Școala Națională de Studii Politice și Administrative
Facultatea de Administrație Publică

CREAREA UNEI NOI PLATFORME PIAS ÎN SĂNĂTATE ȘI IMPLEMENTAREA DIRECTIVEI EUROPENE NIS 2

- Lucrare de disertație, Master în Managementul Sectorului Public -

Coordonator

Conf. Univ. Dr. Cătălin VRABIE

Absolvent

Adrian Emil M. FRĂȚILĂ

București
2025

Instrucțiuni de redactare (A se citi cu atenție!!)

1. Introduceți titlul lucrării în zona aferentă acestuia – nu modificați mărimea sau tipul fontului;
2. Sub titlul lucrării alegeți dacă aceasta este de licență sau de disertație;
3. Introduceți specializarea sau masteratul absolvit în zona aferentă acestuia de pe prima pagină a lucrării;
4. Introduceți numele dvs. complet în zona aferentă acestuia (sub Absolvent (ă));
5. Introduceți anul în care este susținută lucrarea sub București;

NB: Asigurați-vă că ați șters parantezele pătrate din pagina de gardă și cuprins.

6. Trimiteți profesorului coordonator lucrarea doar în format **Microsoft Word** – alte formate nu vor fi procesate;
7. **Nu ștergeți declarația anti-plagiat și nici instrucțiunile** – acestea trebuie să rămână pe lucrare atât în forma tipărită cât și în cea electronică;
8. **Semnați declarația anti-plagiat;**
9. **Cuprinsul este orientativ** – numărul de capitole / subcapitole poate varia de la lucrare la lucrare. **Introducerea, Contextul, Concluziile / Discuțiile și Referințele bibliografice sunt însă obligatorii;**
10. **Este obligatorie folosirea template**-ului. Abaterea de la acesta va cauza întârzieri în depunerea la timp a lucrării.

NB. Lucrările vor fi publicate în extenso pe pagina oficială a hub-ului Smart-EDU, secțiunea Smart Cities and Regional Development: https://scrd.eu/index.php/spr/index.

ATENȚIE: Lucrarea trebuie să fie un produs intelectual propriu. Cazurile de plagiat vor fi analizate în conformitate cu legislația în vigoare.

Declarație anti-plagiat

1. Cunosc că plagiatul este o formă de furt intelectual și declar pe proprie răspundere că această lucrare este rezultatul propriului meu efort intelectual și creativ și că am citat corect și complet toate informațiile preluate din alte surse bibliografice (de ex: cărți, articole, clipuri audio-video, secțiuni de text și sau imagini / grafice).

2. Declar că nu am permis și nu voi permite nimănui să preia secțiuni din prezenta lucrare pretinzând că este rezultatul propriei sale creații.

3. Sunt de acord cu publicarea on-line *in extenso* a acestei lucrări și verificarea conținutului său în vederea prevenirii cazurilor de plagiat.

Numele și prenumele: Frățilă Adrian Emil

Data și semnătura: : 22.12.2024

Cuprins

Abstract

Această cercetare abordează problematica securității cibernetice în sănătate în contextul Directivei Europene NIS 2. **Obiective:** Această lucrare analizează impactul Directivei Europene NIS 2 asupra infrastructurii critice din sănătate, cu un accent deOSE/Entităţi esenţialebit pe modernizarea platformei PIAS/e-Sănătate pentru conformitate cu cerințele de securitate cibernetică. Scopul principal este dezvoltarea unei noi platforme integrate PIAS/e-Sănătate, care să sporească reziliența cibernetică, eficiența operațională și calitatea serviciilor medicale în România. Obiectivele includ analiza cerințelor Directivei NIS 2, evaluarea beneficiilor și provocărilor implementării acesteia, dezvoltarea unei soluții tehnologice moderne și oferirea de recomandări pentru factorii de decizie. **Studii prealabile:** Lucrarea se bazează pe analiza literaturii de specialitate privind securitatea cibernetică și e-Sănătatea, precum și pe bunele practici din alte state europene. Sunt integrate concepte cheie precum reziliența cibernetică, interoperabilitatea datelor și cerințele legislative ale Directivei NIS 2. Studiul contribuie la literatura existentă, completând cercetările publicate în conferințele internaționale SCIC și TRUST. **Metodologie:** Cercetarea utilizează o metodologie mixtă, combinând metode calitative și cantitative. Interviurile semi-structurate cu experți din sănătate și IT oferă perspective detaliate, în timp ce chestionarele aplicate utilizatorilor PIAS cuantifică percepțiile lor. Analiza comparativă cu alte soluții europene sprijină dezvoltarea unui model conceptual validat pentru modernizarea infrastructurii informatice. **Rezultate:** Rezultatele evidențiază că implementarea Directivei NIS 2 reduce incidentele cibernetice, îmbunătățește siguranța datelor și facilitează interoperabilitatea. Totuși, costurile inițiale ridicate și necesitatea colaborării interinstituționale rămân provocări semnificative. **Implicații:** Studiul are implicații importante pentru cercetători, practicieni și decidenți politici, oferind direcții strategice pentru alinierea infrastructurii critice din sănătate la cerințele Directivei NIS 2 și promovând o mai bună securitate cibernetică. **Valoare:** Lucrarea aduce o contribuție originală prin propunerea unui model inovator de integrare a noilor tehnologii, cum ar fi big data și IoT, în domeniul sănătății digitale. Prin aceste contribuții, susține tranziția către un sistem medical mai sigur, eficient și sustenabil în România.

Cuvinte cheie: Protecția datelor sensibile, Reziliență cibernetică medicală, Digitalizare în sănătate, Platforme informatice integrate, Analiza riscurilor cibernetice.

Introducere

În contextul creșterii continue a dependenței de tehnologia informației și comunicațiilor (TIC), asigurarea securității cibernetice a devenit o prioritate globală, fiind esențială pentru protejarea infrastructurii critice și a datelor sensibile. Uniunea Europeană, conștientă de vulnerabilitățile digitale crescânde, a adoptat în 2016 Directiva (UE) privind securitatea rețelelor și sistemelor informatice (Directiva NIS), care a stabilit un cadru comun pentru consolidarea rezilienței cibernetice a statelor membre. Aceasta a fost ulterior actualizată prin Directiva NIS 2 2022/2555, menită să răspundă provocărilor emergente și să aducă cerințe mai stricte pentru protecția Operatorilor de Servicii Esențiale (OSE)/ Entităţi esenţiale.

În România, transpunerea Directivei NIS 2 s-a realizat prin Ordonanţă de Urgenţă Nr. 155/2024 din 30 decembrie 2024 privind securitatea rețelelor și sistemelor informatice, care desemnează OSE/Entităţi esenţiale ca fiind entități critice pentru funcționarea economiei și societății. În cadrul acestei legislații, sectorul sănătății ocupă o poziție de deosebit de sensibilă, având în vedere importanța asigurării continuității serviciilor medicale și protecției datelor pacienților. Definiția și reglementările asociate OSE/Entităţi esenţiale sunt gestionate în România de către Directoratul Național de Securitate Cibernetică (DNSC), entitate responsabilă pentru implementarea politicilor de securitate cibernetică și pentru colaborarea cu instituțiile europene.

Evoluția tehnologiilor digitale, inclusiv utilizarea soluțiilor cloud, analiza big data și dispozitivele IoT, a deschis oportunități majore pentru sectorul sănătății, dar a generat și noi riscuri. Datele pacienților și funcționarea rețelelor spitalicești au devenit ținte valoroase pentru atacurile cibernetice, iar cerințele Directivei NIS 2 aduc standarde înalte de protecție și continuitate operațională. Business Intelligence contribuie la transformarea datelor brute în informații utile și structurate, sprijinind procesele decizionale strategice și operaționale prin instrumente interactive și vizualizări intuitive [1].

În acest context, România a implementat următoarele sisteme IT specifice sectorului medical [2]:

- Sistemul Informatic Unic Integrat (SIUI);

- Sistemul Informatic de Prescripţie Electronică (SIPE);
- Sistemul Cardului Electronic de Asigurări de Sănătate (CEAS);
- Dosarul electronic de Sănătate (DES);
- Serviciul Mobil de Urgenţă, Reanimare şi Descarcerare (SMURD);
- Telemedicină pentru zonele rurale (utilizat mai mult în pandemia Covid19);
- Sistem de clasificare pe grupuri de diagnostic (Grupuri de Diagnostic Înrudite - GDI).

Cu toate acestea, România nu dispune de o instituție dedicată exclusiv coordonării politicilor de e-Sănătate, care să acționeze ca partener tehnic al Comisiei Europene în vederea îndeplinirii obiectivelor comune din acest sector. Ministerul Sănătății rămâne singura autoritate responsabilă pentru toate activitățile medicale desfășurate la nivel național.

Pe baza revizuirii literaturii de specialitate prezentată în capitolul 1, s-au evidențiat o serie de statistici relevante care subliniază provocările și decalajele semnificative ale României în procesul de digitalizare:

- România se confruntă cu provocări majore în procesul de digitalizare, evidențiate de competențele digitale scăzute ale populației;
- În 2021, doar 28% dintre adulți aveau competențe digitale de bază, cel mai scăzut procent din UE, iar această tendință a persistat până în 2023;
- Conform Indicelui DESI 2020, doar 35% dintre persoanele între 16 și 74 de ani aveau competențe digitale elementare, comparativ cu media UE de 58%, în timp ce 18% dintre români nu au utilizat niciodată internetul, iar 34,6% dintre cei peste 55 de ani nu au accesat mediul online;
- Lipsa accesului la internet afectează în special mediul rural, limitând utilizarea platformelor online;
- În sectorul public, 82% dintre utilizatorii de internet interacționează online cu autoritățile publice, dar lipsa interoperabilității și fragmentarea infrastructurii plasează România pe ultimul loc în UE la performanța serviciilor publice digitale;
- În sănătate, 11% din populație nu are asigurare medicală, iar în mediul rural, procentul populației asigurate a scăzut de la 75,8% în 2014 la 63,5% în 2021;
- România ocupă locul trei în UE la nevoile medicale nesatisfăcute;
- Proiecte precum dosarul electronic de sănătate, cu peste 13 milioane de dosare, contribuie la reducerea decalajelor, dar vulnerabilitățile cibernetice rămân o problemă semnificativă, afectând 775.000 de români în 2022 prin atacuri precum phishing și inginerie socială.

Aceste date reflectă nivelul scăzut al competențelor digitale, accesul limitat la infrastructura tehnologică și lipsa interoperabilității sistemelor informatice, factori ce influențează negativ eficiența serviciilor publice și accesul cetățenilor la soluții digitale. În contextul acestei lucrări, care are ca scop dezvoltarea unei platforme integrate e-sănătate conforme cerințelor Directivei NIS 2, aceste statistici justifică necesitatea implementării unor măsuri inovatoare și bine coordonate pentru a îmbunătăți securitatea, eficiența și accesibilitatea infrastructurii critice din sănătate. Astfel, analiza situației actuale devine un fundament solid pentru demersurile propuse, subliniind importanța digitalizării ca factor esențial în modernizarea și protecția infrastructurilor critice.

Vedem astăzi faptul că, utilizarea tehnologiei informaţiei şi comunicaţiilor în domeniul medical este din ce în ce mai răspândită în zilele noastre având un rol strategic în livrarea unor servicii de sănătate mai sustenabile şi eficiente, contribuind la creşterea calităţii şi siguranţei îngrijirii pacientului.

În cadrul acţiunilor prevăzute în Strategia Europa 2020 la care România se aliniază, Uniunea Europeană mizează mult pe dezvoltarea sistemelor şi aplicaţiilor de e-Sănătate şi propune soluţii strategice pentru a face faţă sustenabilităţii, a îngrijirii şi asistenţei medicale.

Tehnologiile emergente și serviciile digitale, precum cele bazate pe cloud, big data, soluții mobile și IoT, au capacitatea de a transforma radical modul în care sunt furnizate și accesate serviciile de sănătate. Acestea generează noi cerințe și așteptări din partea diverselor categorii de utilizatori, inclusiv pacienți, profesioniști din domeniul medical, furnizori de tehnologii și servicii de sănătate, precum și personal administrativ.

În ceea de privesc Directivele Europene NIS (Network and Information Security), ele au ca scop consolidarea securității cibernetice în Uniunea Europeană și promovarea unei abordări armonizate la nivelul statelor membre. Directivele NIS au fost inițial adoptate în 2016, iar NIS 2 reprezintă o revizuire importantă a acestora. NIS 2 aduce schimbări semnificative în ceea ce privește cerințele de securitate cibernetică pentru OSE/ Entităţi esenţiale (Operatorii de Servicii Esențiale) [3, 4].

Operatorul de Servicii Esențiale (OSE/Entităţi esenţiale) este un concept cheie în cadrul Directivei Europene NIS 2 (Network and Information Systems Directive), care a fost transpusă în legislația națională a statelor membre, inclusiv România. Conform definiției oferite de DNSC (Directoratul Național de Securitate Cibernetică) din România, un OSE/Entităţi esenţiale este o entitate care oferă servicii esențiale pentru menținerea activităților economice și societale critice [5].

În lumina celor de mai sus, în cadrul acestei lucrări, ne propunem să analizăm impactul Directivei NIS 2 asupra infrastructurii critice din sănătate (CNAS fiind un OSE/Entitate esenţială), să identificăm cerințele specifice pentru acest sector și să evaluăm eficacitatea măsurilor de securitate cibernetică implementate. De asemenea, vom investiga cum aceste schimbări reglementare afectează furnizorii de servicii de asigurări de sănătate, inclusiv Casa Națională de Asigurări de Sănătate (CNAS), în asigurarea protecției datelor sensibile și a furnizării serviciilor medicale într-un mediu cibernetic sigur. Această analiză va contribui la înțelegerea mai profundă a impactului directivei asupra sectorului sănătății și la promovarea securității cibernetice în acest domeniu vital.

Programul de masterat „Managementul Sectorului Public” oferit de SNSPA a avut o contribuție semnificativă în structurarea și dezvoltarea lucrării de disertație, oferindu-mi atât fundamentele teoretice, cât și instrumentele practice necesare pentru a aborda o temă complexă, cum este crearea unei noi platforme PIAS, aliniată cerințelor Directivei Europene NIS 2.

În cele ce urmează, voi sublinia modul în care principalele cursuri din cadrul masteratului au influențat construcția acestei lucrări:

- *Managementul proiectelor publice* - Acest curs a fost esențial în înțelegerea etapelor necesare pentru dezvoltarea și implementarea unui proiect public complex, precum o platformă națională informatică în sănătate. Am aplicat conceptele de planificare strategică, alocare eficientă a resurselor și evaluare a riscurilor pentru a structura propunerile incluse în lucrare. Totodată, instrumentele de analiză studiate m-au ajutat să propun măsuri concrete pentru optimizarea proceselor și pentru integrarea cerințelor Directivei NIS 2 în proiect.
- *E-guvernare și transformare digitală* - Materia a oferit perspective valoroase asupra procesului de digitalizare a serviciilor publice, inclusiv asupra implementării soluțiilor de e-sănătate. În disertație, am integrat bunele practici internaționale discutate la curs, punând accent pe accesibilitate, interoperabilitate și eficiența utilizării resurselor. Totodată, mi-a permis să înțeleg provocările specifice digitalizării în sectorul public din România, pe care le-am adresat în cadrul analizei critice din lucrare.
- *Etică și integritate în administrația publică* - Un alt element cheie al lucrării este reprezentat de respectarea principiilor etice și de asigurarea transparenței în utilizarea resurselor publice. Acest curs m-a ajutat să conturez recomandări pentru implementarea unei noi platforme informatice PIAS care să respecte atât normele legale, cât și principiile de responsabilitate și integritate.

Integrarea cunoștințelor în lucrarea de disertație - Lucrarea de disertație reflectă o sinteză a cunoștințelor acumulate pe parcursul programului de masterat, aplicate la o problemă reală și complexă din sectorul public românesc. Fiecare capitol al lucrării este fundamentat pe elemente teoretice studiate, completate de soluții practice care răspund atât cerințelor Directivei NIS 2, cât și contextului specific al sănătății publice din România.

Astfel, masteratul „Managementul Sectorului Public" nu doar că a oferit o bază solidă pentru construirea acestei lucrări, ci a contribuit și la dezvoltarea unor competențe relevante pentru cariera mea, pregătindu-mă să abordez provocările complexe din sectorul public cu profesionalism și o viziune orientată spre soluții.

Întrebările și ipotezele de cercetare

În cadrul acestei cercetări au fost formulate atât întrebări, cât și ipoteze de cercetare, menite să contribuie la orientarea și atingerea scopului propus.

Întrebările elaborate pentru această cercetare au fost concepute după cum urmează:

- *Întrebarea 1:* Care sunt costurile și beneficiile implementării Directivei NIS 2 pentru organizații critice din sănătate?
- *Întrebarea 2:* Cum s-au schimbat tipurile de amenințări cibernetice în urma adoptării Directivei NIS 2 în sistemul critic din sănătate?
- *Întrebarea 3:* Cât de eficiente sunt măsurile de securitate implementate pentru a respecta cerințele NIS 2 în protejarea infrastructurii critice?

Ipotezele elaborate pentru această cercetare sunt prezentate după cum urmează:

- *Ipoteza 1:* Implementarea Directivei NIS 2 în infrastructura critică din sănătate va duce la reducerea numărului de incidente cibernetice datorită standardelor stricte de securitate și a măsurilor proactive de prevenire a atacurilor, inclusiv monitorizarea continuă și evaluările periodice de vulnerabilitate;
- *Ipoteza 2:* Costurile inițiale de conformitate cu Directivele NIS 2 în infrastructura critică din sănătate vor fi semnificative, dar vor fi compensate de scăderea costurilor asociate incidentelor cibernetice pe termen lung prin reducerea pierderilor financiare, a timpului de nefuncționare și a impactului negativ asupra reputației;
- *Ipoteza 3:* Colaborarea activă între organizațiile critice din domeniul sănătății pentru schimbul de informații privind amenințările cibernetice va conduce la o creștere a rezilienței și a securității cibernetice în sectorul sănătății deoarece partajarea rapidă a datelor și a celor mai bune practici permite reacții mai eficiente și implementarea de măsuri de protecție îmbunătățite.

Scopul și obiectivele de cercetare

Scopul principal al acestei lucrări de dizertație este de a dezvolta și implementa o nouă platformă PIAS care să fie conformă cu cerințele Directivei Europene NIS 2, contribuind astfel la îmbunătățirea securității și eficienței infrastructurii critice din sănătate pentru OSE/Entităţi esenţiale.
Obiectivele specifice ale lucrării includ:

- Analiza cerințelor directivei NIS 2: identificarea și înțelegerea cerințelor Directivei NIS 2 și evaluarea impactului acesteia asupra infrastructurii critice din sănătate. Acest lucru implică o revizuire detaliată a normelor și standardelor de securitate impuse de directivă;
- Dezvoltarea unei noi platforme integrate e-Sănătate/PIAS: crearea unei platforme moderne și integrate care să îmbunătățească funcționalitățile existente ale PIAS, asigurând în același timp conformitatea cu cerințele de securitate ale Directivei NIS 2. Platforma trebuie să ofere protecție împotriva amenințărilor cibernetice și să faciliteze interoperabilitatea între diferitele entități medicale;

- Evaluarea beneficiilor și provocărilor: realizarea unui studiu de caz pentru a evalua beneficiile aduse de noua platformă în termeni de securitate, eficiență și continuitate a serviciilor. De asemenea, identificarea provocărilor și obstacolelor întâlnite în procesul de implementare;
- Recomandări pentru factorii de decizie: oferirea de recomandări concrete pentru factorii de decizie din domeniul sănătății și IT, bazate pe rezultatele studiului și analizei efectuate. Aceste recomandări vor include bune practici pentru implementarea Directivei NIS 2 și pentru dezvoltarea unor sisteme informatice sigure și eficiente.

Prin atingerea acestor obiective, lucrarea își propune să contribuie la creșterea rezilienței cibernetice a infrastructurii critice din sănătate și la îmbunătățirea serviciilor medicale furnizate cetățenilor. Acest demers este esențial pentru asigurarea protecției datelor sensibile și pentru menținerea continuității serviciilor esențiale în fața amenințărilor cibernetice tot mai complexe.

Metodologia de cercetare

Metodologia utilizată în această cercetare a fost concepută pentru a aborda într-un mod detaliat și structurat problematica modernizării platformei informatice PIAS, cu un accent deosebit pe conformarea cu cerințele Directivei NIS 2. Metodele integrate reflectă o abordare sistematică, menită să asigure validitatea și aplicabilitatea rezultatelor, prin utilizarea unei combinații de metode calitative și cantitative.

Studiul bibliografic și analiza legislativă: Primul pas al cercetării a constat într-un studiu bibliografic cuprinzător, care a inclus analiza literaturii de specialitate, rapoarte tehnice și studii de caz relevante. Obiectivul acestei etape a fost de a identifica tendințele actuale și soluțiile aplicate în modernizarea platformelor informatice din sectorul sănătății. În paralel, analiza cadrului legislativ a evaluat impactul Directivei NIS 2 și al legislației naționale asupra cerințelor de securitate, performanță și interoperabilitate pentru PIAS.

Metode calitative: Metodologia de cercetare a inclus metode calitative pentru a analiza punctele forte și limitările platformei informatice existente PIAS. În cadrul acestei abordări, au fost realizate interviuri semi-structurate cu experți și utilizatori ai acestor platforme, inclusiv personal IT, cadre medicale și reprezentanți ai instituțiilor de reglementare. Interviurile au avut ca scop colectarea perspectivelor directe privind funcționalitatea platformelor, experiențele de utilizare și provocările întâmpinate. Datele calitative au fost completate de analiza documentelor oficiale și a rapoartelor tehnice, pentru a oferi un context detaliat.

Metode cantitative: Pentru validarea concluziilor și extinderea bazei de cunoștințe, cercetarea a inclus și o analiză cantitativă, utilizând date obținute prin chestionare adresate utilizatorilor platformelor informatice. Aceste chestionare au permis măsurarea percepției utilizatorilor asupra funcționalității, securității și eficienței PIAS. Instrumentul de colectare a datelor a fost conceput astfel încât să permită cuantificarea răspunsurilor și analiza statistică a tendințelor, fără a introduce elemente de complexitate suplimentară.

Analiza comparativă: Pentru a sprijini formularea de recomandări practice, metodologia a inclus și o analiză comparativă a soluțiilor similare implementate în alte țări europene. Această etapă a contribuit la adaptarea bunelor practici internaționale la contextul local și a oferit un cadru comparativ pentru evaluarea eficienței modelului propus.

Dezvoltarea modelului conceptual și validarea acestuia: Pe baza informațiilor colectate și analizate, a fost elaborat un model conceptual pentru modernizarea PIAS, care integrează componentele tehnice și organizaționale necesare. Validarea modelului s-a realizat utilizând criterii precum performanța, securitatea, scalabilitatea și alinierea la cerințele Directivei NIS 2. Acest model a fost testat în mod iterativ, prin aplicarea concluziilor obținute în etapele calitative și cantitative.

În concluzie, metodologia abordată asigură o integrare eficientă a perspectivelor teoretice și practice, sprijinind astfel propunerea de soluții viabile pentru optimizarea platformei informatice PIAS. Această integrare permite identificarea și abordarea lacunelor existente, facilitând adaptarea platformelor la cerințele de securitate și funcționalitate actuale, conform Directivei Europene NIS 2.

Prin utilizarea unei combinații de metode calitative și cantitative, cercetarea oferă un cadru cuprinzător pentru luarea deciziilor în domeniul sănătății digitale. Metodologia folosită contribuie nu doar la evaluarea stării curente a sistemelor informatice, ci și la formularea de strategii specifice care să asigure sustenabilitatea și eficiența infrastructurilor critice din sănătate.

Capitolul 1. Stadiul actual în domeniul investigat

1.1. Stadiul actual. Contextualizarea cercetării prin revizuirea literaturii de specialitate

Discursul academic referitor la potențialul sistemelor inteligente a debutat în anul 1950, odată cu publicarea lucrării fundamentale „Computing Machinery and Intelligence" de către Alan Turing. De atunci, cercetările în domeniul Inteligenței Artificiale au abordat un spectru larg de aplicații, de la operațiuni aritmetice automate până la algoritmi pentru jocuri strategice, cum ar fi șahul. Această evoluție continuă să ridice întrebări esențiale despre direcțiile tehnologice, limitele acestora și impactul asupra societății [6].

