Cofinanțat de Uniunea Europeană

AGENȚIA NAȚIONALĂ PENTRU SPORT

Nr. înregistrare: 4985/ 29.04.2026

Aprob,
Președinte
Constantin-Bogdan MATEI

CAIET DE SARCINI

PENTRU ACHIZIȚIA DE

„SERVICII INTEGRATE DE DEZVOLTARE PLATFORMĂ INFORMATICĂ”

ÎN CADRUL PROIECTULUI

“PORTALUL SPORTULUI ROMÂNESC - DIGITALIZAREA SERVICIILOR PUBLICE ALE AGENȚIEI NAȚIONALE PENTRU SPORT„

Sursa de finanțare:

PROGRAMUL CREȘTERE INTELIGENȚA, DIGITALIZARE ȘI INSTRUMENTE FINANCIARE 2021-2027
PRIORITATE: P2 DIGITALIZARE ÎN ADMINISTRAȚIA PUBLICĂ CENTRALĂ ȘI MEDIUL DE AFACERI
OBIECTIV SPECIFIC: VALORIFICAREA AVANTAJELOR DIGITALIZĂRII, ÎN BENEFICIUL CETĂȚENILOR, AL COMPANIILOR, AL ORGANIZAȚIILOR DE CERCETARE ȘI AL AUTORITĂȚILOR PUBLICE
ACȚIUNEA 2.2 E-GUVERNAREA ȘI DIGITALIZAREA ÎN BENEFICIUL CETĂȚENILOR
2.2.1: E-GUV ÎN ADMINISTRAȚIA/INSTITUȚIILE PUBLICE
MĂSURA 1: SERVICII PUBLICE DESTINATE CETĂȚENILOR ȘI/SAU FIRMELOR IDENTIFICATE ÎN CSP GESTIONAT DE ADR ȘI/SAU ÎN CONCORDANȚA CU POLITICA E-GUV
APEL DE PROIECTE: 1
COD MYSMIS2021/SMIS2021+:339169;

Cod CPV Principal:
72200000-7: Servicii de programare si de consultanta software (Rev.2)

Coduri CPV Secundare:
48000000-8: Pachete software și sisteme informatice
30211300-4: Platforme informatice
72265000-0: Servicii de configurare de software
72228000-9: Servicii de dezvoltare de software pentru copii de siguranță (backup) sau recuperare
72227000-2: Servicii de consultanta privind integrarea software (Rev.2)
72268000-1: Servicii de furnizare de software (Rev.2)
48211000-0: Pachete software de interconectare de platforme (Rev.2)
72252000-6: - Servicii de arhivare computerizată (Rev.2)
79995100-6: – Servicii de arhivare (Rev. 2)
48300000-1: Pachete software pentru creare de documente, pentru desen, imagistică, planificare și productivitate
80533100-0: Servicii de formare în informatică
30213300-8: Computer de birou
30213200-7: Tablet PC (Rev.2)
30232110-8: - Imprimante laser
30216110-0: Scanere informatice

CUPRINS

1 Introducere

Această secțiune a Documentației de Atribuire include ansamblul cerințelor pe baza cărora fiecare Ofertant va elabora Oferta (Propunerea Tehnică și Propunerea Financiară) pentru prestarea serviciilor și furnizarea produselor care fac obiectul Contractului ce rezultă din această procedură.

În cadrul acestei proceduri **Agenția Națională pentru Sport (denumită în continuare ANS)** îndeplinește **rolul de Autoritate Contractantă**, respectiv Achizitor în cadrul Contractului.

Pentru scopul prezentei secțiuni a Documentației de Atribuire, orice activitate descrisă într-un anumit capitol din Caietul de Sarcini și nespecificată explicit în alt capitol, trebuie interpretată ca fiind menționată în toate capitolele unde se consideră de către Ofertant că aceasta trebuia menționată pentru asigurarea îndeplinirii obiectului Contractului.

***Cerințele impuse vor fi considerate ca fiind minimale**. Vor fi luate în considerare toate ofertele care îndeplinesc cel puțin cerințele minime din acest caiet de sarcini.*

Oferta ce conține servicii/produse inferioare celor prevăzute în caietul de sarcini sau care nu satisfac cerințele caietului de sarcini va fi declarată ofertă neconformă și va fi respinsă.

Specificațiile tehnice cuprinse în Caietul de sarcini care indică o anumită origine, sursă, producție, un procedeu special, o marcă de fabrică sau de comerț, un brevet de invenție, o licență de fabricație sunt menționate doar pentru identificarea cu ușurință a tipului de produs și NU au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor produse. Aceste specificații vor fi considerate ca având mențiunea "SAU ECHIVALENT".

Sunt acceptate produse cu specificații tehnice superioare celor minime obligatorii.

2 Contextul realizării acestei achiziții

2.1 Informații despre Autoritatea Contractantă

Tabel 1- Informații despre Autoritatea Contractantă

Nr.	Informație	Detaliere
1.	Denumire Organizație	Agenția Națională pentru Sport
2.	Tipul Organizației	Instituție publică, cu personalitate juridică, în subordinea Guvernului și în coordonarea prim-ministrului
3.	Cod de înregistrare fiscală/CIF:	26604620
4.	Adresa poștală:	Str. Vasile Conta, Nr.16, Sector 2, Municipiul București, Cod poștal 020954, cod NUTS: RO321, România
5.	Telefon/Fax:	+40 0213189000
6.	Adresa e-mail:	registratura@sport.gov.ro
7.	Pagina Web:	https://sport.gov.ro/

Agenția Națională pentru Sport (**ANS)** a fost înființată în iunie 2023, prin O.U.G. nr. 59/2023, publicată în Monitorul Oficial la 15.06.2023, preluând atribuțiile, patrimoniul și personalul fostului Minister al Sportului, care a fost desființat. ANS funcționează în subordinea Guvernului și coordonarea Prim-ministrului, fiind condusă de un președinte cu rang de secretar de stat.

Aceasta funcționează ca instituție publică cu personalitate juridică, subordonată Guvernului și coordonată de prim-ministru, având ca principală responsabilitate implementarea strategiilor și politicilor guvernamentale în domeniul sportului.

ANS a preluat toate activitățile, personalul și patrimoniul fostului Minister al Sportului, asigurând continuitatea administrativă și operațională. Instituția este condusă de un președinte cu rang de secretar de stat și doi vicepreședinți cu rang de subsecretar de stat, numiți și eliberați din funcție prin decizie a prim-ministrului.

2.2 Informații despre contextul care a determinat achiziționarea serviciilor

Prezenta achiziție se realizează în contextul implementării de către **Agenția Națională pentru Sport**, a proiectului: **“PORTALUL SPORTULUI ROMÂNESC - DIGITALIZAREA SERVICIILOR PUBLICE ALE AGENȚIEI NAȚIONALE PENTRU SPORT„,** finanțat prin Programul Creștere Inteligența, Digitalizare Și Instrumente Financiare 2021-2027, PRIORITATE: P2 DIGITALIZARE ÎN ADMINISTRAȚIA PUBLICĂ CENTRALĂ ȘI MEDIUL DE AFACERI, OBIECTIV SPECIFIC: VALORIFICAREA AVANTAJELOR DIGITALIZĂRII, ÎN BENEFICIUL CETĂȚENILOR, AL COMPANIILOR, AL ORGANIZAȚIILOR DE CERCETARE ȘI AL AUTORITĂȚILOR PUBLICE, ACȚIUNEA 2.2 E-GUVERNAREA ȘI DIGITALIZAREA ÎN BENEFICIUL CETĂȚENILOR - 2.2.1: E-GUV ÎN ADMINISTRAȚIA/INSTITUȚIILE PUBLICE, MĂSURA 1: SERVICII PUBLICE

DESTINATE CETĂȚENILOR ȘI/SAU FIRMELOR IDENTIFICATE ÎN CSP GESTIONAT DE ADR ȘI/SAU ÎN CONCORDANȚA CU POLITICA EGUV, APEL DE PROIECTE: 1, COD MYSMIS2021/SMIS2021+:339169.

Beneficiarul investiției: Agenția Națională pentru Sport.

2.3 Prezentarea contextului

Agenția Națională pentru Sport își propune să inițieze un proiect ambițios de digitalizare a serviciilor publice oferite federațiilor, cluburilor și sportivilor, precum și altor tipuri de beneficiari ai serviciilor acestora. Acest proiect este parte din efortul pentru alinierea României la tendințele europene și globale de digitalizare, care promovează eficiența, transparența și accesibilitatea serviciilor publice. Digitalizarea administrației publice nu numai că va îmbunătăți calitatea serviciilor oferite, dar va contribui și la creșterea competitivității economice și la integrarea României în economia digitală globală.

2.4 ANS - Profil organizațional

Competența și atribuțiile sunt stabilite prin OUG 57/2019 privind Codul administrativ, cu modificările și completările ulterioare, ale Legii 69/2000 a educației fizice și sportului cu modificările și completările ulterioare, HG 576/2023 privind organizarea, funcționarea și atribuției Agenției Naționale pentru Sport.

Principalele atribuții:

- asigură elaborarea strategiei de punere în aplicare a Programului de guvernare în domeniul sportului;
- fundamentează și propune Guvernului politici în domeniul sportului;
- inițiază, elaborează, avizează proiecte de acte normative în vederea realizării obiectivelor strategice și a politicilor în domeniul sportului;
- asigură, în numele statului român, reprezentarea pe plan intern și internațional în domeniul sportului;
- asigură urmărirea aplicării si controlului legilor si a celorlalte acte normative din domeniul sportului;
- elaborează si susține strategia generala a organizării si dezvoltării activității sportive si reprezintă interesele statului in raport cu federațiile sportive naționale;
- organizează, potrivit legii, formarea, pregătirea profesionala si perfecționarea specialiștilor din domeniul sportului, conlucrând in acest scop cu instituțiile si organismele de specialitate din tara si din străinătate;
- sprijină organizarea si promovarea cercetării științifice si asistentei medicale in domeniul sportiv;
- repartizează bugetul alocat activității sportive pentru activitatea baza contractelor de finanțare a obiectivelor si programelor sportive ale acestora si internaționale oficiale, pe baza aprobării date de Secretariatul General al Guvernului.

In domeniul absorbției fondurilor europene si internaționale:

- asigura absorbția fondurilor europene in domeniul sportului;

- accesează fonduri structurale si de investiții europene destinate susținerii politicilor de coeziune in domeniul sportului, cu respectarea metodologiei specifice, in calitate de gestionar, beneficiar si partener;
- conlucrează cu Agenția Națională pentru Programe Comunitare in Domeniul Educației si Formarii Profesionale, in vederea realizării obiectivelor din domeniul sportului.

In subordinea ANS își desfășoară activitatea următoarele instituții publice finanțate din venituri proprii și subvenții acordate de la bugetul de stat:

1. Direcții județene pentru Sport și a Municipiului București - 42 unități;
2. Cluburi sportive - 48 unități;
3. Complexuri sportive naționale - 11 unități;
4. Institutul Național de Cercetare pentru Sport;
5. Centru Național de Formare și Perfecționare a Antrenorilor;
6. Galeria Marilor Sportivi.

În conformitate cu prevederile legale ANS finanțează în cadrul programelor aprobate și structuri sportive de drept privat, respectiv federații sportive naționale, prin contract anual de finanțare încheiat cu fiecare federație sportivă națională care a îndeplinit condițiile de eligibilitate și în conformitate cu criteriile de finanțare.

Strategia Națională pentru Sport 2022-2032 reprezintă documentul cadru care stabilește viziunea și direcțiile majore de dezvoltare, prin coagularea tuturor eforturilor, resurselor și acțiunilor întreprinse. Procesul de implementare va avea un caracter organic, dinamic și adaptat, în funcție de evoluția mediului extern, precum și a factorilor implicați.

Printre cele 70 de Obiective Strategice pentru Sportul din România, care trebuie implementate în decurs de 10 ani, menționăm:

- Prioritizarea sporturilor olimpice de tradiție, care au adus performanțe României;
- Crearea unui sistem sportiv piramidal transparent, predictibil, axat în special pe aceste sporturi prioritare;
- Descentralizarea structurilor și bazelor sportive din structurile de stat;
- Finanțarea federațiilor prioritare în baza unor strategii pe termen lung, cu obiective finale la Jocuri;
- Olimpice și Paralimpice, dar și cu obiective intermediare;
- Crearea unui sistem în care sportivii de performanță să se poată antrena în cele mai bune condiții, cu accent pe conceptul de pregătire centralizată controlată, construit în jurul unor centre regionale de excelență sau olimpice (6 de vara și 3 de iarnă), care vor putea funcționa pentru sporturile prioritare si voi fi independente;
- Strategia de infrastructură, care să se axeze tot pe ideea dezvoltării sporturilor prioritare;
- Investiții prin programe guvernamentale pentru crearea de noi activități, pentru a da viață bazelor sportive;

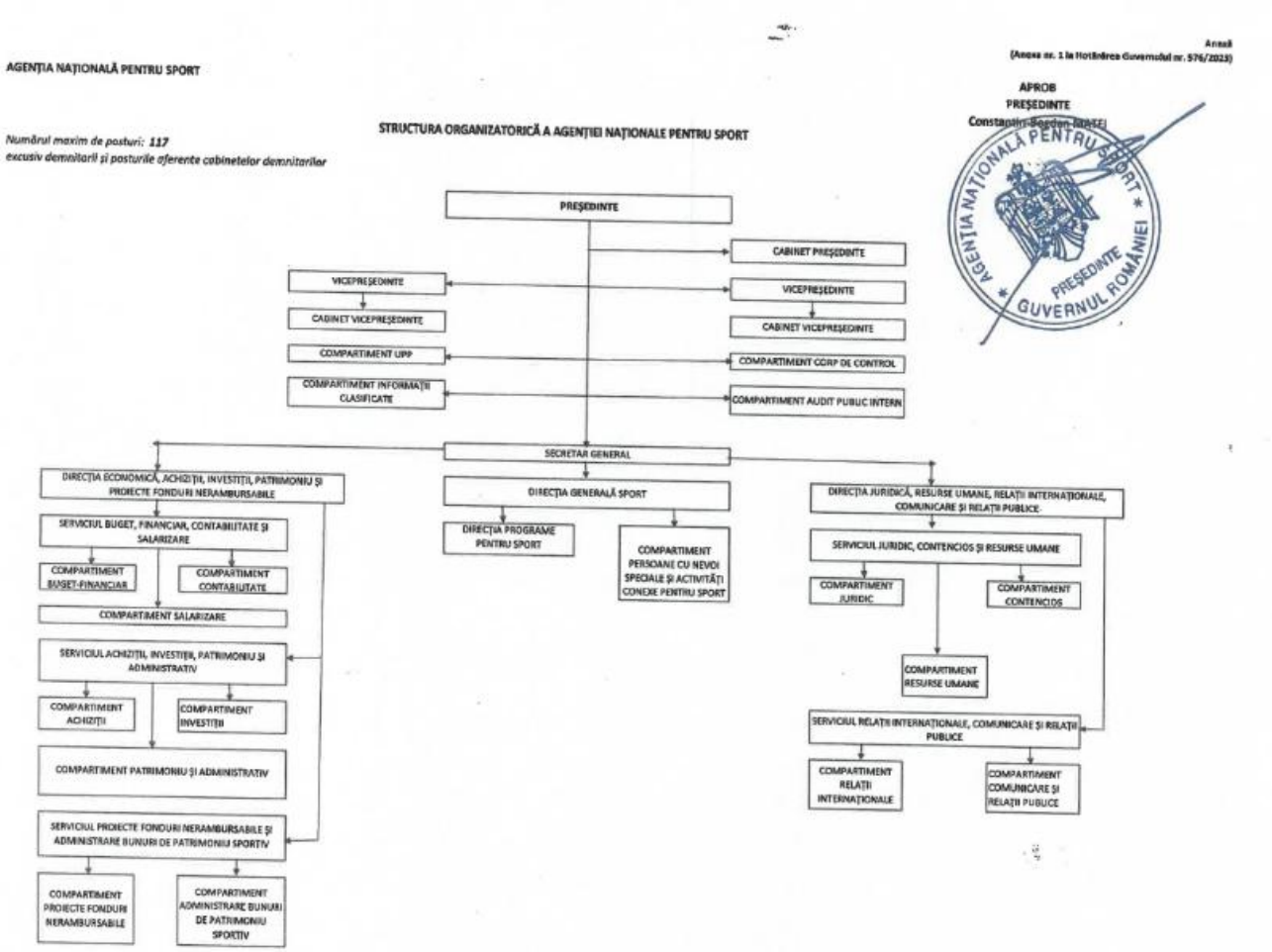
- Elaborarea sistemul de specializare a antrenorilor, ca parte integrantă în Legea Sportului;
- Noua Lege a Sportului, care să vină în sprijinul dezvoltării sporturilor și să asigure stabilitate;
- Crearea unui sistem în care foștii sportivi de performanță să aibă prioritate la reîntoarcerea în sistemul sportiv.

Prezentul proiect, urmărește digitalizarea serviciilor publice și a activităților interne ale ANS în vederea susținerii îndeplinirii obiectivelor Strategiei Naționale pentru Sport 2022-2032.

Prezentul proiect se aliniază îndeosebi cu obiectivul specific OS 3.2: Digitalizare, utilizarea datelor în sport și tratarea sportului ca o știință care prevede următoarele măsuri, acțiuni propuse: - Stimularea cercetării în domeniul sportului și dezvoltarea de mecanisme care să disemineze și să integreze rezultatele cercetării în toate zonele relevante din sport. Dezvoltarea capacitaților si valorificarea expertizei INCS. Dezvoltarea unor mecanisme permanente de colaborare a ministerului, COSR și federațiilor cu universitățile/ facultățile de educație fizică și sport în scopul transferului de know-how, experiență profesională, cercetare. Digitalizarea integrată a sistemelor de management în sportul de performanță și în alte zone relevante. Identificarea oportunităților existente în zona de e-sport. Creșterea capacitații ministerului de colectare, analiză și utilizare a datelor în activitatea desfășurată evidence based decision making luarea deciziilor bazate pe dovezi,

Indicatori macro OS 3.2: Digitalizare, utilizarea datelor în sport și tratarea sportului ca o știință - crearea registrului sportivului funcțional începând cu 2024, - infrastructură digitală pentru managementul datelor din sportul de performanță 2026, - integrarea e-sport-ului în fenomenul sportiv 2026, - structuri și mecanisme instituționale care să furnizeze date relevante în sport pe cele trei domenii: sport de performanță, sport în comunitate, sport în școli 2026, - crearea unui portal digital pentru finanțarea activităților sportive din surse private 2026.

Organigrama ANS, valabilă la data redactării prezentului document, este redată mai jos:



Figură 1: Organigramă

2.5 Informații despre beneficiile anticipate de către Autoritatea Contractantă

Prin realizarea acestui proiect, ANS își propune să răspundă nevoilor actuale și viitoare ale beneficiarilor serviciilor acestora. Modernizarea sistemului informatic va permite o gestionare internă mai eficientă, va facilita accesul la servicii digitale și va asigura un nivel înalt de securitate și conformitate.

Proiectul aduce numeroase beneficii pentru ANS și beneficiarii serviciilor instituției. Iată câteva dintre cele mai importante avantaje:

- **Optimizare**: asigurarea optimizării a infrastructurilor tehnologice și a proceselor de lucru.
- **Eficiență sporită**: Digitalizarea automatizează și optimizează procesele, reducând erorile umane și accelerând fluxurile de lucru.
- **Reducerea costurilor**: Elimină dependența de procesele manuale și documentele fizice, scăzând costurile de stocare și transfer.
- **Acces la informații în timp real**: Permite colectarea și analiza datelor în timp real, facilitând decizii rapide și informate.
- **Îmbunătățirea relației cu beneficiarii**: Facilitează comunicarea digitală, oferind servicii personalizate beneficiarilor.
- **Inovație și adaptabilitate**: Oferă posibilitatea de a dezvolta noi produse și servicii, fiind adaptabil la schimbările pieței.
- **Interconectare**: posibilitatea interconectării cu alte surse de date pentru îmbunătățirea contextului la nivel de instituție sau inter-instituțional.
- **Creșterea numărului de utilizatori digitali ai serviciilor** ANS.
- **Colaborare facilă și interconectare cu instituțiile/organizațiile** ce beneficiază de serviciile ANS.

Rezultatele așteptate în urma implementării proiectului sunt următoarele:

- Creșterea accesibilității, eficienței și transparenței serviciilor publice oferite de Agenția Națională pentru Sport (ANS) prin digitalizarea completă a interacțiunii cu sportivii, antrenorii, organizațiile sportive și publicul larg, în conformitate cu cerințele și standardele naționale și europene.
- Platformă digitală integrată dezvoltată si funcțională.
- Instruirea personalului ANS pentru utilizarea/administrarea platformei digitale dezvoltate prin proiect si instruirea în securitate cibernetică.

2.6 Alte inițiative/proiecte/programe asociate cu această achiziție de servicii

Nu este cazul.

2.7 Factorii interesați și rolul acestora

Proiectul implică mai multe categorii de părți interesate, fiecare cu roluri distincte:

1. Angajații ANS care vor furniza serviciile publice prin utilizarea facilităților puse la dispoziția de platforma integrata dedicată sportului românesc: aprox. 300;

2. Utilizatorii serviciilor publice oferite de ANS. Conform Registrului Național al Sportivilor (RNS) administrat de Institutul Național de Cercetare pentru Sport (INCS) si registrelor gestionate de ANS, există următoarele categorii de utilizatori ai serviciilor publice oferite de ANS:

- Sportivi: 101.728 sportivi activi (utilizatori/vizitatori anual),
- Cluburi sportive afiliate: 4619,
- Cluburi sportive - 48 unități,
- Antrenori: 2620,
- Federații: 56,
- Direcții județene pentru Sport și a Municipiului București: 42 unități,
- Administratori de baze sportive,
- Personal angrenat in sport (medici, preparatori, etc).

3. Autorități și instituții publice care schimbă date și informații ANS în mod constant.

3 Descrierea serviciilor solicitate

3.1 Obiectul achiziției

Obiectul procedurii constă în achiziționarea de **„SERVICII INTEGRATE DE DEZVOLTARE PLATFORMA INFORMATICA”** în cadrul proiectului “PORTALUL SPORTULUI ROMÂNESC„ - DIGITALIZAREA SERVICIILOR PUBLICE ALE AGENȚIEI NAȚIONALE PENTRU SPORT.

În subsidiar, pentru realizarea obiectului principal, se vor avea în vedere:

- Livrare si preluare echipamente hardware.
- Analiza fluxurilor de activitate din cadrul ANS și Proiectarea sistemului.
- Dezvoltare soluție TIC integrată și testare internă Prestator.
- Implementarea măsurilor de securitate cibernetică.
- Implementare sistem integrat.
- Testare finală.
- Instruire administratori si utilizatori.

3.2 Descrierea situației actuale la nivelul beneficiarului

Pentru a înțelege contextul tehnic al implementării proiectului propus, prezentăm în cadrul acestei secțiuni câteva informații de ordin tehnic cu privire la sistemul/sistemele informatice existente în cadrul instituției. Aceste informații sunt importante pentru a înțelege constrângerile de ordin tehnic pe care soluția tehnică propusă va trebui să le acomodeze.

În prezent, informațiile referitoare la structurile sportive sunt disponibile electronic sub forma unor foi de calcul Microsoft Excel, pentru fiecare județ în parte, pe site-ul Agenției Naționale pentru Sport. Această modalitate de stocare reprezintă un impediment în generarea rapoartelor. Spre exemplu, este dificil de aflat câte structuri sportive au fost înregistrate, având o anumită ramura sportivă sau câte sunt “Cluburi Sportive de Drept Privat” întru-un anumit județ pentru o disciplină sportivă.

În aceeași măsură, absența unor criterii stricte de introducere a datelor a făcut posibilă duplicarea coloanelor, îngreunând astfel procesul de selectare. Nu în ultimul rând, pentru cetățeni, este dificil și anevoios de căutat o structură sportivă după denumire, deoarece aceștia vor fi nevoiți să descarce toate tabelele, iar mai apoi să caute în fiecare document, implicând astfel un proces tehnic complex, care nu se regăsește în bagajul de cunoștințe al utilizatorului obișnuit.

O altă problematică abordată este cea a datelor de contact ale structurilor sportive. Registrul Sportiv conține doar adresa ca punct de legătură al ANS cu aceste entități. Având în vedere că în prezent se folosesc mijloace electronice pentru comunicare, este important de menționat că existența unor date precum numărul de telefon sau adresa de email, ar reprezenta un avantaj pentru ANS. Dat fiind numărul ridicat de structuri sportive, este dificil pentru ANS să colecteze aceste date și s-ar dori o descentralizare a sarcinilor, astfel încât sa poată exista si utilizatori aferenți structurilor sportive.

Pe lângă aspectele semnalate mai sus, ANS gestionează și alte problematici, cazuri în care situația este similară, respectiv: baze sportive, școli de antrenori, federații sportive, anuarul sportului românesc etc. În niciunul din cazuri, activitățile nu sunt digitalizate, evidențele fiind ținute

individual/local, fără posibilitatea de interogare a datelor (data mining) și realizarea de statistici la nivel național.

Sistemul actual de înregistrare și prezentare a informațiilor despre diverse activități din cadrul ANS, se bazează pe fișiere locale (foi de calcul Microsoft Excel), este ineficient și dificil de utilizat atât pentru gestionarea internă a datelor cât și pentru accesul public. În acest fel sunt întâmpinate dificultăți în generarea rapoartelor, inconsistență a datelor (duplicare) și complexitatea procesului de căutare pentru cetățeni. Digitalizarea în vederea îmbunătățirii accesului la informații și eficiența administrării datelor în cadrul Agenției Naționale pentru Sport.

SITUATIE INFRASTRUCTURĂ HARDWARE ȘI SOFTWARE:

Hardware:

- 2 servere aplicații Huawei RH2288H V3;
- 2 servere baze de date Huawei RH2288H V3;
- 1 sistem de stocare Maguay PowerStor;
- 1 Rack cu KVM APC Netshelter;
- 1 UPS APC SRT6KRMXLI Smart On-Line;
- 2 switch-uri Brocade 300 24 porturi;
- 10 switch-uri Zyxel GS1900-48 48 porturi ;

Software:

- 18 sisteme de operare de tip server - Windows Server 2012 R2 Standard;
- 2 sisteme de operare de tip server - Windows Server 2012 R2 Datacenter;
- Sistem gestiune baza de date - SQL Server Standard Edition;
- Sistem gestiune baza de date - SQL CAL 2014;
- Sistem gestiune baza de date - SQL Server Business Intelligence;
- 1 server - Windows Server 2008 program economic Indeco
- 2 programe Open-E DSS V7 2015, versiune 7.0up14.9201.15893, 64bit;
- Echipament firewall FortiGate 100F
- 1 Server Bitdefender GravityZone Business Security cu 200 users

3.3 Obiectivele generale și specifice la care contribuie furnizarea produselor și prestarea serviciilor

3.3.1 Obiectivul general

Obiectivul general al proiectului **“PORTALUL SPORTULUI ROMÂNESC - DIGITALIZAREA SERVICIILOR PUBLICE ALE AGENȚIEI NAȚIONALE PENTRU SPORT”** vizează creșterea accesibilității, eficienței și transparenței serviciilor publice oferite de Agenția Națională pentru Sport (ANS) prin digitalizarea completă a interacțiunii cu sportivii, antrenorii, organizațiile sportive și publicul larg, în conformitate cu cerințele și standardele naționale și europene.

Prezentul proiect urmărește digitalizarea activităților interne Agenției Naționale pentru Sport (ANS) precum și a serviciilor publice ce presupun interacțiunea cu beneficiarii (federații, cluburi, sportivi etc.), în vederea minimizării interacțiunii directe cu beneficiarii, prin digitalizarea a fluxurilor de date și a proceselor, în vederea eliminării necesității interacțiunii fizice dintre ANS și beneficiarii serviciilor, precum și a reducerii timpului de procesare a cererilor de soluționare a solicitărilor.

3.3.2 Obiectivele specifice ale proiectului

Obiectivele specifice identificate ca fiind realizabile prin implementarea proiectului propus sunt următoarele:

OS1. Digitalizarea eliberării documentelor pentru sportivi și antrenori:

- Automatizarea procesului de eliberare a Pașaportului Sportivului și a Pașaportului Antrenorului.
- Crearea unui modul pentru gestionarea cererilor de eliberare a Carnetului de Maestru Emerit al Sportului și a Carnetului de Antrenor Emerit.

OS 2. Simplificarea accesului la certificări și recunoașterea calificărilor:

- Dezvoltarea unei platforme online pentru solicitarea și emiterea Certificatelor de clasificare profesională, eliberarea certificatelor de absolvire și a carnetelor de antrenor.
- Digitalizarea procesului de recunoaștere a titlurilor de calificare profesională obținute în state membre ale Uniunii Europene, Spațiului Economic European sau alte state terțe.
- Crearea unui sistem digital pentru gestionarea eficientă a activităților de formare desfășurată de CNFPA.

OS 3. Gestionarea digitală a relației cu federațiile, cluburile sportive, COSR și alte organizații din domeniul sportului:

- Crearea unui sistem digital pentru depunerea și aprobarea avizului prealabil necesar depunerii candidaturii în vederea organizării de competiții internaționale.
- Implementarea unui sistem digital pentru emiterea Certificatului de Identitate Sportivă.
- Implementarea unui sistem digital de raportare a activităților/rezultatelor sportive.
- Integrarea funcționalității în portalul public al ANS pentru o transparență crescută.

OS 4. Facilitarea interacțiunii cu publicul prin soluții moderne:

- Implementarea unui serviciu digital pentru răspunsuri rapide la petiții și solicitări de informații.
- Dezvoltarea unui modul de programare online pentru vizite la Galeria Marilor Sportivi, cu integrarea unui tur virtual interactiv.

OS 5. Promovarea valorilor și patrimoniului sportiv:

- Digitalizarea și inventarierea completă a exponatelor din Galeria Marilor Sportivi, inclusiv dezvoltarea unui tur virtual accesibil online.
- Digitalizarea arhivei istorice prin scanare, clasificare și indexare, asigurând păstrarea și accesul digital la documentele cu valoare istorică.

4 Cerințe privind soluția tehnică

4.1 Cerințe generale

Bazându-se pe experiența anterioară, luând de asemenea în calcul aplicațiile deja existente în cadrul ANS, pentru acest proiect de transformare digitală se solicită folosirea tehnologiilor web și mobile, care să asigure posibilitatea accesării rapide, de pe mai multe tipuri de platforme, cât și posibilitatea actualizării/modificării facile a aplicațiilor, la nevoie.

Utilizarea tehnologiilor web în digitalizarea serviciilor unei instituții oferă numeroase avantaje. Acestea permit accesul facil și rapid la servicii de către utilizatori, indiferent de locație sau dispozitiv, asigurând o inter-conectivitate crescută și o mai bună gestionare a resurselor. Tehnologiile web facilitează actualizările și mentenanța, reducând costurile operaționale și timpul de inactivitate. De asemenea, ele sprijină conformitatea cu standardele de securitate și protecția datelor, esențiale pentru instituțiile care gestionează informații sensibile. În concluzie, tehnologiile web sunt esențiale pentru o transformare digitală eficientă și durabilă.

Pe lângă cerințele funcționale specifice care sunt solicitate în cadrul Capitolului 4.4., pentru implementarea soluției tehnice propuse Ofertanții vor avea în vedere și următoarele obiective non-funcționale:

- Sistemul implementat va respecta atât politicile și reglementările interne privind tehnologia informației, cât și legislația în vigoare privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, precum și orice alte acte normative care se referă la implementarea aplicațiilor sau la domeniul tehnologia informației.
- Interfață Utilizator Intuitivă: Interfața utilizator a sistemului, în ansamblu, precum și a fiecărui subsistem component, va trebui să fie intuitivă (facilă), informativă, fiabilă, atractivă și stabilă. Interfața utilizator, pentru sistemele accesate prin interfață web, trebuie să poată fi accesată utilizând versiuni ale browsere-lor (minim Google Chrome/Microsoft Edge/Safari/Firefox) compatibile atât cu dispozitive de tip desktop/laptop, cât și cu dispozitive și telefoane mobile. Interfața utilizator va fi realizată conform ultimelor versiuni ale standardelor HTML, CSS, XML.
- Vizualizare de Date: Capacitatea de a afișa date într-un mod vizual atractiv, cum ar fi grafice, diagrame și tabele.
- Filtrare și Sortare: Opțiuni pentru a filtra și sorta datele în funcție de diferite criterii pentru a facilita găsirea informațiilor dorite.
- Căutare Avansată: Un sistem de căutare robust care permite utilizatorilor să găsească rapid informații specifice.
- Rapoarte și Export de Date: Funcționalități pentru generarea de rapoarte și posibilitatea de a exporta date în diferite formate, cum ar fi CSV sau PDF.
- Responsivitate: Design care se adaptează la diferite dimensiuni de ecran și dispozitive pentru a asigura o experiență de utilizare consistentă.
- Interfața sistemului va trebui să fie disponibilă cel puțin în limba română, dar sistemul în ansamblul său va trebui să asigure suport/funcționalități multi-language pentru a spori

accesibilitatea, fără efort semnificativ de dezvoltare software . Această măsură nu numai că va facilita accesul, ci și va reflecta respectul față de diversitatea culturală și lingvistică, extinzând conținutul portalului în mai multe limbi, promovând incluziunea și egalitatea de șanse pentru toți cetățenii.

- În cazul modulelor funcționale dezvoltate în cadrul contractului TOATE DREPTURILE PATRIMONIALE DE AUTOR asupra tuturor operelor create de către viitorul Prestator, aferente produsului sau serviciului livrat, SE VOR TRANSFERA CĂTRE BENEFICIAR. împreună cu ultima versiune a codului sursă, comentat și documentat, pentru versiunea sistemului dat inițial în producție și la finalul perioadei de garanție și suport, codul obiect și documentația tehnică detaliată și completă a sistemului. Livrarea codului sursă se va realiza împreună cu un instrument dedicat de gestiune și versionare, instrument ce va putea fi utilizat de Achizitor fără limitări după finalizarea perioadei de suport și garanție, de tip GIT sau echivalent.
- Toate codurile sursă vor include și comentarii scrise în limba română și în acord cu standardele/convențiile de dezvoltare a codului (în forma susținută de limbajul de programare aferent, de exemplu comentarii în interiorul codului). Toate codurile sursă vor fi predate în clar, fără a se aplica procedee de ascundere. Acceptarea predării codului sursă de către Prestator și preluării acestuia de către beneficiar se va realiza doar după validarea acestuia de către Beneficiar în infrastructura proprie, la recepția sistemului informatic implementat.
- Securitate: Protecția datelor prin autentificare, autorizare și criptare pentru a asigura confidențialitatea și integritatea datelor. Componentele sistemului propus trebuie să fie protejate împotriva încercărilor deliberate sau accidentale de acces neautorizat la datele pe care acesta le stochează sau prelucrează. Astfel, sistemul în ansamblul său trebuie să asigure:
  - Securitatea datelor printr-un sistem de limitare a accesului la funcționalitățile aplicației, bazat pe drepturi și defalcat pe mai multe niveluri. Drepturile de acces ale utilizatorilor vor putea fi configurate de administratorii sistemului din interfața sistemului;
  - Împiedicarea utilizatorilor de a se conecta la sistem dacă acesta este în incapacitate temporară de a asigura securitatea datelor sau există suspiciuni că mecanismele de protecție au fost compromise;
  - Închiderea automată a sesiunilor de lucru ale utilizatorilor, în caz de inactivitate pe o anumită durată predeterminată și configurabilă de timp, nu mai mult de 5 minute după ce se înregistrează ca user-ul devine inactiv, pentru a proteja dezvăluirea accidentală a informațiilor către alte persoane care nu sunt autorizate să le primească;
  - Jurnalizarea operațiilor zilnice la nivelul sistemului, individual pentru fiecare utilizator cu drept de acces la modificarea înregistrărilor, cu marcarea orei la care a fost executată fiecare operație, precum și a identității utilizatorului care a inițiat-o;
  - Generarea de rapoarte diverse pentru loguri-le generate la nivelul aplicațiilor, precum și exportul tuturor loguri-lor, cel puțin în format csv. și/sau alte formate standard;

  - Eventualele mecanisme de tip API, interne sau externe, vor fi protejate prin metode de autentificare;
  - Confidențialitatea transferului de informații pentru a proteja informațiile împotriva amenințărilor în orice situație, fie când informația este stocată pe servere, fie când aceasta este transportată.
- Actualizări în Timp Real: Actualizarea datelor în timp real pentru a reflecta cele mai recente informații disponibile.
- Integrare cu Alte Sisteme: Capacitatea de a se integra cu alte aplicații sau sisteme pentru a îmbunătăți fluxurile de lucru și a automatiza procesele:
  - Interconectarea cu ROeID necesită încheierea unui protocol de colaborare între ADR și ANS, protocol ce va fi inițiat de ANS înainte de implementarea integrărilor tehnice.
  - Ofertantul va implementa mecanisme de autentificare compatibile cu infrastructura Cloudului Privat Guvernamental (CPG), asigurând interoperabilitatea cu sistemele de identitate utilizate la nivel guvernamental.
  - Toate mecanismele de autentificare și autorizare vor respecta cerințele de securitate, audit și trasabilitate impuse de ADR și de standardele aplicabile (ISO 27001, NIST, CIS).
- Prestatorul va presta serviciile cu respectarea măsurilor de securitate a informațiilor conforme cu principiile și controalele prevăzute în standardul ISO/IEC 27001:2022 sau echivalent. Dovada conformității nu reprezintă o cerință de calificare și se poate face prin:
  - certificat ISO/IEC 27001 valabil emis de un organism acreditat RENAR sau echivalent european; SAU
  - orice alte mijloace de probă adecvate (rapoarte de audit intern/extern, proceduri interne de securitate, politici de securitate cibernetică, dovezi de conformitate cu NIS2/Directiva 2022/2555) care demonstrează adoptarea unor măsuri echivalente.
- Personalizare: Posibilitatea de a personaliza interfața și funcționalitățile în funcție de preferințele utilizatorului sau de nevoile specifice ale afacerii.
- Posibilitatea implementării fluxurilor de date existente la nivelul ANS, cu funcționalități de aprobare, trimitere comunicări pe email, folosire certificate digitale calificate.
- Modelul de date va fi pus la dispoziția Autorității Contractante, cu toată documentația necesară.
- High Availability: reprezintă o caracteristică a unui sistem, care asigură funcționarea continuă și neîntreruptă, cu scopul de a minimiza timpii de nefuncționare (downtime) și de a asigura accesul continuu la serviciile sau aplicațiile respective. În esență, un sistem cu high availability este proiectat pentru a menține un nivel ridicat de disponibilitate, chiar și în situații de avarie sau când apar probleme neprevăzute. Întregul sistem trebuie să fie astfel proiectat, printr-o combinație de strategii și tehnologii, precum:
  - Redundanță: Componentelor critice (servere, rețele, stocare) li se creează copii de rezervă. Dacă una dintre componente eșuează, celelalte preiau imediat sarcina, asigurând continuitatea serviciilor.

- Failover: Este un mecanism prin care, în cazul în care o componentă a sistemului devine indisponibilă, altă componentă preia automat funcționalitatea sa, astfel încât impactul asupra utilizatorilor să fie minim.
- Load Balancing: Distribuirea cererilor între mai multe servere pentru a împiedica supraîncărcarea și pentru a crește performanța. Aceasta asigură că, în cazul în care un server se defectează, altele pot prelua traficul.
- Clustering: Gruparea serverelor într-un cluster, astfel încât acestea să acționeze ca un singur sistem. Dacă un server din cluster eșuează, altele îi vor prelua automat sarcinile.
- Monitorizare și alerte proactive: Utilizarea de soluții care să monitorizeze constant starea sistemelor și să alerteze echipa tehnică asupra potențialelor probleme, înainte ca acestea să devină critice.

- Sistemul informatic va fi proiectat utilizând principii de arhitectură de tip CLOUD NATIV (modularitate, separarea componentelor, portabilitate și scalabilitate controlată), respectiv operaționalizat în Cloudul Privat Guvernamental (CPG), proiectat astfel încât să permită, în măsura compatibilității tehnice, migrarea către alte medii de tip cloud, public sau privat, în caz de necesitate.
- În dezvoltarea aplicației/sistemului informatic solicitat de ANS se vor utiliza următoarele tehnologii:
  - BI/Dashboards (Business Intelligence/Dashboards): Sistemul va include un modul BI care va permite crearea de rapoarte și dashboard-uri dinamice pentru a facilita analiza datelor colectate, oferind informații utile, în timp real, pentru luarea deciziilor. O serie de dashboard-uri/rapoarte cu privire la situația entităților existente va fi predefinită, în baza unor specificații realizate în cadrul proiectului.
  - Scan/OCR (Optical Character Recognition): Tehnologia OCR va fi folosită pentru a scana și extrage automat informații din documente fizice (CI, CIS), transformându-le în format digital pentru a le integra în sistem, preluând datele în mod automat, simplificând astfel procesul de colectare și procesare a informațiilor.
  - Web/Mobile: Sistemul va fi dezvoltat ca o aplicație web și va include o interfață mobilă, asigurând acces facil pentru utilizatori atât de pe desktop, cât și de pe dispozitive mobile, pentru o utilizare convenabilă și în teren.
  - NLP (natural language processing) și NLG (natural language generation): Vor fi integrate funcționalități de NLP pentru a îmbunătăți procesele de analiză a datelor, automatizare și suport decizional, inclusiv asistenți virtuali (chatbots) care să răspundă automat la cerințele utilizatorilor. De asemenea, chatbot-ul va trebui să fie capabil de crearea de conținut text sau vorbit care să semene cât mai mult cu limbajul uman (în limba română), pe baza unor date structurate sau a unor modele de inteligență artificială.
  - DMS (Document Management System): Sistemul de gestionare a documentelor (DMS) va permite stocarea, organizarea și căutarea eficientă a documentelor digitale, asigurând o administrare corectă și acces rapid la informațiile necesare.
  - Arhivare electronică: procesul de stocare, gestionare și păstrare pe termen lung a documentelor în format digital, folosind tehnologii digitale. Aceasta implică atât

conversia documentelor fizice în format electronic, cât și gestionarea documentelor create direct în formă digitală, asigurând accesul facil, securitatea și integritatea informațiilor.

Prin combinarea acestor tehnologii, sistemul informatic pentru ANS va asigura un management digital integrat, eficient și accesibil, care va contribui la optimizarea proceselor interne și la îmbunătățirea interacțiunii cu cetățenii și agenții economici.

Soluția livrată va fi completă, integrată, cu licență perpetuă de folosire (va intra în patrimoniul ANS) și cu suport/mentenanță pe perioada de implementare a proiectului, dar nu mai puțin de un an de la data încheierii procesului verbal de recepție.

Soluția va fi livrată cu toate manualele în format electronic, și numai după realizarea sesiunilor de instruire cu toți administratorii și utilizatorii din cadrul ANS (conform cap. 6.2.7.).

Toate elementele de infrastructură hardware și software ce vor fi incluse în realizarea sistemului vor trebui să respecte principiul DNSH (Do No Significant Harm) așa cum este acesta enunțat în Regulamentul delegat (UE) 2021/2139 al Comisiei din 4 iunie 2021 de completare a Regulamentului (UE) 2020/852 al Parlamentului European și al Consiliului prin stabilirea criteriilor tehnice de examinare pentru a determina condițiile în care o activitate economică se califică drept activitate care contribuie în mod substanțial la atenuarea schimbărilor climatice sau la adaptarea la schimbările climatice și pentru a stabili dacă activitatea economică respectivă aduce prejudicii semnificative vreunuia dintre celelalte obiective de mediu. Ofertantul va include în Ofertă o declarație cu privire la respectarea principiului DNSH pentru toate elementele componente ale Ofertei, precum și modalitatea concretă în care acestea vor fi asigurate pentru fiecare element de infrastructura de bază și aplicații ofertat, sub sancțiunea declarării ofertei ca neconforme în cazul absenței declarației și descrierii modalității de îndeplinire a cerinței.

Toate produsele și serviciile software de tip antivirus achiziționate prin intermediul acestui proiect vor respecta legea 354/2022 privind protecția sistemelor informatice ale autorităților și instituțiilor publice în contextul invaziei declanșate de Federația Rusă împotriva Ucrainei.

Ofertanții sunt obligați să ia toate măsurile rezonabile și să verifice cu producătorii faptul că produsele ofertate nu sunt End Of Life (EOL) la momentul ofertării și că acestea vor fi disponibile pentru a fi achiziționate și livrate conform calendarului contractului. Nu se vor admite ulterior, pe perioada derulării contractului, modificări substanțiale ale soluției tehnice, cauzate de ofertarea unor elemente tehnice care nu sunt în fapt disponibile pentru livrare. Modificări la momentul livrării ale componentelor soluției tehnice ofertate (în sensul modificării versiunii unei aplicații software sau a modelului unui echipament, față de cele ofertate) se vor admite numai în următoarele condiții:

- cu prezentarea unei declarații pe propria răspundere a furnizorului respectivei componente software sau hardware din care să reiasă că modelul/versiunea ofertată nu mai este disponibilă pentru furnizare și cu precizarea modelului/versiunii cu care a fost înlocuită.
- cu prezentarea unui tabel comparativ între cerințele caietului de sarcini, specificațiile tehnice ale produsului ofertat și respectiv ale produsului cu care acesta a fost înlocuit, din care să reiasă faptul că se respectă toate cerințele tehnice ale caietului de sarcini, iar produsul ofertat este echivalent sau, dacă nu este posibil, atunci este superior celui ofertat din punctul de vedere al tuturor specificațiilor tehnice solicitate.

4.2 Prevederi de securitate

4.2.1 Nivelul de securitate

Stabilirea cerințelor de securitate pentru sistem a fost realizată plecând de la stabilirea nivelului de risc asociat proiectului, conform următoarelor definiții ale nivelelor de risc:

- Nivel mic - Exista un efect limitat la nivelul unei organizații sau a persoanelor in urma pierderii confidențialității, integrității sau disponibilității informațiilor gestionate de sistemele informatice propuse;
- Nivel mediu - Exista un efect grav la nivelul unei organizații sau a persoanelor in urma pierderii confidențialității, integrității sau disponibilității informațiilor gestionate de sistemele informatice propuse;
- Nivel mare - Exista un efect server sau catastrofic la nivelul unei organizații sau a persoanelor in urma pierderii confidențialității, integrității sau disponibilității informațiilor gestionate de sistemele informatice propuse.

Sistem expus in Internet	INFORMATII			
	CONFIDENTIALE	FINANCIARE	PERSONALE	PUBLICE
Acoperire națională; Institutul Național de Cercetare pentru Sport, Centru Național de Formare și Perfecționare a Antrenorilor, Galeria Marilor Sportivi, etc.				
Acoperire regională/locală; Direcții județene pentru Sport și a Municipiului București, Cluburi sportive, Complexuri sportive naționale, etc.				

Având în vedere expunerea în Internet a unor componente ale sistemului (portal public, servicii web de interoperabilitate, mecanisme de schimb electronic de date), precum și natura datelor gestionate (date personale ale sportivilor, date financiare și informații operaționale cu acoperire națională, etc.), sistemul informatic se încadrează în categoria sistemelor informatice cu **RISC MARE**, conform clasificării nivelurilor de risc.

4.2.2 Principii generale care stau la baza asigurării securității cibernetice

Principiile care stau la baza asigurării securității cibernetice ale platformei sunt:

- **Principiul conformității** – Implementarea platformei deține sau poate acomoda mecanisme tehnice pentru aplicarea reglementărilor naționale aplicabile (ex: GDPR) și a standardelor internaționale în vigoare privind protecția informațiilor procesate (ex: ISO).
- **Principiul optimizării costurilor** - toate investițiile necesare pentru asigurarea securității se stabilesc pe baza rezultatelor unui proces periodic de analiză a riscului.
- **Principiul responsabilități de securitate partajate** – rolurile și responsabilitățile entităților implicate în furnizarea și operarea serviciilor trebuie să fie stabilite, reglementate și asumate. Pentru implementarea măsurilor de securitate de către administratorii și beneficiarii resurselor, în concordanță cu responsabilitățile stabilite, platforma trebuie să integreze mecanisme tehnice necesare.

- **Principiul protecției informațiilor**:
  - Informațiile trebuie protejate în tranzit și în stocare împotriva accesării sau modificării de către entități neautorizate;
  - Informațiile trebuie sa fie disponibile fără întârziere la cererea entităților autorizate.
- **Principiul securității pe întreg ciclul de viață al sistemului** - Securitatea este integrată în toate fazele ciclului de viața ale platformei, de la analiză și proiectare până la scoaterea din uz a resurselor sau serviciilor.
- **Principiul transparenței și standardizării** – este recomandat ca platforma să fie auditată periodic de entități terțe evaluatoare pentru a certifica conformitatea cu standardele stabilite de reglementările aplicabile.
- **Principiul securizării operațiunilor** - aplicarea mecanismelor pentru detectarea și prevenirea atacurilor cibernetice, prin raportare la o abordare pe niveluri pentru securizarea proceselor de furnizare a serviciilor din platformă.

4.2.3 Integritatea si securitatea sistemului

Platforma va fi proiectată și dezvoltată cu un accent puternic pe securitate, începând cu principiile de "Security by Design" pentru a integra considerații de securitate în toate funcțiile și modulele. Practici de "Secure Coding" vor fi aplicate pentru a asigura că software-ul este robust împotriva vulnerabilităților. Un "Web Application Firewall" (WAF) va proteja împotriva atacurilor specifice aplicațiilor web. De asemenea va fi asigurată protecție de tip "antiDDOS", pentru a proteja aplicația împotriva atacurilor de tip DDOS (ex. "Cloudflare"). Întregul sistem informatic va fi protejat printr-un firewall, care să blocheze traficul și accesul neautorizat. Autentificarea în doi factori (2FA) și "Single Sign-On" (SSO) cu Active Directory (AD) și soluții de Identity and Access Management (IAM)/Privileged Access Management (PAM) vor fi implementate pentru a spori securitatea autentificării și eficiența gestionării accesului. Aceste măsuri vor asigura că platforma este securizată și ușor de utilizat.

Întregul sistem informatic livrat va trebui să respecte toate prevederile legislative în vigoare, precum și cele ce urmează a intra în vigoare în perioada de sustenabilitate, în măsura posibilității îndeplinirii cerințelor specifice (ex: NIS2, GDPR, DSA, DORA etc.).

Prestatorul are obligația de a dezactiva serviciile și componentele neutilizate la nivelul sistemelor de operare (servere și stații de lucru), pentru reducerea suprafeței de atac și respectarea cerințelor de securitate. Configurarea va fi documentată și prezentată Autorității Contractante.

Cerințele pentru prevederile de securitate sunt prezentate în secțiunea 4.10.

4.3 Alinierea la strategii și legislație

1. Hotărârea Guvernului nr. 908/2017 pentru aprobarea Cadrului National de Interoperabilitate
   - **Soluția va respecta Cadrul Național de Interoperabilitate prin:**
     - **Arhitectură deschisă**: Dezvoltarea unei arhitecturi deschise care să permită integrarea facilă cu alte sisteme și platforme informatice.

- **Schimb de date standardizat**: Utilizarea standardelor naționale și internaționale pentru schimbul de date, asigurând interoperabilitatea și eficiența procesării informațiilor.

2. Legea nr. 242/2022 privind schimbul de date între sisteme informatice și crearea Platformei naționale de interoperabilitate

   - **Soluția va respecta Legea nr. 242/2022 prin:**
     - **Interoperabilitate**: Asigurarea interoperabilității sistemului IT cu alte platforme naționale și europene, facilitând schimbul de date și integrându-se în Platforma națională de interoperabilitate.
     - **Standardizare**: Utilizarea standardelor și protocoalelor comune pentru schimbul de date, asigurându-se că informațiile sunt compatibile și pot fi procesate eficient de diferite sisteme informatice.

3. OUG nr. 89/2022 privind înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizate de autoritățile și instituțiile publice

   - **Soluția va utiliza infrastructuri și servicii informatice de tip cloud pentru a asigura flexibilitatea și scalabilitatea necesare:**
     - **Utilizare cloud guvernamental**: Portalul și aplicațiile mobile vor fi găzduite pe infrastructura de cloud guvernamental, conform prevederilor OUG nr. 89/2022. Aceasta va asigura securitatea, redundanța și accesibilitatea necesare pentru serviciile publice.
     - **Administrare centralizată**: Gestionarea infrastructurii cloud va fi realizată conform standardelor și ghidurilor naționale, asigurându-se că toate datele sunt protejate și gestionate eficient.

4. Hotărârea Guvernului nr. 112/2023 privind aprobarea Ghidului de guvernanță a platformei de cloud guvernamental

   - **Soluția va fi aliniată cu Ghidul de guvernanță a platformei de cloud guvernamental prin:**
     - **Guvernanță clară**: Stabilirea unor politici și proceduri clare de guvernanță pentru administrarea și utilizarea resurselor cloud, conform ghidului aprobat.
     - **Conformitate și audit**: Implementarea unor mecanisme de audit și conformitate pentru a asigura respectarea regulilor și cerințelor de securitate.
     - **Găzduirea platformei în cloud-ul guvernamental.**

5. OUG nr. 112/2018 privind accesibilitatea site-urilor web și a aplicațiilor mobile ale organismelor din sectorul public

   - **Soluția va respecta pe deplin cerințele Ordonanței de Urgență nr. 112/2018 și ale Normelor de monitorizare aprobate prin Decizia Președintelui ADR nr. 815/2022, prin implementarea următoarelor măsuri:**
     - **Conformitate cu standardele de accesibilitate:** Portalul web și aplicațiile mobile vor respecta WCAG 2.1, nivelul de conformitate AA, asigurând accesibilitatea pentru

persoanele cu dizabilități. Interfețele de navigare, formularele, conținutul media și elementele interactive vor fi optimizate pentru accesibilitate.

- **Standardizare tehnică:** Interfețele grafice vor utiliza setul de caractere UTF-8, conform cerințelor de accesibilitate și interoperabilitate.
- **Testare continuă a accesibilității:** Vor fi realizate teste periodice de accesibilitate, inclusiv cu implicarea utilizatorilor cu dizabilități, pentru identificarea și remedierea eventualelor probleme. Rezultatele testelor vor fi documentate și puse la dispoziția Autorității Contractante.
- **Documentație accesibilă:** Toate documentele publicate pe portal vor fi furnizate în formate accesibile, inclusiv PDF-uri cu text selectabil, structuri logice corecte și descrieri alternative pentru imagini.
- **Conformitate cu Normele ADR:** Soluția va implementa cerințele prevăzute în Normele de monitorizare a conformității site-urilor web și aplicațiilor mobile, aprobate prin Decizia ADR nr. 815/2022, asigurând menținerea nivelului de conformitate prevăzut de legislație.

6. Regulamentul (UE) 2016/679 – GDPR

- **Sistemul va fi proiectat astfel încât să aibă în vedere implementarea principiilor Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), atât în ceea ce privește datele angajaților proprii, cât și a cetățenilor, prin:**
  - Protecția datelor angajaților și cetățenilor.
  - Informări și notificări realizate de Beneficiar către persoanele vizate.
  - Măsuri tehnice și organizatorice pentru protecția datelor cu caracter personal.

7. Legea 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cu modificările și completările ulterioare

- **Soluția va include măsuri stricte de securitate cibernetică:**
  - **Infrastructură securizată**: Utilizarea serverelor securizate și a soluțiilor de stocare cloud cu certificări de securitate recunoscute la nivel național și european.
  - **Protecția datelor**: Implementarea de protocoale de criptare pentru toate datele transmise și stocate. Politici stricte de acces și autentificare cu doi factori vor fi aplicate pentru a proteja datele utilizatorilor.
  - **Monitorizare și răspuns la incidente**: Sistemele de monitorizare continuă a securității vor fi integrate pentru a detecta și răspunde rapid la orice breșă de securitate. Un plan de continuitate a afacerii și un plan de răspuns la incidente vor fi elaborate și testate periodic.

8. Legea nr. 179/2022 privind datele deschise și reutilizarea informațiilor din sectorul public

- **Soluția va sprijini principiile Legii nr. 179/2022 prin:**

- **Publicarea datelor deschise**: Datele generate și colectate de Agenția Națională pentru Sport vor fi disponibile publicului într-un format deschis, care permite reutilizarea. Aceste date vor include informații despre evenimente, programe educative, și statistici privind participarea.
- **API-uri deschise**: Dezvoltarea de API-uri care permit accesul automatizat la datele publice, facilitând integrarea cu alte platforme și aplicații.
- **Colaborare cu comunitatea**: Promovarea reutilizării datelor prin colaborarea cu dezvoltatori, cercetători și alte entități interesate. Organizarea de evenimente și ateliere pentru a încuraja inovația bazată pe datele deschise.

9. Hotărârea Guvernului nr. 941/2013 și Hotărârea Guvernului nr. 824/2023 privind organizarea și funcționarea Comitetului Tehnico-Economic pentru Societatea Informațională
   - **Proiectul va colabora cu Comitetul Tehnico-Economic pentru Societatea Informațională prin:**
     - **Consultare și coordonare**: Participarea activă în consultările și coordonările organizate de Comitetul Tehnico-Economic pentru Societatea Informațională, asigurându-se că proiectul respectă toate reglementările și directivele naționale în domeniul ITC.
     - **Alinierea la priorități**: Proiectul va fi aliniat la prioritățile și recomandările stabilite de Comitet, asigurându-se că resursele sunt utilizate eficient și că se atinge un nivel ridicat de interoperabilitate și securitate.
10. Decizia Președintelui Autorității pentru Digitalizarea României (ADR) nr. 815/06.12.2022 pentru aprobarea Normelor de monitorizare a conformității site-urilor web și a aplicațiilor mobile cu cerințele privind accesibilitatea
    - **Proiectul va respecta Normele de monitorizare aprobate prin Decizia nr. 815/2022 prin:**
      - **Monitorizare continuă**: Implementarea unui sistem de monitorizare continuă a conformității site-urilor web și a aplicațiilor mobile cu cerințele de accesibilitate, asigurându-se că toate componentele digitale sunt accesibile tuturor utilizatorilor.
      - **Raportare periodică**: Generarea de rapoarte periodice privind starea conformității și luarea măsurilor corective necesare pentru a remedia eventualele deficiențe identificate.
11. Legea nr. 232 din 19 iulie 2022 privind cerințele de accesibilitate aplicabile produselor și serviciilor
    - **Proiectul va respecta cerințele Legii nr. 232/2022 prin:**
      - **Produse accesibile**: Asigurarea că toate produsele digitale dezvoltate în cadrul proiectului, inclusiv portalul web și aplicațiile mobile, respectă cerințele de accesibilitate stabilite de lege.
      - **Formare și conștientizare**: Organizarea de sesiuni de formare pentru personalul implicat în dezvoltarea și întreținerea produselor digitale, pentru a asigura o înțelegere completă a cerințelor de accesibilitate și a modului de implementare a acestora.

