.eu/eurostat/web/products-eurostat-news/-/edn-20200207-1). Lipsa competențelor digitale limitează drastic posibilitățile de a-și găsi un loc de muncă sau a-și păstra un loc de muncă, de a se dezvolta profesional sau de a beneficia de oportunitățile oferite de era digitală.

Obiectiv:

- Crearea unei rețele sustenabile și scalabile, cu acoperire națională care să devină HUB-uri de dezvoltare de competențe digitale în comunitățile locale orientate pe dezvoltarea competențelor de bază și asigurarea unor servicii accesibile de formare unor categorii marginalizate prin transformarea rețelei de biblioteci, în prezent sub-utilizate. Modernizarea și extinderea a 105 de biblioteci dintre care 5 sedii centrale de biblioteci județene și 100 biblioteci biblioteci rurale sau municipale.
- Actualizarea/realizarea parcului de calculatoare și echipamente tehnice în 1030 de biblioteci.
- Deschiderea de MakerSpace-uri în 10 de biblioteci județene sau municipale precum și spații pentru Biblioteci de lucruri în 100 de biblioteci municipale, orășenești sau rurale. Dezvoltarea de sesiuni de instruire pentru utilizarea echipementelor aferente.
- Instruirea a 1100 de bibliotecari.
- Dezvoltarea de 6 curricule pentru competențe digitale de bază: alfabetizare digitală, comunicare și colaborare, alfabetizare media, creare de conținuturi digitale (inclusiv programare, proiectare și imprimare 3D), siguranță digitală (inclusiv combaterea bullyingului); educație educație financiară și antreprenorială.
- Instruirea a 100.000 de membri ai comunităților deservite de bibliotecile aplicante.
- Realizarea unei platforme de e-learning care să cuprindă și un repository pentru curriculele dezvoltate în cadrul programului, exemple de bune practici din bibliotecile aplicante, rezultatele de impact ale programului pentru a fi utilizate liber de biblioteci și alte entități interesate. Platforma va asigura condițiile de accesibilitate și pentru persoanele cu dizabilități sau nevoi speciale.
- Activarea unei aplicații de raportare automată care să ajute echipa care va realiza monitorizarea, evaluarea regională și națională precum și măsurarea impactului.

Implementare:

Finanțarea va fi deschisă de Ministerul Cercetării, Inovării și Digitalizării prin Unitatea de Transformare Digtală. Vor fi acordate granturi pe baza unei solicitări de finanțare pentru modernizări și extinderi de spații de biblioteci, achiziționarea de calculatoare/tablete și exhipamente instruire, dotare maker-space-uri și biblioteci de obiecte, instruirea membrilor comunităților. Finanțările vor putea fi solicitate de consorții formate din biblioteca județeană (cu rol coordonator) prin consliul județean și biblioteci rurale/municipale împreună prin consiliul județean și autoritatea locală. În funcție de situația din bibliotecile publice din județul respectiv, fiecare consorțiu va face o analiză de nevoi și va include în aplicație planul de activități. Din anul 3 de implementare, vor putea solicita finanțare și consorții formate doar din biblioteci locale prin autoritățile locale, chiar dacă la consorțiu nu participă biblioteca județeană/consiliul județean.

Pentru a asigura o implementare unitară la nivel național, activitățile de dezvoltare a curriculei, livrare a instruirii către bibliotecari, dezvoltare a platformei de e-learning, mentorat și coaching pentru bibliotecari, precum și cele de coordonare, monitorizare, raportare și evaluare vor fi implementate de la nivel național de către un organizație nonguvernamentală au experiență de lucru aplicat, în programe cu derulare națională, în domeniile: educație digitală, dezvoltare comunitară și instruirea bibliotecilor. Astfel, vor fi finanțate dezvoltarea a 6 curricule pentru competențe digitale de bază (alfabetizare digitală, comunicare și colaborare, alfabetizare media,

creare de conținuturi digitale, siguranță digitală; educație educație financiară și antreprenorială), instruirea bibliotecarilor, activități de mentorat și coaching pentru bibliotecari, dezvoltarea unei platforme de e-learning, activitati de coordonare, management de proiect, monitorizare și evaluare de impact, raportare. Echipa de monitorizare va achiziționa un soft (de tip CRM) pentru raportare automată, va asigura comunicare eficientă între echipele din consorții și unitatea de implementare precum și vizite de monitorizare și activități de măsurare a impactului. Organizația non-guvernamentală care va implementa aceste activități va fi selectată în urma unui apel competitiv de către Ministerul Cercetării, Dezvoltării și Inovării.

În caietele de sarcini pentru solicitările de finanțare va fi inclusă obligația beneficiarilor finanțării de se angaja să asigure praguri minime de participare a femeilor de 50% la programele de instruire și respectând toate prevederile legislației în vigoare în domeniul egalității de gen. De asemenea, în linie cu Principiul III al Pilonului european al drepturilor sociale, în vederea creșterii gradului de accesibilitate la programele de dezvoltare a competențelor digitale, vor fi utilizate criterii de stimulare a asumării unor ținte progresive de participare a persoanelor vulnerabile (cum ar fi: persoanele cu dizabilități sau cerințe speciale, persoane expuse riscului de sărăcie sau de excluziune socială, persoane în vârstă, romi sau alte minorități, persoane din comunități izolate). Modernizarea și extinderea spațiilor de bibliotecă va ține cont de reglementările în vigoare pentru accesibilizarea spațiilor pentru persoanele cu dizabilități.

Ajutor de stat:

Investițiile/serviciile necesare implementării acestor măsuri vor fi achiziționate printr-o procedură competitivă, transparentă, nediscriminatorie și necondiționată, nefiind incidente astfel prevederile legislației din domeniul ajutorului de stat.

Grup țintă: Bibilioteci, bibliotecari, persoane fără competențe digitale de bază, șomeri, comunități locale cu precădere din mediul rural și mic urban.