În prezent, termenii Inteligență Artificială, Machine Learning și Deep Learning sunt folosiți frecvent ca sinonime, deși aceștia desemnează concepte distincte. În esență, Machine Learning acoperă un ansamblu variat de metode destinate să ofere calculatoarelor capacități cognitive similare celor umane. Acest domeniu include tehnici precum procesarea limbajului natural (Natural Language Processing), analiza sintactică, optimizarea căutărilor și sistemele expert, toate având ca scop simularea comportamentului uman în cadrul sistemelor informatice [6].

Astăzi dinamica sectorului IT și a tehnologiilor smart este ultra rapidă, viteza de inovare fiind mai mare decât viteza de învățare [7]. Inovarea bazată pe date și informații deține un rol central în cadrul procesului de dezvoltare a orașelor. Big data a devenit un „activ foarte valoros în economie, încurajând apariția de noi industrii, alături de procese, produse și servicii, la rândul lor noi, creând [celor care le gestionează] avantaje competitive semnificative" (OECD, 2015). Exploatarea și explorarea datelor poate aduce valoare adăugată multor sectoare, de la optimizarea proceselor de producție (în industrie) până la creșterea satisfacției cetățeanului când acesta se află pe poziția de consumator de bunuri și servicii. Tehnologiile de tipul smart grid – de care am amintit în capitolul introductiv - generează volume foarte mari de date referitoare la oferta și consumul de energie electrică; gestionate corespunzător, acestea pot spori eficiența [7].

Revoluția *„open data"* - Intenția de a oferi accesul liber la datele colectate de diferite *device*-uri deschide oportunități unice până acum, oportunități care ar putea ajuta transformarea orașelor în care trăim. Trecerea către *open data*, în special cele generate de instituții publice, duce la o creștere a transparenței și a responsabilității, ajutând, pe de o parte, cetățenii să participe la actul de guvernare și, pe de altă parte, factorii de decizie în stabilirea strategiilor de dezvoltare [7].

În ceea ce privește administrația publică, acesteia reprezintă o condiţie primordială dezvoltării economice şi sociale la nivelul întregii societăţii. De asemenea, administrația publică joacă un rol crucial în implementarea modelelor de dezvoltare durabilă, prin adoptarea unor practici care asigură sustenabilitatea operațională și colaborarea interinstituțională, aspecte esențiale în gestionarea infrastructurilor critice [8] .Promovarea şi implementarea tehnologiilor informatice la

nivelul instituţiilor publice vor alinia economia naţională la standardele internaţionale. Promovarea unui tip modern de administraţie, bazat pe tehnică şi cunoaştere, va avea rezultate importante la nivelul întregii societăţi, va schimba mentalităţi şi va modela un alt fel de cultură organizaţională [9]. Atfel, E-guvernarea (concept cunoscut si in spatele englezismului e-gov) este una dintre cele mai – daca nu cea mai – interesanta provocare a Adminitratiei Publice din intreaga lume. E-guvernarea este o simbioza intre societate si tehnologie [9].

E-guvernarea, cunoscută și sub termenul englezesc de „e-gov," reprezintă una dintre cele mai fascinante provocări contemporane pentru administrațiile publice la nivel global. Acest concept se situează la intersecția dintre tehnologie și societate, promovând o transformare digitală a interacțiunii dintre cetățeni, instituții publice și sectorul privat. E-guvernarea nu se rezumă doar la implementarea de platforme tehnologice, ci implică o schimbare profundă în modul de furnizare a serviciilor publice, accentuând transparența, eficiența și accesibilitatea. Această simbioză între inovația tehnologică și nevoile societale redefinește rolul administrației publice în era digitală [9].

În ceea ce privește administrația publică, principalele elemente de IT pentru digitalizarea acesteia includ utilizarea hardware-ului și software-ului adecvat, procesarea de text, calculul tabelar, gestionarea bazelor de date dar și prezentarea profesională a rezultatelor prin intermediul platformelor specifice PowerPoint, prezi, etc. Aceste instrumente tehnologice esențiale contribuie la eficientizarea activităților administrative, facilitând organizarea datelor, analiza informațiilor și comunicarea eficientă. Totodată, sunt abordate aspecte precum securitatea informației și respectarea cadrului legislativ specific digitalizării [10].

Pe lângă toate acestea oamenii secolului 21 se confruntă, atât la locul de muncă dar și în viața de zi cu zi, cu aspecte mai generale preum management de documente, organizarea personala dar și muncă digitală. Mai mult decât atât, întreaga eră digitală aflată în fața debutului fulminant, aduce cu sine pentru om o serie de probleme care, în urmă cu 20 de ani puteau părea ficțiune. Printre acestea se pot enumera consecințe precum stresul digital, lipsa de socializare fizică, amenințările cibernetice, toate acestea conducând până la dezvoltarea unor metode de combatere a acestor pericole, precum detoxifierea digitala [11].

Aplicațiile digitale simplifică activități precum plata taxelor sau cumpărăturile online, eliminând necesitatea unor cunoștințe avansate despre tehnologie. Totuși, diferențele în competențele digitale dintre generații rămân semnificative. În Irlanda, o țară cu performanțe digitale ridicate, peste jumătate (>50%) dintre persoanele de peste 65 de ani nu utilizează Internetul, față de o medie națională de doar 23% [12].

Educația digitală poate aduce beneficii clare, crescând șansele de angajare și accesul la informații sau servicii. Cu toate acestea, mulți oameni în vârstă ezită să adopte noile tehnologii din cauza temerilor legate de dificultatea procesului de învățare. Realitatea demonstrează însă contrariul, numeroase exemple ilustrând succesul acestora în dobândirea de competențe digitale [12]. Incluziunea digitală se extinde dincolo de nevoile vârstnicilor, vizând și categoriile defavorizate, precum persoanele fără loc de muncă, cu dizabilități sau din zone izolate. Programele de formare digitală, denumite „Incluziune digitală" sau „eInclusion", sunt concepute să fie scurte, accesibile și eficiente, având un impact pozitiv semnificativ asupra integrării sociale și economice [12].

Pandemia de COVID-19 a forțat digitalizarea rapidă a instituțiilor din România, expunând însă vulnerabilități semnificative în securitatea cibernetică și protecția datelor. Conform EUROSTAT, doar 28% dintre adulții români aveau în 2021 abilități digitale de bază, cel mai scăzut procent din UE. Până în 2023, această tendință a rămas constantă, România situându-se încă pe ultimul loc în clasamentul competențelor digitale. În 2022, aproximativ 775.000 de români au fost vizați de atacuri cibernetice precum phishing sau inginerie socială, evidențiind nevoia de măsuri mai stricte de securitate [13].

Principalele probleme includ lipsa educației digitale, infrastructura de internet deficitară și vulnerabilitățile în fața atacurilor cibernetice, cum ar fi compromiterea conturilor de e-mail. Deși tehnologiile avansate precum blockchain-ul și autentificarea multi-factorială sunt utilizate pentru protecție, costurile ridicate și complexitatea limitează implementarea lor largă. Totodată, utilizarea inteligenței artificiale în atacurile cibernetice și gestionarea insuficientă a riscurilor asociate subliniază urgența adoptării unor soluții proactive [13].

În domeniul siguranței cibernetice, mai multe guverne, inclusiv cel al Indoneziei, au implementat măsuri concrete pentru a preveni potențialele atacuri și pentru a combate criminalitatea cibernetică. Guvernul indonezian s-a remarcat în mod special prin inițiativele susținute și prin numeroasele apeluri publice lansate în ultimii ani, menite să crească nivelul de conștientizare asupra riscurilor asociate spațiului cibernetic [14].

Un aspect esențial al acestei strategii constă în mobilizarea și implicarea utilizatorilor de platforme sociale, cum ar fi Twitter. Pe lângă conturile oficiale ale sectorului public, cetățenii activi pe aceste platforme contribuie semnificativ la diseminarea mesajelor de prevenire și la popularizarea campaniilor de conștientizare a pericolelor din mediul online. Această colaborare între autorități și comunitatea online reflectă o abordare integrată, în care atât instituțiile statului, cât și societatea civilă joacă un rol complementar în asigurarea securității digitale Prin astfel de inițiative, guvernul indonezian nu doar că își consolidează capacitatea de apărare cibernetică, dar promovează și un model de cooperare intersectorială, subliniind importanța implicării colective în prevenirea criminalității cibernetice. Aceste măsuri pot servi drept exemplu pentru alte state care urmăresc să-și îmbunătățească reziliența în fața provocărilor din spațiul digital [14].

În domeniul informatic, digitalizarea serviciilor publice aduce beneficii semnificative, dar și riscuri considerabile, printre care se numără amenințările cibernetice și atacurile cu programe malware complexe. Virusul Flame reprezintă un exemplu notabil al acestor riscuri, fiind o armă cibernetică sofisticată, capabilă să colecteze date sensibile din sisteme informatice cheie, fără a fi detectată timp de ani de zile. Studiile au arătat că Flame a fost conceput să vizeze un număr redus de computere, având o arhitectură modulară și flexibilă, utilizând tehnologii avansate precum criptarea, tehnicile de „process injection” și analiza vulnerabilităților pentru propagare. Deși a avut ca principal scop colectarea de informații, fără intenții financiare directe, complexitatea sa sugerează o finanțare guvernamentală și utilizări strategice în cadrul unor operațiuni de spionaj cibernetic [15]. Aceste constatări accentuează importanța implementării unor măsuri riguroase de securitate cibernetică în procesul de digitalizare, pentru a proteja infrastructura critică și datele sensibile împotriva unor astfel de amenințări sofisticate.

În articolul său intitulat „Convergența securității digitale”, autorul Cătălin Vrabie analizează în profunzime cinci aspecte esențiale ale transformărilor din domeniul securității cibernetice, abordând evoluția tehnologică, impactul acesteia asupra societății și provocările emergente [16].

Aceste aspecte sunt:

- Evoluția convergenței securității digitale: Autorul descrie trecerea de la interacțiunile punctuale om-mașină la tehnologii care își asumă roluri complexe, până la simularea completă a comportamentului uman în rețele digitale, subliniind creșterea vulnerabilităților asociate;
- Rădăcinile militare ale tehnologiilor digitale: Se evidențiază cum inovațiile militare, precum Internetul sau comunicațiile prin satelit, au modelat utilizările civile și au determinat dependența globală de tehnologia digitală;
- Războaiele cibernetice și spionajul digital: Studiul detaliază modul în care tehnologia a înlocuit complet metodele tradiționale de spionaj, exemplificând prin atacuri celebre precum Stuxnet, care a reconfigurat perspectiva globală asupra securității;
- Vulnerabilitățile globale și riscurile cibernetice: Se subliniază implicațiile mondiale ale atacurilor cibernetice, vizând infrastructuri critice și sisteme economice, cu accent pe necesitatea unor soluții coordonate și robuste;

- Proiecțiile viitoare și soluțiile posibile: Autorul sugerează implementarea de rețele virtuale sofisticate, menite să inducă în eroare atacatorii și să protejeze resursele reale.

În concluzie, importanța crescută a digitalizării și a conectivității globale necesită o abordare complexă, centrată pe educație digitală și implementarea de sisteme de securitate actualizate. Crearea unor tehnologii proactive și adaptabile, alături de instruirea continuă a utilizatorilor, reprezintă soluția sustenabilă pentru protejarea infrastructurilor critice și asigurarea unei tranziții sigure către viitorul digital. Într-un context global marcat de riscuri și oportunități cibernetice, inovația trebuie însoțită de o responsabilitate constantă în gestionarea tehnologiei, pentru a consolida un mediu digital sigur și eficient.

Pe de altă parte, în ceea ce privește supravegherea digitală, autorul Cătălin Vrabie, remarcă, de asemenea, faptul că programele globale, precum PRISM și XKeyscore, facilitează colectarea masivă de date și monitorizarea comunicațiilor, adesea compromițând intimitatea utilizatorilor prin slăbirea intenționată a algoritmilor de securitate. Această practică creează un dezechilibru semnificativ, în care țările mai mici, dependente de infrastructurile digitale ale marilor puteri, sunt vulnerabile la supraveghere necontrolată, fără reciprocitate. Deși supravegherea este justificată adesea prin necesitatea prevenirii terorismului, utilizarea acestor tehnologii vizează uneori persoane și instituții fără legături directe cu astfel de amenințări, ridicând probleme etice serioase. Autorul subliniază necesitatea unei tranziții către platforme open-source dezvoltate colaborativ și a unei educații digitale extinse, pentru a proteja drepturile fundamentale și pentru a crea un mediu digital echilibrat, sigur și etic [17].

Unii autori au concluzionat că digitalizarea sănătății este o prioritate esențială pentru îmbunătățirea accesului la servicii medicale și optimizarea sistemelor de sănătate. În România, aproximativ 11% din populație nu are asigurare de sănătate, ceea ce limitează accesul la servicii medicale, în special în mediul rural, unde procentul populației asigurate a scăzut de la 75,8% în 2014 la 63,5% în 2021. Dezechilibrele teritoriale sunt accentuate, iar rata nevoilor medicale nesatisfăcute, cauzată de distanța față de unitățile medicale, este a treia cea mai mare din Uniunea Europeană [18, 19].

În ceea ce privește soluțiile digitale, inițiativele recente includ implementarea dosarului electronic de sănătate (DES), care până în prezent a înregistrat peste 13 milioane de dosare și facilitează accesul rapid la informațiile esențiale despre pacienți. Alte proiecte notabile sunt rețeta electronică, biletul de trimitere electronic și sistemul de telemedicină, acestea având ca scop reducerea timpilor de așteptare și creșterea calității îngrijirii, inclusiv în zone izolate sau defavorizate [19].

Totodată, cercetările arată că sistemul de sănătate public din România este dezechilibrat financiar, fiecare contribuabil plătind, în medie, asigurări de sănătate pentru alte două persoane care nu contribuie, ceea ce generează incertitudini în sustenabilitatea sistemului. Pentru a rezolva aceste probleme, este esențială digitalizarea sistemului, interoperabilitatea între sistemele medicale naționale și europene și introducerea unor politici care să asigure o distribuție echitabilă a resurselor și accesului la servicii medicale [19].

Lipsa interoperabilității între sistemele medicale limitează schimbul eficient de date, iar România are cel mai mare număr de categorii exceptate de la plata contribuțiilor de sănătate din UE, creând presiuni financiare. Pensionarii și populația din zone izolate suferă cel mai mult, având un nivel ridicat de nevoi nesatisfăcute, iar distanțele mari până la unitățile medicale contribuie la acest decalaj, situând România pe locul trei în UE. Proiectele de digitalizare, precum dosarul electronic de sănătate și telemedicina, împreună cu finanțarea prin PNRR (400 milioane de euro până în 2026), pot reduce aceste disparități. Implementarea Directivei NIS 2 devine esențială pentru a crește securitatea datelor și a reduce incidentele cibernetice, contribuind astfel la o infrastructură medicală mai eficientă și mai sigură [18].

Procesul de digitalizare a administrației publice în România, bazat pe administrația 2.0, a înregistrat progrese prin platforme precum Sistemul Electronic Național și Single Digital Gateway. Totuși, persistă probleme majore, precum lipsa accesului la internet pentru o parte semnificativă a populației rurale și nivelul scăzut de alfabetizare digitală. Conform Institutului Național de Statistică, 34,6% dintre persoanele între 55 și 74 de ani nu au utilizat niciodată internetul, evidențiind dificultăți în adoptarea serviciilor electronice [20].

Dezavantajele includ vulnerabilități cibernetice, dificultăți de gestionare a datelor și lipsa unui standard de compatibilitate pentru dispozitive IoT. O analiză SWOT a arătat puncte slabe precum infrastructura inadecvată și educația digitală deficitară. Deși s-au realizat progrese, precum crearea Autorității pentru Digitalizarea României, multe servicii electronice rămân dificil de utilizat pentru cei mai puțin familiarizați cu tehnologia [20].

Alți autorii vin să reconfirme problemele țării noastre privind digitalizarea. Lipsa accesului la internet afectează semnificativ cetățenii din zonele rurale sau vulnerabile, limitând capacitatea acestora de a utiliza platformele online pentru servicii publice, inclusiv în sănătate. De asemenea, sistemul administrativ românesc a fost considerat nepregătit pentru gestionarea crizelor, cum ar fi pandemia COVID-19, evidențiindu-se necesitatea unei infrastructuri digitale robuste. Metodele precum Lean Six Sigma au fost propuse pentru a instrui funcționarii publici și a îmbunătăți gestionarea cererilor atât în format digital, cât și fizic. Totodată, adoptarea platformelor digitale a fost identificată ca o soluție pentru reducerea birocrației și accelerarea soluționării cererilor, o abordare esențială în alinierea la cerințele Directivei NIS 2. În plus, metodologia D.M.A.I.C. a fost recunoscută ca un instrument util pentru optimizarea proceselor și creșterea eficienței în sectorul sănătății [21].

Un alt studiu relevă multiple beneficii ale implementării inteligenței artificiale (IA) în sănătate, incluzând utilizarea sa în chirurgie minim invazivă, diagnostic avansat, robotică medicală și monitorizarea pacienților în timp real. Unele cercetări evidențiază capacitatea IA de a reduce semnificativ costurile prin scurtarea perioadelor de spitalizare și diminuarea complicațiilor postoperatorii. De exemplu, roboții de sterilizare cu UV sunt raportați ca având eficiență de până la 98% în eliminarea agenților patogeni din sălile de operație. În plus, piața globală de IA în sănătate a înregistrat o creștere rapidă, de la 8,2 miliarde USD în 2021 la o estimare de 49,1 miliarde USD până în 2026, cu o rată compusă de creștere anuală de 48,4% [22].

Cu toate acestea, provocările semnificative în adoptarea IA, inclusiv lipsa unui cadru legal bine definit pentru gestionarea cazurilor de malpraxis asociate tehnologiei. De asemenea, cercetările arată că Europa rămâne în urma SUA și Chinei în ceea ce privește investițiile private în IA aplicată sănătății, recomandându-se investiții anuale de cel puțin 20 de miliarde EUR pentru a reduce decalajele tehnologice. În România, dificultăți precum lipsa finanțării adecvate pentru cercetare contribuie la migrarea specialiștilor, ceea ce îngreunează implementarea și dezvoltarea soluțiilor inovatoare [22].

Studiile indică faptul că numeroase comunități rurale din România nu beneficiază de acces la servicii medicale moderne, ceea ce contribuie la rate ridicate de mortalitate din cauza bolilor netratate. În plus, ineficiența guvernamentală în alocarea fondurilor și lipsa infrastructurii regionale moderne sunt identificate ca probleme majore care limitează accesul la tratamente și diagnostic avansat. De asemenea, se constată dificultăți în aprovizionarea constantă cu medicamente pentru boli cronice, ceea ce amplifică inegalitățile în sănătate [22].

Se poate afirma, deci, faptul că inteligența artificială are potențialul de a transforma semnificativ sectorul sănătății prin creșterea eficienței și accesului la servicii avansate. Totuși, integrarea sa necesită colaborare interdisciplinară și investiții substanțiale în infrastructură și formarea specialiștilor. Adopția IA în sănătate rămâne un proces complex, influențat de factori economici, politici și sociali, dar oferă perspective pozitive pe termen lung pentru îmbunătățirea calității vieții.

Unii autori au apreciat, de asemenea, faptul că digitalizarea administrației publice reprezintă o necesitate urgentă în contextul schimbărilor tehnologice și socio-economice, dar România rămâne pe ultimele locuri în clasamentele europene la acest capitol. Studiile arată că România se află pe locul 28 din 28 în privința serviciilor publice digitale (DESI 2020), iar principala cauză o constituie lipsa interoperabilității sistemelor informatice și carențele în competențele digitale ale personalului. În plus, cadrul legislativ este considerat nefavorabil pentru implementarea soluțiilor moderne [23].

Un alt aspect evidențiat este rezistența la schimbare a funcționarilor publici și lipsa dotărilor tehnologice adecvate, care împiedică adoptarea digitalizării pe scară largă. Autorii recomandă implementarea măsurilor de educare digitală a populației și crearea unor strategii naționale pe termen lung, însoțite de investiții în infrastructură și de alinierea la directivele europene, cum ar fi Directiva NIS 2, pentru a asigura securitatea și eficiența serviciilor publice digitale [23].

Aceste coonstatări sprijină necesitatea unei platforme digitale integrate în sectorul sănătății, aliniate cerințelor Directivei NIS 2, care să îmbunătățească interoperabilitatea și să faciliteze accesul echitabil la servicii pentru toate categoriile de utilizatori.

Alte studii fin să întărească concluziile celorlalți autori, de mai sus, referitoare la performanțele slabe ale tării noastre privind digitalizarea. România se situează pe penultimul loc în Uniunea Europeană în privința gradului de digitalizare a economiei și societății, conform Indicelui DESI 2020. Se remarcă faptul că doar 35% dintre persoanele cu vârste între 16 și 74 de ani au competențe digitale elementare, comparativ cu media UE de 58%, iar 18% dintre români nu au utilizat niciodată internetul. În ceea ce privește serviciile publice digitale, România înregistrează cea mai slabă performanță dintre statele membre, cu toate că 82% dintre utilizatorii de internet interacționează online cu autoritățile publice, plasând țara pe locul 7 la acest capitol [24].

Autorii mai subliniază că sistemul informatic al administrației publice din România este fragmentat, ceea ce duce la o interoperabilitate redusă între instituții și creează sarcini administrative suplimentare pentru cetățeni. Principalele bariere în calea digitalizării sunt lipsa coordonării interinstituționale, migrarea specialiștilor IT din sectorul public și competențele digitale insuficiente. În acest context, implementarea unei soluții de e-guvernare și adoptarea unei legislații privind interoperabilitatea ar putea contribui semnificativ la eficientizarea serviciilor publice [24].

În ceea ce privește România, autorii subliniază multiple deficiențe în domeniul securității sănătății și digitalizării, evidențiind scorul general scăzut de 45,8 în Indexul Global de Securitate a Sănătății, sub media Europei de Est de 46,3. Problemele critice includ detectarea și raportarea epidemiilor, răspunsul rapid la urgențe și sistemul de sănătate, toate fiind sub media regională. De asemenea, infrastructura digitală și mecanismele de coordonare între sectoarele sănătății umane, animale și de mediu sunt insuficiente, afectând schimbul de date necesar pentru o reacție eficientă la crize biologice. Deficiențele sunt amplificate de lipsa facilităților de izolare în spitale și deficitul de personal medical, în special în zonele rurale. În plus, vulnerabilitățile sociale și politice, precum încrederea scăzută a publicului în guvern și cheltuielile generale scăzute pentru sănătate, compromit reziliența sistemului [25].

Toate aceste aspecte, similare cu cele din Republica Moldova [25], justifică necesitatea implementării unor măsuri proactive, cum ar fi investițiile în digitalizare și integrarea sistemelor de sănătate prin platforme conforme Directivei NIS 2, pentru a îmbunătăți securitatea cibernetică și capacitatea de reacție în fața amenințărilor.

Principalele constatări rezultate din analiza stadiului actual al cercetării, fundamentate pe o revizuire cuprinzătoare a literaturii de specialitate, pot fi sintetizate în mod succint, evidențiind aspecte esențiale ce justifică importanța și necesitatea acestei cercetări.

S-a observat faptul că, digitalizarea sănătății și a administrației publice este o necesitate strategică în era tehnologică, având potențialul de a transforma fundamental accesul la servicii și securitatea infrastructurilor critice. Contextul global, marcat de creșterea amenințărilor cibernetice și de cerințele tot mai complexe de conformitate, subliniază importanța implementării Directivei NIS 2 ca măsură esențială pentru protejarea datelor și reducerea vulnerabilităților sistemului. În sectorul sănătății, această directivă oferă un cadru structurat pentru standardizarea măsurilor de securitate, prevenirea incidentelor și asigurarea continuității operaționale a organizațiilor critice, având impact direct asupra siguranței pacienților și calității serviciilor.

Deși conformitatea implică costuri semnificative, studiile arată că aceste investiții vor genera beneficii pe termen lung, prin reducerea pierderilor financiare asociate atacurilor cibernetice, diminuarea timpilor de nefuncționare și protejarea reputației instituțiilor implicate. În plus, interoperabilitatea între sistemele informatice și adoptarea platformelor digitale conforme Directivei NIS 2 vor facilita un schimb de date mai eficient și o coordonare mai bună între instituții, contribuind la optimizarea resurselor și la o reacție mai rapidă în fața crizelor.