12. Măsuri adiționale și respectarea altor acte normative

- **Pe parcursul realizării investiției, vor fi aplicate orice alte acte normative naționale aplicabile în domeniul digitalizării serviciilor publice. Acestea includ, dar nu se limitează la:**
  - **Conformitate legală**: Asigurarea conformității cu toate reglementările legale aplicabile, inclusiv cele privind protecția datelor, securitatea cibernetică, accesibilitatea și interoperabilitatea.
  - **Actualizări și adaptări**: Monitorizarea continuă a cadrului legislativ și adaptarea rapidă a proiectului pentru a reflecta orice modificări sau actualizări ale legislației naționale.
- Măsurile de securitate implementate precum și produsele sau serviciile achiziționate vor respecta următoarele reglementări în vigoare:
  - utilizarea soluțiilor antivirus de proveniență rusă în instituțiile publice este reglementată de Legea nr. 354 din 13 decembrie 2022. Această lege interzice achiziționarea și utilizarea, de către autoritățile și instituțiile publice la nivel central și local, a produselor și serviciilor software de tip antivirus provenind direct sau indirect din Federația Rusă.
  - Ordonanța de Urgență a Guvernului nr. 155/2024, ce a transpus Directiva Uniunii Europene 2022/2555 (NIS2) în legislația națională. Aceasta extinde obligațiile de securitate și la instituții din cadrul administrației publice centrale, precum ANS.

4.4 Cerințe funcționale ale sistemului

Noua aplicație informatică va trebui să digitalizeze și să susțină serviciile, activitățile și procesele de lucru ale ANS, în relația cu federațiile sportive, cluburile, sportivii, bazele sportive, concursurile pe plan național și internațional.

Sistemul:

- va permite managementul ciclului de viată al următoarelor tipuri de entități precum și facilitarea relaționării dintre ele atât ca servicii publice precum și ca procese interne de lucru ale ANS: federații, cluburi, sportivi, baze sportive, competiții interne și internaționale, rezultate sportive, formare profesională antrenori, rezultate și artefacte istorice sportive.
- va permite gestionarea fluxurilor de lucru interne pentru emiterea și managementul certificatelor de identitate sportivă, pentru federațiile sportive și pentru cluburile sportive.
- va permite de asemenea managementul contractelor de finanțare pentru federațiile sportive afiliate.
- va permite federațiilor și cluburilor să-și actualizeze singuri lista de sportivi per ramuri sportive, să înregistreze competițiile din calendarul competițional intern și extern cu rezultatele aferente.va oferi prin portalul public, secțiuni destinate sportivilor și antrenorilor, unde sportivii pot vizualiza istoricul sportiv, pot inițiа transferuri inter-cluburi sau între ramuri sportive etc. (Pașaport sportiv) iar antrenorii își pot vedea istoricul.va permite realizarea automată a tuturor statisticilor anuale de tip Anuarul

Sportului, pe baza rezultatelor sportive introduse de federații sau cluburi în prealabil.va permite digitalizarea Galeriei Marilor Sportivi, cu toate artefactele acesteia. Toate artefactele vor fi disponibile public, digital, iar pentru o minoritate a acestora se va realiza un tip de vizualizare tur virtual-muzeu.

Procesul de omologare a bazelor sportive va fi de asemenea inclus în aplicație alături de procesele interne de lucru ale Centrului National de Formare si Perfecționare a Antrenorilor.

În acest context, în cadrul proiectului se are în vedere **transformarea digitală a serviciilor publice ale ANS, la un grad de sofisticare 4**, care să asigure o interacțiune digitală avansată dintre ANS și beneficiarii serviciilor publice furnizate de acesta. La nivel European există 5 grade de sofisticare a serviciilor electronice: informarea, interacțiunea, interacțiunea bidirecțională, tranzacționarea și personalizarea, respectiv: grad 1 - există materiale de informare online pentru serviciul public; grad 2 - interacțiunea cu cetățeanul se face într-un singur sens (de exemplu, descărcarea formularelor electronice); grad 3 - interacțiunea cu cetățeanul are loc în ambele sensuri (de exemplu, completarea formularelor online); grad 4 - au loc tranzacții în folosirea serviciului public online. Trebuie să fie incluse modalități de decizie, notificare, livrare și plată a serviciilor publice; grad 5 - serviciile sunt automatizate, personalizate – centrate pe utilizator.

Serviciile publice ce trebuie digitalizate sunt prezentate în tabelul de mai jos:

Table 1 - Serviciile publice ce urmează a fi digitalizate

Nr. Crt.	Serviciul public	Departamentul care furnizează serviciul	Registru/Modul asociat	Baza legală
1	Eliberare Certificat de Identitate Sportivă	ANS - Direcția Sport	Registrul Structurilor Sportive (Federații, Cluburi)	HG 576/2023 Art 4 (1) k) recunoaște sau revocă, potrivit legii, existența unei structuri sportive prin înscrierea, respectiv radierea acesteia din Registrul sportive; l) avizează constituirea structurilor sportive, inclusiv înscrierea ca persoane juridice a cluburilor sportive profesioniste organizate ca societăți sportive pe acțiuni, respectiv retrage avizul de funcționare a acestora;
2	Eliberare Carnet Maestru Emerit al Sportului, Carnet Antrenor Emerit	ANS - Direcția Sport	Registrul Sportivilor și Antrenorilor	Ordinul MTS nr. 1072/2016 privind acordarea titlurilor de "Maestru emerit al sportului", "Maestru al sportului", respectiv de "Antrenor emerit"

Nr. Crt.	Serviciul public	Departamentul care furnizează serviciul	Registru/Modul asociat	Baza legală
3	Aprobare prealabilă necesară organizării de competiții internaționale	ANS - Direcția Sport	Registrul Structurilor Sportive (Federații)	HG 576/2023 Art 4 (1) o) autorizează desfășurarea pe teritoriul României a campionatelor mondiale, europene și regionale și participarea reprezentativelor naționale la campionatele mondiale și europene organizate în străinătate, precum și la campionatele regionale;
4	Răspuns petiții/solicitare informații	ANS – Serviciul Comunicare	Registratură	
5	Eliberare Pașaportul Sportivului	ANS & INCS	Registrul sportivilor si antrenorilor	Ordin ANS 302/2023 pentru aprobarea Regulamentului privind constituirea Registrului național al sportivilor şi antrenorilor HG 576/2023 Art 4 (1) i) supraveghează și controlează respectarea de către structurile sportive a dispozițiilor legale în vigoare și a prevederilor cuprinse în statutele și în actele de constituire a acestora;
6	Eliberare Pașaportul Antrenorului	ANS & INCS	Registrul sportivilor si antrenorilor	Ordin ANS 302/2023 pentru aprobarea Regulamentului privind constituirea Registrului național al sportivilor și antrenorilor HG 576/2023 Art 4 (1) i) supraveghează și controlează respectarea de către structurile sportive a dispozițiilor legale în vigoare și a prevederilor cuprinse în statutele și în actele de constituire a acestora;
7	Serviciu programare vizita Galeria Marilor Sportivi	ANS – Galeria Marilor Sportivi	Galeria Marilor Sportivi	Ordin MTS 734/2015

Nr. Crt.	Serviciul public	Departamentul care furnizează serviciul	Registru/Modul asociat	Baza legală
8	Eliberare certificat de absolvire	CNFPA	Registrul scolii de antrenori	HG 576/2023 Art 4 (1) j) organizează sau sprijină, potrivit legii, formarea, pregătirea profesională și perfecționarea specialiștilor din domeniul sportului, conlucrând în acest scop cu instituțiile și organismele de specialitate din țară și din străinătate;
9	Eliberare carnete antrenor	CNFPA	Registrul scolii de antrenori	HG 576/2023 Art 4 (1) j) organizează sau sprijină, potrivit legii, formarea, pregătirea profesională și perfecționarea specialiștilor din domeniul sportului, conlucrând în acest scop cu instituțiile și organismele de specialitate din țară și din străinătate;
10	Certificat de clasificare profesionala	CNFPA	Registrul scolii de antrenori	HG 576/2023 Art 4 (1) j) organizează sau sprijină, potrivit legii, formarea, pregătirea profesională și perfecționarea specialiștilor din domeniul sportului, conlucrând în acest scop cu instituțiile și organismele de specialitate din țară și din străinătate;
11	Recunoaștere a titlurilor de calificare profesionala pentru profesia de antrenor, obținute într-un stat membru al Uniunii Europene, al Spațiului Economic European, in Confederația Elvețiana sau într-un stat terț.	CNFPA	Registrul scolii de antrenori	HG 576/2023 Art 4 (1) j) organizează sau sprijină, potrivit legii, formarea, pregătirea profesională și perfecționarea specialiștilor din domeniul sportului, conlucrând în acest scop cu instituțiile și organismele de specialitate din țară și din străinătate;

Descrierea succintă a serviciilor publice ce urmează a fi digitalizate este realizată în cele ce urmează:

1. Răspuns petiții/solicitare informații: digitalizarea activităților de registratura, prin posibilitatea transmiterii solicitărilor online, clasificarea automată a acestora și transmiterea către departamentele responsabile. Acest modul are rolul de a oferi posibilitatea managementului digital și automat al solicitărilor de orice fel, ce nu se încadrează deja în alte categorii de mai jos.
2. Eliberarea și managementul certificatelor de identitate sportivă (depunerea documentației, procesul de management al solicitării de recunoaștere și înscriere în Registrul sportiv organizat la ANS, emiterea digitală a certificatului de identitate sportivă, revocarea recunoașterii funcționării structurilor sportive și radierea acestora din Registrul sportiv):
    a. Managementul registrului federațiilor sportive în baza legii sportului (69/2000): depunerea a documentației în vederea înregistrării în Registrul sportiv organizat la ANS, procesul de management al solicitării de recunoaștere și înscriere în Registrul sportiv/finanțare, emiterea digitală a certificatului de identitate sportivă, revocarea recunoașterii funcționării federațiilor sportive naționale și radierea acestora din Registrul sportiv, actualizare date oficiale federație, crearea de conturi de utilizator specifice pentru federație în vederea actualizării datelor proprii.
    b. Managementul registrului cluburilor sportive: depunerea a documentației în vederea înregistrării în Registrul sportiv organizat la ANS, procesul de management al solicitării de recunoaștere și înscriere în Registrul sportiv, emiterea digitală a certificatului de identitate sportivă, revocarea recunoașterii funcționării cluburilor sportive și radierea acestora din Registrul sportiv.
    c. Managementul registrului altor tipuri de structuri sportive: asociații județene și ale municipiului București pe ramură de sport, ligi profesioniste, asociații sportive, alte organizații sportive naționale.
3. Managementul registrului sportivilor și antrenorilor: înrolare, asociere sportiv per club și federație, stocare rezultate sportive și istoric sportiv, afișare informații disponibile către beneficiari precum și către sportiv (portal public), definire workflow-uri de înrolare/legitimare/afiliere/dezafiliere sportiv la club/ramură sportivă/federație.
    a. Pașaportul sportivului: spațiu public digital destinat sportivului, în care sportivul sau tutorele legal, își poate vizualiza istoricul sportiv, rezultate, și poate iniția workflow-uri de tip: înrolare/legitimare club sportiv, obținere viză medicală, transferul între cluburi etc.
    b. Pașaportul Antrenorului: spațiu public digital destinat antrenorului, în care își poate vizualiza istoricul ca antrenor, rezultate, și poate iniția workflow-uri de tip: angajare/afiliere club sportiv, management sportivi club, istoric cariere- pregătire profesională etc.
4. Managementul registrului bazelor sportive: Evidenta si management a bazelor sportive omologate, eliberarea certificatului de omologare, revocarea certificatului de omologare.

5. Anuarul sportului: publicație oficială care compilează și prezintă informații detaliate despre activitatea sportivă din România pe parcursul unui an calendaristic, și este un instrument esențial de documentare, analiză și informare pentru toți actorii implicați în domeniul sportiv.
6. Gala Marilor Sportivi: inventarierea digitală a tuturor exponatelor, și expunerea acestora pe portalul public al ANS pentru vizionare, precum și realizarea unui tur virtual tip muzeu pentru exponatele cele mai importante.
7. Digitalizarea serviciilor publice ale CNFPA, așa cum sunt ele descrise în cadrul subcapitolului dedicat.
8. Arhivarea electronică a arhivei istorice scriptice a ANS: conversia documentelor fizice în format electronic, cât și gestionarea documentelor create direct în formă digitală, asigurând accesul facil, securitatea și integritatea informațiilor (500 ml).

În secțiunile următoare sunt prezentate cerințele funcționale detaliate ale sistemului informatic.

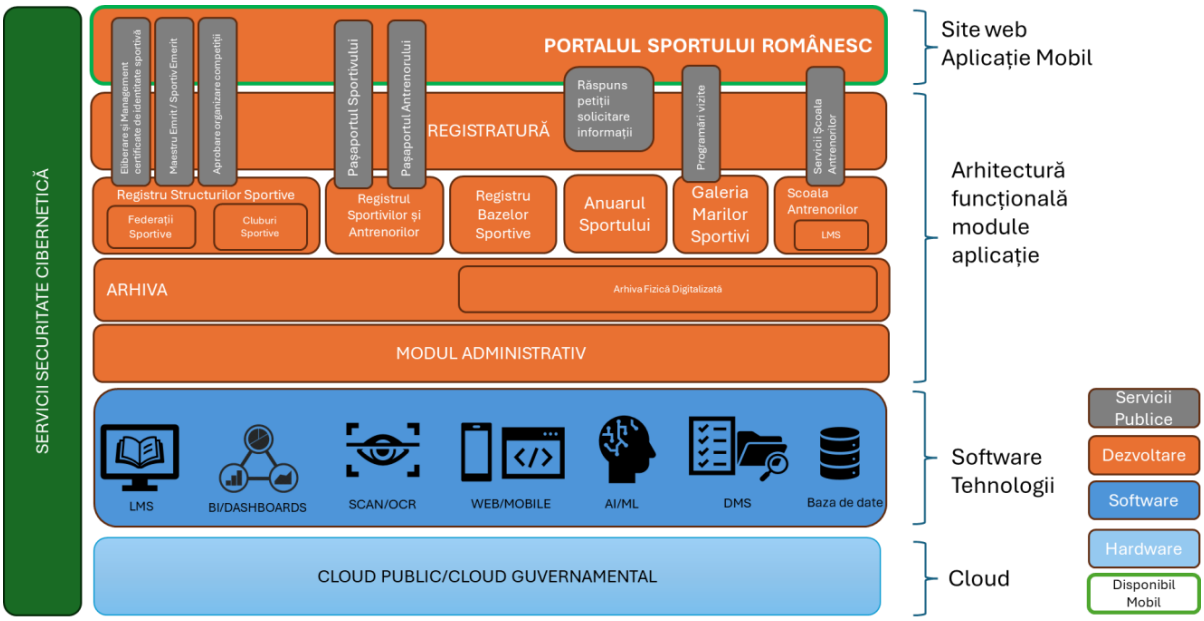
4.5 Arhitectura funcțională a sistemului

La proiectarea, realizarea și implementarea sistemului informatic, se va ține cont de următoarele principii generale:

- **Principiul legalității:** care presupune crearea și exploatarea sistemului informatic în conformitate cu legislația națională în vigoare și a normelor și standardelor internaționale recunoscute în domeniu;
- **Principiul divizării arhitecturii pe nivele:** constă în proiectarea independentă a componentelor sistemului în conformitate cu standardele de interfață dintre nivele;
- **Principiul arhitecturii bazate pe servicii:** constă în distribuirea funcționalității aplicației în unități mai mici, distincte - numite servicii - care pot fi distribuite într-o rețea și pot fi utilizate împreună pentru a crea aplicații destinate implementării funcțiilor de business ale sistemului informatic;
- **Principiul datelor sigure:** stipulează introducerea datelor în sistem doar prin canale autorizate și autentificate;
- **Principiul securității informaționale:** presupune asigurarea unui nivel adecvat de integritate, selectivitate, accesibilitate și eficiență pentru protecția datelor de pierderi, alterări, deteriorări și acces nesancționat;
- **Principiul transparenței:** presupune proiectarea și realizarea conform principiului modular, cu utilizarea standardelor transparente în domeniul tehnologiilor informatice și de telecomunicații;
- **Principiul expansibilității:** stipulează posibilitatea extinderii și completării sistemului informatic cu noi funcții sau îmbunătățirea celor existente;
- **Principiul scalabilității:** presupune asigurarea unei performanțe constante a soluției informatice la creșterea volumului de date și a solicitării sistemului informatic;

- **Principiul simplității și comodității utilizării:** presupune proiectarea și realizarea tuturor aplicațiilor, mijloacelor tehnice și de program accesibile utilizatorilor Sistemului, bazate pe principii exclusiv vizuale, ergonomice și logice de concepție;
- **Principiul integrității, plenitudinii și veridicității datelor:** presupune implementarea mecanismelor care permit păstrarea conținutului și interpretării univoce a datelor în condițiile unor influențe accidentale și eliminării fenomenelor de denaturare sau lichidare accidentală a acestora, furnizarea unui volum de date suficient executării funcțiilor de business ale sistemului informatic și asigurarea unui grad înalt de corespundere a datelor cu starea reală a obiectelor pe care le reprezintă și care fac parte dintr-un sector concret al sistemului informatic.

Dispunerea componentelor funcționale și logice este reprezentată schematic în diagrama următoare:



Figură 2 - Arhitectura funcțională

Componentele principale ale sistemului propus sunt:

- Portal Public ANS
- Modul Registratură – Management documente
- Modul Registrul Sportiv – Federații și Cluburi
- Modul Registrul Sportivilor și Antrenorilor
- Modul Registrul Bazelor Sportive
- Modul Anuarul Sportului
- Modul Galeria Marilor Sportivi
- Modul CNFPA
- Modul Arhivare electronica
- Modul Administrativ

- Chatbot/Asistent Virtual
- Rapoarte Business Intelligence
- Aplicații de mobil

Secțiunile de mai jos descriu funcțional fiecare dintre modulele prezentate în figura de mai sus. Pe lângă aceste cerințe detaliate, specifice, aplicația trebuie să implementeze și următorul set de funcționalități, cross-module:

Tipuri de conturi/acces:

- Sportiv (vizualizare istoric individual, inițiere proces de transfer sau dezafiliere).
- Personal Federație Sportivă (Administrator sau Utilizator; drepturi de modificare asupra cluburilor,
- calendarului competițional și sportivilor afiliați, ramurilor sportive).
- Personal Club Sportiv (Administrator sau Utilizator: drepturi de modificare a sportivilor)
- Personal ANS: Administrator, Utilizator Managerial și Utilizator (drepturi în funcție de necesități).
- Personal CNFPA: Administrator, Utilizator CNFPA (drepturi doar pentru fluxurile de lucru ale CNFPA).
- Galeria Marilor Sportivi: Administrator sau Utilizator (drepturi pentru actualizare/modificare baza de date artefacte, procesare bilete online).

4.5.1 Portal Public ANS

Un portal public este o interfață digitală accesibilă publicului larg prin intermediul internetului. Acesta servește ca punct de intrare centralizat către diverse servicii, informații sau resurse oferite de către o organizație, guvern sau altă entitate.

Portalul public ANS reprezintă interfața instituției cu publicul, respectiv modalitatea prin care serviciile digitalizate ale instituției sunt disponibile populației/partenerilor.

Portalul public al ANS va include tot conținutul prezentului site precum și noile funcționalități ce urmează a fi dezvoltate.

Portal public al ANS va fi conceput ca un ecosistem digital centralizat, având obiectivul dublu de a asigura migrarea și integrarea exhaustivă a conținutului existent, simultan cu implementarea noilor module funcționale prevăzute în prezentul Caiet de sarcini.

Din perspectivă operațională, platforma va acționa ca o interfață unică de transparență instituțională, diseminând către marele public informații esențiale precum datele administrative (program, contact), statistici de performanță, Anuarul Sportului, precum și registrul actualizat al federațiilor și cluburilor sportive.

Complementar palierului public, arhitectura sistemului va include zone cu acces controlat (autentificat), dedicate exclusiv stakeholderilor instituționali (federații, sportivi, structuri sportive), ale căror specificații funcționale sunt detaliate în secțiunile următoare. Întreaga soluție va fi livrată sub forma unei platforme web unificate, optimizată pentru accesibilitate multi-device, garantând o experiență fluidă, inclusiv pe terminalele mobile.

Toate funcționalitățile vor fi unificate în cadrul unei singure aplicații web, accesibilă și de pe dispozitive mobile.

Componenta Front-office, va asigura accesul online la serviciile gestionate exclusiv de către Autoritatea Contractantă și va fi compusă din:

- Portal web;
- Facilități de transmitere integral electronică a documentelor aferente solicitărilor;
- Primirea electronică a răspunsurilor sau a documentelor solicitate, cu sau fără semnătură electronică;
- Informare/asistență online cu privire la serviciile publice;
- Transmitere de notificări cu privire la statusul serviciilor publice accesate de un cetățean.

Cerințele pentru fiecare dintre secțiunile private sunt prezentate în subcapitolele următoare.

4.5.1.1 Cerințe funcționale

1. Portal și interfață utilizator

- Soluția trebuie să fie implementată ca un portal web centralizat care să acționeze ca interfață unică de acces pentru toți beneficiarii
- Portalul trebuie să includă o structură de navigație logică și intuitivă (ghidare contextuală), concepută pentru a permite utilizatorilor să identifice și să acceseze rapid problematica administrativă dorită.
- Portalul trebuie să afișeze, în mod structurat, informații detaliate și actualizate privind documentele necesare, procedurile și condițiile de eligibilitate pentru eliberarea de acte, autorizări sau certificate.

2. Acces și autentificare utilizatori

- Sistemul trebuie să permită accesul anonim (fără autentificare) la secțiunile și serviciile de natură publică (ex: informare procedurală, descărcare de formulare, etc.).
- Accesarea serviciilor care implică date personale sau care necesită dovedirea identității solicitantului trebuie să fie condiționată de o autentificare prealabilă pe baza unui cont de utilizator valid.
- Identificatorul unic al contului de utilizator în Portal trebuie să fie adresa de e-mail a utilizatorului.
- Sistemul trebuie să implementeze mecanisme de validare care să asigure unicitatea adresei de email la nivelul întregii baze de utilizatori a Portalului.
- Adresa de email a utilizatorului trebuie să fie utilizată ca principal canal electronic de corespondență și notificare cu acesta.
- Serviciile ce impun legal dovedirea identității vor fi accesibile doar utilizatorilor care s-au autentificat cu succes și al căror cont a fost supus unui proces de verificare a identității.

3. Servicii electronice

- Sistemul trebuie să fie capabil să gestioneze și să implementeze două categorii distincte de servicii: Servicii Electronice Complete și Servicii Electronice Parțiale.
- Serviciile Complete trebuie să permită utilizatorilor transmiterea integrală, electronică, a dosarelor/solicitărilor și primirea ulterioară, tot în format electronic, a răspunsurilor oficiale sau a documentelor solicitate.
- Serviciile Parțiale trebuie să permită inițierea electronică a solicitării și depunerea documentelor, dar să necesite ridicarea documentelor finale emise de la ghișeu

4. Formulare și depunere solicitări

- Portalul trebuie să ofere o secțiune dedicată inițierii de demersuri administrative prin completarea de formulare electronice web.
- Formularele web trebuie să suporte o gamă diversă de solicitări, incluzând: solicitări de informații, depunere online de documente, depunere de petiții și înscrieri în audiență. Pentru depunerea de petiții si înscrierea in audienta trebuie sa existe secțiuni separate.
- Accesibilitatea funcționalităților de solicitare (autentificat vs. neautentificat) trebuie să fie configurabilă la nivel de serviciu.
- Sistemul trebuie să implementeze o funcționalitate de pre-populare (auto-completare) a câmpurilor din formularele web, utilizând datele deja stocate în profilul utilizatorului autentificat
- Funcționalitatea de pre-populare trebuie să poată fi configurată și aplicată în mod selectiv pentru fiecare formular web aferent unui serviciu electronic.

5. Documente și generare PDF

- Sistemul trebuie să ofere utilizatorilor posibilitatea de a descărca formulare tipizate oficiale în format electronic (ex: PDF, .doc, .docx, etc), destinate serviciilor care, din motive legale sau procedurale, necesită predare fizică la ghișeu.
- Imediat după completarea formularului web, Portalul trebuie să genereze automat un fișier PDF care să replice vizual formatul tipizat oficial al instituției.
- Fișierul PDF generat automat trebuie să fie completat automat cu datele structurate introduse de solicitant prin formularul web.

6. Spațiu Privat Virtual (SPV)

- Sistemul trebuie să ofere utilizatorilor autentificați un spațiu privat virtual SPV securizat (profil sau "My Account") destinat stocării datelor și personalizării serviciilor.
- Spațiul privat trebuie să permită utilizatorului stocarea, vizualizarea și actualizarea datelor sale de contact permanente.
- Spațiul privat trebuie să suporte funcționalitatea de încărcare și stocare securizată (upload) a documentelor justificative frecvent utilizate în solicitări (ex. copia scanată a C.I.). Aceste fișiere pe care le încarcă ulterior poate sa le vizualizeze si sa le folosesc in momentul depuneri oricărui formular.

- Sistemul trebuie să stocheze automat și să facă disponibile în spațiul privat virtual SPV toate documentele oficiale eliberate electronic de către instituție ca răspuns la solicitările utilizatorului.
- Sistemul trebuie să mențină și să afișeze în spațiul privat un istoric complet al tuturor interacțiunilor utilizatorului, incluzând solicitările transmise și documentele primite.
- Sistemul trebuie să permită utilizatorului autentificat să acceseze spațiul virtual privat pentru a-și actualiza și gestiona informațiile și documentele stocate in orice moment.

7. Notificări și status solicitări

- Sistemul trebuie să gestioneze și să realizeze informarea automată a solicitantului (prin email) cu privire la stadiul actual al rezolvării solicitării sale.
- Sa ofere posibilitatea de a vizualiza in orice moment care este stadiul prelucrări documentului depus. Ulterioarele completări de documente care sunt solicitate sa fie transmise pe email, apoi in email sa existe un link prin intermediul căruia sa fi redirecționa pe portal si sa iți ofere posibilitatea de a depune ulterior documente adiționale.

8. Interacțiune și suport utilizatori

- Sistemul trebuie să includă un mecanism integrat de colectare a feedback-ului de la utilizatori (rating, comentarii) pe fiecare serviciu, pentru a facilita îmbunătățirea continuă.
- Portalul trebuie să includă o interfață de tip chatbot (asistent virtual) pentru a răspunde la întrebări frecvente și a oferi ghidare contextuală utilizatorilor. In plus pe lângă funcționalul de a răspunde la diferite întrebări acest asistent virtual trebuie sa completeze diverse formulare si sa genereze diverse documente pe baza detaliilor care le deține despre persoana in cauza atât pe baza datelor cat si a documentelor pe care acesta le are in SPV. Acest Chatbot trebuie sa includă un NLP (natural language processing) inteligent care dintr-un panou de administrare sa existe posibilitatea de al antrena si al limita doar la contextul specificului instituției. Nu se accepta integrări cu ChatGPT, Gemini, DeepSeek si alte tool-uri din sfera aceasta. Se dorește un model propriu.

9. Funcționalități specifice (muzeu)

- Soluția trebuie să permită achiziționarea online a biletelor pentru muzeu, prin selectarea tipului de bilet, a datei și intervalului orar, calcularea automată a prețului și generarea unui bilet electronic cu cod unic.
- Soluția trebuie să includă o zonă dedicată prezentării muzeului, a exponatelor in 2D, 3D și a expozițiilor, care să ofere informații detaliate despre descriere, perioadă de desfășurare, program de vizitare, tarife și materiale multimedia.

10. Administrare

- Soluția trebuie să asigure un panou de administrare securizat, prin care administratorii să poată gestiona utilizatorii, expozițiile și rezervările de bilete, precum și să genereze rapoarte privind activitatea portalului.

4.5.1.2 Cerințe funcționale configurabile

1. Funcționalități muzeu

- Soluția va trebui să ofere un sistem de gestionare a serviciilor muzeului, care să includă bilete și informații despre expoziții, detaliile funcționale urmând a fi stabilite în etapa de analiză.
- Soluția trebuie să includă o zonă publică pentru prezentarea muzeului și a expozițiilor, iar structura, conținutul și modul de afișare vor fi definite în analiza sistemului.
- Soluția trebuie să permită rezervarea și achiziția biletelor online, detaliile privind tipurile de bilete, tarifele și fluxul de plată urmând a fi stabilite în etapa de analiză.

2. Management conținut public

- Soluția trebuie să asigure administrarea și actualizarea conținutului publicat, funcționalitățile exacte și modul de implementare vor fi stabilite in etapa de analiza ulterior.
- Soluția trebuie să permită definirea și configurarea tuturor informațiilor vizibile public (fără autentificare) acestea vor fi stabilite în urma etapei de analiză.
- Soluția trebuie să permită administrarea conținutului public dintr-un panou de administrare (pagini, secțiuni, bannere, texte, media) toate acestea vor fi stabilite in etapa de analiza.
- Soluția trebuie să permită definirea paginilor publice obligatorii (ex. Termeni și condiții, Politică de confidențialitate, Contact), conform cerințelor stabilite în analiză.

3. Formulare și fluxuri

- Soluția trebuie să permită definirea tuturor tipurilor de formulare (înregistrare, profil, cereri, contact, aplicare, feedback etc.) în etapa de analiză a proiectului.
- Soluția trebuie să permită configurarea fluxurilor asociate formularelor (ex. validare, aprobare, respingere, notificare), conform cerințelor din analiză.
- Soluția trebuie să permită atașarea de documente în formulare, cu reguli clare de validare (format, dimensiune, număr fișiere), conform analizei.

4. Notificări și date

- Soluția trebuie să permită configurarea notificărilor (email/in-app/SMS) asociate fluxurilor și acțiunilor portalului, conform etapei de analiză.
- Soluția trebuie să permită descărcarea/exportul anumitor date (ex. facturi, certificate), dacă este stabilit în etapa de analiză.

5. Raportare

- Soluția trebuie să permită generarea de rapoarte și monitorizarea activităților, indicatorii și structura rapoartelor urmând a fi definiți în etapa de analiza.

4.5.1.3 Cerințe tehnice

1. Cerințe generale

- Soluția trebuie să fie o soluție COTS, matură, licențiată perpetuu, pentru un număr nelimitat de utilizatori.

2. Arhitectură și integrare

- Integrarea software între Portal și aplicațiile interne trebuie să fie realizată primar prin servicii web standard (Web Services).
- Să ofere posibilitatea integrării unei game largi de servicii și date externe folosind tehnologii cunoscute ca SOAP, REST, dar și module API.

3. Preluare automată date & procese interne

- Sistemul trebuie să asigure preluarea automată a datelor structurate introduse de solicitant și transmiterea/introducerea acestora în bazele de date ale aplicațiilor de tip back-office ale instituției.
- Mecanismul de preluare automată a datelor trebuie să fie proiectat pentru a elimina necesitatea reintroducerii manuale a informațiilor de către funcționari în aplicațiile interne.
- Sistemul trebuie să includă un strat de validare și transformare a informațiilor structurate furnizate de solicitanți, în vederea asigurării compatibilității cu schemele altor aplicații interne.
- În urma primirii unei solicitări, Portalul trebuie să declanșeze automat fluxurile și procesele instituționale interne de rezolvare.
- Procesele declanșate automat trebuie să includă distribuirea automată a sarcinilor către personalul responsabil din departamentele instituției, conform naturii demersului.

4. Securitate & GDPR

- Canalul de comunicație dintre Portal și Aplicația de Management va fi securizat integral prin utilizarea protocoalelor de criptare a datelor în tranzit (de tip SSL/TLS). Astfel, se va asigura confidențialitatea și integritatea informațiilor schimbate între sisteme, prevenind interceptarea sau alterarea neautorizată a acestora.
- Se va implementa o soluție de securitate pentru asigurarea complianței GDPR.
- Soluția de securitate va permite audit și rapoarte specifice directivei europene GDPR, executate la nivelul infrastructurii IT.

5. Control acces & politici parole

- Restricționarea accesului utilizatorilor la anumite pagini sau secțiuni de pagini.
- Să ofere posibilitatea segregării accesului și controlului administrativ (grupuri de utilizatori, organizații, roluri, roluri administrative, politici de parole).
- Să ofere posibilitatea setării de Politici de parole personalizate ce forțează utilizatorii să folosească anumite caractere sau formate.

6. Modul Administrare

6.1 Form Builder

- Modulul de Administrare trebuie să includă un Form Builder (Constructor de Formulare) vizual de tip drag-and-drop și intuitiv, destinat configurării de către utilizatorii non-tehnici.
- Form Builder-ul trebuie să permită configurarea avansată a logicii condiționale (inteligența) în formulare (ex: ascunderea/afișarea dinamică a unor câmpuri/secțiuni).
- Form Builder-ul trebuie să ofere o interfață de administrare pentru maparea explicită a fiecărui câmp din formularul web la câmpul corespondent din schemele de integrare/baza de date Back-Office.

6.2 Generare documente

- Modulul de Administrare trebuie să permită configurarea regulilor și template-urilor pentru Generarea automată a Documentelor PDF, inclusiv definirea poziției și formatului datelor mapate.
- Modulul de Administrare trebuie să ofere o funcționalitate de previzualizare în timp real a formularelor și a logicii condiționale înainte de publicarea acestora.

6.3 Notificări

- Modulul de Administrare trebuie să ofere o interfață (CMS) pentru crearea și editarea centralizată de template-uri (șabloane) pentru toate notificările prin email generate de sistem.
- Template-urile de email trebuie să suporte inserarea de variabile dinamice (placeholders) preluate contextual din solicitarea utilizatorului sau din sistem (ex: [Nume_Utilizator], [Numar_Inregistrare]).
- Sistemul trebuie să permită administratorului să configureze notificări separate și personalizate pentru diferite etape și statusuri ale procesului (ex: Solicitare primită, Solicitare soluționată).
- Să ofere posibilitatea blocării notificărilor sau limitarea acestora în funcție de tip sau canalul de transmitere de către fiecare utilizator.

7. UX, performanță & responsive

- Să ofere facilitate de caching pentru sporirea performanței.
- Tehnologii web „responsive”: Pentru servicii simple (informare, plată, solicitare pe bază de formular), în vederea obținerii unei experiențe optime pe dispozitive mobile (smartphone și tabletă).
- Adaptarea poziției informației și a câmpurilor la dimensiunea și orientarea ecranului dispozitivului mobil utilizat.

8. Compatibilitate browsere

- Compatibilitate browsere: Utilizarea cu browserele cele mai răspândite pe calculatoarele desktop (Edge, Mozilla Firefox, Safari, Google Chrome).

9. Baze de date suportate

- Suport pentru bazele de date relaționale (MySQL, Microsoft SQL Server, Oracle, PostgreSQL).

10. Multilingvism

- Să ofere suport multilingv in limbi multiple.

11. Bibliotecă multimedia

- Să ofere o facilitate de bibliotecă multimedia (stocarea imaginilor, documentelor, fișierelor de tip video).

4.5.2 Modul Registratură – Management documente

Scopul principal al modulului este gestionarea eficientă și centralizată a tuturor documentelor și corespondenței instituției.

Acesta optimizează fluxurile de lucru interne, asigură transparența și trasabilitatea documentelor și facilitează interacțiunea cu beneficiarii externi precum federații, cluburi și sportivi.

4.5.2.1 Cerințe funcționale

Modulul va trebui sa permită înregistrarea documentelor intrate și ieșite, distribuirea automată către departamentele sau persoanele responsabile și monitorizarea în timp real a stadiului fiecărui document.

Prin acces rapid și securizat la informații, control al accesului și integrare cu alte sisteme, modulul de registratură îmbunătățește eficiența operațională, reduce costurile și asigură conformitatea cu reglementările legale privind gestionarea documentelor și protecția datelor. Implementarea acestuia contribuie la modernizarea ANS, promovând o funcționare optimă și orientată spre performanță în contextul digitalizării instituționale.

Modulul Registratură gestionează fluxurile de documente specifice, precum Registrul Structurilor Sportive, Registrul Sportivilor și Antrenorilor, Registrul Bazelor Sportive etc.

Acesta este esențial pentru organizarea și monitorizarea corespondenței între ANS și diverse entități beneficiare, asigurând trasabilitatea și centralizarea informațiilor.

Modulul Registratură trebuie integrat în ecosistemul Portalului Sportului Românesc, facilitând gestionarea eficientă a documentelor și interacțiunea cu beneficiarii.

El va trebui să se conecteze cu alte funcționalități ale aplicației, cum ar fi Arhiva și Modulul Administrativ, utilizând tehnologii precum Scan/OCR și DMS (Document Management System) pentru a îmbunătăți accesul, transparența și securitatea documentelor.

Statistică petiții/solicitări 2022-2023:

An	Petiții	Cereri informații de interes public
2023	175	142
2022	319	117

Figură 3 - Statistică petiții/solicitări 2022-2023

Registratura electronică va include toate procesele de lucru (workflow-uri) pentru toate modulele funcționale descrise în prezentul Caiet de sarcini și va funcționa ca un sistem de ticketing la nivel de instituție, alocând numere automat, ținând evidența tuturor documentelor primite/transmise, statusul acestora și persoana responsabilă.

Un workflow (flux de lucru) în contextul unui sistem informatic reprezintă o secvență automatizată de activități sau pași logici prin care datele, documentele sau sarcinile trec de la un participant la altul, în scopul îndeplinirii unui proces specific.

Acesta modelează procesele de afaceri sau operaționale ale unei organizații, asigurând că activitățile sunt realizate în ordinea corectă, de către persoanele potrivite și în conformitate cu regulile și politicile stabilite.

Elemente cheie ale unui workflow în sistemele informatice:

- Activități sau sarcini: Reprezintă acțiunile individuale care trebuie îndeplinite. Acestea pot fi automate (efectuate de sistem) sau manuale (efectuate de utilizatori).
- Secvențiere și logică de proces: Definește ordinea în care activitățile sunt realizate și condițiile sau regulile care determină fluxul de lucru (de exemplu, ramificări bazate pe decizii, bucle).
- Participanți sau roluri: Persoane sau sisteme care execută activitățile din workflow. Acestea sunt adesea definite prin roluri (ex.: "manager", "asistent", "aprobator") pentru a facilita atribuirea și gestionarea sarcinilor.
- Date și documente: Informațiile care sunt procesate și transferate între activități. Acestea pot include formulare, rapoarte, fișiere sau alte tipuri de date.
- Reguli și politici: Setul de condiții și constrângeri care guvernează comportamentul workflow-ului, asigurând conformitatea cu procedurile organizaționale și reglementările externe.

Importanța unui workflow în sistemele informatice:

- Automatizare: Reduce intervenția manuală prin automatizarea sarcinilor repetitive, ceea ce duce la eficiență crescută și reducerea erorilor.
- Standardizare: Asigură că procesele sunt urmate în mod consistent, conform standardelor și politicilor organizației.
- Transparență și monitorizare: Permite urmărirea în timp real a progresului sarcinilor, identificarea blocajelor și generarea de rapoarte pentru analiză și îmbunătățire.
- Colaborare îmbunătățită: Facilitează comunicarea și coordonarea între diferite departamente sau membri ai echipei prin clarificarea responsabilităților și așteptărilor.
- Scalabilitate: Permite gestionarea eficientă a volumelor mari de activități și adaptarea la schimbările din mediul de afaceri.

Exemplu - Procesul de aprobare a unei cereri de concediu:

- Angajatul completează și trimite o cerere.
- Cererea este automat trimisă managerului direct pentru aprobare.

- Dacă este aprobată, resursele umane sunt notificate pentru actualizare în sistem.
- Dacă este *respinsă, angajatul este notificat cu motivele respingerii*.

Metadate Critice pentru Procesarea Documentelor la Registratură

Tabelul de mai jos detaliază specificațiile metadatelor necesare pentru asigurarea trasabilității, conformității și guvernanței fluxului de documente.

Tabel 2 - specificațiile metadatelor necesare pentru asigurarea trasabilității, conformității și guvernanței fluxului de documente

Câmp	Metadată (terminologie profesională)	Descriere și funcție
Nr. înreg. (intrare)	Identificator unic de Înregistrare	ID secvențial, alocat automat la primire, esențial pentru urmărire (tracking).
Data înregistrării	Data intrării în Registrul Electronic	Timestamp-ul oficial care inițiază calculul termenului legal.
Modalitate adresare	Canal de Primire	Tipul sursei documentului (Fizic, Poștal, Electronic, Platformă).
Secțiunea Solicitant și Clasificare		
Nume petent	Numele/Denumirea Solicitantului	Identitatea fizică sau juridică a inițiatorului documentului.
Calitate petent	Tip Entitate/Rol Petent	Clasificare predefinită (Persoană Fizică, Persoană Juridică, Presă/Media).
Subiect	Rezumat Executiv al Obiectului	Descriere concisă și indexabilă a conținutului.
Domeniu	Clasificarea Tematică Principală	Categorizare detaliată (ex: Achiziții Publice, Cheltuieli Operaționale, Activitatea Liderilor Instituției).
Status L544	Încadrare Legală (Legea 544)	Flag binar care indică incidența Legii nr. 544/2001 (pentru raportare).

Câmp	Metadată (terminologie profesională)	Descriere și funcție
Secțiunea Guvernanță și Termene		
Nr. de zile pt. răspuns conf. legii	Termen Legal de Răspuns	Numărul de zile lucrătoare impuse de cadrul normativ aplicabil.
Termen răspuns (calcul automat)	Data Scadentă Automată (Deadline)	Data finală calculată de sistem pe baza Termenului Legal și a datei de intrare.
Timp de răspuns	Metrică de Performanță (Durată Procesare)	Timpul efectiv (zile/ore) necesar pentru finalizarea cazului (utilizat pentru KPI).
Secțiunea Workflow Intern și Ieșire		
Responsabil în cadrul Serviciului Comunicare	Operator de Flux	Persoana responsabilă cu monitorizarea și finalizarea procesului.
Adresă internă solicitare punct de vedere	Structura de Referință Internă	Identificarea departamentului/structurii către care s-a trimis solicitarea de informații.
Adresă internă (nr. intern și dată)	Referință Circuit Intern Inițial	Numărul și data alocate solicitării de punct de vedere interne.
Revenire adresă internă (nr. și dată)	Referință Răspuns Intern	Numărul și data primirii răspunsului de la structura internă.
Data expediere răspuns	Data Finalizării Răspunsului	Data la care documentul oficial de răspuns a fost expediat către petent.
Nr. ieșire răspuns	Identificator Ieșire (ID de Expediere)	Numărul unic al documentului oficial din registrul de ieșire.

Câmp	Metadată (terminologie profesională)	Descriere și funcție
Modalitate comunicare răspuns	Canal de Răspuns	Metoda utilizată pentru expediere (Poștă Recomandată, Email Semnat, etc.).
Observații	Jurnal de Proces / Note de Audit	Câmp text pentru notarea aspectelor specifice, esențiale pentru auditabilitatea cazului.
Reclamație administrativă sau plângere în instanță	Stadiu Litigios (Monitorizare Risc)	Flag care indică dacă documentul escaladează într-un nivel de contestație legală.

4.5.2.2 Cerințe tehnice

Soluția trebuie să fie o soluție COTS, matură, licențiată perpetuu, pentru un număr nelimitat de utilizatori.

Modulul pentru managementul documentelor va avea cel puțin următoarele module, dezvoltate de același producător si proiectate pentru o funcționare împreună în același sistem:

- Depozit si captura de documente
- Registratură electronica
- Fluxuri de lucru

4.5.2.2.1 Depozit si captura de documente

Modulul depozit de documente va asigura constituirea depozitului de documente electronice operaționale, asigurând funcționalitățile minimale enumerate în cadrul acestui capitol, grupate pe categorii.

Organizare

- Sistemul va trebui sa asigure stocarea documentelor într-un depozit centralizat, accesibil integral prin intermediul unei interfețe web.
- Modelul de date trebuie să permită tratarea documentului și a metadatelor asociate, fără limitări tehnice privind numărul de atribute, volumul de documente sau capacitatea totală de stocare gestionată. Această structură va trebuie sa permită definirea de seturi de metadate specifice pentru fiecare tip de document, facilitând regăsirea rapidă și organizarea logică.
- Soluția trebuie să permită organizarea documentelor într-o structură arborescentă intuitivă.
- Sistemul va trebui sa integreze mecanisme de administrare a termenelor de păstrare și arhivare automată în funcție de tipul documentului. Pentru optimizarea spațiului și a

acurateței datelor, vor fi implementate instrumente de identificare a fișierelor duplicat, bazate atât pe denumire, cât și pe amprenta digitală a conținutului.

- Sistemul va oferi utilizatorilor funcționalități de productivitate, precum marcarea documentelor accesate frecvent într-o secțiune de "Favorite". De asemenea, aplicația trebuie să permită crearea de "colecții de documente" – grupări logice temporare de fișiere din depozit, destinate unor grupuri de lucru specifice (comisii, echipe de proiect). Aceste colecții vor permite accesul controlat la un set de documente eterogene, fără a fi necesară mutarea sau multiplicarea fizică a acestora din locațiile lor originale.
- Sistemul trebuie să asigure securitatea datelor prin definirea de drepturi de acces granulare la nivel de dosar, document sau metadate, asigurând conformitatea cu politicile de confidențialitate.
- Orice modificare adusă structurii organizatorice, editarea metadatelor sau accesarea documentelor va fi înregistrată automat într-un jurnal de audit (audit trail).

Definire structură organizatorică organigramă care sa conțină elementele organizaționale din cadrul instituției, responsabili de aceste departamente si relațiile de subordonare. Sistemul trebuie sa permită:

- Posibilitatea de a vizualiza toate departamentele și compartimentele sub formă de tabel.
- Trebuie să existe funcționalitatea de a adăuga un departament nou prin butonul dedicat.
- Modulul trebuie să permită comutarea vizualizării din lista departamente către un vizual de "Organigramă".
- Posibilitatea de a căuta un departament specific folosind o bară de căutare.
- Modulul trebuie să permită utilizatorului să selecteze numărul de rânduri afișate pe pagină (ex: 50 rânduri).
- Trebuie să existe funcționalitatea de a exporta datele din tabel în formatele: Excel, CSV, PDF.
- Posibilitatea de a copia datele din tabel în clipboard ("Copy") și de a le tipări direct ("Print").
- Modulul trebuie să permită sortarea coloanelor (ascendent/descendent).
- Posibilitatea de a edita detaliile unui departament existent.
- Posibilitatea de a șterge un departament din sistem, cu atenționare cu privire la legăturile care vor fi afectate.
- Posibilitatea de a selecta departamentul ierarhic superior dintr-o listă de tip dropdown.
- Posibilitatea de a desemna un coordonator de compartiment dintr-o listă de utilizatori.
- Posibilitatea de a vizualiza sau selecta tipul compartimentului (ex: Serviciu).
- Modulul trebuie să permită adăugarea unei descrieri textuale detaliate a compartimentului.

- Trebuie să existe funcționalitatea de a asocia mai mulți utilizatori ai platformei unui singur compartiment (multi-select/tags).
- Trebuie să existe funcționalitatea de a genera vizual o organigramă arborescentă care să reflecte ierarhia instituției (de la Director Executiv până la compartimente specifice).
- Modulul trebuie să afișeze clar relațiile de subordonare (părinte-copil) între entități.
- Posibilitatea de a naviga înapoi la lista tabelară din modul de vizualizare grafică.

Indexare

- Sistemul trebuie să repartizeze automat documentele în folderele corespunzătoare pe baza unor reguli predefinite (ex: tip document, dată, emitent), eliminând sortarea manuală.
- Aplicația va avea capacitatea de a genera automat directoare noi dacă structura necesară stocării nu există deja.
- Sistemul va indexa atât atributele fișierului (autor, dată, titlu), cât și întreg conținutul text (Full-Text Search), permițând regăsirea informației după cuvinte cheie.
- Indexarea se va realiza nativ pentru o gamă largă de formate: pachetul MS Office (Word, Excel), fișiere structurate (XML), PDF-uri și formate grafice (JPEG, TIFF, BMP).
- Pentru fișierele de tip imagine și PDF-urile scanate, sistemul va iniția automat procesul de OCR (recunoaștere optică a caracterelor) în fundal. Această procesare se va executa asincron, fără a afecta performanța sau disponibilitatea aplicației pentru utilizator. În oferta tehnică, Ofertantul trebuie să detalieze modul prin care acest proces rulează izolat de fluxul principal.
- Textul din imagini va fi convertit în format editabil/indexabil, devenind astfel vizibil pentru motorul de căutare al aplicației.

Încărcarea/descărcarea documentelor electronice

- Trebuie să existe funcționalitatea de a deschide o fereastră modală (pop-up) cu titlul "Selectează fișier" pentru gestionarea documentelor.:
- Posibilitatea de a încărca fișiere prin mecanismul "Drag & Drop" (tragere fișiere în zona marcată).
- Trebuie să existe funcționalitatea de a deschide selectorul de fișiere al sistemului de operare prin click pe zona de încărcare.
- Modulul trebuie să permită scanarea directă a documentelor fizice printr-un buton dedicat "Scanează".
- Modulul trebuie să afișeze o listă a fișierelor disponibile, prezentând pentru fiecare: iconița specifică formatului (PDF, Word, Imagine), numele fișierului, data și ora încărcării, precum și utilizatorul care l-a încărcat.
- Trebuie să existe funcționalitatea de a filtra sau căuta un fișier specific folosind bara de "Căutare...".
- Modulul trebuie să suporte diverse tipuri de fișiere (PDF, .docx, .jpeg, .png).

- Posibilitatea de a șterge definitiv un fișier din listă folosind butonul "Șterge".
- Trebuie să existe funcționalitatea de a selecta un fișier pentru a fi utilizat în procesul curent.
- Posibilitatea de a previzualiza conținutul documentului într-o fereastră dedicată ("Preview Document") înainte de descărcare sau tipărire.
- Modulul trebuie să permită navigarea între paginile documentului (afișare "1 / x").
- Trebuie să existe funcționalitatea de a ajusta nivelul de zoom (mărire/micșorare) și de a vedea procentul de afișare.
- Posibilitatea de a roti documentul sau de a ajusta modul de vizualizare (fit to width/height).
- Modulul trebuie să permită descărcarea documentului curent.
- Trebuie să existe funcționalitatea de a tipări documentul direct din fereastra de previzualizare.
- Modulul trebuie să randeze corect elementele grafice din documente (ștampile, semnături, antete colorate, etc).
- Modulul trebuie să permită configurarea unei acțiuni automate de tip "Semnătură Electronică" la finalizarea etapei de redactare a unui răspuns.
- Modulul trebuie sa permită semnarea documentelor direct in platforma.
- Modulul trebuie sa atenționeze utilizatori care au de semnat documente sau fac parte dintr-un flux de semnare, cu notificări prin email, sau notificări de tip push, in aplicație.
- Trebuie să existe funcționalitatea de a adăuga o etapă nouă în flux-ul deja definit. • Posibilitatea de a defini ordinea persoanelor care trebuie sa semneze documentul.
- Modulul trebuie să permită denumirea specifică a fiecărei etape (ex: "Aprobare", "Verificare", "Avizare").
- Trebuie să existe funcționalitatea de a selecta tipul etapei dintr-o listă predefinită (ex: "Aprobare").
- Posibilitatea de a asocia un departament specific fiecărei etape (ex: "Departament Financiar", "Comercial").
- Modulul trebuie să permită desemnarea unui utilizator specific care să primească sarcina în acea etapă (ex: "Utilizator1").
- Trebuie să existe funcționalitatea de a bifa opțiunea "Aprobare" sau "Avizare" pentru a defini natura deciziei în etapa respectivă.
- Posibilitatea de a activa opțiunea "Începe după ce a fost aprobat de" pentru a crea dependențe între etape.
- Modulul trebuie să permită selectarea dintr-o listă a etapei anterioare care condiționează pornirea etapei curente.

- Posibilitatea de a vizualiza rezumatul fluxului într-un tabel cu coloanele următoare: Ordine, Denumire, Tip Etapa, Departament, Utilizator, Aprobare, Avizare, Începe după ce a fost aprobat de, Este obligatorie, Vede documentul, Semnătura electronica.
- Modulul trebuie să permită ștergerea unei etape configurate greșit.

Navigare, căutare și filtrare

- Sistemul trebuie să includă un motor de căutare avansat, capabil să indexeze și să interogheze simultan atât metadatele documentelor (titlu, autor, dată, număr înregistrare), cât și conținutul propriu-zis al acestora. Această funcționalitate trebuie să acopere obligatoriu textul extras din documentele scanate (rezultat în urma procesului OCR), asigurând regăsirea informațiilor indiferent de formatul original al fișierului.
- Soluția trebuie sa ofere mecanisme avansate de filtrare și sortare, interfața de listare a rezultatelor trebuie să ofere opțiuni de filtrare multi-criterială (faceted search) pentru a restrânge rapid seturile mari de date. Utilizatorii trebuie să poată filtra documentele cel puțin după: tipul documentului, intervale de timp, starea documentului, autor și etichete (tag-uri). De asemenea, sistemul va permite sortarea dinamică a listelor (alfabetic, cronologic, relevanță) fără reîncărcarea paginii.
- Soluția informatică va pune la dispoziție o structură de navigare intuitivă, organizată ierarhic (tip arbore de dosare sau categorii logice), care să permită utilizatorilor localizarea vizuală a documentelor. Navigarea trebuie să fie asistată de elemente de tip "breadcrumbs" pentru a indica poziția curentă în structură și pentru a facilita revenirea rapidă la nivelurile superioare.

Operații asupra documentelor/colaborare

- Modulul trebuie să permită afișarea și stocarea informațiilor de identificare ale unui document (număr unic, data emiterii și categoria/tipul documentului, etc).
- Trebuie să existe funcționalitatea de a gestiona statusurile documentului pentru a reflecta etapa în care se află acesta (ex: stadiu incipient, în lucru, finalizat).
- Posibilitatea de a înregistra și afișa datele de identificare ale unei entități externe (partener/client), inclusiv date de contact și identificatori fiscali.
- Modulul trebuie să integreze un vizualizator de documente care să permită consultarea conținutului fără descărcarea fișierului.
- Trebuie să existe funcționalitatea de a manipula vizualizarea documentului prin comenzi de zoom, rotire și navigare între pagini.
- Posibilitatea de a executa acțiuni directe de export (descărcare) și imprimare din cadrul ferestrei de vizualizare.
- Trebuie să existe funcționalitatea de a vizualiza istoricul complet al acțiunilor, cu marcaje temporale și identificarea utilizatorilor care au interacționat cu documentul.
- Posibilitatea de a diferenția vizual între etapele parcurse și cele viitoare ale unui flux de lucru.

- Modulul trebuie să pună la dispoziție butoane de control pentru avansarea documentului în următoarea etapă a fluxului (aprobare/procesare).
- Trebuie să existe funcționalitatea de a modifica sau șterge înregistrarea curentă, în funcție de drepturile de acces ale utilizatorului.
- Posibilitatea de a adăuga note interne sau observații asociate documentului sau unei etape specifice din proces.
- Modulul trebuie să pună la dispoziție multiple metode de introducere a documentelor în sistem: încărcare locală (drag-and-drop), scanare directă sau selecție din biblioteca existentă.
- Trebuie să existe funcționalitatea de a clasifica fișierele în funcție de nivelul de acces (fișiere personale vs. fișiere publice/partajate).
- Posibilitatea de a vizualiza metadatele fișierului (extensie, dimensiune, autor, data încărcării) înainte de a fi utilizat într-un proces.
- Trebuie să existe funcționalitatea de a gestiona ciclul de viață al fișierului, incluzând opțiuni de ștergere, descărcare sau imprimare directă.
- Modulul trebuie să permită crearea de fluxuri de lucru secvențiale (workflow-uri), unde fiecare etapă este definită prin roluri, responsabili și tipul de acțiune solicitat (aprobare, avizare).
- Trebuie să existe funcționalitatea de a condiționa progresul unui document în funcție de finalizarea etapelor anterioare (dependențe între pași).
- Posibilitatea de a vizualiza în timp real "traseul" documentului printr-o componentă de istoric/audit care să înregistreze fiecare interacțiune a utilizatorilor.
- Modulul trebuie să permită configurarea unor cerințe tehnice speciale pentru anumite etape, cum ar fi aplicarea obligatorie a unei semnături electronice.
- Trebuie să existe funcționalitatea de a adăuga note de subsol sau comentarii la nivel de document, vizibile pentru toți participanții din flux.
- Modulul trebuie să ofere butoane de control contextual pentru avansarea documentului de ex: "Trimite spre aprobare" sau pentru editarea datelor de bază ale acestuia.
- Modulul trebuie să integreze o componentă de editare de tip "What You See Is What You Get" (WYSIWYG) care să permită deschiderea documentelor (DOCX, XLSX) direct în interfața aplicației, eliminând necesitatea descărcării.
- Modulul trebuie să asigure compatibilitatea totală cu formatele standard, păstrând formatarea, tabelele, antetele și subsolurile exact ca în aplicațiile desktop (Microsoft Word/LibreOffice).
- Posibilitatea de a bloca documentul pentru alți utilizatori în momentul în care acesta este deschis în modul "Editare" (File Locking), pentru a evita conflictele de versiuni.
- Modulul trebuie să pună la dispoziție o bară de instrumente completă pentru formatarea textului: stiluri (headings), fonturi, aliniere, liste punctate și inserare de tabele/imagini.