Calendar: 2022 - 30 iunie 2026

I19. Scheme dedicate perfecționării/recalificării angajaților din firme (Alocare 36 mil. euro)

Provocari: Analize[6] recente au arătat că transformarea digitală a economiei și tranziția către paradigma 4.0 este condiționată de o transformare a competențelor forței de muncă, inclusiv a modelului actualizare a acestora și o generalizare a programelor de formare pe parcursul vieții, precum și de o plajă amplă de noi competențe atât de tip soft skills cât, mai ales, tehnice, printre care competențele digitale precum programarea, securitatea cibernetică, analiza datelor devin necesare și pentru lucrătorii slab calificați. Studiul citat menționează, de asemenea, dificultatea mai ridicată a obținerii competențelor tehnice, comparativ cu alte tipuri de competențe necesare unei tranziții către paradigma 4.0.

[6] Skills for industry curriculum guidelines 4.0. Future-proof education and training for manufacturing in Europe. https://op.europa.eu/en/publication-detail/-/publication/845051d4-4ed8-11ea-aece-01aa75ed71a1

Lipsa competențelor forței de muncă a fost identificată ca a doua cea mai importantă barieră în calea investițiilor (72%) conform celui mai recent EIB Investors Survey în România.[7] Lipsa competențelor este identificată ca o barieră majoră și de analiza What holds Romanian firms back, raport care observă, în plus, că lipsa competențelor forței de muncă este percepută într-o măsură semnificativ mai mare de către IMM-uri decât de către întreprinderile mari.[8] În ceea ce privește competențele digitale, doar 31% din cetățenii României au competențe digitale cel puțin de bază, în vreme ce doar 10% au competențe digitale avansate. Totodată, conform datelor Eurostat, România ocupă ultimul loc în UE cu privire la firmele care au asigurat training pentru dezvoltarea/actualizarea competențelor digitale ale angajaților (6% din întreprinderi atât în 2020 cât și în 2019 față de 24% la nivel UE în 2019)[9].

Obiectiv: Intervenția are drept obiectiv să sprijine IMM-urile din România să își recalifice forța de muncă în domenii tehnice cheie (prgramare/coding, data analytics, cyber-security, computer-assisted design, additive manufacuring). Prin această intervenție se vizează atât creșterea competitivității forței de muncă cât și a firmelor.

Implementare:

Programul va fi implementat de MCID și va consta în următoarele activități.

- Dezvoltarea de către MCID a unei curricule naționale pentru upskilling-ul forței de muncă în ceea ce privește competențele digitale, în special pentru aplicarea folosirii unor tehnologii emergente (Cyber-Physical Systems, Robotics, Internet of Things, Big Data, Machine Learning, Artificial Intellignce, RPA, additive manufacturing, blockchain). Curricula va conține și teste standard de absolvire pe care beneficiarii programelor de training vor trebui sa le treacă. Curricule detaliate pentru fiecare dintre aceste subiecte, definirea obiectivelor de învățare, a instrumentelor, a cadrului de evaluare, a conținutului și a structurii materialelor de sprijin sunt încă de elaborat pentru care vor fi necesare expertize specifice care nu sunt disponibile în minister. MCID va achiziționa serviciile unui consultant privat în vederea realizării acestei curricule în conformitate cu legislația de achiziție publică – 1.000.000 EUR
- Dezvoltarea unei platforme de e-learning cloud-ready găzduită, inclusiv modul de testare de MCID. 50.000 EUR
- Cursurile vor avea durata de 2 zile și vor fi susținute pe baza curriculei de mai sus de firme acreditate de training.
- Firmele de training vor primi voucher pe baza rezultatelor testele de absolvire a cursurilor (150 EUR/per cursant care a absolvit cu succes programul in baza testarii in platforma cloud).

România se plasează pe ultimul loc (31) printre statele europene cu privire la dezvoltarea competențelor, aflându-se pe ultimul loc în ceea ce privește sub-indicatorul participarea în programe de formare recentă. Lipsa competențelor forței de muncă este una dintre cauzele

[7] European Investment Bank Investment Survey https://www.eib.org/attachments/efs/eibis_2020_romania_en.pdf
[8] What holds Romanian firms back
https://www.eib.org/attachments/efs/economics_working_paper_2019_08_en.pdf
[9] Eurostat https://ec.europa.eu/eurostat/databrowser/view/isoc_ske_ittn2/default/table?lang=en

adoptării scăzute de către firmele românești ale unor tehnologii avansate (Big Data, Cyber-Phyisical Systems/IoT, Artificial Intelligence)
Se estimează că vor beneficia de formare 248.000 de angajați livrate prin intermediul a 200 firme training.

Vor aplica IMM-urile care doresc să beneficieze de aceste cursuri. Selecția va fi efectuată pe baza principiului primul venit, primul servit, în limita bugetului alocat.

De asemenea, intervențiile vor veni în completarea măsurilor din cadrul Pilonului 3 destinate adoptării de tehnologii digitale de către IMM-uri. În vederea accesării programelor de formare pentru implementarea programului vor fi respectate criteriile de privind egalitatea de gen și de șanse în corespundere cu principiile Pilonului european al drepturilor sociale.

Operaționalizarea grupului operativ în minister, achiziționarea furnizorului de programe de învățământ, a dezvoltatorului platformei IT, contractarea acestor servicii, informarea și comunicarea către potențialele grupuri țintă vor avea loc în prima parte a desfășurării. Implementării urmând ulterior a fi dezvoltate curriculumul, platforma IT, informarea și comunicarea către potențialele grupuri țintă.

Ajutor de stat:

Pentru implementarea acestei reforme se va realiza o schemă de ajutor de minimis, elaborată în conformitate cu prevederile Regulamentului (UE) nr. 1407/2013. Valoarea totală maximă a ajutoarelor de minimis de care poate beneficia o întreprindere unică este de 200.000 de euro pentru o perioadă de trei ani fiscali consecutivi.

În plus, pentru eliminarea unui eventual ajutor de stat la nivelul formatorilor, aceştia vor fi selectaţi printr-o procedură competitivă, transparentă, necondiţionată şi nediscriminatorie, care va avea în vedere inclusiv elementele de natură economică din ofertele depuse de aceştia.