Totodată, nivelul scăzut al competențelor digitale, alături de reticența la schimbare și fragmentarea infrastructurii, reprezintă bariere majore care trebuie depășite. Educația digitală, formarea personalului și implementarea unor strategii naționale bine fundamentate sunt esențiale pentru crearea unui sistem robust. Colaborarea între organizații, schimbul de informații despre amenințările cibernetice și adoptarea celor mai bune practici la nivel european sunt factori care vor amplifica reziliența sectorului de sănătate.

În lumina celor de mai sus, putem concluziona faptul că, Directiva NIS 2 devine un instrument indispensabil pentru atingerea obiectivelor de securitate cibernetică, eficiență operațională și accesibilitate echitabilă la servicii. Integrarea tehnologiilor avansate, cum ar fi inteligența artificială și automatizarea proceselor, deschide calea pentru inovare și o adaptare mai bună la cerințele viitoare. Aceste transformări nu doar că răspund nevoilor imediate, ci creează un model sustenabil de dezvoltare, centrat pe protecția cetățenilor, reducerea inegalităților și promovarea unui mediu digital sigur și eficient. Alinierea la cerințele Directivei NIS 2 nu este doar o obligație legală, ci o oportunitate de a redefine calitatea serviciilor publice și de a poziționa sistemul național de sănătate în rândul celor mai performante din Europa.

1.2. Cadrul specific. Analiza legislației, politicilor și obiectivelor naționale

Legislația care să reglementeze și să sprijine funcționarea eficientă a domeniului e-Sănătate este încă insuficient dezvoltată atât în România, cât și la nivelul Uniunii Europene. Una dintre cele mai mari provocări din acest sector este legată de lipsa de standardizare, care complică implementarea și utilizarea soluțiilor tehnologice în sănătate.

Protecția și securitatea datelor utilizate în sistemele e-Sănătate reprezintă o prioritate absolută, având în vedere că mulți utilizatori manifestă rezerve în a adopta aceste tehnologii din cauza preocupărilor legate de confidențialitate. Eforturile de standardizare trebuie să respecte cerințele legale și sociale de protecție a vieții private a pacienților, precum și să asigure securitatea datelor acestora. Este esențial să fie implementate măsuri riguroase în ceea ce privește transferul de date, integritatea informațiilor, accesul controlat și autentificarea utilizatorilor [26]..

În țările în curs de dezvoltare, există mai mulți factori care împiedică atingerea unor standarde înalte în e-Sănătate. Conform cercetărilor realizate de Telecommunication Standardization Sector of the International Telecommunications Union (ITU-T), principalele deficiențe sunt [26]:

- Lipsa conștientizării importanței standardelor naționale;

- Participarea redusă a industriei în procesul de elaborare a standardelor;
- Finanțare insuficientă pentru dezvoltarea standardizării;
- Resurse umane inadecvate pentru acest domeniu;
- Implicare limitată în dezvoltarea standardelor internaționale;
- Infrastructură tehnică deficitară pentru aplicarea standardelor.
- Adoptarea soluțiilor informatice în sănătate progresează mai lent decât în alte sectoare.

Acest lucru se datorează unor factori precum preocupările legate de protecția datelor personale în cazul schimbului de informații, dar și investițiilor inițiale ridicate necesare pentru implementare. Totuși, costurile de întreținere ulterioare sunt, în general, mai reduse. În plus, utilizatorii acestor sisteme trebuie să fie instruiți în colectarea și analiza datelor, ceea ce implică, de exemplu, cunoștințe de programare. Pe de altă parte, uneori, decidenții, managerii de spitale, personalul medical și cetățenii nu sunt suficient informați cu privire la beneficiile și economiile pe termen lung aduse de utilizarea tehnologiilor e-Sănătate [26].

Confidențialitatea informațiilor medicale a fost și rămâne o valoare fundamentală a relației dintre medic și pacient. Astfel, accesul la datele electronice din sănătate trebuie protejat prin proceduri sigure de identificare și autentificare.

Din perspectivă juridică, Regulamentul european nr. 910/2014 privind identificarea electronică și creșterea încrederii va contribui la sporirea eficienței serviciilor publice și private în mediul online. În plus, protecția datelor personale este reglementată la nivel european prin Directiva privind protecția datelor.

În era digitală, sistemele informatice din domeniul sănătății sunt fundamentale pentru furnizarea eficientă și sigură a serviciilor medicale. Aceste sisteme gestionează date sensibile și asigură comunicarea între diferite entități medicale, contribuind la îmbunătățirea calității îngrijirii pacienților. Cu toate acestea, creșterea dependenței de tehnologie și de rețelele informatice expune infrastructurile critice din sănătate la riscuri cibernetice semnificative. În acest context, Directivele Europene, în special Directiva NIS 2 (Network and Information Security), impun standarde stricte pentru securitatea și reziliența rețelelor și sistemelor informatice utilizate de Operatorii de Servicii Esențiale (OSE/Entităţi esenţiale).

PIAS (Platforma Informatică a Asigurărilor de Sănătate) și SIUI (Sistemul Informatic Unic Integrat) sunt componente esențiale ale infrastructurii informatice din sănătate în România. Aceste platforme sunt responsabile pentru gestionarea și procesarea informațiilor legate de asigurările de sănătate și serviciile medicale furnizate cetățenilor. Totuși, în fața provocărilor cibernetice actuale și a cerințelor impuse de Directiva NIS 2, este necesară o actualizare și integrare a acestor sisteme pentru a asigura o protecție adecvată a datelor și o continuitate a serviciilor esențiale.

Capitolul 2. Dezvoltarea integrată a unor soluții de e-Sănătate, cu anvergură națională - CNAS

Într-un context marcat de transformări digitale rapide și de creșterea importanței rezilienței cibernetice în sectorul sănătății, acest capitol explorează soluțiile propuse pentru modernizarea și integrarea infrastructurilor informatice ale Casei Naționale de Asigurări de Sănătate (CNAS). În strânsă legătură cu obiectivele Directivei NIS 2, capitolul își propune să ofere o perspectivă detaliată asupra necesității și modului de implementare a unei platforme informatice de e-Sănătate, care să răspundă cerințelor de securitate cibernetică și interoperabilitate.

Pornind de la provocările identificate anterior, această secțiune se concentrează pe obiectivele și structura unui proiect național dedicat e-Sănătății, detaliind avantajele și pașii necesari pentru

implementarea acestuia. De asemenea, sunt analizate oportunitățile și riscurile implicate, pentru a oferi o viziune clară asupra transformărilor necesare în sectorul medical din România.

2.1. Detalii generale

Pentru a asigura modernizarea și digitalizarea sectorului de sănătate din România, acest proiect național propune dezvoltarea unei soluții integrate de e-Sănătate, sub coordonarea Casei Naționale de Asigurări de Sănătate (CNAS). Această inițiativă urmărește atât îmbunătățirea funcționalității și interoperabilității sistemelor existente, cât și creșterea nivelului de securitate cibernetică în conformitate cu cerințele Directivei NIS 2.

În această secțiune, sunt prezentate elementele esențiale ale proiectului, precum instituțiile implicate, sursele de finanțare, obiectivele generale și specifice, precum și o analiză a factorilor ce influențează implementarea sa. Detalierea acestor aspecte oferă o perspectivă completă asupra strategiei de implementare și a impactului preconizat asupra sistemului de sănătate.

Denumirea instituției solicitante:
- CNAS – Casa Națională de Asigurări de Sănătate din Romania

Sursa de finanțare:
- FEDR (2021-2028) proiect european
- PNRR – Planul național de redresare și reziliență

Axa prioritară/cod apel:
- PRIORITATEA 6: Digitalizarea sistemului medical

Denumire/tip de instituții partenere :
- CNAS, MS, STS

Titlul proiect:
- Dezvoltarea integrată a unor soluții de e-sănătate, cu anvergură națională- CNAS

Valoarea totală estimată a proiectului:
- 50,66 milioane euro (old)

Durata estimată a proiectului:
- 4 ANI (2024-2028)

Zona geografică vizată de proiect:
- Romania

Tabel 1. Analiza SWOT a implementării soluțiilor de e-Sănătate la nivel național [26]

PUNCTE FORTE	**PUNCTE SLABE**
-Creştere rapidă pe piaţa serviciilor de bunăstare fizică susţinută de tehnologiile digitale;	-Lipsa informării şi a încrederii în soluţiile specifice e-Sănătate în rândul pacienţilor, cetăţenilor şi al cadrelor medicale;
-Reconfigurarea proceselor de acordare a îngrijirilor medicale sunt paşi importanţi în telemedicina modernă;	-Nivel scăzut al interoperabilităţii soluţiilor de e-Sănătate;
-Convergenţa dintre tehnologiile wireless şi dispozitivele medicale cu	-Număr mic de informaţii la scară largă care să demonstreze rentabilitatea

serviciile de asistenţă medicală şi socială favorizează apariţia unor noi activităţi economice; -e-Sănătate oferă servicii de asistenţă medicală personalizate şi centrate asupra cetăţeanului; -Mijloc de a îmbunătăţi eficienţa şi eficacitatea sistemelor, precum şi controlul acestora şi de a reduce cheltuielile; -Interes în a promulga strategii de e-Sănătate; -Scăderea continuă a prețului la tehnologiile TIC.	financiară a instrumentelor şi serviciilor de e-Sănătate; -Lipsa de claritate juridică pentru aplicaţiile mobile specifice domeniului sănătăţii şi al bunăstării fizice; -Lipsa transparenţei în ceea ce priveşte utilizarea datelor colectate de astfel de aplicaţii; -Schimbări frecvente în structura de management a Ministerului Sănătăţii; -Lipsa unei legislaţii obligatorii privind cadru de standardizare; -Lipsa cooperării între instituţiile abilitate; -Utilizare insuficientă a standardelor internaţionale.
OPORTUNITĂȚI	**AMENINȚĂRI**
-Platforma e-Sănătate sprijină integrarea socială și economică, promovează egalitatea de șanse, îmbunătățește calitatea vieții și încurajează responsabilizarea pacienților prin sporirea transparenței. -Acces la servicii şi informaţii precum şi utilizarea mijloacelor de comunicare sociale în domeniul sănătăţii; -Posibilitatea de a utiliza experienţa altor state membre UE şi a OMS;	-Grad scăzut de pregătire a utilizatorilor de aplicaţii de e-Sănătate; -Costurile iniţiale ridicate ale creării sistemelor de e-Sănătate; -Disparitățile regionale în accesul la servicii TIC, regiunile dezavantajate confruntându-se cu acces restrâns. -În plus, cadrele juridice insuficiente sau fragmentate, în special în domeniul e-Sănătății, se reflectă în absența sistemelor de rambursare.

Analiza SWOT scoate în evidență complexitatea transformării digitale a sectorului de sănătate din România, subliniind atât oportunitățile majore, cât și provocările critice care trebuie abordate.

Pe de o parte, soluțiile de e-Sănătate au potențialul de a revoluționa modul în care sunt furnizate serviciile medicale, prin reducerea costurilor, creșterea eficienței și personalizarea îngrijirilor. Integrarea tehnologiilor moderne, cum ar fi telemedicina și dispozitivele wireless, poate deschide noi oportunități economice și sociale, sprijinind incluziunea și egalitatea de șanse.

Pe de altă parte, implementarea acestor soluții este încetinită de provocări precum lipsa interoperabilității, reticența utilizatorilor și cadrul juridic insuficient. Costurile ridicate și disparitățile regionale accentuează decalajele în accesul la servicii moderne, iar lipsa unei strategii coerente de colaborare între instituții împiedică progresul necesar.

Concluzionând, pentru a valorifica pe deplin potențialul soluțiilor de e-Sănătate, este esențial să se investească în educația digitală, în infrastructură și în crearea unui cadru legislativ clar și unitar. Doar prin depășirea acestor obstacole și printr-o strategie bine coordonată, România poate transforma aceste provocări în oportunități reale pentru îmbunătățirea sistemului medical și creșterea calității vieții cetățenilor săi.

2.2. Obiectiv general si obiective specifice

În continuare, sunt prezentate obiectivul general al proiectului și obiectivele specifice care stau la baza implementării soluțiilor de e-Sănătate. Acestea subliniază pașii esențiali pentru atingerea scopului propus și contribuția lor la modernizarea sistemului medical.

OBIECTIVUL DE POLITICĂ 1:

- Europă mai inteligentă, prin inovare, digitalizare, transformare economică și sprijinirea întreprinderilor mici și mijlocii

OBIECTIV SPECIFIC: RSO1.2.

- Valorificarea avantajelor digitalizării, în beneficiul cetățenilor, al companiilor, al organizațiilor de cercetare și al autorităților publice

2.3. Schimbarea pe care lucrarea dorește să o aducă

Lucrarea propune dezvoltarea și implementarea unui sistem național integrat de sănătate digitală, PIAS/e-Sănătate, care vizează îmbunătățirea eficienței, accesibilității și calității serviciilor medicale. Prin automatizarea proceselor administrative, gestionarea dosarelor electronice și integrarea informațiilor între furnizorii de servicii de sănătate, acest sistem poate transforma modul în care sunt furnizate îngrijirile medicale, reducând birocrația, crescând transparența și facilitând coordonarea între profesioniștii din domeniu. În plus, se va asigura protecția datelor pacienților prin implementarea unor măsuri de securitate avansate.

Dezvoltare software PIAS/e-Sănătate cu anvergură națională. Exemple de servicii noi care ar putea fi furnizate urmare a sprijinului acordat:

- sistem de programări și de trimiteri;
- automatizarea fluxurilor aferente certificatelor de concediu medical, a biletelor de trimitere, a scrisorilor medicale, a recomandărilor privind îngrijirile la domiciliu, a dispozitivelor medicale;
- trasee pentru pacienții cu boli cronice / boli rare;
- soluții de management clinic pentru pacientul critic; ATI;
- transplant;
- sistem de urmărire a rezultatelor probelor de laborator;
- dezvoltarea de baze de date pentru diagnostic sau de sisteme care implică înregistrarea nominală;
- sisteme de securitate pentru acces la distanță;
- sisteme de stocare electronică a rezultatelor medicale și a datelor pacienților;
- serviciu / portal reglementări, proceduri și instrumente / facilități pentru schimbul de informații între furnizorii de servicii medicale de diferite niveluri și alte servicii publice, inclusiv servicii comunitare;
- transmiterea datelor către unități sanitare specializate pentru managementul pacienților în cadrul rețelelor clinice;
- sisteme de audit clinic;
- sisteme de conectare la rețele europene;
- tele-monitorizarea pentru managementul bolilor cronice și post acut.

Despre software-ul în sine:

- Eficiență îmbunătățită: PIAS poate simplifica procesele administrative și de gestionare a dosarelor medicale, contribuind astfel la o eficiență crescută în furnizarea serviciilor de sănătate. Prin digitalizarea informațiilor, se poate reduce birocrația și timpul petrecut cu

documentarea, permitând personalului medical să se concentreze mai mult asupra îngrijirii pacienților;

- Accesibilitate îmbunătățită: un sistem integrat poate facilita accesul la informații medicale critice și istoricul pacienților, inclusiv pentru medici și pacienți. Acest lucru poate îmbunătăți coordonarea îngrijirii și ajuta la evitarea repetării investigațiilor și tratamentelor;
- Redundanța redusă: cu PIAS/e-Sănătate, se pot evita teste inutile și proceduri medicale care au fost deja efectuate în altă parte, deoarece informațiile pot fi partajate între furnizorii de servicii de sănătate. Acest lucru poate economisi resurse și reduce costurile pentru sistemul de sănătate;
- Monitorizare mai bună: PIAS/e-Sănătate poate oferi instrumente de monitorizare și analiză a datelor care ajută la identificarea tendințelor și a problemelor de sănătate la nivel de populație. Acest lucru poate ajuta la dezvoltarea și implementarea politicilor de sănătate mai eficiente;
- Securitatea datelor: implementarea unui PIAS/e-Sănătate poate include măsuri de securitate puternice pentru protejarea datelor medicale sensibile. Astfel, se poate preveni accesul neautorizat la informațiile pacienților și se pot respecta regulamentele privind confidențialitatea datelor;
- Creșterea calității îngrijirii medicale: un sistem integrat poate ajuta la asigurarea faptului că pacienții primesc îngrijirea corectă și la timp. Prin furnizarea mai rapidă a informațiilor relevante și prin creșterea coordonării între diferiți furnizori de servicii de sănătate, calitatea îngrijirii medicale poate crește semnificativ;
- Transparență: PIAS/e-Sănătate poate crește transparența în ceea ce privește costurile, procedurile și performanța serviciilor de sănătate, ceea ce poate ajuta la implicarea mai activă a pacienților în deciziile legate de sănătate și la monitorizarea eficienței sistemului de sănătate;

Desigur, implementarea cu succes a unui astfel de sistem necesită o planificare atentă, resurse adecvate și aderarea tuturor părților implicate. În plus, trebuie să fie luate în considerare aspecte legate de confidențialitatea datelor și securitatea cibernetică pentru a proteja informațiile sensibile ale pacienților.

În concluzie, dezvoltarea și implementarea sistemului PIAS/e-Sănătate reprezintă un pas esențial în modernizarea infrastructurii de sănătate din România, având potențialul de a îmbunătăți semnificativ eficiența, accesibilitatea și calitatea serviciilor medicale. Prin integrarea proceselor administrative și a datelor pacienților, sistemul va reduce birocrația, va facilita coordonarea între furnizorii de servicii de sănătate și va spori transparența și securitatea informațiilor. De asemenea, se va contribui la optimizarea resurselor, reducerea costurilor și îmbunătățirea monitorizării sănătății la nivel național. Totodată, succesul implementării acestui sistem depinde de o planificare riguroasă, resurse adecvate și o colaborare eficientă între toate părțile implicate, pentru a asigura protecția datelor sensibile și respectarea reglementărilor de confidențialitate.

2.4. Cum propune proiectul să realizeze schimbarea

Un proiect de implementare a e-Sănătate/PIAS propune o serie de strategii și acțiuni pentru a realiza schimbarea anticipată în sistemul de sănătate. Aceste strategii variază în funcție de obiectivele proiectului și de contextul specific, dar pot include următoarele elemente:

- Planificare și analiză: proiectul începe cu o evaluare aprofundată a sistemului de sănătate existent pentru a identifica nevoile, deficiențele și oportunitățile de îmbunătățire. Această analiză poate include implicarea părților interesate, cum ar fi medici, personal medical, pacienți și factori de decizie;
- Definirea obiectivelor și a priorităților: proiectul stabilește obiective clare pentru implementarea PIAS, precum îmbunătățirea accesului la informații medicale, reducerea

redundanței în furnizarea de servicii, creșterea eficienței sau îmbunătățirea coordonării îngrijirii. Prioritățile sunt stabilite în funcție de nevoile identificate;

- Design și dezvoltare: proiectul implică dezvoltarea și configurarea platformei PIAS pentru a se potrivi cu cerințele specifice ale sistemului de sănătate. Aceasta poate include dezvoltarea unor aplicații sau software personalizat pentru colectarea și gestionarea datelor medicale, precum și pentru a facilita comunicarea între diferiții furnizori de servicii;
- Instruire și educație: proiectul prevede instruirea personalului medical și administrativ cu privire la utilizarea PIAS/e-Sănătate și a noilor procese și proceduri. Aceasta asigură o tranziție mai lină la noul sistem și maximizează eficiența sa;
- Testare și optimizare: implementarea PIAS/e-Sănătate este supusă unor etape de testare pentru a se asigura că funcționează corespunzător și îndeplinește obiectivele stabilite. Orice deficiențe sau probleme sunt identificate și rezolvate în această fază;
- Partajarea informațiilor și colaborarea: Proiectul încurajează colaborarea și partajarea de informații între furnizorii de servicii de sănătate, asigurând astfel o coordonare mai bună a îngrijirii medicale. Acest lucru poate implica standardizarea dosarelor medicale electronice și a protocoalelor de comunicare;
- Monitorizare și evaluare continuă: proiectul stabilește mecanisme de monitorizare și evaluare pentru a urmări impactul implementării PIAS asupra sistemului de sănătate. Acest lucru permite ajustarea continuă și optimizarea sistemului pe măsură ce se dezvoltă;
- Angajarea părților interesate: proiectul implică și implică activ părțile interesate, cum ar fi pacienții, medicii, asociațiile profesionale și factorii de decizie, pentru a asigura acceptarea și susținerea continuă a sistemului;
- Securitate și confidențialitate: un aspect crucial al proiectului este asigurarea securității datelor și respectarea reglementărilor privind confidențialitatea datelor medicale, precum Regulamentul General de Protecție a Datelor (GDPR) în Europa;
- Educație a pacienților: pacienții trebuie să fie informați cu privire la modul în care noul sistem le va afecta și cum își pot gestiona propriile date medicale în cadrul PIAS/e-Sănătate.

Scopul final este îmbunătățirea calității îngrijirii medicale și creșterea eficienței sistemului de sănătate. Proiectul de implementare a PIAS urmărește o transformare digitală cuprinzătoare, bazată pe strategii clare, precum planificarea și analiza sistemului existent, stabilirea obiectivelor și priorităților, dezvoltarea unei platforme adaptate, instruirea personalului și implicarea activă a părților interesate.

Testarea, optimizarea, asigurarea confidențialității datelor și educarea pacienților sunt componente critice ale procesului, asigurând o tranziție lină și sustenabilă. Proiectul promovează colaborarea între furnizorii de servicii și standardizarea dosarelor medicale, urmărind îmbunătățirea coordonării îngrijirii. Prin monitorizare și evaluare continuă, sistemul poate fi ajustat în funcție de nevoile emergente, contribuind la modernizarea și eficientizarea infrastructurii medicale. Astfel, PIAS reprezintă o soluție esențială pentru un sistem de sănătate mai eficient, centrat pe pacient și adaptabil la cerințele viitorului.

2.5. Grupurile țintă vizate

Grupurile țintă vizate sunt diverse și includ actori esențiali ai sistemului de sănătate. Acestea variază de la pacienți și personal medical, până la instituții și factori de decizie, fiecare având un rol specific în adoptarea și funcționarea acestui sistem. Identificarea și implicarea acestor grupuri sunt cruciale pentru succesul proiectului, deoarece fiecare contribuie la crearea unui ecosistem integrat și eficient.

Categoriile vizate sunt detaliate mai jos:

- *Pacienții*: Pacienții sunt beneficiarii finali ai e-Sănătate/PIAS. Aceștia au dreptul să acceseze rapid și în condiții de siguranță datele și informațiile medicale despre ei înșiși, să monitorizeze starea lor de sănătate și să fie implicați în deciziile privind îngrijirea medicală;
- *Personalul medical:* Medicii, asistentele, farmaciștii și alți profesioniști din domeniul sănătății au nevoie de acces rapid la datele pacienților pentru a furniza îngrijire medicală de calitate e-Sănătate/PIAS poate simplifica schimbul de informații între diferite specialități medicale și instituții de sănătate;
- *Instituții medicale*: Spitalele, clinicile, laboratoarele și alte instituții medicale sunt părți interesate majore în implementarea e-Sănătate/PIAS. Ele trebuie să fie capabile să integreze sistemul în infrastructura și procesele lor existente;
- *Autorități și factori de decizie:* Factorii de decizie din cadrul sistemului de sănătate, precum ministerele sănătății, organizațiile de asigurare medicală și organisme de reglementare, sunt responsabili pentru definirea politicilor și reglementărilor care guvernează e-Sănătate/PIAS.
- *Asociații profesionale și sindicale:* Asociațiile medicale, sindicatele și alte organizații care reprezintă interesele personalului medical pot fi implicate în procesul de implementare și pot juca un rol în susținerea sau ajustarea proiectului;
- *Terțe părți și furnizori de tehnologie:* Companiile de tehnologie, furnizorii de servicii IT și alte entități terțe care dezvoltă și furnizează software și soluții tehnologice pentru e-Sănătate/PIAS sunt parte integrantă a procesului de implementare;
- *Publicul larg*: Populația în general poate fi informată și educată cu privire la beneficiile e-Sănătate/PIAS, iar opinia publică poate avea un impact asupra implementării și finanțării proiectului;
- *Instituții de învățământ și cercetare:* Universitățile, instituțiile de învățământ medical și organizațiile de cercetare pot avea un interes în colaborarea cu e-Sănătate/PIAS pentru cercetare și dezvoltare;
- *Sectorul privat:* Companiile și organizațiile din sectorul privat care furnizează servicii și produse medicale, precum și cele implicate în dezvoltarea de tehnologii și soluții IT, pot beneficia de implementarea e-Sănătate/PIAS și pot avea un rol în proces;
- *Organizații Non-Guvernamentale (ONG-uri):* Organizațiile non-guvernamentale din domeniul sănătății pot juca un rol în susținerea e-Sănătate/PIAS și în furnizarea de servicii medicale în comunități.