- Trebuie să existe funcționalitatea de a efectua acțiuni de "Undo" și "Redo" nelimitate în timpul sesiunii de editare curente.
- Posibilitatea de a utiliza funcția "Find and Replace" (Caută și Înlocuiește) direct în interiorul documentului deschis în aplicație.
- Modulul trebuie să permită inserarea de comentarii și sugestii direct pe text (Track Changes), facilitând colaborarea între utilizatorii care revizuiesc documentul în etape diferite ale fluxului.
- Trebuie să existe funcționalitatea de a salva automat o versiune nouă a documentului după fiecare sesiune de editare finalizată, păstrând în spate istoricul complet al modificărilor (Versioning).
- Posibilitatea de a compara două versiuni ale aceluiași document direct în aplicație, evidențiind diferențele de text adăugate sau șterse.
- Modulul trebuie să permită colaborarea multi-utilizator în timp real (unde este cazul), afișând cursorul și numele utilizatorilor care editează simultan diferite secțiuni ale documentului.
- Trebuie să existe funcționalitatea de a restricționa modul "Editare" doar pentru anumite etape ale fluxului (ex: doar în etapa de "Draft" sau "Revizuire").
- Modulul trebuie să actualizeze automat zona de previzualizare imediat ce editorul este închis, astfel încât utilizatorii din următoarele etape să vadă versiunea cea mai recentă.
- Posibilitatea de a adăuga automat metadate din sistem (cum ar fi numărul de înregistrare sau data curentă) direct în conținutul documentului.
- Modulul trebuie să permită editarea simultană a aceluiași document de către mai mulți utilizatori, fără a fi necesară reîncărcarea paginii sau descărcarea fișierului.
- Trebuie să existe funcționalitatea de a vizualiza în timp real prezența celorlalți colaboratori prin indicatori vizuali (avatare sau inițiale).
- Posibilitatea de a identifica poziția exactă a fiecărui utilizator în document prin cursoare colorate individualizate, etichetate cu numele utilizatorului respectiv.
- Modulul trebuie să asigure sincronizarea instantanee a modificărilor (latență minimă), astfel încât orice caracter tasta de un utilizator să fie vizibil imediat tuturor celorlalți participanți.
- Modulul trebuie să utilizeze algoritmi avansați de rezolvare a conflictelor (ex: Operational Transformation sau CRDT) pentru a asigura că modificările simultane asupra aceluiași paragraf sunt îmbinate corect, fără pierderi de date.
- Posibilitatea de a urmări „istoria vie” a documentului, unde sistemul înregistrează cine, ce și când a modificat, permițând auditarea fiecărei intervenții în timpul sesiunii colaborative.
- Trebuie să existe funcționalitatea de a adăuga comentarii direct pe secțiuni de text selectate, creând fire de discuție între utilizatori direct în interiorul documentului.

- Modulul trebuie să permită utilizarea funcției de "Tagging" (menționarea unui coleg folosind @Nume) pentru a atrage atenția unui anumit utilizator asupra unei secțiuni care necesită revizuire.
- Posibilitatea de a activa modul „Sugestii” (Track Changes colaborativ), unde modificările propuse de un utilizator sunt marcate distinct și trebuie aprobate sau respinse de proprietarul documentului.
- Modulul trebuie să permită definirea unor drepturi granulare de acces la nivel de document: "Doar Vizualizare", "Comentator" sau "Editor Complet".
- Trebuie să existe funcționalitatea de a restricționa editarea anumitor zone din document (ex: antet, subsol sau clauze contractuale fixe) prin utilizarea de secțiuni protejate/blocate.
- Modulul trebuie să ofere o experiență de editare fluidă, cu suport pentru scurtături de tastatură (Hotkeys) identice cu cele din aplicațiile desktop (Ctrl+C, Ctrl+V, Ctrl+Z, Ctrl+S).
- Trebuie să existe funcționalitatea de a importa și exporta documente în formatele .docx și .pdf fără a altera structura de obiecte sau formatarea complexă creată în timpul editării colaborative.

Scanarea documentelor direct din aplicație

- Sistemul trebuie să permită scanarea documentelor și încărcarea acestora printr-un proces asincron, care nu blochează interfața utilizatorului.
- Conversie OCR avansată și indexare "Full-Text" pentru orice fișier încărcat (imagine sau PDF scanat), sistemul va trebui sa execute procesul de OCR (Optical Character Recognition) și conversia în format PDF/A Searchable.
- Soluția trebuie să suporte atât recunoașterea textului tipărit, cât și a scrisului de mână (ICR) de pe formulare. Scopul este ca întregul conținut al documentului să devină indexabil, permițând utilizatorilor să regăsească documentul căutând după orice cuvânt din interiorul acestuia, nu doar după titlu.
- Sistemul va trebui sa extragă automat informațiile din aceste zone (ex: număr factură, dată, CNP) și le va popula direct în metadatele fișierului. Această funcționalitate trebuie completată de un vizualizator (viewer) interactiv care permite utilizatorului să selecteze text din imagine și să îl transfere în câmpurile de metadate prin "drag and drop", pentru situațiile ad-hoc.
- Sistemul va aplica reguli de validare și chei de control asupra datelor extrase automat prin OCR (Optical Character Recognition). În cazul în care informațiile preluate nu respectă formatul definit (nu trec validarea) sau dacă gradul de încredere al recunoașterii este scăzut, documentul va fi marcat distinct pentru revizuire.
- Utilizatorii trebuie să aibă la dispoziție o interfață de validare manuală rapidă pentru a corecta erorile de extragere înainte ca documentul să intre în fluxul operațional sau să fie exportat (în formate precum JSON, DOCX sau PDF/A).

4.5.2.2.2 Registratură electronica

- Modulul trebuie să asigure gestionarea centralizată a tuturor documentelor înregistrate în sistem, indiferent de tipul acestora (intrare, ieșire, interne), printr-o interfață unitară de tip listă.
- Modulul trebuie să permită afișarea documentelor într-un tabel structurat, care să includă cel puțin: număr de înregistrare, dată, emitent/petent, adresă, tip document, tip act, conținut pe scurt, termen de soluționare și stare curentă.
- Trebuie să existe posibilitatea de a sorta documentele afișate în registru după oricare dintre câmpurile disponibile, atât crescător, cât și descrescător.
- Trebuie să existe funcționalitatea de a selecta unul sau mai multe documente simultan, în vederea aplicării unor acțiuni comune.
- Modulul trebuie să permită efectuarea de acțiuni asupra documentelor selectate, precum transmiterea către alți utilizatori sau compartimente.
- Trebuie să existe o evidențiere vizuală distinctă pentru documentele marcate ca urgente, si cele pentru care termenul este pe punctul sa expire.
- Modulul trebuie să afișeze avertizări vizuale pentru documentele care au termenul de soluționare depășit sau care se apropie de expirare.
- Trebuie să existe posibilitatea de navigare în listă prin paginare, precum și setarea numărului de înregistrări afișate pe pagină.
- Modulul trebuie să includă un mecanism de filtrare avansată care să permită restrângerea listei de documente pe baza mai multor criterii simultan.
- Trebuie să existe posibilitatea de a filtra documentele după an calendaristic și după intervale predefinite de timp (ex. ultimele luni).
- Trebuie să existe posibilitatea de a filtra documentele în funcție de compartimentul responsabil, tipul de act și starea documentului.
- Trebuie să existe funcționalitatea de filtrare după număr de document și după interval de date de înregistrare.
- Modulul trebuie să permită efectuarea unei căutări textuale generale în câmpurile relevante ale documentelor.
- Trebuie să existe funcționalitatea de afișare și ascundere a zonei de filtrare avansată, pentru o utilizare eficientă a interfeței.
- Trebuie să existe posibilitatea de resetare completă a filtrelor aplicate și revenire la afișarea implicită.
- Modulul trebuie să permită înregistrarea documentelor de intrare, ieșire și interne, prin formulare dedicate fiecărui tip de document.
- Trebuie să existe funcționalitatea de generare automată a numărului de înregistrare, conform regulilor stabilite la nivelul instituției, trebuie sa existe posibilitatea de a aplica si un șablon la numerele înregistrate de forma (F-1, F-2, sau CTR1, CTR2).

- Modulul trebuie să permită completarea datelor obligatorii și opționale, cu marcarea clară a câmpurilor obligatorii.
- Trebuie să existe posibilitatea de introducere a datelor externe ale documentului, precum număr și dată emitere.
- Trebuie să existe funcționalitatea de selectare a petentului/destinatarului și de completare a adresei acestuia, in plus trebuie sa existe posibilitatea de a alege daca se folosește cu nomenclator de persoane atât fizice cat si juridice sau se completează detaliile la liber.
- Modulul trebuie să permită asocierea documentului cu un compartiment responsabil.
- Trebuie să existe posibilitatea de selectare a tipului de act dintr-o listă predefinită, care in orice moment să se poată adaugă un tip nou de document fără a fi nevoie de intervenția unui administrator.
- Trebuie să existe posibilitatea de completare a conținutului pe scurt și a detaliilor suplimentare ale documentului.
- Modulul trebuie să permită stabilirea termenului de soluționare, exprimat în zile calendaristice sau lucrătoare, pornind de la asta se va calcula automat termenul de răspuns al documentului ținând cont de toate zilele libere, weekenduri, etc .
- Modulul trebuie să permită accesarea unei pagini dedicate de vizualizare a detaliilor complete ale documentului.
- Trebuie să existe afișarea clară a stării curente a documentului și a istoricului acesteia. Modulul trebuie să afișeze informații privind data înregistrării și utilizatorul care a efectuat operațiunea.
- Trebuie să existe afișarea compartimentului responsabil și a tipului documentului.
- Modulul trebuie să afișeze termenul de soluționare, precum și numărul de zile rămase până la expirare.
- Trebuie să existe afișarea unui cod unic de verificare al documentului, cod unic care va fi folosit de petent pentru a verifica starea documentului direct din portal. Acest cod va fi transmis fie pe email fie in recipisa de înregistrare a documentului la registratura.
- Modulul trebuie să permită atașarea unuia sau mai multor fișiere de diferite formate la un document în momentul înregistrării sau ulterior.
- Trebuie să existe funcționalitatea de afișare structurată a fișierelor atașate documentului.
- Trebuie să existe posibilitatea de descărcare și vizualizare a fișierelor atașate cu extensiile cele mai comune (pdf, xls, xlsx, doc, docx, png, jpg, etc) direct in aplicație fără sa fie descărcate.
- Modulul trebuie să asigure delimitarea clară între fișierele atașate documentului inițial și cele atașate ca parte a unui răspuns la document.
- Trebuie să existe funcționalitatea de transmitere a documentelor între utilizatori și compartimente, în conformitate cu fluxurile interne.

- Modulul trebuie să permită selectarea unuia sau mai multor destinatari pentru fiecare transmitere. Căutarea sa poate fi făcută atât după numele utilizatorului cat si după departament.
- Trebuie să existe opțiunea de păstrare a documentului în lucru pentru utilizatorul curent.
- Modulul trebuie să păstreze și să afișeze istoricul complet al circulației documentului, incluzând sursa, destinația și datele asociate.
- Trebuie să existe afișarea datei de creare și a ultimei actualizări a fiecărei etape de circulație.
- Modulul trebuie să permită completarea și înregistrarea răspunsului aferent unui document.
- Trebuie să existe posibilitatea de selectare a tipului de răspuns, în conformitate cu procedurile interne.
- Modulul trebuie să permită adăugarea de comentarii și observații la soluționarea documentului.
- Trebuie să existe funcționalitatea de modificare a stării documentului pe baza rezultatului soluționării.
- Modulul trebuie să includă stări multiple ale documentului, precum rezolvat, parțial rezolvat, clasat sau anulat, etc.
- Trebuie să existe posibilitatea de atașare a documentelor justificative la răspuns. Aceste documente trebuie sa fie preluate sau generate din mai multe surse. Prima sursa este ceea ce este descris mai sus partea de colaborare asupra documentelor, unde fiecare utilizator/angajat va trebuie sa își redacteze răspunsul si ulterior sa îl atașeze la document. A doua sursa este generarea automată a răspunsurilor repetitive pe baza unor template-uri predefinite in aplicație.
- Trebuie sa existe posibilitatea de transmite răspunsul petentului pe mai multe cai. Prima cale este pe email, răspunsul trebuie sa se poată transmite direct din aplicație de pe document, fie de pe smtp-ul general configurat, fie de pe adresa personală a fiecărui utilizator. A doua cale este de al transmite direct in portal, si in final a treia cale personal, posta, etc.
- Modulul trebuie să permită afișarea și gestionarea documentelor recepționate prin email. Înregistrarea acestora trebuie sa se facă direct in aplicație, si cu un singur click sa se preia toate atașamentele si tot conținutul email-ului.
- Trebuie sa permită gestionarea mai multor căsuțe de email.
- Trebuie să existe posibilitatea de filtrare a documentelor provenite din email după stare, adresă de email și perioadă.
- Modulul trebuie să permită căutarea în conținutul emailurilor recepționate.
- Trebuie să existe afișarea informațiilor esențiale ale emailului, precum expeditor, dată și existența atașamentelor.

- Trebuie să existe posibilitatea de marcare a emailurilor ca fiind înregistrate sau neînregistrate în registratură.
- Modulul trebuie să permită selectarea și ștergerea multiplă a emailurilor.
- Trebuie sa existe posibilitatea ca toate formularele ce sunt depuse de către petenți sa fie înregistrate printr-un mecanism simplu in registratura in diferite registre.
- Trebuie sa permită definirea de registre multiple.
- Modulul trebuie să permită generarea de rapoarte privind documentele înregistrate, pe baza criteriilor selectate.
- Trebuie să existe posibilitatea de filtrare a datelor incluse în raport.
- Modulul trebuie să permită exportul rapoartelor în formate uzuale, precum Excel, CSV și PDF.
- Trebuie să existe funcționalitatea de copiere a datelor generate și de tipărire a rapoartelor.
- Rapoartele trebuie să includă informații relevante precum număr de înregistrare, emitent, conținut, compartiment, destinatar, stare și tip act.
- Modulul trebuie să asigure trasabilitatea completă a fiecărui document pe întregul său ciclu de viață.
- Trebuie să existe funcționalitatea de înregistrare automată a tuturor acțiunilor efectuate asupra documentelor.
- Modulul trebuie să păstreze istoricul modificărilor, incluzând utilizatorul, data, ora și tipul acțiunii.
- Trebuie să existe posibilitatea de consultare a jurnalului de audit pentru fiecare document.
- Modulul trebuie să permită generarea de rapoarte de audit.
- Modulul trebuie să permită configurarea notificărilor automate pentru evenimente relevante (când a fost rezolvat un document, când urmează sa expire in funcție de cate zile setez eu ca utilizator, etc).
- Trebuie să existe funcționalitatea de notificare la apropierea termenului de soluționare.
- Modulul trebuie să notifice utilizatorii în cazul depășirii termenului limită.
- Trebuie să existe notificări la primirea unui document nou.
- Modulul trebuie să permită notificări la transmiterea sau redirecționarea documentelor.
- Notificările trebuie să poată fi transmise atât în aplicație, cât și prin email.
- Modulul trebuie să permită definirea și configurarea fluxurilor de lucru pentru documente.
- Trebuie să existe posibilitatea de configurare a etapelor de procesare a documentelor.
- Modulul trebuie să permită stabilirea regulilor de tranziție între etape.

- Trebuie să existe posibilitatea de configurare a fluxurilor diferite în funcție de tipul documentului.
- Modulul trebuie să permită vizualizarea grafică a stadiului documentului în cadrul fluxului.
- Modulul trebuie să permită aplicarea semnăturii electronice asupra documentelor direct in aplicație.
- Modulul trebuie să permită verificarea validității semnăturii electronice.
- Trebuie să existe posibilitatea de semnare individuală sau multiplă a documentelor.
- Modulul trebuie să păstreze istoricul semnărilor aplicate.
- Modulul trebuie să permită arhivarea documentelor în conformitate cu termenele legale de păstrare.
- Trebuie să existe posibilitatea de clasificare a documentelor în arhivă.
- Modulul trebuie să permită consultarea documentelor arhivate, în regim de citire. Trebuie să existe funcționalitatea de marcare a documentelor pentru eliminare conform legislației.
- Modulul trebuie să asigure păstrarea integrității documentelor arhivate.
- Modulul trebuie să permită integrarea cu sisteme externe prin interfețe de tip API.
- Trebuie să existe posibilitatea de integrare cu sisteme de autentificare centralizată.
- Modulul trebuie să permită schimbul de date cu alte aplicații instituționale.
- Modulul trebuie să asigure autentificarea securizată a utilizatorilor.
- Trebuie să existe mecanisme de control al accesului bazate pe roluri.
- Modulul trebuie să asigure confidențialitatea și integritatea datelor.
- Trebuie să existe funcționalități de protecție împotriva accesului neautorizat.
- Modulul trebuie să permită jurnalizarea accesărilor documentelor.
- Trebuie să existe măsuri de conformitate cu legislația privind protecția datelor cu caracter personal.
- Modulul trebuie să permită operarea simultană a mai multor utilizatori.
- Trebuie să existe un timp de răspuns optim pentru operațiunile uzuale.
- Modulul trebuie să permită gestionarea unui volum mare de documente. Modulul trebuie să permită configurarea nomenclatoarelor utilizate (persoane, documente, tipuri de răspuns, template-uri de documente, etc.).
- Trebuie să existe posibilitatea de personalizare a câmpurilor, si posibilitatea de adăugare câmpuri adiționale
- Modulul trebuie să permită configurarea termenelor implicite.
- Trebuie să existe posibilitatea de adaptare a interfeței la nevoile instituției.
- Modulul trebuie să permită configurarea formatelor de numerotare.

- Modulul trebuie să ofere o interfață intuitivă și ușor de utilizat.
- Trebuie să existe suport pentru utilizarea aplicației pe diferite rezoluții acesta va trebuie sa poată fi accesibila si de pe telefon, deci daca este un volum mare de date acestea trebuie sa fie organizate cat mai optim.
- Modulul trebuie să permită accesul prin browser web.
- Trebuie să existe mesaje clare de eroare și confirmare, in cazul când se șterg anumite informații.
- Modulul trebuie să permită completarea ulterioară a informațiilor asociate unui document deja înregistrat, fără a afecta datele inițiale de înregistrare.
- Trebuie să existe funcționalitatea de adăugare de observații textuale suplimentare, asociate documentului, într-o secțiune dedicată de completări.
- Modulul trebuie să permită actualizarea termenului de soluționare în cadrul secțiunii de completări, cu păstrarea evidenței modificărilor.
- Trebuie să existe posibilitatea de a atașa documente suplimentare în cadrul completărilor, distinct de atașamentele inițiale ale documentului.
- Modulul trebuie să permită salvarea completărilor ca acțiuni independente, fără a modifica istoricul inițial al documentului.
- Trebuie să existe validarea câmpurilor obligatorii din secțiunea de completări înainte de salvare.
- Modulul trebuie să permită definirea documentelor cu termen de soluționare prestabilit, exprimat numeric în zile.
- Trebuie să existe posibilitatea de configurare a tipului de termen (ex. zile calendaristice, zile lucrătoare).
- Modulul trebuie să afișeze în mod explicit termenul asociat documentului în cadrul secțiunilor de detaliu și completări.
- Trebuie să existe posibilitatea de modificare a termenului doar de către utilizatori autorizați.
- Orice modificare a termenului trebuie să fie înregistrată în istoricul documentului.
- Modulul trebuie să permită suspendarea termenului de soluționare al unui document, printr-o funcționalitate dedicată.
- Trebuie să existe obligativitatea completării motivului suspendării termenului.
- Modulul trebuie să permită inițierea suspendării termenului doar pentru documentele care au un termen activ.
- Pe perioada suspendării, termenul de soluționare trebuie să fie oprit automat. ● Modulul trebuie să evidențieze vizual documentele cu termen suspendat.
- Trebuie să existe funcționalitatea de reluare a termenului de soluționare după suspendare.

- Modulul trebuie să păstreze un istoric complet al tuturor suspendărilor de termen asociate unui document.
- Istoricul suspendărilor trebuie să includă cel puțin: utilizatorul care a efectuat suspendarea, data suspendării și motivul suspendării.
- Modulul trebuie să afișeze istoricul suspendărilor într-o secțiune distinctă, accesibilă din detaliile documentului.
- Trebuie să existe posibilitatea de consultare a istoricului suspendărilor fără drept de modificare.
- Istoricul suspendărilor trebuie să fie inclus în trasabilitatea documentului.
- Modulul trebuie să permită configurarea drepturilor de acces pentru operațiunile de completare și suspendare termen.
- Trebuie să existe restricții privind cine poate suspenda sau modifica termenul unui document.
- Modulul trebuie să afișeze mesaje clare de confirmare pentru acțiunile de suspendare termen.
- Trebuie să existe mesaje de eroare explicite în cazul în care suspendarea nu poate fi efectuată.
- Toate acțiunile trebuie să fie înregistrate în jurnalul de audit.
- Modulul trebuie să integreze completările și suspendările de termen în fluxul de viață al documentului.
- Starea documentului trebuie să reflecte corect existența unei suspendări active.
- Modulul trebuie să țină cont de suspendări în calculul termenelor și al notificărilor.
- Notificările automate trebuie adaptate în funcție de suspendarea sau reluarea termenului.
- Modulul trebuie să permită generarea de rapoarte privind documentele cu termen suspendat.
- Trebuie să existe posibilitatea de raportare a duratei suspendărilor.
- Modulul trebuie să permită filtrarea documentelor în funcție de existența sau inexistența suspendărilor.
- Rapoartele trebuie să includă informații privind motivele suspendării și utilizatorii implicați.

4.5.2.2.3 Fluxuri de lucru

Permite gestiunea proceselor cu documente, asigurând circulația documentelor pe trasee ierarhice sau pre-configurate, cu posibilitatea aprobării sau respingerii acestora, standardizarea, distribuirea și circulația informațiilor și a documentelor interne în cadrul organizației, precum și a celor generate în relația cu terți.

Cerințe:

- Sistemul trebuie să includă un motor de fluxuri de lucru integrat, configurabil și extensibil, destinat gestionării proceselor asociate documentelor înregistrate în aplicație.
- Motorul de fluxuri de lucru trebuie să respecte un standard consacrat în domeniu, precum BPMN 2.0 sau un standard echivalent, recunoscut la nivel internațional.
- Modulul de workflow trebuie să permită definirea, publicarea și modificarea fluxurilor de lucru fără a necesita modificări ale codului sursă, reinstalarea aplicației/aplicațiilor conexe sau intervenții de tip IT asupra infrastructurii sau schemei bazei de date.
- Modulul trebuie să permită definirea și întreținerea fluxurilor de lucru printr-o interfață grafică vizuală, utilizând mecanisme de tip „drag & drop”.
- Proiectarea fluxurilor de lucru trebuie să fie realizată direct din aplicație, fără utilizarea unor instrumente externe.
- Fluxurile de lucru trebuie să poată fi proiectate pe baza organigramei instituției, incluzând structuri ierarhice, departamente, grupuri de lucru și roluri.
- Sistemul trebuie să permită definirea de tipuri de documente, formulare asociate fiecărui flux de lucru, utilizatori acțiuni.
- Modulul trebuie să permită definirea de fluxuri standard, precum și fluxuri ad-hoc, inițiate de utilizatori autorizați.
- Modulul trebuie să permită proiectarea fluxurilor de lucru cu:
  - sarcini singulare (secvențiale);
  - sarcini paralele, executate simultan de mai mulți utilizatori sau grupuri.
- Pentru activitățile paralele, sistemul trebuie să permită definirea condițiilor de terminare, precum:
  - finalizarea tuturor sarcinilor;
  - finalizarea unui număr minim de sarcini; ○ finalizarea unei sarcini specifice.
- Sistemul trebuie să permită definirea de comenzi condiționale în cadrul fluxurilor de lucru, pe baza variabilelor și metadatelor documentului.
- Modulul trebuie să permită definirea și utilizarea variabilelor de proces, care să influențeze logica de rutare și deciziile din flux.
- Sistemul trebuie să permită definirea termenelor limită pentru fiecare etapă a fluxului de lucru, ulterior cu notificări push sau pe email.
- Modulul trebuie să permită programarea unui timp maxim de expirare pentru un flux de lucru.
- Sistemul trebuie să permită marcarea distinctă a momentului de:
- primire a unei sarcini;
- începere efectivă a lucrului asupra documentului.
- Timpul de la primire și timpul efectiv de lucru trebuie să fie contorizate și ulterior generat raportare separat.

- Sistemul trebuie să permită escaladarea automată a sarcinilor în cazul în care nu există un răspuns într-un interval de timp configurabil.
- Modulul trebuie să permită definirea grupurilor și rolurilor implicate în fluxurile de lucru.
- Sistemul trebuie să permită selectarea explicită a unui utilizator dintr-un grup de lucru, astfel încât documentele să nu fie transmise automat tuturor membrilor grupului.
- Sistemul trebuie să permită blocarea editării documentelor după anumite etape ale fluxului de lucru.
- Modulul trebuie să permită editarea documentelor direct in aplicație de către utilizatorii implicați în fluxul de lucru, în funcție de drepturile asociate etapei curente.
- Sistemul trebuie să permită definirea și validarea metadatelor obligatorii pentru fiecare etapă a fluxului de lucru.
- Modulul trebuie să permită returnarea documentelor prin respingere, cu posibilitatea selectării etapei din flux la care documentul se întoarce.
- Sistemul trebuie să permită revenirea documentului la etapa anterioară sau la o altă etapă specificată din fluxul de lucru.
- Documentele respinse trebuie să fie marcate vizual distinct (ex. culoare roșie).\
- Utilizatorii trebuie să poată adăuga comentarii obligatorii la respingerea sau finalizarea unei sarcini.
- Sistemul trebuie să informeze utilizatorii prin e-mail sau notificări de tip push cu privire la:
  - primirea unei noi sarcini;
  - existența unei sarcini restante;
  - expirarea sau apropierea termenelor limită.
- Notificările transmise prin e-mail sau push trebuie să permită deschiderea directă a sarcinii asociate din aplicație.
- Modulul trebuie să permită inițierea de fluxuri ad-hoc de comunicare, cu mai multe niveluri de aprobare, avizare, recepție sau informare.
- Pentru fiecare nivel al fluxului ad-hoc, utilizatorii trebuie să poată selecta unul sau mai mulți utilizatori și/sau grupuri din organigramă.
- Sistemul trebuie să permită declanșarea schimburilor de date cu sisteme externe prin API-uri standardizate, înainte de inițierea unui flux de lucru, după inițiere sau la orice etapă a fluxului.
- Modulul trebuie să permită inițierea automată a fluxurilor de lucru în timpul procesului de scanare a documentelor.
- Sistemul trebuie să permită inițierea altor fluxuri de lucru din interiorul unui flux aflat în derulare.

- Modulul trebuie să permită mutarea automată a fișierelor în dosare predefinite, după finalizarea anumitor etape din flux.
- Sistemul trebuie să permită vizualizarea grafică a traseului documentului, indicând clar etapa curentă din flux.
- Modulul trebuie să permită marcarea etapelor fluxului cu culori diferite, pentru reflectarea progresului.
- Sistemul trebuie să genereze un istoric complet al fluxurilor de lucru, atât pentru utilizatori individuali, cât și la nivelul întregii organizații.
- Administratorii trebuie să poată genera un tabel centralizat cu toate fluxurile de lucru și informațiile asociate acestora.
- Sistemul trebuie să permită exportul definiției fluxurilor de lucru în format imagine, pentru prezentare și avizare.
- Sistemul trebuie să permită semnarea electronică a documentelor în cadrul etapelor de aprobare din fluxul de lucru, pentru fiecare utilizator implicat.
- Modulul trebuie să permită aplicarea de semnături electronice sau ștampile scanate pe documente de tip Word și PDF, în cadrul fluxului de aprobare.
- Semnăturile aplicate trebuie să fie înregistrate în istoricul documentului și al fluxului de lucru.
- Modulul trebuie să permită administrarea delegărilor pentru utilizatorii aflați în concediu medical sau de odihnă.
- Sistemul trebuie să redirecționeze automat sarcinile către utilizatorii delegați.
- Administratorii trebuie să poată opri sau suspenda un flux de lucru aflat în derulare, în condiții controlate și auditate.
- Pe durata contractului de implementare, Prestatorul trebuie să asigure implementarea și configurarea tuturor fluxurilor de lucru furnizate de Autoritatea Contractantă.
- Fluxurile de lucru vor fi implementate conform competențelor exclusive ale Autorității Contractante.
- Prestatorul trebuie să asigure configurarea fluxurilor fără costuri suplimentare pentru autoritate, în limita cerințelor furnizate.

Pe durata contractului de implementare a sistemului informatic Ofertantul devenit Prestator va asigura implementarea si configurarea tuturor fluxurilor de lucru (procese) in cadrul aplicației instalate, în măsura in care aceste fluxuri sunt cunoscute si furnizate de către autoritatea contractanta, conform competentelor exclusive ale acesteia.

4.5.2.3 Cerințe funcționale configurabile

- Pe lângă cerințele încadrate ca funcționalități existente în soluția DMS (COTS), se vor avea în vedere o serie de dezvoltări și extinderi ce vor fi detaliate și implementate ulterior, în baza etapelor de analiză, proiectare și dezvoltare.

- Sistemul trebuie sa permită extinderea și configurarea metadatelor asociate documentelor, inclusiv definirea de câmpuri personalizate, reguli de validare și liste de valori predefinite, în funcție de necesitățile operaționale identificate în etapa de analiză detaliată.
- De asemenea, se va analiza și configura mecanismul de fluxuri de lucru personalizate, cu posibilitatea definirii de etape multiple de aprobare, reguli condiționale, termene limită, notificări automate și mecanisme de escaladare. Structura exactă a acestor fluxuri va fi stabilită în urma analizei proceselor interne și va fi detaliată în documentația de proiectare funcțională.
- În funcție de concluziile etapei de analiză, se vor defini și implementa eventuale integrări cu alte sisteme interne sau externe, prin intermediul API-urilor sau al altor mecanisme de interoperabilitate, în vederea asigurării unui schimb automatizat de date și a eliminării operațiunilor manuale redundante.
- Sistemul va putea fi extins cu funcționalități suplimentare de raportare și monitorizare, incluzând generarea de rapoarte personalizate privind statusul documentelor, timpii de procesare și aprobare, trasabilitatea operațiunilor, activitatea utilizatorilor și indicatori de performanță relevanți. Structura rapoartelor și indicatorii urmăriți vor fi definiți ulterior, în baza cerințelor identificate.
- Se va analiza implementarea unor reguli avansate de retenție și arhivare a documentelor, incluzând termene diferențiate de păstrare, arhivare automată și mecanisme de ștergere conform politicilor interne și cerințelor legale aplicabile. Parametrii exacți vor fi stabiliți în etapa de analiza.
- Totodată, pot fi avute în vedere extinderi ale mecanismelor de versionare și audit, inclusiv compararea versiunilor, restaurarea selectivă a acestora, precum și păstrarea unui istoric detaliat al modificărilor efectuate asupra documentelor.
- Pe parcursul etapei de analiză detaliată și proiectare funcțională și tehnică, pot fi identificate câmpuri suplimentare, funcționalități, reguli de business, integrări sau optimizări necesare pentru alinierea completă a sistemului DMS la procesele organizației. Acestea vor fi documentate în livrabilele de analiză și vor face obiectul etapelor ulterioare de configurare și dezvoltare, în baza specificațiilor agreate între părți.

4.5.3 Modul Registrul Sportiv – Federații și Cluburi

4.5.3.1 Context general

Acest registru are rolul de a înregistra și administra informațiile privind structurile sportive, respectiv federațiile sportive, cluburile sportive (persoane juridice de drept public sau de drept privat fără scop lucrativ înființate conform OUG 26), asociațiile județene și alte municipiului București pe ramura de sport înființate conform OUG 26, ligile profesioniste și alte organizații sportive naționale.

Cluburile pot fi mono-sportive sau polisportive, constituite sau înființate, după caz, în scopul organizării și administrării unei activități sportive și care au drept obiectiv promovarea uneia sau mai multor discipline sportive, practicarea acestora de către membrii lor și participarea la activitățile și competițiile sportive.

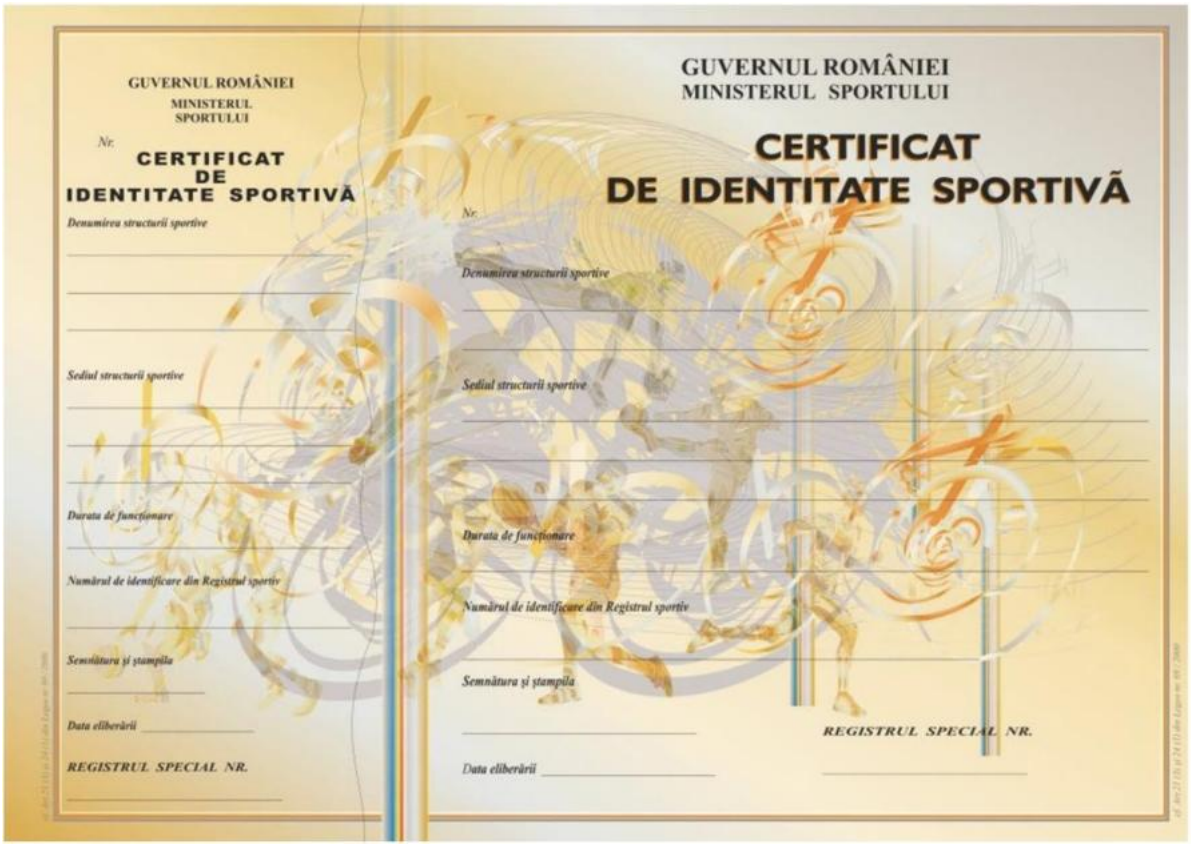
Legea Sportului (Legea nr. 69/2000) reglementează funcționarea structurilor sportive, iar Certificatul de Identitate Sportivă (CIS) este necesar pentru a opera legal.

După înființare și obținerea tuturor avizelor necesare de la judecătorie, federațiile și cluburile pot depune un număr de acte specifice în funcție de tipul de structură în vederea obținerii CIS.

Certificatele CIS sunt tipărite de către de Imprimeria Națională și eliberate Agenția Națională pentru Sport (ANS). În prezent acest proces se desfășoară manual, parțial prin email și/sau documente aduse fizic sau trimise prin poștă la registratura ANS, fiind dificil de gestionat în special pentru structurile sportive din provincie.

Cluburile revin la ANS pentru actualizarea înregistrărilor atunci când apar modificări (precum schimbarea adresei, denumirii, sau a componenței organelor de conducere, administrare și control sau alte modificări aduse actelor constitutive).

Un nou certificat se emite atunci când sediul este mutat într-un alt județ. Pot fi solicitate și duplicate ale certificatelor. În cazul radierii sau revocării, este investigată posibilitatea de a semnala cluburile sportive care s-au închis (informații colectate de la ANAF, judecătorii etc.).



Figură 4 - Model Certificat de Identitate Sportivă

4.5.3.2 Federații sportive naționale

4.5.3.2.1 Context

Federațiile sportive sunt organizații naționale care au rolul de a coordona, reglementa și promova o anumită ramură sportivă. Ele sunt structuri juridice recunoscute de stat și sunt responsabile pentru dezvoltarea sportului de performanță, formarea și susținerea sportivilor și antrenorilor, organizarea competițiilor oficiale și implementarea strategiei naționale pentru sportul respectiv.

Federațiile sportive reprezintă punctul central de organizare pentru cluburile și asociațiile sportive afiliate, oferindu-le suport și îndrumare. De asemenea, ele sunt responsabile pentru stabilirea regulilor de joc, formarea și certificarea antrenorilor și arbitrilor, gestionarea competițiilor și menținerea unor standarde ridicate de etică și disciplină.

Rolurile și responsabilitățile unei federații sportive includ:

- Organizarea și promovarea competițiilor: Federațiile coordonează competițiile oficiale de la nivel local până la nivel național și susțin participarea la competițiile internaționale. Ele creează calendare competiționale și stabilesc regulamente pentru desfășurarea întrecerilor sportive.
- Dezvoltarea sportului de performanță: Asigură formarea și pregătirea sportivilor de elită, contribuind la dezvoltarea echipelor naționale și la creșterea performanței la nivel internațional.
- Reglementarea și normarea activităților: Federațiile elaborează norme, reguli și standarde pentru desfășurarea activităților sportive, asigurând conformitatea cu normele internaționale și cu cele stabilite de federațiile internaționale de profil.
- Afilierea la federații internaționale: Federațiile naționale sunt membre ale federațiilor internaționale de specialitate și reprezintă țara la nivel internațional. Ele au responsabilitatea de a implementa regulile și politicile stabilite la nivel global.
- Coordonarea și susținerea cluburilor sportive și sportivilor: Federațiile oferă suport cluburilor sportive afiliate, sprijinind atât sportul de masă, cât și sportul de performanță. Ele organizează programe de formare pentru antrenori și arbitri și facilitează accesul sportivilor la resurse.
- Educație și dezvoltare: Contribuie la educația sportivilor și a antrenorilor prin cursuri și certificări. Totodată, promovează valorile sportului în societate, cum ar fi fair-play-ul, integritatea și incluziunea.
- Finanțarea activităților sportive: Federațiile gestionează fondurile alocate sportului respectiv, inclusiv subvenții de la autorități, sponsorizări și resurse proprii, pentru a asigura o dezvoltare constantă și sustenabilă.

Federațiile sportive sunt astfel o componentă vitală în organizarea și promovarea sportului într-o țară, contribuind la dezvoltarea sportului de performanță , a sportului pentru toți și a sportului

FEDERAȚIA ROMÂNĂ DE CANOTAJ

Denumirea federatiei, conform certificatului de identitate sportiva
FEDERATIA ROMANA DE CANOTAJ
Adresa: Bucuresti, str. Vasile Conta, nr. 16
Tel:021/317.32.00 Fax: 012/317.32.01; e-mail: office@frcanotaj.ro
Website: http://www.frcanotaj.ro
Data infiintarii: anul 1925
Datele inscrise in Certificatul de Identitate Sportiva : Nr. de identificare B/C/00021/2002 , data eliberarii 29.01.2002

Organul de conducere si administrare a activitatii federatiei
Denumirea organului de conducere si administrative: Comitetul Executiv
Componenta organului de conducere si administrative: Presedinte: Lipă Elisabeta suspendata in data de 30.06.2023
Vicepresedinte: Guerli Valentin presedinte interimar din 30.06.2023
Membrii: Adamovici Sebastian, Serban Calin, Chermes Viorica, Stratan Dan, Talpes Andrei, Szabo Gabriela, Tudosa Ciprian
Birou Executiv: Presedinte: Guerli Valentin; Membru: Chermes Viorica

Comisiile si / sau colegiile federale
Colegiul antrenorilor: Presedinte Macovei Rodica
Colegiul arbitrilor: Presedinte Macovei Rodica
Comisie de competitii si materiale: Presedinte Adamovici Sebastian
Comisie pentru juniori: Presedinte Macovei Rodica
Comisie pentru medii de informare si marketing: Presedinte Chermes Viorica
Comisie sportivilor: Presedinte Tudosa Ciprian
Comisie pentru dezvoltare: Presedinte Guerli Valentin
Comisie medicala: Presedinte Ovean Vasile
Comisie de disciplina: Presedinte Serban Calin
Comisie antidoping: Presedinte Ovean Vasile

Federatia Internationala la care este afiliata
Denumirea federatiei internationale: Federatia Internationala de Canotaj / Federation Internationale des Societes d'Aviron/ International Rowing Federation
Data infiintarii federatiei internationale: anul 1892 luna iunie ziua 25
Adresa: Elvetia, Lausanne Tel +41(0)216178373 Fax +41(0)216178375 e-mail.info@fisa.org
Website: http://www.worldrowing.com
Data afilierii la federatia internationala: anul 1927 luna 08 ziua 19
Reprezentantii romani in federatia internationala :

Federatia Europeana la care este afiliata
Denumirea federatiei europene: Asociatia Balcanica de Canotaj, / Balkan Rowing Association
Data infiintarii federatiei europene: anul 1972 luna aprilie ziua 13
Adresa: Romania, Bucuresti Tel 021/317.32.00 Fax 021/317.32.01 e-mail office@balkanrowing.com
Website: http://www.balkanrowing.com
Data afilierii la federatia internationala: anul 1973 luna aprilie ziua 13

Sponsorii / partenerii oficiali ai federatiei

HERBALIFE	ALBALACT SA
NEGRO 2000	COVALACT SA
SC ERBASU CONSTRUCTI	DORNA LACTATE SA
IBB HIB ROMANIA	B&B COLLECTION SRL
UNICREDIT BANK	CEC BANK SA
SANOVITA	CRAMELE CRICOVA SRL
FITERMAN PHARMA	DENTISTS INTERNATIONAL SRL
REGINA MARIA	DEUTSCHE LEASING ROMANIA IFN
FUNDATIA TIRIAC	KAUFLAND ROMANIA SC
BDO AUDIT SRL	MACROMEX SRL
PHOENICIA EXPRESS SRL	TOP LINE EUROPA SRL
MASPEX ROMANIA SA - BUCOVINA	TIRIAC AUTO FORD
LABORATOARELE MEDICA SRL	CIGA ENERGIE

Fisa de identificare a cluburilor sportive si asociatiilor judetene pe ramura de sport, membre ale federatiei in anul 2023

Nr.crt.	Denumire	Adresa	Nr. identificare	Tip club
1	AC WEST SPORT Arad	Str. EPISCOP Roman Ciorogariu, nr.27	AR/A2/00084/2008	Structură sportivă de drept privat
2	ACS Vointa Arad	Str. Mahal Mureșului, nr. 31	AR/A2/00129/2007	Structură sportivă de drept privat
3	Clubul Sportiv Olimpia Bucuresti	Sos. Ialomiței, nr.128 A	B/A1/00039/2001	Structura sportiva de drept public
4	CS Triumf Bucuresti	Str. Primo Nebiolo, nr.2	B/A1/00040/2001	Structură sportivă de drept public
5	Clubul Sportiv Dinamo Bucuresti	Sos. Șt. cel Mare, nr. 7-9	B/A1/00043/2001	Structura sportiva de drept public
6	Clubul Sportiv al Armatei "Steaua" Bucuresti	B-dul Ghencea, nr. 35	B/A1/00044/2001	Structură sportivă de drept public
7	CS Rapid Bucuresti	Sos. Giulești,nr.18	B/A1/00048/2001	Structura sportiva de drept public
8	Club Sportiv Municipal Bucuresti	Calea Vitan, Nr.2412, Etaj 1	B/A1/00010/2007	Structura sportiva de drept public
9	Clubul Sportiv Botosani	Str. Calea Nationala, nr. 184	BT/A1/00009/2001	Structură sportivă de drept privat
10	A.S. Olimpia Botosani	aval Gh.Avramescu, nr. 28	BT/A2/00169/2019	Structură sportivă de drept privat
11	Clubul Sportiv Municipal Calarasi	B-dul Republicii, nr. 39	CL/A1/00012/2001	Structură sportivă de drept public
12	CSS Calarasi	B-dul Republicii, nr. 39	CL/A1/00186/2001	Structură sportivă de drept public
13	Asociatia Judeteana de Canotaj Calarasi	B-dul Republicii, nr. 39	CL/B/00002/2003	Asociatie judeteana pe ramura de sport
14	CS Moldova Noua	Nr. Balcescu, nr.26, Moldova Noua	CS/A1/00008/2011	Structura sportiva de drept public
15	CSM Constanta	D Cantemir, nr.2, et 2, Constanta	CT/A1/00007/2022	Structură sportivă de drept public
16	Clubul Sportiv Farul Constanta	Str. Decebal, nr. 22	CT/A1/00014/2001	Structură sportivă de drept public
17	LPS Nicolae Rotaru Constanta	Str. Ion Corvin, nr. 2	CT/A1/00215/2001	Structura sportiva de drept public
18	Clubul Sportiv Universitar Simona Halep Constanta	B-dul Mamaia, nr. 124, Cta	CT/A1/00225/2001	Structura sportiva de drept public
19	Asociatia Judeteana de Canotaj Constanta	Str. Soveja- Parc, Constanta	CT/B/00002/2001	Asociatie judeteana pe ramura de sport
20	Sport Club Municipal Deva	Str. Octavian Goga nr. 1, Deva	HD/A1/ 00001/2006	Structura sportiva de drept public
21	A.C.S.O. VOLUNTARI PANTELIMON	Ivd Birunirei, nr. 80A, Pantelimon	IF/A2/00024/2018	Structură sportivă de drept privat
22	Clubul Sportiv Municipal Iasi	Str. Smardan, nr. 5	IS/A1/00021/2001	Structură sportivă de drept public
23	CSS Unirea Iasi	Aleea Grigore Ghica-Voda,nr.28	IS/A1/00118/2001	Structura sportiva de drept public
24	Asociatia Judeteana de Canotaj Iasi	Biz. Nautica Bordsant,Aroneanu	IS/B/00001/2004	Asociatie judeteana pe ramura de sport
25	CSS Orsova	Str. Crizantemelor 13 A	MH/A1/00003/2015	Structura sportiva de drept public
26	Club Sportiv Municipal Turnu- Severin	Str. Crisan, nr. 27	MH/A1/00009/2004	Structura sportiva de drept public
27	Clubul Sportiv Muncsul Tg. Mures	Str. Parcul Sportiv Municipal, nr.4	MS/A1/00023/2001	Structura sportiva de drept public
28	Clubul Sportiv "Cetatuia" Piatra Neamt	Str. Șt. cel Mare, nr.53	NT/A1/00024/2001	Structura sportiva de drept public
29	LPS Piatra Neamt	Str. Obor, nr. 2	NT/A1/00165/2001	Structura sportiva de drept public
30	Clubul Sportiv Valentin Piatra Neamt	Str. Bistritei, nr.16	NT/A2/00109/2005	Structură sportivă de drept privat
31	Clubul Sportiv Moldocor Piatra Neamt	B-dul Decebal, nr. 73	NT/A2/00167/2003	Structură sportivă de drept privat
32	Asociatia Judeteana de canotaj Neamt	Str.Bistritei, nr.16	NT/B/00001/2005	Asociatie judeteana pe ramura de sport
33	Clubul Sportiv Municipal Suceava	B-dul 1Decembrie 1918, nr.7	SV/A1/00031/2001	Structură sportivă de drept public
34	Colegiul Nat. "Nicu Gane" Falticeni	Str. Sucevei, nr. 105	SV/A1/00206/2001	Structura sportiva de drept public
35	Asociatia Club Sportiv Nada Florilor Falticeni	str. Horticolei nr. 6, jud Suceava	SV/A2/00201/2013	Structură sportivă de drept privat
36	CSS Berga Timisoara	Str. Amforei, nr. 1	TM/A1/00009/2001	Structura sportiva de drept public
37	Clubul Sportiv Municipal Timisoara	Str. FC Ripensia, nr.29	TM/A1/00034/2001	Structură sportivă de drept public
38	Clubul Sportiv Universitar Politehnica Timisoara	Str. P-ta Horatiu, nr. 1	TM/A1/00244/2001	Structura sportiva de drept public
39	Asociatia Judeteana de Canotaj Timis	Calea Sagului, nr.43/A	TM/B/00001/2010	Asociatie judeteana pe ramura de sport

pentru persoanele cu nevoi speciale, la reprezentarea pe plan internațional și la asigurarea respectării regulilor și eticii sportive.

Figură 5 - Exemplu detalii federație sportivă

4.5.3.2.2 Cerințe funcționale

- Modulul trebuie să permită definirea unei federații sportive ca entitate principală în sistem, cu toate datele de identificare și structurare necesare.
- Trebuie să existe posibilitatea de a defini și gestiona sub-entitățile aferente unei federații, conform structurii organizatorice și funcționale stabilite.
- Modulul trebuie să permită asocierea unei federații cu una sau mai multe ramuri sportive.
- Sistemul trebuie să asigure evidența completă a relațiilor dintre federații, structuri afiliate și competiții.
- Modulul trebuie să permită gestionarea procesului de afiliere a cluburilor sportive și asociațiilor județene pe ramură de sport.
- Trebuie să existe posibilitatea de a evidenția distinct structurile afiliate și cele neafiliate, cu restricționarea participării la competiții pentru cele neafiliate.
- Modulul trebuie să permită urmărirea istoricului afilierii fiecărei structuri sportive.
- Modulul trebuie să permită inițierea și aprobarea modificării sediului unei structuri sportive.
- Modulul trebuie să permită gestionarea schimbării denumirii unei structuri sportive, cu păstrarea istoricului denumirilor.
- Trebuie să existe posibilitatea de a adăuga sau elimina ramuri sportive pentru o structură afiliată.
- Modulul trebuie să permită gestionarea procesului de eliberare a Certificatului de Identitate Sportivă (CIS), inclusiv starea acestuia (emis, suspendat, retras).
- Modulul trebuie să permită definirea și administrarea calendarului competițional la nivel de federație și ramură sportivă.
- Trebuie să existe posibilitatea de a stabili perioade, locații, categorii de vârstă și niveluri competiționale.
- Modulul trebuie să permită asocierea competițiilor cu structurile sportive și sportivii participanți.
- Sistemul trebuie să permită actualizarea și versionarea calendarului competițional.
- Modulul trebuie să permită introducerea și validarea rezultatelor sportive pentru fiecare competiție.
- Trebuie să existe posibilitatea de a corela rezultatele cu sportivii, cluburile și ramurile sportive.
- Modulul trebuie să permită generarea automată de statistici sportive.

- Sistemul trebuie să asigure utilizarea rezultatelor în scopul întocmirii Anuarului Sportului.
- Modulul trebuie să permită vizualizarea și gestionarea fișei individuale a fiecărui sportiv.
- Trebuie să existe posibilitatea de a modifica datele sportivilor, cu păstrarea istoricului modificărilor.
- Modulul trebuie să permită asocierea sportivilor cu cluburi sportive, ramuri sportive și competiții.
- Sistemul trebuie să permită urmărirea eligibilității sportivilor pentru competiții.
- Modulul trebuie să permită inițierea, aprobarea și finalizarea transferurilor sportivilor între cluburi.
- Trebuie să existe posibilitatea de a defini tipuri de transfer (definitiv, temporar).
- Modulul trebuie să păstreze istoricul complet al transferurilor fiecărui sportiv.
- Sistemul trebuie să permită validarea dreptului de participare al sportivului după transfer.
- Modulul trebuie să permită gestionarea listelor de sportivi propuși pentru competiții internaționale.
- Trebuie să existe un flux de aprobare pentru participarea sportivilor la competiții internaționale.
- Modulul trebuie să permită urmărirea stării aprobărilor și deciziilor emise.
- Modulul trebuie să permită introducerea și actualizarea datelor necesare întocmirii Anuarului Sportului.
- Trebuie să existe posibilitatea de a genera rapoarte și situații centralizate pentru anuar.
- Modulul trebuie să permită exportul datelor într-un format standardizat.
- Registrul sportiv trebuie să fie structurat în două subregistre distincte, corespunzătoare categoriilor de structuri sportive gestionate.
- Modulul trebuie să permită administrarea separată a informațiilor pentru fiecare subregistru.
- Trebuie să existe posibilitatea de a diferenția structurile cu și fără personalitate juridică.
- Modulul trebuie să permită accesul Direcțiilor Județene pentru Sport în vederea gestionării proceselor aflate în responsabilitatea acestora.
- Direcțiile Județene trebuie să poată emite certificate pentru structurile sportive fără personalitate juridică.
- Modulul trebuie să asigure trasabilitatea completă a activităților realizate de Direcțiile Județene.
- Sistemul trebuie să permită Autorității Naționale pentru Sport drepturi de vizualizare asupra tuturor activităților și rezultatelor gestionate în cadrul registrului sportiv.
- Modulul trebuie să asigure acces la rapoarte centralizate și statistici relevante pentru ANS.

- Drepturile ANS trebuie să fie limitate la vizualizare, fără posibilitatea de modificare a datelor.
- Modulul trebuie să asigure jurnalizarea tuturor operațiunilor efectuate în sistem.
- Trebuie să existe posibilitatea de auditare a modificărilor și deciziilor.
- Sistemul trebuie să respecte principiile de securitate, integritate și confidențialitate a datelor.
- Toate procesele din Modulul Registru Sportiv trebuie să poată fi inițiate, urmărite și finalizate prin intermediul Registraturii Electronice și al Motorului de Workflow.
- Orice operațiune cu impact administrativ sau juridic trebuie să genereze automat un document înregistrat în Registratura Electronică.
- Toate informațiile care ajung si se gestionează cu ajutorul acestui modul trebuie sa fie conectate cu portalul si restul modulelor. Acest modul trebuie sa fie o continuare a funcționalului din portal, registratura, documente.

4.5.3.3 Cluburi sportive

4.5.3.3.1 Context

Sunt organizații cu personalitate juridică care au ca principal obiectiv promovarea și dezvoltarea activităților sportive la nivel local, național sau internațional. Ele pot fi înființate sub forma unor asociații fără scop patrimonial (nonprofit), societăți comerciale sportive (cu scop lucrativ) sau instituții de drept public organizate pentru a sprijini practicarea sportului.

Cluburile sportive joacă un rol esențial în promovarea sportului, dezvoltarea sportivilor și organizarea de competiții. Ele sunt componente fundamentale ale sistemului sportiv din România, contribuind la creșterea performanței sportive, la formarea tinerelor talente și la promovarea unui stil de viață activ în comunitate.

Tipuri de cluburi sportive:

1. Cluburi sportive persoane juridice de drept privat fără scop lucrativ:

Sunt cluburi înființate ca organizații neguvernamentale, fără scop patrimonial, în baza Ordonanței nr. 26/2000 privind asociațiile și fundațiile. Aceste cluburi se axează pe activități de promovare a sportului pentru toți, sportul școlar și universitar, sportul pentru persoane și nevoi speciale și a sportului de performanță.

2. Societăți comerciale sportive:

Cluburi înregistrate ca societăți comerciale pe acțiuni care au scopul de a dezvolta și promova sportul, dar și de a genera profit din activități legate de sport, cum ar fi bilete la meciuri, sponsorizări și alte surse de venit.

3. Cluburi sportive persoane juridice de drept public:

Aceste cluburi sportive sunt organizate în subordinea organelor administrației publice centrale, locale sau în subordinea instituțiilor de învățământ superior de stat.

Rolul și obiectivele cluburilor sportive:

- Promovarea sportului: Cluburile sportive promovează sportul pentru toți, sportul școlar și universitar, sportul pentru persoane și nevoi speciale și sportul de performanță, asigurând infrastructura necesară și facilități pentru practicarea diverselor ramuri sportive.
- Pregătirea sportivilor: Cluburile sportive organizează activități de antrenament și asigură sprijinul necesar pentru pregătirea sportivilor de performanță, oferindu-le acces la antrenori calificați și echipamente adecvate.
- Organizarea de competiții: Cluburile sportive participă și organizează competiții sportive la nivel local, național sau internațional, contribuind la dezvoltarea și creșterea vizibilității sportului în comunitate.
- Dezvoltarea sportivilor tineri: Cluburile sportive contribuie la descoperirea și formarea tinerelor talente sportive, asigurând programe de instruire pentru copii și adolescenți.
- Integrarea socială: Cluburile sportive au și un rol social important, prin promovarea incluziunii, a disciplinei și a sănătății în rândul comunității. Ele contribuie la integrarea socială a tinerilor și a persoanelor din medii defavorizate prin sport.

Structura și organizarea cluburilor sportive:

- Consiliul de administrație sau comitetul de conducere: Conducerea unui club sportiv este asigurată de o structură de decizie care poate fi formată din membri ai consiliului de administrație (în cazul societăților comerciale) sau dintr-un comitet de conducere (în cazul asociațiilor).
- Adunarea generală: În cazul asociațiilor, Adunarea Generală este organul suprem de decizie și este formată din membrii clubului.
- Antrenori și personal de suport: Cluburile sportive angajează antrenori calificați, preparatori fizici, fizioterapeuți și alți specialiști care sprijină sportivii în pregătirea și dezvoltarea lor.

Cluburile sportive pot fi, în funcție de tipul de sporturi practicate:

- Monosportive: Specializate pe o singură ramură sportivă (de exemplu, fotbal, tenis).
- Polisportive: Care dezvoltă mai multe ramuri sportive în cadrul aceleiași organizații (de exemplu, atletism, baschet, natație și pentatlon modern).

Certificatul de Identitate Sportivă (CIS):

- Pentru a funcționa legal, cluburile sportive din România trebuie să obțină un Certificat de Identitate Sportivă (CIS) eliberat de Agenția Națională pentru Sport (ANS). Acest certificat atestă înregistrarea oficială a clubului ca structură sportivă.

Afilierea la federații sportive:

Cluburile pot alege să se afilieze la federațiile sportive naționale pentru a putea participa la competițiile oficiale organizate de acestea. Afilierea permite sportivilor legitimați să reprezinte clubul la nivel național și internațional.

Sistemul va permite cluburilor să-și actualizeze singure lista de sportivi per ramuri sportive, să înregistreze competițiile din calendarul competițional intern și extern cu rezultatele aferente.