Grup țintă: IMM-uri inovatoare și angajații acestora

Calendar: 2022-31 decembrie 2025

Complementaritatea investițiilor:

Din perspectiva digitalizării, PNRR, prin cele 4 direcții de acțiune propuse pentru realizarea obiectivului general de transformare digitală a României, va fi complementar cu Programul Europa Digitală (Digital Europe Programme) care vizează accelerarea transformării digitale a economiei, industriei și societății europene, beneficii aduse cetățenilor, administrațiilor publice și întreprinderilor din Uniune și îmbunătățirea competitivității Europei în cadrul economiei digitale mondiale, contribuind în același timp la reducerea decalajului digital în Uniune și consolidând autonomia strategică a Uniunii prin sprijin holistic, transsectorial și transfrontalier și o contribuție mai solidă din partea Uniunii.

Astfel Pilonul II prezintă complementarități și sinergii cu Obiectivul specific nr. 3: securitatea cibernetică și încrederea, Obiectivul specific nr. 4: competențele digitale avansate și Obiectivul

specific nr. 5: dezvoltarea, utilizarea optimă a capacităților digitale și interoperabilitatea din cadrul programului Europa Digitală.

Investițiile, prevazute în cadrul Pilonului II – Transformare digitală, sunt complementare cu cele ce urmează a fi finanțate din FESI, în cadrul următoarelor programe operaționale:Programul Operational Crestere Inteligenta, Digitalizare si Instrumente Financiare (POCIDIF), Programele Operationale Regionale (POR-uri), Programul Operational Educație și Ocupare (POEO), Programul Operational Sănătate (POS), Programul Operational Tranziție Justă (POTJ).

În ceea ce privește digitalizarea administrației publice, în cadrul Pilonului II sunt prevăzute intervenții sub formă de proiecte mature, care pot fi realizate în orizontul de timp impus prevederile Regulamentului 2021/241 de instituire a Mecanismului de redresare și reziliență și răspund obiectivului de realizare a arhitecturii digitale guvernamentale, a elementelor cheie de interoperabilitate și cloud guvernamental, digitalizare a operațiunilor interne la nivelul autorităților publice centrale/instituțiilor.

- ✓ POCIDIF vizează continuarea investițiilor începute prin POC 2014-2020, respectiv introducerea conceptului de e-guvernare (evenimente din viața cetățenilor și mediului de afaceri). Diferențierea investițiilor aferente PNRR/POCIDIF are în vedere prevederile Regulamentului Politicii de Coeziune, care permit implementarea investițiilor pe o perioada mai îndelungată, cu posibilitatea de prelungire/ fazare.

- ✓ POTJ va fi finanța nevoile de dezvoltare din mai multe sectoare, printre care și digitalizarea serviciilor publice locale.

- ✓ POS cuprinde intervenții pentru digitalizarea sistemului medical.

Dezvoltarea competențelor digitale reprezintă un aspect important din PNRR care vizează creșterea competențelor digitale pentru diverse categorii de populație, inclusiv pentru unele categorii specifice de beneficiari, precum funcționarii publici pentru dezvoltarea competențelor digitale și a competențelor software ale forței de muncă, specialiști în analiză și design pentru sectorul public, formare de formatori în domeniul securității cibernetice, dar și pentru populația generală prin crearea unei rețele naționale a bibliotecilor ca hub-uri de învățare digitală. Efecte scontate vor fi susținute pe termen lung fiind complementare cu investițiile din:

- ✓ POCIDIF - *Digitalizare in educație,* prin care vor fi finantate platforme informatice cu conținut educațional, soluții wireless campus, laboratoare pentru dezvoltare competențe digitale, soluții pentru digitalizarea și centralizarea informațiilor din educație, la nivel național.

- ✓ POR - intervenții complementare orientate către dezvoltarea de abilităţi şi competenţe privind adoptarea tehnologiilor avansate.

- ✓ POEO - *Învățarea pe tot parcursul vieții* vizează o serie de intervenții prin care se dorește creșterea calității sistemului de formare profesională a adulților (dezvoltarea sistemului de asigurare a calității, formarea formatorilor/ instructorilor/ coordonatorilor de ucenicie din formarea profesională continuă, actualizarea/ revizuirea/ dezvoltarea de noi standarde ocupaționale/calificări profesionale conform noilor cerințe ale pieței muncii de încurajarea participării populației la diferite module de formare), dar și diversificarea ofertei de formare în

vederea creșterii nivelului de competențe pe diferite paliere și care se adresează în mod orizontal populației, răspunzând unor nevoi de formare diverse.

✓ Erasmus+: dobândirea de competențe digitale, pe baza experienței dobândite în ceea ce privește mobilitatea.

✓ InvestEU: competențe digitale, dezvoltarea unei infrastructuri pentru conectivitatea digitală, fie fizică, fie virtuală, în special prin proiecte care **sprijină** implementarea de rețele digitale.

✓ Horizon Europe: implementarea la nivel național și regional, într-un cadru european, a capacităților digitale și a celor mai recente tehnologii digitale în domenii de interes public (cum ar fi sănătatea, administrația publică, justiția și educația) sau în caz de disfuncționalitate a pieței (cum ar fi digitalizarea întreprinderilor, în special a întreprinderilor mici și mijlocii).

✓ Creative Europe: activități de formare și de mentorat menite a spori capacitatea operatorilor din domeniul audiovizual de a se adapta la noile evoluții ale pieței și la noile tehnologii digitale.Granturile SEE și Norvegiene: cercetare în domeniul tehnologiei comunicațiilor și informației.

✓ Orizont Europa: aloca un buget specific în cadrul pilonului „Provocări globale și competitivitate industrială europeană" pentru clusterul „Dezvoltarea digitală, industria și spațiul" pentru dezvoltarea de tehnologii generice (IA și robotică, internet de nouă generație, HPC și volume mari de date, tehnologii digitale esențiale, care combină tehnologia digitală cu alte tehnologii).

✓ Sinergic, prin Mecanismul pentru interconectarea Europei se au în vedere consolidarea capacităților și a infrastructurii digitale la scară largă pentru tehnica de HPC, IA, securitatea cibernetică și competențele digitale avansate, care vizează integrarea și implementarea la scară largă, la nivelul întregii Europe, a soluțiilor digitale inovatoare critice, existente sau testate, într-un cadru al Uniunii în domenii de interes public sau în cazuri de disfuncționalitate a pieței. Programul urmează să fie implementat, în principal, prin investiții strategice și coordonate cu statele membre, mai ales prin achiziții publice comune, în capacități digitale care urmează să fie partajate pe întreg teritoriul Europei și în acțiuni la nivelul Uniunii care sprijină interoperabilitatea și standardizarea, în cadrul procesului de dezvoltare a pieței unice digitale.