În concluzie, succesul implementării sistemului e-Sănătate/PIAS depinde în mare măsură de implicarea activă și colaborarea tuturor grupurilor țintă identificate. De la pacienți și personal medical, până la autorități, instituții de învățământ și sectorul privat, fiecare actor joacă un rol esențial în crearea unui ecosistem eficient și integrat. Este crucial ca proiectul să răspundă nevoilor și preocupărilor fiecărei părți implicate, să promoveze transparența, să asigure o comunicare constantă și să construiască un cadru de încredere. Doar printr-o abordare colaborativă și inclusivă se poate garanta succesul pe termen lung al e-Sănătate/PIAS și impactul pozitiv asupra întregului sistem de sănătate.

2.6. Identificarea problemelor la nivelul grupului țintă

Identificarea problemelor la nivelul grupurilor țintă este un pas crucial în procesul de implementare a unui e-Sănătate/PIAS. Aceasta ne ajută să înțelegem nevoile și preocupările acestor grupuri, să adaptați strategiile de implementare și să vă asigurați că proiectul abordează cu succes aceste probleme.

Iată câteva exemple de probleme potențiale la nivelul grupurilor țintă:

1. Pacienți:

- Acces dificil la datele lor medicale;
- Temeri legate de confidențialitatea datelor personale de sănătate;
- Dificultăți în utilizarea sistemului din cauza lipsei de competențe tehnologice.

2. Personalul Medical:
- Rezistență la schimbare și adaptare la noile tehnologii;
- Suprasolicitare datorită unei noi sarcini de lucru sau a nevoii de formare;
- Îngrijorări legate de securitatea datelor și confidențialitatea pacienților.

3. Instituții Medicale:
- Compatibilitatea cu sistemele și infrastructura existente poate crea dificultăți tehnice;
- Riscul de erori sau probleme tehnice care pot afecta furnizarea de servicii medicale.

4. Autorități și factori de decizie:
- Gestionarea bugetului și asigurarea finanțării continue a proiectului;
- Reglementările și politicile guvernamentale pot necesita ajustări pentru a se potrivi cu e-Sănătate/PIAS.

5. Asociații Profesionale și Sindicale:
- Asigurarea că interesele și standardele profesionale sunt respectate;
- Implicarea personalului medical în deciziile legate de proiect.

6. Publicul larg:
- Informarea și educația publicului cu privire la beneficiile și utilizarea e-Sănătate/PIAS.

7. Sectorul Privat:
- Rolul și implicațiile pentru companiile din sectorul privat care furnizează servicii medicale sau tehnologie.
- Colaborarea cu sectorul privat în implementarea și dezvoltarea e-Sănătate/PIAS.

8. ONG-uri:
- Potențialul impact asupra organizațiilor non-guvernamentale care furnizează servicii medicale și sprijin comunităților.

9. Instituții de învățământ și cercetare:
- Implicarea acestor instituții în dezvoltarea, testarea și evaluarea e-Sănătate/PIAS.

Pentru a identifica aceste probleme, se pot desfășura discuții cu reprezentanți ai fiecărui grup țintă, se pot organiza întâlniri de consultare și se pot efectua sondaje sau cercetări de piață pentru a colecta feedback și opinii. După identificarea acestor probleme, se pot dezvolta planuri și soluții pentru a aborda aceste preocupări și pentru a asigura succesul proiectului. Este important să existe o comunicare deschisă și colaborare între toate părțile implicate pentru a depăși aceste obstacole și a implementa cu succes PIAS.

2.7. Echipa de proiect

Echipa de proiect implicată în reconstrucția sau implementarea e-Sănătate/PIAS ar trebui să fie compusă dintr-o varietate de specialiști și experți care pot asigura o abordare coordonată și eficientă a procesului. Această echipă ar putea include următoarele roluri:
- *Manager de Proiect:* Responsabil de planificarea generală a proiectului, supravegherea implementării, stabilirea bugetului și termenelor, gestionarea riscurilor și raportarea către factorii de decizie;

- *Arhitect de Sistem:* Specializat în proiectarea și dezvoltarea infrastructurii și a software-ului necesar pentru e-Sănătate/PIAS, astfel încât să se potrivească nevoilor sistemului de sănătate;
- *Expert în protecția datelor:* Asigură respectarea reglementărilor privind securitatea și confidențialitatea datelor medicale, cum ar fi GDPR, și implementează măsuri de securitate adecvate pentru protejarea informațiilor pacienților;
- *Specialist în resurse umane:* Ajută la gestionarea personalului, inclusiv recrutarea, instruirea și gestionarea schimbărilor în rândul angajaților;
- *Consultant medical:* Oferă expertiză medicală pentru a asigura că e-Sănătate/PIAS îndeplinește cerințele clinice și se aliniază cu cele mai bune practici medicale;
- *Analist de date:* Responsabil de analiza datelor pentru a identifica tendințe și modele care pot contribui la îmbunătățirea serviciilor de sănătate;
- *Specialist în comunicare:* Gestionarea comunicării interne și externe, inclusiv informarea și angajarea părților interesate, cum ar fi personalul medical, pacienții și publicul larg;
- *Jurist:* Asigură că toate aspectele legale ale proiectului sunt acoperite și că contractele cu terții sunt în regulă;
- *Specialist în finanțe:* Monitorizează bugetul și cheltuielile proiectului, asigurându-se că resursele sunt gestionate eficient;
- *Manager de calitate:* Monitorizează calitatea și conformitatea cu standardele, asigurându-se că e-Sănătate/PIAS îndeplinește obiectivele stabilite;
- *Pacient/Persoană care reprezintă pacienții:* Este important să fie inclusă o voce care să reprezinte interesele și perspectivele pacienților în proiect, pentru a asigura că e-Sănătate/PIAS îndeplinește nevoile și așteptările acestora;
- *Asociere cu furnizori de servicii de sănătate:* Colaborarea cu furnizorii de servicii de sănătate, cum ar fi spitalele, clinicile și laboratoarele medicale, este crucială pentru a asigura integrarea eficientă a e-Sănătate/PIAS în întregul sistem;
- *Specialist în Training și Educație:* Responsabil de dezvoltarea și implementarea programelor de instruire pentru personalul medical și administrativ, precum și pentru pacienți, pentru a se asigura că toți utilizatorii pot utiliza eficient e-Sănătate/PIAS;
- *Echipă tehnică și dezvoltatori software:* Programatori și ingineri de software specializați în dezvoltarea și întreținerea aplicațiilor și platformelor tehnologice necesare e-Sănătate/PIAS;
- *Echipa de testare:* Testeri care verifică funcționalitatea corectă a e-Sănătate/PIAS și identifică eventuale probleme sau erori.

Această echipă ar trebui să lucreze împreună sub coordonarea unui manager de proiect pentru a implementa cu succes e-Sănătate/PIAS și pentru a aduce îmbunătățiri semnificative în sistemul de sănătate existent. Este important ca toate părțile implicate să fie bine coordonate și să aibă un scop comun de a îmbunătăți calitatea îngrijirii medicale și eficiența sistemului de sănătate.

În concluzie, succesul implementării e-Sănătate/PIAS depinde de o echipă diversificată și bine pregătită, care să colaboreze eficient pentru atingerea obiectivelor proiectului. Fiecare specialist aduce o contribuție esențială, iar o comunicare constantă, sprijin reciproc și o viziune comună sunt elemente-cheie pentru realizarea unui sistem integrat, sigur și eficient, care să răspundă nevoilor întregului ecosistem de sănătate.

2.8. Activitățile din cadrul proiectului

Implementarea unei Platforme Informatice a Asigurărilor de Sănătate (PIAS)/e-Sănătate implică o serie de activități complexe care trebuie să fie coordonate cu atenție pentru a asigura succesul proiectului. Aceste activități variază în funcție de scopul și dimensiunea proiectului, dar iată câteva activități cheie care pot fi desfășurate în cadrul proiectului de implementare a PIAS.

1. Planificarea proiectului:

- Definirea obiectivelor și a scopului proiectului;
- Stabilirea bugetului și a resurselor necesare;
- Crearea unui calendar al etapelor și termenelor de implementare.

2. Analiză și evaluare:

- Evaluarea situației actuale a sistemului de sănătate;
- Identificarea nevoilor și problemelor existente;
- Consultarea părților interesate pentru a colecta feedback și sugestii.

3. Selectarea și configurarea tehnologiei:

- Alegerea platformei și a software-ului adecvat pentru e-Sănătate/PIAS;
- Configurarea și personalizarea software-ului pentru a se potrivi cu cerințele sistemului de sănătate.

4. Instruire și educație:

- Dezvoltarea programelor de instruire pentru personalul medical, administrativ și pentru pacienți;
- Furnizarea de instruire și suport tehnic pentru utilizatorii e-Sănătate/PIAS.

5. Testarea și optimizarea:

- Testarea sistemului pentru a identifica erori și probleme tehnice;
- Remedierea problemelor și optimizarea funcționalităților e-Sănătate/PIAS.

6. Implementarea și lansarea inițială:

- Implementarea efectivă a e-Sănătate/PIAS în instituțiile medicale;
- Lansarea inițială și pregătirea pentru utilizarea operativă.

7. Monitorizarea și evaluarea continuă:

- Monitorizarea performanței e-Sănătate/PIAS și a utilizării acestuia;
- Colectarea de date pentru evaluarea impactului proiectului.

8. Securitate și protecția datelor:

- Implementarea măsurilor de securitate pentru protejarea datelor medicale sensibile;
- Asigurarea conformității cu reglementările privind protecția datelor.

9. Comunicare și implicare a părților interesate:

- Dezvoltarea unui plan de comunicare pentru a informa și angaja părțile interesate;
- Organizarea de întâlniri, seminarii și consultări cu părțile interesate.

10. Gestionarea schimbării:

- Abordarea rezistenței la schimbare și promovarea adoptării e-Sănătate/PIAS;
- Monitorizarea și gestionarea problemelor și preocupărilor privind schimbarea.

11. Supravegherea bugetului și a resurselor:

- Gestionarea bugetului proiectului și urmărirea cheltuielilor;
- Asigurarea utilizării eficiente a resurselor.

12. Educație a pacienților:

- Dezvoltarea materialelor educaționale pentru pacienți;
- Informarea pacienților cu privire la modul de utilizare a e-Sănătate/PIAS și a beneficiilor acestuia.

13. Colaborarea cu furnizorii de servicii de sănătate:

- Implicarea furnizorilor de servicii medicale în procesul de implementare;
- Asigurarea compatibilității și interconectivității cu diferitele instituții de sănătate.

14. Asigurarea calității și conformității:

- Dezvoltarea și implementarea standardelor și procedurilor de asigurare a calității;
- Asigurarea conformității cu regulamentele și cerințele legale.

15. Evaluarea impactului și raportare:

- Evaluarea impactului proiectului asupra calității îngrijirii medicale și a eficienței sistemului de sănătate;
- Raportarea rezultatelor și recomandărilor factorilor de decizie.

Aceste activități sunt doar o parte din procesul de implementare a e-Sănătate/PIAS și pot fi adaptate la nevoile specifice ale proiectului.

2.9. Tipuri de resurse pentru implementarea proiectului

Implementarea unui proiect de e-Sănătate/PIAS necesită o varietate de resurse pentru a fi realizată cu succes. Aceste resurse pot fi grupate în mai multe categorii, după cum sunt descrise mai jos.

1. Resurse financiare PNRR/FEDR:

- Buget pentru dezvoltarea și implementarea e-Sănătate/PIAS;
- Fonduri pentru achiziționarea de hardware și software;
- Finanțare pentru instruirea personalului și pentru gestionarea proiectului.

2. Resurse tehnice:

- Echipamente hardware, cum ar fi servere, stații de lucru, terminale și dispozitive mobile;
- Software și licențe necesare pentru funcționarea e-Sănătate/PIAS;
- Echipamente de comunicații și infrastructură IT.

3. Resurse umane:

- Personal specializat, inclusiv programatori, dezvoltatori software, ingineri de rețea și experți în securitatea datelor;
- Personal medical și administrativ pentru utilizarea e-Sănătate/PIAS;
- Manager de proiect și echipă de proiect pentru planificare și gestionarea implementării.

4. Resurse pentru formare și educație:

- Programe de instruire pentru personalul medical și administrativ în utilizarea e-Sănătate/PIAS;
- Mijloace pentru dezvoltarea materialelor educaționale pentru pacienți.

5. Resurse pentru comunicare și implicarea părților interesate:

- Resurse pentru comunicarea și implicarea părților interesate, cum ar fi organizarea de întâlniri, seminarii și campanii de informare;
- Realizarea de materiale de comunicare și promovare.

6. Resurse pentru testare și calitate:

- Echipament și software de testare pentru a evalua funcționalitățile e-Sănătate/PIAS și pentru a identifica eventualele probleme;
- Resurse pentru asigurarea calității și conformității cu standardele.

7. Resurse pentru securitate și protecția datelor:

- Resurse pentru implementarea măsurilor de securitate, inclusiv sisteme de protecție a datelor, criptare și autentificare;
- Consultanți în securitatea cibernetică și conformitate cu reglementările privind protecția datelor.

8. Resurse pentru gestionarea schimbării:

- Echipă dedicată pentru gestionarea schimbării și pentru abordarea rezistenței la schimbare;
- Resurse pentru formare suplimentară și sprijin pentru personalul care trebuie să se adapteze la e-Sănătate/PIAS.

9. Resurse pentru monitorizare și evaluare:

- Sisteme de monitorizare a performanței e-Sănătate/PIAS;
- Resurse pentru colectarea și analiza datelor pentru evaluarea impactului proiectului.

10. Resurse juridice și de conformitate:

- Consultanți juridici pentru a asigura respectarea reglementărilor legale și a reglementărilor privind protecția datelor;
- Resurse pentru dezvoltarea și actualizarea politicilor și procedurilor de conformitate;

11. Resurse pentru educație a pacienților:

- Resurse pentru dezvoltarea de materiale educaționale pentru pacienți, cum ar fi broșuri și materiale online;
- Sisteme de comunicare și platforme pentru informarea pacienților.

Aceste resurse sunt esențiale pentru planificarea și implementarea unui proiect e-Sănătate/PIAS și asigurarea că acesta funcționează eficient și aduce beneficii semnificative în sistemul de sănătate.

2.10. Activități previzionate

Implementarea unui e-Sănătate/PIAS implică o serie de activități planificate și bine structurate pentru a asigura o implementare eficientă și de succes.

Iată câteva dintre activitățile previzionate care pot fi desfășurate în acest sens:

1. Planificare și definirea obiectivelor:

- Identificarea obiectivelor clare ale proiectului e-Sănătate/PIAS;
- Dezvoltarea unui plan de implementare detaliat care să includă obiectivele, termenele și bugetul.

2. Analiza și evaluarea inițială:

- Evaluarea situației actuale a sistemului de sănătate pentru a identifica nevoile și problemele existente;
- Consultarea părților interesate pentru a colecta feedback și sugestii.

3. Selecția tehnologiei și dezvoltarea software-ului:

- Alegerea platformei tehnologice potrivite și a software-ului necesar;
- Dezvoltarea și configurarea software-ului pentru a se potrivi cu cerințele și nevoile sistemului de sănătate.

4. Instruire și educație:

- Dezvoltarea programelor de instruire pentru personalul medical și administrativ, precum și pentru pacienți;
- Furnizarea de instruire și suport tehnic pentru utilizatorii e-Sănătate/PIAS.

5. Testarea și optimizarea:

- Testarea extensivă a e-Sănătate/PIAS pentru a identifica erori și probleme tehnice;
- Remedierea problemelor și optimizarea funcționalităților.

6. Implementarea și lansarea inițială:

- Implementarea efectivă a e-Sănătate/PIAS în instituțiile medicale și în sistemul de sănătate;
- Lansarea inițială și pregătirea pentru utilizarea operativă.

7. Monitorizarea și evaluarea continuă:

- Monitorizarea performanței e-Sănătate/PIAS și a utilizării acestuia;
- Colectarea de date pentru evaluarea impactului proiectului.

8. Securitate și protecția datelor:

- Implementarea măsurilor de securitate pentru a proteja datele medicale sensibile;
- Asigurarea conformității cu reglementările privind protecția datelor.

9. Comunicare și implicarea părților interesate:

- Dezvoltarea și implementarea unui plan de comunicare pentru a informa și angaja părțile interesate;
- Organizarea de întâlniri, seminarii și campanii de informare.

10. Gestionarea schimbării:

- Abordarea rezistenței la schimbare și promovarea adoptării e-Sănătate/PIAS;
- Monitorizarea și gestionarea problemelor și preocupărilor privind schimbarea.

11. Supravegherea bugetului și a resurselor:

- Gestionarea bugetului proiectului și urmărirea cheltuielilor;
- Asigurarea utilizării eficiente a resurselor.

12. Educație a pacienților:

- Dezvoltarea materialelor educaționale pentru pacienți;
- Informarea pacienților cu privire la modul de utilizare a e-Sănătate/PIAS și a beneficiilor acestuia.

13. Colaborarea cu furnizorii de servicii de sănătate:

- Implicarea furnizorilor de servicii medicale în procesul de implementare;
- Asigurarea compatibilității și interconectivității cu diferitele instituții de sănătate.

14. Asigurarea calității și conformității:

- Dezvoltarea și implementarea standardelor și procedurilor de asigurare a calității;
- Asigurarea conformității cu regulamentele și cerințele legale.

15. Evaluarea impactului și raportare:

- Evaluarea impactului proiectului asupra calității îngrijirii medicale și a eficienței sistemului de sănătate;
- Raportarea rezultatelor și recomandărilor factorilor de decizie.

Aceste activități sunt esențiale pentru asigurarea că e-Sănătate/PIAS este implementat eficient, cu succes și că aduce îmbunătățiri semnificative în sistemul de sănătate.

2.11. Rezultate așteptate

Implementarea unui sistem e-Sănătate/PIAS are ca obiectiv aducerea unor rezultate pozitive și îmbunătățiri semnificative în sistemul de sănătate. Rezultatele așteptate pot varia în funcție de obiectivele specifice ale proiectului și de nevoile sistemului de sănătate.

O parte din potențialele rezultate așteptate sunt descrise mai jos:

- Acces îmbunătățit la informații medicale: Pacienții și personalul medical ar trebui să aibă acces mai rapid și mai ușor la informațiile medicale, inclusiv istoricul pacientului, rezultatele testelor, diagnozele și tratamentele anterioare;
- Coordonare mai bună a îngrijirii medicale: e-Sănătate/PIAS va trebui să faciliteze schimbul de informații între diferiți furnizori de servicii de sănătate, permițând o coordonare mai bună a îngrijirii medicale și evitarea duplicării inutile a testelor și procedurilor;
- Reducerea erorilor medicale: Prin consolidarea datelor medicale și accesul la istoricul complet al pacientului, e-Sănătate/PIAS va contribui la reducerea erorilor medicale;
- Eficiență sporită: e-Sănătate/PIAS va contribui la eficientizarea proceselor administrative și medicale, reducând timpul și costurile asociate cu administrarea sistemului de sănătate;
- Îmbunătățirea managementului stocurilor și a medicamentelor: Un e-Sănătate/PIAS bine configurat poate ajuta la gestionarea eficientă a stocurilor de medicamente și echipamente medicale, asigurând disponibilitatea acestora în mod adecvat;
- Promovarea sănătății publice: e-Sănătate/PIAS va furniza date și informații necesare pentru monitorizarea și gestionarea problemelor de sănătate publică, cum ar fi epidemiile și campaniile de vaccinare;
- Creșterea transparenței și a responsabilității: e-Sănătate/PIAS va contribui la o mai mare transparență în sistemul de sănătate, permițând pacienților să-și urmărească propria îngrijire și responsabilizând furnizorii de servicii de sănătate;
- Reducerea costurilor: O administrare mai eficientă a sistemului de sănătate și reducerea erorilor pot contribui la reducerea costurilor pentru pacienți, guverne și asiguratori de sănătate;
- Îmbunătățirea satisfacției pacienților: Prin facilitarea accesului la informații și îmbunătățirea coordonării îngrijirii medicale, e-Sănătate/PIAS poate contribui la creșterea satisfacției pacienților;
- Facilitarea cercetării și dezvoltării în domeniul sănătății: e-Sănătate/PIAS poate furniza date esențiale pentru cercetare și dezvoltare în domeniul sănătății, contribuind la avansarea cunoștințelor medicale.

Acestea sunt câteva exemple de rezultate așteptate, dar pot exista și altele, în funcție de specificul proiectului și de nevoile sistemului de sănătate. Este important să se stabilească obiective clare și măsurabile pentru proiectul PIAS și să se monitorizeze progresul în atingerea acestor obiective pentru a evalua impactul și succesul proiectului.

Capitolul 3. Implementarea Directivei NIS 2 în România

3.1 Introducere

Directiva NIS 2 transpusă în legislația din România prin Ordonanță de Urgență Nr. 155/2024 din 30 decembrie 2024 reprezintă un pilon fundamental în consolidarea securității cibernetice la

nivelul Uniunii Europene. Aceasta stabilește cerințe minime și un cadru comun pentru protejarea rețelelor și sistemelor informatice, fiind aplicabilă operatorilor de servicii esențiale și furnizorilor de servicii digitale. În acest context, România, ca stat membru al Uniunii Europene, a transpus și implementat prevederile directivei, adaptând cadrul legislativ și instituțional național.

În cadrul acestui capitol analizează procesul de implementare a Directivei NIS 2 în România, evidențiind principalele schimbări legislative, cadrul instituțional dezvoltat, precum și provocările potențiale asociate implementării acestei directive.

3.2. Cadrul legislativ național principal și subsecvent

Implementarea Directivei (UE) 2022/2555 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (Directiva NIS 2, Ordonanţă de Urgenţă Nr. 155/2024 din 30 decembrie 2024) a presupus adoptarea unui cadru legislativ solid, menit să asigure o aplicare eficientă a cerințelor acesteia în România.

Acest cadru legislativ are la bază acte normative de referință care reglementează identificarea și gestionarea riscurilor cibernetice, stabilirea responsabilităților pentru operatorii de servicii esențiale și furnizorii de servicii digitale, precum și mecanismele de cooperare națională și europeană.

Legea nr. 362/2018 reprezintă piatra de temelie a legislației naționale în domeniu, reglementând cerințele generale și definind responsabilitățile autorităților competente și ale entităților afectate. În completare, au fost emise mai multe acte normative subsecvente, menite să detalieze aspectele tehnice și operaționale ale implementării Directivei NIS 2. Printre acestea, se numără norme tehnice, metodologii și hotărâri guvernamentale care stabilesc cerințele minime de securitate, valorile de prag pentru determinarea efectului perturbator semnificativ al incidentelor și organizarea Registrului operatorilor de servicii esențiale.

Principalele acte normative care constituie cadrul legislativ național sunt următoarele:

- Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune;
- Legea nr. 362/2018, care reglementează asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice;
- Ordinul nr. 1.323/2020, care aprobă Normele tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale;
- Hotărârea nr. 976/2020, care stabilește valorile de prag pentru determinarea efectului perturbator semnificativ al incidentelor în rețelele și sistemele informatice ale operatorilor de servicii esențiale;
- Hotărârea nr. 963/2020, care aprobă Lista serviciilor esențiale;
- Ordinul nr. 599/2019, care aprobă Normele metodologice pentru identificarea operatorilor de servicii esențiale și furnizorilor de servicii digitale;
- Ordinul nr. 600/2019, care reglementează organizarea și funcționarea Registrului operatorilor de servicii esențiale;
- Ordinul nr. 601/2019, care stabilește Metodologia de evaluare a efectului perturbator semnificativ al incidentelor în rețelele și sistemele informatice.
- Ordonanţă de Urgenţă Nr. 155/2024 din 30 decembrie 2024 privind instituirea unui cadru pentru securitatea cibernetică a reţelelor şi sistemelor informatice din spaţiul cibernetic naţional.

Aceste acte legislative oferă un cadru clar și structurat pentru implementarea măsurilor de securitate cibernetică, sprijinind astfel consolidarea unui spațiu digital rezilient și sigur, atât la nivel național, cât și european.

3.3. Operatorii de servicii esențiale OSE/Entităţi esenţiale

Operatorii de servicii esențiale sunt entități publice esenţiale sau private esenţiale care furnizează servicii cruciale pentru menținerea funcționării normale a societății și economiei. Aceste servicii sunt vitale pentru bunăstarea cetățenilor, pentru siguranța națională și pentru stabilitatea economică. În Uniunea Europeană, termenul este reglementat prin Directiva (UE) 2022/2555 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, cunoscută și sub denumirea de Directiva NIS 2 (Network and Information Systems Directive).