4.5.3.3.2 Cerințe funcționale

- Modulul are ca scop asigurarea unui cadru informatic unitar prin care cluburile sportive să își poată gestiona autonom datele, sportivii, personalul, participarea la competiții și obligațiile administrative, cu respectarea fluxurilor de lucru și a regulilor stabilite de federații și autoritățile competente.
- Modulul trebuie să permită acces controlat pentru cluburi sportive, pe baza rolurilor și drepturilor definite.
- Toate operațiunile efectuate de cluburi trebuie să fie supuse fluxurilor de lucru configurabile, acolo unde este necesar.
- Sistemul trebuie să asigure trasabilitatea completă a modificărilor și deciziilor.
- Modulul trebuie să funcționeze interconectat, cu registratura electronică.
- Sistemul trebuie să permită inițierea procesului de creare a unui cont de club sportiv.
- Cont care poate fi accesat de club prin intermediul portalului.
- Modulul trebuie să colecteze toate datele necesare conform specificațiilor legale și operaționale.
- Crearea contului trebuie să fie supusă unui flux de aprobare configurabil.
- După aprobare, clubul trebuie să primească acces la funcționalitățile sistemului.
- Modulul trebuie să permită cluburilor actualizarea datelor proprii.
- Actualizările trebuie să fie supuse validării prin workflow, în funcție de tipul modificării.
- Sistemul trebuie să păstreze istoricul tuturor modificărilor efectuate.
- Modulul trebuie să permită inițierea cererilor de ștergere sau dezactivare a contului.
- Dezactivarea trebuie să fie realizată doar după parcurgerea unui flux de aprobare a dezactivări.
- Datele istorice trebuie păstrate în sistem, conform regulilor de arhivare.
- Sistemul trebuie să permită inițierea procesului de obținere a Certificatului de Identitate Sportivă.
- Fluxul de lucru trebuie să includă etape de verificare, avizare și aprobare.
- După finalizarea fluxului, CIS-ul trebuie generat și asociat automat clubului.
- Sistemul trebuie să permită urmărirea stării cererii CIS în timp real.
- Modulul trebuie să permită inițierea cererilor de afiliere la una sau mai multe federații.
- Afilierea trebuie să fie condiționată de îndeplinirea criteriilor stabilite de federație.
- Procesul trebuie gestionat printr-un flux de lucru multi-etapă.
- Starea afilierii trebuie actualizată automat în sistem.
- Modulul trebuie să permită introducerea, actualizarea și ștergerea sportivilor.
- Datele sportivilor trebuie să fie structurate pe ramuri sportive.

- Sistemul trebuie să valideze unicitatea sportivilor în cadrul clubului și al ramurii sportive.
- Modulul trebuie să permită asocierea sportivilor cu cluburi, ramuri sportive și competiții.
- Sistemul trebuie să gestioneze istoricul asocierilor și modificărilor.
- Modulul trebuie să permită administrarea personalului clubului (antrenori, staff medical, personal auxiliar).
- Trebuie să existe asocierea personalului cu ramuri sportive și competiții. ● Modificările trebuie să fie supuse fluxurilor de validare, unde este cazul.
- Sistemul trebuie să permită înscrierea sportivilor la competiții interne și internaționale.
- Modulul trebuie să permită sa verifice eligibilitatea sportivilor.
- Înscrierea trebuie să fie supusă unui flux de aprobare configurabil.
- Sistemul trebuie să permită retragerea sau modificarea listelor de sportivi înscriși.
- Modulul trebuie să permită introducerea și actualizarea vizelor medicale pentru sportivi.
- Sistemul trebuie să urmărească valabilitatea vizelor medicale.
- Trebuie să existe notificări automate pentru vizele expirate sau care urmează să expire.
- Participarea la competiții trebuie blocată automat în lipsa unei vize medicale valide, acest lucru trebuie sa notifice personalul ANS si clubul.
- Modulul trebuie să permită evidența taxelor datorate de cluburi.
- Sistemul trebuie să permită înregistrarea plăților și a restanțelor.
- Participarea clubului la anumite activități trebuie condiționată de achitarea taxelor. ● Modulul trebuie să permită generarea de rapoarte financiare specifice.
- Modulul trebuie să permită introducerea și actualizarea datelor necesare Anuarului Sportului.
- Datele trebuie să fie corelate cu competițiile, sportivii și rezultatele înregistrate.
- Validarea datelor trebuie realizată prin fluxuri de lucru.
- Sistemul trebuie să permită exportul datelor într-un format standardizat.
- Cluburile trebuie să poată introduce competiții interne și externe.
- Modulul trebuie să permită introducerea rezultatelor aferente competițiilor.
- Rezultatele trebuie să fie supuse validării prin workflow.
- Sistemul trebuie să permită utilizarea rezultatelor pentru statistici și rapoarte.
- Modulul trebuie să permită definirea și utilizarea fluxurilor de lucru pentru toate procesele critice.
- Sistemul trebuie să genereze un istoric complet al fluxurilor de lucru.
- Utilizatorii trebuie să poată vizualiza stadiul proceselor inițiate.

- Modulul trebuie să gestioneze toate datele necesare pentru susținerea workflow-urilor definite.
- Metadatele trebuie să fie configurabile și validabile.
- Sistemul trebuie să permită extinderea structurii de date fără impact major asupra funcționării.

4.5.3.4 Asociații Județene și ale municipiului București pe ramuri de sport

4.5.3.4.1 Context

Asociațiile județene și ale municipiului București pe ramuri de sport sunt persoane juridice de drept privat, având drept scop organizarea activității în ramura de sport respectivă la nivelul județului sau al municipiului București, cu respectarea statutelor și regulamentelor federațiilor sportive naționale.

Dobândirea personalității juridice se face în condițiile legii, ca organizație asociație fără scop lucrativ.

Asociațiile județene și ale municipiului București pe ramuri de sport sunt constituite din secțiile asociațiilor și cluburilor sportive cuprinse în sistemul competițional județean, afiliate și recunoscute de acestea.

Obiectivele, drepturile și îndatoririle asociațiilor județene și ale municipiului București pe ramuri de sport decurg din statutele și regulamentele federațiilor sportive naționale corespunzătoare, precum și din puterea delegată de către acestea.

La nivelul județului, respectiv al municipiului București, se poate constitui, pentru o ramură de sport, o singură asociație județeană.

Certificatul de Identitate Sportivă (CIS):

Pentru a funcționa legal, Asociațiile județene și ale municipiului București pe ramuri de sport trebuie să obțină un Certificat de Identitate Sportivă (CIS) eliberat de Agenția Națională pentru Sport (ANS). Acest certificat atestă înregistrarea oficială a asociației ca structură sportivă.

Afilierea la federații sportive:

Asociațiile județene și ale municipiului București pe ramuri de sport se afiliază la federațiile sportive naționale.

4.5.3.4.2 Cerințe funcționale

1. Administrarea entității

- Modulul trebuie să permită definirea unei Asociații Județene / a Municipiului București ca entitate distinctă în sistem, cu toate datele de identificare necesare.
- Sistemul trebuie să permită gestionarea statutului juridic, a datelor de contact, a conducerii și a documentelor constitutive.
- Modulul trebuie să permită actualizarea datelor asociației, cu păstrarea istoricului modificărilor.

2. Gestionarea afilierii

- Modulul trebuie să permită gestionarea procesului de afiliere la federația sportivă națională corespunzătoare.
- Sistemul trebuie să permită evidențierea stării afilierii (afiliat / neafiliat / suspendat).
- Orice modificare a statutului de afiliere trebuie să fie supusă unui flux de aprobare.

3. Administrarea structurilor sportive afiliate

- Modulul trebuie să permită gestionarea cluburilor și secțiilor sportive afiliate la nivel județean.
- Sistemul trebuie să permită evidența cluburilor afiliate și neafiliate, cu restricționarea participării la competiții pentru cele neafiliate.
- Modulul trebuie să permită urmărirea istoricului afilierilor și dezafilierilor.

4. Gestionarea competițiilor județene

- Modulul trebuie să permită definirea calendarului competițional județean.
- Sistemul trebuie să permită stabilirea locațiilor, categoriilor de vârstă și nivelurilor competiționale.
- Modulul trebuie să permită înscrierea sportivilor și cluburilor în competițiile județene.
- Rezultatele competițiilor trebuie să fie introduse, validate și transmise automat către federația națională.

5. Certificatul de Identitate Sportivă (CIS)

- Modulul trebuie să permită inițierea și gestionarea procesului de obținere a CIS.
- Sistemul trebuie să permită urmărirea stării CIS (emis, suspendat, retras).
- Direcțiile Județene trebuie să poată emite CIS pentru structurile fără personalitate juridică.

6. Interacțiunea cu Direcțiile Județene pentru Sport

- Modulul trebuie să permită Direcțiilor Județene gestionarea proceselor aflate în responsabilitatea lor.
- Sistemul trebuie să asigure trasabilitatea completă a activităților realizate de Direcțiile Județene.

7. Audit și control acces

- Toate operațiunile trebuie să fie jurnalizate.
- Accesul trebuie controlat pe roluri (Asociație, DJTS, ANS).
- Istoricul modificărilor trebuie păstrat integral.

4.5.3.5 Ligile profesioniste

4.5.3.5.1 Context

Ligile profesioniste sunt structuri sportive constituite prin asocierea cluburilor sportive profesioniste pe ramuri de sport.

Ligile profesioniste sunt persoane juridice de drept privat, autonome, neguvernamentale, apolitice și fără scop lucrativ.

Ligile profesioniste, ca structuri sportive subordonate federațiilor sportive naționale, își desfășoară activitatea în baza statutelor și regulamentelor proprii.

Statutele ligilor profesioniste se aprobă de adunările generale și se avizează în mod obligatoriu de federațiile sportive naționale și de Agenția Națională pentru Sport.

Înființarea ligilor profesioniste ca structuri sportive și dobândirea personalității juridice se face în condițiile legii, în baza acordului federației sportive naționale corespunzătoare și a avizului obligatoriu al Agenției Naționale pentru Sport.

Pentru o ramură de sport se poate constitui o singură ligă națională profesionistă. Prin excepție, se pot înființa ligi profesioniste, pe niveluri competiționale, în cadrul aceleiași ramuri de sport.

Ligile profesioniste organizează competiția oficială profesionistă în ramura de sport respectivă și la nivelul stabilit de federația sportivă națională.

Certificatul de Identitate Sportivă (CIS):

Pentru a funcționa legal, ligile profesioniste trebuie să obțină un Certificat de Identitate Sportivă (CIS) eliberat de Agenția Națională pentru Sport. Acest certificat atestă înregistrarea oficială ca structură sportivă.

4.5.3.5.2 Cerințe funcționale

1. Administrarea entității

- Modulul trebuie să permită definirea unei ligi profesioniste ca entitate distinctă, cu toate datele de identificare necesare.
- Sistemul trebuie să permită gestionarea statutului juridic, a conducerii, a regulamentelor și a documentelor constitutive.
- Modulul trebuie să păstreze istoricul modificărilor asupra datelor ligii.

2. Afilierea la federația sportivă națională

- Modulul trebuie să permită gestionarea procesului de afiliere a ligii la federația sportivă națională.
- Sistemul trebuie să permită evidențierea stării afilierii (activă, suspendată, retrasă).
- Orice modificare a statutului de afiliere trebuie să fie supusă unui flux de aprobare.

3. Administrarea cluburilor profesioniste

- Modulul trebuie să permită gestionarea cluburilor profesioniste membre ale ligii.
- Sistemul trebuie să permită evidența cluburilor afiliate și neafiliate.
- Modulul trebuie să permită urmărirea istoricului afilierilor cluburilor la ligă.

4. Calendar competițional profesionist

- Modulul trebuie să permită definirea calendarului competițional profesionist.

- Sistemul trebuie să permită stabilirea etapelor, locațiilor, categoriilor și nivelurilor competiționale.
- Modulul trebuie să permită asocierea competițiilor cu cluburile și sportivii participanți.
- Calendarul trebuie să fie versionat, cu păstrarea istoricului modificărilor.

5. Rezultate și statistici

- Modulul trebuie să permită introducerea și validarea rezultatelor competițiilor profesioniste.
- Sistemul trebuie să permită generarea automată de statistici sportive.
- Rezultatele trebuie să fie utilizabile în Anuarul Sportului și în rapoartele federației.

6. Certificatul de Identitate Sportivă (CIS)

- Modulul trebuie să permită gestionarea procesului de obținere și actualizare a CIS pentru ligile profesioniste.
- Sistemul trebuie să permită urmărirea stării CIS (emis, suspendat, retras).

7. Transferuri și eligibilitate

- Modulul trebuie să permită gestionarea transferurilor sportivilor între cluburile profesioniste.
- Sistemul trebuie să permită verificarea eligibilității sportivilor pentru competițiile profesioniste.
- Toate transferurile trebuie să fie supuse unui flux de aprobare.

8. Audit și control acces

- Toate operațiunile trebuie jurnalizate.
- Accesul trebuie controlat pe roluri (Ligă, Federație, ANS).
- Istoricul modificărilor trebuie păstrat integral.

4.5.4 Modul Registrul Sportivilor și Antrenorilor

Activitatea este reglementată prin **Ordinul nr. 302 din 5 octombrie 2023.**

Registrul național al sportivilor și antrenorilor cuprinde evidența sportivilor de performanță legitimați la federațiile sportive naționale, cluburile sportive de care aparțin, categoria de vârstă, rezultatele la competițiile sportive naționale și internaționale aflate în calendarul federațiilor sportive naționale, precum și antrenorii, pe categorii de clasificare și licențiere.

Datele colectate prin Registrul național al sportivilor și antrenorilor vor fi utilizate de către Agenția Națională pentru Sport pentru elaborarea politicilor publice pentru domeniul sport, furnizarea de informații reale care vor servi la fundamentarea proiectului de buget al Agenției Naționale pentru Sport, constituirea surselor de date pentru realizarea strategiilor federațiilor sportive naționale și pentru un management performant în vederea obținerii medaliilor și rezultatelor internaționale.

Fiecare federație sportivă națională are obligația de a constitui registrul sportivilor și antrenorilor propriu. Completarea și actualizarea registrului sportivilor și antrenorilor este o activitate

permanentă. Președintele federației sportive naționale răspunde de exactitatea datelor înscrise în registrul sportivilor și antrenorilor.

Datele referitoare la sportivi, pe categorii de vârstă, cluburile sportive de care aparțin, precum și rezultatele la competițiile sportive naționale și internaționale sunt transmise Institutului Național de Cercetare pentru Sport, persoană împuternicită de Agenția Națională pentru Sport cu prelucrarea datelor, în vederea introducerii lor în Registrul național al sportivilor și antrenorilor.

Implementarea Registrului Național al Sportivilor și Antrenorilor are ca obiectiv principal îmbunătățirea managementului sportiv în România, prin asigurarea unei evidențe clare și actualizate a tuturor sportivilor și antrenorilor, facilitând astfel dezvoltarea și promovarea sportului de performanță.

4.5.4.1 Registrul Sportivilor

4.5.4.1.1 Context

Registrul Național al Sportivilor (RNS) este administrat de Institutul Național de Cercetare pentru Sport (INCS) pentru Agenția Națională pentru Sport (ANS) și are rolul de a centraliza și gestiona informațiile despre sportivii legitimați în federațiile și cluburile sportive din România. Acesta asigură recunoașterea oficială a sportivilor, monitorizează conformitatea cu reglementările, facilitează alocarea resurselor și sprijină monitorizarea dopajului. Registrul contribuie la o evidență clară, eficientă și transparentă, sprijinind strategia națională pentru dezvoltarea sportului și luarea de decizii informate în domeniu.

La data scrierii prezentului document, în RNS erau activi peste 100.000 de sportivi activi repartizați la 4619 cluburi afiliate, conform tabelului de mai jos.

Figură 6 -Date Registrul Național al Sportivilor și Antrenorilor (sursa: INCS)

4.5.4.1.2 Cerințe funcționale

Sportivul reprezintă o entitate centrală a sistemului informatic, având relații directe cu cluburile sportive, federațiile sportive, competițiile, rezultatele sportive, vizele medicale și obligațiile financiare.

- Sistemul trebuie să asigure o evidență unică, coerentă și actualizată a sportivilor, utilizând CNP-ul ca identificator unic la nivel național.
- Sistemul trebuie să permită administrarea sportivilor prin mai multe canale de acces, în funcție de rolul utilizatorului.
- Datele sportivilor trebuie să fie unice, consistente și sincronizate la nivelul întregului sistem.
- Orice modificare a datelor trebuie să fie trasabilă și supusă regulilor de validare și workflow.

- Sistemul trebuie să respecte cerințele GDPR privind datele cu caracter personal.
- Portal Public – Cont sportiv individual:
  - Aplicația trebuie să permită deschiderea unui cont de sportiv prin portalul public.
  - CNP-ul trebuie să fie utilizat ca și cheie unică de identificare.
  - Crearea contului trebuie să poată fi realizată de sportiv sau de tutorele legal.
  - Sistemul trebuie să valideze unicitatea sportivului și să returneze mesaje de eroare la tentativele de dublare.
- Funcționalități disponibile sportivului / tutorelui legal:
  - Posibilitatea de a solicita transferul între cluburi.
  - Posibilitatea de a iniția procesul de dez-afiliere sportivă.
  - Posibilitatea de a actualiza datele personale.
  - Posibilitatea de a consulta istoricul competițiilor și rezultatele sportive. ○ Posibilitatea de a solicita afilierea la un club sportiv.
- Modul Cluburi Sportive:
  - Sistemul trebuie să permită cluburilor sportive gestionarea sportivilor proprii.
  - Cluburile trebuie să poată introduce, modifica și șterge datele sportivilor, în limitele drepturilor acordate.
  - Modulul trebuie să permită introducerea și actualizarea vizelor medicale.
  - Modulul trebuie să permită evidența taxelor achitate de sportivi.
  - Toate operațiunile trebuie să fie supuse fluxurilor de lucru, acolo unde este cazul.
- Modul Federații Sportive:
  - Sistemul trebuie să permită federațiilor sportive administrarea sportivilor.
  - Federațiile trebuie să poată introduce, modifica și șterge datele sportivilor.
  - Modulul trebuie să permită înrolarea sportivilor în competiții.
  - Federațiile trebuie să poată introduce și valida rezultatele sportive.
  - Drepturile de modificare trebuie să fie configurabile pe ramuri sportive.
- Sistemul trebuie să permită introducerea unui sportiv de către federație, club sau individ.
- Introducerea trebuie să fie supusă validării automate a CNP-ului.
- Fluxul trebuie să includă verificări de consistență a datelor.
- Sistemul trebuie să permită importul sportivilor în masă.
- Importul trebuie să poată fi realizat din fișiere de tip Excel/CSV sau din alte sisteme informatice.
- Sistemul trebuie să valideze automat datele și să raporteze erorile.
- Sistemul trebuie să permită inițierea solicitărilor de ștergere a datelor sportivului.

- Ștergerea trebuie să fie realizată în conformitate cu prevederile GDPR.
- Fluxul de ștergere trebuie să fie supus aprobării.
- Sistemul trebuie să permită actualizarea rezultatelor sportive.
- Modificările trebuie să fie supuse validării prin workflow.
- Sistemul trebuie să păstreze istoricul rezultatelor.
- Sistemul trebuie să permită înscrierea sportivilor în competiții.
- Sistemul trebuie să verifice automat eligibilitatea sportivilor.
- Înscrierea trebuie să fie supusă fluxurilor de aprobare configurabile.
- Sistemul trebuie să permită transferuri între cluburi.
- Sistemul trebuie să permită transferuri între federații sau ramuri sportive.
- Transferurile trebuie să fie gestionate prin fluxuri de lucru multi-etapă.
- Istoricul transferurilor trebuie păstrat permanent.
- Sistemul trebuie să permită gestionarea următoarelor date:
  - Nume și prenume
  - CNP
  - Fotografie actuală
  - Data nașterii
  - Adresă și date de contact
  - Date tutore legal (pentru minori)
  - Relația cu tutorele legal
  - Istoric competiții
  - Rezultate sportive
  - Vize medicale
  - Taxe anuale achitate
- Sistemul trebuie să blocheze introducerea dublurilor de sportivi.
- Orice modificare trebuie validată conform rolului utilizatorului.
- Sistemul trebuie să afișeze mesaje clare de eroare și avertizare.
- Sistemul trebuie să păstreze un istoric complet al tuturor modificărilor efectuate asupra sportivului.
- Trebuie să existe audit pe utilizator, dată și tip de operațiune.
- Istoricul trebuie să fie disponibil pentru rapoarte și verificări.
- Accesul la datele sportivilor trebuie să fie strict controlat pe bază de roluri.

- Datele cu caracter personal trebuie protejate conform GDPR.
- Sistemul trebuie să permită anonimizarea sau ștergerea datelor, conform legislației.

4.5.4.2 Registrul Antrenorilor

4.5.4.2.1 Context

Registrul Antrenorilor este administrat de către federațiile sportive naționale în colaborare cu Agenția Națională pentru Sport (ANS). Federațiile sportive naționale au responsabilitatea principală de a colecta, verifica și actualiza informațiile referitoare la antrenorii care activează în ramurile sportive pe care le coordonează. Aceste federații se asigură că antrenorii respectă cerințele de calificare și certificare, iar datele sunt centralizate și înregistrate în Registrul Antrenorilor.

ANS coordonează și supraveghează acest proces, asigurând o evidență națională centralizată a tuturor antrenorilor, indiferent de disciplina sportivă. ANS poate folosi aceste informații pentru a facilita procesul de licențiere, pentru a asigura conformitatea cu reglementările legale și pentru a susține dezvoltarea continuă a antrenorilor, oferind acces la cursuri de perfecționare și programe de formare profesională.

Astfel, administrarea Registrului Antrenorilor este un proces colaborativ între federațiile sportive, care se ocupă de gestionarea specifică pe ramură sportivă, și ANS, care centralizează și monitorizează datele la nivel național.

4.5.4.2.2 Cerințe funcționale

- Antrenorul reprezintă o entitate esențială în cadrul sistemului informatic, având relații directe cu cluburile sportive, federațiile sportive, sportivii, competițiile și bazele sportive.
- Sistemul trebuie să asigure o evidență unică, națională și actualizată a antrenorilor, utilizând CNP-ul ca identificator unic.
- Sistemul trebuie să permită gestionarea antrenorilor prin mai multe canale de acces, în funcție de rolul utilizatorului.
- Datele antrenorilor trebuie să fie unice, consistente și sincronizate la nivelul întregului sistem.
- Orice modificare trebuie să fie trasabilă și supusă regulilor de validare și workflow.
- Sistemul trebuie să respecte cerințele privind protecția datelor cu caracter personal.
- Aplicația trebuie să permită crearea unui cont public de antrenor.
- CNP-ul trebuie utilizat ca identificator unic.
- Antrenorul trebuie să poată introduce și actualiza datele personale.
- Sistemul trebuie să valideze unicitatea antrenorului și să afișeze mesaje de eroare în cazul introducerilor duplicate.
- Sistemul trebuie să permită cluburilor sportive gestionarea datelor antrenorilor proprii.
- Cluburile trebuie să poată asocia antrenorii cu sportivi, ramuri sportive și competiții.
- Modificările trebuie să fie supuse fluxurilor de validare, acolo unde este cazul.
- Sistemul trebuie să permită federațiilor sportive administrarea datelor antrenorilor.

- Federațiile trebuie să poată valida calificările, rezultatele și statutul antrenorilor.
- Drepturile de modificare trebuie să fie configurabile pe ramuri sportive.
- Sistemul trebuie să permită gestionarea următoarelor categorii de date:
  - Nume și prenume
  - CNP
  - Fotografie actuală
  - Data nașterii
  - Adresă și date de contact
  - Calificări obținute și certificări
  - Rezultate obținute cu sportivii
  - Cluburi și federații la care activează sau a activat
  - Istoric profesional
- Sistemul trebuie să permită introducerea și actualizarea datelor antrenorului de către:
  - antrenor (prin portalul public),
  - cluburi sportive,
  - federații sportive.
- Introducerea și modificarea datelor trebuie să fie supuse validării automate și manuale.
- Orice modificare trebuie înregistrată în istoricul antrenorului.
- Sistemul trebuie să permită depunerea documentației necesare pentru obținerea titlului de antrenor emerit.
- Procesul trebuie gestionat printr-un flux de lucru configurabil.
- Fluxul trebuie să includă etape de verificare, avizare și aprobare.
- La finalizarea fluxului, statutul antrenorului trebuie actualizat automat.
- Sistemul trebuie să blocheze introducerea dublurilor de antrenori.
- Orice încercare de introducere a unui antrenor existent trebuie să genereze un mesaj clar de eroare.
- Datele trebuie validate în funcție de rolul utilizatorului.
- Antrenorul trebuie să poată fi asociat cu:
  - sportivi,
  - cluburi sportive,
  - federații sportive,
  - competiții și baze sportive.
- Sistemul trebuie să permită vizualizarea relațiilor active și istorice.

- Sistemul trebuie să ofere un serviciu public denumit „Pașaport Antrenor”.
- Pașaportul Antrenor trebuie să permită vizualizarea datelor publice ale antrenorului.
- Accesul la datele sensibile trebuie restricționat.
- Portalul trebuie să fie disponibil atât pentru antrenor, cât și pentru publicul autorizat.
- Sistemul trebuie să permită acces public controlat la datele sportivilor și antrenorilor.
- Datele afișate public trebuie să respecte regulile de protecție a datelor.
- Sistemul trebuie să genereze un istoric complet al modificărilor.
- Trebuie să existe audit pe utilizator, dată și tip de operațiune.
- Datele trebuie să fie disponibile pentru raportare și verificare.
- Sistemul trebuie să afișeze mesaje clare și explicite pentru erorile de validare.
- Utilizatorii trebuie notificați în cazul modificărilor importante de statut.
- Sistemul trebuie să permită configurarea notificărilor.

4.5.5 Modul Registrul Bazelor Sportive

4.5.5.1 Context

Agenția Națională pentru Sport (ANS) are atribuții limitate în procesul de omologare a bazelor sportive, întrucât responsabilitatea principală pentru omologare aparține federațiilor sportive. Cu toate acestea, ANS joacă un rol de suport și coordonare, având următoarele atribuții.

- Monitorizarea procesului de omologare: ANS urmărește procesul de omologare derulat de federațiile sportive, asigurându-se că toate bazele sportive care doresc omologare respectă standardele și procedurile stabilite.
- Gestionarea Registrului Bazelor Sportive: ANS are rolul de a administra Registrul Bazelor Sportive, inclusiv evidența bazelor omologate și neomologate. Aceasta implică înregistrarea și actualizarea datelor transmise de către federații sportive sau de către alte autorități.
- Asigurarea transparenței: ANS asigură accesul la informații legate de bazele sportive omologate, astfel încât acestea să fie disponibile publicului și tuturor părților interesate. Astfel, ANS promovează transparența și facilitează accesul la datele privind omologarea bazelor sportive.
- Suport și consiliere: ANS oferă suport și consiliere federațiilor sportive și altor entități implicate în procesul de omologare, clarificând aspecte legislative și procedurale legate de standardele pe care bazele sportive trebuie să le îndeplinească.
- Monitorizarea destinației și utilizării bazelor: După omologare, ANS are obligația de a urmări utilizarea și destinația bazelor sportive, astfel încât acestea să fie folosite în conformitate cu scopul pentru care au fost certificate, asigurând că bazele sportive contribuie la dezvoltarea sportului.

- Coordonarea cu alte autorități: ANS colaborează cu federațiile sportive, direcțiile sportive județene și consiliile locale pentru a gestiona bazele sportive neomologate și pentru a asigura actualizarea registrului.

Deși atribuțiile ANS sunt mai mult de supraveghere și coordonare, rolul său este esențial pentru a menține o evidență corectă și pentru a asigura utilizarea adecvată a bazelor sportive la nivel național.

Baze sportive omologate: Omologarea bazelor sportive este responsabilitatea federațiilor sportive, care au atribuția de a evalua și certifica aceste baze prin eliberarea unui certificat de omologare. În momentul de față, sunt omologate 63 de baze sportive. Chiar dacă o bază nu este înregistrată în registru, aceasta poate funcționa fără restricții.

Baze sportive neomologate: Aceste baze pot fi atât din domeniul public, cât și din domeniul privat. Direcțiile sportive și consiliile locale au dreptul de a adăuga în registru aceste baze sportive neomologate.

Informațiile înregistrate despre baze includ denumirea bazei sportive, adresa, numele administratorului, o descriere a facilităților și materiale multimedia (fotografii și filme).

Modulul Registru Baze Sportive are ca scop gestionarea completă, centralizată și standardizată a informațiilor referitoare la bazele sportive la nivel național, în vederea monitorizării destinației, utilizării, stării fizice și situației juridice a acestora, sub coordonarea Agenției Naționale pentru Sport (ANS).

4.5.5.2 Cerințe funcționale

- Modulul trebuie să permită evidența tuturor bazelor sportive, indiferent de forma de proprietate sau administrare.
- Sistemul trebuie să asigure o clasificare standardizată a bazelor sportive.
- Accesul la date trebuie să fie controlat pe bază de roluri și competențe.
- Toate operațiunile asupra bazelor sportive trebuie să fie supuse fluxurilor de lucru.
- Sistemul trebuie să asigure trasabilitate completă și audit.
- Modulul trebuie să permită clasificarea bazelor sportive conform următoarelor categorii:
  - B1 – Tabel pentru bazele aflate în domeniul public al statului și în subordinea ANS
  - B2 – Tabel pentru bazele aflate în domeniul privat al statului și în subordinea ANS
  - B3 – Tabel pentru bazele aflate în domeniul public al statului și în subordinea CJ și/sau CL
  - B4 – Tabel pentru bazele aflate în domeniul privat al statului și în subordinea CJ și/sau CL
  - B5 – Tabel pentru bazele aflate anterior în domeniul public al statului, transferate în domeniul privat
  - B6 – Tabel pentru bazele aflate anterior în domeniul privat al statului, transferate în domeniul privat

- B7 – Tabel pentru bazele aflate în domeniul public al statului și în subordinea altor departamente
- B8 – Tabel pentru bazele aflate în domeniul privat al statului și în subordinea altor departamente
- B9 – Tabel pentru bazele sportive desființate și reamenajate pe alt amplasament

- Modulul trebuie să permită gestionarea următoarelor date generale:
  - Denumire bază sportivă
  - Adresa
  - Starea actuală a bazei sportive
  - Descriere tehnică și suprafețe (mp) – bază sportivă
  - Omologat
  - Persoana juridică deținătoare a dreptului de proprietate
  - Persoana juridică deținătoare a dreptului de folosință/administrare, prin: închiriere/comodat/concesiune/altă formă legală
  - Denumire UPS "Descriere UPS
  - Caracteristici tehnice"
  - Județ
  - Situație juridica/Intabulat/neintabulat/domeniul public/privat al statului
  - Stare fizica FUNCTIONAL/NEFUNCTIONAL
  - OMOLOGAT DE FEDERATIA (daca este cazul)
  - Total tipuri UPS
  - BAZA SPORTIVA COMPONENTA UPS-uri
  - UPS construcții acoperite
  - Sala polivalenta
  - Sala specializata jocuri: Baschet, Handbal, Volei
  - Sala specializata gimnastica/gimnastica ritmica
  - Sala specializata atletism indoor
  - Sala specializata atletica grea (haltere)
  - Sala specializata scrima
  - Sala specializata lupte
  - Sala specializata judo
  - Sala specializata arte marțiale
  - Sala specializata culturism si/sau fitness
  - Sala specializata dans sportiv

- Sala specializata popice
- Sala specializata bowling
- Sala specializata box
- Sala specializata badminton
- Sala specializata tenis de masa
- Sala specializata escalada
- Sala specializata forța, recuperare
- Piscina cu: Bazin natație, Bazin polo, Bazin sărituri, Bazin înot sincron
- Patinoar
- Velodrom
- Arena de tenis
- Alte tipuri de construcții
- UPS de tipul terenuri si/sau instalații sportive in aer liber
- Stadion: Fotbal, Rugby, Atletism, Baseball, Combinat (jocuri si atletism), Hipodrom, Velodrom
- Piscina descoperita cu: Bazin natație, Bazin polo, Bazin sărituri, Patinoar descoperit
- Teren de golf
- Terenuri mari de sport (jocuri cu mingea): Fotbal, Rugby, Baseball, Hochei pe iarba
- Terenuri mici de sport (jocuri cu mingea): Oina, Handbal, Fotbal-Tenis, Tenis, Baschet, Volei
- Piste si terenuri de atletism: Pista alergări, Pista alergări viteza, Teren probe aruncări, Teren probe sărituri
- Pista ciclism, Pista carting, Pista motociclism, Pista automobilism, Pista modelism Automodele
- Aeromodele Navomodele
- Pista role
- Pista karting
- Alte piste (se specifica)
- Poligon tir cu arcul
- Poligon trageri
- Terenuri echitație: Centre echitație, Pista trap, Manej
- Teren cariera: UPS canotaj, UPS Kaiaccanoe, Bazin cursa dreapta, Slalom Râu
- Pârtii sporturi de iarnă: Schi, Sanie, ○ Snowboard, Piste sporturi de iarna, Bob, ○ Patinaj viteza, Curling Start bob/sanie.

- Trambulina sărituri schi
- Turn parașutism
- Alte tipuri de spatii pentru practicarea sportului
- UPS de tipul terenuri si/sau instalații sportive in aer liber
- Teren de sport(se specifica) Piscina Patinoar Altele (se specifica)
- CC construcții cu funcțiuni complementare
- Spatii cazare sportivi
- Spatii alimentație sportivi
- Spatii tehnice (instalații specifice)
- Clădiri independente vestiare sportivi
- Clădiri administrative Altele (se va specifica).

- Sistemul trebuie să implementeze un set complet de workflow-uri configurabile, care să guverneze întreg ciclul de viață al unei baze sportive în registru, de la introducerea inițială până la dezafectare sau schimbarea statutului juridic.
- Introducerea unei baze sportive trebuie realizată printr-un flux controlat de tip inițiere – validare – aprobare – publicare.
- Workflow-ul trebuie să permită completarea etapizată a datelor generale, tehnice, juridice și operaționale.
- Sistemul trebuie să permită atașarea documentelor justificative (acte de proprietate, documentație tehnică, schițe, avize etc.).
- Publicarea bazei sportive în registru trebuie să fie condiționată de validarea completitudinii datelor obligatorii.
- Modificarea datelor unei baze sportive trebuie să fie realizată printr-un workflow de actualizare.
- Sistemul trebuie să permită diferențierea între:
  - actualizări minore (date descriptive),
  - actualizări majore (schimbare statut juridic, stare funcțională, structură UPS).
- Actualizările majore trebuie supuse unui proces de aprobare explicită.
- Istoricul modificărilor trebuie păstrat integral.
- Sistemul nu va permite ștergerea fizică a bazelor sportive din registru.
- Dezactivarea trebuie să păstreze toate datele istorice și relațiile existente.
- Pentru bazele din categoria B9 trebuie să existe evidență separată a relocării sau reamenajării.
- Sistemul trebuie să permită inițierea procesului de omologare de către entitățile autorizate.

- Workflow-ul de omologare trebuie să includă:
  - transmiterea documentației,
  - evaluarea de către federația competentă, ○ emiterea deciziei de omologare.
- Statutul de omologare trebuie să fie corelat cu tipurile de competiții permise.
- Sistemul trebuie să gestioneze termenele de valabilitate ale omologărilor.
- Sistemul trebuie să permită înregistrarea și gestionarea comunicărilor cu terți (instituții publice, federații, administratori).
- Comunicările trebuie asociate explicit unei baze sportive.
- Trebuie păstrat istoricul complet al comunicărilor, inclusiv documentele atașate.
- Sistemul trebuie să implementeze un mecanism avansat de control al accesului bazat pe roluri și competențe.
- ANS trebuie să beneficieze de drepturi complete de:
  - administrare date,
  - validare,
  - aprobare,
  - raportare și audit.
- Accesul la date trebuie limitat în funcție de:
  - tipul bazei sportive,
  - aria geografică,
  - categoria juridică.
- Sistemul trebuie să permită definirea de roluri custom.
- Accesul la operațiuni critice trebuie să fie jurnalizat și supus aprobării.
- Sistemul trebuie să păstreze istoricul complet al tuturor operațiunilor.
- Pentru fiecare modificare trebuie înregistrate:
  - utilizatorul,
  - data și ora,
  - tipul operațiunii,
  - valorile anterioare și ulterioare.
- Jurnalele de audit trebuie să fie accesibile doar utilizatorilor autorizați.
- Sistemul trebuie să ofere capabilități avansate de raportare, incluzând:
  - rapoarte privind starea bazelor sportive (funcțional / nefuncțional),
  - rapoarte pe categorii B1–B9,
  - rapoarte privind gradul de omologare,

- rapoarte de utilizare și distribuție geografică,
- export de rapoarte în formate standard (PDF, Excel).

4.5.6 Modul Anuarul Sportului

4.5.6.1 Context

Anuarul Sportului este o publicație de statistică oficială care compilează și prezintă informații detaliate despre rezultatele sportivilor români pe parcursul unui an calendaristic la nivel național și internațional. Acesta este publicat de către Agenția Națională pentru Sport și servește drept instrument esențial de informare, analiză și arhivare pentru toți cei implicați în sectorul sportiv.

Anuarul Sportului reprezintă o sursă de referință pentru Institutul Național de Statistică și pentru toate părțile interesate din domeniul sportiv, oferind o imagine clară asupra progreselor, performanțelor și activităților sportivilor și structurilor sportive din România. Este un instrument esențial pentru dezvoltarea politicilor în sport, pentru a urmări evoluția activităților și pentru a promova imaginea sportului românesc atât la nivel național, cât și internațional.

Conținutul Anuarului Sportului:

- Statistici și rezultate: Include rezultate de competiții naționale și internaționale, recorduri, clasamente și performanțele notabile ale sportivilor din România.
- Informații despre structurile sportive: Prezintă detalii despre federațiile sportive naționale, cluburi, asociații, precum și clasamente și activitățile acestora în anul respectiv.
- Profiluri de sportivi și antrenori: Cuprinde informații biografice (care se vor regăsi doar în baza de date și nu vor fi publicate) și descrierea performanțelor sportivilor români, precum și detalii despre antrenorii care i-au pregătit.
- Competiții și evenimente sportive: Prezintă principalele momente, fapte și evenimente (competiții naționale și internaționale) desfășurate într-un an calendaristic în cadrul mișcării sportive românești
- Programe și politici publice în sport: Anuarul include detalii despre politicile naționale de dezvoltare a sportului, investițiile realizate în infrastructura sportivă și strategiile guvernamentale adoptate pentru a sprijini sectorul sportiv.

Scopurile Anuarului Sportului:

- Arhivare și documentare: Păstrează un istoric detaliat al activității sportive din România, fiind o resursă importantă pentru cercetători, oficiali, și istorici în sport.
- Informare publică: Asigură acces la informații actualizate despre sportul românesc pentru jurnaliști, academicieni, oficiali și pasionați de sport.
- Monitorizare și evaluare: Facilitează evaluarea progreselor realizate în sport, contribuind la analiza și planificarea viitoarelor strategii pentru dezvoltarea sportului în România.
- Transparență și responsabilitate: Prin publicarea datelor oficiale, se asigură transparența activităților și utilizării resurselor publice în sport, precum și promovarea responsabilității organizațiilor sportive.

Acces și utilizare:

- Versiune tipărită: Este distribuită Institutului Național pentru Statistică, instituțiilor sportive, federațiilor, bibliotecilor și altor organizații interesate.
- Versiune digitală: Poate fi accesată online pe site-urile oficiale ale autorităților sportive, cum ar fi Agenția Națională pentru Sport, pentru a oferi acces ușor la informații și a sprijini digitalizarea.

4.5.6.2 Cerințe funcționale

- Modulul Anuarul Sportului trebuie să asigure generarea automată, centralizată și unitară a statisticilor oficiale și a clasamentelor sportive, pe baza datelor introduse în sistem de federațiile sportive naționale, cluburile sportive și alte entități autorizate.
- Modulul trebuie să funcționeze ca sursă oficială de raportare, publicare și arhivare a rezultatelor sportive la nivel național și internațional.
- Modulul trebuie să genereze automat clasamentele și statisticile, fără introducere manuală de calcule.
- Toate statisticile trebuie să fie generate exclusiv pe baza datelor validate existente în sistem.
- Algoritmii de calcul trebuie să fie unitari, transparenți și reutilizabili.
- Modulul trebuie să permită recalcularea statisticilor în cazul modificării datelor sursă.
- Modulul trebuie să permită generarea de:
  - clasament general pe federații;
  - clasament separat pentru probe olimpice;
  - clasament separat pentru probe neolimpice.
- Clasamentele trebuie să fie generate pe perioade configurabile (an competițional, ciclu olimpic etc.).
- Modulul trebuie să evidențieze contribuția fiecărei competiții la punctajul total.
- Modulul trebuie să permită calcularea punctajelor pe județe. Clasamentele trebuie generate distinct pentru:
  - probe olimpice;
  - probe neolimpice.
- Județul trebuie determinat automat în funcție de afilierea sportivilor sau unităților sportive.
- Modulul trebuie să permită generarea clasamentelor individuale ale sportivilor români. Clasamentele trebuie să poată fi filtrate pe:
  - ramură sportivă;
  - tip competiție;
  - categorie de vârstă;
  - nivel competițional.

- Modulul trebuie să genereze: clasament general; clasamente distincte pentru probe olimpice și neolimpice.
- Modulul trebuie să permită identificarea automată a unităților din subordinea ANS.
- Clasamentele trebuie generate separat pentru: probe olimpice; probe neolimpice.
- Modulul trebuie să permită clasificarea unităților sportive din subordinea ME.
- Clasamentele trebuie generate distinct pentru probe olimpice și neolimpice.
- Modulul trebuie să permită calcularea punctajelor pentru: seniori; tineret; juniori; cadeți. Punctajele trebuie să fie agregate pe federații și ramuri sportive.
- Modulul trebuie să genereze: clasament pe medalii; punctaj general; punctaj pe categorii de clasificare sportivă. Județul trebuie corelat automat cu structurile sportive și sportivii.
- Modulul trebuie să genereze: clasament general unități sportive; clasamente distincte pentru unitățile din subordinea ANS; clasamente distincte pentru unitățile din subordinea Ministerului Educației.
- Modulul trebuie să includă evidența activităților organizate și conduse de federațiile sportive naționale.
- Trebuie să existe posibilitatea de a înregistra:
  - structura organizațională;
  - organele de conducere;
  - activitatea competițională;
  - clasamentele aferente. Aceste informații trebuie corelate cu statisticile și clasamentele generate.
- Modulul trebuie să includă toți algoritmii necesari pentru:
  - calcul punctaje;
  - agregare rezultate;
  - clasificare pe criterii multiple.
- Algoritmii trebuie să fie documentați și parametrizabili.
- Sistemul trebuie să permită adaptarea algoritmilor la modificări de regulamente sportive.
- Sistemul trebuie să permită validarea datelor înainte de generarea statisticilor.
- Modulul trebuie să evidențieze explicit:
- ce date lipsesc; ○ ce federații nu au transmis datele necesare;
- ce perioade sunt incomplete.
- Trebuie să existe notificări automate către entitățile responsabile.
- Publicarea trebuie să fie permisă doar după finalizarea validării.
- Clasamentele publicate trebuie să fie marcate ca „oficiale”.

- Sistemul trebuie să păstreze versiuni istorice ale clasamentelor publicate.
- Modulul trebuie să permită publicarea statisticilor în portalul public. Clasamentele trebuie să poată fi: vizualizate online; exportate în formate standard (PDF, Excel). Accesul la datele detaliate trebuie controlat pe roluri.
- Sistemul trebuie să asigure trasabilitatea completă a datelor utilizate în calcule. Pentru fiecare clasament trebuie să existe: sursa datelor; data generării; utilizatorul responsabil.
- Modulul trebuie să permită arhivarea anuală a Anuarului Sportului.

Almanah online

- Modulul trebuie să preia automat și exclusiv datele validate din sistemul central al Anuarului Sportului.
- Modulul nu trebuie să permită introducerea manuală a datelor statistice.
- Orice modificare sau republicare a clasamentelor oficiale trebuie să actualizeze automat informațiile din Almanah.
- Modulul trebuie să includă un tablou de bord public cu indicatori agregați anual și pe perioade configurabile.
- Dashboard-ul trebuie să permită filtrarea datelor după: an competițional; ciclu olimpic; ramură sportivă; probă olimpică / neolimpică; categorie de vârstă; județ; nivel competițional.
- Modulul trebuie să afișeze grafice dinamice privind: evoluția performanțelor în timp; distribuția medaliilor; comparații între federații; comparații între județe.
- Modulul trebuie să includă hartă interactivă a României cu distribuția performanțelor pe județe.
- Toate vizualizările trebuie să permită export în format PDF și Excel.
- Modulul trebuie să permită generarea și afișarea următoarelor clasamente: clasament general național; clasament pe federații; clasament pe județe; clasament individual sportivi; clasament unități sportive; clasament pe medalii; clasament pe punctaj general; clasament pe categorii de clasificare sportivă.
- Clasamentele trebuie generate distinct pentru: probe olimpice; probe neolimpice; unități din subordinea ANS; unități din subordinea Ministerului Educației.
- Modulul trebuie să permită filtrarea clasamentelor după: ramură sportivă; categorie de vârstă (seniori, tineret, juniori, cadeți); tip competiție; nivel competițional; perioadă configurabilă.
- Clasamentele trebuie să permită: sortare multiplă; căutare rapidă; filtrare avansată; generare link permanent; export în formate standard.
- Fiecare clasament trebuie să fie marcat explicit cu statusul: „Provizoriu”, „Validat” sau „Oficial”.
- Modulul trebuie să genereze automat profil public pentru fiecare sportiv, care să includă:

- performanțe anuale;
- medalii obținute;
- clasări relevante;
- participări la competiții;
- evoluție în timp;
- contribuția la punctajul total al federației și județului.

- Modulul trebuie să prevină publicarea oricăror date cu caracter personal nedestinate accesului public.
- Profilul public al antrenorului trebuie să includă: sportivii pregătiți; rezultatele obținute de aceștia; contribuția la punctajele agregate.
- Modulul trebuie să includă o secțiune dedicată evidențierii performanțelor notabile ale anului.
- Sistemul trebuie să permită generarea automată a unui timeline al competițiilor și rezultatelor majore.
- Modulul trebuie să evidențieze: recorduri stabilite; participări la competiții internaționale majore; performanțe istorice raportate la ediții anterioare.
- Modulul trebuie să permită afișarea pentru fiecare federație: structură organizațională; organe de conducere; competiții organizate; activitate competițională anuală; rezultate agregate.
- Modulul trebuie să permită afișarea pentru fiecare unitate sportivă: afiliere; județ; performanțe; poziționare în clasamente.
- Datele afișate trebuie corelate automat cu statisticile generate.
- Modulul trebuie să includă funcționalitate de căutare avansată.
- Căutarea trebuie să permită interogarea după: sportiv; antrenor; federație; competiție; an; medalie; județ; categorie de vârstă.
- Modulul trebuie să permită publicarea doar a datelor validate oficial.
- Clasamentele publicate trebuie marcate „Oficial”.
- Modulul trebuie să păstreze versiuni istorice anuale ale Almanahului.
- Sistemul trebuie să permită navigarea între edițiile anuale.
- Trebuie să existe posibilitatea generării unei versiuni digitale oficiale arhivabile a fiecărei ediții.

4.5.7 Modul Galeria Marilor Sportivi

4.5.7.1 Context

"Galeria Marilor Sportivi" este o inițiativă dedicată celebrării realizărilor sportivilor de elită din România, oferind o platformă pentru a păstra și a prezenta moștenirea sportivă națională.

Aceasta servește drept un spațiu în care sunt expuse trofee, medalii, echipamente, fotografii și alte artefacte care ilustrează parcursul carierelor unor sportivi remarcabili.

Prin intermediul acestei galerii, publicul poate descoperi povestea marilor campioni ai României, performanțele lor și contribuțiile aduse sportului la nivel național și internațional.

"Galeria Marilor Sportivi" are rolul de a păstra și de a promova amintirea marilor performanțe sportive și de a inspira următoarele generații prin exemple de muncă, ambiție și succes. Este o parte importantă a culturii sportive naționale și contribuie la conștientizarea valorilor și a impactului sportului asupra societății.

Rolul și importanța "Galeriei Marilor Sportivi":

- Omagiu adus sportivilor de elită: Galeria este un spațiu în care sunt onorați sportivii care au obținut rezultate excepționale, atât la nivel național, cât și internațional, aducând recunoaștere României pe scenele mondiale. Aici sunt prezentate poveștile lor, eforturile și sacrificiile care au stat la baza succeselor obținute.
- Conservarea patrimoniului sportiv: păstrează și arhivează obiecte și documente care reflectă istoria sportului românesc, contribuind la conservarea patrimoniului sportiv și la transmiterea acestuia către generațiile viitoare.
- Inspirație pentru tineri: Galeria reprezintă o sursă de inspirație pentru tinerii sportivi și pentru toți cei interesați de sport, prin exemplele de perseverență, determinare și excelență oferite de campioni. Prin expunerea poveștilor lor, inspiră tinerii să își urmeze visele și să devină, la rândul lor, campioni.
- Educație și promovare a sportului: joacă un rol educativ, oferind informații despre diferitele ramuri sportive, despre competițiile la care au participat sportivii și despre istoria sportului românesc. Vizitatorii pot afla detalii despre evoluția sporturilor, tehnici de antrenament, dar și despre valorile și principiile care stau la baza succesului sportiv.
- Evenimente și activități conexe: poate găzdui și diverse evenimente, cum ar fi întâlniri cu sportivi, lansări de cărți sau conferințe tematice legate de sport, contribuind astfel la dezvoltarea culturii sportive în România.

Expozițiile din Galeria Marilor Sportivi includ, de obicei:

- Trofee și medalii câștigate la competiții majore (Olimpiade, Campionate Mondiale și Europene).
- Echipamente sportive purtate de sportivi în timpul competițiilor importante.
- Fotografii și înregistrări video care documentează momente semnificative din carierele sportivilor.
- Documente oficiale și materiale care ilustrează parcursul carierei unor sportivi de renume.

Galeria Marilor Sportivi adăpostește peste 10.000 artefacte (diplome, trofee și medalii, fanioane, cupe, fotografii, materiale sportive) care au aparținut unor fruntași ai sportului românesc. Dintre acesta, 7000 de piese necesită atenție deosebită.

4.5.7.2 Cerințe funcționale

- Modulul trebuie să includă un sistem integrat de management al vizitelor în cadrul Galeriei Marilor Sportivi.
- Trebuie să existe posibilitatea de a programa vizite individuale și de grup, cu selecția:

o datei și intervalului orar;

o tipului de vizită (individuală, ghidată, eveniment special).

- Sistemul trebuie să permită definirea capacității maxime de vizitatori pe interval orar.
- Modulul trebuie să permită configurarea tipurilor de bilete (standard, redus, gratuit, eveniment).
- Trebuie să existe funcționalitatea de vânzare online a biletelor, cu:
  - generare automată de bilete electronice;
  - identificare unică (cod QR sau echivalent).
- Sistemul trebuie să permită validarea biletelor la acces.
- Modulul trebuie să păstreze evidența vizitelor efectuate și a biletelor vândute.
- Trebuie să existe rapoarte privind:
  - numărul de vizitatori;
  - gradul de ocupare;
  - venituri generate.

Tur virtual al Galeriei Marilor Sportivi

1. **Tur virtual tip muzeu**

Prestatorul va dezvolta un tur virtual tip muzeu, utilizând artefactele fotografiate, pentru exponatele considerate reprezentative. Lista finală a exponatelor incluse în tur va fi stabilită în etapa de analiză și proiectare.

- Modulul trebuie să permită realizarea unui tur virtual al Galeriei Marilor Sportivi.
- Turul virtual trebuie să permită navigarea interactivă între zonele galeriei.
- Pentru fiecare piesă expusă trebuie să existe posibilitatea de:
  - vizualizare detaliată;
  - asociere conținut text;
  - redare conținut audio și video.
- Modulul trebuie să permită integrarea unui ghid audio care să ruleze pe fundal în timpul turului virtual.
- Ghidul audio trebuie să poată fi:
  - activat/dezactivat de utilizator;
  - sincronizat cu piesele vizualizate.
- Modulul trebuie să permită integrarea materialelor multimedia provenite din Arhiva TVR.

- Conținutul multimedia trebuie să fie accesibil atât în turul virtual, cât și în paginile individuale ale pieselor.

Managementul arhivei digitale

- Modulul trebuie să includă un sistem complet de management al arhivei digitale de artefacte.
- Trebuie să existe posibilitatea de:
  - introducere artefact;
  - actualizare informații;
  - ștergere/dezactivare artefact.
- Pentru fiecare artefact trebuie să poată fi asociate:
  - imagini;
  - materiale video;
  - materiale audio;
  - documente digitale.
- Modulul trebuie să permită clasificarea artefactelor pe:
  - ramuri sportive;
  - sportivi;
  - competiții;
  - perioade istorice.
- Federațiile sportive trebuie să aibă:
  - drept de introducere date pentru artefactele proprii;
  - drept de vizualizare asupra întregii arhive, conform nivelului de acces.
- Orice modificare a datelor din arhivă trebuie să fie supusă unui control de acces și să fie auditabilă.

Expoziții digitale

- Modulul trebuie să permită definirea și administrarea expozițiilor digitale.
- Expozițiile trebuie să poată fi grupate pe ramuri sportive.
- Trebuie să existe posibilitatea de:
  - asociere artefacte la o expoziție;
  - ordonare personalizată a pieselor expuse;
  - definire descrieri și contexte tematice.
- Modulul trebuie să permită publicarea și retragerea expozițiilor.
- Expozițiile trebuie să poată fi afișate atât în turul virtual, cât și pe site-ul public.

Multilingvism

- Site-ul Galeriei Marilor Sportivi trebuie să fie disponibil în minimum două limbi:
  - limba română;
  - limba engleză.
- Modulul trebuie să permită gestionarea conținutului multilingv pentru:
  - descrieri sportivi;
  - artefacte;
  - expoziții;
  - ghid audio/text.
- Utilizatorul trebuie să poată schimba limba de afișare în orice moment.
- Structura trebuie să permită adăugarea ulterioară de noi limbi.

Control acces și audit

- Accesul la funcționalitățile de administrare trebuie să fie controlat pe roluri.
- Modulul trebuie să păstreze jurnalizarea tuturor operațiunilor efectuate.
- Trebuie să existe istoricul modificărilor asupra artefactelor și expozițiilor.

4.5.7.3 Digitalizarea artefactelor

Prestatorul va asigura digitalizarea completă a colecției „Galeria Marilor Sportivi”, incluzând inventarierea digitală, fotografierea 2D a tuturor artefactelor, fotografierea 3D/multi-unghi pentru artefactele selectate de Beneficiar și publicarea online a întregii colecții. Pentru un subset stabilit de Beneficiar, prestatorul va furniza vizualizări avansate de tip tur virtual / muzeu digital.

2. **Inventariere digitală**

Prestatorul va realiza inventarierea digitală completă a tuturor artefactelor (diplome, trofee și medalii, fanioane, cupe, fotografii, materiale sportive etc.) din „Galeria Marilor Sportivi”, estimată la peste 10.000 de piese, prin crearea unei evidențe digitale care să includă cel puțin: identificator unic, descriere, categorie, stare, proveniență și alte metadate necesare gestionării colecției. Dintre acestea, aproximativ 7.000 de piese necesită atenție deosebită, conform clasificării furnizate de beneficiar. Acestea vor fi manipulate și digitalizate conform unor proceduri speciale, aplicabile obiectelor fragile sau cu valoare patrimonială, cu respectarea legislației în vigoare privind protejarea și manipularea bunurilor culturale mobile (inclusiv Legea nr. 182/2000, Legea nr. 311/2003 și normele tehnice aferente), acolo unde este cazul. Prestatorul va utiliza personal instruit, echipamente adecvate și condiții controlate de lucru, va documenta fiecare manipulare și va răspunde integral pentru integritatea fizică a acestor piese pe durata operațiunilor de inventariere, fotografiere 2D/3D și publicare digitală.

Ofertantul va descrie în cadrul ofertei procedurile operaționale detaliate pentru manipularea, pregătirea, digitalizarea și repunerea în siguranță a artefactelor, cu evidențierea distinctă a măsurilor aplicate celor aproximativ 7.000 de piese care necesită atenție deosebită, conform clasificării furnizate de Beneficiar. Procedurile vor include cel puțin:

- metodologia de manipulare a obiectelor fragile, incluzând personalul autorizat/instruit, echipamentele utilizate și condițiile de lucru controlate (iluminare, temperatură, umiditate);
- fluxul de inventariere digitală, cu indicarea modului de preluare, etichetare, înregistrare și documentare a fiecărui artefact;
- procedurile de fotografiere 2D și 3D/multi-unghi, cu descrierea setup-ului tehnic, a poziționării obiectelor sensibile și a măsurilor de protecție împotriva deteriorării;
- măsurile de trasabilitate și control al integrității, incluzând modul de documentare a fiecărei manipulări și raportarea incidentelor;
- procedurile de repunere în siguranță a artefactelor după fotografiere;
- măsurile suplimentare aplicate pieselor clasificate ca necesitând atenție deosebită, distinct de fluxul standard.

3. **Fotografiere 2D**

Prestatorul va realiza fotografiere 2D pentru toate artefactele, respectând următoarele cerințe minime:

- iluminare uniformă, fără umbre dure sau reflexii excesive;
- rezoluție minimă 12 MP;
- fundal neutru și consistent;
- acuratețe cromatică adecvată;
- livrarea fișierelor în formate standard (JPEG/PNG pentru web, TIFF pentru arhivă, dacă este necesar).

4. **Fotografiere 3D (multi-unghi)**

Prestatorul va realiza fotografiere 3D pentru artefactele selectate, prin captură multi-unghi, respectând următoarele cerințe minime:

- set de fotografii realizate din unghiuri multiple, care să permită percepția tridimensională;
- iluminare constantă pe toate cadrele;
- rezoluție minimă 12 MP pentru fiecare cadru;
- livrarea seturilor de imagini într-un format compatibil cu vizualizatoare 3D de tip „spin view”.

5. **Publicare online**

Prestatorul va publica artefactele fotografiate pe portalul public al ANS, în format optimizat pentru vizualizare, accesibilitate și încărcare rapidă.

4.5.8 Modul CNFPA

4.5.8.1 Context

Centrul Național de Formare și Perfecționare a Antrenorilor (CNFPA) este o instituție specializată în formarea, perfecționarea și certificarea antrenorilor din România, funcționând sub autoritatea **ANS**. Scopul său principal este de a sprijini dezvoltarea competențelor profesionale ale antrenorilor, asigurând un nivel ridicat de calitate în pregătirea sportivilor la toate nivelurile.

CNFPA are un rol crucial în asigurarea calității antrenamentului sportivilor români, prin formarea și perfecționarea continuă a antrenorilor. Prin cursuri specializate, certificări, și programe de formare continuă, CNFPA contribuie la creșterea profesionalismului în sportul românesc și la menținerea unui nivel ridicat de competitivitate în competițiile internaționale.