Prin prisma investițiilor propuse pentru asigurarea securității cibernetice, PNRR prezintă elemente de complementaritate și sinergie cu programul Orizont Europa, care prevede investiții pentru consolidarea capacităților digitale pentru HPC, IA, tehnologiile registrelor distribuite (de exemplu tehnologia blockchain), securitatea cibernetică și competențele digitale avansate i cadrul Pilonului II "Provocări globale și competitivitate industrială europeană"– Clusterul 3 "Securitate civilă pentru societate", dar și cu alte programe precum: Europa Digitală – Securitatea cibernetică și încrederea și Fondul pentru securitate internă.

2. Aspecte de autonomie strategică și securitate

Deși reformele și investițiile propuse în PNRR au în vedere facilitarea accesului cetățeanului la tehnologia informației și comunicațiilor, ceea ce reprezintă una dintre premisele bunei funcționări a societății moderne, trebuie avute în vedere amenințările provenite din spațiul cibernetic și riscurile crescute generate de utilizarea masivă a datelor în rețele.

Rețelele 5G reprezintă punctul de lansare a societății moderne din ce în ce mai digitalizate, marcând adevărate schimbări în modul în care va funcționa societatea în ansamblul ei, fie că vorbim de aspecte economice, politice, culturale, sau de viața de zi cu zi a oamenilor. Sunt în cauză miliarde de sisteme conectate, inclusiv în sectoare critice precum energia, transportul, serviciile bancare și sănătatea, precum și sistemele de control industrial care transportă informații sensibile și care susțin sistemele de siguranță.

Alături de toate aceste beneficii incontestabile, asigurarea securității spațiului cibernetic constituie o preocupare majoră a tuturor actorilor implicați, mai ales la nivel instituțional, unde se concentrează responsabilitatea elaborării şi aplicării de politici coerente în domeniu. Prin urmare, întrucât sunt susceptibile să apară breșe de securitate mai proeminente în rețelele 5G, în comparație cu situația din rețelele existente, asigurarea securității și rezilienței rețelelor 5G este esențială.

În ajutorul Statelor Membre, la nivelul UE s-a adoptat un set de instrumente comune privind măsurile de atenuare a riscurilor de securitate legate de lansarea a celei de-a cincea generație de rețele mobile C*ybersecurity of 5G networks EU Toolbox of risk mitigating measures*.

Astfel România a făcut un prim pas în implementarea Recomandării Comisiei Europene, prin efectuarea analizelor privind aspectele de autonomie strategică și securitate și propunerea de măsuri pentru adresarea riscurilor identificate și alte măsuri de mitigare a acestora, atât în ceea ce privește Cloud-ul Guvernamental, cât și pentru cele legate de utilizarea rețelelor 5G.

Analiza de securitate privind investiția de Cloud Guvernamental

Sistemele cloud reprezintă un punct critic în digitalizarea serviciilor publice dedicate cetățenilor într-o societate modernă. Sistemele cloud permit asigurarea unui grad ridicat de disponibilitate și interconectare a serviciilor publice dedicate persoanelor fizice și juridice, fapt ce duce la creșterea calității vieții cetățenilor.

În vederea asigurării succesului implementării și operaționalizării sistemului cloud național avem în vedere identificarea, evaluarea și minimizarea riscurilor ce pot apărea în acest proces. În efectuarea acestei analize au fost avute în vedere următoarele categorii de amenințări pentru:

I. Guvernanță

Migrând serviciile clientului în cloud, acesta pierde controlul total asupra securității datelor proprii. Astfel clientul va prelua o serie de riscuri de securitate asociate providerului de cloud.

Există situația în care un utilizator poate solicita mecanisme de securitate peste capacitatea pe care o poate oferi providerul de cloud sau situații în care clientul (tenant) dorește mecanisme de

securitate sub nivelul minim cerut de către provider, datorită tehnologiei vechi utilizate în serviciul care trebuie migrat. În acest caz serviciile migrate în cloud nu pot fi utilizate la capacitate maximă și pot genera erori sau breșe de securitate.

În același timp există riscul ca resursele să nu fie utilizate în mod eficient, fapt pentru care se recomandă implementarea măsurilor specifice de control și monitorizare a resurselor utilizate.

Pentru minimizarea riscului, providerul de cloud trebuie să facă dovada nivelului de securitate pe care îl poate oferii clientului (tenant) iar operațiile de migrare a serviciilor naționale destinate cetățenilor trebuie gestionate unic, pe baza unor criterii bine stabilite, la nivel național.

II. Strategie de furnizare a serviciilor

Prioritizarea incorectă a acomodării serviciilor naționale în cloud poate duce la calitatea scăzută a serviciilor digitale furnizate către cetățeni.

Este necesar ca la nivel național să se efectueze o strategie națională pentru prioritizarea implementării sau migrării serviciilor oferite de către stat pentru persoanele fizice și juridice în cloud.

III. Implementarea arhitecturii

În proiectarea, implementarea și operaționalizarea unui sistem cloud pot apărea riscuri privind:

- izolarea defectuoasă a datelor sensibile
- posibilități limitate de configurare
- rigiditatea în adaptarea la noile tehnologii
- implementarea aplicațiilor care să nu utilizeze eficient facilitățile unui sistem de tip cloud
- performanța scăzută datorită unor resurse hardware neconforme

Pentru minimizarea riscurilor prezentate sunt necesare măsuri de pregătire a personalului care va proiecta, implementa și operationaliza sistemul cloud. Totodată, sunt necesare măsuri precum:

- analiza pieței marilor producători de sisteme cloud
- analiza standardelor de implementare și a celor mai bune practici recomandate în domeniu
- documentarea privind „lecțiile învățate” din experiența altor oraganizații care au implementat sisteme cloud.