Categorii principale de operatori de servicii esențiale;

- Energie;
- Transporturi;
- Bănci și piețe financiare;
- Aprovizionare cu apă potabilă și distribuție;
- Infrastructuri digitale;
- Sectorul sănătății.

În ceea ce privește sectorul sănătății întâlnim următoarele servicii:

- Spitale și Unități Medicale - Spitalele publice și private, clinicile care oferă servicii medicale esențiale, unitățile de primiri urgențe;
- Servicii de Asistență Medicală Primară - cabinetele medicilor de familie, centrele de permanență și policlinicile;
- Laboratoare Medicale - laboratoare de analize medicale care efectuează teste esențiale pentru diagnosticarea și monitorizarea pacienților;
- Servicii de Sănătate Publică - direcțiile de sănătate publică, Institutul Național de Sănătate Publică și alte institute de sănătate publică;
- Servicii de Ambulanță - serviciile de ambulanță publice și private, serviciul de urgență 112 în contextul asistenței medicale;
- Furnizori de Produse și Servicii Medicale - distribuitorii și furnizorii de medicamente esențiale, furnizorii de echipamente medicale critice.

3.4. Cerințe de securitate și rezultate așteptate

În contextul implementării Directivei Europene NIS 2 în sectorul sănătății, cerințele de securitate cibernetică joacă un rol central în asigurarea protecției infrastructurilor critice și a datelor sensibile. Această secțiune analizează cerințele principale ce trebuie îndeplinite pentru a atinge obiectivele de reziliență cibernetică și modernizare a platformelor informatice din sănătate. De asemenea, sunt evidențiate rezultatele așteptate în urma implementării soluțiilor propuse, punând accent pe securitate, eficiență operațională și interoperabilitate.

Acest model a fost dezvoltat și structurat de autor, având ca scop principal oferirea unui ghid comprehensiv și bine organizat pentru alinierea organizațiilor la cerințele esențiale impuse de Directiva NIS 2 și legislația aferentă, precum Legea 362/2018.

Modelul cuprinde un set detaliat de cerințe tehnice și organizatorice, clasificate pe domenii-cheie ale securității cibernetice, cu scopul de a:

- Asigura conformitatea cu standardele și normele naționale și internaționale în domeniul securității IT;
- Îmbunătăți guvernanța și procesele de management al securității informației;
- Proteja infrastructurile critice și rețelele esențiale împotriva amenințărilor cibernetice;

- Dezvolta reziliența organizațională prin procese de detecție, prevenire și răspuns la incidente.

Modelul este organizat în mai multe secțiuni, incluzând domenii precum:
- Guvernanța securității informației;
- Protecția rețelelor și sistemelor informatice;
- Apărarea cibernetică;
- Reziliența în caz de incidente.

Fiecare cerință este însoțită de rezultatele așteptate și documentele suport necesare implementării, ceea ce face din acest model un instrument valoros pentru organizații.

Modelul este destinat operatorilor de servicii esențiale, furnizorilor de servicii digitale și altor entități care au nevoie să implementeze măsuri clare și eficiente de securitate. Prin utilizarea acestuia, organizațiile își pot dezvolta planuri de securitate personalizate, asigurându-se că respectă atât cerințele legale, cât și cele operaționale.

Toate secțiunile și detaliile incluse în acest model reprezintă o creație proprie a autorului, bazată pe cercetări ample, experiență practică și o înțelegere aprofundată a cadrului de reglementare NIS 2. Acest raport reflectă eforturile mele de a contribui la îmbunătățirea standardelor de securitate cibernetică în organizațiile moderne.

Tabelul de mai jos prezintă o sinteză a cerințelor cheie și a impactului anticipat al acestora asupra infrastructurii informatice din sănătate, oferind o perspectivă structurată asupra priorităților de conformitate și a beneficiilor estimate. Acesta a fost realizat de către autor, având ca sursă un curs de specializare pentru responsabili NIS 2, unde au fost abordate cerințele și indicatorii specifici necesari pentru asigurarea conformității în cadrul unui audit de securitate cibernetică. Materialele utilizate în cadrul acestui curs au oferit un cadru detaliat privind standardele și bunele practici aplicabile infrastructurilor critice, contribuind la fundamentarea analizei din prezenta cercetare.

Tabel 2.1. Cerințe de securitate și rezultate așteptate

Nr	Secțiune	Cerințe de securitate	Rezultate așteptate
1		**Analizarea și evaluarea riscurilor** -Analiza riscurilor de securitate -Gestionarea riscurilor de securitate -Evaluarea riscurilor de securitate	-Analiza riscurilor de securitate a rețelelor și sistemelor informatice (ARNIS) -Metodologie de gestionare a riscurilor furnizării serviciilor esențiale (MEGRE) -Registrul de risc organizațional (RERO)
2	**Managementul securității informației**	**Realizarea planurilor de securitate. Politica de securitate:** -Politica de securitate -Implementarea politicii de securitate	-Politica de securitate a rețelelor și sistemelor informatice care asigură furnizarea serviciilor esențiale (PONIS) -Sistemul de management al securității informației (SMSI) -Raport privind implementarea politicii de securitate a rețelelor și sistemelor informatice care asigură furnizarea serviciilor esențiale și a documentelor de aplicare a acesteia (RAIPOD)
3		**Acreditarea de securitate**	-Procesul de acreditare (PEANIS) -Decizia de acreditare (DANIS) -mapa de acreditare de securitate (MANIS)

Nr	Secțiune	Cerințe de securitate	Rezultate așteptate
		-Acreditarea rețelelor și sistemelor informatice -Revizuirea validării acreditării de securitate	
4		**Indicatori de securitate** -Indicatori de securitate -Metode de evaluare a securității	-Indicatori de evaluare (IEC) -Metoda de evaluare a indicatorilor de conformitate (MEIEC)
5		**Verificarea conformității cu privire la securitatea informației. Audit de securitate** -Evaluarea conformității -Auditul de securitate	-Procedură privind evaluarea conformității NIS și efectuarea auditului de securitate a rețelelor și sistemelor informatice (PRECAS) -Raport de evaluare a conformității (RAEC) -Raport de audit de securitate a rețelelor și sistemelor informatice (RASNIS)
6		**Testarea și evaluarea securității rețelelor și sistemelor informatice** -Testare și evaluare securitate	- Document de analiză privind testarea și evaluarea nivelului de securitate al rețelelor și sistemelor informatice (RATES) - Raport tehnic detaliat privind incidentele de compromitere a securității rețelelor și sistemelor informatice (ATECNIS)
7		**Asigurarea securității personalului** -Asigurarea securității personalului -Verificarea înțelegerii responsabilităț	-Program de prezentare a securității pentru tot personalul (PRASP) -Fisa post (FP) -Contract individual de munca (CIM) -Contract colectiv de munca (CCM) -Instructaje de securitate pentru angajați (ISA) -Verificări privind cunoștințele de securitate ale angajaților (VCSA) -Contractele de servicii sau furnizare servicii externe (COSE/ENTITĂŢI ESENŢIALE)
8		**Conștientizarea și instruirea utilizatorilor** -Instrumente de conștientizare -Instruirea și prezentarea securității	-Resurse esențiale pentru informarea și instruirea angajaților cu privire la diversele amenințări cibernetice și metodele adecvate de protecție, având scopul de a reduce riscul incidentelor de securitate informatică - Program de instruire în domeniul securității pentru întregul personal (PRASA) - Program de formare în securitate pentru personalul care utilizează rețelele și sistemele informatice ce sprijină furnizarea serviciilor critice (PRISA)
9		**Gestionarea activelor** -Inventarierea și gestionarea activelor	-Lista activelor, sistemelor și proceselor organizației (LASPO) -Procedură privind etichetarea și clasificarea datelor și informațiilor (PRECDI)
10	**Managementul ecosistemului**	**Cartografierea ecosistemului**	-Situația cartografică a ecosistemului (SICAE)

Nr	Secțiune	Cerințe de securitate	Rezultate așteptate
		-Descrierea ecosistemului	-Lista riscurilor potențiale identificate și evaluarea acestora în furnizarea serviciilor esențiale (LIRIE)
11		**Relațiile ecosistemului** -Stabilirea relațiilor ecosistemului -Acorduri la nivel de serviciu	-Procedură de stabilire a relațiilor ecosistemului (PROSRE) - Inventar al acordurilor privind nivelul serviciilor și al mecanismelor de audit pentru rețele și sisteme informatice (LASMA)
12	**Managementul arhitecturii**	**Managementul configurației rețelelor și sistemelor informatice** -Arhitectura NIS; -Instalarea echipamentelor și serviciilor	-Schema arhitecturii rețelelor și sistemelor informatice (SANIS); -Analiza riscurilor de securitate a rețelelor și sistemelor informatice (ARNIS); -Mapa de acreditare de securitate (MANIS).
13		**Managementul suporților de memorie externă:** -Suporți de memorie externă	-Procedură privind utilizarea suporților de memorie externă (PRUSME); -Registre de evidență a suporților de memorie externă (RESME).
14		**Segregarea și segmentarea rețelelor și sistemelor informatice**	-Procedură privind segregarea și segmentarea rețelelor și sistemelor informatice utilizate (PROSE/ENTITĂŢI ESENŢIALES); -Schema arhitecturii rețelelor și sistemelor informatice (SANIS).
15		**Filtrarea traficului** Filtrarea fluxurilor	- Metodologie pentru controlul traficului de rețea (PROFIT); -Analiza riscurilor de securitate a rețelelor și sistemelor informatice (ARNIS).
16		**Garantarea securității produselor și serviciilor asociate rețelelor și sistemelor informatice:** -Asigurarea protecției criptografice -Managementul cheilor de criptare	-Procedură pentru asigurarea protecției criptografice pentru informații și resurse (PRAPC); -Managementul cheilor de criptare (MACC).
17		**Protecția împotriva malware:**	-Procedură pentru asigurarea protecției malware (PRAPMA)

Nr	Secțiune	Cerințe de securitate	Rezultate așteptate
		-Protecție malware	
18	**Managementul administrării**	**Administrarea conturilor:** -Conturi de administrare	-Lista conturilor de administrare (LICA)
19		**Administrarea rețelelor și sistemelor informatice:** -Utilizarea sistemelor de administrare; -Parole administrare.	-Procedură privind utilizarea sistemelor informatice de administrare (PRUSIA); - Strategia de securitate pentru rețele și sisteme informatice; - Jurnale de audit ale evenimentelor generate de resursele utilizate în administrarea sistemelor (JIERUA); -Document sigilat conținând parole pentru accesul la sistemele informatice și de administrare a rețelelor (PPSIA).
20		**Managementul accesului de la distanță** Lucrul la distanță	-Procedură privind lucrul la distanță (PROLD); Procedură pentru asigurarea protecției criptografice pentru informații și resurse (PRAPC)
21	**Managementul identității și accesului**	**Managementul identificării și autentificării utilizatorilor:** -Identificarea utilizatorilor; -Autentificarea utilizatorilor.	-Evidența conturilor pentru utilizatori și pentru procesele automatizate (ECUPA) -Analiza riscurilor de securitate a rețelelor și sistemelor informatice (ARNIS); -Mapa de acreditare de securitate (MANIS); -Mecanism de autentificare pentru utilizatori și procese automatizate la resursele rețelelor și sistemelor informatice (MEAUP)
22		**Managementul drepturilor de acces:** -Acordarea drepturilor de acces; -Verificarea conturilor privilegiate;	-Politica de securitate a rețelelor și sistemelor informatice (PONIS); -Lista conturilor privilegiate pe nivele de acces și funcționalități accesabile (LICPA); -Lista conturilor de administrare (LICA); -Sistem de verificare a potențialelor modificări ale unui cont privilegiat (SIVMOC).
23	**Managementul mentenanței**	**Mentenanța rețelelor și sistemelor informatice:** -Menținere securitate;	- Procedură pentru asigurarea securității rețelelor și sistemelor informatice; - Procedură pentru diminuarea riscurilor asociate utilizării unei versiuni depășite (PRORUVI);

Nr	Secțiune	Cerințe de securitate	Rezultate așteptate
		-Actualizare resurse Protejare resurse.	-Politica de securitate a rețelelor și sistemelor informatice (PONIS) -Mapa de acreditare de securitate (MANIS); -Procedură pentru asigurarea protecției criptografice pentru informații și resurse (PRAPC).
24		**Sisteme control industrial SCADA: Monitorizare, control și achiziții de date:** -Sisteme de control industriale; -Limitarea accesului	-Cerințe de securitate specifice pentru sistemele de control industrial (CEISC); -Analiza riscurilor de securitate și implementarea măsurilor de securitate pentru limitarea accesului neautorizat (ANISMS).
25	**Managementul securității fizice**	**Asigurarea protecției fizice a rețelelor și sistemelor informatice:** -Acces la resurse	-Procedură privind accesul și securitatea resurselor și informațiilor (PRASI)
26	**Managementul detecției**	**Managementul vulnerabilităților și alertelor de securitate:** -Fluxul alertelor de securitate; -Evaluarea și monitorizarea vulnerabilităților.	- Procedură pentru identificarea incidentelor de securitate ce impactează rețelele și sistemele informatice; - Sistem de monitorizare și înregistrare a evenimentelor în rețele și sisteme informatice (SIENIS); - Dosar de acreditare a securității (MANIS); -Proces de identificare, clasificare, remediere și eliminare a vulnerabilităților (PEIREV); - Program pentru gestionarea vulnerabilităților în rețelele și sistemele informatice (PGMAVU)Analiza riscurilor de securitate a rețelelor și sistemelor informatice (ARNIS).
27		**Înregistrarea evenimentelor:** -Monitorizare evenimente; -Sisteme de management.	- Sistem de monitorizare și înregistrare a evenimentelor în rețelele și sistemele informatice (SIENIS); - Gestionarea monitorizării, investigării și identificării rapide a principalelor cauze de compromitere a securității, precum și a încălcărilor politicilor de securitate.
28		**Jurnalizarea și asigurarea**	-Sistem de corelație și analiză de jurnal (SCAJ)

Nr	Secțiune	Cerințe de securitate	Rezultate așteptate
		trasabilității activităților în cadrul rețelelor și sistemelor informatice: -Jurnalizare și trasabilitate	
29	**Managementul incidentelor de securitate**	**Răspuns la incidente de Securitate:** -Fluxul incidentelor; -Monitorizarea incidentelor; -Gestionarea incidentelor.	- Procedură pentru gestionarea, răspunsul și analiza incidentelor care impactează funcționarea sau securitatea rețelelor și sistemelor informatice; - Sistem de monitorizare și gestionare a evenimentelor și incidentelor de securitate; -Sistem informatic destinat gestionării incidentelor (SIDGI).
30		**Raport incidente:** -Raportarea incidentelor	-Procedură pentru raportarea incidentelor de securitate (PRORIS)
31		**Comunicarea cu Autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice (ANSRSI) și CSIRT Național** -Interconectare națională; -Responsabili NIS; -Gestionare informații primite de la CERT-RO;	-Procedură de interconectare la serviciul de alertare și cooperare al CERT-RO - (PISAC); -Lista responsabililor NIS (LIRNIS); -Procedură pentru gestionarea informațiilor primite și, după caz, a măsurilor de securitate adoptate (PRIMSA).
32	**Managementul continuității afacerii**	**Asigurarea disponibilității serviciului esențial și a funcționării rețelelor și sistemelor informatice** -Asigurarea disponibilității	-Procedură privind managementul asigurării disponibilității serviciului esențial, în caz de incident de securitate cibernetică (PRADE).
33		**Gestionarea recuperării datelor în situații de dezastre** -Recuperarea datelor	-Procedură privind managementul recuperării datelor în caz de dezastre, precum și în caz de incidente severe de securitate cibernetică (PROMRE);

Nr	Secțiune	Cerințe de securitate	Rezultate așteptate
34	**Managementul crizelor**	**Organizarea gestionării crizelor** -Organizarea gestionării crizelor cibernetice	- Procedură pentru organizarea managementului crizelor în caz de incidente de securitate cibernetică, pentru garantarea continuității activităților organizaționale
35		**Procesul de gestionare a crizelor** -Gestionarea crizelor cibernetice	-Procese de gestionare a crizelor (PEGEC)

În concluzie, tabelul sintetizează cerințele și indicatorii care stau la baza conformității cu Directiva NIS 2, esențiale pentru trecerea unui audit de securitate cibernetică. Aceste elemente oferă un ghid practic pentru evaluarea nivelului de protecție al infrastructurilor critice și subliniază importanța unei implementări eficiente și coordonate. Prin respectarea acestor cerințe, se poate asigura atât protecția datelor sensibile, cât și creșterea rezilienței și încrederii utilizatorilor în sistemele informatice din sănătate.

3.5. Managementul riscului

Managementul riscului reprezintă un element central în implementarea Directivei NIS 2, având rolul de a identifica, evalua și trata riscurile asociate infrastructurilor critice din sănătate. Această secțiune explorează principiile și metodele utilizate în procesul de management al riscurilor, cu accent pe specificul sectorului sanitar și cerințele reglementative impuse de directivă. Obiectivul este de a crea un cadru proactiv care să minimizeze vulnerabilitățile și să asigure continuitatea operațională într-un mediu expus amenințărilor cibernetice tot mai sofisticate.

		Nesemnificativ	Minor	Moderat	Major	Extrem
		1	2	3	4	5
Rar	1					
Improbabil	2					
Moderat	3					
Probabil	4					
Aproape sigur	5					

Fig 1 Evaluarea riscurilor [27, 28]

Tabel 2.2 Probabilitatea de risc [27, 28]

Probabilitatea		Descriere
5	Aproape sigur > 60% - < 80%	Nicio strategie sau strategie actuală nu va rezolva această problemă, vor fi necesare alternative, acțiuni de atenuare care trebuie făcute urgent.
4	Probabil > 40% - 60%	Strategia actuală probabil nu va rezolva această problemă. Vor fi necesare alternative, vor fi necesare acțiuni de atenuare.
3	Moderat > 20 to 40%	Este posibil ca strategia actuală să nu rezolve această problemă. Pot fi necesare alternative, trebuie luate în considerare acțiuni de atenuare.
2	Improbabil > 5 to 20%	Strategia actuală ar trebui să rezolve această problemă.

1	Rar 5% sau mai putin	Acțiunile curente sunt în ordine. Problema poate fi rezolvată rapid și ușor.

Tabel 2.3 Impactul riscului [27, 28]

Impact		Descriere
5	Extrem	Eșec operațional inacceptabil
4	Major	Pierderea capacității operaționale
3	Moderat	Este necesară o acțiune de remediere
2	Minor	Impact operațional limitat
1	Nesemnificativ	Impact operațional minim

Acest model de evaluare a riscurilor, prezentat în tabelul 2.4, a fost conceput și realizat de autor, având la bază principiile fundamentale ale gestionării riscurilor cibernetice conform cerințelor legislative și normativelor în vigoare, precum Legea 362/2018 și standardele NIS 2.

Modelul urmărește să faciliteze identificarea, analiza și prioritizarea riscurilor asociate rețelelor și sistemelor informatice utilizate în furnizarea serviciilor esențiale. Este structurat astfel încât să fie ușor de utilizat, oferind un cadru sistematic pentru:

- Determinarea riscurilor potențiale;
- Evaluarea impactului și a probabilității acestora;
- Definirea măsurilor de remediere și mitigare;
- Monitorizarea continuă a riscurilor identificate.

Modelul este destinat organizațiilor care doresc să-și consolideze poziția în domeniul securității cibernetice, aliniindu-se cerințelor de conformitate și îmbunătățind reziliența față de amenințările digitale.

Tabel 2.4 Evaluarea riscurilor

ID	Descrierea riscului	Proprietar	Descrierea impactului	Prob	Impact	Prioritate	Risc acceptat	Masuri implementate pentru reducerea/transferul/evitarea riscului	Data finalizare masura	Cost	Status	Prob	Impact	Prioritate	Modif. prioritate	Status	Ultima actualizare
1	**Server baza de date**																
1.1	Furtul datelor prin accesul neautorizat in serverul de baze de date prin utilizarea unor credentiale valide	RSI	Pierderea increderii clientilor Actiuni juridice impotriva companiei Amenzi	1	5		NU	Monitorizare acces pe serverul de baze de date Criptarea datelor confidentiale	30.09.2023	1000 E	50%1	3			Inchis	15.10.2024
1.2	Furtul datelor prin accesul neautorizat in serverul de baze de date prin exploatarea unei brese de securitate a sistemului de operare al serverului	RSI		1	5		NU	Instalarea patch-rilor si update-urilor in mod regulat	Permanent	-	100%1	2			Inchis	15.10.2024
1.3	Furtul datelor prin accesul neautorizat in serverul de baze de date prin exploatarea unei brese de securitate a software-ului instalat pe server (in afara de sistemul de operare)	RSI		1	5		NU	Instalarea patch-rilor si update-urilor in mod regulat	Permanent	-	100%1	2			Inchis	15.10.2024
1.4	Furtul datelor prin accesul autorizat al unui angajat in	RSI		1	5		NU	Monitorizarea accesului administratorul	30.09.2023	1000 E	50%1	5			Deschis	15.10.2024

	serverul de baze de date						ui de baze de date									
1.5	Stergerea/modificarea datelor prin accesul neautorizat in serverul de baze de date prin utilizarea unor credentiale valide	RSI	1	5		NU	Monitorizare acces pe serverul de baze de date Backup baze de date	30.09.2023	500 E	50%1	1			Deschis	15.10.2024
1.6	Stergerea/modificarea datelor prin accesul neautorizat in serverul de baze de date prin exploatarea unei brese de securitate a sistemului de operare al serverului	RSI	1	5		NU	Instalarea patch-rilor si update-urilor in mod regulat Backup baze de date	Permanent	-	100%1	1			Inchis	15.10.2024
1.7	Stergerea/modificarea datelor prin accesul neautorizat in serverul de baze de date prin exploatarea unei brese de securitate a software-ului instalat pe server (in afara de sistemul de operare)	RSI	1	5		NU	Instalarea patch-rilor si update-urilor in mod regulat Backup baze de date	Permanent	-	100%1	1			Inchis	15.10.2024
1.8	Stergerea/modificarea datelor prin accesul autorizat al unui angajat in serverul de baze de date	RSI	1	5		NU	Monitorizare acces pe serverul de baze de date Backup baze de date	30.09.2023	500 E	100%1	1			Inchis	15.10.2024
2	**Aplicatia ccccc**															

2.1	Furtul datelor prin accesul neautorizat	RSI	Pierderea increderii clientilor Actiuni juridice impotriva companiei Amenzi	2	3		NU	Monitorizarea accesului	30.09.2023	500 E	100%1	3			Inchis	15.10.2024
2.2	Stergerea/modificarea datelor prin accesul neautorizat	RSI		2	3		NU	Monitorizarea accesului	30.09.2023	500 E	100%1	3			Inchis	15.10.2024
2.3	Nefunctionarea aplicatiei datorita unui attack de tip DDoS	RSI		3	3		NU	Blocarea posibilitatii de autentificare dupa 3 incercari nereusite	30.09.2023	-	100%1	3			Inchis	15.10.2024
3	**Aplicatia gggg**																
3.1	Furtul datelor prin accesul neautorizat	RSI	Pierderea increderii clientilor Actiuni juridice impotriva companiei Amenzi	2	3		NU	Monitorizarea accesului	30.09.2023	500 E	100%1	3			Inchis	15.10.2024
3.2	Stergerea/modificarea datelor prin accesul neautorizat	RSI		2	3		NU	Monitorizarea accesului	30.09.2023	500 E	100%1	3			Inchis	15.10.2024
3.3	Nefunctionarea aplicatiei datorita unui attack de tip DDoS	RSI		3	3		NU	Blocarea posibilitatii de autentificare dupa 3 incercari nereusite	30.09.2023	-	100%1	3			Inchis	15.10.2024
4	**Aplicatia aaaaaaa**																
4.1	Furtul datelor prin accesul neautorizat	RSI	Pierderea increderii clientilor Actiuni juridice impotriva companiei Amenzi	2	3		NU	Monitorizarea accesului	30.09.2023	500 E	100%1	3			Inchis	15.10.2024
4.2	Stergerea/modificarea datelor prin accesul neautorizat	RSI		2	3		NU	Monitorizarea accesului	30.09.2023	500 E	100%1	3			Inchis	15.10.2024
4.3	Nefunctionarea aplicatiei datorita unui attack de tip DDoS	RSI		3	3		NU	Blocarea posibilitatii de autentificare dupa 3 incercari nereusite	30.09.2023	-	100%1	3			Inchis	15.10.2024
5	**Aplicatia aaa**																