Rolul și atribuțiile Centrului Național de Formare și Perfecționare a Antrenorilor:

1. **Formarea inițială a antrenorilor:**
   - CNFPA oferă cursuri de formare inițială pentru cei care doresc să devină antrenori, asigurându-se că aceștia dobândesc cunoștințele și abilitățile necesare pentru a începe o carieră în acest domeniu.
   - Aceste cursuri acoperă aspecte teoretice și practice, incluzând noțiuni de psihologie sportivă, metodologie de antrenament, fiziologia efortului, precum și regulamentele competiționale specifice diferitelor ramuri sportive.
2. **Perfecționarea și actualizarea competențelor:**
   - Pentru antrenorii activi, centrul oferă programe de perfecționare și cursuri de formare continuă, astfel încât aceștia să fie la curent cu cele mai noi metodologii, tehnici și practici în domeniul sportului.
   - Perfecționarea continuă este esențială pentru adaptarea la cerințele în schimbare ale sportului modern, oferind antrenorilor instrumentele necesare pentru a maximiza performanțele sportivilor.
3. **Certificarea și licențierea antrenorilor:**
   - CNFPA are responsabilitatea de a emite certificate și licențe care atestă calificarea și competențele profesionale ale antrenorilor. Aceste documente sunt necesare pentru ca un antrenor să poată activa oficial în România, la nivel național sau internațional.
   - Formarea continuă este un proces prin care antrenorii trebuie să își reînnoiască statutul de antrenor, dovedind participarea la cursuri de perfecționare și îmbunătățirea continuă a competențelor.
4. **Elaborarea și actualizarea curriculei de formare:**
   - CNFPA colaborează cu federațiile sportive și cu alte instituții naționale și internaționale pentru a dezvolta și actualiza curriculele de formare a antrenorilor. Aceasta asigură că programele educaționale reflectă cele mai noi tendințe și standarde în sportul de performanță.
5. **Organizarea și colaborarea cu federațiile sportive:**
   - Centrul lucrează îndeaproape cu federațiile sportive naționale pentru a asigura formarea specifică fiecărei ramuri sportive și pentru a răspunde nevoilor particulare ale fiecărei discipline.

- În colaborare cu federațiile, CNFPA organizează cursuri și workshop-uri destinate antrenorilor implicați în sporturile olimpice, neolimpice și de masă.

6. **Promovarea eticii și valorilor în sport:**
   - CNFPA pune accent pe promovarea unui set de valori esențiale în sport, cum ar fifair-play-ul, respectul pentru adversar și integritatea în activitățile sportive.
   - Antrenorii sunt educați nu doar în metodele de antrenament, ci și în importanța creării unui mediu pozitiv și motivant pentru sportivi, având un rol important în formarea lor, **atât pe plan sportiv, cât și personal.**
7. **Programe de dezvoltare internațională:**
   - Centrul colaborează cu instituții și organizații internaționale pentru a facilita schimburi de experiență și pentru a implementa cele mai bune practici din alte sisteme sportive dezvoltate. Astfel, antrenorii au acces la programe care le permit să obțină experiență internațională.

Beneficiile CNFPA pentru sportul românesc:

- Profesionalizarea antrenorilor: Prin cursurile și certificările oferite, CNFPA contribuie la profesionalizarea antrenorilor, ceea ce duce la îmbunătățirea calității pregătirii sportivilor.
- Actualizare constantă: Antrenorii sunt la curent cu cele mai noi metodologii și tehnologii, ceea ce contribuie la dezvoltarea sportului de performanță în România.
- Uniformizarea standardelor: CNFPA asigură o uniformizare a nivelului de pregătire și competențe în rândul antrenorilor, ceea ce contribuie la îmbunătățirea performanței generale a sportivilor la nivel național.

4.5.8.2 Cerințe funcționale

- Modulul CNFPA trebuie să asigure suportul informatic complet pentru desfășurarea activităților didactice, administrative și de certificare profesională a antrenorilor. Activitățile didactice ale CNFPA se vor desfășura prin platforme specializate, acreditate de Ministerul Muncii.
- În cadrul sistemului vor fi disponibile următoarele fluxuri de lucru:
  - Eliberare certificate de absolvire.
  - Eliberare carnete de antrenori.
  - Certificate de clasificare profesională.
  - Eliberarea de atestate de recunoaștere profesionala pentru ocupația de antrenor, obținute Într-un stat membru al Uniunii Europene, al Spațiului Economic European, în Confederația Elvețiana sau într-un stat terț. Platforma pentru depunerea documentelor și obținerea atestatului.
  - Promovare antrenori, încărcare documente si obținere certificat de promovare.
  - Semnare de Protocoale pentru Formare si Atestare a Antrenorilor (ANS, Federație si CNFPA).

- Catalog electronic.
- Evidența antrenorilor ce au urmat cursurile școlii. Interconectare cu modulul federații/cluburi.
- Gestionarea cursurilor organizate de ANS:
  - ✓ Monitorizează activitatea cursanților, cum ar fi progresul în cursuri, notele obținute, și timpul petrecut pe platformă.
  - ✓ Testare și evaluare: Permite crearea de teste, quiz-uri și evaluări pentru a măsura înțelegerea și performanța cursanților.
  - ✓ Comunicare și colaborare: Include funcții pentru comunicare, cum ar fi forumuri, chat-uri, sau conferințe video.
  - ✓ Raportare și analiză: Generează rapoarte despre activitatea utilizatorilor și performanța cursurilor pentru a sprijini luarea deciziilor.
  - ✓ Automatizare: Simplifică procese administrative, cum ar fi înscrierea automată, notificările și certificarea.
  - ✓ Crearea de conținut interactiv: Permite crearea, organizarea și stocarea cursurilor și materialelor educaționale.

- Soluția trebuie să permită configurarea structurii cursurilor (capitole, lecții, materiale, evaluări), precum și adăugarea, modificarea sau eliminarea câmpurilor aferente cursurilor (ex. descriere, durată, nivel, acreditare), în funcție de cerințele stabilite în analiză.
- Soluția trebuie să permită extinderea structurii cursurilor ulterior lansării, fără afectarea cursurilor existente.
- Soluția trebuie să permită integrarea unuia sau mai multor procesoare de plăți, stabilite în etapa de analiză, precum și integrarea ulterioară a unui procesator nou, dacă acesta nu este disponibil inițial.
- Soluția trebuie să asigure compatibilitate cu plăți unice, plăți recurente (abonamente) și eventual rate, dacă acestea sunt definite în analiză.
- Soluția trebuie să permită definirea modelelor de certificate conform specificațiilor stabilite în etapa de analiză.
- Soluția trebuie să permită configurarea fluxului de obținere a certificatului (ex. finalizare curs, promovare examen, validare manuală).
- Soluția trebuie să permită modificarea modelelor de certificate ulterior, fără a afecta certificatele deja emise.
- Soluția trebuie să permită descărcarea certificatelor și validarea acestora (ex. cod unic/QR).
- Soluția trebuie să permită definirea rolurilor și permisiunilor (Admin, Tutor, Student, Super Admin ANS).
- Soluția trebuie să permită adaptarea ulterioară a fluxurilor operaționale în funcție de concluziile analizei detaliate.

4.5.8.3 Cerințe tehnice

Pentru facilitarea și eficientizarea procesului de instruire continuă a utilizatorilor din cadrul instituțiilor beneficiare, Ofertantul va furniza o **platformă de tip Learning Management System (LMS),** care va integra funcționalități de creare, administrare, distribuție și analiză a conținutului educațional digital.

Platforma va dispune de mecanisme tehnice avansate care să permită obținerea unor experiențe de învățare interactive, adaptive și personalizate, fiind utilizată pentru dezvoltarea și livrarea unui conținut educațional atractiv, coerent și ușor de parcurs.

Soluția va integra capabilități complete pentru gestionarea ciclului de viață al conținutului educațional, inclusiv creare (authoring), organizare, publicare, distribuție, evaluare și analiză, precum și funcționalități de colaborare, interacțiune și suport decizional bazate pe inteligență artificială.

Platforma LMS va fi proiectată modular, permițând extinderea funcționalităților în funcție de necesitățile identificate în etapa de analiză și de prioritățile beneficiarului, fără a introduce dependențe de tehnologii incompatibile cu infrastructura Cloudului Guvernamental.

- Soluția trebuie să fie o soluție COTS, matură, licențiată perpetuu, pentru un număr nelimitat de utilizatori.
- Soluția va fi integrată cu DMS și va oferi un sistem complet pentru crearea și gestionarea, cu posibilitatea extinderii funcționalităților prin add-on-uri în funcție de necesități.

CMS / Authoring

- Soluția va include un sistem de definire și gestionare a conținutului (CMS), cu următoarele funcționalități:
  - Crearea, gestionarea și actualizarea conținutului de învățare, utilizând texte, imagini, video, platforme externe, chestionare și teste.
  - Importarea și exportarea lecțiilor în format JSON (JavaScript Object Notation).
  - Exportarea lecțiilor în format SCORM (Sharable Content Object Reference Model).
  - Interfață pentru definirea parametrilor de calibrare a unei lecții.
  - Transformarea, cu ajutorul inteligenței artificiale, a unor fișiere PDF în fluxuri de învățare.

Authoring Tool

- Soluția va include un modul de authoring dedicat pentru crearea, editarea și gestionarea conținutului educațional digital.
  - Editor vizual de tip drag-and-drop pentru crearea materialelor educaționale.
  - Gestionarea structurii cursului prin mecanisme de tip layers, incluzând selectare, blocare (locking), ascundere și reordonare elemente.
  - Crearea de conținut interactiv: drag & drop, hotspot, exerciții de ordonare logică, simulări și exerciții interactive complexe.
  - Organizarea resurselor prin taxonomii, etichete și metadate.

- Gestionarea centralizată a fișierelor media, inclusiv posibilitatea de înlocuire globală a resurselor.
- Administrarea ciclului de viață al conținutului prin workflow-uri (Draft, In Review, Published, Archived, Withdrawn).
- Personalizarea aspectului vizual al cursurilor (Design System).
- Definirea de variabile de proiect (text, numeric, boolean) și implementarea de reguli logice pentru parcursuri dinamice de învățare.
- Suport pentru versionare (version history), restaurare și funcționalități undo/redo.
- Editare colaborativă în timp real, inclusiv mecanisme de locking pentru prevenirea suprascrierii.
- Gestionarea colaborativă a conținutului, cu posibilitatea de adăugare co-autori și control granular al accesului pe proiecte.
- Instrumente integrate pentru accesibilitate (a11y), inclusiv suport pentru alt text și etichete ARIA.

- Soluția va:
  - include acces la o bibliotecă extinsă de resurse multimedia (imagini, video, ilustrații).
  - include minimum 25 de șabloane interactive pentru crearea lecțiilor digitale.
  - permite generarea automatizată de lecții pe baza unor seturi de cuvinte cheie sau prompturi definite de utilizator.
  - permite generarea automată a planurilor de lecție pe baza conținutului creat.
  - permite publicarea și reutilizarea conținutului educațional într-o bibliotecă comună accesibilă utilizatorilor autorizați.
  - permite actualizarea și versionarea conținutului publicat.
  - include ghiduri interactive, tutoriale și materiale de suport pentru utilizatori.

Inteligență Artificială

- Soluția va permite:
  - generarea automată de resurse multimedia (text-to-image, text-to-speech).
  - generarea automată a structurii și conținutului cursurilor (secțiuni, texte, evaluări).
  - generarea automată de întrebări și teste de evaluare aliniate la conținut.
  - asistență AI pentru redactarea, adaptarea, extinderea și optimizarea conținutului educațional.
- Soluția va permite utilizarea unui asistent de învățare bazat pe inteligență artificială, integrat în platformă, care va include:
  - interfață hibridă voce-text în limba română;
  - definirea unei baze de cunoștințe la nivel de lecție;

- interogarea conținutului pe baza întrebărilor cursanților;
- generarea și actualizarea automată a unei hărți de cunoștințe pentru fiecare utilizator;
- evaluarea continuă a nivelului de cunoștințe;
- personalizarea conținutului și a traiectoriilor de învățare;
- integrarea unui asistent virtual contextual în cadrul lecțiilor.

- Soluția va permite administrarea centralizată a motorului AI, inclusiv configurarea furnizorului, gestionarea securizată a cheilor API și definirea politicilor de utilizare.

Analytics și Monitorizare

- Soluția va permite:
  - colectarea și analizarea indicatorilor de engagement ai utilizatorilor.
  - monitorizarea progresului la nivel de curs, modul și lecție.
  - înregistrarea scorurilor, timpului petrecut și istoricului cursurilor parcurse.
  - generarea de rapoarte detaliate privind progresul și performanța utilizatorilor.
  - generarea de statistici la nivel de curs (număr utilizatori, rată de finalizare, implicare).
  - exportul rapoartelor în formate standard (CSV, PDF).
- Soluția va permite:
  - generarea de rapoarte de învățare individuale;
  - monitorizarea în timp real a sesiunilor de training;
  - calcularea metricilor de implicare pentru identificarea utilizatorilor cu implicare redusă;
  - definirea și analiza programelor analitice aferente cursurilor;
  - generarea automată de rapoarte de tip hartă de cunoștințe (knowledge coverage);
- Soluția va genera audit logs detaliate și imuabile pentru toate acțiunile utilizatorilor și administratorilor.
- Soluția va permite monitorizarea evenimentelor de securitate și filtrarea avansată a jurnalelor de activitate.

Tracking și progres

- Soluția va permite monitorizarea progresului la nivel granular (curs, modul, lecție, secțiune, slide).
- Soluția va înregistra automat parcurgerea conținutului și interacțiunile utilizatorilor.
- Soluția va permite reluarea automată a lecțiilor din punctul exact de întrerupere.

Experiență Utilizator și Experiență Curs

- Soluția va include:

- interfață intuitivă și ușor de utilizat.
- dashboard personalizat și calendar de activități.
- gestionarea grupelor de studiu.
- catalog de cursuri cu descrieri detaliate, evaluări și clasificări.
- filtrare și căutare avansată a cursurilor.

- Soluția va include:
  - sistem de notificări în timp real;
  - suport pentru comenzi rapide și command palette;
  - posibilitatea de previzualizare a conținutului;
  - posibilitatea de partajare a conținutului prin link securizat;
  - spațiu personal de tip „My Account”.
- Soluția va include o pagină detaliată a cursului care va afișa descrierea completă, informații despre instructor, număr de utilizatori înscriși și evaluări.
- Soluția va permite afișarea curriculumului complet al cursului, inclusiv lecții gratuite de probă.
- Soluția va include un player de curs dedicat care va permite navigarea între lecții și module, afișarea progresului, marcarea lecțiilor ca finalizate și reluarea automată a lecției.
- Soluția va permite configurarea restricțiilor pentru conținut video.

Evaluare

- Soluția va asigura:
  - Crearea de chestionare complexe (răspuns unic, multiplu, asociere, completare, eseu, upload).
  - Bancă de întrebări reutilizabilă.
  - Configurarea parametrilor de evaluare (punctaj, prag, încercări, temporizator).
  - Feedback detaliat pentru răspunsuri
  - Evaluare automată și manuală.
- Soluția va permite:
  - definirea de bariere logice de parcurgere;
  - utilizarea variabilelor de sesiune în evaluare;
  - clasificarea automată a răspunsurilor în limbaj natural;
  - re-antrenarea clasificatorilor pentru evaluări deschise.

Administrare LMS

- Soluția va asigura:
  - administrarea completă a cursurilor (durată, acces, vizibilitate).

- configurarea accesului (public, privat, protejat).
- organizarea cursurilor pe module și lecții.
- configurarea notificărilor automate.

- Soluția va permite administrarea utilizatorilor printr-un sistem RBAC (Role-Based Access Control), incluzând:
  - definirea rolurilor (administrator, autor, evaluator, utilizator etc.);
  - gestionarea conturilor utilizatorilor;
  - blocarea/deblocarea accesului;
  - asocierea utilizatorilor cu instituții sau grupuri.

Social și Colaborare

- Soluția va asigura:
  - Forum și mesagerie pentru interacțiune.
  - Evaluări și recenzii pentru cursuri.
  - Comunități asociate cursurilor.
  - Comentarii și întrebări la nivel de lecție.
- Soluția va permite:
  - comentarii contextuale pe conținut;
  - thread-uri de discuții;
  - marcarea problemelor ca rezolvate;
  - integrarea feedback-ului în workflow-ul de aprobare.

Monetizare

- Soluția va asigura:
  - coș de cumpărături și înscriere la cursuri.
  - suport pentru metode de plată multiple (ex: paypal, stripe sau echivalent).
  - cupoane și reduceri.
  - configurare acces pe bază de plată și abonamente.
  - configurare flux checkout.
  - generarea de rapoarte financiare detaliate.

Integrare

- Soluția va asigura:
  - integrarea cu servicii externe (email marketing, sisteme externe).
  - integrarea cu un sistem DMS pentru gestionarea documentelor educaționale.

Extensibilitate

- Soluția va asigura:
  - extinderea funcționalităților prin module (add-on-uri).
  - integrarea cu module pentru gamificare, social și abonamente.

Control Livrare Conținut

- Soluția va asigura:
  - livrarea conținutului educațional în mod programat (content drip).
  - configurarea accesului secvențial la lecții în funcție de progres.

Accesibilitate și Mobile

- Soluția va asigura:
  - conformitate cu standardele WCAG 2.1.
  - suport pentru screen reader.
  - navigare completă prin tastatură.
  - opțiuni de contrast și ajustare fonturi.
  - subtitrări și transcrieri pentru conținut multimedia.
- Soluția va asigura:
  - design responsive pentru desktop, tabletă și mobil;
  - suport complet pentru interacțiuni tactile;
  - adaptarea automată a layout-ului pe dispozitive mobile;
  - posibilitatea de testare a vizualizării pe diferite tipuri de dispozitive.

4.5.9 Modul Arhivă

Modulul Arhivă Electronică joacă un rol esențial în eficientizarea proceselor de administrare din cadrul ANS, contribuind la stocarea sigură și accesibilă a documentelor/dosarelor, automatizarea preluării datelor și gestionarea eficientă a informațiilor pe termen lung.

Modulul trebuie să asigure acces rapid și controlat la documente, trasabilitate totală și o interconectare eficientă cu alte module și instituții, contribuind astfel la digitalizarea completă a activităților de administrare și la creșterea transparenței și a eficienței operaționale.

4.5.9.1 Cerințe tehnice

- Soluția trebuie să fie o soluție COTS, matură, licențiată perpetuu, pentru un număr nelimitat de utilizatori.
- Modulul trebuie să asigure stocarea centralizată, sigură și scalabilă a documentelor și dosarelor electronice, contribuind la eliminarea dependenței de infrastructuri locale și la creșterea accesibilității informațiilor.
- Cerințe legale și de conformitate:

- Modulul trebuie să respecte Legea nr. 135/2007 privind arhivarea documentelor în formă electronică și alte acte normative conexe, inclusiv Legea nr. 201/2024 și Ordinul MCID nr. 20717 din 9 mai 2024.
- Modulul trebuie să respecte standardele tehnice aplicabile pentru arhivarea electronică (ISO 14721 – OAIS pentru arhivare digitală pe termen lung, ISO 15489 pentru managementul documentelor).
- Modulul trebuie să asigure conformitatea cu cerințele din standardele ISO/IEC 27001 pentru securitatea informațiilor.
- Modulul trebuie să respecte cerințele Regulamentului (UE) 2016/679 (GDPR), asigurând confidențialitatea, integritatea și disponibilitatea datelor cu caracter personal.

- Securitate și protecția datelor
  - Modulul trebuie să includă măsuri avansate de securitate cibernetică, precum:
    - criptarea datelor stocate și în tranzit;
    - autentificare multifactorială pentru utilizatori;
    - protecție împotriva atacurilor cibernetice.
  - Modulul trebuie să includă mecanisme de verificare a autenticității și integrității documentelor arhivate, în conformitate cu cerințele legale aplicabile.
  - Modulul trebuie să includă mecanisme de backup periodic, care să permită:
    - recuperarea documentelor în caz de avarie;
    - protecția împotriva pierderii accidentale a datelor.
  - Accesul la documente trebuie să fie strict controlat pe bază de roluri și drepturi, astfel încât:
    - doar utilizatorii autorizați să poată vizualiza, modifica sau șterge documente;
    - datele sensibile să fie protejate corespunzător.
- Stocare și retenție
  - Modulul trebuie să permită stocarea documentelor, asigurând:
    - disponibilitate ridicată;
    - scalabilitate în funcție de volum;
    - continuitatea operațională.
  - Modulul trebuie să permită arhivarea documentelor mai vechi de un număr de ani, pragul fiind configurabil și stabilit în cadrul proiectului.
  - Modulul trebuie să asigure păstrarea documentelor pe termen lung, în conformitate cu legislația și normele aplicabile.
  - Modulul trebuie să permită definirea și aplicarea regulilor de retenție, inclusiv eliminarea sau arhivarea finală a documentelor la expirarea perioadei legale.
- Clasificare, indexare și căutare

- Modulul trebuie să asigure o structură de clasificare care să faciliteze accesul rapid, filtrarea și administrarea eficientă a documentelor.
- Modulul trebuie să asigure indexarea automată a documentelor încărcate, pe baza metadatelor relevante, cum ar fi:
  - tip document;
  - nume solicitant;
  - identificatori unici (ex. CNP);
  - dată document
  - alți indecși
- Indexarea trebuie să fie realizată automat la momentul încărcării sau preluării documentelor.
- Modulul trebuie să dispună de funcționalități avansate de căutare, care să permită regăsirea documentelor după:
  - CNP;
  - nume utilizator;
  - tip document;
  - alte criterii multiple combinate.
- Căutarea trebuie să fie rapidă și să susțină activitățile de procesare, verificare și control.

- Procesare documente și OCR
  - Modulul trebuie să includă funcționalități OCR (Optical Character Recognition) pentru:
    - procesarea documentelor scanate;
    - extragerea automată a datelor relevante din documente precum: buletine, certificate de înregistrare, alte informații;
  - Datele extrase trebuie să poată fi utilizate ulterior în fluxurile de lucru ale aplicației, reducând introducerea manuală și riscul de erori.
  - Administratorii trebuie să poată:
    - valida documentele încărcate;
    - asocia documentele cu cereri, dosare sau entități din sistem.
- Audit și trasabilitate
  - Modulul trebuie să păstreze istoricul complet al acțiunilor efectuate asupra documentelor, incluzând:
    - cine a accesat documentul;
    - ce modificări au fost realizate;
    - data și ora operațiunii.

- Toate acțiunile trebuie să fie jurnalizate automat.
- Modulul trebuie să permită generarea de rapoarte de audit privind:
  - activitatea utilizatorilor;
  - accesările și modificările documentelor.

- Interoperabilitate și integrare
  - Modulul trebuie să fie interconectat cu modulul DMS al aplicației, pentru:
    - reutilizarea documentelor;
    - evitarea duplicării informațiilor;
    - susținerea fluxurilor de lucru integrate.
  - Interconectarea trebuie să permită schimbul de date controlat și securizat.
  - Modulul trebuie să permită exportul documentelor și al metadatelor asociate în formate standardizate.
- Digitalizare și arhivă istorică
  - Modulul trebuie să permită digitalizarea documentelor și integrarea acestora în arhivă.
  - Documentele scanate trebuie:
    - transformate în format electronic;
    - indexate;
    - integrate complet în modulul Arhivă Electronică.
  - Arhiva digitalizată trebuie să fie accesibilă printr-un modul special dedicat arhivei istorice, distinct de documentele curente, dar integrat funcțional.
- Stocare centralizată
  - Stocare Cloud: Pe perioada prestării serviciilor de arhivare, toate documentele vor fi stocate într-un sistem cloud pus la dispoziție de Ofertant, . Acest lucru contribuie la accesibilitate, siguranță și scalabilitate. Ofertantul va prezenta în Ofertă modalitatea de transfer a arhivei în Cloudul Guvernamental, unde va fi operaționalizat sistemul informatic.
  - Documentele vor fi organizate pe categorii specifice, cum ar fi documentele de identitate (buletine), CIS-uri. Aceste categorii vor facilita accesul rapid și gestionarea eficientă a informațiilor.

Toate cerințele legate de organizarea documentelor, scanarea și digitalizarea arhivei, clasificarea pe categorii, regulile de retenție și modul de acces vor fi detaliate și validate în etapa de analiză a proiectului.

În această fază se vor stabili specificațiile exacte pentru fiecare funcționalitate, astfel încât dezvoltarea și configurarea soluției să se realizeze conform nevoilor reale ale ANS.

4.5.9.2 Cerințe funcționale

- Modulul trebuie să permită gestionarea completă a ciclului de viață al documentelor, de la creare și încărcare până la arhivare și eliminare, în conformitate cu legislația aplicabilă.
- Modulul trebuie să respecte cerințele Arhivelor Naționale privind organizarea, păstrarea și gestionarea documentelor electronice.
- Gestionare documente
  - Modulul trebuie să permită încărcarea documentelor de către utilizatori și asocierea acestora cu cereri, dosare sau entități existente.
  - Administratorii trebuie să poată valida documentele încărcate și să le asocieze corespunzător în sistem.
  - Modulul trebuie să permită gestionarea documentelor semnate electronic, utilizând semnături conforme cu standardele legale.
- Acces și utilizare documente
  - Modulul trebuie să permită regăsirea, vizualizarea și descărcarea documentelor de către utilizatorii autorizați.
  - Modulul trebuie să permită accesul diferențiat la documente, în funcție de rolurile utilizatorilor.
- Căutare, filtrare și organizare
  - Modulul trebuie să permită căutarea documentelor pe baza metadatelor și a unor criterii multiple.
  - Modulul trebuie să permită filtrarea și sortarea documentelor în funcție de metadate relevante.
  - Modulul trebuie să permită organizarea documentelor pe categorii predefinite și configurabile, precum:
    - documente de identitate (CI, pașapoarte);
    - CIS-uri;
    - alte tipuri de documente relevante activităților ANS.
- Interacțiune și feedback utilizator
  - Modulul trebuie să furnizeze mesaje de confirmare pentru operațiunile efectuate asupra documentelor (ex. încărcare, modificare, ștergere).
  - Modulul trebuie să semnaleze erorile și să ofere feedback utilizatorilor în cazul operațiunilor nereușite.
- Reguli de retenție
  - Modulul trebuie să permită aplicarea regulilor de retenție configurate, inclusiv gestionarea documentelor în funcție de durata de păstrare stabilită.
  - Regulile de retenție vor fi stabilite și configurate în cadrul proiectului.
- Raportare și monitorizare

- Modulul trebuie să permită vizualizarea informațiilor relevante privind documentele și activitatea utilizatorilor.
- Modulul trebuie să contribuie la monitorizarea utilizării sistemului și optimizarea proceselor administrative.

4.5.9.3 Cerințe generale și servicii asociate

- Prestatorul trebuie să asigure implementarea soluției conform cerințelor beneficiarului.
- Prestatorul trebuie să asigure suport tehnic disponibil în regim 8/5.
- Soluția trebuie să beneficieze de mentenanță preventivă și corectivă pe perioada implementării proiectului.
- Soluția trebuie să fie actualizată periodic pentru a asigura conformitatea cu cerințele legale și evoluțiile tehnologice.
- Modulul trebuie să permită migrarea datelor din sisteme existente fără pierderi de informații.
- Soluția trebuie să includă planuri de recuperare în caz de dezastru (Disaster Recovery), pentru asigurarea continuității operaționale.
- Prestatorul trebuie să asigure instruirea utilizatorilor și furnizarea documentației complete.
- Prestatorul trebuie să ofere un cost transparent și detaliat pentru fiecare componentă a soluției și serviciilor asociate.
- Modulul trebuie să permită generarea de rapoarte periodice privind activitatea arhivei și starea documentelor.

4.5.9.4 Servicii de arhivare

Proiectul vizează scanarea unei părți din arhiva fizică existentă la sediul ANS (Str. Vasile Conta nr. 16, București). Din volumul total de 2.274 metri liniari depozitați în sediu, în cadrul prezentului proiect se vor scana 500 metri liniari, echivalentul a peste 9.850 de biblioraftur, însumând aproximativ 2,5 milioane de pagini (estimare medie, calculată pe baza unui volum mediu de cca. 250 pagini/biblioraft).

Serviciile de arhivare fizică, transport, depozitare temporară și digitizare aferente Modulului Arhivă au caracter strict accesoriu față de obiectul principal al contractului – dezvoltarea platformei informatice integrate. Aceste servicii sunt necesare exclusiv pentru popularea inițială, testarea și validarea funcționalităților modulului Arhivă (căutare, indexare, regăsire, structură metadate). Prestarea lor nu reprezintă cerință de calificare, ci cerință tehnică aferentă implementării modulului, iar operatorii economici pot îndeplini aceste activități direct sau prin subcontractare, conform legislației aplicabile.

Tabel 3 - Estimare Distribuție Formate

Format Document	Proporție Estimată	Număr Aproximativ Pagini

A4 (standard)	90%	**2.250.000**
A3/Altele (A2-A0)	10%	**250.000**

Documentele sunt în stare bună, organizate în dosare, necesitând operațiuni standard de pregătire pentru scanare (debroșare) și refacerea ulterioară a dosarelor.

Documentele trebuie scanate și transformate în format electronic, pentru a putea fi integrate în noua soluție informatică. În acest sens arhiva fizică va fi disponibilă printr-un modul special din cadrul arhivei.

Ofertantul va prezenta în Ofertă modalitatea de transfer a arhivei în Cloudul Guvernamental, unde va fi operaționalizat sistemul informatic.

Cadrul legal

În România, arhivarea documentelor în format electronic este reglementată de Legea nr. 135/2007, intitulată Legea privind arhivarea documentelor în formă electronică. Această lege stabilește cadrul juridic pentru crearea, conservarea, consultarea și utilizarea documentelor electronice arhivate.

În anul 2024, Legea nr. 201/2024 a adus completări și modificări semnificative Legii Arhivelor Naționale nr. 16/1996 și Legii nr. 135/2007, adaptând legislația la evoluțiile tehnologice și la necesitatea asigurării integrității și autenticității documentelor electronice.

Ordinul nr. 20717 din 9 mai 2024, emis de Ministerul Cercetării, Inovării și Digitalizării, aprobă Normele tehnice privind procedura de acreditare a administratorilor de arhivă electronică și procedura de avizare a sistemelor electronice de arhivare. Acest ordin abrogă anteriorul Ordin nr. 493/2009 și stabilește cadrul legal actualizat pentru arhivarea electronică a documentelor în România.

4.5.9.4.1 Cerințe privind atestarea

Prestatorul trebuie să îndeplinească condițiile legale pentru realizarea serviciilor, respectiv trebuie să dețină autorizările impuse de lege pentru serviciile prestate.

Prestatorul trebuie să fie **notificat** ca administrator de arhivă electronică la autoritatea de reglementare și supraveghere specializată și să utilizeze **sisteme de arhivare electronică avizate** conform prevederilor Legii nr. 135/2007 și ale Ordinului MCID nr. 20717/2024.

Ofertanții vor prezenta autorizările deținute pentru prestarea tuturor serviciilor de arhivare (păstrare si conservare, prelucrare arhivistică, legătorie, utilizarea documentelor deținute) respectiv:

- Autorizații de funcționare valabile, emise de către Arhivele Naționale (Serviciul/Biroul Județean competent) și de către Inspectoratul General pentru Situații de Urgență (prin unitățile subordonate - ISU), pentru locația/spațiul de depozitare unde se vor presta serviciile. Documentele trebuie să ateste conformitatea spațiului pentru activități de păstrare și conservare arhivistică.

- **Acreditare valabilă** pentru prestarea serviciilor de arhivare electronică, emisă în conformitate cu **Legea nr. 135/2007** și cu normele tehnice aprobate prin **Ordinul MCID nr. 20717/2024** (care abrogă Ordinul 493/2009).

Ofertantul trebuie să facă dovada deținerii mijloacelor de transport (autoturisme/autovehicule) necesare pentru relocarea arhivei în condiții de siguranță și în termenul solicitat, iar în cazul în care acestea au o masă maximă autorizată mai mare de 2,5 tone, trebuie să dețină certificat de competență profesională pentru manager de transport și licență de transport rutier valabilă, eliberate de Autoritatea Rutieră Română.

4.5.9.4.2 Cerințe privind serviciile solicitate

Pe durata contratului Prestatorul va asigura îndeplinirea următoarelor activități:

1. Preluarea documentelor și transportul la locația prestatorului;
2. Gruparea si ordonarea documentelor;
3. Constituirea unităților arhivistice;
4. Inventarierea unităților arhivistice;
5. Digitizarea (scanarea) documentelor, care cuprinde: pregătirea documentelor pentru scanare; digitizarea (scanarea) documentelor existente în arhiva fizică;
6. Indexarea (date structurate, maxim 5 indecși/unitate arhivistică) - indexarea unităților arhivistice cu maxim 5 indecși/unitate arhivistică; indexarea fișierelor rezultate in urma scanării într-o bază de date;
7. Indexarea (date nestructurate – full text search - OCR) indexarea tip full-text search a documentelor scanate;

4.5.9.4.2.1 Preluarea documentelor și transportul la locația prestatorului

Documentele se vor preda după semnarea contractului aferent acestei proceduri în baza proceselor verbale de predare-primire, care vor fi semnate de către reprezentanții ambelor părți.

Documentele vor fi preluate din depozitele actuale in mod organizat

Mijloacele de transport utilizate pentru transportul documentelor trebuie să fie carosate pentru evitarea deteriorării acestora în timpul transportului.

Prestatorul va asigura personalul necesar manipulării documentelor ce vor fi preluate de la locațiile indicate anterior.

Prestatorul are obligația transportului cutiilor în condiții de siguranță pentru a evita deteriorarea acestora. Pe fiecare cutie introdusă în depozit, operatorul economic declarat câștigător are obligația de a asigura un cod astfel încât cutia să fie identificată unic în arhiva acestuia.

4.5.9.4.2.2 Gruparea si ordonarea documentelor

Documentele vor fi grupate pe structurile organizatorice și în cadrul acestora vor fi ordonate cronologic, pe probleme și termene de păstrare conform criteriilor de ordonare stabilite de comun acord cu reprezentantul beneficiarului, în baza prevederilor legale în vigoare.

4.5.9.4.2.3 Constituirea unităților arhivistice (dosarelor)

Documentele preluate vor fi ordonate pe structurile organizatorice ale autorității contractante, cronologic, pe probleme și termene de păstrare. Anterior constituirii dosarelor se elimină tot ce poate deteriora suportul documentelor (ace, cleme, agrafe, etc.), precum și orice file nescrise (excepție paginile albe relevante din punct de vedere arhivistic), dublete, ciorne, etc.

4.5.9.4.2.4 Legarea unităților arhivistice

Documentele ordonate se vor introduce în coperți de carton fiind legate în așa fel încât să se asigure citirea completă a textului, datelor și rezoluțiilor, fiind astfel constituite unitățile arhivistice (dosarele). Operatorul economic va asigura copertile de carton și celelalte furnituri necesare legării documentelor, precum și înscrierea pe copertă a datelor de identificare ale dosarului, respectiv:

- denumirea instituției,
- denumirea compartimentului creator,
- indicativul din nomenclator,
- numărul dosarului și anul,
- conținutul pe scurt al dosarului,
- numărul volumului (daca este cazul),
- datele extreme,
- termenul de păstrare.

Un dosar nu va avea un număr mai mare de 250 file. În cazul depășirii acestui număr de file se vor constitui mai multe volume ale aceluiași dosar. Dosarele legate vor fi introduse în cutii de arhivă furnizate de prestator. Atât pe unitățile arhivistice cât și pe cutii se vor aplica coduri de bare pentru o mai bună identificare a documentului.

4.5.9.4.2.5 Inventarierea unităților arhivistice

Inventarele vor cuprinde toate dosarele cu aceleași termene de păstrare create în cursul unui an de către un compartiment/departament. În cazul dosarelor formate din mai multe volume, în inventar fiecărui volum îi va fi atribuit un număr curent distinct.

Dosarele care cuprind acte din mai mulți ani vor fi inventariate la anul de început, menționându-se în inventar datele extreme.

La rubrica „Conținutul pe scurt al dosarului” vor fi precizate genurile de documente pe care le conține respectivul dosar și acțiunea sau problema/problemele la care se refera. Emitentul și destinatarul vor fi trecuți în inventar numai dacă sunt alții decât creatorul fondului.

La sfârșitul inventarului se va menționa: „Prezentul inventar format din ____ file conține ____ dosare, registre”, urmate de data întocmirii și de numele și semnătura persoanei care a întocmit inventarul.

Predarea inventarelor se va face pe baza de proces verbal de predare-primire și vor fi predate inventarele pe suport de hârtie (1 exemplar original) și pe un suport de memorie externa.

4.5.9.4.2.6 Digitizarea (scanarea) documentelor

Operațiunile de digitizare si indexare a documentelor din arhiva se vor realiza cu respectarea dispozițiilor Legii Arhivelor Naționale nr. 16/1996, cu modificările și completările ulterioare, a

reglementărilor în vigoare privind conservarea, accesul și protecția informației cu caracter public sau privat, a legii nr. 135/2007 privind arhivarea documentelor in forma electronică și a Ordinului nr. 20717 din 9 mai 2024, emis de Ministerul Cercetării, Inovării și Digitalizării, care aprobă Normele tehnice privind procedura de acreditare a administratorilor de arhivă electronică și procedura de avizare a sistemelor electronice de arhivare.

Serviciile de scanare se vor desfășura la sediul Prestatorului, în spatii special amenajate cu sisteme de monitorizare, protecție și alarmare la efracție și incendii, cu personalul specializat al prestatorului, cu echipamentele specializate a acestuia, automat sau manual, în funcție de starea fizică și formatul documentelor, astfel încât sa se respecte securitatea și integritatea documentelor.

Anterior scanării, documentele vor fi supuse unor operațiuni de pregătire constând în:

- Îndepărtarea capselor (dacă este necesar)
- Îndreptarea colțurilor (dacă este necesar)
- Lipirea paginilor rupte (pentru paginile scanate ADF)

În timpul procesului de scanare, Prestatorul va asigura integritatea și securitatea fizică totală a documentelor, fără a distruge documentele de hârtie.

Documentele se vor scana alb negru sau color, fata-verso, după caz, la o rezoluție de min. 300 dpi în cazul formatelor până la A3, respectiv minim 200 dpi pentru formatele mai mari. Pentru fiecare unitate arhivistică în parte, se va crea un document digital în format pdf/pdf searchable multipage.

Criteriul de calitate va fi lizibilitatea, urmărindu-se ca imaginile rezultate să aibă cea mai bună lizibilitate indiferent de starea fizică a documentelor.

Astfel, fișierele rezultate:

- nu vor avea pagini albe rezultate din erori de scanare, se vor păstra doar paginile albe relevante din punct de vedere arhivistic;
- vor avea fundalul paginii (background) eliminat;
- imaginile rezultate vor fi orientate astfel încât să poată fi citite fără rotire;
- imaginile cu grad mare de inclinare vor fi îndreptate;
- pe cât posibil vor fi eliminate impuritățile;
- dimensiunea maximă a unei hărți/planșe format A0 va fi de 3 MB la o rezoluție de minim 200 DPI color.
- numărul de pagini pentru documentele mai mari de formatul A3 vor fi echivalate cu numărul de pagini format A4 corespondent. (exemplu A0 =16 A4)

Documentele vor fi scanate utilizând ultima generație de scannere. Soluția de scanare folosită trebuie să acopere toate tipurile de scanare, pentru toate tipurile de documente:

- scanare color automată (tip ADF) și color manuală utilizând unitate flatbed format A3 sau A4, acolo unde este cazul;
- scanare color manuală cu camera foto fără contact cu originalul pentru documente deteriorate sau fragile.

Selectarea scanerelor va depinde de calitatea fizică și dimensiunea documentelor în format de hârtie. Numărul scanerelor va fi stabilit de operatorul economic luând în considerație volumul care trebuie procesat în unitatea de timp și capacitatea de producție, pe baza experienței anterioare a operatorului economic. Verificarea echipamentelor de scanare se realizează exclusiv în etapa de execuție a contractului, ca parte a procesului de recepție a serviciilor de digitizare, și nu în etapa de evaluare a ofertelor. Această verificare nu reprezintă criteriu de evaluare și nu influențează calificarea sau punctajul ofertelor.

Ofertantul va prezenta în propunerea tehnică specificațiile tehnice ale echipamentelor de scanare propuse (producător, model, rezoluție optică minimă 300 dpi color / 400 dpi alb-negru, viteză minimă de scanare, format maxim document acceptat, compatibilitate software OCR).

Pe parcursul executării contractului, autoritatea contractantă își rezervă dreptul de a verifica la sediul prestatorului conformitatea echipamentelor utilizate față de cele declarate în ofertă. Verificarea are ca obiect exclusiv confirmarea conformității și nu poate conduce la solicitarea de echipamente suplimentare sau diferite față de cele ofertate.

Criteriile de acceptare sunt: respectarea rezoluției minime, a vitezei minime de scanare și a formatului maxim acceptat. Neconformitatea constatată constituie abatere contractuală și se sancționează conform clauzelor contractuale privind penalitățile.

Supervizorii procesului de scanare sau specialiștii în asigurarea calității vor realiza cel puțin o evaluare vizuală a calității fiecărui document scanat, înainte de scrierea imaginii digitale pe DVD/HDD sau orice alt suport stabilit de comun acord cu autoritatea contractantă. Serviciul de scanare va fi realizat cu personal calificat și cu experiență de lucru practică în proiecte similare. O descriere a calificărilor și experienței va fi inclusă de către Operatorul economic în cadrul ofertei.

4.5.9.4.2.7 Indexarea (date structurate, maxim 5 indecși)

În procesul de preluare a datelor, trebuie avute în vedere următoarele dificultăți de care trebuie să se țină cont în cadrul ofertei:

- datele trebuie capturate (transferate) corect si livrate, fără a modifica sensul lor original;
- personalul Prestatorului ce va fi implicat in implementarea contractului trebuie să învețe structura unui dosar si al actelor din el și semnificația informațiilor, în funcție de poziționarea acesteia (secțiunea din care fac parte, etc.) pentru a putea interpreta corect informațiile în vederea preluării acestora;
- sunt dese situațiile când scrisul este greu descifrabil.

Datele vor fi preluate folosind sediul, resursele umane, echipamentele hardware și instrumentele software de care dispune operatorul economic. Prestatorul va descrie toate aceste dotări de care dispune pentru prestarea serviciilor utilizate precum și locația unde se va desfășura această activitate.

Formatul fișierelor în care datele structurate (metadatele) vor fi exportate este **XML**. Fișierul XML va asigura legătura logică între indecșii extrași și fișierul digital corespondent (**PDF/PDF Searchable**), prin includerea unei referințe unice (nume fișier/cale relativă) pentru fiecare unitate arhivistică.

Structura schemei XML (XSD), nomenclatura fișierelor și regulile de denumire (bazate pe indecșii stabiliți) vor fi detaliate în etapa de analiză și aprobate de beneficiar înainte de începerea fluxului de producție, pentru a asigura compatibilitatea cu mecanismul de import al soluției informatice."

Orice neconcordanță identificată în procesul de preluare a datelor de pe documentele sursă cum ar fi: identificare greșită a documentelor, informații lipsă în documentul sursă, etc. vor fi raportate într-un format structurat în cadrul unui Raport Tehnic de Neconformități, care urmează a fi luat la cunoștință și aprobat de către Echipa de proiect din cadrul fiecăreia dintre cele trei instituții membre ale Asocierii de autorități contractante. Formatul și structura acestui raport vor fi detaliate în cadrul ofertei, acesta putând fi ajustat (cu acordul beneficiarului) în cadrul etapei de analiză ce va preceda elaborarea Raportului Inițial.

Următoarele tipuri de probleme vor fi incluse în raportul privind neconcordanțelor, care urmează să fie elaborat la finalizarea serviciilor de conversie:

- Informații lipsă în pagină - de la scanare;
- Indecși înregistrați aproximativ de către operatorii prestatorului de servicii de conversie, din cauza caracterului indescifrabil;
- Indecși obligatorii lipsă din documentul scanat. Pentru identificarea rapida a documentelor, filtrare-căutare in arhiva digitala, prestatorul va crea o baza de date cu informațiile specifice pentru fiecare dosar in parte, conform nomenclatorului dosarelor confirmat de Arhivele Naționale, pus la dispoziție de către beneficiar.

Fiecare set de indecși trebuie să conțină un index unic (cod QR/cod de bare) pentru corelare cu dosarul fizic și copia digitală a acestuia și un set de până la 5 indecși specifici categoriei de documente, necesari pentru filtrare – căutare (ex: Direcție, Serviciu, Birou, Anul, Conținutul pe scurt al dosarului (opis)) – aceștia din urmă urmând a fi stabiliți de comun acord cu Beneficiarul în cadrul activităților de analiză, în funcție de categoriile unităților arhivistice și orice alți factori considerați esențiali.

Datele obținute în procesul de conversie vor fi pregătite pentru importul în cadrul arhivei digitale.

4.5.9.4.2.8 Indexarea (date nestructurate – full text search)

Prestatorul va stabili împreună cu beneficiarul care sunt documentele care necesită scanarea și includerea în arhiva electronică în format pdf, cu indexare tip full text search (tip OCR), care să permită căutarea în cadrul documentului PDF afișat cu posibilitatea de evidențiere a cuvintelor găsite.

4.5.9.4.2.9 Păstrarea documentelor pe durata prestării serviciilor

Păstrarea documentelor se va realiza cu respectarea prevederilor în vigoare.

Documentele de arhivă se vor păstra în depozite construite special sau în încăperi amenajate în acest scop, avizate de către Arhivele Naționale, cu asigurarea condițiilor necesare pentru păstrarea corespunzătoare a documentelor și pentru protecția lor față de acțiunea agenților de deteriorare: praf, lumina solară, solicitări la uzura mecanică, variații de temperatură și umiditate, temperaturi excesive, surse de infecție sau întreținere a agenților biologici, pericol de foc, inundații sau infiltrării de apă.

Caracteristici minime ale depozitului de arhivă solicitat:

- Depozitul trebuie să respecte condițiile legale prevăzute de Legea Arhivelor Naționale nr. 16/1996*, cu modificările ulterioare,* și normele tehnice *aplicabile privind condițiile de păstrare a documentelor. Prestatorii vor garanta disponibilitatea documentelor după cum urmează*:
    - transmiterea în format digital scanat a documentului solicitat în maximum 4 ore lucrătoare de la solicitare, în regim de urgență;
    - punerea la dispoziție/livrarea documentului original la sediul ANS în maximum 24 de ore lucrătoare pentru urgențe și maximum 5 zile lucrătoare în regim normal. Ofertantul va prezenta în propunerea tehnică modalitatea concretă de asigurare a acestor termene (localizare spațiu, mijloace de transport, resurse umane alocate etc.).
- Să fie dotat cu rafturi, rastele, dulapuri și alte mijloace de depozitare specifice, de preferință din metal acoperit cu vopsele stabile, anticorozive și fără emanații;
- Elementele de păstrare a arhivei (rafturi, dulapuri, etc) să fie compatibile cu dimensiunile materialului suport al documentelor (hârtie, film, etc), ale materialelor de protecție ale acestora (cutii, containere, etc), ale spațiului aferent, asigurându-se accesul lejer la documente (materialul depozitat) și posibilitatea unei evacuări rapide în caz de necesitate;
- Amplasarea rafturilor să fie (pe cat posibil) perpendicular pe sursa de lumina naturala, cu protecție la aceasta cu storuri (transparente) iar iluminatul artificial sa urmărească culoarul dintre rafturi;
- Să nu fie amplasat în construcții provizorii.
- Să nu fie amplasat în poduri, mansarde, subsoluri tehnice sau în încăperi inundabile.
- Să nu fie amplasat, deasupra, dedesubtul sau în vecinătatea magaziilor de substanțe explozibile, inflamabile, corozive, de coloranți, a încăperilor în care se lucrează cu foc deschis, a ghenelor de reziduuri menajere.
- Sistemele de depozitare să fie asigurate pentru a preveni riscurile de accidentare sau distrugere a documentelor datorită prăbușirii acestora;
- Distanțele între pereți și rafturi, ca și intre rafturi să fie în conformitate cu prevederile Instrucțiunilor privind activitatea de arhiva aprobate de conducerea Arhivelor Naționale, respective sa asigure un spațiu liber de 0,7 – 0,8 m lățime și cu coridoare centrale de 1,5 – 2,0 m lățime, pe lungimea sau pe lățimea depozitului, pentru manevrarea documentelor;
- Depozitul de arhivă să fie dotat cu scări de arhivă, cărucioare de transport dosare, mese și scaune;
- Depozitul de arhivă, conținând documente scrise, trebuie să asigure un microclimat caracterizat prin temperaturi cuprinse între 15 – 24° C și umiditate relativă de 50 – 60 %;
- Pentru măsurarea și urmărirea parametrilor de microclimat, depozitul trebuie să fie dotat cu aparate de control (termometre, higrometre și alte asemenea), iar citirile vor fi consemnate într-un caiet de depozit;
- Depozitul trebuie să se poată aerisi natural. Această aerisire se va efectua atunci când umiditatea atmosferică se încadrează în limitele specificate, fără a se depăși 1 – 3

schimburi de aer/oră, iar viteza curentului de aer se va înscrie în limitele de 0,1 – 0,3 metri/secundă;

- Reparațiile interioare, zugrăvelile si lucrările de întreținere a depozitului de arhiva se fac ori de cate ori este nevoie, asigurându-se in permanenta igiena încăperilor si funcționarea normala a instalațiilor electrice si sanitare;
- Pentru prevenirea incendiilor se interzice folosirea focului deschis, a radiatoarelor, reșourilor, fumatului in incinta depozitului, precum si utilizarea comutatoarelor, întrerupătoarelor sau altor instalații electrice defecte sau care prezinta riscuri de incendii;
- În depozit se va asigura curățenia și ordinea interioară, pentru a se evita insalubrizarea acestuia sau instalarea de focare biologice (rozătoare, insecte, mucegai);
- Înlăturarea agenților dăunători se face prin desprăfuire, curățire mecanică, dezinsecție și deratizare. Desprăfuirea documentelor se face cu perii moi, iar absorbția prafului rezultat, cu aspiratoare electrice. Dezinfecția, dezinsecția și deratizarea depozitului de arhivă se fac ori de cate ori este nevoie și cel puțin o dată la 5 ani;
- Depozitul de arhivă, ca și terenul învecinat construcției de arhivă vor fi menținute în ordine și curățenie, cu păstrarea liberă a căilor de acces, a locurilor din apropierea gurilor de apă și a instalațiilor de stingere a incendiilor;
- Depozitul și celelalte încăperi din vecinătatea acestuia vor fi prevăzute cu stingătoare portabile, cu încărcătură de dioxid de carbon și praf sau gaze inerte, asigurându-se toate celelalte condiții necesare stingerii incendiilor, prevăzute în normele de stat în vigoare;
- Depozitul va fi prevăzut cu mijloace de alarmare și semnalizare anti incendiu, iar după caz și cu instalații de stingere automată a incendiilor.
- Depozitul de arhivă va fi dotat cu instalații automate de stingere a incendiilor care nu afectează materialul arhivistic și sunt dimensionate corespunzător. Sunt obligatorii instalațiile de stingere automata a incendiilor cu gaze inerte pentru toate spatiile de depozitare.
- Deținătorul depozitului este obligat să păstreze în stare perfectă de funcționare utilajele și materialele de prevenire și stingere a incendiilor, conform normelor de dotare și să le controleze (și să certifice) periodic existența și starea de funcționare a acestora, conform prevederilor legale;
- Ferestrele și celelalte locuri de acces (uși) vor fi prevăzute cu gratii care să prevină intrarea prin efracție în depozit;
- Depozitul trebuie să aibă asigurata paza permanenta care să asigure inviolabilitatea depozitului, iar și personalul de pază să știe sa întrebuințeze mijloacele și instalațiile de alarmare și de intervenție.
- Depozitul să aibă acreditările de funcționare de la Serviciul Arhivelor Naționale si de la ISU;

Ofertanții trebuie să facă dovada că au capacitatea prestării serviciilor de transport și de depozitare a arhivei. În acest sens, ofertanții vor descrie în cadrul propunerii tehnice locațiile în care vor fi

depozitate documentele pe parcursul desfășurării acordului-cadru, precum și forma de deținere a acestora, prezentând documente în acest sens, inclusiv autorizațiile legale ale respectivelor spații.

De asemenea, se vor detalia echipamentele necesare depozitării, transportului și manipulării cutiilor cu documente cu prezentarea documentelor care atestă forma de deținere a acestora (chirie, proprietate, etc.).

Documentele constituite se introduc în cutii de carton, în raport de natura și dimensiunea lor, puse la dispoziție de prestatorul de servicii de depozitare, pe compartimente și în cadrul compartimentului pe ani și termene de păstrare și se depozitează pe rafturi. Cutiile de arhivare vor fi identificate printr-un număr unic pe exteriorul cutiei.

Fondul arhivistic va fi așezat conform Legii 16/1996, republicată, unitar, cronologic, pe servicii și termene de păstrare.

Pe durata păstrării documentelor în depozitele prestatorului, se va asigura:

- verificarea și monitorizarea condițiilor optime de temperatură, umiditate și luminozitate pentru conservarea documentelor;
- verificarea și monitorizarea funcționarii echipamentelor tehnice de asigurare a climatului în spațiul destinat gestionarii documentelor;
- verificarea integrității mijloacelor speciale de protecție a documentelor (cutii);
- monitorizarea planului de masuri de întreținere a documentelor de arhivă (desprăfuire, dezinsecție și dezinfecție periodică).

4.5.10 Modul Administrativ

Modulul administrativ pentru aplicația web a ANS presupune un set de funcționalități esențiale pentru gestionarea eficientă a activităților interne și pentru facilitarea administrării documentelor, utilizatorilor și proceselor specifice.

Cerințe:

1. **Gestionarea Utilizatorilor și Rolurilor**

- Modulul trebuie să permită afișarea unei liste centralizate de administratori, sub formă de tabel, care să includă cel puțin numele complet, username-ul, rolul/rolurile asociate, adresa de email, statusul de verificare al emailului și data verificării.
- Modulul trebuie să permită sortarea ascendentă și descendentă a listei de administratori după fiecare coloană afișată în tabel.
- Trebuie să existe posibilitatea de a filtra lista administratorilor prin intermediul unui câmp de căutare globală care să permită identificarea acestora după nume, username sau email.
- Modulul trebuie să permită configurarea numărului de înregistrări afișate pe pagină, cu actualizarea dinamică a tabelului.
- Trebuie să existe funcționalitatea de a exporta datele afișate din tabelul de administratori în formate multiple (Copy, Excel, CSV, PDF), păstrând structura coloanelor vizibile.
- Trebuie să existe funcționalitatea de a genera o versiune tipărită a listei de administratori.

- Modulul trebuie să permită inițierea fluxului de adăugare a unui administrator nou printr-un buton dedicat.
- Modulul trebuie să permită accesarea acțiunilor de vizualizare, editare și ștergere pentru fiecare administrator, direct din lista de administratori.
- Modulul trebuie să permită vizualizarea detaliilor de cont ale unui administrator într-o pagina dedicata, distinct de lista de administratori.
- Trebuie să existe funcționalitatea de a afișa informațiile de identificare ale administratorului, incluzând numele complet, username-ul și adresa de email.
- Modulul trebuie să permită afișarea statusului de verificare al emailului, împreună cu data la care acesta a fost verificat.
- Modulul trebuie să permită afișarea rolurilor atribuite administratorului sub formă de elemente vizuale distincte.
- Trebuie să existe posibilitatea de a elimina un rol atribuit unui administrator direct din ecranul de detalii.
- Modulul trebuie să permită configurarea permisiunilor individuale ale unui administrator, organizate pe module funcționale ale aplicației.
- Trebuie să existe posibilitatea de a activa sau dezactiva accesul unui administrator la fiecare modul funcțional
- Modulul trebuie să evidențieze permisiunile care sunt moștenite din rolurile atribuite administratorului, printr-un indicator vizual distinct.
- Trebuie să existe posibilitatea de a activa sau dezactiva permisiuni specifice din cadrul fiecărui modul, precum accesul la meniu sau accesul deplin la funcționalități critice.
- Modulul trebuie să permită activarea sau dezactivarea simultană a tuturor permisiunilor asociate unui modul.
- Trebuie să existe funcționalitatea de extindere și restrângere a listelor de permisiuni pentru fiecare modul, pentru o navigare mai ușoară.
- Modulul trebuie să permită modificarea informațiilor de bază ale unui utilizator, inclusiv numele complet, username-ul și adresa de email.
- Trebuie să existe validări pentru câmpurile obligatorii, astfel încât salvarea datelor să nu fie permisă în lipsa acestora.
- Modulul trebuie să permită configurarea a minim 3 metode de autentificare în doi pași pentru un utilizatori(Google Authenticator, Email, SMS).
- Modulul trebuie să permită inițierea procesului de schimbare a parolei unui utilizator.
- Trebuie să existe posibilitatea de a activa contul unui utilizator din ecranul din interfața daca acesta nu își mai regăsește email-ul de activare.
- Modulul trebuie să permită afișarea unei liste centralizate de roluri, care să includă denumirea rolului și numărul de utilizatori asociați fiecăruia.

- Trebuie să existe posibilitatea de a sorta lista rolurilor după denumire sau numărul de utilizatori.
- Modulul trebuie să permită exportarea listei de roluri în multiple formate (Copy, Excel, CSV, PDF).
- Trebuie să existe funcționalitatea de a tipări lista rolurilor.
- Trebuie să existe posibilitatea de a naviga între paginile listei de roluri.
- Modulul trebuie să permită definirea sau modificarea denumirii unui rol, cu validarea obligatorie a acestui câmp.
- Modulul trebuie să permită configurarea permisiunilor asociate unui rol, organizate pe module funcționale.
- Trebuie să existe posibilitatea de a acorda sau revoca accesul la modulele principale ale aplicației.
- Modulul trebuie să permită activarea granulară a permisiunilor specifice fiecărui modul.

2. Managementul Federațiilor, Cluburilor, Sportivilor și Antrenorilor

- Modulul trebuie să permită administrarea centralizată a tuturor tipurilor de entități definite în sistem, incluzând federații, cluburi, sportivi, antrenori, competiții și rezultate.
- Trebuie să existe posibilitatea de a vizualiza lista entităților pentru fiecare tip, într-un format tabelar, cu informații relevante de identificare.
- Modulul trebuie să permită afișarea statusului curent al fiecărei entități, astfel încât administratorii să poată identifica rapid starea acesteia.
- Trebuie să existe funcționalitatea de a filtra și căuta entitățile în funcție de tip, status sau criterii de identificare.
- Modulul trebuie să permită accesarea unui ecran de detalii pentru fiecare entitate, unde să fie afișate informațiile complete asociate acesteia.
- Trebuie să existe posibilitatea de a efectua operațiuni specifice asupra entităților, în funcție de tipul acestora și de statusul curent.
- Modulul trebuie să permită inițierea acțiunilor de creare, modificare, activare, dezactivare sau arhivare a entităților, conform procedurilor definite.
- Trebuie să existe posibilitatea de a urmări modificările efectuate asupra unei entități, inclusiv schimbările de status.
- Modulul trebuie să asigure că operațiunile disponibile asupra unei entități sunt condiționate de drepturile utilizatorului și de rolurile asociate acestuia.
- Modulul trebuie să permită monitorizarea în timp real a statusului entităților administrate.
- Trebuie să existe posibilitatea de a identifica entitățile aflate în stări critice, nefinalizate sau care necesită intervenție.
- Modulul trebuie să asigure respectarea procedurilor stabilite pentru fiecare tip de entitate.