IV. Securitatea infrastructurii

La nivelul securității infrastructurii, riscurile care pot apărea în arhitectura propusă, bazată pe multiple centre de date, se pot rezuma astfel:

– securitatea sistemelor: practici inadecvate de securitate implementate de client (tenant), sisteme de tip end-user compromise care accesează sistemul cloud și configurarea greșită a sistemelor din interiorul cloudului;

– securitatea rețelelor: compromiterea interfețelor de management, configurarea greșită a comunicațiilor între centrele de date, expunerea la atacuri de tip DDoS sau lipsa măsurilor de protecție privind atacurile care pot fi generate de resursele interne;

– securitatea aplicațiilor: instalarea în cloud a aplicațiilor care nu pot fi suficient testate din punct de vedere al securității, folosirea metodelor neconforme de acces de către personalul responsabil, interconectarea aplicațiilor realizate în tehnologii cloud cu aplicații tradiționale și lipsa sau insuficienta jurnalizare a evenimentelor;

– confidențialitatea datelor clienților: providerul de cloud are acces la cheile de criptare utilizate de client, providerul de cloud implementează mecanisme superficiale pentru managementul cheilor sau utilizează protocoale sau funcții de securitate vulnerabile.

– managementul vulnerabilităților: aplicarea întârziată a actualizărilor de securitate, lipsa asigurării acestora de către producători sau gestionarea superficială a vulnerabilităților introduse de către clientul(tenant-ul) cloud.

Măsurile necesare pentru remedierea posibilelor deficiente prezentate mai sus constau în asigurarea personalului necesar cu pregătire adecvată, pregătirea continua a personalului, stabilirea și implementarea măsurilor procedurale pentru standardizarea modului de lucru, controlul și actualizarea periodică a acestora, corelat cu analiza periodică a riscurilor de securitate.

În plus Serviciul de Telecomunicații Speciale asigură servicii de tip Internet Service Provider care oferă protecția adecvată, inclusiv mecanisme anti-DDoS. Acestea vor fi furnizate sistemului cloud ce urmează a fi implementat.

Prin PNRR se are în vedere corelarea implementării sistemului cloud cu creșterea capacității serviciilor de tip Internet Service Provider asigurate de Serviciul de Telecomunicații Speciale.

V. Controlul accesului și managementul identității

Securitatea sistemului cloud poate fi afectată dacă integrarea sistemelor de management al identității externe cu sistemele specifice oferite de tehnologia cloud implementată este defectuoasă. În același timp atribuirea greșită a rolurilor în cadrul sistemului poate genera breșe de securitate.

Din punct de vedere al managementului accesului, securitatea sistemului cloud este vulnerabilă la implementarea eronată sau limitată a mecanismelor de control acces.

Minimizarea riscurilor prezentate mai sus se poate realiza prin asigurarea personalului necesar cu pregătire adecvată, implementarea masurilor procedurale pentru standardizarea modului de lucru și efectuarea periodică a testelor de securitate.

VI. Managementul informațiilor (datelor)

Riscurile privitoare la gestionarea datelor se pot grupa astfel:

– riscuri asupra datelor stocate: acces neautorizat la sisteme de stocare, stocare neprotejata, lipsa mecanismelor de validare a integrității;

– riscuri asupra datelor în tranzit: posibilitatea de exfiltrării datelor, utilizarea canalelor de comunicații nesecurizate;

– riscuri asupra datelor în procesare: necunoașterea proprietarului datelor, accesul neautorizat sau folosirea improprie a datelor

– sanitizarea datelor: utilizarea uneltelor inadecvate, necunoașterea locației unde sunt stocate datele.

Totodată există riscul ca sistemul cloud să nu fie implementat corect în conformitate cu cerințele legale cu privire la protecția datelor cu caracter personal, date privind proprietatea intelectuală sau alte date confidențiale și verificată implementarea.

În vederea reducerii nivelului de risc se au în vedere asigurarea testelor periodice de securitate, asigurarea realizării și implementării procedurilor specifice de lucru și asigurarea selectării tehnologiilor potrivite furnizate de producători de încredere.

VII. Asigurarea disponibilității

Disponibilitatea serviciilor găzduite în sistemul cloud poate fi afectată de:

– oversubscription – utilizarea inadecvată a mai multor resurse decât sunt fizic disponibile în perioade de suprasolicitare;

– proiectarea eronată a unor puncte critice unice (single-point-of-failure);

– imposibilitatea de testare periodică a planurilor de recuperare în caz de dezastru și în caz de avarie

– neasigurarea resurselor necesare, datorită unui lanț defectuos de aprovizionare (Bad Supply Chain).

Măsurile necesare pentru minimizare riscului trebuie abordate prin asigurarea calității proiectării, administrării, gestionarii și asigurării resurselor necesare.

Totodată, Serviciul de Telecomunicații a prevăzut în implementarea proiectului, dotarea a patru centre de date, minim Tier 3, dedicate sistemului cloud, asigurând geo-redundanță.

VIII. Administrarea Sistemului (IT Operations)

Pe parcursul întregului ciclu de viață al sistemului cloud, procesele necesare administrării se supun atât riscurilor de natură tehnică cât și riscurilor privind gestionarea operațiunilor. Astfel se pot identifica la acest moment riscuri privind:

– managementul schimbărilor: planuri de migrare inadecvate, comunicarea inadecvată a modificărilor, vicii în lanțul de aprobare a schimbărilor

– managementul incidentelor: identificarea și notificarea întârziată a breșelor de securitate, vizibilitate limitată a resurselor în timpul investigațiilor de securitate, probleme în izolarea propagării efectelor breșelor de securitate.

– managementul bunurilor: asigurarea insuficientă a resurselor financiare pentru achiziția licențelor necesare.

– securitatea fizică a centrelor de date: furtul resurselor, analiza inadecvată a factorilor externi care pot perturba activitatea sistemelor, analiza inadecvată a factorilor de mediu.

Pentru a reduce posibilitatea de impact asupra sistemului cloud implementat este avută în vedere gestionarea operațiilor în conformitate cu standardele internaționale în domeniu. Totodată securitatea fizică este prevăzută pe mai multe nivele, de la perimetrul exterior către zona de „core" a sistemului, cu mecanisme de control și monitorizare, adaptate nivelului de securitate necesar în zona respectivă.

IX. Managementul furnizorilor de tehnologie (Vendor Management)

Posibilitățile restrânse ale pieței producătorilor de sisteme de tip cloud și lipsa standardizării tehnologice generează riscuri financiare ridicate prin posibilitatea restrânsă de integrare între tehnologiile furnizate de aceștia.