5.1	Furtul datelor prin accesul neautorizat	RSI	Pierderea increderii clientilor Actiuni juridice impotriva companiei Amenzi	2	3		NU	Monitorizarea accesului	30.09.2023	500 E	100%1	3				Inchis	15.10.2024
5.2	Stergerea/modificarea datelor prin accesul neautorizat	RSI		2	3		NU	Monitorizarea accesului	30.09.2023	500 E	100%1	3				Inchis	15.10.2024
5.3	Nefunctionarea aplicatiei datorita unui attack de tip DDoS	RSI		3	3		NU	Blocarea posibilitatii de autentificare dupa 3 incercari nereusite	30.09.2023	-	100%1	3				Inchis	15.10.2024
6	**Aplicatia ccccc**																	
6.1	Furtul datelor prin accesul neautorizat	RSI	Pierderea increderii clientilor Actiuni juridice impotriva companiei Amenzi	2	3		NU	Monitorizarea accesului	30.09.2023	500 E	100%1	3				Inchis	15.10.2024
6.2	Stergerea/modificarea datelor prin accesul neautorizat	RSI		2	3		NU	Monitorizarea accesului	30.09.2023	500 E	100%1	3				Inchis	15.10.2024
6.3	Nefunctionarea aplicatiei datorita unui attack de tip DDoS	RSI		3	3		NU	Blocarea posibilitatii de autentificare dupa 3 incercari nereusite	30.09.2023	-	100%	1	3			Inchis	15.10.2024
7	**Echipamentele IT**																	
7.1	Accesul neautorizat datorat pierderii/furtului unui laptop folosit pentru conectarea in aplicatii cu drepturi privilegiate	RSI	Pierderea increderii clientilor Actiuni juridice impotriva companiei Amenzi	2	5		NU	Implementarea Politicii de Lucru la distanta	01.08.2023	-	100%	1	2			Inchis	15.10.2024
8	**Plecarea angajatilor**																	
8.1	Demisia RSI	Adm	Posibilitatea accesului	2	2		NU	Anularea drepturilor de	Permanent	-	100%	1	1			Inchis	15.10.2024

8.2	Demisia administratorului de baze de date	Adm	neautorizat dupa plecare	2	2		NU	acces Instruirea unei persoane pentru a putea prelua responsabilitatile	Permanent	-	100%	1	1		Inchis	15.10.2024
8.3	Demisia Directorului General	Adm	Imposibilitatea, pe termen scurt, de a administra aplicatiile si bazele de date	2	2		NU	Motivarea angajatilor	Permanent	-	100%	1	1		Inchis	15.10.2024
9	**Riscuri operationale**																
9.1	Retragerea autorizarii de functionare	Adm	Imposibilitatea de a oferi serviciile	1	5		NU	Verificarea periodica a cerintelor de mentinere a autorizarii	Permanent	-	100%	1	1		Inchis	15.10.2024
9.2	Nefunctionarea aplicatiei de plati	Adm	Imposibilitatea de a oferi serviciile	1	2		NU		-	-	-					

3.6. Model de implementare a auditului de securitate cibernetică

Auditul public intern evoluează ca un instrument esențial de guvernanță, contribuind la optimizarea proceselor interne și sprijinind managementul prin utilizarea mai eficientă și eficace a resurselor disponibile [29]. Auditul de securitate energetică este un pas important în asigurarea protecției infrastructurilor critice și a conformității cu cerințele Directivei NIS 2. Într-un sector atât de sensibil precum cel energetic, unde orice vulnerabilitate poate avea consecințe majore, auditul are rolul de a identifica riscurile și de a propune măsuri concrete pentru reducerea acestora. În continuare, este prezentat un exemplu practic de audit realizat în sectorul securității energetice.

Această lucrare reprezintă o contribuție originală în domeniul securității cibernetice, fiind elaborată și redactată în întregime de către autor. Modelul de raport prezentat constituie o propunere metodologică propriu-zisă pentru realizarea unui audit de securitate IT, conform cerințelor legale și reglementărilor conexe.

Modelul de raport de audit de securitate IT este structurat pentru a sprijini organizațiile în procesul de asigurare a unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice.

Documentul este organizat astfel încât să acopere următoarele aspecte principale:

- Destinatarii raportului: Identificarea entităților implicate și responsabilitatea acestora în procesul de distribuție și utilizare a raportului.
- Obiectivul auditului: Evaluarea conformității cu legislația specifică NIS 2, identificarea vulnerabilităților și formularea recomandărilor pentru remedierea acestora.
- Documente de referință: Referințe legislative și normative relevante pentru securitatea cibernetică.
- Tipul auditului și activitățile realizate: Auditul calificat include evaluarea riscurilor operaționale, testarea de penetrare și verificarea implementării planului de măsuri.
- Concluzii și recomandări: Identificarea neconformităților și recomandări detaliate pentru reducerea riscurilor identificate.
- Opinia auditorului: Emiterea unei opinii formale privind nivelul de conformitate, cu opțiuni pentru opinii pozitive, negative sau cu rezerve.

Acest model este conceput pentru a servi drept ghid operațional și metodologic pentru auditorii de securitate cibernetică, oferind un cadru standardizat care permite analiza sistematică a stării de securitate a unei organizații. De asemenea, facilitează alinierea la cerințele legale și implementarea unui plan de măsuri pentru consolidarea rezilienței cibernetice.

Prin prezentul document, reafirm originalitatea și unicitatea acestui model de raport, elaborat pe baza cunoștințelor și experienței personale acumulate în domeniul auditării securității IT.

Raportul de audit de securitate IT (RASEC), întocmit conform prevederilor legale, este documentat sub numărul ... din data de ... Acesta reprezintă versiunea finală 1.0, incluzând toate informațiile necesare pentru evaluarea conformității infrastructurii IT cu cerințele legale în vigoare.

1. Destinatarii raportului

SC auditat SRL – auditat
Directoratul National de Securitate Cibernetica – Autoritatea Națională pentru Securitatea Rețelelor si Sistemelor Informatice
SC auditor SRL – auditor
Auditul de securitate IT a fost realizat in baza contractului nr .....
.....

Raportul de audit (RASEC) este proprietatea SC auditat SRL si acesta este responsabil pentru distribuția acestuia către părțile interesate. Raportul de audit conține informații confidențiale.
2. Operatorul de servicii esențiale

3. Tipul serviciului de audit furnizat/ efectuat

Auditul a fost realizat in baza:

- Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice;
- Ordonanță de Urgență nr. 119 din 22 iulie 2020 pentru modificarea și completarea Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice;
- Ordinul nr. 1323/2020 pentru aprobarea Normelor tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale.
- Ordonanță de Urgență Nr. 155/2024 din 30 decembrie 2024 privind instituirea unui cadru pentru securitatea cibernetică a reţelelor şi sistemelor informatice din spaţiul cibernetic naţional civil

Tipul auditului: Audit calificat in baza Legii 362/2018.
Activități de audit:
Obiectivele auditului:
Activitatea auditată:
Sediul auditat:
Perioada audit:

4. Datele de identificare ale auditorului

5. Descrierea sferei auditului

6. Evaluarea anuala a riscurilor operaționale

7. Testarea de penetrare

8. Implementarea planului de măsuri asumat de operatorul economic la ultimul audit de securitate

9. Concluziile auditorului de securitate cibernetica si Opinia de audit

<u>Neconformități:</u>

Neconformitatea 1:

Descrierea neconformității:

Cerința din cadrul Ordinului 1323/2020:

Importanta neconformității:

Riscurile asociate:

Măsuri compensatorii:

Recomandări:

OPINIA

in conformitate cu obligațiile legale impuse de Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cu modificările și completările ulterioare (Legea NIS), de Normele tehnice privind cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale, motiv pentru care exprimăm: OPINIE NEGATIVA / POZITIVĂ/ CU REZERVE

PENTRU opinie negativă, conform Art 28, Al 4, punctul b („Auditorul de securitate cibernetică notifică atât operatorului economic auditat, cât și autorității competente la nivel național, prin e-mail (nis@cert.ro), în maximum 5 zile de la constatare.

Pentru toate neconformitățile si recomandările identificate auditatul va documenta un Plan de Masuri ce va conține pentru fiecare neconformitate si recomandare cel puțin: modalitatea de închidere a neconformității, termenul de închidere, responsabilul. Planul de Masuri va fi transmis Auditorului pentru avizare si Directoratului National de Securitate Cibernetica in urma avizării de către Auditor. Planul de masuri trebuie transmis in maxim 30 de zile.

10. Asumarea responsabilității de către operatorul economic

Data finalizării raportului de audit: .....

Semnături
SFARSITUL DOCUMENTULUI

`Număr de înregistrare și data	*Număr de înregistrare și data*
Autoritate contractantă	*CONTRACTANT*
_____ / _____	_____ / _____

Proiect: “Sistem INTEGRAT de Management în Sistemul de Asigurări Sociale de Sănătate” - cod SIPOCA XXX

Privind: “Dezvoltarea și implementarea sistemului INTEGRAT de Management în Sistemul de Asigurări Sociale de Sănătate”

Raport de testare, de securitate/Audit de securitate, de performanță

Beneficiar: xxxxx

Data: XXX

Tabel 2.5 Autori

Nume și prenume	Funcție	Semnătura
XXX	Specialist testare	XXX

Tabel 2.6 Aprobări

	Nume și prenume	Funcție	Data	Semnatură
Verificat		Manager de proiect adjunct		
Aprobat		Coordonator testare		
Aprobat		Manager Proiect		
Verificat		Expert IT		

Scop

Scopul acestui document constă în prezentarea rezultatelor testării de acceptanță a platformei „e-Sănătate", realizate de către Beneficiar împreună cu Prestatorul în cadrul proiectului "Sistem Integrat de Management în Sistemul de Asigurări Sociale de Sănătate" - cod SIPOCA xxx".

Destinatari

Prezentul document, reprezintă livrabilul etapei de testare a sistemului, și conține scenariile de testare funcțională privind Procesele de analiză.

Documentul este adresat:

- Comisiei de testare de acceptanță a beneficiarului;
- Echipei de testare a beneficiarului;
- Echipei de testare a furnizorului
- Descrierea testelor

Centralizator scenarii de testare

Lista scenariilor de testare parcurse în etapa de acceptanță a platformei „e-Sănătate" este prezentată în Lvr VI.2 Scenarii de test.

Definiția severității

Tabel 2.7 Definiția severităților din procesul intern de testare

Severitate	Definiție
Severitate Nivel 1 Critic	Definiție: Orice defect alocat cu impact critic în business, ce provoacă una din următoarele: (i) utilizatorul suferă o pierdere completă sau substanțială a serviciilor, sau (ii) defecțiunea unui proces de business critic, sau

Severitate	Definiție
	(iii) impact în serviciile furnizate de utilizator sau determină pierderi de venituri.
Severitate Nivel 2 Major	Definiție: Orice defect alocat care provoacă impact în business, astfel: (i) defecțiunea în sine determină un impact critic în business, iar acesta este redus prin faptul că defecțiunea poate fi evitată, sau (ii) anumite funcționalități din cadrul Soluției sunt dezactivate, dar procesul de business este încă operațional.
Severitate Nivel 3 Mediu	Definiție: Orice defect alocat ce provoacă impact minim în business, utilizatorul nu suferă pierderea totală a serviciului, iar defectul nu generează efecte semnificative în utilizarea Soluției.
Severitate Nivel 4 Minor	Definiție: Orice defect alocat care nu generează impact în business, dar afectează funcționalități minore sau Soluția funcționează corect, dar apar probleme estetice.

Informații testare

Mediul utilizat pentru activitățile de testare
Pentru activitatea de testare au fost folosite mediile instalate și configurate în cadrul proiectului.

Activități de testare

În continuare sunt listate activitățile de testare efectuate pentru această livrare, după cum urmează:

- Creare scenarii/cazuri de test;
- Execuție scenarii/cazuri de test;
- Raportarea defectelor;
- Crearea raportului de testare.

Aceste activități au fost realizate în mai multe iterații, pana la corectarea defectelor înregistrate.
Rezultatele testelor de acceptanță realizate de Beneficiar

Tabel 2.8 Rezultatele testelor de acceptanță

Cod	Denumire	Status	Observații
Procese analiză			
UC - CNAS - 01 – TC-01	Vizualizare dashboard-uri/rapoarte predefinite		
UC - CNAS - 02 – TC-01	Vizualizare CONTROL-RAP-09 Analize avansate		
UC - CNAS - 03 – TC-01	Vizualizare raport NORME-RAP-04 Centralizator stomatologie		
Procese administrative			
UC - CNAS - 04 – TC-01	Pregătire date pentru analize ad-hoc		
UC - CNAS - 05 – TC-01	Construire dashboard		
UC - CNAS - 05 – TC-02	Construire raport		
UC - CNAS – 06 – TC-01	Definire indicator în dashboard/raport existent		
UC - CNAS – 07 – TC-01	Definire analiză avansată ad-hoc		

Cod	Denumire	Status	Observații
UC – CNAS – 14 – TC-01	Pregătire date pentru alimentarea Portalului extern – zona publica		
UC - CNAS - 16 – TC-01	Zonă de informare furnizori de servicii medicale		
UC - CNAS - 17 – TC-01	Zonă de informare a instituțiilor publice		
Procese de concatenare inițială din bazele de date replicate			
UC - CNAS - 08 TC-01	Autentificarea Data Integration Studio		
UC - CNAS - 08 – TC-02	Verificare: Procese de concatenare inițială din bazele de date replicate		
UC - CNAS - 08 – TC-03	Autentificarea Management Console		
UC - CNAS - 08 – TC-04	Verificare: Procesele organizate pentru rulare automată		
UC - CNAS - 08 – TC-05	Verificare: Status execuţie job-uri concatenare şi istorizare		
Procese Zonă de informare publică generică			
UC-CNAS-09 – TC-01	Vizualizarea indicatorilor la nivelul hărții Administrative a României in xxx		
UC-CNAS-10 – TC-01	Upload manual de date în sistem		
UC-CNAS-15: TC-01	Accesare componentă xxx		
UC-CNAS-15: TC-02	Accesare și funcționare pagină principală xxx		
UC-CNAS-15: TC-03	Accesare meniuri din xxx		
UC-CNAS-15: TC-04	Accesare și funcționare pagină Informații Asigurați		
UC-CNAS-15: TC-05	Accesare și funcționare pagină Informații Furnizori		
UC-CNAS-15: TC-06	Accesare și funcționare pagină Informații Publice		
UC-CNAS-15: TC-07	Accesare și funcționare pagină de contact		
UC-CNAS-15: TC-08	Afișare zonă de administrare		
UC-CNAS-15: TC-09	Creare pagini web		
UC-CNAS-15: TC-10	Modificare pagini web		
UC-CNAS-15: TC-11	Ștergere pagini web		
UC-CNAS-15: TC-12	Creare widget-uri		
UC-CNAS-15: TC-13	Modificare widget-uri		
UC-CNAS-15: TC-14	Ștergere widget-uri		
UC-CNAS-15: TC-15	Adăugare upload fișiere		
UC-CNAS-15: TC-16	Ștergere upload fișiere		
UC-CNAS-15: TC-17	Adăugare nomenclator relaționat		
UC-CNAS-15: TC-18	Modificare nomenclator relaționat		
UC-CNAS-15: TC-19	Ștergere nomenclator relaționat		
UC-CNAS-15: TC-20	Funcționare și accesare meniu “Setări generale”		
UC-CNAS-15: TC-21	Creare pagină în meniul de administrare		
UC-CNAS-15: TC-22	Modificare pagină în meniul de administrare		
UC-CNAS-15: TC-23	Ștergere pagină în meniul de administrare.		
UC-CNAS-15: TC-24	Creare cont membru echipa		
UC-CNAS-15: TC-25	Modificare cont membru echipă		

Cod	Denumire	Status	Observații
UC-CNAS-15: TC-26	Ștergere cont membru echipă		
UC-CNAS-15: TC-A01	Adăugare și ștergere rapoarte		
UC-CNAS-15: TC-A02	Selectare și completare zona Contact		
UC-CNAS-15: TC-A03	Contact General Settings		
UC-CNAS-15: TC-A04	Cookies		
UC-CNAS-15: TC-A05	File Upload		
UC-CNAS-15: TC-A06	Autentificare în portalul extern.		
UC-CNAS-15: TC-A07	Accesare pagină “Acasă” a xxx		
UC-CNAS-15: TC-A08	Accesare pagină “Informații Asigurați” a xxx.		
UC-CNAS-15: TC-A09	Accesare pagină “Informații Furnizori” a xxx.		
UC-CNAS-15: TC-A010	Creare/Modificare/Ștergere nomenclatoare relaționate		
UC-CNAS-15: TC-A011	Accesare pagină “Informații Publice”.		
UC-CNAS-15: TC-A012	Accesare pagină “Politică de confidențialitate”.		
UC-CNAS-15: TC-A013	Vizualizare/Creare/Modificare/Ștergere Cont membru echipă.		
UC-CNAS-15: TC-A014	Accesare pagină “Termeni și Condiții”.		
UC-CNAS-15: TC-A015	Vizualizare pagini admin.		
UC-CNAS-15: TC-A016	Vizualizare/Creare/Modificare/Ștergere Widget-uri.		
UC-CNAS-03 – TC-01	Accesare și funcționare pagina de portal extern de pe un dispozitiv mobil		
Procese Portal xxx			
UC - CNAS - 11 – TC-01:	Utilizatorul se autentifică în portalul xxxx		
UC - CNAS - 11 – TC-01	Utilizatorul se autentifică în portalul xxx		
UC - CNAS - 11 – TC-02	Utilizatorul face o cerere pentru o resursă disponibilă pentru el în portal, în baza rolurilor pe care acesta le are la nivelul soluției.		
UC - CNAS - 11 – TC-03	Utilizatorul urmărește statusul cererii sale direct în portalul web.		
UC - CNAS - 11 – TC-04	Aprobare cerere		
UC - CNAS - 11 – TC-05	Utilizatorul primește în portal confirmarea primirii resursei cerute		
UC - CNAS – 12 -	Înregistrare utilizator intern nou (angajat)		
UC - CNAS - 12 – TC-01	Simularea creării unui utilizator intern nou în sistemul PIAS prin ștergerea unui utilizator deja provizionat în „e-Sănătate” de către un administrator al xxx		
UC - CNAS - 12 – TC-02	Utilizatorul nou creat este înrolat în componentele de management al utilizatorilor și acces în sistem prin mecanisme xxx		
UC - CNAS - 12 – TC-03	Utilizatorul nou creat se autentifică în sistemul „e-Sănătate”		
UC - CNAS - 13 –	Înregistrare utilizator extern		
UC - CNAS - 13 – TC-01	Înregistrare utilizator extern - furnizor de servicii medicale		

Cod	Denumire	Status	Observații
UC - CNAS - 13 – TC-02	Utilizatorul extern furnizor de servicii medicale nou creat se autentifică în sistemul „e-Sănătate”		
UC - CNAS – 13.1 – TC-01	Înregistrare utilizator extern – de la instituții cu care CNAS are protocoale de colaborare		
UC - CNAS – 13.1 – TC-02	TC-04: Utilizatorul extern - de la instituții cu care CNAS are protocoale de colaborare - nou creat se autentifică în sistemul „e-Sănătate”		
UC – CNAS – 03 Vizualizare rapoarte de pe dispozitive mobile			
UC - CNAS - 1 – TC-02	TC-02: Utilizatorul extern - user alte institutii cu care CNAS a încheiat protocoale de colaborare se autentifică în sistemul xxxx de pe dispozitivul mobil		
Procese de replicare			
UC - CNAS - 18 – TC-01	Validare repository replicare PIAS		
UC - CNAS - 18 – TC-02	Validare repository replicare SIPE		
UC - CNAS - 18 – TC-03	Validare repository replicare CEAS		
UC - CNAS - 18 – TC-04	Validare repository replicare DES		
UC - CNAS - 18 – TC-05	Validare repository replicare ERP		
UC - CNAS - 18 – TC-06	Validare process checksum PIAS		
UC - CNAS - 18 – TC-07	Validare process checksum SIPE		
UC - CNAS - 18 – TC-08	Validare process checksum CEAS		
UC - CNAS - 18 – TC-09	Validare process checksum DES		
UC - CNAS - 18 – TC-10	Validare process checksum ERP		
UC - CNAS - 18 – TC-11	Validare process replicare PIAS		
UC - CNAS - 18 – TC-12	Validare process replicare SIPE		
UC - CNAS - 18 – TC-13	Validare process replicare CEAS		
UC - CNAS - 18 – TC-14	Validare process replicare DES		
UC - CNAS - 18 – TC-15	Validare process replicare ERP		
UC - CNAS - 18 – TC-16	Validare process replicare - sursa incrementala		
UC - CNAS - 18 – TC-17	Validare process replicare - generare rapoarte		
UC - CNAS - 18 – TC-18	Process replicare - generare notificari		
UC - CNAS - 18 – TC-19	Verificare adaugare coloana xxx		
UC - CNAS - 18 – TC-20	Proces replicare – verificare eliminare coloane nefolosite		
UC - CNAS - 18 – TC-21	Proces replicare – confirmare disponibilitate informatii xxx		
UC - CNAS - 18 – TC-22	Proces replicare – adaugare comentarii tabele / coloane		
UC - CNAS - 18 – TC-23	Proces replicare – auditare lista useri care modifica tabele repository		
UC - CNAS - 18 – TC-24	Proces replicare – creare semafor proces xxxx		
UC - CNAS - 18 – TC-25	Proces replicare - generare notificări		

Cod	Denumire	Status	Observații
TUC - CNAS - 18 – TC-26	Proces replicare - generare notificări – liste predefinite		
Procese de transformare			
UC - CNAS – 19 – TC - 01	Concatenare inițială în xxx din bazele de date replicate în xxxx		
UC - CNAS – 20 – TC - 01	Transformare în xxxx		
Procese de alimentare xxx din modelul de date final			
UC - CNAS - 21 – TC-01	Alimentare BigData în xxx		
UC - CNAS - 21 – TC-02	Alimentare BigData în xxx		
UC - CNAS - 21 – TC-03	Alimentare BigData din alte surse în xxx		
UC - CNAS - 21 – TC-04	Alimentare BigData din alte surse în xxx		
UC - CNAS - 21 – TC-05	Alimentare BigData în componenta de raportare SuperSet în xxx		
UC - CNAS - 21 – TC-06	Alimentare BigData în componenta de raportare SuperSet în xxx		
Procese de alimentare a zonelor de analiză din Stagiul xxx			
UC - CNAS - 22 – TC-01	Verificare replicare xxx catre xxx		
UC - CNAS - 22 – TC-02	Verificare replicare xxx catre xxx		
UC - CNAS - 22 – TC-03	Verificare replicare xxx catre xxx		
UC - CNAS - 22 – TC-04	Verificare replicare xxx catre xxx		
UC - CNAS - 22 – TC-05	Verificare replicare xxx catre xxx		
UC - CNAS – 22 – TC-06	Verificare replicare xx catre xxx,		
UC - CNAS - 22 – TC-07	Verificare replicare xxx catre xxx		
Procese xxx			
UC - CNAS - 23 – TC-01	Verificare autentificare în componenta NIFI din xxx		
UC - CNAS - 23 – TC-02	Verificare autentificare în componenta xxx din xxx		
UC - CNAS - 24 – TC-01	Crearea unui flux de lucru în NIFI din xxx		
UC - CNAS - 24 – TC-02	Executarea unui flux de lucru în NIFI din xxx		
UC - CNAS - 25 – TC-01	Realizare analize și vizualizare în componenta xxx din xxx		
UC - CNAS - 25 – TC-02	Realizare analize și vizualizare în componenta xxx din xxx		
UC - CNAS - 25 – TC-03	Partajare raport în componenta xxx		
UC - CNAS - 25 – TC-04	Descărcare raport în componenta SuperSet		
UC - CNAS - 26 – TC-01	Generarea unei raportări în componenta xxx din xxx		
Procese de backup/restore			
UC - CNAS - 27 – TC-01	Verificare Backup Stage 1		
UC - CNAS - 27 – TC-02	Verificare Backup Stage 2		
UC - CNAS - 27 – TC-03	Verificare Backup Stage 3		
UC - CNAS - 27 – TC-04	Verificare Backup Stage 4		