- Trebuie să existe posibilitatea de a vizualiza entitățile și operațiunile disponibile în funcție de drepturile fiecărui utilizator.
- Modulul trebuie să asigure trasabilitatea acțiunilor realizate de administratori asupra entităților.

3. Raportare și Statistici

- Modulul trebuie să permită generarea de rapoarte personalizate pe baza datelor existente în sistem, utilizând funcționalități de tip Business Intelligence.
- Trebuie să existe posibilitatea de a defini și genera rapoarte detaliate privind numărul de sportivi activi, în funcție de ramura sportivă, la un moment de timp specificat.
- Modulul trebuie să permită generarea de rapoarte care să evidențieze evoluția sportivilor în timp, în funcție de club, sport și federație.
- Trebuie să existe posibilitatea de a selecta criterii multiple pentru generarea rapoartelor, inclusiv perioade de timp, tipuri de entități și structuri organizaționale.
- Modulul trebuie să permită agregarea și corelarea datelor provenite din mai multe tipuri de entități pentru obținerea unor rapoarte complexe.
- Modulul trebuie să permită configurarea structurii rapoartelor, inclusiv selectarea indicatorilor și a dimensiunilor de analiză.
- Trebuie să existe posibilitatea de a personaliza nivelul de detaliere al rapoartelor, de la vizualizări agregate la analize detaliate.
- Trebuie să existe posibilitatea de a compara datele între diferite perioade de timp sau între diferite structuri organizaționale.
- Modulul trebuie să permită actualizarea dinamică a rapoartelor în funcție de criteriile selectate.
- Modulul trebuie să permită afișarea rapoartelor sub formă de tabele analitice, grafice și alte reprezentări vizuale relevante.
- Modulul trebuie să permită construirea și afișarea de dashboard-uri analitice care să grupeze mai multe rapoarte și indicatori.
- Modulul trebuie să permită interacțiunea cu elementele vizuale, pentru explorarea detaliată a datelor afișate.
- Modulul trebuie să permită accesul la rapoarte și dashboard-uri în funcție de rolurile și permisiunile utilizatorilor.
- Trebuie să existe posibilitatea de a restricționa vizualizarea anumitor date sau indicatori sensibili.
- Modulul trebuie să asigure integritatea și consistența datelor utilizate în rapoarte.
- Trebuie să existe trasabilitate asupra utilizării rapoartelor și a configurărilor acestora, în limitele permisiunilor acordate.

4. Gestionarea Documentelor și Evidențelor

- Modulul trebuie să permită gestionarea electronică a dosarelor și documentelor aferente solicitărilor emise în sistem.
- Trebuie să existe posibilitatea de a asocia documente justificative unei solicitări sau unei entități specifice.
- Modulul trebuie să permită stocarea documentelor de tip copie act de identitate, cazier judiciar și alte documente justificative relevante.
- Trebuie să existe posibilitatea de a organiza documentele pe categorii și tipuri, în funcție de natura acestora.
- Modulul trebuie să permită accesarea documentelor individuale din cadrul unui dosar electronic.
- Trebuie să existe posibilitatea de a vizualiza metadatele asociate fiecărui document.
- Modulul trebuie să permită organizarea documentelor în structuri logice, asociate solicitărilor, utilizatorilor sau entităților relevante.
- Trebuie să existe posibilitatea de a grupa documentele într-un dosar electronic corespunzător fiecărei solicitări.
- Modulul trebuie să permită gestionarea versiunilor documentelor, în cazul în care sunt încărcate actualizări sau corecții.
- Modulul trebuie să permită controlul accesului la documente și dosare pe baza rolurilor și permisiunilor utilizatorilor.
- Trebuie să existe posibilitatea de a restricționa accesul la anumite tipuri de documente cu caracter sensibil.
- Modulul trebuie să asigure confidențialitatea documentelor stocate, prin mecanisme de acces controlat.
- Trebuie să existe trasabilitate asupra accesării și modificării documentelor, pentru asigurarea conformității.
- Modulul trebuie să permită încărcarea electronică a documentelor de către utilizatori autorizați.
- Trebuie să existe posibilitatea de a încărca documente în cadrul unui dosar sau al unei solicitări specifice.
- Modulul trebuie să integreze funcționalități de recunoaștere optică a caracterelor (OCR) pentru documentele încărcate.
- Trebuie să existe posibilitatea de a extrage automat informații relevante din documentele procesate prin OCR.
- Modulul trebuie să permită utilizarea informațiilor extrase pentru completarea automată a câmpurilor asociate solicitărilor sau entităților.
- Trebuie să existe posibilitatea de a vizualiza și verifica datele extrase din documente înainte de validarea acestora.

- Modulul trebuie să permită marcarea documentelor procesate prin OCR ca fiind verificate sau nevalidate.
- Modulul trebuie să permită utilizarea informațiilor extrase pentru accelerarea procesului de validare a documentelor.
- Trebuie să existe posibilitatea de a identifica neconcordanțe între datele extrase și informațiile existente în sistem.
- Modulul trebuie să permită reluarea procesului de prelucrare pentru documentele care necesită corecții.
- Trebuie să existe posibilitatea de intervenție manuală asupra datelor extrase, în limitele permisiunilor acordate.
- Modulul trebuie să asigure integritatea documentelor stocate și a datelor extrase prin OCR.
- Trebuie să existe mecanisme de protecție împotriva accesului neautorizat sau modificării necontrolate a documentelor.
- Modulul trebuie să permită păstrarea istoricului de prelucrare și validare a documentelor.
- Trebuie să existe posibilitatea de auditare a operațiunilor efectuate asupra documentelor și datelor asociate.

5. Fluxuri de Comunicare Internă

- Modulul trebuie să permită administratorilor configurarea alertelor și notificărilor automate asociate diferitelor evenimente sau condiții din sistem.
- Trebuie să existe posibilitatea de a defini tipuri de alerte pentru situații precum expirarea documentelor obligatorii, inclusiv viza medicală.
- Modulul trebuie să permită configurarea condițiilor de declanșare a alertelor, în funcție de datele și statusurile entităților monitorizate.
- Modulul trebuie să permită configurarea destinatarilor alertelor, în funcție de roluri, entități sau responsabilități.
- Modulul trebuie să permită transmiterea automată a notificărilor către utilizatori, fără intervenție manuală.
- Modulul trebuie să asigure transmiterea notificărilor relevante către utilizatorii vizați de evenimentele identificate.
- Trebuie să existe posibilitatea de a personaliza conținutul notificărilor în funcție de tipul evenimentului sau al alertei.
- Modulul trebuie să permită marcarea notificărilor ca transmise și recepționate.
- Modulul trebuie să permită utilizarea alertelor ca mecanism de prevenire a neconformităților.
- Modulul trebuie să permită urmărirea stadiului de conformitate al utilizatorilor în raport cu notificările primite.

- Modulul trebuie să permită identificarea automată a situațiilor care necesită emiterea unor decizii sau acte de constatare.
- Trebuie să existe posibilitatea de a corela evenimentele și statusurile entităților cu regulile și procedurile stabilite.
- Modulul trebuie să permită urmărirea istoricului notificărilor transmise.
- Modulul trebuie să contribuie la reducerea timpului necesar pentru transmiterea deciziilor administrative.
- Trebuie să existe posibilitatea de intervenție manuală a administratorilor în situații justificate, în limitele permisiunilor acordate.

6. Monitorizarea și Auditarea Activităților

- Modulul trebuie să permită monitorizarea detaliată a tuturor acțiunilor efectuate de utilizatori în aplicație.
- Trebuie să existe funcționalitatea de a înregistra fiecare acțiune relevantă realizată de un utilizator, indiferent de modulul în care aceasta are loc.
- Modulul trebuie să permită identificarea utilizatorului care a efectuat o acțiune, inclusiv rolul acestuia în sistem.
- Trebuie să existe posibilitatea de a urmări cronologic activitatea utilizatorilor, pe baza datei și orei exacte a evenimentelor.
- Modulul trebuie să permită diferențierea tipurilor de evenimente, precum creare, modificare sau alte operațiuni administrative.
- Modulul trebuie să permită înregistrarea valorilor anterioare și a valorilor noi pentru fiecare modificare realizată în sistem.
- Trebuie să existe funcționalitatea de a asocia fiecare modificare cu modulul sau componenta asupra căreia s-a intervenit.
- Modulul trebuie să permită afișarea detaliată a modificărilor efectuate, inclusiv a câmpurilor afectate.
- Modulul trebuie să asigure o trasabilitate completă a modificărilor, de la inițiere până la finalizare.
- Modulul trebuie să permită evidențierea autentificărilor reușite ale utilizatorilor.
- Trebuie să existe funcționalitatea de a înregistra tentativele de autentificare eșuate.
- Modulul trebuie să permită asocierea tentativelor de autentificare cu adresa IP și browser-ul utilizat.
- Trebuie să existe posibilitatea de a analiza frecvența și distribuția autentificărilor eșuate.
- Modulul trebuie să permită identificarea potențialelor riscuri de securitate pe baza autentificărilor suspecte.
- Modulul trebuie să permită afișarea adresei IP de la care a fost realizată fiecare acțiune.

- Trebuie să existe posibilitatea de a vizualiza informații despre browser-ul și mediul de acces utilizat.
- Modulul trebuie să permită corelarea evenimentelor cu adresa web sau endpoint-ul accesat.
- Trebuie să existe funcționalitatea de a identifica sursa exactă a fiecărei acțiuni în cadrul aplicației.
- Modulul trebuie să permită filtrarea log-urilor în funcție de utilizator, tip de eveniment, modul sau perioadă de timp.
- Trebuie să existe posibilitatea de a căuta în log-uri după criterii relevante.
- Modulul trebuie să permită afișarea unui număr configurabil de înregistrări per pagină.
- Trebuie să existe funcționalitatea de sortare a înregistrărilor în funcție de câmpuri cheie.
- Modulul trebuie să permită analiza separată a autentificărilor reușite și eșuate.
- Modulul trebuie să permită exportul log-urilor și al istoricului de activități în formate multiple.
- Trebuie să existe posibilitatea de a genera rapoarte de audit pe baza criteriilor selectate.
- Modulul trebuie să permită tipărirea rapoartelor de audit.
- Trebuie să existe funcționalitatea de a utiliza datele de audit pentru verificări interne sau controale externe.
- Modulul trebuie să permită reutilizarea informațiilor de audit în procesele de analiză și conformitate.
- Modulul trebuie să permită accesarea informațiilor de audit doar de către utilizatori autorizați.
- Trebuie să existe funcționalitatea de a restricționa accesul la log-uri sensibile. Modulul trebuie să asigure integritatea datelor de audit, prevenind modificarea sau ștergerea neautorizată.
- Trebuie să existe posibilitatea de a păstra istoricul de audit pe perioade configurabile.

4.5.11 Chatbot/Asistent Virtual

Chatbot-ul reprezintă un modul software conceput pentru a simula și a procesa conversațiile umane, permițând utilizatorilor să interacționeze cu dispozitive digitale sau servicii online într-un mod natural, folosind limbajul obișnuit. Chatboții pot fi integrați în diverse platforme, cum ar fi site-uri web și reprezintă un instrument pentru automatizarea interacțiunilor, îmbunătățirea eficienței operaționale și oferirea unui suport constant și personalizat.

În contextul ANS, chatbot-ul digital trebuie să înțeleagă solicitările utilizatorilor și să răspundă automat întrebărilor și cererilor pe baza informațiilor disponibile în portal sau a fluxurilor de lucru agreate.

4.5.11.1 Cerințe funcționale

- Modulul trebuie să poată răspunde la întrebările utilizatorilor, să ofere informațiile solicitate, să preia cererile și să îi îndrume către serviciile online disponibile în platformă (exemplu: posibilitatea de a oferi răspunsuri la întrebări privind obținerea CIS pentru cluburi sportive).
- Modulul trebuie să permită ghidarea utilizatorilor în completarea cererilor, încărcarea documentelor și utilizarea serviciilor digitale.
- Modulul trebuie să permită utilizarea ca surse de informații a datelor publice din:
  - Registrul Sportiv (Federații și Cluburi)
  - Registrul Sportivilor și Antrenorilor
  - Registrul Bazelor Sportive
  - Anuarul Sportului
- Modulul trebuie să permită furnizarea de link-uri și instrucțiuni clare către serviciile digitale ANS.
- Modulul trebuie să permită accesul la informații publice și să asigure filtrarea datelor pentru a evita expunerea informațiilor confidențiale.
- Modulul trebuie să permită generarea de răspunsuri sintetice, agregate și statistice (ex. pe județ, regiune sau ramură sportivă), fără expunerea datelor personale.
- Modulul trebuie să permită furnizarea de informații statistice privind distribuția sportivilor, cluburilor și bazelor sportive.
- Modulul trebuie să permită oferirea de sugestii suplimentare și link-uri către dashboard-uri sau rapoarte publice (BI).
- Modulul trebuie să contribuie la creșterea transparenței instituționale prin acces facil la date publice.
- Modulul trebuie să prevină generarea de răspunsuri care nu sunt conforme cu procedurile ANS.
- Modulul trebuie să utilizeze NLP pentru înțelegerea întrebărilor și furnizarea de răspunsuri relevante.
- Modulul trebuie să permită interacțiunea în mai multe limbi și să genereze confirmări automate.
- Modulul trebuie să permită suport operatorilor umani și generarea de rapoarte privind interacțiunile.
- Modulul trebuie să asigure accesibilitate pentru utilizatori cu dizabilități.
- Modulul trebuie să fie extensibil și să permită integrarea ulterioară a unor noi module sau surse de date.
- Modulul trebuie să permită analiza nevoilor recurente și optimizarea serviciilor digitale.
- Modulul trebuie să permită moduri diferite de interacțiune pentru utilizatori interni și externi.

Mai multe detalii privind funcționalitățile și tipurile de răspunsuri vor fi stabilite și dezvoltate ulterior, în urma etapei de analiză a proiectului.

4.5.11.2 Cerințe tehnice

- Soluția trebuie să fie o soluție COTS, matură, licențiată perpetuu, pentru un număr nelimitat de utilizatori.
- Modulul trebuie să permită integrarea unui chatbot bazat pe inteligență artificială în platforma web/portal.
- Trebuie să existe posibilitatea de a integra chatbot-ul ca modul extern, interoperabil cu platforma existentă.
- Modulul trebuie să permită disponibilitatea chatbot-ului 24/7, fără dependență de operatori umani.
- Trebuie să existe funcționalitatea de a accesa chatbot-ul din orice pagină a portalului printr-un widget configurabil.
- Modulul trebuie să permită funcționarea chatbot-ului atât pentru utilizatori autentificați, cât și pentru utilizatori neautentificați.
- Modulul trebuie să includă un mecanism de înțelegere a limbajului natural (NLP) care să permită recunoașterea intențiilor utilizatorilor.
- Modulul trebuie să utilizeze mecanisme de generare automată a limbajului natural (NLG) pentru a produce răspunsuri coerente, naturale și adaptate contextului conversației.
- Trebuie să existe posibilitatea de a identifica entitățile relevante din mesajele utilizatorilor, exprimate liber, în limbaj natural.
- Modulul trebuie să permită chatbot-ului să proceseze întrebări formulate diferit, dar cu același scop.
- Trebuie să existe funcționalitatea de a răspunde automat solicitărilor utilizatorilor în funcție de informațiile disponibile în portal.
- Modulul trebuie să permită adaptarea răspunsurilor în funcție de tipul solicitării și contextul conversației.
- Modulul trebuie să permită identificarea și interpretarea stării emoționale a utilizatorului, în vederea adaptării tonului și conținutului răspunsurilor.
- Modulul trebuie să permită furnizarea de informații privind procedurile administrative gestionate de instituție.
- Modulul trebuie să permită furnizarea informațiilor privind documentele necesare pentru omologarea bazelor sportive.
- Trebuie să existe funcționalitatea de a explica pașii necesari pentru completarea cererilor.
- Modulul trebuie să permită ghidarea utilizatorilor pas cu pas în cadrul fluxurilor de lucru agreate.

- Trebuie să existe posibilitatea de a direcționa utilizatorii către serviciile online relevante disponibile în platformă.
- Modulul trebuie să permită redirecționarea automată către formularele sau modulele corespunzătoare solicitării.
- Trebuie să existe posibilitatea de a explica tipurile de documente solicitate și formatele acceptate.
- Modulul trebuie să permită verificarea preliminară a completitudinii documentelor încărcate.
- Modulul trebuie să permită verificarea calității și validității documentelor încărcate.
- Modulul trebuie să permită furnizarea de recomandări personalizate în funcție de solicitarea utilizatorului.
- Trebuie să existe posibilitatea de interacțiune prin conversație vocală.
- Trebuie să existe funcționalitatea de a utiliza chatbot-ul ca instrument principal de comunicare digitală.
- Modulul trebuie să permită înregistrarea integrală a dialogurilor purtate cu utilizatorii.
- Trebuie să existe posibilitatea de a consulta ulterior istoricul conversațiilor.
- Modulul trebuie să permită asocierea conversațiilor cu utilizatori sau sesiuni unice.
- Modulul trebuie să permită accesul utilizatorilor cu rol administrativ la configurările chatbot-ului.
- Trebuie să existe posibilitatea de a gestiona scenarii de conversație și fluxuri predefinite.
- Trebuie să existe funcționalitatea de a actualiza conținutul informațional utilizat de chatbot.
- Modulul trebuie să utilizeze un model de inteligență artificială implementat și rulat pe arhitectura locala sau într-un mediu controlat.
- Trebuie să existe funcționalitatea de a opera chatbot-ul fără dependență de platforme externe publice.
- Modulul trebuie să excludă utilizarea platformelor de tip ChatGPT, Gemini sau alte servicii publice similare.
- Trebuie să existe posibilitatea de a controla integral datele utilizate de modelul AI.
- Modulul trebuie să permită îmbunătățirea continuă a răspunsurilor chatbot-ului pe baza interacțiunilor reale.
- Trebuie să existe funcționalitatea de a adapta comportamentul chatbot-ului în funcție de modificările legislative sau procedurale.
- Modulul trebuie să permită actualizarea periodică a cunoștințelor modelului AI.
- Modulul trebuie să permită validarea conținutului utilizat pentru antrenarea modelului AI de către utilizatori autorizați.

- Modulul trebuie să permită utilizarea documentației oficiale, procedurilor interne și informațiilor publice ANS ca surse de date și antrenare pentru modelul AI.
- Modulul trebuie să permită ajustarea regulilor de răspuns în conformitate cu politicile instituției.
- Modulul trebuie să permită revizuirea și corectarea răspunsurilor oferite de chatbot, din partea de administrare.
- Trebuie să existe mecanisme de audit privind utilizarea și antrenarea modelului AI.
- Modulul trebuie să permită trasabilitatea modificărilor aduse modelului AI.
- Modulul trebuie să permită utilizarea tehnologiei AI în conformitate cu reglementările aplicabile sectorului public.
- Trebuie să existe funcționalitatea de a adapta soluția AI la nevoile instituției fără limitări impuse de platforme externe.
- Ofertantul va prezenta în propunerea tehnică metodologia de gestionare a riscurilor specifice sistemelor de inteligență artificială, incluzând cel puțin: identificarea și evaluarea riscurilor, măsuri de mitigare, transparența algoritmică și guvernanța IA. Metodologia propusă trebuie să respecte principiile generale de gestionare a riscurilor pentru sisteme IA. Conformitatea cu standardul SR ISO/IEC 42001:2024 sau cu un standard internațional echivalent constituie un avantaj tehnic, fără a reprezenta o cerință obligatorie de calificare.

4.5.12 Rapoarte Business Intelligence

În prezent, la nivelul ANS și al instituțiilor subordonate (Direcții județene pentru Sport și a Municipiului București, Cluburi sportive, Complexuri sportive naționale, Institutul Național de Cercetare pentru Sport, Centru Național de Formare și Perfecționare a Antrenorilor, Galeria Marilor Sportivi), activitățile de raportare se realizează utilizând machete de raportare în format .xls/doc cu frecvență lunară, trimestrială, semestrială și anuală.

Transmiterea datelor se realizează prin e-mail, instituțiile subordonate raportând către ANS, iar ulterior datele sunt centralizate manual la nivel național.

Acest mod de lucru implică:

- consum ridicat de timp,
- introducerea duplicată a datelor,
- risc crescut de erori,
- lipsa unei imagini consolidate în timp real.

Se urmărește transformarea sistemului actual într-un **sistem centralizat și automatizat de raportare**, bazat pe o platformă de tip Business Intelligence (BI), care să permită:

- colectarea automată a datelor,
- centralizarea și agregarea acestora,
- generarea de rapoarte și dashboard-uri interactive,

- suport decizional în timp real.

Platforma software de tip Business Intelligence (BI) va reprezenta un sistem integrat pentru:

- colectarea datelor din multiple surse,
- procesarea și agregarea acestora,
- stocarea într-un depozit de date (data warehouse / data mart),
- vizualizarea și analiza datelor prin rapoarte și dashboard-uri.

Soluția va include mecanisme de tip ETL (Extract, Transform, Load) pentru integrarea datelor din surse interne și externe.

Soluția BI va integra funcționalități de tip GIS (Geographic Information System), permițând:

- colectarea și utilizarea datelor geografice,
- vizualizarea datelor în context spațial (hartă),
- analiza distribuției teritoriale a indicatorilor (ex. număr cluburi sportive pe județ/localitate),
- identificarea de tipare și tendințe bazate pe localizare.

Soluția va asigura următoarele capabilități:

Colectare și integrare date

- Preluarea datelor din sisteme interne și externe (baze de date, DMS, CRM, ERP, fișiere).
- Eliminarea raportărilor manuale bazate pe fișiere Excel transmise prin e-mail.
- Validarea datelor la introducere.

Vizualizare și raportare

- Generarea de:
  - rapoarte standard,
  - dashboard-uri interactive,
  - grafice și diagrame.
- Posibilitatea filtrării și segmentării datelor.
- Exportul rapoartelor în formate standard (PDF, Excel, CSV).

Suport decizional

- Furnizarea de informații sintetice pentru management.
- Identificarea oportunităților și riscurilor.
- Monitorizarea performanței instituționale.

Exemple de utilizare

- Raport privind activitatea documentelor procesate într-o perioadă determinată.
- Dashboard pentru monitorizarea performanței utilizatorilor.

- Vizualizare geografică a distribuției cluburilor sportive la nivel național.

4.5.12.1 Cerințe funcționale

Integrare și surse de date

- Modul BI va centraliza și analiza datele provenite din celelalte module ale aplicației pentru a sprijini procesul decizional și planificarea strategică în sportul național.
  - Modul Registrul Sportiv – Federații și Cluburi: informații despre structura cluburilor, afilierea la federații, localizarea și activitățile desfășurate.
  - Modul Registrul Sportivilor și Antrenorilor: date despre sportivi, antrenori, ramuri sportive, rezultate și performanțe.
  - Modul Registrul Bazelor Sportive: locația și dotările bazelor sportive, disponibilitate și utilizare.
  - Modul Anuarul Sportului: statistici agregate, rapoarte anuale și date istorice privind activitatea sportivă, dar și date din restul modulelor.

Toate datele necesare pentru modulul BI vor fi colectate din aceste module, iar alte surse de date suplimentare vor fi identificate și clarificate în etapa de analiză a proiectului, pentru a asigura completitudinea și corectitudinea informațiilor utilizate în raportare și decizie strategică.

De asemenea, alte situații specifice și surse de date suplimentare vor fi identificate și clarificate în etapa de analiză a proiectului, pentru a asigura completitudinea și corectitudinea informațiilor utilizate în raportare și decizie strategică.

Analiză și vizualizare

- Vizualizare indicatori: numărul de sportivi pe județ, club sau ramură sportivă, preluat din modulele registru sportiv și registru sportivi/antrenori.
- Analiză geospațială (GIS): corelarea datelor statistice cu informații geografice pentru reprezentarea pe hărți interactive.
- Agregare și detaliere: vizualizarea datelor pe localitate, județ sau regiune și posibilitatea de a urmări evoluția activităților sportive în timp și spațiu.
- Monitorizare activitate sportivă: identificarea zonelor cu activitate intensă, distribuția cluburilor și localizarea exactă a competițiilor sportive.
- Sprijin decizional: fundamentarea deciziilor privind susținerea anumitor ramuri sportive și analiza impactului acestora la nivel teritorial.
- Identificarea Dublelor legitimări: permite identificarea situațiilor de dublă legitimare, în condiții ilegale.

Raportare și colaborare

- Raportare și partajare: generarea automată a rapoartelor în formate configurabile, exportul datelor pentru utilizare ulterioară, publicarea de dashboard-uri și partajarea cu instituții partenere.
- Actualizare și consistență a datelor: preluarea automată a datelor din celelalte module, asigurarea corectitudinii și disponibilității acestora pentru raportare și colaborare.

- Transparență și planificare strategică: utilizarea datelor BI pentru luarea deciziilor în planificarea sportivă și creșterea transparenței instituționale.
- Soluția trebuie să permită vizualizarea indicatorilor precum numărul de sportivi pe județ, club sau ramură sportivă.
- Trebuie să existe funcționalitatea de a afișa date agregate pe localitate, județ sau regiune și de a analiza evoluția activităților sportive în timp și spațiu.
- Soluția trebuie să permită identificarea zonelor cu activitate sportivă intensă și monitorizarea distribuției cluburilor și competițiilor sportive pe teritoriu.
- Trebuie să existe funcționalitatea de corelare a datelor statistice cu informații geografice.
- Soluția trebuie să permită reprezentarea datelor pe hărți interactive, cu actualizare dinamică și localizarea exactă a competițiilor sportive.
- Soluția trebuie să permită analiza impactului deciziilor la nivel teritorial și fundamentarea deciziilor privind susținerea anumitor ramuri sportive.
- Trebuie să existe funcționalitatea de a utiliza datele BI în procesele de planificare strategică și luarea deciziilor bazate pe informații centralizate.
- Soluția trebuie să permită publicarea de dashboard-uri pentru informarea publicului și partajarea rapoartelor cu instituții partenere.
- Trebuie să existe funcționalitatea de raportare automată către instituții autorizate, livrare a rapoartelor în formate configurabile și exportul datelor pentru utilizare ulterioară.
- Soluția trebuie să asigure date actualizate și corecte pentru colaborare.
- Trebuie să existe funcționalitatea de administrare centralizată a setărilor de raportare.
- Soluția trebuie să contribuie la creșterea transparenței instituționale.

4.5.12.2 Cerințe tehnice

- Soluția trebuie să fie o soluție COTS, matură, licențiată perpetuu, pentru un număr nelimitat de utilizatori.
- Soluția trebuie să fie de tip Business Intelligence (BI).
- Modulul trebuie să permită colectarea, integrarea și analiza datelor provenite din modulele sistemului ANS.
- Trebuie să existe funcționalitatea de a extrage date din surse multiple interne ale platformei.
- Trebuie să existe posibilitatea de a asigura acces rapid și eficient la datele analizate.
- Modulul trebuie să permită procese automate de extragere a datelor din sistemele sursă.
- Trebuie să existe funcționalitatea de a transforma datele pentru a fi utilizabile în scopuri analitice.
- Modulul trebuie să permită programarea proceselor ETL la intervale configurabile.

- Trebuie să existe posibilitatea de a gestiona volume mari de date fără afectarea performanței aplicației.
- Modulul trebuie să asigure consistența și integritatea datelor analizate.
- Modulul trebuie să permită crearea și afișarea de dashboard-uri vizuale interactive.
- Modulul trebuie să permită filtrarea dinamică a datelor afișate în dashboard-uri.
- Trebuie să existe funcționalitatea de a actualiza vizualizările în timp real sau aproape de timp real.
- Modulul trebuie să permită adaptarea dashboard-urilor în funcție de rolul utilizatorului.
- Modulul trebuie să permită utilizatorilor definirea de rapoarte personalizate direct din aplicație.
- Trebuie să existe un configurator vizual de rapoarte, bazat pe opțiuni predefinite.
- Modulul trebuie să permită crearea rapoartelor fără a necesita scrierea de interogări în baza de date.
- Trebuie să existe posibilitatea de a salva și reutiliza rapoarte personalizate.
- Modulul trebuie să includă un set de rapoarte standard predefinite.
- Trebuie să existe funcționalitatea de a afișa numărul total de documente gestionate de aplicație.
- Modulul trebuie să permită vizualizarea documentelor create sau modificate într-o perioadă selectabilă.
- Modulul trebuie să permită definirea rapoartelor de tip alertă pe documente și activități.
- Trebuie să existe posibilitatea de a identifica documente nou create într-un interval specificat.
- Modulul trebuie să permită identificarea documentelor care urmează să expire într-o perioadă definită.
- Trebuie să existe funcționalitatea de a analiza activitatea utilizatorilor pe departamente.
- Modulul trebuie să permită planificarea automată a generării rapoartelor.
- Modulul trebuie să permită livrarea automată a rapoartelor prin email.
- Trebuie să existe posibilitatea de a configura livrarea zilnică, săptămânală sau lunară.
- Trebuie să existe funcționalitatea de a selecta destinatari individuali sau grupuri de utilizatori.
- Modulul trebuie să permită livrarea rapoartelor către adrese de email configurabile.
- Modulul trebuie să permită analiza eficienței fluxurilor de lucru definite în sistem.
- Trebuie să existe posibilitatea de a vizualiza durata medie de finalizare a fiecărui flux.
- Modulul trebuie să permită analiza duratei medii de rezolvare a sarcinilor pentru fiecare utilizator.

- Trebuie să existe funcționalitatea de a identifica blocaje și întârzieri în procesele de aprobare.
- Modulul trebuie să permită filtrarea analizelor pe intervale de timp selectabile.
- Soluția trebuie să permită procesarea și analizarea datelor operaționale în scopul generării de indicatori de performanță.
- Soluția trebuie să permită detectarea automată a structurii bazei de date DMS.
- Soluția trebuie să permită identificarea relațiilor între tabelele existente (documente, taskuri, utilizatori, fluxuri etc.).
- Soluția trebuie să permită extragerea periodică a datelor din baza de date DMS.
- Trebuie să existe funcționalitatea de transformare a datelor operaționale într-un model analitic de tip STAR SCHEMA.
- Soluția trebuie să permită calcularea automată a:
  - duratei taskurilor
  - duratei fluxurilor de lucru
  - timpului de aprobare
  - timpului de rezolvare documente
  - depășirii termenelor SLA
  - timpului de stagnare în proces
  - numărului de reasignări
- Soluția trebuie să permită calcularea automată a indicatorilor de performanță pentru:
  - utilizatori
  - departamente
  - tipuri de documente
  - fluxuri de lucru
- Trebuie să existe funcționalitatea de calcul a:
  - Efficiency Score
  - Delay Score
  - Throughput Score
  - Approval Quality Score
- Soluția trebuie să permită vizualizarea scorurilor sub formă de grafice radar.
- Soluția trebuie să permită monitorizarea respectării termenelor SLA.
- Trebuie să existe funcționalitatea de clasificare a documentelor în:
  - rezolvate în termen
  - rezolvate cu întârziere

  - critice
- Soluția trebuie să permită afișarea trendului de respectare SLA în timp.
- Trebuie să existe funcționalitatea de identificare a departamentelor cu cele mai multe depășiri SLA.
- Soluția trebuie să permită identificarea etapelor de proces unde documentele petrec cel mai mult timp.
- Trebuie să existe funcționalitatea de analiză a duratei complete a fluxurilor de lucru.
- Trebuie să existe funcționalitatea de vizualizare a fluxului documentelor între departamente.
- Soluția trebuie să permită monitorizarea volumului de lucru per utilizator.
- Trebuie să existe funcționalitatea de identificare a utilizatorilor supraîncărcați.
- Soluția trebuie să permită analiza vechimii taskurilor active.
- Soluția trebuie să permită afișarea următoarelor tipuri de grafice:
  - Donut Chart – pentru respectare SLA
  - Line Chart – pentru trenduri
  - Bar Chart – pentru comparații între departamente
  - Heatmap – pentru distribuția taskurilor
  - Histogram – pentru vechimea taskurilor
  - Funnel Chart – pentru fluxul documentelor
  - Sankey Diagram – pentru traseul documentelor
  - Radar Chart – pentru scoruri de performanță
  - Calendar Heatmap – pentru volum zilnic
- Soluția trebuie să includă un modul de analiză bazat pe inteligență artificială.
- Trebuie să existe funcționalitatea de adresare a întrebărilor în limbaj natural.
- Soluția trebuie să permită generarea automată de interogări SQL pe baza întrebărilor utilizatorului.
- Soluția trebuie să utilizeze un chat NLP (natural language processing) local instalat în infrastructura actuala, nu se accepta integrări cu ChatGPT, Gemini si alte aplicații terțe. Se va detalia de către ofertant ce model local folosește, si modul cum se poate antrena acest model.
- Soluția trebuie să permită generarea automată de grafice pe baza întrebărilor adresate.
- Trebuie să existe funcționalitatea de salvare a analizelor generate în dashboard.
- Soluția trebuie să execute interogări exclusiv în regim read-only.
- Trebuie să existe funcționalitatea de validare a interogărilor generate de AI.

4.5.13 Aplicații de mobil

Platforma software livrată va fi disponibilă de asemenea într-o aplicație mobilă. Modulele ce vor fi disponibile prin aplicația mobilă vor fi reprezentate de părțile publice ale portalului ANS, modulele specifice sportivilor și structurilor sportive precum și asistentul virtual.

Toate datele și interfețele ce urmează a fi disponibile în aplicația mobilă vor fi stabilite în faza de analiză și proiectare a sistemului informatic, din cadrul implementării proiectului.

Aplicația mobilă pentru ANS va facilita în mod considerabil interacțiunea utilizatorilor cu administrația, reducând birocrația și oferind acces rapid și eficient la servicii esențiale. De asemenea, va îmbunătăți capacitatea ANS de a monitoriza și măsura activitățile. Aplicația mobilă devine astfel un element crucial pentru digitalizarea completă a proceselor și pentru modernizarea activităților de administrare.

Aplicația mobilă va reprezenta o extensie a platformei web, menită să ofere acces mai facil utilizatorilor la diverse funcționalități și servicii administrative. Aceasta va fi concepută pentru a răspunde cerințelor specifice ale ANS și pentru a facilita accesul la informații și procese, atât pentru utilizatorii externi (publicul larg, turiști, agenți economici), cât și pentru personalul ANS.

4.5.13.1 Aplicație mobilă portal

Cerințe minime:

- Aplicația mobilă trebuie să reprezinte o extensie funcțională a platformei web ANS, oferind utilizatorilor acces facil și rapid la principalele servicii administrative și informații publice, direct de pe dispozitive mobile.
- Aplicația trebuie să fie disponibilă pentru Android și iOS.
- Trebuie să existe posibilitatea de a accesa aplicația mobilă atât de către utilizatori externi (cetățeni, sportivi, cluburi, agenți economici), cât și de către personalul ANS, în funcție de drepturile asociate fiecărui rol.
- Modulul trebuie să permită utilizarea aplicației fără autentificare pentru accesarea informațiilor publice, dar și autentificarea securizată pentru accesarea funcționalităților avansate.
- Aplicația mobilă trebuie să funcționeze astfel încât să reducă interacțiunile birocratice și să ofere o experiență digitală coerentă și intuitivă.
- Trebuie să existe funcționalitatea de a consulta Registrul Sportiv direct din aplicația mobilă, permițând utilizatorilor să identifice rapid cluburi sportive, federații și structuri afiliate.
- Aplicația trebuie să permită afișarea detaliată a informațiilor relevante pentru fiecare entitate sportivă, inclusiv date de contact, statut juridic și ramuri sportive practicate.
- Trebuie să existe posibilitatea de a vizualiza bazele sportive pe hartă, cu indicarea localizării geografice și a facilităților disponibile.
- Modulul trebuie să permită filtrarea și căutarea bazelor sportive după criterii precum județ, localitate, tip de sport sau statut de omologare.

- Trebuie să existe funcționalitatea de a consulta statutul bazelor sportive, pentru a informa utilizatorii cu privire la gradul de conformitate al acestora.
- Trebuie să existe funcționalitatea de a iniția și depune cereri pentru obținerea Certificatului de Identitate Sportivă direct din aplicația mobilă.
- Modulul trebuie să permită utilizatorilor autorizați să urmărească evoluția cererilor CIS, de la depunere până la soluționare.
- Trebuie să existe posibilitatea de a primi notificări automate atunci când statusul unei cereri CIS se modifică.
- Modulul trebuie să permită actualizarea electronică a informațiilor cluburilor sportive, reducând necesitatea depunerii documentelor în format fizic.
- Trebuie să existe funcționalitatea de a valida datele introduse înainte de transmiterea cererilor, pentru a preveni erorile și întârzierile în procesare.
- Aplicația trebuie să includă un calendar național al competițiilor sportive, accesibil din aplicația mobilă, care să centralizeze evenimentele organizate de federații și cluburi.
- Trebuie să existe posibilitatea de a consulta competițiile sportive în funcție de perioadă, locație sau ramură sportivă.
- Aplicația trebuie să permită utilizatorilor să își definească evenimentele de interes și să primească notificări personalizate.
- Trebuie să existe funcționalitatea de a urmări modificările intervenite în programul competițiilor.
- Modulul trebuie să contribuie la creșterea gradului de informare și participare la evenimentele sportive.
- Trebuie să existe posibilitatea de a consulta Registrul Național al Sportivilor și Antrenorilor direct din aplicația mobilă.
- Modulul trebuie să permită sportivilor și antrenorilor să își actualizeze datele personale și profesionale.
- Trebuie să existe funcționalitatea de a vizualiza statutul legitimității și calificărilor aferente.
- Modulul trebuie să asigure transmiterea datelor actualizate către sistemele centrale ANS, în conformitate cu procedurile interne.
- Trebuie să existe posibilitatea de a consulta istoricul relevant al activității sportive.
- Trebuie să existe funcționalitatea de a accesa un ghid digital al bazelor sportive, conceput pentru a sprijini utilizatorii în identificarea infrastructurii sportive disponibile.
- Aplicația trebuie să permită utilizatorilor să raporteze probleme legate de starea bazelor sportive, contribuind astfel la o mai bună gestionare a infrastructurii.
- Aplicația trebuie să faciliteze colectarea informațiilor din teren, utile în procesul decizional ANS.

- Trebuie să existe funcționalitatea de a analiza feedback-ul primit pentru îmbunătățirea serviciilor.
- Aplicația trebuie să includă o secțiune dedicată informării utilizatorilor cu privire la activitățile și inițiativele ANS.
- Aplicația să existe funcționalitatea de a publica și distribui știri, anunțuri și comunicări oficiale.
- Aplicația trebuie să permită accesul la resurse educaționale relevante pentru sportivi, antrenori și structuri sportive.
- Trebuie să existe posibilitatea de a consulta ghiduri și materiale de bună practică.
- aplicația trebuie să contribuie la creșterea nivelului de informare și profesionalizare a comunității sportive.
- Trebuie să existe funcționalitatea de a comunica direct cu ANS prin intermediul aplicației mobile.
- Aplicația trebuie să permită transmiterea solicitărilor și întrebărilor într-un mod structurat.
- Trebuie să existe funcționalitatea de a primi notificări și alerte privind termene importante, expirări sau obligații administrative.
- Aplicația Trebuie să permită configurarea preferințelor de notificare de către utilizatori.
- Aplicația trebuie să contribuie la creșterea gradului de conformitate și la respectarea termenelor legale.
- Trebuie să existe funcționalitatea de a colecta feedback din partea utilizatorilor privind serviciile și infrastructura sportivă.
- Aplicația trebuie să permită evaluarea evenimentelor sportive și a bazelor sportive.
- Trebuie să existe posibilitatea de a analiza feedback-ul la nivel centralizat.
- Aplicația trebuie să sprijine ANS în identificarea nevoilor reale ale comunității sportive.
- Trebuie să existe posibilitatea de a consulta informații generale despre muzeu, programul de funcționare și regulile de vizitare.
- Aplicația trebuie să permită accesarea unei zone dedicate serviciilor oferite de muzeul instituției (tururi ghidate, ateliere, evenimente, audio-ghid etc.).
- Trebuie să existe posibilitatea de a vizualiza descrierea detaliată a fiecărui serviciu, inclusiv durata, prețul, condițiile de participare și disponibilitatea.
- Aplicația trebuie să permită rezervarea serviciilor disponibile direct din interfața mobilă.
- Trebuie să existe funcționalitatea de achiziționare a biletelor de intrare în muzeu prin intermediul aplicației mobile.
- Aplicația trebuie să permită selectarea tipului de bilet (adult, elev/student, pensionar, grup etc.) și a numărului de bilete dorite.

- Aplicația trebuie să permită selectarea datei și a intervalului orar pentru vizitare, în funcție de disponibilitatea muzeului.
- Aplicația trebuie să permită efectuarea plăților online în condiții de siguranță, prin integrarea cu procesatori de plăți autorizați.
- Trebuie să existe funcționalitatea de generare automată a biletului electronic, inclusiv cod QR sau cod unic pentru validarea la acces.
- Aplicația trebuie să permită stocarea și vizualizarea biletelor achiziționate în contul utilizatorului.
- Trebuie să existe posibilitatea de programare a accesului în muzeu pe baza unui sistem de sloturi orare, în vederea gestionării fluxului de vizitatori.
- Aplicația trebuie să permită modificarea sau anularea programării, în conformitate cu politica muzeului.
- Trebuie să existe funcționalitatea de transmitere automată a confirmărilor și notificărilor privind rezervările și achizițiile efectuate.
- Aplicația trebuie să permită vizualizarea unui tur digital al muzeului, inclusiv hartă interactivă a sălilor și a exponatelor.
- Trebuie să existe funcționalitatea de accesare a informațiilor multimedia aferente exponatelor (text, imagini, audio, video).
- Aplicația trebuie să permită utilizarea unui tur ghidat digital în timpul vizitei fizice.
- Trebuie să existe posibilitatea accesării unui tur virtual pentru utilizatorii care nu pot vizita fizic muzeul.
- Trebuie să existe funcționalitatea de colectare a feedback-ului din partea vizitatorilor privind experiența de vizitare.
- Trebuie să existe posibilitatea generării de rapoarte privind numărul de vizitatori, biletele vândute și gradul de ocupare pe intervale orare.
- Trebuie să existe funcționalitatea de a utiliza datele colectate în procesele de îmbunătățire continuă.
- Trebuie să existe posibilitatea accesării catalogului de cursuri organizate de CNFPA.
- Aplicația trebuie să permită filtrarea cursurilor după categorie, nivel, ramură sportivă și tip (formare inițială / perfecționare).
- Trebuie să existe posibilitatea vizualizării paginii detaliate a cursului, incluzând obiectivele, durata, condițiile de înscriere și informații despre lector.
- Aplicația trebuie să permită înscrierea la cursuri direct din interfața mobilă.
- Trebuie să existe funcționalitatea de achiziționare online a cursurilor cu integrare securizată a plăților.
- Aplicația trebuie să permită aplicarea codurilor de reducere, dacă este cazul.

- Trebuie să existe posibilitatea accesării cursurilor într-un player dedicat, optimizat pentru mobil.
- Aplicația trebuie să permită parcurgerea lecțiilor în format multimedia (video, audio, text, documente atașate).
- Trebuie să existe funcționalitatea de descărcare a materialelor educaționale pentru consultare offline (acolo unde este permis).
- Aplicația trebuie să permită marcarea lecțiilor ca finalizate și afișarea progresului în timp real.
- Trebuie să existe o bară de progres care să indice procentul de finalizare a cursului.
- Trebuie să existe funcționalitatea de susținere a testelor și chestionarelor direct din aplicația mobilă.
- Aplicația trebuie să permită afișarea rezultatelor obținute și a feedback-ului aferent evaluărilor.
- Trebuie să existe posibilitatea generării și descărcării certificatelor de absolvire în format digital.
- Aplicația trebuie să permită vizualizarea și descărcarea carnetului de antrenor în format electronic.
- Trebuie să existe funcționalitatea de reînnoire a licenței prin încărcarea documentelor necesare și urmărirea statusului solicitării.
- Aplicația trebuie să permită depunerea documentelor pentru obținerea atestatului de recunoaștere profesională pentru antrenorii formați.
- Trebuie să existe posibilitatea încărcării documentelor justificative în format electronic (PDF, imagine).
- Aplicația trebuie să permită urmărirea statusului solicitărilor depuse.
- Trebuie să existe funcționalitatea de solicitare a promovării profesionale și obținere a certificatului de promovare.
- Trebuie să existe posibilitatea consultării catalogului electronic cu notele și evaluările obținute.
- Aplicația trebuie să permită accesul la istoricul cursurilor urmate și al certificărilor obținute.
- Trebuie să existe funcționalitatea de interconectare cu modulul federații/cluburi pentru validarea statutului de antrenor activ.
- Aplicația trebuie să permită comunicarea directă între cursanți și instructori prin mesagerie internă.
- Trebuie să existe funcționalitatea de participare la forumuri sau discuții aferente cursurilor.
- Aplicația trebuie să permită primirea notificărilor privind:

  - înscrierea la curs
  - programarea examenelor
  - expirarea licenței
  - emiterea certificatelor
- Trebuie să existe posibilitatea configurării preferințelor de notificare.
- Aplicația trebuie să sprijine CNFPA în analiza performanței programelor de formare și în actualizarea curriculei.
- Trebuie să existe un flux digital complet pentru emiterea certificatelor de absolvire.
- Aplicația trebuie să permită generarea automată a certificatului în urma îndeplinirii condițiilor de promovare.
- Trebuie să existe posibilitatea actualizării statutului carnetului (activ, suspendat, expirat).
- Aplicația trebuie să permită generarea certificatelor de clasificare profesională în baza criteriilor stabilite de CNFPA și ANS.
- Trebuie să existe posibilitatea validării și arhivării electronice a certificatelor emise.
- Trebuie să existe o secțiune dedicată oportunităților de finanțare și sponsorizare destinate structurilor sportive.
- Aplicația trebuie să permită afișarea apelurilor deschise pentru:
  - granturi;
  - programe de finanțare naționale;
  - finanțări europene;
  - scheme de sprijin guvernamental; ○ oportunități de sponsorizare.
- Trebuie să existe posibilitatea filtrării oportunităților de finanțare după tip, domeniu sportiv, valoare estimată și termen limită de depunere.
- Trebuie să existe posibilitatea descărcării documentelor aferente apelurilor de finanțare.
- Aplicația trebuie să permită depunerea cererilor de finanțare direct prin intermediul platformei mobile.
- Trebuie să existe un flux digital complet pentru aplicare, care să includă:
  - completarea formularului electronic;
  - validarea automată a câmpurilor obligatorii;
  - atașarea documentelor justificative;
  - confirmarea depunerii.
- Aplicația trebuie să permită încărcarea documentelor în formate standard (PDF, DOC, XLS, imagini).
- Trebuie să existe posibilitatea salvării aplicației în draft și reluării completării ulterioare.

- Aplicația trebuie să genereze un număr unic de înregistrare pentru fiecare cerere depusă.
- Trebuie să existe posibilitatea urmăririi în timp real a statusului cererilor depuse.
- Aplicația trebuie să permită afișarea etapelor procesului de evaluare, precum:
- cerere depusă;
  - în evaluare;
  - solicitare clarificări;
  - aprobată;
  - respinsă;
- Trebuie să existe funcționalitatea de notificare automată a solicitantului la schimbarea statusului cererii.
- Aplicația trebuie să permită transmiterea clarificărilor solicitate de evaluator direct prin platformă.
- Aplicația trebuie să permită generarea de rapoarte centralizate privind:
  - numărul de cereri depuse;
  - valoarea totală solicitată;
  - valoarea totală aprobată;
  - gradul de absorbție a fondurilor;
  - distribuția finanțărilor pe ramuri sportive.
- Aplicația trebuie să sprijine instituția în identificarea domeniilor cu nevoi ridicate de finanțare și în fundamentarea politicilor publice.
- Trebuie să existe o secțiune dedicată transparenței financiare a ANS, accesibilă prin aplicația mobilă.
- Aplicația trebuie să permită publicarea și consultarea rapoartelor financiare oficiale.
- Trebuie să existe posibilitatea vizualizării alocărilor bugetare pe:
  - programe sportive;
  - federații;
  - cluburi;
  - proiecte finanțate;
  - categorii de cheltuieli.
- Aplicația trebuie să permită afișarea execuției bugetare într-un format sintetic și ușor de înțeles.
- Trebuie să existe posibilitatea descărcării documentelor financiare în format electronic.
- Aplicația trebuie să includă indicatori statistici privind:
  - distribuția fondurilor;

  - gradul de utilizare a bugetului;
  - evoluția finanțărilor în timp.
- Trebuie să existe actualizare periodică a datelor publicate, conform obligațiilor legale privind transparența instituțională.
- Trebuie să existe o funcționalitate dedicată raportării activităților și rezultatelor cluburilor sportive.
- Aplicația trebuie să permită structurilor sportive introducerea datelor privind:
  - activitățile desfășurate;
  - competițiile organizate;
  - participarea la competiții;
  - rezultate obținute;
  - număr sportivi legitimați;
  - număr antrenori activi.
- Trebuie să existe posibilitatea încărcării documentelor justificative aferente activităților raportate.
- Aplicația trebuie să permită completarea unor formulare standardizate pentru asigurarea uniformității datelor colectate.
- Trebuie să existe un asistent virtual inteligent integrat în aplicația mobilă, care să ofere suport utilizatorilor în accesarea și utilizarea funcționalităților aplicației.
- Aplicația trebuie să permită interacțiunea cu asistentul virtual prin limbaj natural, printr-o interfață conversațională de tip chat.
- Asistentul virtual trebuie să ofere ghidare pas cu pas pentru completarea formularelor, depunerea cererilor, încărcarea documentelor și utilizarea serviciilor disponibile.
- Aplicația trebuie să permită furnizarea de informații personalizate, în funcție de rolul și profilul utilizatorului (sportiv, antrenor, club, federație, personal ANS etc.).
- Trebuie să existe posibilitatea generării de notificări proactive privind termene limită, expirări, documente lipsă sau obligații administrative.
- Asistentul virtual trebuie să faciliteze căutarea și interogarea registrelor și bazelor de date prin comenzi conversaționale.
- Aplicația trebuie să permită inițierea directă a unor acțiuni din interfața asistentului virtual, precum rezervări, înscrieri, programări sau depuneri de cereri.
- Asistentul virtual trebuie să contribuie la reducerea erorilor administrative, prin validarea preliminară a informațiilor introduse de utilizatori.
- Trebuie să existe mecanisme de colectare a feedback-ului privind calitatea răspunsurilor oferite de asistentul virtual, pentru îmbunătățirea continuă a serviciului.

- Aplicația trebuie să asigure respectarea normelor privind protecția datelor și accesul diferențiat la informații, în funcție de nivelul de autorizare al utilizatorului.
- Asistentul cu funcționalități de NLP (natural language processing) trebuie sa fie un model propriu care sa poate fi antrenat si să învețe pe baza datelor existente. Nu se accepta aplicații terțe de genul OpenAI, Gemini, etc.
- Ofertantul devenit prestator va trebui sa gestioneze tot procesul de publicare, actualizare conform politicilor Google, Apple, etc.

4.5.13.2 Aplicatia mobila Document management system (DMS) dedicată

Cerințe minime:

- Aplicația trebuie să fie disponibilă exclusiv utilizatorilor interni ai organizației.
- Aplicația trebuie să se conecteze securizat la aplicația Web în care este implementat DMS-ul.
- Aplicația trebuie să utilizeze aceleași reguli de business și aceleași permisiuni definite în sistemul Web.
- Aplicația trebuie să fie disponibilă pentru Android și iOS.
- Aplicația trebuie să funcționeze doar pe baza autentificării utilizatorilor interni.
- Aplicația trebuie să permită autentificarea utilizatorilor folosind conturile interne existente.
- Aplicația trebuie să permită autentificarea prin biometrie (amprentă/Face ID), după prima autentificare validă.
- Aplicația trebuie să gestioneze sesiunea utilizatorului în mod securizat.
- Aplicația trebuie să aplice drepturile și rolurile utilizatorului exact ca în sistemul Web.
- Aplicația trebuie să blocheze accesul după un număr configurabil de încercări eșuate de autentificare.
- Aplicația trebuie să permită vizualizarea listei de documente la care utilizatorul are acces.
- Aplicația trebuie să permită filtrarea documentelor după criterii precum: dată, tip document, autor, status, departament, alte criterii.
- Aplicația trebuie să permită căutarea documentelor după cuvinte-cheie.
- Aplicația trebuie să permită vizualizarea detaliilor unui document.
- Aplicația trebuie să permită descărcarea documentelor pentru vizualizare.
- Aplicația trebuie să permită vizualizarea istoricului versiunilor unui document. ● Aplicația trebuie să permită încărcarea de documente noi.
- Aplicația trebuie să permită actualizarea documentelor existente, în funcție de drepturile utilizatorului.
- Aplicația trebuie să permită ștergerea documentelor, dacă utilizatorul are drepturi.
- Aplicația trebuie să permită atașarea de fișiere suplimentare la un document existent.

- Aplicația trebuie să permită adăugarea și modificarea metadatelor asociate documentelor.
- Aplicația trebuie să permită vizualizarea documentelor aflate în flux de aprobare.
- Aplicația trebuie să permită aprobarea sau respingerea documentelor.
- Aplicația trebuie să permită adăugarea de comentarii în cadrul fluxului de aprobare.
- Aplicația trebuie să permită vizualizarea istoricului acțiunilor din workflow.
- Aplicația trebuie să trimită notificări utilizatorului atunci când are documente în așteptare.
- Aplicația trebuie să ofere notificări push pentru:
  - documente noi alocate utilizatorului;
  - documente respinse;
  - documente aprobate;
  - modificări importante asupra documentelor urmărite.
- Aplicația trebuie să permită configurarea tipurilor de notificări primite.
- Aplicația trebuie să permită dezactivarea notificărilor în funcție de preferințele utilizatorului.
- Aplicația trebuie să permită scanarea documentelor folosind camera dispozitivului.
- Aplicația trebuie să permită încărcarea imaginilor și conversia acestora în PDF.
- Aplicația trebuie să permită partajarea internă a documentelor prin generarea de link-uri securizate.
- Aplicația trebuie să permită marcarea documentelor ca „favorite”.
- Aplicația trebuie să permită accesul rapid la documentele recent vizualizate.
- Aplicația trebuie să permită descărcarea temporară a documentelor pentru acces offline.
- Aplicația trebuie să utilizeze conexiuni securizate (HTTPS/TLS).
- Aplicația trebuie să cripteze datele sensibile stocate local.
- Aplicația trebuie să implementeze mecanisme de timeout automat al sesiunii.
- Aplicația trebuie să permită ștergerea automată a datelor locale la deconectare.
- Aplicația trebuie să încarce lista de documente într-un timp optim.
- Aplicația trebuie să gestioneze eficient fișiere de dimensiuni mari.
- Aplicația trebuie să optimizeze traficul de date prin paginare și încărcare progresivă (lazy loading).
- Aplicația trebuie să înregistreze toate acțiunile utilizatorului relevante (vizualizare, modificare, aprobare, ștergere).
- Aplicația trebuie să transmită logurile către sistemul central de audit al DMS-ului.

- Aplicația trebuie să respecte politicile interne privind retenția datelor și auditul.
- Aplicația trebuie să ofere o interfață intuitivă și adaptată dispozitivelor mobile.
- Aplicația trebuie să permită utilizarea în mod portrait și landscape. ● Aplicația trebuie să respecte identitatea vizuală a organizației.
- Aplicația trebuie să ofere mesaje clare de eroare și confirmare a acțiunilor.
- Ofertantul devenit prestator va trebui sa gestioneze tot procesul de publicare ca privata, actualizare conform politicilor Google, Apple, etc.

4.6 Arhitectură hardware/cloud

Sistemul informatic va fi proiectat utilizând principii de arhitectură de tip CLOUD NATIV (modularitate, separarea componentelor, portabilitate și scalabilitate controlată), respectiv operaționalizat în Cloudul Privat Guvernamental (CPG), proiectat astfel încât să permită, în măsura compatibilității tehnice, migrarea către alte medii de tip cloud, public sau privat, în caz de necesitate.

Conceptul de cloud-native, în contextul prezentului proiect, se referă la proiectarea aplicației astfel încât să permită modularitate, separarea componentelor, portabilitate între medii cloud, precum și scalare controlată și reziliență, în limitele capabilităților tehnice și operaționale ale platformei Cloudului Privat Guvernamental.

Informații referitoare la componenta de Cloud Guvernamental

Prezentăm mai jos câteva informații referitoare la componenta de Cloud Guvernamental, mai multe informații, inclusiv toate specificațiile tehnice de conectare/accesare, urmând a fi puse la dispoziția prestatorului în cadrul etapei de analiză și proiectare:

- Autoritatea pentru Digitalizarea României (ADR) este responsabilă pentru implementarea, coordonarea și guvernanța proiectului Cloudului Guvernamental.
- Platforma **tehnică:** Componenta de Cloud Dedicat a Cloudului Privat Guvernamental este bazată pe tehnologia Microsoft Azure Stack Hub. Sistemul informatic trebuie să fie complet compatibil cu această platformă..
- **Licențe COTS - regim BYOL:** Licențele de tip Commercial off-the-shelf (COTS), care vor fi utilizate de către sistemul informatic, trebuie să fie achiziționate, furnizate și incluse în oferta Prestatorului, **prin intermediul prezentului contract**, în numele și pentru tenant (instituția care dezvoltă/deține sistemul informatic), în regim Bring Your Own License (BYOL);
- **Imagini și compatibilitate:** Se recomandă utilizarea imaginilor oficiale din **Azure Marketplace**, pentru a asigura compatibilitatea testată cu Azure (https://learn.microsoft.com/en-us/azure-stack/operator/azure-stack-marketplace-azure-items?view=azs-2408) sau compatibilitatea cu Microsoft Azure Stack Hub să fie certificată de către producător / furnizor;
- În cazul utilizării unor imagini din surse externe, responsabilitatea pentru compatibilitate, securitate și funcționare revine integral tenantului.