În cadrul proiectării trebuie avută în vedere posibilitatea de acomodare în centrele de date a mai multor tehnologii de la producători diferiți pentru continuarea furnizării serviciilor în cazuri de excepție.

X. Sustenabilitatea proiectului - Resurse umane, implicații legale și financiare

Complexitatea sistemului cloud are implicații, altele decât tehnologice, în asigurarea serviciilor, legate de pregătirea personalului implicat, asigurarea cadrului legal și asigurarea resurselor financiare necesare.

Se pot identifica următoarele riscuri:

– resurse umane: pregătirea insuficientă a personalului, probleme în asigurarea atragerii și retenției personalului calificat datorită unui pachet salarial deficitar față de piața privată;

– legale: reglementarea deficitară privind utilizarea sistemelor de cloud;

– financiare: impredictibilitatea posibilității alocării resurselor financiare necesare pe termen lung.

În implementarea sistemului cloud este prevăzută achiziționarea serviciilor de pregătire a personalului implicat. Aceste servicii vor fi asigurate în continuare pentru menținerea unui nivel ridicat de aptitudini profesionale.

La nivel național trebuie realizate reglementările specifice pentru asigurarea resurselor financiare sub forma salarială sau alte pachete motivaționale pentru atragerea și retenția personalului.

Din punct de vedere legal, reglementările naționale trebuie sa prevadă faptul ca principiul implementării proiectelor tehnice ale statului trebuie sa aibă în vedere în primul rând eficientizarea utilizării resurselor financiare și tehnice (cloud first). În același timp prevederile legale trebuie să prioritizeze alocările financiare pentru asigurarea sustenabilității sistemului cloud.

Analiza de securitate privind utilizarea rețelelor 5G

I. Scenarii de risc legate de măsuri de securitate insuficiente

1. Configurarea greşită a rețelelor

La nivelul infrastructurilor TIC sunt implementate soluții software și echipamente hardware uzate fizic și moral, respectiv a căror perioadă de viață a expirat (end-of-life). Aceste disfuncții sunt generate de o serie de factori, dintre care cei mai semnificativi sunt:

- atenția scăzută acordată de instituții privește bugetarea investitiilor pe segmentul TIC;

- deficitul de forță de muncă înregistrat pe piața muncii în domeniul TIC, în care este nevoie de specialiști înalt calificați;

- lipsa de atractivitate a pachetului salarial oferit de către instituțiile care gestionează infrastructuri TIC, fapt care generează provocări ceea ce privește retenția personalului calificat;

- personal TIC insuficient calificat sau cărora nu li se asigură un cadru de acces la cursuri de pregătire profesională astfel încât să fie la curent cu evoluția tehnologică.

Prin urmare, deficiențele mai sus menționate generează configurări și utilizări gresite ale rețelelor și sistemelor TIC, aspecte ce potențează apariția unor breșe de securitate, care pot fi exploatate în cadrul unor campanii de atac cibernetic cu impact direct la adresa atât a confidențialității, integrității și disponibilității datelor și serviciilor furnizate cât și a imaginii entității afectate.

2. Lipsa controalelor de acces

La nivelul unor entități care gestionează rețelele și sistemele TIC s-au înregistrat situații în care:

- sistemele de control al accesului funcționează deficitar ori sunt dezactivate;

- elemente componente ale infrastructurii TIC sunt situate în spații neconforme, care nu respectă standardele de securitate și siguranță;

- în privința administrării infrastructurii TIC, există cazuri în care politicile de securitate nu sunt respectate ori a căror implementare este deficitară și foarte greu de asigurat că acestea sunt respectate;

- se înregistrează situații în care nu sunt implementate sisteme destinate gestionării drepturilor de acces pentru fiecare utilizator în parte;

Așadar, se impune necesitatea implementării unor proceduri și protocoale de acces, care să fie respectate cu strictețe de către toate persoanele care au acces la nivelul entităților care gestionează rețelele și sistemele TIC.

II. Scenarii de risc legate de 5G „supply chain" (întregul lanț 5G)

3. Calitatea scăzută a produselor

Având în vedere evoluțiile înregistrate în domeniul TIC, precum și necesitatea de a asigura interoperabilitatea serviciilor publice, caracterizate de o creștere din ce în ce mai mare a gradului de externalizare a serviciilor, toți acești factori generează, pe cale de consecință, o creștere a nivelului riscurilor de securitate cibernetică.

În acest sens, se conturează riscul dezvoltării și utilizării unor soluții software și echipamente hardware cu tehnologii ce prezintă vulnerabilități de securitate cibernetică sau care nu respectă principiul *secure-by-design,* aspecte ce pot facilita derularea unor atacuri cibernetice la adresa acestora.

Prin urmare, în condițiile creșterii numărului de producători pentru un anumit tip de tehnologie, este necesară crearea unor mecanisme de validare și autorizare din perspectiva securității cibernetice a acestora, care să ofere garanții de credibilitate și securitate cibernetică.

Acest lucru este necesar întrucât în ultimii ani a crescut incidența de atacuri cibernetice derulate prin exploatarea unor vulnerabilități pe linia lanțului de aprovizionare.

4. Dependență de un anumit furnizor în cadrul unei rețele sau lipsa diversității la nivel național

În contextul principiilor de organizare a unor proceduri de achiziții publice, în care licitațiile sunt adjudecate cu predilecție pe principiul celei mai avantajoase oferte de preț, există riscul ca entitățile să devină dependente de o anumită soluție ori producător.

Astfel, având în vedere creșterea exponențială a amenințărilor la adresa securității cibernetice, este important ca în evaluarea ofertelor să se analizeze atât soluțiile/ echipamentele, cât și producătorii din perspectiva securității cibernetice.

De asemenea, existența unor autorizări prealabile a producătorilor va conduce la crearea unei piețe TIC competitive și sigure, aspect de natură a nu crea dependență față de un anumit producător.

III. Scenarii de risc legate de modus operandi al actorilor care reprezintă amenințări principale

5. Interferența statului prin „lanțul de aprovizionare" 5G

În ultimii ani, mai multe state au adoptat diverse poziții care au avut în vedere implementarea unor mecanisme de "*vetting*" ale unor producători, care ar putea genera amenințări în planul

securității naționale. Această situație este generată de activitățile din spațiul cibernetic cu caracter maling ale unor state, care vor urmări influențarea sau perturbarea lanțului de aprovizionare, inclusiv prin derularea de campanii de atacuri cibernetice.