Cod	Denumire	Status	Observații
UC - CNAS - 27 – TC-05	Verificare frecventa Backup Stage 1		
UC - CNAS - 27 – TC-06	Verificare frecventa backup Stage 2		
UC - CNAS - 27 – TC-07	Verificare frecventa backup Stage 3		
UC - CNAS - 27 – TC-08	Verificare frecventa Backup Stage 4		
UC - CNAS - 27 – TC-09	Verificare dump DB replicare (Oracle x)		
UC - CNAS - 27 – TC-10	Verificare frecventa dump DB replicare (Oracle x)		
UC - CNAS - 28 – TC-01	Verificare Restore Stage 1		
UC - CNAS - 28 – TC-02	Verificare Restore Stage 2/ Stage3		
UC - CNAS - 28 – TC-03	Verificare Restore Stage 4		
UC - CNAS - 28 – TC-04	Verificare Restore DB Replicare		
UC - CNAS - 29 – TC-01	Generare backup-uri prin componenta		
UC - CNAS - 29 – TC-02	Verificare existentă backup-uri generate de		
UC - CNAS - 30 – TC-01	Restore Servere de aplicație utilizând		
UC - CNAS - 30 – TC-02	Verificare Restore Servere de aplicație utilizând		
Procese Securitate Sistem/Audit de Securitate			
UC - CNAS - 33 – TC-01	Validarea faptului că fișierele de configurare implicite și cunoscute au fost eliminate		
UC - CNAS - 33 – TC-02	Aceasta testare își propune sa identifice vulnerabilitățile aflate pe serverele si echipamentele aflate in scop, exploatabile de orice potențial atacator care are acces la acestea prin rețea.		
UC - CNAS - 33 – TC-03	Colectarea informațiilor se efectuează folosind aplicații (scripturi) pentru identificarea suprafeței de atac.		
UC - CNAS - 33 – TC-04	Se va verifica daca politicile de protecție firewall sunt definite si aplicate pentru serviciile expuse in internet.		
UC - CNAS - 33 – TC-05	Se verifica daca echipamentul de tip xxx si xxx expune in internet porturi care pot genera vulnerabilități		
UC - CNAS - 33 – TC-06	Se testează daca in cazul unui atac de tip DDOS echipamentele de tip xxx reacționează si izolează atacul		
UC - CNAS - 33 – TC-07	Se testează daca in cazul unui atac de tip DDOS echipamentele de tip xxx reacționează si izolează atacul		
UC - CNAS - 33 – TC-08	Se identifica daca sistemul prezinta vulnerabilități prin publicarea de documente cu cod executabil si cu semnătura de viruși.		
UC - CNAS - 33 – TC-09	Se identifica daca in sistemele productive se utilizează credențiale de acces implicite (exemplu admin/admin)		

Cod	Denumire	Status	Observații
UC - CNAS - 33 – TC-10	Colectarea informațiilor se efectuează folosind aplicații (scripturi) pentru identificarea suprafeței de atac.		
UC - CNAS - 33 – TC-11	Se va determina daca portalul expune legături la terțe sisteme sau la alte domenii care pot sa ofere informații atacatorului		
UC - CNAS - 33 – TC-12	Se va testa xxx pentru vulnerabilități de tip SLQ Injection		
UC - CNAS - 33 – TC-13	Se va testa xxx referitor la capacitatea de asigurare a serviciilor in cazul unui atât de tip DDoS		
UC - CNAS - 33 – TC-14	Se va determina medoda de accesare a panoului de administrare a portalului si se va încerca forțarea accesului		
UC - CNAS - 33 – TC-15	Colectarea informațiilor se efectuează folosind aplicații (scripturi) pentru identificarea suprafeței de atac.		
UC - CNAS - 33 – TC-16	Se va determina daca portalul expune legături la terțe sisteme sau la alte domenii care pot sa ofere informații atacatorului		
UC - CNAS - 33 – TC-17	Se va testa portalul intern pentru vulnerabilități de tip SLQ Injection		
UC - CNAS - 33 – TC-18	Se va testa portalul intern referitor la capacitatea de asigurare a serviciilor in cazul unui atât de tip DDoS		
UC - CNAS - 33 – TC-19	Se va încerca forțarea accesului in portalul intern		
UC - CNAS - 33 – TC-20	Se identifica daca sistemul are vulnerabilități la administrarea utilizatorilor		
UC - CNAS - 33 – TC-21	Se testează posibilitatea unor atacuri folosind retransmiterea alterata a cererii de modificare atât in mod autentificat cat si in mod neautentificat pentru toate rolurile utilizatorilor de test disponibile pentru a determina daca putem modifica parametrii de sistem		
UC - CNAS - 33 – TC-22	Colectarea informațiilor se efectuează folosind aplicații (scripturi) pentru identificarea suprafeței de atac.		
UC - CNAS - 33 – TC-23	Se va testa soluția xxx pentru vulnerabilități de tip SLQ Injection		
UC - CNAS - 33 – TC-24	Se va încerca forțarea accesului la soluția xxx		
UC - CNAS - 33 – TC-25	Se identifica daca sistemul are vulnerabilități la administrarea utilizatorilor		
UC - CNAS - 33 – TC-26	Se testează posibilitatea unor atacuri folosind retransmiterea alterata a cererii de modificare atât in mod autentificat cat si in mod neautentificat pentru toate rolurile utilizatorilor de test disponibile pentru a determina daca putem modifica parametrii de sistem		

Cod	Denumire	Status	Observații
UC - CNAS - 33 – TC-27	Se identifica daca sistemul are vulnerabilități la autentificare in cadrul modulului de acces unic referitor la numărul de sesiuni permise		
UC - CNAS - 33 – TC-28	Se testează criptarea credentialelor pe canalul de autentificare		
UC - CNAS - 33 – TC-29	Se testează cookie-urile de sesiune prin atacuri de manipulare a sesiunilor si a cookie-urilor		
UC - CNAS - 33 – TC-30	Se testează tokenurile aplicației care mențin utilizatorii autentificați pe toata perioada sesiunilor si după expirarea sesiunilor sau deautentificarea utilizatorilor		
UC - CNAS - 33 – TC-31	Se testează funcționalitățile de schimbare a parolei si de schimbare neautorizata a acesteia de către un atacator		
UC - CNAS - 33 – TC-32	Se testează funcționalitatea de tip lockout pentru un anumit număr de încercări de autentificare eșuate;		
UC - CNAS - 33 – TC-33	Se testează autentificarea forțata si prin utilizarea de credențiale de acces implicite (de exemplu admin/admin)		
Procese Performanță Sistem			
UC-CNAS-34: TC-01	Simulare 10 conexiuni concurente pentru Accesare dashboarduri xx		
UC-CNAS-34: TC-02	Simulare 100 de conexiuni concurente pentru Accesare dashboarduri xxx		
UC-CNAS-34: TC-03	Simulare 5000 de conexiuni concurente pentru Accesare dashboarduri xxx		
UC-CNAS-34: TC-04	Simulare 10.000 de conexiuni concurente pentru Accesare dashboarduri xxx		
UC-CNAS-34: TC-05	Simularea a 10 conexiuni concurente pe xxx		
UC-CNAS-34: TC-06	Simulare 100 conexiuni concurente xxx		
UC-CNAS-34: TC-07	Simularea a 1000 de conexiuni concurente xxx		
UC-CNAS-34: TC-8	Testarea timpului de răspuns pentru obținerea de rapoarte predefinite		

Rezultatele testelor de acceptanță evidențiază conformitatea sistemului cu majoritatea cerințelor tehnice și de securitate stabilite inițial. Cele mai importante concluzii includ:

- *Performanța generală* – Sistemul îndeplinește standardele de performanță stabilite, ceea ce demonstrează un nivel înalt de funcționalitate și scalabilitate în condiții normale de operare.
- *Identificarea punctelor slabe* – Au fost observate câteva vulnerabilități care necesită îmbunătățiri, în special în zonele legate de interoperabilitate sau de protecția datelor sensibile.
- *Respectarea cerințelor de securitate* – Testele au confirmat un nivel adecvat de protecție împotriva principalelor tipuri de amenințări cibernetice, însă sunt necesare actualizări pentru a aborda riscurile emergente.
- *Recomandări pentru optimizare* – Pe baza rezultatelor, sunt propuse acțiuni specifice pentru îmbunătățirea eficienței și securității sistemului, în vederea alinierii complete la cerințele Directivei NIS 2.

În ansamblu, testele de acceptanță oferă o bază solidă pentru implementarea operațională a sistemului, subliniind necesitatea monitorizării continue și a ajustării periodice pentru menținerea conformității.

3.7 Concluzii

Directiva NIS 2 este un pilon esențial în consolidarea securității cibernetice la nivel european. Implementarea acesteia în România a adus schimbări semnificative în domeniul securității informaționale, generând reforme atât legislative, cât și instituționale. În ciuda provocărilor inițiale, rezultatele demonstrează progrese clare în consolidarea rezilienței cibernetice și alinierea la standardele europene.

Prin identificarea și reglementarea operatorilor de servicii esențiale, România a făcut un pas important către protejarea infrastructurilor critice. De asemenea, implementarea măsurilor impuse de Directivă a încurajat colaborarea interinstituțională și a crescut gradul de conștientizare privind importanța securității cibernetice.

Pe termen lung, succesul Directivei NIS 2 în România investiții continue în educație și tehnologie, de adaptarea la noile provocări cibernetice și de cooperarea strânsă cu partenerii internaționali. Prin aceste eforturi, Directiva NIS 2 poate deveni un catalizatornsformarea digitală a României, asigurând protecția datelor sensibile și un mediu cibernetic sigur pentru cetățeni și organizații.

Capitolul 4. Oportunități, idei si ipoteze de cercetare în implementarea Directivei Europene NIS 2 în Casa Națională de Asigurări de Sănătate

4.1. Concepte generale

Acest subcapitol explorează principiile fundamentale și măsurile esențiale necesare pentru implementarea Directivei NIS 2 în contextul infrastructurilor critice din sănătate. Directiva subliniază importanța asigurării unui nivel înalt de securitate cibernetică prin evaluarea riscurilor, stabilirea unor politici clare și adoptarea măsurilor tehnice și organizaționale adecvate.

Se vor detalia aspecte precum gestionarea identității și a accesului, instruirea personalului, planificarea răspunsului la incidente și colaborarea cu autoritățile de reglementare. Aceste măsuri au scopul de a asigura protecția datelor sensibile și reziliența sistemelor critice în fața amenințărilor cibernetice, contribuind astfel la securitatea și continuitatea serviciilor esențiale.

O parte dintre aceste concepte sunt enumerate în cele ce urmează:

- Evaluarea riscurilor și identificarea entităților critice: Primul pas constă în evaluarea riscurilor cibernetice la care este expusă infrastructura critică din sănătate, inclusiv CNAS. Aceasta implică identificarea activelor critice și a amenințărilor potențiale;
- Dezvoltarea politicii de securitate cibernetică: Implementarea Directivei NIS 2 necesită dezvoltarea unei politici de securitate cibernetică coerente și actualizate pentru a se conforma cerințelor directivei. Această politică ar trebui să includă obiective clare, măsuri de securitate, roluri și responsabilități;
- Măsuri tehnice și organizaționale de securitate cibernetică: Implementarea măsurilor tehnice, precum actualizarea software-ului, monitorizarea securității rețelei și criptarea datelor, este esențială pentru protejarea infrastructurii critice. De asemenea, se vor implementa măsuri organizaționale pentru a asigura o abordare cuprinzătoare a securității;

- Gestionarea identității și a accesului: Un aspect crucial este asigurarea gestionării corespunzătoare a identității și a accesului la sisteme și date. Acest lucru implică autentificare în doi factori, controlul accesului și monitorizarea activității utilizatorilor.
- Instruirea personalului: Personalul de la CNAS și din infrastructura critică din sănătate trebuie instruit cu privire la practicile de securitate cibernetică și la modul corect de a răspunde la incidentele cibernetice;
- Planificarea răspunsului la incidente: Infrastructura critică din sănătate ar trebui să aibă planuri de răspuns la incidente pregătite pentru a acționa rapid și eficient în cazul unui atac cibernetic sau a unei breșe de securitate;
- Colaborare cu autoritățile de reglementare: CNAS și alte organizații critice din sănătate ar trebui să colaboreze cu autoritățile de reglementare și cu alte părți interesate pentru a se conforma cerințelor directivei și pentru a beneficia de sprijin în domeniul securității cibernetice;
- Monitorizarea și auditarea continuă: Este crucială monitorizarea continuă a securității cibernetice și auditarea regulată pentru a se asigura că măsurile de securitate sunt eficiente și actualizate;
- Raportarea incidentelor: Conform Directivei NIS 2, incidentele de securitate cibernetică trebuie raportate autorităților competente. CNAS și alte organizații trebuie să fie pregătite să respecte această cerință;
- Adaptarea la schimbările legale și tehnologice: Directivele NIS 2 și peisajul tehnologic evoluează în timp. Implementarea trebuie să fie dinamică și adaptabilă la aceste schimbări;
- Implementarea Directivei NIS 2 are ca obiectiv asigurarea securității cibernetice și a rezilienței în fața amenințărilor cibernetice în infrastructura critică din sănătate. Aceasta presupune eforturi constante pentru a se asigura că organizația este pregătită să facă față riscurilor cibernetice în continuă evoluție.

4.2. Ipoteze de cercetare și instrumentele metodologice utilizate

Iată trei ipoteze de cercetare legate de implementarea Directivei NIS 2 în infrastructura critică din sănătate:

- Ipoteza 1: Implementarea Directivei NIS 2 în infrastructura critică din sănătate va duce la reducerea numărului de incidente cibernetice;
- Ipoteza 2: Costurile inițiale de conformitate cu Directivele NIS 2 în infrastructura critică din sănătate vor fi semnificative, dar vor fi compensate de scăderea costurilor asociate incidentelor cibernetice pe termen lung;
- Ipoteza 3: Colaborarea activă între organizațiile critice din domeniul sănătății pentru schimbul de informații privind amenințările cibernetice va conduce la o creștere a rezilienței și a securității cibernetice în sectorul sănătății.

Ipoteza 1:
Pentru a testa Ipoteza 1, care sugerează că implementarea Directivei NIS 2 în infrastructura critică din sănătate va duce la reducerea numărului de incidente cibernetice, putem utiliza o serie de instrumente metodologice cum ar fi:

- Analiza istoricului incidentelor cibernetice: Pentru a evalua evoluția incidentelor cibernetice în infrastructura critică din sănătate înainte și după implementarea Directivei NIS 2, putem analiza istoricul incidentelor. Aceasta implică colectarea și analiza datelor privind incidentele dintr-un interval de timp predefinit;
- Compararea cu organizații asemănătoare: Comparăm numărul și tipurile de incidente cibernetice în infrastructura critică din sănătate cu organizații similare care nu au implementat Directivea NIS 2.

Pentru analiza trendurilor utilizam instrumente de analiză pentru a identifica trendurile și modelele în incidentele cibernetice înainte și după implementarea Directivei NIS 2. Astfel, putem observa dacă există o tendință descrescătoare în incidente de securitate cibernetică. Instrumente propuse sunt descrise după cum urmează:

- Interviuri și chestionare: Intervievam personalul de securitate cibernetică și altele persoane implicate în implementarea Directivei NIS 2 pentru a obține perspective calitative cu privire la impactul acesteia asupra incidentelor cibernetice;
- Monitorizarea sistemelor de securitate: Utilizam instrumente de monitorizare a sistemelor de securitate pentru a urmări activitatea și a detecta orice încercare de atac sau incidente cibernetice în timp real. Aceasta poate ajuta la evaluarea eficacității măsurilor de securitate implementate;
- Analiza bugetară: Evaluarea bugetului alocat securității cibernetice înainte și după implementarea Directivei NIS 2 ne poate ajuta să înțelegem resursele financiare implicate și modul în care acestea au influențat incidentele cibernetice;
- Colectarea de date statistice: Colectați date statistice despre incidentele cibernetice din surse publice și private pentru a obține o imagine cuprinzătoare a evoluției acestor incidente în domeniul sănătății.

Ipoteza 2:
Pentru a testa Ipoteza 2, care sugerează că costurile inițiale de conformitate cu Directivele NIS 2 în infrastructura critică din sănătate vor fi semnificative, dar vor fi compensate de scăderea costurilor asociate incidentelor cibernetice pe termen lung. Din punct de vedere metodologic, se vor urma pașii enumerati mai jos:

- Analiza costurilor de implementare a directivei NIS 2: Evaluam și cuantificam costurile inițiale de implementare a măsurilor de securitate cibernetică necesare pentru a respecta cerințele Directivei NIS 2. Acest lucru poate implica analiza cheltuielilor cu achiziționarea de echipamente, software, formare și resurse umane;
- Analiza costurilor incidentelor cibernetice Pre-NIS 2: Colectam date cu privire la costurile asociate incidentelor cibernetice care au avut loc în infrastructura critică din sănătate înainte de implementarea Directivei NIS 2. Aceste date includ costurile de recuperare, costurile de reputație și orice alte cheltuieli asociate incidentelor;
- Analiza costurilor incidentelor cibernetice Post-NIS 2: Continuam să colectam date privind costurile incidentelor cibernetice care au avut loc după implementarea Directivei NIS 2. Comparam aceste costuri cu cele pre-NIS 2 pentru a evalua dacă au avut loc schimbări semnificative;
- Evaluarea Roi-ului (Return on Investment): Calculam Roi-ul asociat implementării Directivei NIS 2, comparând costurile inițiale cu economiile realizate prin reducerea costurilor incidentelor cibernetice;
- Analiza tendințelor bugetare: Examinarea evoluției bugetelor alocate securității cibernetice în perioada pre-NIS 2 și post-NIS 2 poate dezvălui schimbări semnificative în alocarea resurselor financiare;
- Interviuri cu factorii de decizie: Intervievam factorii de decizie și managerii care au autoritate asupra bugetelor pentru a obține perspective despre modul în care au fost luate deciziile în ceea ce privește alocarea resurselor financiare;
- Studii de caz în sectorul sănătății: Cercetam și analizam studiile de caz din sectorul sănătății care au implementat Directivele NIS 2 pentru a evalua impactul financiar al acestor măsuri;
- Analiza costurilor de conformitate pe termen lung: Analizam costurile de conformitate și menținere a măsurilor de securitate pe termen lung, inclusiv cheltuielile continue pentru actualizări, formare și monitorizare.

Ipoteza 3:
Pentru a testa Ipoteza 3, care sugerează că colaborarea activă între organizațiile critice din domeniul sănătății pentru schimbul de informații privind amenințările cibernetice va conduce la

o creștere a rezilienței și a securității cibernetice în sectorul sănătății. În acest sens putem utiliza o serie de instrumente metodologice:

- Interviuri și chestionare: Intervievam reprezentanții organizațiilor critice din domeniul sănătății pentru a evalua nivelul actual de colaborare și schimb de informații cu privire la amenințările cibernetice. Chestionarele pot fi folosite pentru a obține date structurate cu privire la aceste aspecte;
- Analiza de rețea și hărți de contact: Realizam o analiză de rețea pentru a identifica conexiunile existente între organizații. Hărțile de contact pot arăta modul în care organizațiile comunică între ele și cum se desfășoară schimbul de informații;
- Analiza cazurilor de studiu: Studiile de caz pot fi utilizate pentru a evalua modul în care colaborarea a avut impact asupra rezilienței și securității cibernetice în cazuri specifice. Acestea pot oferi exemple concrete de beneficii;
- Evaluarea politicilor și procedurilor de colaborare: Examinarea politicilor și procedurilor existente legate de colaborarea și schimbul de informații pentru a evalua gradul de formalizare și eficacitatea acestora;
- Monitorizarea fluxului de informații: Utilizam instrumente de monitorizare pentru a urmări fluxul de informații și date cu privire la amenințările cibernetice între organizații. Acest lucru ne poate ajuta să evaluam frecvența și relevanța schimbului de informații.
- Evaluarea rezultatelor la nivelul sectorului: Analizam datele și informațiile disponibile pentru a evalua dacă, la nivelul sectorului sănătății, colaborarea a condus la o reducere a incidentelor cibernetice sau la o mai bună pregătire pentru acestea;
- Analiza bugetară: Evaluam resursele financiare alocate colaborării și schimbului de informații și comparam aceste costuri cu beneficiile și rezultatele obținute.

4.3. Interviu cu profesioniști din sănătate despre funcționalitatea SIUI și PIAS în România

Chestionarul de interviu

a) Cunoștințe despre SIUI și PIAS:

- Ce experiență aveți cu utilizarea sistemului unic integrat în sănătate (SIUI) și platformei integrate de asigurări de sănătate (PIAS)?
- Cum considerați că aceste sisteme au influențat gestionarea dosarelor pacientilor și procesul de validare a serviciilor în sectorul sănătății?

b) Eficiența și Accesibilitatea Sistemului:

- Cum apreciați eficiența sistemului SIUI în facilitarea accesului la informații medicale relevante în timp real?
- Există aspecte ale sistemului PIAS care ar putea fi îmbunătățite pentru a crește accesibilitatea și eficiența asigurărilor de sănătate?

c) Beneficiile și provocările implementării:

- Care sunt principalele beneficii pe care le-ați observat ca furnizor de servicii de sănătate datorită implementării SIUI și PIAS?
- Există provocări semnificative în utilizarea acestor sisteme și cum credeți că pot fi abordate?

d) Securitatea datelor și confidențialitatea:

- Cum sunt gestionate aspectele de securitate a datelor și confidențialitate în cadrul sistemului SIUI și PIAS?
- Care sunt măsurile pe care le-ați putea adopta pentru a asigura protecția datelor pacienților în procesul de utilizare a acestor sisteme?

e) Integrarea tehnologiei în practică:

- Cum a influențat integrarea sistemelor informatice sănătatea practicii dumneavoastră cotidiene?
- Considerați că există o nevoie de formare suplimentară pentru a maximiza beneficiile sistemului SIUI și PIAS?

f) Feedback-ul utilizatorilor:

- Ați primit feedback de la pacienți sau colegi cu privire la experiența lor în utilizarea sistemului SIUI sau PIAS? Care au fost principalele aspecte evidențiate?

g) Inovații și actualizări:

- Cum percepeți evoluția acestor sisteme în timp și ați observat îmbunătățiri semnificative de la momentul implementării?
- Există caracteristici sau funcționalități pe care le-ați dori să fie adăugate sau îmbunătățite în viitor?

h) Colaborarea interprofesională:

- Cum a facilitat sistemul SIUI și PIAS colaborarea între profesioniștii din domeniul sănătății, precum și între aceștia și instituțiile de asigurări de sănătate?

i) Perspective asupra viitorului:

- Care sunt așteptările dumneavoastră cu privire la evoluția sistemelor informatice în domeniul sănătății în România în următorii ani?
- Cum credeți că aceste sisteme ar putea contribui la îmbunătățirea generală a sistemului de sănătate?

Sistemul Unic Integrat în Sănătate (SIUI) și Platforma Informatică a Asigurărilor de Sănătate (PIAS) joacă un rol central în digitalizarea și eficientizarea sectorului sanitar din România. Pentru a înțelege mai bine impactul acestor sisteme asupra activității zilnice a profesioniștilor din sănătate, s-a realizat un interviu cu aproximativ 30 de specialiști din domeniu. Rezultatele acestui studiu oferă o perspectivă detaliată asupra beneficiilor, provocărilor și oportunităților de îmbunătățire asociate utilizării acestor platforme informatice.

În cadrul acestui demers, respondenții au oferit informații valoroase despre experiența lor cu SIUI și PIAS, evaluând aspecte precum eficiența sistemelor, accesibilitatea datelor, securitatea informațiilor, integrarea tehnologiei în practica zilnică și impactul asupra colaborării interprofesionale. De asemenea, au fost identificate provocări specifice legate de utilizarea acestor platforme și direcțiile de dezvoltare necesare pentru creșterea eficienței și siguranței în sectorul sanitar.

Analiza calitativă a răspunsurilor a fost structurată pe mai multe teme, inclusiv gradul de cunoaștere a SIUI și PIAS, eficiența și accesibilitatea sistemelor, beneficiile și dificultățile implementării, precum și perspectivele asupra viitorului digitalizării în sănătate. Aceste rezultate evidențiază atât progresul realizat, cât și oportunitățile de perfecționare a acestor platforme pentru a răspunde mai bine nevoilor utilizatorilor.

1. Cunoștințe despre SIUI și PIAS

Profesioniștii din sănătate intervievați au descris experiențe extinse cu utilizarea sistemului SIUI și a platformei PIAS. În general, aceștia consideră că sistemele au avut un impact pozitiv asupra modului de gestionare a dosarelor pacienților, facilitând accesul rapid la informații esențiale și simplificând procesul de validare a serviciilor medicale. Totuși, au fost evidențiate și provocări, cum ar fi complexitatea utilizării pentru anumite funcționalități.