- **Dimensionarea mașinilor virtuale:** Mașinile virtuale utilizate de sistemul informatic vor fi dimensionate în conformitate cu specificațiile oficiale Azure https://learn.microsoft.com/en-us/azure-stack/user/azure-stack-vm-considerations?view=azs-2408&tabs=az1%2Caz2#vm-sizes .
- **Portabilitate și migrare:** Arhitectura aplicației va permite migrarea controlată a componentelor sistemului către alte medii cloud publice sau private, în caz de necesitate, utilizând mecanisme standardizate (ex.: șabloane declarative, imagini compatibile, containere conforme OCI), fără dependențe critice de servicii proprietare care nu pot fi replicate sau înlocuite în alte medii. Portabilitatea se referă la nivelul aplicației și al resurselor virtualizate, în limitele compatibilității platformelor țintă.

Caracteristici tehnice și parametri specifici

Aplicațiile vor fi proiectate și dezvoltate pentru a fi găzduite în mediu cloud, utilizând resurse virtualizate, sub formă de mașini virtuale și/sau containere, care găzduiesc servicii sau componente funcționale distincte (ex. servicii sau microservicii).

Sistemul informatic va fi compatibil din punct de vedere tehnic cu servicii de stocare în cloud (ex. stocare obiect, arhivare, backup), permițând integrarea cu furnizori de servicii cloud conform standardelor deschise și cu serviciile de stocare disponibile în CPG.

Sistemul informatic va fi compatibil din punct de vedere tehnic cu servicii de baze de date găzduite în medii cloud, permițând utilizarea și integrarea acestora în conformitate cu standardele deschise și cu capabilitățile platformei CPG.

Nu vor fi achiziționate echipamente hardware dedicate, infrastructura necesară fiind asigurată prin serviciile de tip IaaS disponibile în cadrul Cloudului Privat Guvernamental.

Ofertanții trebuie să includă în ofertă toate componentele necesare pentru operaționalizarea, administrarea și securizarea aplicațiilor în Cloudul Privat Guvernamental, inclusiv resursele de infrastructură, licențele software, precum și orice componente suplimentare necesare (de exemplu: tehnologii de virtualizare, containerizare, orchestrare sau monitorizare), pentru o perioadă de minimum 36 de luni de la finalizarea implementării, în conformitate cu arhitectura și specificul soluției tehnice propuse.

Implementarea sistemului informatic trebuie să asigure performanța, scalabilitatea, disponibilitatea și securitatea aplicațiilor, prin utilizarea unor mecanisme adecvate de alocare și dimensionare a resurselor (CPU, memorie, stocare), monitorizare, backup, precum și mecanisme de asigurare a continuității operaționale.

Elasticitate și Scalabilitate

- Sistemul va permite adăugarea sau eliminarea resurselor de calcul (mașini virtuale, containere) și de a ajusta resursele existente (CPU, memorie) în funcție de cerere.

Auto-scaling

- Mecanismele de scalare vor fi implementate în funcție de capabilitățile platformei și ale soluției tehnice propuse.
- Mecanismele de scalare automată vor fi implementate în limitele capabilităților platformei și ale soluției tehnice propuse.

- Funcționalitățile de auto-scaling vor fi utilizate în măsura în care sunt compatibile cu platforma Cloudului Privat Guvernamental (Azure Stack Hub).
- Pentru componentele care nu beneficiază de auto-scaling nativ, ofertantul va implementa mecanisme alternative de scalare (manuală controlată sau automată orchestrată, la nivel de mașini virtuale sau containere), pe baza unor metrici de performanță definite (ex. utilizare CPU, memorie, latență, număr de cereri).

Reziliență și Disponibilitate

- Failover: mecanism prin care, în cazul indisponibilității unei componente, o altă componentă preia automat funcționalitatea acesteia, asigurând continuitatea serviciilor.

Replicare și redundanță

- Stocarea datelor în mai multe locații pentru a asigura continuitatea serviciului în caz de defecțiuni hardware sau software.

Securitate

- Controlul accesului și autentificare: Implementarea mecanismelor de control acces și autentificare pentru a proteja resursele și datele.
- Criptare: Utilizarea criptării pentru a proteja datele în tranzit și în repaus.
- Monitorizare și audit: Sistemele de monitorizare și audit pentru detectarea și răspunsul la incidentele de securitate.

Observabilitate și Monitorizare

- Colectarea și analizarea metricilor de performanță și a logurilor pentru a detecta problemele și pentru a asigura funcționarea optimă.

Alerte și notificări

- Configurarea alertelor pentru evenimente critice și notificarea echipelor responsabile in timp real.

Stocare:

- Capacitatea de stocare disponibilă și tipurile de stocare utilizate (SSD, HDD).
- Backup și restaurare: Strategii de backup și proceduri de restaurare pentru a proteja datele și pentru a asigura recuperarea rapidă în caz de dezastru.

Integrare și Interoperabilitate

- Arhitectura soluției va permite integrarea cu sisteme externe relevante, în măsura în care acest lucru este necesar pentru funcționarea aplicației și este compatibil cu infrastructura Cloudului Privat Guvernamental.
- Integrarea se va realiza prin mecanisme standardizate (API, servicii web, protocoale securizate), fără introducerea unor dependențe de platforme sau servicii care nu pot fi implementate în cadrul Cloudului Guvernamental.
- Integrarea cu sisteme externe se va realiza fără afectarea securității, performanței sau conformității cu cerințele Cloudului Guvernamental.

Utilizarea platformei cloud

- Soluția va utiliza capabilitățile platformei Azure Stack Hub pentru operarea în cadrul Cloudului Guvernamental.
- Arhitectura generală a soluției este concepută pentru a opera într-un mediu eterogen, în care coexistă multiple platforme de infrastructură și de containerizare. În mod particular, platforma trebuie să asigure integrarea cu tehnologii utilizate frecvent în sectorul public, inclusiv platforme cloud bazate pe tehnologii open- source
- Integrarea nu se limitează la simple conexiuni de rețea, ci trebuie să permită administrarea unificată a resurselor, aplicarea de politici comune și operarea într-un mod coerent la nivelul identității, politicilor de securitate, monitorizării centralizate și guvernanței operaționale, asigurând vizibilitate și control unitar asupra resurselor gestionate, indiferent de platforma subiacentă.

Arhitectura va permite:

- utilizarea mecanismelor de definire a resurselor pe bază de șabloane (de tip ARM templates sau echivalent), pentru:
  - mașini virtuale,
  - rețele virtuale, gateway-uri, load balancere,
  - servicii de stocare (blob, file, queue etc.);
- integrarea cu serviciile de identitate existente (ex. integrare cu un director de tip Active Directory), astfel încât autentificarea și autorizarea să fie gestionate unitar;
- folosirea facilităților locale de backup și restaurare, precum și integrarea cu soluții externe pentru protecția datelor;
- expunerea de mecanisme de monitorizare și raportare a consumului de resurse, astfel încât datele colectate din mediul Azure Stack să poată fi corelate cu restul infrastructurii gestionate de platformă.

Soluția nu va introduce dependențe de servicii sau tehnologii care nu pot fi implementate în cadrul Cloudului Privat Guvernamental, asigurând portabilitatea și sustenabilitatea pe termen lung.

4.6.1 Platformă Cloud

Arhitectura sistemului informatic va include două noduri, unul activ și unul pasiv, configurate pentru redundanță și disponibilitate ridicată (high availability).

Fiecare nod trebuie să conțină componente precum:

- load balancere redundante,
- servere de aplicație,
- cluster pentru căutări rapide și distribuite
- cluster pentru baze de date.

Nodul Activ: Este nodul principal care va gestiona sarcina curentă a aplicației, răspunzând solicitărilor venite de la utilizatori.

Nodul Pasiv: Acesta va funcționa ca rezervă și va prelua toate operațiunile în cazul în care nodul activ devine indisponibil. Acest mecanism va ajuta la asigurarea unei disponibilități ridicate și la reducerea timpului de nefuncționare.

Load Balancers: Sunt responsabile pentru distribuirea uniformă a cererilor către serverele de aplicație pentru a preveni supraîncărcarea unui singur server. Acestea sunt configurate în mod redundant pentru a asigura continuitatea în cazul unei defecțiuni.

Serverele de Aplicație: 2 per nodul activ) și 2 per nodul pasiv găzduiesc aplicațiile externe care servesc utilizatorii. Serverele sunt organizate astfel încât să răspundă la solicitările utilizatorilor, având configurații redundante în nodul pasiv pentru failover.

Cluster căutări rapide și distribuite: Reprezintă un grup de noduri responsabile pentru indexarea și căutarea datelor în sistem. Componenta va fi implementată utilizând o tehnologie consacrată, capabilă să asigure indexare performantă, scalabilitate și reziliență. Ofertantul va specifica tehnologia propusă, mecanismele de replicare, cerințele de resurse și modul de integrare cu restul arhitecturii. Acesta este folosit pentru a furniza rezultate rapide la căutări și pentru a permite o analiză avansată a datelor. Fiind distribuit între mai multe mașini virtuale, clusterul poate gestiona volume mari de date și asigură redundanță în caz de defecțiune.

Clusterul de baze de date reprezintă componenta responsabilă pentru stocarea datelor persistente ale sistemului. Acesta este configurat într-o arhitectură redundantă, pentru a asigura continuitatea datelor și recuperarea în caz de eșec.

Clusterul va utiliza mecanisme de replicare controlată (primary-replica), sincronă sau asincronă, în funcție de tehnologia aleasă, fiind accesibil componentelor aplicației în mod controlat și asigurând continuitatea operațională în scenarii de failover.

Fluxul general al sistemului:

- Traficul către aplicație este direcționat de serverul DNS către unul dintre load balancere.
- Load balancerul distribuie cererile către serverele de aplicație disponibile (în nodul activ), care gestionează logica aplicației și răspund solicitărilor.
- Serverele de aplicație interacționează cu clusterul pentru căutarea și indexarea datelor și cu clusterul de baze de date pentru operațiuni de stocare și gestionare a datelor.
- În cazul unei defecțiuni a nodului activ, nodul pasiv preia automat toate funcționalitățile, iar mecanismele de failover (load balancer și health checks) redirecționează traficul către nodul pasiv. DNS-ul este actualizat conform politicilor de TTL configurate, pentru a asigura continuitatea serviciului.

Arhitectura logică a platformei este construită pe un model stratificat, care separă clar responsabilitățile funcționale și permite extinderea, operarea și mentenanța soluției într-un mod predictibil și modular. Fiecare strat îndeplinește un rol specific, dar interacționează cu celelalte prin interfețe standardizate, asigurând interoperabilitate și scalabilitate pe termen lung.

Modelul este inspirat din bune practici pentru arhitecturi cloud-native, enterprise-grade și din standardele de proiectare a sistemelor complexe utilizate la nivel internațional.

Stratul de interfață reprezintă punctul unic de acces pentru utilizatori și administratori, oferind o experiență coerentă, intuitivă și adaptată rolurilor organizaționale. Acesta asigură:

- acces centralizat la resurse, servicii, procese și instrumente operaționale;
- vizualizări agregate ale infrastructurilor multi-cloud, resurselor și aplicațiilor;
- fluxuri de aprobare și control organizate pe roluri și politici interne;
- afișarea stării infrastructurii, consumului de resurse, costurilor și alertelor;
- acces securizat, diferențiat pe profiluri (administratori, operatori, dezvoltatori, utilizatori finali);
- suport pentru acces prin browser web modern, cu interfață responsivă.

Obiectivul acestui strat este de a simplifica operarea, de a oferi transparență și de a reduce timpul necesar efectuării sarcinilor administrative.

Stratul de orchestrare și execuție reprezintă nucleul operațional al platformei, fiind responsabil de coordonarea tuturor proceselor informatice și de execuția acțiunilor asupra infrastructurii. Componenta include:

- interpretarea fluxurilor declarative de orchestrare;
- aplicarea politicilor configurate la fiecare pas operațional;
- rularea acțiunilor secvențiale, paralele sau condiționate;
- automatizarea ciclului de viață al aplicațiilor și resurselor;
- mecanisme de tranzacționare operațională (retry, rollback, validare);
- execuție controlată a proceselor în mediile configurate, în limitele platformelor suportate..

Acest strat permite instituției să implementeze un model operațional standard, reproducibil și auditat, reducând dependența de procese manuale și riscul de eroare umană.

Stratul de observabilitate oferă capacitatea de a monitoriza, analiza și diagnostica toate operațiunile platformei și comportamentul resurselor gestionate. Acesta:

- colectează unificat metrici, loguri și trasări distribuite;
- corelează automat datele pentru identificarea rapidă a incidentelor;
- asigură mecanisme de alertare multi-canal;
- oferă analize predictive pentru capacitate, disponibilitate și performanță.

Scopul acestui strat este creșterea transparenței operaționale și reducerea semnificativă a timpului de remediere a incidentelor.

Stratul de stocare si persistenta gestionează datele, configurațiile și metadatele platformei, oferind:

- provisioning dinamic al volumelor de stocare;
- snapshot-uri automate pentru protecția datelor;
- backup-uri conforme politicilor instituției;
- replicare cross-site pentru continuitate operațională.

Acest strat asigură integritatea și disponibilitatea datelor esențiale și permite operarea în scenarii multi-site sau cu cerințe ridicate de reziliență.

Această arhitectură este proiectată pentru disponibilitate ridicată, reziliență și toleranță la erori, utilizând componente redundante pentru a minimiza impactul eventualelor defecțiuni asupra utilizatorilor finali.

Mai jos este reprezentată arhitectura generică minimală a platformei cloud. Ofertanții vor dimensiona si scala necesarul de resurse in funcție de arhitectura si necesarul soluției software ofertate pentru a asigura funcționarea conformă si îndeplinirea tuturor cerințelor din prezentul Caiet de sarcini.

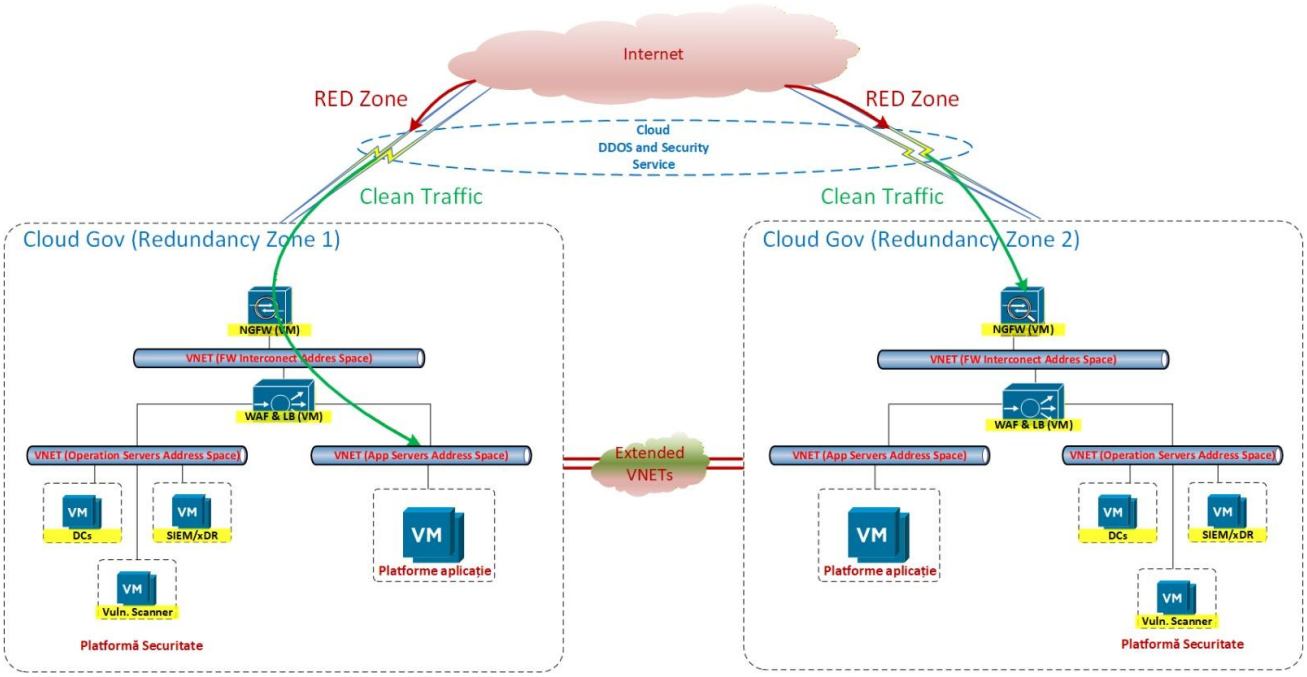


Figura 1 - Arhitectura generică minimală platformă cloud

Dimensionarea componentelor funcționale și a celor de suport trebuie să asigure minimul de resurse de procesare după cum urmează:

Tabel 4 - Dimensionarea componentelor

Nr. crt.	Componentă	Nr. VM	Rol	CPU / VM	RAM / VM	Storage / VM
1	Aplicație DMS	2	Active + Passive	6 vCPU	12 GB	300 GB SSD
2	Aplicatie Portal (intern + extern)	2	Active + Passive	6 vCPU	12 GB	300 GB SSD
3	Bază de date (DB)	2	Primary + Replica	6 vCPU	24 GB	1 TB SSD
4	BI (Business Intelligence)	2	Active + Passive	6 vCPU	12 GB	150 GB SSD
5	LMS	1	Standalone	3 vCPU	6 GB	100 GB SSD

Nr. crt.	Componentă	Nr. VM	Rol	CPU / VM	RAM / VM	Storage / VM
6	Tur virtual 3D	1	Standalone	6 vCPU	12 GB	300 GB SSD
7	Chatbot	1	Standalone	4 vCPU	8 GB	50 GB SSD
8	Servicii auxiliare	2	Procesare	3 vCPU	6 GB	100 GB SSD
9	Resurse cache	2	Cache + sesiuni	4 vCPU	8 GB	50 GB SSD
10	Load Balancer	2	Routing trafic	2 vCPU	2 GB	15 GB SSD
11	Monitoring	1	Observabilitate	2 vCPU	4 GB	15 GB SSD
12	Web Application Firewall (WAF) Enterprise	2	WAF	8 vCPU	16 GB	15 GB SSD
13	Cloud Firewall	2	Firewall Perimetru	1 vCPU	2 GB	32 GB SSD
14	Soluție SIEM	1	Nod central (mgmt + analiză)	8 vCPU	16 GB	500 GB SSD
		1	Nod colectare / indexare	4 vCPU	16 GB	250 GB SSD
15	Scanner extern de vulnerabilități	1	Scaner Vulnerabilități	4 vCPU	16 GB	30 GB SSD
16	Soluție tip MDR Plus	1	MDR	4 vCPU	16 GB	30 GB SSD
17	Identity and Access Management (IAM), platforma security	3	Cluster security	8 vCPU	32 GB	300 GB SSD

Estimarea specificațiilor de mai sus a fost realizată în baza arhitecturii generice din figura 2. Specificațiile tehnice reflectă viziunea proiectantului asupra cerințelor minime ale sistemului și pot varia în funcție de arhitectura tehnică a soluției propuse de ofertant.

Nivelul de detaliere a componentelor este diferențiat în mod intenționat: resursele infrastructurale (mașini virtuale, CPU, RAM, stocare) sunt definite explicit, în vederea asigurării predictibilității și comparabilității ofertelor, în timp ce elementele de orchestrare, integrare multi-platformă și operare sunt prezentate la nivel conceptual, pentru a permite ofertanților flexibilitate în definirea soluției tehnice optime.

Ofertantul are obligația de a detalia în propunerea tehnică modul concret de implementare a acestor componente și concepte, precum și modul în care soluția propusă asigură îndeplinirea cerințelor funcționale și nefuncționale ale sistemului.

Ofertanții vor dimensiona, instala si configura mediul de Disaster Recovery (DR) în regim activ-pasiv, complet separat de mediul de producție, dimensionat corespunzător astfel încât să asigure funcționarea integrală a aplicațiilor și serviciilor critice în scenariu de failover, fără degradări majore de performanță. Dimensionarea se va realiza pe baza specificațiilor hardware ale mediului de producție furnizate mai sus. Toate componentele software (sisteme de operare, baze de date, aplicații middleware etc.) vor fi licențiate corespunzător pentru scenariul activ-pasiv, cu respectarea politicilor producătorilor..

Ofertantul este responsabil pentru analiza necesarului de resurse, furnizarea licențelor, implementarea și documentarea arhitecturii DR, precum și pentru demonstrarea fezabilității soluției prin testarea planului de disaster recovery.

Ofertantul va include în cadrul propunerii tehnice și financiare toate resursele necesare pentru operarea aplicației într-un mediu cloud pentru o perioadă de 36 de luni de la finalizarea implementării sistemului.

Aceasta va include, fără a se limita la:

- resurse de computing (mașini virtuale / instanțe cloud) necesare rulării aplicațiilor;
- resurse de stocare persistentă pentru baze de date, fișiere și backup;
- servicii de rețea virtuală necesare comunicării interne și externe;
- mecanisme de backup și recuperare în caz de dezastru (Disaster Recovery);
- servicii de monitorizare și administrare a infrastructurii;
- licențe necesare pentru sistemele de operare și alte componente software ale infrastructurii.

Ofertantul va descrie în oferta tehnică infrastructura hardware și componentele logice echivalente utilizate în mediul cloud, inclusiv:

- servere virtuale (VM / compute instances);
- echipamente virtuale de rețea (routere, load balancere, gateway-uri);
- firewall-uri virtuale;
- sisteme de stocare (block storage, object storage);
- mecanisme de backup și replicare.

De asemenea, ofertantul va specifica:

- tipul instanțelor de calcul utilizate (CPU, RAM, disk);
- mecanismele de high availability și fault tolerance;
- modul de segmentare a rețelei (VPC / rețele virtuale);
- modul de protecție și filtrare a traficului (firewall, WAF, IDS/IPS).

Ofertantul va furniza și configura 20 conexiuni VPN IPSec securizate pentru utilizatorii beneficiarului.

Aceste conexiuni vor permite:

- acces securizat la sistem din rețeaua beneficiarului sau din locații externe;
- criptarea traficului de date;
- autentificare securizată a utilizatorilor.

Soluția VPN va include:

- gateway VPN dedicat;
- configurarea tunelurilor IPSec;
- managementul accesului utilizatorilor;
- posibilitatea extinderii numărului de conexiuni dacă este necesar.

Infrastructura trebuie să asigure un nivel ridicat de disponibilitate și continuitate operațională.

Prestatorul va furniza servicii de suport tehnic și mentenanță pentru infrastructura cloud, incluzând:

- monitorizarea continuă a sistemului;
- remedierea incidentelor tehnice;
- actualizarea componentelor infrastructurii;
- optimizarea performanței sistemului.

Suportul tehnic va fi disponibil conform unui SLA (Service Level Agreement) stabilit în contract.

Prestatorul va asigura suport tehnic pentru infrastructura cloud în situațiile în care echipa de suport software escaladează incidente sau probleme tehnice.

Acest suport va include:

- investigarea incidentelor legate de infrastructură;
- diagnosticarea problemelor de performanță;
- intervenții asupra infrastructurii cloud;
- colaborarea cu echipa software pentru remedierea problemelor

4.6.2 Platformă de virtualizare

Soluția dezvoltată și furnizată în cadrul proiectului va utiliza un mediu virtualizat modern, care permite alocarea dinamică și eficientă a resurselor hardware.

Mediul virtualizat trebuie să ofere:

- posibilitatea scalării dinamice a resurselor (CPU, RAM, storage);
- management centralizat al infrastructurii;
- distribuirea sarcinilor între mai multe instanțe;
- mecanisme de auto-scaling și load balancing;

posibilitatea izolării mediilor (ex: dezvoltare, test, producție)

Soluția, va trebui să poată rula sub formă de mașini virtuale sau containere.

Platforma de virtualizare livrată în cadrul proiectului va trebui să suporte următoarele cerințe:.

1. **Suportă Virtualizare de tip Bare Metal**:

- Virtualizare de tip 1, se referă la o metodă de virtualizare în care hipervizorul este instalat direct pe hardware-ul fizic al serverului, fără a necesita un sistem de operare gazdă intermediar. Acest tip de virtualizare oferă performanțe superioare și eficiență, deoarece hipervizorul controlează direct resursele hardware și gestionează mașinile virtuale (VM-uri).

2. **Suport pentru Multiple Sisteme de Operare**:

- Permită rularea mai multor sisteme de operare invitate (guest) pe același hardware fizic, inclusiv distribuții Linux, Windows, BSD, CentOS și altele.

3. **Performanță și Scalabilitate**:

- Utilizează funcționalități avansate ale CPU-urilor moderne pentru a asigura performanțe aproape native pentru VM-uri.
- Suportă scalarea pe sisteme multiprocesor și gestionează eficient resursele pentru un număr mare de VM-uri.

4. **Securitate**:

- Fiecare VM rulează într-un mediu izolat, utilizând caracteristici de securitate pentru a asigura protecția datelor și resurselor.

5. **Administrare și Management**:

- Oferă instrumente de administrare atât prin linie de comandă, cât și prin interfețe grafice, facilitând gestionarea VM-urilor.
- Integrarea cu soluții de management și orchestrare permite suport pentru medii de cloud privat și public.

6. **Stocare și Rețea**:

- Compatibilitatea cu mecanismele de stocare și rețea suportate de platforma Cloudului Privat Guvernamental (Azure Stack Hub), precum și cu formatele standardizate de imagini și volume utilizate în mediile virtualizate moderne.
- Suport pentru mecanisme de virtualizare a rețelei, care să permită conectivitate flexibilă, segmentare logică a rețelei și integrarea cu serviciile de rețea ale platformei.

7. **Snapshot-uri și Backup**:

- Permite crearea de snapshot-uri ale VM-urilor, facilitând backup-ul și restaurarea rapidă în caz de nevoie.

Capabilități operaționale ale soluției:

Platforma trebuie să ofere un set coerent de funcționalități pentru managementul unificat al infrastructurii, aplicațiilor, agenților AI și proceselor operaționale, cu accent pe automatizare, guvernanță și trasabilitate completă.

Funcționalitățile se aplică în mod transversal asupra mediilor on-premises, cloud privat, cloud hibrid și platformelor containerizate.

Platforma trebuie să asigure un mecanism unificat de gestionare a resurselor IT pe care le orchestrează și le provizionează, incluzând infrastructură virtuală, resurse containerizate, servicii de rețea și componente de stocare. Toate resursele create, modificate sau dezafectate prin intermediul platformei vor fi înregistrate, monitorizate și administrate centralizat, pe baza unui model comun.

Platforma va opera cu noțiunea de **resursă gestionată** („managed resource”), însemnând resurse care:

- au fost create, actualizate sau șterse prin platformă (ex. workflow, deployment, integrare Terraform/Kubernetes din platformă); sau
- au fost înrolate explicit în platformă de un operator autorizat (prin import sau API), astfel încât să poată fi urmărite și administrate în continuare.

4.6.2.1 Inventariere și descoperire automată

Platforma trebuie să mențină un inventar centralizat, coerent și actualizat al tuturor resurselor gestionate. Inventarierea se referă atât la resursele nou create, cât și la urmărirea în timp a stării și a caracteristicilor lor tehnice.

Inventarierea automată se va aplica tuturor resurselor gestionate de platformă și va utiliza datele obținute prin mecanisme de orchestrare (ex. Kubernetes, Terraform, API-uri de infrastructură) și metadatele asociate deployment-urilor.

4.6.2.1.1 Descoperire multi-platformă în contextul resurselor gestionate

Platforma va asigura descoperirea și înregistrarea resurselor pe care le gestionează în cadrul infrastructurilor integrate (Kubernetes, ecosisteme cloud sau orchestrări executate prin platformă), fără a pretinde scanare arbitrară a unor medii externe neînrolate.

Soluția trebuie să permită:

- identificarea automată a resurselor create prin intermediul platformei în:
  - clustere Kubernetes/containere orchestrate;
  - infrastructuri definite prin template-uri declarative (ex. Terraform, YAML) rulate prin platformă;
  - componente de infrastructură instanțiate prin workflows;
- maparea fiecărei resurse la:
  - deployment-ul din care provine;
  - workspace-ul asociat.

Platforma va utiliza informațiile expuse de sistemele integrate (ex. API-uri Kubernetes, API-uri ale furnizorilor de infrastructură) doar pentru resursele pentru care a orchestrat sau coordonat direct procesul de creare ori înrolare.

Pentru fiecare resursă gestionată, platforma trebuie să poată citi cel puțin:

- identificatorul nativ al resursei în sistemul subiacent (ex. UID Kubernetes, ID instanță);

- starea raportată de sistem (Running, Pending, Failed, Succeeded etc.);
- resursele alocate (CPU, memorie, stocare, rețea, alte atribute relevante);
- metadate asociate (etichete, adnotări, namespace, cluster etc.).

Această descoperire multi-platformă va fi condiționată de contextul gestionat de platformă, adică numai pentru resurse pe care platforma le creează, le orchestrează sau le urmărește explicit prin intermediul deployment-urilor și workflow-urilor.

4.6.2.1.2 Mecanisme de sincronizare continuă

Platforma trebuie să mențină catalogul de resurse în concordanță cu starea reală a acestora, așa cum este raportată de sistemele tehnice integrate (ex. Kubernetes, infrastructură declarativă orchestrată prin platformă). În acest scop, soluția va implementa mecanisme de sincronizare continuă pentru resursele gestionate.

Platforma va asigura:

- **actualizare automată a stării resurselor**, prin:
  - interogări periodice ale API-urilor infrastructurii pentru resursele gestionate;
  - recepționarea de evenimente sau notificări (acolo unde infrastructura suportă mecanisme reactive – ex. watch în Kubernetes);
  - corelarea răspunsurilor cu resursele din catalog;
- **alinierea metadatelor resurselor**, astfel încât:
  - modificările efectuate în infrastructură asupra resurselor gestionate (ex. restart automat, reschedulare de pod) să fie reflectate în catalog;
  - schimbările de configurare efectuate prin platformă să fie marcate clar ca atare.

Mecanismele de sincronizare trebuie să țină cont de următoarele situații:

1. Resurse modificate direct în infrastructură

Dacă o resursă gestionată este modificată direct în sistemul subiacent (de ex. un operator intervine manual din consola Kubernetes pentru un deployment creat inițial prin platformă), atunci:

- platforma va detecta schimbarea la sincronizare;
- va actualiza metadatele și starea în catalog.

2. Resurse eliminate direct din infrastructură

Dacă o resursă gestionată este ștearsă direct în infrastructură:

- platforma va marca resursa în catalog ca „dispărută din mediul tehnic” la următoarea sincronizare;
- va oferi posibilitatea operatorului de a:
  - șterge înregistrarea din catalog; sau
  - recrea resursa printr-un nou deployment, dacă este cazul.

2. Resurse nou create prin platformă

În momentul în care un workflow sau deployment finalizează provizionarea:

- resursele raportate ca create de infrastructură vor fi înregistrate imediat în catalog;
- legăturile lor cu deployment-ul și workspace-ul asociat vor fi create automat.

Platforma va păstra pentru fiecare resursă informații privind:

- momentul ultimei sincronizări;
- sursa sincronizării (interogare periodică, eveniment push, update din workflow).

4.6.2.2 Management multi-cloud / multi-cluster și administrarea resurselor Kubernetes

Platforma trebuie să asigure un mod unificat de utilizare a infrastructurilor distribuite pe mai multe tehnologii și furnizori (cloud privat, cloud public, infrastructură on-premises, clustere Kubernetes/containere), astfel încât instituția să poată opera întreg ecosistemul digital ca pe un singur ansamblu logic, nu ca pe insule tehnologice separate.

Soluția va permite definirea și înregistrarea centralizată a mai multor **clustere Kubernetes** și folosirea lor ca **ținte de deployment** pentru workload-uri containerizate provizionate prin platformă. În acest model, platforma nu înlocuiește și nu dublează instrumentele native de administrare a clusterelor, ci le folosește ca infrastructuri deja existente, peste care adaugă:

- un registru centralizat de clustere;
- un mod standardizat de a trimite deployment-uri de infrastructură și aplicații către aceste clustere;
- o vizibilitate agregată asupra workload-urilor Kubernetes create prin platformă.

Platforma va oferi un **registru centralizat de clustere**, în care:

- fiecare cluster este definit o singură dată și poate fi reutilizat în mai multe deployment-uri și fluxuri de orchestrare;
- se poate vedea în ce contexte organizaționale (workspaces/proiecte) este folosit fiecare cluster;
- se asigură o separare clară între:
    - instrumentele care creează și administrează clusterele (console native, tool-uri de infrastructură, platforme diverse de virtualizare si orchestratoare de containere)
    - platforma de orchestrare, care folosește aceste clustere ca destinații pentru deployment-urile de infrastructură și aplicații containerizate.

În paralel, platforma va avea capabilitatea să administreze, la nivel logic, **resursele Kubernetes generate prin intermediul ei** (workload-uri containerizate) pe clusterele înregistrate, astfel încât:

- pentru fiecare deployment Kubernetes lansat din platformă să existe o corespondență clară cu:
    - clusterul țintă și namespace-ul utilizat;
    - șablonul declarativ (manifest/Helm) și parametrii folosiți;
    - starea curentă a resurselor (în măsura în care acestea pot fi interogate din cluster);

- operatorii să poată vedea, dintr-un singur punct, **lista workload-urilor containerizate** provizionate prin platformă, filtrate după:
    - cluster și namespace;
    - workspace/proiect/mediu sau serviciu aplicativ.

Administrarea resurselor Kubernetes de către platformă va avea următoarele caracteristici:

- platforma tratează workload-urile Kubernetes ca pe **resurse gestionate declarativ**, create pe baza șabloanelor și a deployment-urilor configurate în platformă;
- platforma permite **vizualizarea și urmărirea stării** pentru resursele Kubernetes provizionate din ea (de exemplu, statusul deployment-urilor, execuția joburilor), fără a pretinde control total asupra tuturor resurselor existente în cluster;
- platforma nu intervine asupra clusterelor sau resurselor Kubernetes care nu sunt asociate deployment-urilor gestionate, respectând astfel responsabilitățile echipelor care administrează direct clusterul.

Prin aceste mecanisme, instituția obține:

- un mod coerent de a decide **„ce aplicăm, unde aplicăm și în ce mediu”**, atunci când vorbim de workload-uri containerizate;
- o hartă clară a relației dintre:
    - clusterele Kubernetes existente,
    - aplicațiile și resursele containerizate provizionate prin platformă;
- un cadru standard în care deployment-urile multi-cloud și multi-cluster sunt orchestrate, urmărite și auditate dintr-un singur punct, cu respectarea rolurilor și responsabilităților din instituție.

4.6.2.3 Managementul workload-urilor containerizate

Platforma va oferi capabilitatea de a gestiona, într-un mod unitar și controlat, **workload-urile containerizate** care rulează pe clustere Kubernetes înregistrate în sistem. Scopul acestui modul este ca instituția să poată defini, lansa, configura și urmări aplicațiile containerizate utilizând procese declarative și standardizate, fără a depinde de intervenții manuale directe în consola clusterelor sau de scripturi punctuale dificil de menținut.

Soluția nu înlocuiește instrumentele native de administrare a clusterelor Kubernetes, ci le completează, concentrându-se pe:

- **definirea și lansarea** workload-urilor containerizate, pe baza unor descrieri declarative reutilizabile;
- **configurarea aplicațiilor** prin ConfigMaps și Secrets gestionate într-un mod centralizat și securizat;
- **monitorizarea stării** workload-urilor create prin intermediul platformei, în contextul mediilor și clusterelor în care acestea rulează.

Prin acest model, platforma tratează workload-urile containerizate ca pe resurse gestionate la nivel de „servicii aplicative”, nu ca pe instanțe izolate. Orice aplicație containerizată implementată prin platformă este:

- definită printr-un set de descrieri declarative;
- asociată clar cu:
  - un cluster și un namespace;
  - un grup, mediu sau proiect instituțional;
- însoțită de informații privind configurația utilizată (ConfigMaps, Secrets) și starea de execuție.

Pentru mediile Kubernetes, platforma va avea rolul de **strat de orchestrare și guvernanță a workload-urilor**, nu de strat de administrare de infrastructură (creare/upgrade de cluster). În mod concret:

- platforma va folosi clustere Kubernetes existente, expuse prin API-urile lor standard;
- deployment-urile vor fi trimise din platformă către aceste clustere, pe baza definițiilor declarative și a parametrilor specificați;
- doar workload-urile create sau gestionate prin platformă vor fi urmărite și prezentate în mod centralizat – restul resurselor existente în cluster vor rămâne în responsabilitatea echipelor care administrează direct infrastructura.

În domeniul **configurării aplicațiilor**, platforma va susține utilizarea:

- **ConfigMaps** pentru configurări nesensibile (parametri de aplicație, endpoint-uri, flags, setări locale);
- **Secrets** pentru valori sensibile (parole, token-uri, chei), integrându-se cu serviciul de tip vault al platformei, astfel încât valorile să nu fie expuse în clar în manifestele sau fișierele de configurare.

Aceste resurse sunt tratate ca parte a modelului operațional al aplicației, nu ca artefacte dispersate:

- sunt asociate explicit cu deployment-urile sau serviciile în care sunt utilizate;
- pot fi versionate sau actualizate în mod controlat, ca parte a unui flux de modificare;
- pot fi gestionate diferit pe medii, respectând separarea credențialelor și a setărilor între DEV/TEST/PREPROD/PROD.

La nivel de **monitorizare a stării workload-urilor**, platforma va oferi o vizualizare centralizată a aplicațiilor containerizate provizionate prin intermediul ei, per:

- mediu (DEV, TEST, PREPROD, PROD);
- cluster și namespace;
- serviciu / aplicație.

Pentru fiecare workload gestionat, platforma va afișa, în măsura în care mediul tehnic permite:

- statusul deployment-ului (în curs de rollout, disponibil, parțial disponibil, etc.);

- sinteza stării pod-urilor (număr de replici dorite vs. replici active, status, etc.);
- informații utile pentru operatori în procesul de diagnosticare și remediere (de exemplu, mesaje de eroare la nivel de rollout, eșec la trimiterea imaginii, lipsa resurselor etc.).

În contextul sectorului public, acest model va aduce următoarele beneficii:

- **standardizare** a modului în care aplicațiile containerizate sunt definite, lansate și configurate, fără practici ad-hoc greu de auditat;
- **trasabilitate** completă asupra cine, când și cu ce parametri a lansat sau modificat un deployment Kubernetes;
- **separarea rolurilor și responsabilităților**: echipele de infrastructură administrează clusterele; echipele de aplicații și operațiuni utilizează platforma pentru a gestiona workload-urile;
- **aliniere la principii DevOps/DevSecOps**, prin integrarea cu pipeline-uri și prin tratamentul declarativ al configurațiilor și secretelor.

4.6.2.3.1 Definirea și lansarea deployment-urilor Kubernetes

Platforma va oferi capabilitatea de a defini și lansa, într-un mod controlat și repetabil, **deployment-uri Kubernetes** către clusterele înregistrate în sistem. Scopul este ca instituția să poată gestiona aplicațiile containerizate pe baza unor descrieri declarative, fără intervenții manuale în consola clusterelor și fără dependență de scripturi ad-hoc dificil de întreținut.

a) Model declarativ pentru workload-uri Kubernetes

Soluția va include un model declarativ prin care deployment-urile Kubernetes sunt descrise pe baza unor fișiere de tip manifest (YAML) sau a unor pachete echivalente (de exemplu, chart-uri Helm sau șabloane echivalente), astfel încât:

- configurația aplicațiilor să fie tratată ca **artefact gestionat**, nu ca operațiune punctuală;
- aceeași definiție de deployment să poată fi utilizată în mai multe medii (DEV/TEST/PREPROD/PROD), cu diferențe controlate doar prin parametri;
- istoricul modificărilor asupra definițiilor (versiuni, autori, date) să poată fi urmărit și auditat.

Platforma va permite:

- înregistrarea și stocarea centralizată a descrierilor de deployment Kubernetes;
- asocierea fiecărei descrieri cu:
  - un nume unic al serviciului sau aplicației;
  - versiunea configurației.

b) Selectarea clusterului, a namespace-ului și a mediului

La lansarea unui deployment Kubernetes, platforma va permite operatorului să specifice în mod explicit:

- **clusterul țintă**, selectat din lista de clustere înregistrate;
- **namespace-ul** în care va rula aplicația;

Platforma va oferi mecanisme prin care se asigură că:

- un deployment de tip producție nu este lansat accidental într-un mediu de test (sau invers);
- există o corespondență clară între:
    - obiectul de configurare (descrierea de deployment);
    - mediul pentru care este utilizat;
    - clusterul și namespace-ul în care a fost implementat.

Acest model va reduce riscul erorilor operaționale și permite maparea clară a aplicațiilor la mediile și clusterele în care rulează.

c) Parametrizare și valori pentru deployment

Platforma va permite parametrizarea deployment-urilor Kubernetes, astfel încât aceeași definiție de bază să poată fi utilizată în mai multe contexte, schimbând doar seturile de valori. În acest sens, platforma va:

- permite definirea de **parametri de configurare** (ex. imagini de container, resurse CPU/memorie, endpoint-uri externe, nume de secrete, număr de replici);
- permite asocierea de **seturi de valori** per mediu (de exemplu, un fișier sau un profil de valori pentru DEV, altul pentru PROD);
- permite utilizarea valorilor sensibile (parole, token-uri, chei) prin integrarea cu serviciul de tip *vault*, fără a expune aceste valori în clar în manifestele stocate.

La momentul lansării deployment-ului, platforma va combină:

- descrierea declarativă a deployment-ului;
- parametrii și valorile asociate mediului și workspace-ului;
- secretele și variabilele sensibile obținute din serviciul de tip vault (acolo unde este cazul);

și va genera o configurație completă, pregătită pentru a fi aplicată în clusterul țintă.

d) Lansarea deployment-urilor și controlul execuției

Platforma va permite inițierea deployment-urilor Kubernetes prin:

- interfața grafică, unde operatorul:
    - selectează aplicația/deployment-ul;
    - alege mediul, clusterul și namespace-ul;
    - verifică parametrii și valorile asociate;
- API-ul expus, care permite:
    - integrarea cu pipeline-uri de tip CI/CD;
    - declanșarea automată a deployment-urilor ca parte din fluxuri de orchestrare mai complexe.

În momentul lansării, platforma va:

- valida configurația (de exemplu, va verifica prezența parametrilor obligatorii și a referințelor către secrete);
- transmite manifestele către clusterul Kubernetes țintă, utilizând mecanismele standard ale acestuia;
- înregistra în jurnalul intern de execuție:
    - cine a inițiat deployment-ul;
    - când a fost inițiat;
    - ce versiune de configurare a fost utilizată;
    - ce cluster și namespace au fost vizate.

Astfel, fiecare deployment va deveni un eveniment controlat, urmărit și auditabil, nu doar o comandă punctuală executată de pe stația unui operator.

e) Urmărirea statusului deployment-urilor lansate prin platformă

Platforma va avea capabilitatea să urmărească starea deployment-urilor Kubernetes **create prin intermediul ei**, astfel încât:

- pentru fiecare deployment lansat, platforma va putea interoga periodic sau la cerere clusterul țintă pentru a determina:
    - dacă resursele au fost create cu succes;
    - dacă există erori în procesul de rollout (de exemplu, pod-uri în stare de crashloop);
    - câte replici sunt active și sănătoase;
- informațiile de status trebuie să fie prezentate într-o formă agregată:
    - pe deployment (aplicație);
    - pe mediu;
    - pe cluster și namespace.

Această capabilitate va fi limitată la resursele și deployment-urile pe care platforma le-a creat sau le gestionează. Platforma nu va intervini și nu va raporta în mod automat asupra resurselor Kubernetes care nu au fost provizionate prin ea, respectând astfel separarea responsabilităților.

f) Beneficii operaționale pentru instituție

Prin introducerea unui mecanism standardizat pentru definirea și lansarea deployment-urilor Kubernetes, platforma va:

- reduce dependența de comenzi manuale, scripturi locale și cunoștințe punctuale de administrare a clusterelor;
- asigura **repetabilitatea** deployment-urilor între medii și clustere, folosind aceleași definiții și aceleași procese;
- oferi trasabilitate completă asupra:
    - cine a lansat un deployment;
    - ce versiune a aplicației a fost implementată;

- în ce cluster și mediu rulează aplicația;

- facilita integrarea cu practicile DevOps și CI/CD, prin API-uri standard pentru lansarea deployment-urilor ca parte din pipeline-uri automatizate.

4.6.2.3.2 ConfigMaps, Secrets și configurarea aplicațiilor

Platforma trebuie să aibă capabilitatea să gestioneze, într-un mod centralizat și controlat, **configurarea aplicațiilor containerizate și a funcțiilor serverless** care sunt implementate pe clustere Kubernetes înregistrate în sistem. Accentul este pus pe:

- definirea parametrilor de configurare direct din interfața platformei;
- utilizarea mecanismelor standard Kubernetes (inclusiv ConfigMaps și Secrets) la nivel de aplicatie, fără a necesita intervenții manuale sau scripturi ad-hoc din partea operatorilor.

Platforma nu își propune să înlocuiască toate instrumentele native Kubernetes pentru administrarea ConfigMaps și Secrets, ci să ofere un **mod unitar, sigur și auditabil** de a configura aplicațiile și funcțiile care sunt lansate prin intermediul ei.

a) Configurarea aplicațiilor containerizate

Platforma va oferi o interfață prin care operatorii pot configura aplicațiile containerizate gestionate, astfel încât:

- să poată fi definite principalele caracteristici ale aplicației, cum ar fi:
  - imaginea containerului care va fi utilizată;
  - parametrii de rulare (de exemplu, anumite argumente sau valori de configurare);
  - resursele minime și maxime (cereri și limite de CPU/memorie), acolo unde este cazul;
- să poată fi asociate configurații specifice fiecărui mediu (DEV/TEST/PREPROD/PROD), fără a dubla inutil definițiile de bază ale aplicației;
- să existe o mapare clară între:
  - aplicația definită în platformă;
  - clusterul și namespace-ul în care va fi executată;
  - setul de configurări logice asociate acestei aplicații.

Configurarea este tratată ca parte a modelului operațional al aplicației: atunci când un operator selectează o aplicație pentru deployment, platforma îi pune la dispoziție valorile de configurare relevante pentru mediu și context, astfel încât procesul de lansare să fie repetabil și controlat.

Chiar dacă detaliile de implementare la nivel de cluster (inclusiv ConfigMaps și alte resurse native) sunt gestionate efectiv de Kubernetes, **centrarea configurării la nivelul platformei** va permite:

- reducerea erorilor manuale;
- consolidarea cunoașterii într-un singur punct;
- auditarea deciziilor de configurare.

b) Configurarea și execuția funcțiilor serverless

Platforma va include capabilitatea de a lucra cu un **framework de tip function-as-a-service (FaaS)** integrat cu Kubernetes, permițând:

- definirea funcțiilor serverless pe baza unor **imagini container** furnizate de operatori sau de echipele de dezvoltare;
- adăugarea acestor imagini în platformă, împreună cu metadate relevante (nume funcție, descriere, mediu țintă, parametri de execuție);
- execuția funcțiilor serverless direct din interfața platformei, prin invocarea lor controlată, în scop de:
    - testare funcțională;
    - execuții operaționale programate sau manuale;
    - automatizare a unor pași specifici în fluxuri mai mari de orchestrare.

Platforma va permite:

- execuția funcțiilor serverless;
- definirea unor parametri de intrare pentru funcții, acolo unde acest lucru este suportat, și reutilizarea acestor funcții în mai multe scenarii operaționale.

c) Relația cu ConfigMaps și Secrets la nivel de cluster

Deși platforma nu va expune în interfață un modul dedicat pentru gestionarea tuturor resurselor de tip ConfigMap și Secret din clustere, modelul de configurare folosit va fi compatibil cu practicile Kubernetes standard:

- configurările definite în platformă vor putea fi transpuse, atunci când este cazul, în resurse native la nivel de cluster (ConfigMaps, Secrets, variabile de mediu), prin mecanismele de deployment existente;
- aplicațiile și funcțiile gestionate prin platformă vor putea consuma valori care, la nivel de cluster, ajung să fie reprezentate în ConfigMaps și Secrets;
- responsabilitatea gestionării detaliate a acestor resurse va rămâne la echipele care administrează clusterele, în timp ce platforma va oferi un strat de **abstracție și control** asupra configurării logice a aplicațiilor.

Această abordare va asigura:

- compatibilitate cu politicile de securitate și administrare deja implementate în cadrul instituției;
- posibilitatea ca echipele de infrastructură să utilizeze în continuare instrumentele consacrate pentru Kubernetes;
- reducerea curbei de învățare pentru echipele funcționale, care pot lucra cu modele de configurare la un nivel mai apropiat de aplicație, nu de infrastructură.

d) Guvernanță și trasabilitate a modificărilor de configurare

Orice modificare de configurare realizată prin platformă asupra aplicațiilor containerizate va fi:

- asociată cu utilizatorul (sau procesul) care a inițiat modificarea;

- corelată cu mediul, clusterul și contextul în care această configurare este utilizată;
- înregistrată în jurnalul de audit al platformei, astfel încât să poată fi reconstituit istoric:
    - ce valori sau parametri au fost utilizați la momentul unei anumite implementări;
    - cine a efectuat schimbările de configurare;
    - ce efect a avut schimbarea (de exemplu, declanșarea unui nou deployment).

Acest nivel de trasabilitate este esențial în contextul sectorului public, unde:

- schimbările de configurare trebuie să poată fi explicate și justificate;
- impactul asupra serviciilor critice trebuie evaluat;
- conformitatea cu politicile interne și cu reglementările externe trebuie demonstrată.

Prin modul în care gestionează configurarea aplicațiilor containerizate și a funcțiilor serverless, platforma va permite instituției:

- să standardizeze modul de definire și aplicare a configurărilor în medii Kubernetes, fără a expune direct operatorii la toate detaliile tehnice ale clusterelor;
- să reducă riscul de erori cauzate de diferențe nesistematice între medii (DEV/TEST/PREPROD/PROD), prin utilizarea unui model comun de configurare;
- să utilizeze funcții serverless în scenarii operaționale și de automatizare, fără a necesita cunoștințe detaliate despre framework-ul tehnic de execuție;
- să mențină controlul și trasabilitatea asupra configurațiilor, într-un mod compatibil cu cerințele de audit și conformitate specifice sectorului public.

4.6.2.3.3 Monitorizarea stării workload-urilor containerizate

Platforma va avea capabilitatea să ofere o **vizibilitate centralizată asupra stării și consumului de resurse** pentru workload-urile containerizate implementate pe clusterele Kubernetes înregistrate. Monitorizarea este orientată în special către:

- utilizarea resurselor (CPU, memorie) la nivel de workload;
- eficiența alocării resurselor (requests vs. utilizare efectivă);
- estimarea și analiza costurilor asociate rulării workload-urilor;
- corelarea acestor informații cu mediile, proiectele și spațiile organizaționale (workspace-uri) ale instituției.

Soluția nu își propune să substituie complet sistemele de monitorizare infrastructurală existente, ci să ofere un **mod unificat, integrat în platformă**, de a urmări comportamentul workload-urilor containerizate gestionate prin ea, din perspectiva:

- utilizării resurselor și costurilor;
- identificării zonelor de supra-alocare sau sub-utilizare;
- prioritizării optimizărilor operaționale și financiare.

a) Vizualizare centralizată a workload-urilor implementate prin platformă

Platforma va permite agregarea informațiilor despre workload-urile Kubernetes **create și gestionate prin intermediul ei**, astfel încât operatorii să poată vedea, dintr-o singură interfață:

- lista workload-urilor containerizate, filtrabilă după:
  - cluster;
  - namespace;
  - aplicație/serviciu;
- principalele caracteristici relevante pentru operare:
  - numărul de replici configurate;
  - resursele solicitate (requests) și limitele configurate pentru CPU și memorie;
  - asocierea cu proiecte, echipe sau direcții din cadrul instituției (prin etichete și metadate).

Monitorizarea este orientată în mod explicit către workload-urile care fac parte din **modelul operațional al platformei**, nu doar către toate resursele existente în cluster, respectând astfel separarea responsabilităților dintre:

- echipele care administrează infrastructura Kubernetes în ansamblu;
- echipele care gestionează aplicațiile prin intermediul platformei.

b) Integrarea unui modul specializat de analiză a resurselor și costurilor

Platforma va include, în mod integrat, un **modul specializat de analiză a consumului de resurse și a costurilor asociate workload-urilor Kubernetes**, al cărui interfață este **încorporată (embedded)** în consola platformei. Prin intermediul acestui modul, platforma permite:

- monitorizarea în timp aproape real a:
  - utilizării CPU și memoriei la nivel de:
    - pod;
    - deployment;
    - namespace;
    - cluster;
  - diferenței dintre resursele solicitate (requests) și consumul efectiv;
- estimarea costurilor asociate resurselor consumate, pe baza:
  - tarifelor definite pentru resursele de calcul și stocare;
  - mapării dintre namespace-uri, workload-uri.

Platforma va oferi, prin acest modul:

- **dashboard-uri dedicate** pentru:
  - vizualizarea costurilor per mediu (ex.: dev-test vs. producție);
  - analiza costurilor per serviciu/aplicație;
- **filtre și agregări** pentru:

- concentrarea asupra unui anumit cluster sau namespace;
- izolarea workload-urilor cu impact bugetar semnificativ;
- identificarea workload-urilor cu raport slab între resurse alocate și resurse utilizate.

Acest modul va fi accesibil din interfața platformei, fără a obliga operatorii să comute între mai multe aplicații sau console independente.

d) Identificarea supra-alocării, sub-utilizării și oportunităților de optimizare

Prin consolidarea datelor privind utilizarea resurselor și a costurilor, platforma va permite identificarea:

- workload-urilor care au **resurse supra-alocate** (de exemplu, requests/limits ridicate, dar utilizare efectivă redusă);
- workload-urilor care sunt **constant aproape de saturație** (semnalând potențiale probleme de performanță sau necesitatea de scalare);
- mediilor în care resursele sunt **sub-utilizate** în mod sistematic, sugerând posibilitatea de consolidare sau de ajustare a configurațiilor.

Platforma va asigura:

- vizualizări sintetice pentru decidenți (de exemplu: top workload-uri după cost, după gradul de utilizare a resurselor);
- detalii tehnice pentru echipele de operare (ex.: evoluția în timp a consumului pentru un deployment critic).

Acest tip de monitorizare va susține inițiativele de **optimizare a costurilor (FinOps)** și îmbunătățirea eficienței operaționale, și va permite:

- identificarea rapidă a zonele de risipă;
- prioritzarea acțiunilor de tuning și reconfigurarea;
- documentarea deciziilor de dimensionare a infrastructurii.

e) Integrarea cu fluxurile operaționale ale platformei

Monitorizarea workload-urilor containerizate nu va fi un modul izolat, ci va fi integrată cu restul funcționalităților platformei. Astfel:

- atunci când un deployment este lansat sau modificat prin platformă, acesta devine automat vizibil în modulul de monitorizare, în contextul:
  - mediului;
  - clusterului;
  - namespace-ului;
- datele de consum și cost pot fi folosite pentru:
  - fundamentarea deciziilor de revizuire a configurațiilor (ex.: ajustarea requests/limits);
  - alimentarea rapoartelor de cost și utilizare la nivel de platformă;

- susținerea proceselor de planificare a capacității (capacity planning).

Operatorii și responsabilii de buget vor putea folosi informațiile din modulul de monitorizare pentru:

- a valida dacă un nou deployment sau o schimbare de configurație produce efectele dorite (de exemplu, reducerea costurilor sau îmbunătățirea utilizării resurselor);
- a detecta din timp deviații față de un comportament normal al unui serviciu, înainte ca acestea să se transforme în incidente majore.

Prin integrarea unui modul specializat de monitorizare a workload-urilor containerizate și a costurilor asociate, platforma va oferi instituției:

- **transparență asupra consumului de resurse** în mediile Kubernetes, din perspectiva aplicațiilor reale și a proiectelor cărora le aparțin;
- **suport pentru decizii informate** privind dimensionarea infrastructurii, optimizarea configurațiilor și planificarea bugetară;
- **reducerea dependenței de multiple instrumente disparate** pentru a înțelege ce se întâmplă în mediile containerizate – operatorii pot porni analiza direct din platformă;
- **aliniere la bune practici moderne** de gestionare a costurilor și resurselor în medii cloud-native, cu accent pe responsabilizarea liniilor de business și a echipelor consumatoare de resurse IT.

4.6.3 Continuitate operațională și Disaster Recovery (DR)

Platforma trebuie să sprijine instituția în definirea și implementarea unei strategii coerente de **continuitate operațională și recuperare în caz de dezastru (Disaster Recovery)**, acționând ca un orchestrator al proceselor necesare pentru restabilirea serviciilor critice în cazul unor incidente majore.

Soluția nu substituie mecanismele de backup sau replicare ale infrastructurii, ci le coordonează și le integrează într-un cadru unitar, auditabil și repetabil.

4.6.3.1 Orchestrarea proceselor de Disaster Recovery (DR)

Platforma va permite modelarea proceselor de DR sub formă de fluxuri de lucru declarative, în care sunt descrise, în ordine logică, toate acțiunile necesare pentru:

- activarea infrastructurii de rezervă (clustere, resurse de calcul, servicii de rețea);
- restaurarea aplicațiilor și a configurațiilor asociate;
- reconectarea aplicațiilor la bazele de date și la serviciile externe de care depind;
- verificarea funcțională de bază a serviciilor după recuperare.

Aceste fluxuri de lucru vor putea include:

- apeluri către API-urile sistemelor de backup și replicare deja existente în infrastructură;
- execuții de scripturi sau comenzi necesare pentru comutarea traficului (de exemplu, actualizarea înregistrărilor DNS sau a configurațiilor de load balancing);

- pași de validare automată (health checks, verificări de disponibilitate) și pași de aprobare manuală, acolo unde este necesar controlul uman.

Modelarea DR în acest mod permite instituției să aibă un „playbook” clar, codificat și executabil, reducând dependența de proceduri informale sau greu de urmărit.

4.6.3.2 Failover și comutare controlată între site-uri

Platforma trebuie să permită descrierea și orchestrarea scenariilor de failover și fallback între site-ul principal și site-urile de rezervă (on-premises sau cloud), pe baza fluxurilor de lucru definite.

În acest cadru:

- comutarea de la mediul principal la mediul de rezervă se va face prin execuția unui set de pași bine definiți (pornire resurse, aplicare configurații, actualizare rutare, verificare disponibilitate);
- comutarea înapoi (failback) către mediul principal, după remedierea incidentului, va fi de asemenea orchestrată, cu grijă pentru consistența datelor și pentru minimizarea întreruperilor suplimentare.