6. Exploatarea rețelelor 5G de către crima organizată sau grup de criminalitate organizată care vizează utilizatorii finali

Grupările de atacatori cibernetici își pot adapta modul de acțiune prin exploatarea rețelelor 5G care le oferă posibilitatea de a extinde suprafața de atac și de a amplifica consecințele atacurilor.

IV. Scenarii de risc în legătură cu interdependențe între rețelele 5G și alte sisteme critice

7. Întreruperea semnificativă a infrastructurilor sau serviciilor critice

Interoperabilitatea și interconectivitatea rețelelor și sistemelor TIC, coroborat cu folosirea pe scară largă a noilor tehnologii, de multe ori fără un nivel de securitate cibernetică adecvat, generează riscul ca atacurile cibernetice să vizeze inclusiv indisponibilizarea în masă a infrastructurilor critice sau serviciilor oferite de acestea.

8. Eroare masivă a rețelelor din cauza întreruperii alimentării cu energie electrică sau alte sisteme de sprijin

Funcționarea optimă a rețelelor și sistemelor TIC este dată de alimentarea în flux continuu cu energie electrică. Pot fi înregistrate întreruperi ale furnizării cu energie electrică din cauze diverse, precum: fenomene meteorologice, cedarea unor elemente ale infrastructurii de transport, lipsa unor soluții redundante (ex. UPS), evenimente cu impact transfrontalier, care afectează echilibrul rețelei europene sau chiar derularea unor atacuri cibernetice la adresa unor infrastructuri TIC de control industrial.

Întrucât sectorul energiei electrice prezintă o valență critică deosebită, fiind în relație de interdependență cu sisteme din alte state, precum și cu entități din domenii diverse, care asigură servicii esențiale pentru populație, un incident de securitate cibernetică poate genera efecte în lanț la nivel național și (pan)european.

Prin urmare, entitățile care gestionează astfel de infrastructuri trebuie să implementeze soluții avansate de securitate cibernetică, de asigurare a redundanței alimentării cu energie electrică, precum și mecanisme de management al incidentelor de securitate cibernetică și de asigurare a rezilienței.

V. Scenarii de risc legate de utilizatorul final al dispozitivelor

9. Exploatarea IoT (Internet of Things), a telefoanelor sau a dispozitivelor inteligente

Industria IoT este în plină dezvoltare, oferind oportunități nelimitate. În acest context, un grad ridicat de atenție trebuie să se îndrepte către nivelul de securitate al dispozitivelor și rețelelor de acest tip. Pentru a face față acestor provocări este esențială înțelegerea principalelor amenințări cu care utilizatorii dispozitivelor IoT se vor confrunta, pe parcurs ce nivelul de utilizare a acestora va crește:

– atacuri asupra rețelei – presupun compromiterea dispozitivelor IoT prin intermediul rețelei la care acestea sunt conectate. Acest tip de atac cibernetic permite atacatorului să controleze dispozitivele IoT și să le gestioneze cum dorește;

– atacuri de tip Distributed Denial of Service (DDoS) - atacatorul utilizează rețele de boți pentru a trimite foarte multe mesaje către o rețea, care are în componență dispozitive IoT. Astfel, aceasta este suprasolicitată, indisponibilizând toate sistemele conectate. Atacurile DDoS asupra dispozitivelor IoT funcționează în mod similar acelora derulate împotriva oricărui alt tip de dispozitiv;

– atacuri prin care se vizează blocarea frecvențelor radio - acestea afectează dispozitivele IoT conectate wireless, determinând pierderea conexiunii sau diminuarea abilității de a comunica cu rețeaua. Acest gen de atacuri sunt derulate, cel mai frecvent, asupra sistemelor de alarmă de tip IoT.

În contextul dezvoltării IoT, principala provocare rămâne lipsa unor standarde internaționale de securitate cibernetică, un aspect esențial fiind reprezentat de faptul că acestea pot fi pe de o parte victimă, iar pe de altă parte platformă/infrastructură utilizată în derularea altor atacuri cibernetice. Un alt risc este generat de rapiditatea evoluției tehnologice, fapt ce stă la baza unei lipse generale de interes pentru aspectele de securitate cibernetică, atât din partea utilizatorilor cât și din partea producătorilor de dispozitive IoT.

Incidentele de securitate cibernetică şi atacurile cibernetice majore cu care s-au confruntat în ultimii ani unele state şi organizaţii internaţionale au determinat conştientizarea necesităţii adoptării unor strategii şi politici în domeniul securităţii cibernetice.

În România se are în vedere adoptarea de măsuri strategice, tehnice și de suport pentru implementare de către autoritățile și agențiile responsabile naționale, în funcție de capacitățile și competențele fiecăreia.

Conform celor opt măsuri strategice identificate în cadrul C*ybersecurity of 5G networks EU Toolbox of risk mitigating measures*, pentru limitarea riscurilor, în România se află în elaborare cadrul normativ național în domeniul securității cibernetice, armonizat cu prevederile legislației internaționale, care să creeze un cadru național de securitate adecvat și care să faciliteze, pe baze voluntare, cooperarea bilaterală și schimbul prompt și eficient de informații între autoritățile competente pentru combaterea utilizării infrastructurilor critice ICT în scopuri teroriste sau criminale.

În acest context, este de menționat apariția în luna iunie 2021, a Legii nr.163/2021 privind adoptarea unor măsuri referitoare la infrastructuri informatice şi de comunicaţii de interes naţional şi condiţiile implementării reţelelor 5G, act normativ ce stabilește, între altele, o serie de aspecte

strategice ce țin de domeniul securității comunicațiilor prin rețelele 5G, inclusiv cu privire la producătorii de echipamente, tehnologii şi programe software.