2. Eficiența și Accesibilitatea Sistemului

Respondenții au evidențiat că SIUI are potențialul de a oferi acces în timp real la date medicale relevante, însă uneori întâmpină dificultăți tehnice care afectează eficiența sistemului. În ceea ce privește PIAS, participanții au menționat că există oportunități de îmbunătățire, în special în privința interfeței și a accesibilității datelor.

3. Beneficiile și Provocările Implementării
Beneficiile recunoscute de participanți includ accesul rapid la informațiile pacienților și îmbunătățirea gestionării dosarelor medicale. Totuși, provocările frecvent menționate au fost legate de probleme tehnice recurente și de necesitatea unei instruiri mai bune pentru utilizatori, astfel încât să poată exploata pe deplin funcționalitățile sistemelor.

4. Securitatea Datelor și Confidențialitatea
Majoritatea intervievaților au exprimat încredere în măsurile de securitate ale SIUI și PIAS, dar au subliniat necesitatea implementării unor soluții mai robuste pentru protejarea datelor pacienților. Printre sugestii se numără actualizări regulate de securitate și programe de formare continuă pentru personal.

5. Integrarea Tehnologiei în Practică
Integrarea acestor platforme informatice a fost percepută ca un factor transformator în practica zilnică, contribuind la creșterea eficienței și la îmbunătățirea fluxurilor de lucru. Cu toate acestea, respondenții au remarcat că o formare suplimentară ar putea amplifica semnificativ beneficiile sistemelor.

6. Feedback-ul Utilizatorilor
Interlocutorii au raportat un feedback pozitiv din partea pacienților și colegilor, care au apreciat accesibilitatea crescută a datelor și îmbunătățirea comunicării între diferite entități medicale. Totuși, s-au remarcat și nemulțumiri legate de erorile tehnice ocazionale.

7. Inovații și Actualizări
Deși unii participanți au observat progrese în evoluția SIUI și PIAS, majoritatea au exprimat dorința de a vedea îmbunătățiri mai consistente. S-a accentuat necesitatea unor interfețe mai intuitive și a unor funcționalități suplimentare care să răspundă mai bine nevoilor utilizatorilor.

8. Colaborarea Interprofesională
Sistemele informatice au fost apreciate pentru rolul lor în facilitarea colaborării între profesioniști și instituții, însă unii respondenți au evidențiat că acest aspect ar putea fi îmbunătățit prin integrarea unor funcții care să susțină mai bine comunicarea interprofesională.

9. Perspective asupra Viitorului
Participanții au manifestat optimism în ceea ce privește viitorul digitalizării în sănătate, subliniind potențialul acestor sisteme de a contribui la creșterea eficienței și securității în sectorul sanitar. Totodată, au accentuat importanța implicării continue a utilizatorilor în procesul de dezvoltare și actualizare a platformelor.
Aceste statistici reflectă percepțiile și experiențele profesioniștilor din sănătate privind SIUI și PIAS, evidențiind atât beneficiile, cât și provocările acestor sisteme, precum și direcțiile de îmbunătățire necesare pentru a spori eficiența și securitatea în sectorul sanitar din România.

Pentru a obține o imagine mai cuprinzătoare asupra implementării Directivei NIS 2 în sănătate, am decis să extindem metodologia utilizată. Dacă inițial datele calitative au fost colectate prin interviuri cu factori de decizie și experți din domeniu, acestea au fost completate cu un sondaj de opinie cantitativ. Scopul a fost de a evalua percepțiile și nivelul de pregătire al profesioniștilor din sănătate în fața cerințelor Directivei NIS 2.

Interviurile ne-au oferit informații detaliate despre provocările și oportunitățile asociate cu această directivă, dar pentru a verifica dacă aceste perspective sunt reprezentative pentru o populație mai

largă, a fost necesar un chestionar structurat. Astfel, am conceput un sondaj care să includă atât întrebări generale, cât și specifice, acoperind domenii precum familiarizarea cu directiva, provocările anticipate, măsurile necesare și impactul asupra activității.

Chestionarul a fost aplicat unui eșantion de 384 de respondenți, reprezentativ pentru sectorul sănătății din România. Întrebările utilizate în sondaj sunt prezentate mai jos.

Chestionarul de sondaj

1. Sondaj de opinie – implementarea Directivei NIS 2 în sănătate:
Cât de familiarizat(ă) sunteți cu Directivei NIS 2 și impactul său asupra infrastructurii din sănătate?
Foarte familiarizat(ă), Familiarizat(ă), Nici familiarizat(ă), nici necunoscut(ă), Necunoscut(ă)

2. Considerați că implementarea Directivei NIS 2 este esențială pentru securitatea infrastructurii din sănătate?
Da, Nu, Nu știu / Nu am o opinie

3. Ați participat la sesiuni de formare sau instruire referitoare la Directivei NIS 2 în ultimul an?
Da, Nu, Nu știu / Nu am o opinie

4. Care credeți că sunt cele mai mari provocări în implementarea Directivei NIS 2 în infrastructura din sănătate? (Puteți selecta mai multe răspunsuri)
- Resurse financiare limitate,
- Lipsa expertizei tehnice,
- Rezistența la schimbare în organizații,
- Compromisuri privind confidențialitatea datelor pacienților,
- Necesitatea actualizării tehnologice,
- Altele (specifică)

5. Cât de pregătit(ă) simțiți că este echipa dumneavoastră în privința implementării Directivei NIS 2?
Foarte pregătit(ă), Pregătit(ă), Nici pregătit(ă), nici nepregătit(ă), Nepregătit(ă)

6. Ce măsuri credeți că ar trebui luate pentru a sprijini profesioniștii din sănătate în procesul de implementare a Directivei NIS 2?
Raspuns scurt:……..

7. Ați întâmpinat dificultăți în colaborarea cu alte entități din sistemul de sănătate în ceea ce privește implementarea Directivei NIS 2?
Da, Nu, Nu știu / Nu am o opinie

8. Cât de transparent considerați că este procesul de implementare a Directivei NIS 2 în organizația dumneavoastră?
Foarte transparent, Transparent, Nici transparent, nici opac, Opac

9. Credeți că implementarea Directivei NIS 2 va avea un impact semnificativ asupra eficienței serviciilor de sănătate?
Da, Nu, Nu știu / Nu am o opinie

10. Ați identificat posibile vulnerabilități în infrastructura din sănătate care ar necesita o atenție sporită în cadrul implementării Directivei NIS 2?
Raspuns scurt:……..

11. Care este nivelul dvs. de încredere în măsurile de securitate cibernetică existente în infrastructura de sănătate a organizației dumneavoastră?

Foarte înalt, Înalt, Nici înalt, nici scăzut, Scăzut, Foarte scăzut

12. Ați observat o creștere a incidentelor de securitate cibernetică în ultimul an în cadrul organizației dumneavoastră?

Da, Nu, Nu știu / Nu am o opinie

13. Credeți că implementarea Directivei NIS 2 va afecta eficacitatea serviciilor medicale acordate pacienților?

Da, Nu, Nu știu / Nu am o opinie

14. Cum apreciați nivelul de colaborare între sectorul public și privat în implementarea Directivei NIS 2 în sănătate?

Foarte bun, Bun, Nici bun, nici rău, Rău, Foarte rău

15. Ați fost consultat(ă) în procesul de luare a deciziilor legate de implementarea Directivei NIS 2 în organizația dumneavoastră?

Da, Nu, Nu știu / Nu am o opinie

16. Cât de bine considerați că este comunicată importanța securității cibernetice în sănătate în rândul personalului medical și administrativ?

Foarte bun, Bun, Nici bun, nici rău, Rău, Foarte rău

17. Credeți că autoritățile publice oferă suficiente resurse și sprijin pentru implementarea Directivei NIS 2 în sectorul sănătății?

Da, Nu, Nu știu / Nu am o opinie

18. Care sunt, în opinia dumneavoastră, cele mai mari beneficii ale implementării Directivei NIS 2 în sănătate?
Raspuns scurt:……..

19. Ați fost implicat(ă) în procesul de evaluare a riscurilor asociate cu implementarea Directivei NIS 2 în organizația dumneavoastră?

Da, Nu, Nu știu / Nu am o opinie

20. Ce măsuri considerați că ar trebui luate pentru a asigura securitatea datelor pacienților în contextul implementării Directivei NIS 2?
Raspuns scurt:……..

21. Ați observat schimbări semnificative în politicile de securitate cibernetică ale organizației dumneavoastră în urma Directivei NIS 2?

Da, Nu, Nu știu / Nu am o opinie

22. Cum apreciați gradul de conștientizare a personalului în ceea ce privește riscurile cibernetice în organizația dumneavoastră?

Foarte înalt, Înalt, Nici înalt, nici scăzut, Scăzut, Foarte scăzut

23. Credeți că infrastructura din sănătate este pregătită să facă față amenințărilor cibernetice emergente?

Da, Nu, Nu știu / Nu am o opinie

24. Care sunt principalele schimbări pe care ați dori să le vedeți în strategiile de securitate cibernetică în sănătate pentru a face față mai bine amenințărilor?
Raspuns scurt:……..

25. Ce sugestii aveți pentru îmbunătățirea procesului de implementare a Directivei NIS 2 în infrastructura de sănătate?
Raspuns scurt:……..

Calculul dimensiunii eșantionului (numărul de participanți) necesar pentru un sondaj depinde de mai mulți factori, având în vedere că N=60,000 (mărimea populației estimată a profesioniștilor din sănătate în România) , rezulta un eșantion de aproximativ n =384 profesionisti din sanatate sa raspunda la toate intrebarile din chestionar, pentru un nivel de încredere de 95%.

În urma sondajului de opinie la care au participat 384 de profesioniști din domeniul sănătății, s-au conturat câteva concluzii esențiale privind implementarea Directivei NIS 2 în infrastructura critică din sănătate.

În această continuare, se vor prezenta concluziile generale obținute în urma analizei cantitative a răspunsurilor colectate prin sondajul de opinie aplicat unui eșantion reprezentativ de 384 de profesioniști din domeniul sănătății. Analiza acestor date ne oferă o imagine clară asupra percepției și pregătirii sectorului sanitar din România în privința implementării Directivei NIS 2, evidențiind principalele provocări, măsurile necesare și impactul perceput asupra securității infrastructurii critice din sănătate. Prin urmare, concluziile vor reflecta atât aspectele pozitive identificate, cât și domeniile care necesită îmbunătățiri, având în vedere contextul specific al cerințelor Directivei NIS 2 și al implementării acesteia în sectorul sanitar.

Concluziile generale în urma analizării răspunsurilor primite de la respondenți:

- Familiarizarea cu Directiva NIS 2 și impactul său: Majoritatea respondenților nu sunt familiarizați cu Directiva NIS 2, dar recunosc impactul său semnificativ asupra infrastructurii din sănătate;
- Esențialitatea implementării Directivei NIS 2: Profesioniștii din sănătate consideră aproape unanim că implementarea Directivei NIS 2 este esențială pentru securitatea infrastructurii din sănătate, evidențiind importanța protecției datelor sensibile și a continuității operaționale;
- Provocările în implementare: Printre cele mai mari provocări identificate se numără resursele financiare limitate, lipsa expertizei tehnice și rezistența la schimbare. Aceste aspecte trebuie adresate prin alocarea de fonduri adecvate și prin programe de formare și educare a personalului;
- Pregătirea echipei și măsuri de sprijin: Respondenții au indicat că echipele lor sunt în general bine pregătite pentru implementarea Directivei NIS 2, dar au subliniat necesitatea unor măsuri suplimentare de sprijin, cum ar fi sesiuni de formare continuă și actualizări tehnologice;
- Colaborarea și transparența: Colaborarea cu alte entități din sistemul de sănătate și transparența procesului de implementare sunt considerate bune, dar există loc de îmbunătățire. O comunicare mai eficientă între sectorul public și privat ar putea optimiza implementarea Directivei NIS 2;
- Impactul asupra eficienței și serviciilor medicale: Implementarea Directivei NIS 2 este percepută ca având un impact pozitiv asupra eficienței serviciilor de sănătate și asupra calității îngrijirilor acordate pacienților, prin reducerea incidentelor cibernetice și îmbunătățirea managementului datelor;
- Încrederea în măsurile de securitate: Nivelul de încredere în măsurile de securitate cibernetică existente este în general ridicat, dar profesioniștii sunt conștienți de necesitatea continuării eforturilor pentru îmbunătățirea politicilor de securitate și adaptarea lor la amenințările emergente;

- Eficacitatea măsurilor și pregătirea infrastructurii: Măsurile de securitate implementate sunt considerate eficiente, iar infrastructura din sănătate este percepută ca fiind pregătită să facă față amenințărilor cibernetice emergente. Cu toate acestea, este necesară o evaluare continuă a riscurilor și actualizarea periodică a strategiilor de securitate;
- Sugestii pentru îmbunătățire: Profesioniștii au sugerat mai multe măsuri pentru îmbunătățirea procesului de implementare a Directivei NIS 2, inclusiv creșterea finanțării pentru tehnologia de securitate, intensificarea formării personalului și îmbunătățirea colaborării interinstituționale.

Aceste concluzii reflectă o percepție pozitivă asupra impactului Directivei NIS 2 și subliniază necesitatea unor eforturi continue și coordonate pentru a asigura o implementare eficientă și durabilă în sectorul sănătății din România.

4.4. Discuții și concluzii finale

Sistemul de sănătate din România traversează o perioadă de transformare digitală profundă, necesară pentru a răspunde provocărilor contemporane și a se alinia cerințelor Uniunii Europene în materie de securitate cibernetică și eficiență operațională. Directiva NIS 2, adoptată ca parte a unei strategii europene unitare de securitate, impune standarde înalte pentru infrastructurile critice, inclusiv cele din domeniul sănătății, subliniind importanța protecției datelor sensibile și a continuității serviciilor esențiale.

În acest context, Platforma Informatică a Asigurărilor de Sănătate (PIAS)/e-Sănătate și Sistemul Informatic Unic Integrat (SIUI) reprezintă piloni ai infrastructurii digitale din sănătate, dar limitările lor actuale subliniază necesitatea unei platforme noi și integrate, care să adreseze atât funcționalitățile de bază, cât și cerințele impuse de Directiva NIS 2. Această platformă ar trebui să asigure eficiență, interoperabilitate și securitate sporită, contribuind la transformarea sistemului sanitar într-un ecosistem rezilient și performant.

Scopul acestui capitol este de a analiza concluziile generale obținute în urma unui sondaj reprezentativ și de a evidenția aspectele critice și oportunitățile asociate cu digitalizarea sănătății în România, precum și cu implementarea Directivei NIS 2. Printr-o abordare academică riguroasă, vom explora atât perspectivele profesioniștilor din sănătate, cât și măsurile necesare pentru îmbunătățirea infrastructurii digitale și a securității cibernetice.

Implementarea Directivei NIS 2 în sectorul sănătății din România relevă o serie de provocări și oportunități care trebuie abordate strategic pentru a maximiza beneficiile digitalizării.

1. Complexitatea infrastructurii și necesitatea modernizării
Sistemele informatice existente, precum PIAS/e-Sănătate, au jucat un rol esențial în digitalizarea inițială a sănătății, însă lipsa de interoperabilitate, redundanțele și limitările tehnologice actuale subliniază necesitatea unei platforme noi, mai scalabile și mai flexibile. Această platformă trebuie să integreze funcționalitățile existente și să permită extinderea pentru a răspunde cerințelor viitoare.

2. Directiva NIS 2 – catalizator pentru schimbare
Directiva NIS 2 aduce standarde clare și riguroase privind securitatea cibernetică, fiind atât un imperativ legal, cât și o oportunitate strategică. Cerințele privind evaluarea riscurilor, protecția infrastructurilor critice și raportarea incidentelor impun o reevaluare fundamentală a modului în care sunt gestionate datele și procesele în sănătate.

3. Educația digitală și conștientizarea riscurilor

Un obstacol major identificat îl reprezintă competențele digitale scăzute ale personalului medical și administrativ. Lipsa unei educații adecvate în domeniul securității cibernetice și al utilizării platformelor informatice accentuează vulnerabilitățile. Este imperativ ca programele de formare să fie intensificate, iar conștientizarea riscurilor să fie o prioritate în rândul tuturor utilizatorilor.

4. Impactul asupra serviciilor medicale
Digitalizarea, sprijinită de cerințele Directivei NIS 2, promite să îmbunătățească semnificativ accesibilitatea și calitatea serviciilor medicale. Introducerea dosarului electronic de sănătate, telemedicina și integrarea datelor din diverse surse vor contribui la optimizarea resurselor și la o mai bună coordonare între furnizorii de servicii medicale.

5. Colaborare interinstituțională și parteneriate public-private
Implementarea Directivei NIS 2 nu poate fi realizată în izolare. Colaborarea între instituțiile publice și private, schimbul de bune practici cu alte state membre și implicarea companiilor de tehnologie vor fi esențiale pentru crearea unui sistem digital de sănătate robust și eficient.

6. Perspective asupra viitorului
Digitalizarea sănătății și conformarea la cerințele Directivei NIS 2 oferă României oportunitatea de a se poziționa ca un lider regional în inovarea sanitară. Investițiile în tehnologii emergente, cum ar fi inteligența artificială și analiza predictivă, pot transforma modul în care sunt furnizate serviciile medicale, contribuind la un sistem mai rezilient și orientat către pacient.

Digitalizarea sistemului de sănătate din România, susținută de implementarea Directivei NIS 2, este esențială pentru modernizarea infrastructurii și asigurarea unor servicii medicale de calitate. Crearea unei noi platforme informatice integrate, care să răspundă atât nevoilor operaționale, cât și cerințelor de securitate, reprezintă un pas crucial.

Provocările, cum ar fi lipsa de resurse, competențele limitate și rezistența la schimbare, pot fi depășite prin alocarea de fonduri adecvate, programe de formare și o colaborare eficientă între toate părțile implicate. În același timp, oportunitățile oferite de tehnologiile emergente, interoperabilitatea extinsă și o mai bună securitate cibernetică vor contribui la crearea unui sistem sanitar rezilient, eficient și sigur.

Prin implementarea Directivei NIS 2 și modernizarea infrastructurii informatice, România nu doar că își va îmbunătăți sistemul de sănătate, ci va demonstra capacitatea de a răspunde provocărilor cibernetice contemporane, consolidând încrederea cetățenilor și a partenerilor europeni.

Referințe bibliografice

[1] A. Grigorescu, D. Baiasu e I. C. Razvan , «Business Intelligence, the New Managerial Tool: Opportunities and Limits,» en *"Ovidius" University Annals, Economic Sciences Series*, 2020.

[2] CNAS, «Sistemul Informatic Unic Integrat + Prescripţia Electronică + Cardul Electronic de Asigurări de Sănătate,» Casa Naţională de Asigurări de Sănătate din România, București, 2021.

[3] U. Europeană, «DIRECTIVA (UE) 2022/2555 A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI din 14 decembrie 2022 privind securitatea rețelelor și a sistemelor informatice,» Parlamentul European, Bruxelles, 2022.

[4] Parlamentul European, «Directiva (UE) 2016/1148 privind securitatea rețelelor și sistemelor informatice,» 2016.

[5] DNSC, «Despre DNSC,» Directoratul Național de Securitate Cibernetică, fără an.

[6] C. Vrabie, AI: de la idee la implementare. Traseul sinuos al Inteligenţei Artificiale către maturitate, București: Pro Universitaria Publishing House, 2024.

[7] C. Vrabie e E. Dumitrascu, Smart Cities. De la Idee la implementare sau despre cum tehnologia poate da stralucire mediului urban, Universul Academic Publishing house & Universitara Publishing house, 2018.

[8] I. B. Berceanu e C. E. Nicolescu, «Collaborative Public Administration—A Dimension of Sustainable Development: Exploratory Study on Local Authorities in Romania,» 2024.

[9] C. Vrabie, Elemente de E-Guvernare, București: Pro Universitaria Publishing House, 2024.

[10] C. Vrabie, Elemente de IT pentru Administraţia Publică, București: Pro Universitaria Publishing House.

[11] V. Baltac, Lumea Digitala. Concepte Esentiale, București: Editura: EXCEL XXI BOOKS, 2015.

[12] V. Baltac, Mituri si realitate in lumea digitala. Blog, comentarii eseuri., București: EXCEL XXI BOOKS, 2016.

[13] G.-L. Popa , «Risk management, protection, and security of personal data in Romania,» en *International Conference on Machine Intelligence & Security for Smart Cities (TRUST) Proceedings*, 2024.

[14] C. Vrabie, Explorarea campaniei de prevenire a criminalității cibernetice pe Twitter: dovezi de la guvernul indonezian, vol. Vol. 7, SCRD, 2023a, p. 9–24.

[15] C. Vrabie, «O operatiune cu stil – The Flame,» *Smart Cities International Conference (SCIC) Proceedings*, vol. 5, pp. 161-172, 2017.

[16] C. Vrabie, «Convergenta securitatii digitale,» en *Smart Cities International Conference (SCIC) Proceedings*, 2023b.

[17] C. Vrabie, «Libertatea ta incepe unde se termina intimitatea mea,» *Smart Cities International Conference (SCIC) Proceedings*, vol. 4, pp. 135-147, 2016.

[18] C. SICLOVAN, «The role of NHIH in the digitalization of health, smart citycondition,» en *Smart Cities International Conference (SCIC) Proceedings 11, (Jun. 2024),*, 2024.

[19] C. SICLOVAN, «Rolul CNAS în digitalizarea sănătății, condiție smart city,» en *Smart Cities International Conference (SCIC) Proceedings. 11, (Jun. 2024)*, 2024.

[20] L.-F. BUTNARIU (BADEA), «Rolul IoT in dezvoltarea administratiei publice. Administratia 2.0,» en *Smart Cities International Conference (SCIC) Proceedings. 9, (Apr. 2023)*, 2023.

[21] L.-F. BADEA (BUTNARIU), «Utilizarea Sase Sigma in administratia publica,» en *Smart Cities International Conference (SCIC) Proceedings. 8, (Apr. 2023)*, 2023.

[22] N. D. Badea, «Perspectives and implications in the use of artificial intelligence in healthcare,» en *SMART CITIES: Sustainability and Innovation*, 2023.

[23] R. DAMASCHIN e M. and MIHĂILĂ, «Digitalizarea administratiei publice din Romania in raport cu tendintele europene.,» en *Smart Cities International Conference (SCIC) Proceedings 8, (Apr. 2023)*, 2023.

[24] C. MANDA , «Digitalizarea administratiei publice din Romania – intre nevoile si aspiratiile unei societati moderne a secolului XXI,» en *Smart Cities International Conference (SCIC) Proceedings. 9, (Apr. 2023)*, 2023.

[25] M. DUMITRAȘCO , «Critical aspects of health security of the Republic of Moldova compared to eastern European countries, in the context of the COVID-19 pandemic,» en *Smart Cities International Conference (SCIC) Proceedings. 9, (Apr. 2023)*, 2023..

[26] ICI București, «Cercetări privind standardizarea și interoperabilitatea în domeniul soluțiilor e-Health," Raport de cercetare etapa 2/2016,» 2016.

[27] ISO, «ISO 27005 Riscul de securitate a informațiilor».

[28] R. CHIȚESCU, «Managementul Proiectelor: Suport de Curs,» 2022.

[29] . A. Dumitrescu, Mapping the Audit Work. Standards in Internal Audit Practice, Bucuresti, 2019.

[30] C. Vrabie, «Artificial Intelligence Promises to Public Organizations and Smart Cities.,» *Digital Transformation. Lecture Notes in Business Information Processing*, vol. 465, 8 12 2022.

[31] V. Baltac, «Smart cities—A view of societal aspects,» *Smart Cities*, vol. 2, nr 4, 2019.

[32] C. Vrabie, «E-Government 3.0: An AI Model to Use for Enhanced Local Democracies,» *Sustainability*, 2023.

[33] M. Tegmark, Life 3.0: Being Human in the Age of Artificial Intelligence, Penguin books, 2017.

[34] A. F. RAHMAT, C. VRABIE e G. B. SOESILO, «Exploring the Cybercrime Prevention Campaign on Twitter: Evidence from the Indonesian Government,» *SCRD*, vol. 7, nr 2, p. 9–24, 2023.

[35] C. Vrabie, «Convergenta securitatii digitale,» *Smart Cities International Conference (SCIC) Proceeding*, vol. 3, pp. 267-277, 2015.