În acest moment, proiectul Strategiei Naționale de Securitate Cibernetică 2021-2026 (document de politici publice referitor la protecția rețelelor IT și OT) este finalizat, aflându-se în procedura de aprobare. Scopul Strategiei de securitate cibernetică a României este de a defini şi de a menţine un mediu virtual sigur, cu un înalt grad de reziliență şi de încredere, bazat pe infrastructurile cibernetice naționale, care să constituie un important suport pentru securitatea națională şi buna guvernare, pentru maximizarea beneficiilor cetăţenilor, mediului de afaceri şi ale societății românești, în ansamblul ei.

Strategia de securitate cibernetică a României prezintă obiectivele, principiile şi direcțiile majore de acţiune pentru cunoaşterea, prevenirea şi contracararea amenințărilor, vulnerabilităților şi riscurilor la adresa securităţii cibernetice a României şi pentru promovarea intereselor, valorilor şi obiectivelor naţionale în spaţiul cibernetic. În scopul asigurării coerenţei şi eficienţei acţionale, Strategia de securitate cibernetică a României, urmăreşte îndeplinirea obiectivului naţional de securitate privind „asigurarea securităţii cibernetice", cu respectarea principiilor şi caracteristicilor Strategiei naţionale de apărare şi Strategiei naţionale de protecţie a infrastructurilor critice.

Evaluarea profilului de risc al furnizorilor și aplicarea restricțiilor pentru furnizorii considerați cu risc ridicat va fi realizată sub incidența Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cu modificările și completările ulterioare. Legea stabilește cadrul juridic și instituțional, măsurile și mecanismele necesare în vederea asigurării unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice și a stimulării cooperării în domeniu, corelată cu prevederile Directivei 1148/2016 privind creșterea încrederii în Piața Digitală Unică și este adresată în mod exclusiv operatorilor economici (publici sau privați) din două categorii mari:

- Operatorii de servicii esențiale din 7 categorii economice importante (Energie, Transporturi, Medical, Bancar, Piețe financiare, Furnizare de apă potabilă, Infrastructuri Digitale);
- Furnizorii de servicii digitale din 3 categorii: Motoare de căutare, Piețe online, Servicii cloud.

Noua Lege a apărării şi securităţii cibernetice a României, care se preconizează că va intra în vigoare la sfârșitul anului 2022, va stabili cadrul legal și instituțional pentru organizarea și desfășurarea activităților în domeniile securității cibernetice și apărării cibernetice, mecanismelor de cooperare și responsabilităților instituții din domeniile menționate. În acest mod va fi creat un ecosistem național de prevenire și răspuns la incidente, prin stabilirea de cerințe de asigurare a securității informatice a serviciilor furnizate, cerințe de notificare a incidentelor survenite, mecanisme de răspuns la nivel național și de participare la răspunsul comun în cadrul ecosistemului european creat de Directiva NIS.

Pe plan instituțional, proiectul de act normativ privind crearea Directoratului Național de Securitate Cibernetică, programat să se materializeze până la finalul acestui an, vizează crearea

unei instituții puternice cu atribuții sporite în domeniul securității cibernetice, care să urmărească la nivel național dezvoltarea, preluarea și implementarea celor mai bune practici în domeniu.

În aceeași direcție, operaționalizarea Centrului european de competențe în materie de securitate cibernetică de la București, așteptată să se producă în perioada următoare, va deschide noi paliere de studiu și în final de contracarare a amenințărilor și vulnerabilităților, prin finanțarea la nivelul Uniunii Europene a proiectelor cu specific pe domeniul securității cibernetice, cu implicarea industriei de profil și a mediului academic într-un cadru concurențial, multinațional. Centrul va colabora cu o rețea de centre naționale de coordonare desemnate de statele membre ale Uniunii Europene, în strânsă cooperare cu Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA).

Pe lângă aceste măsuri strategice, sunt stabilite măsuri tehnice și organizatorice adecvate și proporționale, conforme celor unsprezece identificate in documentul european mai sus menționat (C*ybersecurity of 5G networks EU Toolbox of risk mitigating measures),* pentru a gestiona riscurile la adresa securității cibernetice și rezilienței rețelelor, a sistemelor informatice și interoperabilității acestora prin:

– evaluarea stării de securitate și a vulnerabilităților rețelelor și sistemelor informatice;

– elaborarea de politici și proceduri de securitate cibernetică în conformitate cu standarde internaționale de securitate a informației și sistemelor informaționale, de management al riscului, sau cu cerințele legale aplicabile;

– folosirea de soluții care utilizează inteligența artificială;

– asigurarea interoperabilității între componentele informatice de securitate;

– protecția sistemelor informatice și a informațiilor vehiculate la nivelul instituțiilor, autorităților publice şi operatorilor privaţi;

– asigurarea de condiții optime de securitate cibernetică pentru facilitarea desfășurării de la distanță a activității angajaților;

– eficientizarea și crearea de premise pentru a continua modernizarea infrastructurilor TIC cu valențe critice pentru securitatea națională, inclusiv prin minimizarea timpului dedicat activităților de recuperare și restaurare ca urmare a incidentelor sau atacurilor cibernetice.

– cursuri de pregătire profesională în materie de securitate cibernetică specific pentru absolvenți și studenți (igienă cibernetică, control și protecția datelor, siguranța utilizării noilor tehnologii).

Aceste aspecte vor face obiectul analizelor de detaliu ale instituțiilor cu atribuții în domeniu, urmând a fi dublate de completarea cadrului național privind securitatea cibernetică, după caz, cu acte normative specifice la nivelul legislației naționale secundare.

PNRR vizează transformarea digitală a României prin adoptarea tehnologiilor digitale în toate sectoarele și domeniile de activitate ale instituțiilor statului și pentru creșterea numărului de cetățeni și companii care să beneficieze de oportunitățile oferite de digitalizare, dar totodată și asigurarea respectării drepturilor şi libertăților fundamentale ale cetățenilor şi a intereselor de securitate națională, într-un cadru legal adecvat.

Cunoașterea pe scară largă a riscurilor şi amenințărilor derivate din activitățile desfășurate în spațiul cibernetic, precum şi a modului de prevenire şi contracarare a acestora necesită o comunicare şi cooperare eficiente între actorii specifici în acest domeniu. Din acest punct de vedere se conturează necesitatea dezvoltării culturii de securitate cibernetică, iar o combinație adecvată a diferitelor tipuri de măsuri pentru atenuarea riscurilor identificate constituie astfel soluțiile optime pentru contracarare a acestora.