Platforma va permite includerea în aceste fluxuri a operațiunilor necesare pentru menținerea integrității datelor, în măsura în care infrastructura subiacentă asigură replicarea acestora. Obiectivele de recuperare (de tip RPO/RTO) stabilite de instituție (de exemplu, RPO < 15 minute, RTO < 1 oră) vor putea fi susținute prin combinarea mecanismelor de replicare existente cu fluxurile de orchestrare oferite de platformă.

4.6.3.3 Testare periodică și automatizată a planurilor de DR

Platforma trebuie să permită testarea periodică a planurilor de DR, fără a afecta mediile de producție, pentru a valida faptul că procedurile definite pot fi executate cu succes și în intervalele de timp așteptate.

În acest sens, soluția va:

- permite lansarea controlată a scenariilor de DR în medii de test sau pre-producție, utilizând aceleași fluxuri de orchestrare ca în producție, dar asupra unor seturi de resurse dedicate testării;
- înregistra toate etapele executate, timpii corespunzători și eventualele erori, oferind rapoarte detaliate care pot fi utilizate pentru îmbunătățirea continuă a planurilor;
- pune la dispoziție mecanisme de planificare (de exemplu, programarea automată a unor teste trimestriale), astfel încât instituția să poată demonstra, inclusiv în fața organelor de audit sau reglementare, că planurile de DR sunt verificate și actualizate în mod sistematic.

Prin acest model, platforma devine un element central al strategiei de continuitate operațională, asigurând nu doar documentarea, ci și execuția efectivă și testarea repetabilă a proceselor de DR.

4.6.4 Software de bază

4.6.4.1 Sisteme de operare desktop - 50 buc.

Se va achiziționa un număr de **50 (cincizeci) de licențe** pentru sisteme de operare de tip desktop, preinstalate de producătorul echipamentului, cu suport comercial activ și compatibile cu infrastructura și aplicațiile utilizate de ANS.

Cerințe generale:

- Sistemul de operare trebuie să fie preinstalat de producătorul echipamentului;
- Cheile de activare trebuie să fie integrate în firmware (BIOS/UEFI), astfel încât reinstalarea sistemului de operare să se realizeze fără introducerea manuală a cheii de produs;
- Licențele trebuie să fie verificabile prin mecanisme oficiale ale producătorului (ex.: pe baza seriei echipamentului sau a identificatorului hardware);
- Licențele trebuie să fie de tip **perpetuu**, cu drept de utilizare nelimitat în timp;
- Licențele trebuie să permită instalarea și reinstalarea sistemului de operare fără costuri suplimentare;
- Activarea trebuie să se poată realiza prin metode suportate oficial (ex.: cheie de produs, activare centralizată KMS/MAK sau echivalent);
- Licențele trebuie să fie verificabile prin mecanisme oficiale ale producătorului;

Cerințe tehnice:

- Suport pentru procesoare x64 (64-bit);
- Suport pentru minimum 128 GB RAM și cel puțin 2 procesoare logice;
- Funcționalitate de conectare la domeniu (domain join) și management prin Group Policy;
- Suport pentru criptarea datelor la nivel de disc (de ex. BitLocker sau echivalent);
- Actualizări automate de securitate și sistem, cu posibilitate de control în rețele enterprise;
- Acces la magazin de aplicații certificat și securizat;
- Interfață grafică modernă (UI/UX) în limba română sau engleză;
- Funcționalități de multitasking, suport nativ pentru aplicații multiple în ferestre și desktopuri virtuale;
- Compatibilitate:
    - Compatibil cu aplicațiile existente în infrastructura beneficiarului (ex: MS Office, aplicații educaționale/contabile/medicale etc.);
    - Compatibil cu soluțiile antivirus, de management de rețea și periferice (imprimante, scanere etc.);
    - Instalare pe echipamente de tip PC/Laptop conform specificațiilor tehnice menționate.

4.6.4.2 Suita de productivitate- 50 buc.

Se va achiziționa un număr de 50 de licențe pentru o suită de productivitate instalabilă local (on-premise), cu licență perpetuă (permanentă), fără costuri recurente de abonament și fără dependență de rulare exclusiv cloud.

Soluția ofertată trebuie să ofere funcționalități cel puțin echivalente cu cele ale unei suite de birou lansate în anul 2021 sau ulterior.

Cerințe tehnice:

- Suita de productivitate trebuie să includă aplicații echivalente cu:
  - procesor de text;
  - editor de foi de calcul;
  - aplicație pentru prezentări;
  - client de poștă electronică;
  - aplicație pentru notițe digitale.

Cerințe funcționale minime:

- Interfață în limba română și/sau engleză;
- Compatibilitate nativă cu formatele de fișiere standard de birou: .docx, .xlsx, .pptx;
- Compatibilitate cu sistemul de operare utilizat;

Cerințe privind licențierea:

- Tip licență: Licență de tip perpetuu (permanentă), fără limită de timp în utilizare și fără costuri de subscripție/abonament recurente, instalabilă offline, fără necesar de conexiune permanentă la internet. Licența trebuie să permită reinstalarea sistemului de operare pe același hardware sau pe hardware echivalent în caz de defecțiune;
- Instalare și utilizare: Licențele trebuie să permită instalarea locală (offline). Utilizarea aplicațiilor nu trebuie să fie condiționată de o conexiune permanentă la internet după activare.
- Activare: activare individuală sau centralizată (ex.: cheie unică de volum sau chei individuale), în funcție de modelul de licențiere ofertat.
- Drept de instalare pe stațiile de lucru indicate (minim 1 dispozitiv per licență). Drept de reinstalare pe același echipament sau pe echipament echivalent, în caz de defecțiune.
- Documentație: Furnizarea licențelor în format electronic sau fizic și a cheilor de activare aferente, a certificatelor de autenticitate (după caz), precum și a documentației tehnice de instalare/configurare în limba română sau engleză

4.6.4.3 Sistem de operare pentru Server – 2 buc.

Se va achiziționa un număr de 2 (două) licențe pentru sistem de operare de tip server, destinate utilizării în infrastructura IT a instituției, implementate într-un mediu de cloud privat guvernamental.

Soluția ofertată trebuie să fie un sistem de operare server cu suport comercial activ (până cel puțin 31.12.2029), compatibil cu infrastructura cloud propusă, capabil de: virtualizare (Hyper-V sau echivalent), integrare Active Directory sau echivalent LDAP, suport containere (Docker/Kubernetes sau echivalent). Se acceptă sisteme Linux sau Windows Server cu funcționalități echivalente..

Cerințe tehnice:

- Sistemul de operare trebuie să fie disponibil cu interfață grafică (GUI) și să permită administrarea facilă a serviciilor;

- Sistemul de operare trebuie să ofere funcționalități cel puțin echivalente cu un sistem de operare server modern cu suport comercial activ, incluzând minimum, incluzând minimum:
  - servicii de domeniu de tip Active Directory Domain Services (AD DS) sau echivalent;
  - servicii DNS;
  - servicii DHCP;
  - integrare în infrastructuri mixte (Windows și Linux);
  - suport pentru roluri standard de server (ex.: management utilizatori, politici de grup, servicii de fișiere și imprimare, securitate și control acces);
- Sistemul de operare trebuie să permită administrarea centralizată a utilizatorilor și resurselor;
- Sistemul de operare trebuie să fie compatibil cu infrastructuri virtualizate și platforme de cloud privat;

Cerințe funcționale minime

- Interfață disponibilă în limba engleză (și/sau română, dacă este disponibilă);
- Stabilitate, securitate și performanță în exploatare;
- Posibilitatea aplicării actualizărilor de securitate și funcționalitate;
- Suport pentru administrare locală și de la distanță (remote management);

Cerințe privind licențierea

- Tip licență: **licență perpetuă (permanentă)**, fără costuri de subscripție/abonament pentru sistemul de operare;
- Licența trebuie să permită utilizarea în medii virtualizate și în infrastructuri de tip cloud privat, inclusiv reasignarea pe instanțe virtuale echivalente;
- Licența trebuie să fie conformă cu politicile producătorului privind utilizarea în medii virtualizate (ex.: drepturi de virtualizare incluse);
- Drept de reinstalare și migrare între instanțe virtuale, în cadrul aceleiași infrastructuri;
- Activare: prin cheie de produs sau mecanism specific producătorului;

Livrare și documentație

- Furnizarea licențelor în format electronic și/sau fizic, împreună cu:
  - cheile de activare;
  - certificatele de autenticitate (după caz);
- Furnizarea documentației tehnice de instalare și configurare;
- Asigurarea accesului la portalul producătorului pentru:
  - descărcarea imaginilor;
  - actualizări și patch-uri de securitate;
- Perioadă minimă de acces la actualizări: **36 de luni**;

- Documentația va fi disponibilă în limba română și/sau engleză.

4.6.4.4 Soluție de management centralizat pentru infrastructura IT – 1 buc.

Se va achiziționa **1 (una) soluție de management centralizat** pentru infrastructura IT, destinată administrării unitare a stațiilor de lucru și serverelor, în mediu de **cloud privat/hibrid guvernamental** bazat pe tehnologii de tip Azure Stack Hub.

Soluția trebuie să ofere funcționalități moderne de administrare, distribuție software, inventariere, configurare și securitate, compatibile cu infrastructura utilizată de ANS..

1. **Scopul implementării**

- administrarea centralizată a echipamentelor IT (stații de lucru și servere);
- creșterea nivelului de securitate, standardizare și automatizare;
- utilizarea infrastructurii cloud privat/hibrid (Azure Stack Hub) ca platformă de găzduire;
- respectarea cerințelor de suveranitate a datelor și operare în mediu controlat.

2. **Cerințe generale**

Soluția trebuie să:

- fie complet funcțională în infrastructuri de tip Azure Stack Hub;
- permită administrarea centralizată a echipamentelor IT;
- fie susținută oficial de producător;
- fie scalabilă și ușor de extins;
- funcționeze fără dependență de servicii cloud publice externe.

3. **Cerințe funcționale minime**

Administrarea dispozitivelor

Soluția trebuie să permită:

- administrarea centralizată a stațiilor de lucru și serverelor;
- organizarea resurselor în colecții statice și dinamice;
- aplicarea de politici diferențiate;

Inventariere hardware și software

Soluția trebuie să asigure:

- inventarierea automată hardware și software;
- actualizarea periodică a informațiilor colectate;
- generarea de rapoarte detaliate privind configurația echipamentelor;
- exportul rapoartelor în formate standard;

Management aplicații

Soluția trebuie să permită:

- distribuirea aplicațiilor din infrastructura Azure Stack Hub;

- instalarea, dezinstalarea și actualizarea controlată a aplicațiilor;
- rularea implementărilor fără intervenția utilizatorului final;
- planificarea și automatizarea proceselor de deployment;

Management actualizări (Patch Management)

Soluția trebuie să:

- gestioneze actualizările sistemelor de operare;
- permită controlul manual sau automat al actualizărilor;
- furnizeze rapoarte privind nivelul de conformitate;
- funcționeze integrat cu infrastructura existentă;

Implementarea sistemelor de operare

Soluția trebuie să permită:

- implementarea sistemelor de operare utilizând imagini standardizate;
- standardizarea configurațiilor;
- reprovisionarea echipamentelor existente;

Monitorizare și jurnalizare

Soluția trebuie să ofere:

- monitorizarea stării componentelor soluției;
- jurnalizarea completă a activităților administrative;
- generarea de alerte pentru evenimente critice;

4. Cerințe specifice de implementare

Soluția trebuie să:

- fie instalată pe mașini virtuale găzduite în infrastructura Azure Stack Hub;
- utilizeze componente compatibile (compute, storage, networking);
- permită izolarea față de cloud public;
- respecte principiile de cloud privat și hibrid;
- funcționeze în condiții de acces restricționat la internet (după caz);

5. Cerințe de securitate

Soluția trebuie să:

- fie integrată cu Active Directory;
- utilizeze mecanisme de control al accesului de tip RBAC;
- asigure comunicații securizate între componente;
- respecte politicile interne de securitate ale autorității contractante;
- ofere control granular al accesului administratorilor;

6. **Cerințe tehnice**

Compatibilitate

- compatibilitate cu sisteme de operare server suportate de producător ;
- integrare cu sisteme de baze de date compatibile (ex.: SQL Server);
- operare stabilă în mediu virtualizat de tip Azure Stack Hub;

Scalabilitate

- posibilitatea extinderii numărului de echipamente administrate;
- extindere fără întreruperi majore de serviciu;
- adaptabilitate la creșterea resurselor în infrastructura cloud;

7. **Cerințe de licențiere**

- Tip licențiere: **licență perpetuă (permanentă)**, fără limită de timp în utilizare și fără costuri de subscripție recurente;
- Licențele trebuie să permită utilizarea în medii virtualizate și cloud privat;
- Licențierea trebuie să fie conformă cu politicile producătorului pentru implementări on-premise și cloud privat;

8. **Servicii incluse**

Prestatorul va asigura:

- instalarea și configurarea soluției în infrastructura Azure Stack Hub;
- integrarea cu infrastructura IT existentă;
- testarea și validarea funcționalităților;
- furnizarea documentației tehnice și de operare;
- instruirea personalului desemnat;
- suport tehnic pe perioada contractuală.

4.6.4.5 Sistem de gestiune a bazelor de date - 1 pachet

Cerințe tehnice:

Pentru asigurarea securității și integrității datelor gestionate, SGBDR-ul ofertat trebuie să dispună de mecanisme pentru:

- Criptarea datelor
- Restricționarea accesului (citire, scriere) utilizatorilor la nivelul obiectelor (tabele, câmpuri) din baza de date
- Utilizarea de constrângeri asupra tipurilor și valorilor datelor
- Utilizarea de constrângeri de tip cheie primară
- Utilizarea de constrângeri pentru a se asigura că nici o valoare duplicată nu este introdusă într-o coloană care nu participă la o cheie primară

- SGBDR-ul trebuie să permită salvarea totală și/sau parțială a bazei de date și să dispună de funcționalități de administrare cu următoarele caracteristici :
    - Interfață grafică de utilizare (GUI - graphical user interface)
    - Vizualizarea grafică a structurii tabelelor și a relațiilor dintre acestea sub formă de
    - diagrame de tip ERD (Entity Relationship Diagram)
    - Ferestre SQL multiple pentru a construi și executa scripturi
    - Adăugarea, modificarea și ștergerea obiectelor bazei de date (tabel, index, vedere, constrângere, trigger, procedură stocată)
    - Administrarea utilizatorilor și drepturilor de acces
    - Examinarea listei de conexiuni active la server, cu indicarea aplicației client, utilizatorului, bazei de date accesate, stării tranzacției curente și a eventualelor deadlock-uri
    - Realizarea salvărilor și restaurărilor bazelor de date
    - Exportul datelor în formate uzuale (cel puțin CSV, XML, JSON).

4.6.5 Echipamente hardware individuale (enduser)

Pentru a asigura o funcționare eficientă și performantă a activităților desfășurate de ANS, înlocuirea echipamentelor IT existente devine o necesitate imperativă. Multe dintre calculatoarele și laptopurile actuale sunt depășite moral și tehnologic, ceea ce afectează negativ productivitatea, calitatea serviciilor și capacitatea de a răspunde cerințelor moderne de operare.

Echipamentele vechi sunt limitate din punct de vedere al performanțelor, având dificultăți în rularea aplicațiilor necesare, încetinind procesele de lucru și necesitând frecvent intervenții pentru reparații sau întreținere. Această situație nu doar că generează costuri suplimentare, dar și pune în pericol continuitatea activităților critice și capacitatea de a furniza servicii eficiente către public și parteneri. Echipamentele învechite nu mai pot susține eficient soluțiile software moderne, necesare pentru digitalizarea și gestionarea datelor, pentru a respecta standardele de securitate cibernetică și pentru a permite interconectarea cu alte instituții relevante.

De asemenea, este necesară uniformizarea echipamentelor utilizate, pentru a asigura un mediu IT standardizat, ușor de administrat și cu o interoperabilitate crescută. Echipamentele eterogene, cu specificații diferite, îngreunează procesele de configurare, mentenanță și suport tehnic, ceea ce duce la o alocare ineficientă a resurselor și la creșterea timpilor de întârziere pentru remedierea problemelor. Folosirea unor dispozitive uniformizate permite implementarea unor politici IT coerente, simplifică întreținerea infrastructurii și asigură compatibilitatea cu aplicațiile folosite în mod curent.

Înlocuirea calculatoarelor și laptopurilor existente cu echipamente moderne și standardizate va conduce la o creștere semnificativă a eficienței operaționale, reducerea costurilor asociate întreținerii și, totodată, va sprijini obiectivele ANS de digitalizare și modernizare a activităților. Prin urmare, înlocuirea echipamentelor IT învechite nu reprezintă doar o actualizare tehnologică, ci o investiție strategică în eficiența și calitatea serviciilor publice oferite de ANS.

Necesarul de echipamente de calcul individuale este următorul:

4.6.5.1 Calculator desktop de tip AIO – 50 buc.

Componenta	Cerință tehnică
Chipset	Același producător cu procesorul
Procesor	Minim Ultra 5, Minim 14 nuclee, minim 14 fire de execuție, minim 24MB cache, frecvență turbo minim 5.0GHz
Memorie instalată	Minim 1x16GB, DDR5, pana la 5600 MT/s
Memorie maximă	Minim 2 sloturi fizice SoDIMM pe placa de baza Suportă minim 64 GB
Grafică	Suportă rezoluție minim 5120 x 3200 la o frecvență de minim 60Hz
Stocare	Minim 512GB SSD, MTBF minim 1.400.000 ore Minim 1 port M.2
Conectivitate	Placa de rețea integrata minim Gigabit Wireless de ultimă generație, Wi-fi 6E Bluetooth ultima generație
Sursa de alimentare	Sursa de alimentare externa cu adaptor minim 130 Watt
Porturi de conectare (nu se accepta hub-uri USB sau alte adaptoare)	- minim 1 port Display Port 1.4a - minim 1 port USB Type C de viteză minim 10Gbps - minim 1 port USB de viteză minim 10Gbps - minim 2 porturi USB de viteză minim 5Gbps - minim 2 porturi USB de viteza minim 480Mbps - minim 1 port audio - minim 1 SD card 4.0
Accesorii	Tastatură și mouse același brand cu sistemul de calcul
Audio	Boxe stereo integrate, minim 3W x 2
Software instalat cu licență	Sistem de operare de tip desktop, preinstalat de producător, cu suport comercial activ, compatibil cu infrastructura și aplicațiile utilizate de ANS. Sistemul de operare trebuie să permită: – administrare centralizată (politici de grup sau mecanisme echivalente), – criptare completă a discului (funcționalități de tip BitLocker sau echivalent), – autentificare multi-factor, – integrare în infrastructura de identitate existentă (ex. servicii de director compatibile). Se acceptă sisteme de operare cu funcționalități și caracteristici echivalente.

Componenta	Cerință tehnică
	Cheile de activare vor fi incorporate în BIOS pentru a permite reinstalarea sistemului de operare Licențele trebuie să fie verificabile pe site-ul producătorului folosind seria echipamentului livrat.
Caracteristici de securitate	Chip/modul de securitate integrat pe placa de baza tip TPM 2.0 care oferă posibilitatea criptării datelor atât hardware cat si software Certificat FIPS 140-2 Nivel 2 MIL-STD 810H Blocare cu senzor de intruziune
Carcasa, Dimensiuni, Display si alte cerințe	Diagonala ecranului: 23.8“ cu rezoluție FHD (1920x1080) de tip IPS Non-Touch cu certificare Blue Light, Luminozitate minimă 250 cd/m2, contrast tipic minim 1500:1, unghi de vizibilitate min 178/178, Cameră digitală RBG de 2,07 MP integrată în carcasa matricei. Retractabilă mecanic în carcasă (nu este permisă răsucirea sau scoaterea camerelor) Carcasa trebuie să permită utilizarea unui dispozitiv de securitate fizică sub forma unui cablu metalic, iar capacul din spate trebuie să fie detașabil fără a fi nevoie de unelte. Sistem de montare VESA 100. Sistemul trebuie să salveze jurnalele de evenimente în BIOS. Fiecare computer trebuie să fie identificat printr-un număr de serie unic aplicat pe carcasă și stocat permanent în BIOS. Stand ajustabil pe înălțime pana la 100mm, pivot 45 grade, pivot 90 grade, tilt -5/30 grade
Greutate ansamblu fără stand	Maxim 7Kg cu toate componentele instalate
Garanție și suport	Durata minimă a suportului tehnic al producătorului este de 36 luni. Modul de implementare a serviciilor de suport tehnic: • Raportarea telefonică a defecțiunilor în timpul săptămânii, între orele 8 și 17. • Portal online gratuit dedicat al producătorului pentru raportarea defecțiunilor și gestionarea solicitărilor de servicii. • Suport opțional prin chat online. Suportul tehnic pentru echipament va fi furnizat de la distanță sau la locul de instalare a dispozitivului, în funcție de tipul de defecțiune raportat. În cazul unei defecțiuni clasificate drept reparație la locul de instalare a dispozitivului, piesa de schimb necesară pentru reparație și/sau tehnicianul de service va ajunge la locul indicat de client în următoarea zi lucrătoare de la momentul acceptării efective a solicitării de către Departamentul suport tehnic.

Componenta	Cerință tehnică
	Capacitatea de a verifica perioada curentă și nivelul de asistență tehnică pentru dispozitive prin intermediul site-ului web al producătorului. Posibilitatea de a descărca versiunile curente ale driverelor și firmware-ului dispozitivului prin intermediul site-ului web al producătorului, de asemenea, pentru dispozitivele cu suport tehnic inactiv. Se va prezenta (alat la ofertare cat si la livrare) declarație in original din partea producătorului pentru confirmarea garanției și a serviciilor menționate.

4.6.5.2 Tablete – 25 buc.

Componenta	Cerință tehnică
Tableta portabila robusta de clasa fully- rugged, proiectata pentru a rezista la condiții de mediu dure și extreme la utilizare în teren, concepute pentru a face față la șocuri, vibrații, căderi, temperaturi extreme, umiditate și praf, ceea ce le face potrivite pentru utilizare în medii industriale, în aer liber, în sănătate, în serviciile de utilitate publică și în alte medii similare, cu următoarele cerințe minimale.	
Chipset	Placă de bază compatibilă cu procesorul oferit, cu suport pentru conectivitate modernă, incluzând cel puțin: - port USB-C cu standard de viteză de generație recentă (USB 3.2 Gen 2 sau superior), - WiFi 6E sau superior, - Bluetooth 5.x sau superior. Se acceptă tehnologii echivalente care asigură performanțe și interoperabilitate cel puțin similare.
Procesor	Procesor x86-64 de generație recentă (lansat după 01.01.2023), cu minimum 8 nuclee și performanță minimă demonstrabilă prin benchmark public (ex. PassMark CPU ≥ 15.000 sau echivalent). Accelerator AI integrat (NPU) cu performanță de minimum 40 TOPS sau echivalent. Cache procesor: minimum 8 MB. Frecvență turbo: minimum 4.7 GHz sau performanță echivalentă demonstrabilă. Suport pentru funcții avansate de administrare și securitate la nivel enterprise (ex. tehnologii de administrare remote, securitate hardware și management centralizat sau funcționalități echivalente).
Memorie instalata	Minim 16GB, LPDDR5x, 8533 MT/s, dual-channel
Placa video	Integrata cu suport pentru 3 monitoare externe
SSD	Minim M.2 256GB PCIe NVMe, MTBF 1.4 milioane ore

Componenta	Cerință tehnică
Display	12 inch Touch FHD+ (1920x1200) IPS, Anti-Glare, tehnologie Wide-viewing angle, unghi de vedere orizontal/vertical min +/-88°C, luminozitate1200 nits, contrast minim 1000:1, pixel pitch 0.135 x 0.135 mm Moduri de atingere (deget sau pen, mănuși, apă)
Conectivitate	minim WiFi 7 (802.11be), 2x2, Bluetooth 5.4 sau superior (fără restricție de producător) modul 5G Snapdragon X72 eSIM
Multimedia	Integrat, minim 2 difuzoare 2.5w Camere integrate 8MP front cu IR/RGB (suport pentru autentificare biometrică prin recunoaștere facială) 11MP rear cu flash și microfon integrat
Porturi native (nu se accepta hub-uri USB sau alte adaptoare)	2 x Thunderbolt 4 cu port cover 1 x USB 3.2 Gen 1 1 x HDMI 2.1 1 x port audio 1 x microSD card slot
Baterie	2 celule, minim 35.6Whr, tehnologie ce permite încărcare rapidă la 80% in 1ora
Accesorii (același brand cu sistemul de calcul)	Tastatura compatibila cu sistemul de calcul Interfața conectare POGO PIN Standard IP66
Caracteristici de securitate	Un cip hardware dedicat integrat în placa de bază (TPM 2.0) pentru a crea și gestiona cheile de criptare generate de calculator. Încercarea de a scoate cipul va deteriora placa de bază. Securitatea trebuie să poată cripta documentele sensibile stocate pe hard disk cu ajutorul cheii hardware. Verificarea cheilor de criptare generate de calculator trebuie să aibă loc într-un chipset dedicat de pe placa de bază.
Software	Sistem de operare preinstalat de producător, cu suport comercial activ, compatibil cu aplicațiile și infrastructura utilizată de ANS. Sistemul de operare trebuie să permită: - administrare centralizată prin mecanisme standard (MDM sau echivalent), - criptare completă a datelor, - autentificare multi-factor,

Componenta	Cerință tehnică
	- integrare cu infrastructura de identitate a ANS (servicii de director compatibile), - reinstalarea sau resetarea sistemului de operare fără necesitatea introducerii manuale a cheilor de activare sau a altor date de licențiere. Se acceptă sisteme de operare cu funcționalități și caracteristici echivalente.
Software suplimentar	Împreună cu computerul oferit este inclus un software cu o licență de utilizare nelimitată în timp ce permite: - actualizați și instalați toate driverele, aplicațiile furnizate în imaginea sistemului de operare a producătorului, BIOS cu certificat de compatibilitate al producătorului la cea mai recentă versiune disponibilă, - posibilitatea, înainte de instalare, de a verifica fiecare driver, aplicație, BIOS direct pe site-ul web al producătorului, utilizând o conexiune la internet cu redirecționare automată și, în special, informații: a. privind modificările și îmbunătățirile referitoare la actualizări b. data ultimei actualizări c. prioritatea actualizărilor d. compatibilitatea cu sistemele de operare e. ce componentă hardware este afectată de actualizare f. toate actualizările anterioare cu informațiile menționate anterior de la litera a la litera e. - o listă cu cele mai recente actualizări, împărțite în actualizări critice (care necesită instalare imediată), recomandate și opționale - posibilitatea de a activa/dezactiva funcția de repornire automată în cazul în care aceasta este necesară pentru instalarea unui driver sau a unei aplicații care o necesită. - identificarea modelului calculatorului oferit, numărul de serie al calculatorului, informații privind data ultimei actualizări, în special data (zz-mm-ani)

Componenta	Cerință tehnică
	- verificați istoricul actualizărilor cu informații despre driverele care au fost instalate, cu data exactă (zz-mm-ana) și versiunea (revizuirea versiunii). - lista detaliată a driverelor, aplicațiilor, BIOS necesare cu informații despre versiunea instalată în prezent pentru calculatorul oferit, cu posibilitatea de a exporta într-un fișier cu extensia *.xml - un raport care să includă informații privind verificarea actualizărilor, actualizările găsite, actualizările descărcate, actualizările instalate cu o defalcare detaliată a componentelor afectate, erorile din timpul verificării, instalarea și posibilitatea de a exporta un astfel de raport într-un fișier *.xml. Raportul trebuie să includă data exactă (zz-mm-ana) și
Servicii	Accesul la informații trebuie sa fie realizat direct de către fabricantul echipamentelor printr-un centru care sa asigure asistenta la nivel global, care sa permită monitorizarea furnizării on-site a rezoluțiilor necesare, si care sa asigure in același timp coordonarea pro-activa a managementului evenimentelor si a comunicării Managementul cazurilor, inclusive escaladarea evenimentelor pentru o rezoluție rapida Managementul escaladărilor prin asigurarea unui singur punct de contact la fabricantul echipamentelor pentru gestionarea incidentelor, escaladarea evenimentelor deosebite si raportarea stadiului incidentelor in concordanta cu descrierea serviciilor atașate sistemelor furnizate. Acces telefonic pentru semnalarea si investigarea problemelor hardware si software ale sistemelor furnizate direct la fabricantul echipamentelor, inclusiv acces la baza de cunoștințe a acestuia
Greutate si dimensiuni	Dimensiuni max admise: 30mmx305mmx210mm Maxim 1.35kg fara accesorii
Rezistenta si conformitate cu standardele internaționale	Șasiul echipamentului este ranforsat, îndeplinind testele: MIL-STD-810 G/H (vibrații, șoc funcțional, pătrunderii apei și prafului și temperaturilor extreme, altitudine, șoc termic, îngheț/dezgheț, standby tactic la funcționare) IEC 60529: IP-66

Componenta	Cerință tehnică
	ANSI ISA 12.12.01 + CSA Interval termic de funcționare: -28°C până la 62°C ENERGY STAR 8.0 EPEAT Gold FIPS 140-2 certification pentru TPM 2.0 Este necesară o declarație din partea contractantului însoțită de o declarație din partea producătorului privind respectarea standardelor de mai sus.
Garanție și suport	**Minim 24 luni** Se va prezenta (atât la ofertare cat si la livrare) declarație in original din partea producătorului pentru confirmarea garanției și a serviciilor menționate.

4.6.5.3 Imprimante departamentale – 3 buc.

Componenta	Cerința tehnică
Funcții disponibile	Copiator, imprimanta rețea, scaner rețea, opțional fax
Dimensiuni hârtie la tipărire	A5R - 320 x 460 mm; banner minim 304 x 1200 mm
Duplex automat	inclus
Suport echipament cu roti	inclus
Viteza copiere/imprimare	minim 25/15 ppm A4/A3 color si monocrom
Greutate maxima hârtie din toate casetele si tava manuala (bypass)	minim 300 g/m^2
Greutate maxima hârtie in mod duplex automat	minim 256 g/m^2
Timp de încălzire	maxim 13 secunde din modul low power
Alimentator manual de hârtie (bypass)	minim 100 coli la 80 g/m^2
Alimentator automat de documente	- scanare fata-verso a originalelor la o singura trecere - detecție alimentare multipla - capacitate: minim 300 coli la 80 g/m^2 - greutăți acceptate ale hartiei: 35 – 200 g/m^2
Capacitate alimentare cu hârtie	minim 1200 coli la 80 g/m^2; 2 casete si bypass
Capacitate ieșire hârtie	minim 400 coli la 80 g/m^2

Componenta	Cerința tehnică
Memorie	minim 4 GB RAM
Stocare date	minim 128 GB
Conectivitate standard	USB 2.0, Gigabit Ethernet 10BaseT / 100BaseTX / 1000BaseT
Conectivitate opțională	WirelessLAN, Bluetooth, WiFi Direct
interfața utilizator	ecran tactil, color, diagonala minim 10 inch
Funcții Copiere	
Prima copie (mono / color)	maxim 6 secunde / maxim 8 secunde
Zoom	25-400% in pași de 1%
Rezoluție copiere	600 x 600 dpi
Alte functii copiere	Sortare electronica, sortare prin alternare, copiere carduri ID, ștergere margini, 2in1, 4in1
Funcții Scanare	
Rezoluție scanare	600 x 600 dpi
Viteza de scanare	minim 240 ppm alb-negru si color (A4, 300 dpi)
Funcții scanare	WS Scan, Scan to USB, Scan to E-Mail, Scan to File (SMB, FTP, FTPS, Local), Scan to Box (e-Filing), WIA, TWAIN
Formate fișiere obținute automat in urma scanării	JPEG, Multi/Single Page TIFF/XPS/PDF, Secure PDF,Slim PDF, PDF/A, PDF/A-2
Funcții Tipărire	
Limbaj de imprimare	PCL5e, PCL5c, PCL6 (PCL XL), XPS, PDF, PostScript 3
Rezoluție tipărire	1200 x 1200dpi, 2 biti
Sisteme de operare compatibile	Windows 11/10/8.1, Windows Server 2022/2019/2016/2012 R2/2012 (64 bit), Mac OS 10.12-12, Linux/Unix, Citrix, SAP, AS/400
Funcții	- posibilitate de tipărire in tandem cu un alt echipament similar; - tipărire de pe suport memorie USB; - tipărire directa e-mail; - păstrare tipărire in Hold

Componenta	Cerința tehnică
Alte funcții	
Securitate	- minim 1000 coduri de acces departamentale - minim 10000 coduri de acces utilizatori - tipărire privată - criptare date
Garanție	Minim 24 luni
Alte cerințe	
Consumabile incluse la livrare	pentru minim 38.000 pagini A4 la o încărcare de 5% pe fiecare culoare
Furnizorul va prezenta autorizări din care sa reiasă ca minim 2 persoane au fost instruite pentru service pent produsele furnizate. Autorizările vor fi emise de către producătorul echipamentelor sau de distribuito autorizați ai acestora in Romania.	

4.6.5.4 Scanner performant TIP BUSSINESS – 1 buc.

Componenta	Cerință tehnică
Tip scaner	Scaner sheetfed cu alimentare de coli
Rezoluție scaner	600 DPI x 600 DPI (orizontal x vertical)
Interval scanare	215,9 mm x 6.096 mm (orizontal x vertical)
Scanning range min	50,8 mm x 50,8 mm (orizontal x vertical)
Formate hârtie	A4 (21.0x29,7 cm), A5 (14,8x21,0 cm), A6 (10,5x14,8 cm), B5, B6, Letter, Legal, Carte poștală, Cărți de vizită, Carduri de plastic
Profunzime de culoare	Intrare: 30 Bits Color , Ieșire: 24 Bits Color
Senzor cu ultrasunete	Da
Sursă de lumină	Tehnica ReadyScan LED
Rezoluție de ieșire	75, 100, 150, 200, 240, 300, 600, 1200 DPI
Display LCD	Tip: Color, Ecran senzitiv, Diagonală: 10,9 cm

Componenta	Cerință tehnică
Viteză de scanare	Monocrom: 35 Pagini/min. - Color: 35 Pagini/min. măsurată cu Dimensiune: A4 , Rezoluție: 300 dpi
Capacitate de setare a hârtiei	100 Coli
Greutate hârtie ADF	Auto loading: 27 - 413 g/m²
Tip alimentator automat de documente	Scanare dublă la o singură trecere a colii
Alimentare automată cu documente	200 Pagini
Duplex Scan	Da
Caracteristici Scanare	Funcționare standalone, Degradare culoare RGB, Capacitate avansată de eliminare culori/îmbunătățire, Ignoră paginile goale, Îndepărtare perforații, Prelucrare avansată imagini, Setări prestabilite, Corectare automată a poziției înclinate a hârtiei, ieșire pe ecran dublă (numai Windows), rotire automată a imaginii, Îmbunătățire text, Scan to Cloud Storage
Formate ieșire	BMP, JPEG, TIFF, Scanare către multi TIFF, PDF, Scanare către PDF căutabil, PDF/A, PNG
Advanced document integration	Scanare către email, Scanare către FTP, Scanare către Microsoft SharePoint®, Scanare către folder Web, Scanare către folder de rețea, Scanare către USB
Volum scanare	4.000 Pagini pe zi
Conexiuni	Wi-Fi Direct, Gazdă USB, LAN wireless IEEE 802.11a/b/g/n, USB 3.2 Gen 1x1
Sisteme operative compatibile	Mac OS 11. x, Mac OS 12. x, Mac OS X 10.11.x sau versiune superioară, Windows 10, Windows 10 (32/64 bit), Windows 11, Windows 7 (32/64 bit), Windows 8 (32/64 biți)
Temperatură	Funcționare 5° C - 35° C, Depozitare -25° C - 60° C
Umiditate a aerului	Funcționare 15% - 80%, Depozitare 15% - 85%
Garanție	**Minim 12 luni** On-site Next business day

4.7 Cerințe de interconectare/interoperabilitate și accesibilitate

Platforma va include un strat dedicat integrării cu sisteme interne și externe, asigurând un flux coerent de date și interoperabilitate în conformitate cu standardele instituționale. Acest strat va:

- expune API-uri standardizate (REST, OpenAPI 3.x);
- permite integrarea bidirecțională cu ITSM, CMDB, DevOps și sisteme de identitate;
- suporta webhook-uri, sisteme de mesagerie și evenimente interne/extern;
- asigura compatibilitate cu infrastructuri eterogene (virtualizare, containere, cloud public/privat);
- permite extinderea și personalizarea conectorilor, fără modificarea nucleului platformei.

Prin acest strat se va asigura continuitatea operațională în mediile existente și flexibilitatea necesară evoluțiilor viitoare.

Platforma trebuie să fie deschisă și extensibilă, oferind un ecosistem complet de **API-uri și mecanisme de integrare** care permit conectarea cu aplicații existente în instituție, cu sisteme externe și cu instrumente standard de DevOps, ITSM și monitorizare. Obiectivul este ca soluția să nu reprezinte un „sistem închis”, ci un hub de integrare care se poate conecta la arhitectura digitală existentă și viitoare a instituției.

Platforma informatică trebuie sa fie dezvoltată conform unei arhitecturi (API-first), în care:

- stratul de prezentare este complet decuplat de stratul de business și de date;
- toate funcționalitățile sistemului sunt accesibile exclusiv prin API-uri.

Backend-ul platformei nu va conține elemente sau dependențe specifice interfeței grafice (UI).

Orice aplicație client (portal web, aplicații mobile, aplicații terțe, sisteme externe) va interacționa cu sistemul exclusiv prin intermediul API-urilor expuse.

Toate modulele platformei vor comunica între ele doar prin API-uri, fără acces direct la baze de date sau la logica internă a altor module.

Comunicarea inter-modulară va fi:

- stateless;
- bazată pe contracte bine definite;
- independentă de tehnologia de implementare a fiecărui modul.

Sistemul va permite extinderea ulterioară prin adăugarea de noi module sau servicii fără modificări majore asupra celor existente.

Platforma va expune API-uri standardizate pentru schimbul de date și integrare, după cum urmează:

- REST APIs (Representational State Transfer): Utilizează metode HTTP (GET, POST, PUT, DELETE) și este cunoscut pentru simplitatea și scalabilitatea sa.
- SOAP APIs (Simple Object Access Protocol): Protocol bazat pe XML pentru schimbul de informații structurate în implementații web services.

- GraphQL: Limbaj de interogare pentru API-uri, care permite clientului să solicite exact datele necesare și nimic mai mult.
- gRPC : Sistem de apeluri de proceduri la distanță (RPC) creat de Google, care utilizează Protocol Buffers pentru serializarea datelor.

Platforma va expune un API REST documentat conform specificației OpenAPI 3.x, permițând:

- consultarea și gestionarea programatică a resurselor administrate (deployment-uri, fluxuri de lucru, integrare, configurații, secrete etc.);
- integrarea cu aplicații interne ale instituției sau cu soluții terțe, care pot interacționa cu platforma prin apeluri HTTP standard;

Accesarea API-ului se va face în condiții de securitate (prin mecanisme de autentificare și autorizare) și cu respectarea politicilor de audit și logare, astfel încât operațiunile efectuate prin API să fie trasabilă.

Formatele de date acceptate vor fi JSON și XML, conform cerințelor de interoperabilitate.

Platforma va include un API Gateway care va constitui punctul unic de acces pentru toate API-urile expuse.

API Gateway-ul va gestiona cel puțin următoarele:

- autentificare și autorizare;
- rate limiting și throttling;
- logging și audit;
- rutarea cererilor către modulele backend corespunzătoare.

Toate API-urile vor fi securizate în mod implicit.

Măsurile minime de securitate obligatorii includ:

- autentificare și autorizare prin OAuth 2.0 și OpenID Connect;
- utilizarea tokenurilor de acces (ex. JWT);
- criptarea comunicațiilor prin HTTPS/TLS;
- validarea și sanitizarea datelor de intrare;
- protecție împotriva abuzurilor prin rate limiting;
- logging și monitorizare a accesului la API-uri.

Sistemul nu va utiliza mecanisme de autentificare dependente de sesiuni UI.

Toate API-urile vor fi versionate explicit.

Sistemul va asigura compatibilitatea înapoi (backward compatibility) pentru versiunile anterioare de API.

Modificările de API vor fi gestionate astfel încât să nu afecteze funcționalitățile existente fără o perioadă de tranziție.

Furnizorul va livra documentație completă pentru toate API-urile expuse.

Documentația va include:

- descrierea endpoint-urilor;
- structura request/response;
- coduri de eroare;
- exemple de utilizare.

Documentația va fi disponibilă într-un format standard (ex. OpenAPI/Swagger).

Platforma va expune un API bidirecțional pentru integrarea cu alte sisteme informatice interne sau externe. API-ul va permite:

- operațiuni de tip „pull data”;
- operațiuni de tip „push data”.

Platforma va oferi mecanisme pentru:

- integrarea cu sisteme de tip **IT Service Management (ITSM)**, astfel încât: anumite evenimente din platformă (de exemplu, eșecul unui deployment sau al unui workflow critic) să poată genera automat tichete de incident sau de schimbare;
- informațiile privind starea serviciilor și execuțiile relevante să poată fi consultate direct din sistemul ITSM;
- sincronizarea cu **baze de date de management al configurației (CMDB)**, prin:
  - expunerea de API-uri sau feed-uri de date care descriu resursele, relațiile dintre ele și starea lor;
  - posibilitatea actualizării automate a înregistrărilor CMDB la crearea, modificarea sau dezafectarea resurselor prin intermediul platformei.

De asemenea, platforma va permite integrarea cu alte sisteme prin:

- acțiuni din workflows de tip HTTP/HTTPS, GraphQL, SOAP, baze de date sau comenzi la distanță (SSH, scripturi);
- utilizarea de **webhook-uri** pentru a notifica aplicații externe la apariția unor evenimente relevante (de exemplu, finalizarea unui deployment, schimbarea stării unui job, apariția unui incident).

Sistemul trebuie să respecte condițiile Legii 242/2022 și standardele de interoperabilitate prevăzute în NRRI (Ordinul MCID nr. 21286 din 26.10.2023), privind schimbul de date și interoperabilitatea, respectiv să fie capabil să se conecteze și să comunice eficient cu alte sisteme informatice ale autorităților și instituțiilor publice, utilizând standarde deschise și API-uri bine definite prin utilizarea de standarde deschise (XML, JSON) și adoptarea unor protocoale de comunicare comune (ex. HTTPS, RESTful APIs).

Platforma dezvoltată în cadrul proiectului se va interconecta cu ROeID, și va folosi și această platformă pentru identificarea și autentificarea utilizatorilor. Având în vedere extinderea serviciilor pentru mai multe categorii de funcționari publici, interconectarea cu ROeID va aduce mari beneficii în acest sens, nefiind necesară înregistrarea pe portalul ANS a noilor utilizatori. Aceștia se vor putea folosi de ROeID pentru înregistrare.

Platforma dezvoltată în cadrul proiectului se va interconecta cu PDURo/PCUe (Portalul Digital Unic al României), conform Hotărârii Guvernului nr. 112/2023).

În contextul strategic național, soluția se aliniază cu direcțiile prevăzute de Strategia Națională de Cloud Guvernamental , de Strategia Națională pentru Transformare Digitală si de Cadrul European de Interoperabilitate (EIF), care promovează interoperabilitatea si digitalizarea serviciilor publice, adoptarea de soluții hibride și standarde deschise, reutilizarea componentelor software și consolidarea infrastructurilor informatice ale administrației publice.

Prin realizarea acestei investiții, ANS va obține o infrastructură IT unitară, flexibilă și sigură, pregătită pentru integrarea ulterioară a tehnologiilor emergente, cum ar fi automatizarea inteligentă, analiza predictivă sau managementul asistat de inteligență artificială.

4.8 Cerințe generale pentru aplicațiile web

4.8.1 Cerințe legate de implementarea funcțiilor de accesibilitate

Platforma va fi adaptata pentru a putea fi accesata si de utilizatori care suferă de diverse dizabilități, precum deficiente de vedere, auz, mobilitate etc.. În acest sens, interfețele de utilizator ale tuturor aplicațiilor livrate trebuie să respecte cerințele de accesibilitate minimale, conform legislației naționale în vigoare (OUG 112/2018 cu modificările și completările ulterioare precum și Norma din 2022 de monitorizare a conformității site-urilor web și a aplicațiilor mobile cu cerințele privind accesibilitatea), respectând de asemenea standardul WCAG 2.1 Level AA minim.

În cadrul proiectului vor fi respectate următoarele principii și cerințe:

Principii generale de accesibilitate:

1. **Perceptibilitate**:
   - Alternative textuale pentru conținut non-text (imagini, grafice).
   - Subtitrări și descrieri audio pentru conținut video și audio.
   - Contrast vizual minim între text și fundal (minim 4.5:1 pentru text normal).
2. **Operabilitate**:
   - Accesibilitate completă prin tastatură.
   - Navigare clară, consistentă, fără capcane de tastatură.
   - Evitarea elementelor care declanșează convulsii (ex. trei clipiri/secundă).
3. **Inteligibilitate**:
   - Structuri logice și relații între elemente.
   - Limbaj simplu și clar.
   - Mesaje de eroare descriptive și sugestii de corecție.
4. **Robustețe**:
   - Compatibilitate cu tehnologiile asistive și standarde de accesibilitate (EN 301 549, WCAG 2.1).

Cerințe tehnice:

1. **Niveluri de conformitate:**
   - Nivel minim: WCAG 2.1, nivel AA.
   - Încurajarea conformării la nivel AAA.
2. **Conținut media**:
   - Prezența subtitrărilor pentru conținut preînregistrat.
   - Descrieri alternative pentru hărți și diagrame interactive.
3. **Design și structură**:
   - Design responsiv pentru diverse dispozitive
   - Text redimensionabil fără pierderea conținutului.
   - Evitarea folosirii exclusive a culorilor pentru transmiterea informației.
4. **Testare și evaluare**:
   - Teste automate și manuale de accesibilitate.
   - Feedback de la utilizatori printr-un mecanism publicat pe site.

Obligații administrative:

1. **Declarația de accesibilitate**:
   - Publicată și actualizată periodic.
   - Include motivele eventualelor inaccesibilități și alternativele oferite.
2. **Monitorizare și raportare**:
   - Evaluări periodice ale conformității.
   - Rapoarte de inspecție realizate de organisme acreditate (tip A).
3. **Responsabilitate și instruire**:
   - Personal dedicat accesibilității și formare anuală.
   - Publicarea ghidurilor și a informațiilor despre cerințele de accesibilitate.

4.8.2 Interfață de utilizare adaptata la dispozitivul utilizat

În vederea asigurării unei experiențe de utilizare optime și adaptată indiferent de dispozitivul utilizat, vor fi implementate următoarele cerințe, atât în interfețele web ale soluției cât și în cea mobile.

- Responsivitate: Interfața va fi proiectată pentru a se adapta automat la dimensiunile și rezoluția ecranului dispozitivului utilizat (desktop, tabletă, telefon mobil).
- Design Flexibil: Se vor folosi tehnici de design responsiv, cum ar fi grile fluide și imagini flexibile, pentru a asigura o experiență de utilizare consistentă.
- Compatibilitate Cross-browser: Interfața va fi testată și optimizată pentru a funcționa corect pe toate browserele majore (Chrome, Firefox, Safari, Edge).

- Navigare Intuitivă: Elementele de navigare vor fi simplificate și ușor accesibile pe toate dispozitivele, utilizând meniuri hamburger pentru mobile și bare laterale pentru desktop.
- Performanță: Interfața va fi optimizată pentru a oferi timpi de încărcare rapizi pe toate dispozitivele, utilizând tehnici de optimizare a resurselor.
- Touch-friendly: Pe dispozitivele cu ecran tactil, interfața va fi proiectată cu butoane și elemente interactive suficient de mari pentru a fi ușor de utilizat.
- Feedback Vizual: Interfața va oferi feedback vizual clar pentru acțiunile utilizatorilor, cum ar fi apăsarea unui buton sau completarea unui formular.
- Accesibilitate: Se vor implementa bune practici de accesibilitate, cum ar fi suportul pentru cititoare de ecran și navigarea prin tastatură, pentru a asigura utilizarea de către persoanele cu dizabilități.

4.9 Cerințe legate de aplicațiile software dezvoltate

Aplicații software dezvoltate

Toate pachetele software și aplicațiile software dezvoltate vor fi livrate cu licențiere nelimitată/perpetuă și cu transfer total sau parțial al codului sursă și a livrabilelor cu posibilitatea modificării ulterioare de către beneficiar a aplicației livrate. Vor fi acceptate atât soluții open-source cât și comerciale de tip COTS (commercial off the shelf)

Opțiunea licențierii fără limitări a soluției și transferul codului sursă și a livrabilelor în formă prelucrabilă/editabilă, va permite instituției modificarea sub orice formă a soluției fără a depinde de furnizor.

Codul sursă livrat către instituție va fi compilabil și funcțional, respectând următoarele cerințe:

1. **Licență Open Source sau COTS:**
   - Aplicația trebuie să fie distribuită sub o licență open-source recunoscută (de exemplu, MIT, Apache 2.0, GPLv3), care permit beneficiarului să aibă acces/drept de proprietate nemijlocit la codul sursă,

   sau

   - Aplicația trebuie să fie distribuită sub o licență comercială de tip COTS, care să permită beneficiarului să aibă acces/drept de proprietate la codul sursa dezvoltat în cadrul proiectului pentru personalizările realizate conform cerințelor proiectului.
   - Toate componentele și bibliotecile utilizate trebuie să aibă licențe compatibile cu licența principală a aplicației.
   - Se va evita folosirea de pachete software pe bază de subscripție. În cazul în care nu este posibil, toate costurile vor fi clar detaliate în ofertă, atât cele incluse în ofertă cât și cele ulterioare.
2. **Servicii de mentenanță și suport**
   - Întregul sistem va fi livrat cu minim un an de suport tehnic asigurat, ce va include mentenanța corectivă pentru toate pachetele software și funcționalitățile livrate.

- Furnizorul soluției trebuie să ofere posibilitatea de achiziție de mentenanța corectivă și evolutivă a întregului sistem dezvoltat pe o perioadă de minim 5 ani.
- În cazul în care Autoritatea Contractantă solicită modificări/adaptări în structura website-ului, prestatorul se obligă să efectueze, conform solicitărilor, toate activitățile prevăzute în prezentul caiet de sarcini, pe toată durata de implementare a contractului.

3. **Actualizări**
   - Sistemul va fi actualizat pe toată durata contractului (vulnerabilități, probleme tehnice etc.)
4. **Documentație Completă:**
   - Codul sursă trebuie să fie însoțit de documentația tehnică completă, care include descrierea arhitecturii sistemului, specificațiile funcționale și nefuncționale, ghidul de instalare și configurare, precum și manualul de utilizare.
   - Vor fi livrate codurile sursă necompilate, editabile, comentate și documentate, ale părților componente ale website-ului, inclusiv a elementelor de grafică, precum și toate informațiile relevante privind programele folosite pentru dezvoltare, kit instalare pentru software standard, kit sau procedură de instalare pentru elementele custom.
   - Documentația trebuie să fie clară, concisă și ușor de înțeles.
5. **Structura Codului:**
   - Beneficiarul va avea acces nemijlocit la codul sursă pentru dezvoltări/modificări ulterioare.
   - Codul sursă trebuie să fie bine organizat, cu o structură logică a directoarelor și a fișierelor.
   - Orice adăugiri sau modificări ale codului sursă default vor fi clar evidențiate și explicate.
   - Fiecare fișier de cod trebuie să conțină un antet cu informații despre autor, data creației și descrierea funcționalității.
6. **Calitatea Codului:**
   - Codul trebuie să respecte standardele de codare convenite de dezvoltatorul limbajului de programare sau a mediului de dezvoltare (de exemplu, PEP 8 pentru Python, PSR-12 pentru PHP).
   - Codul trebuie să fie curat, comentat adecvat și să evite redundanțele.
7. **Testare și Validare:**
   - Codul sursă trebuie să includă un set complet de teste unitare, teste de integrare și, dacă este cazul, teste de performanță.
   - Toate testele trebuie să fie documentate și să includă instrucțiuni pentru rularea lor.
8. **Compatibilitate și Interoperabilitate:**
   - Codul trebuie să fie compatibil cu platformele și sistemele specificate în caietul de sarcini.

- Codul trebuie să respecte standardele de interoperabilitate și să includă mecanisme pentru integrarea cu alte sisteme.

9. **Licențiere și Proprietate:**
   - Instituția publică trebuie să dețină drepturile necesare pentru utilizarea și modificarea codului.
   - Licențele pentru software-ul dezvoltat oferit trebuie să fie perpetue.

4.10 Securitatea sistemului

Sistemul informatic care face obiectul achiziției va trebuie să asigure un nivel ridicat de securitate cibernetică, adecvat unui sistem informatic utilizat în sectorul public, expus prin API-uri și integrat cu alte sisteme instituționale și externe. Securitatea va fi concepută independent de orice interfață grafică și va fi aplicată unitar tuturor punctelor de acces.

Platforma va trebui protejată împotriva unui spectru larg de amenințări cibernetice, asigurând confidențialitatea, integritatea și disponibilitatea datelor, precum și protecția informațiilor aparținând organizației și utilizatorilor săi.

Toate serviciile expuse prin API-uri vor avea mecanisme proprii de securitate, incluzând autentificare, autorizare, validare a parametrilor și limitarea frecvenței cererilor. Sistemul va fi protejat împotriva executării de comenzi malițioase asupra bazelor de date și a tentativelor de acces neautorizat.

Sistemul va genera loguri detaliate pentru toate operațiunile relevante de securitate, inclusiv autentificări, autorizări, accesări de date și apeluri API. Aceste loguri vor fi protejate împotriva modificării și vor permite auditarea completă a activităților.

Vor fi implementate mecanisme de monitorizare continuă pentru detectarea comportamentelor suspecte și a incidentelor de securitate.

Accesul la rețea va fi controlat strict, iar canalele de comunicație vor fi securizate prin protocoale criptate și, unde este cazul, VPN.

Bazele de date vor fi protejate împotriva accesului direct neautorizat, fiind accesibile exclusiv prin intermediul serviciilor backend autorizate. Vor fi implementate mecanisme de control al accesului, criptare, audit și backup regulat.

Prestatorul va pune la dispoziție soluția livrată, în forma complet integrată, pentru efectuarea testelor de penetrare (black box și white box) și a auditului tehnic, realizate de terțe părți contractate de Autoritatea Contractantă prin proceduri separate de achiziție.

Prestatorul va asigura, fără costuri suplimentare, toate elementele necesare desfășurării acestor activități, incluzând, dar fără a se limita la: – acces la mediile de test și producție (după caz); – conturi dedicate; – documentație tehnică; – arhitectură și diagrame; – cod sursă (acolo unde este aplicabil); – suport tehnic pe durata derulării testelor și auditului.

Recepția finală a soluției se va realiza numai după remedierea integrală a tuturor vulnerabilităților, neconformităților sau deficiențelor identificate în cadrul testelor de penetrare și al auditului tehnic, confirmarea remedierii fiind realizată de entitatea terță care a efectuat verificările.

Rezultatele testelor vor fi documentate, iar vulnerabilitățile identificate vor fi remediate și retestate.

Sistemul va include mecanisme de backup regulat și proceduri clare de recuperare în caz de incidente. Aceste proceduri vor fi testate periodic pentru a asigura continuitatea serviciilor și integritatea datelor.

Pe lângă cerințele funcționale de securitate detaliate în capitolele următoare, soluția trebuie să respecte și un set de cerințe non-funcționale care privesc modul de operare, izolare și audit. Se impune ca:

- mediile de lucru (dezvoltare, testare, pre-producție, producție) să fie clar segregate, atât din punct de vedere al infrastructurii (rețele, acces la date), cât și al drepturilor de acces, astfel încât datele și configurațiile sensibile din producție să nu fie expuse în medii inferioare;
- toate acțiunile importante (autentificări, modificări de configurare, execuții de fluxuri, operațiuni asupra resurselor critice) să fie jurnalizate în mod centralizat, astfel încât să existe audit complet și trasabilitate pentru „cine a făcut ce și când”;
- accesul la platformă și la resursele administrate să fie acordat conform principiului „least privilege”, cu roluri bine definite și cu revizuiri periodice ale drepturilor.

Din perspectivă non-funcțională, se va asigura că:

- logurile de securitate și de audit pot fi exportate sau integrate cu sisteme existente de tip SIEM sau alte platforme de monitorizare a securității, în conformitate cu politicile instituției;
- există posibilitatea de a configura politici de retenție a logurilor, în concordanță cu cerințele legale și interne (de exemplu, păstrarea anumitor categorii de loguri pe perioade extinse);
- configurările de securitate pot fi revizuite și adaptate în timp, fără a afecta disponibilitatea generală a serviciilor.

Vor fi implementate mecanisme de monitorizare continuă pentru detectarea comportamentelor suspecte și a incidentelor de securitate.

Toate serviciile expuse prin API-uri vor avea mecanisme proprii de securitate, incluzând autentificare, autorizare, validare a parametrilor și limitarea frecvenței cererilor. Sistemul va fi protejat împotriva executării de comenzi malițioase asupra bazelor de date și a tentativelor de acces neautorizat.

Sistemul va genera loguri detaliate pentru toate operațiunile relevante de securitate, inclusiv autentificări, autorizări, accesări de date și apeluri API. Aceste loguri vor fi protejate împotriva modificării și vor permite auditarea completă a activităților.

Accesul la rețea va fi controlat strict, iar canalele de comunicație vor fi securizate prin protocoale criptate și, unde este cazul, VPN.

Bazele de date vor fi protejate împotriva accesului direct neautorizat, fiind accesibile exclusiv prin intermediul serviciilor backend autorizate. Vor fi implementate mecanisme de control al accesului, criptare, audit și backup regulat.

Sistemul trebuie să fie prevăzut cu capabilități de tip Data Loss Prevention (DLP), care să asigure detectarea și prevenirea exfiltrării neautorizate a datelor, monitorizarea fluxurilor de date și aplicarea automată a politicilor de protecție a datelor sensibile.

Sistemul va respecta Regulamentul (UE) 2016/679 și legislația națională aplicabilă. Vor fi implementate mecanisme de anonimizare, clasificare și identificare automată a documentelor care conțin date cu caracter personal.

Sistemul va include mecanisme de backup regulat și proceduri clare de recuperare în caz de incidente. Aceste proceduri vor fi testate periodic pentru a asigura continuitatea serviciilor și integritatea datelor.

Sistemul achiziționat va trebui să respecte si să aibă implementate minim următoarele măsuri de securitate:

1. **Securitatea aplicațiilor web dezvoltate – implementare cod sursa securizat:**

Ofertantul va avea obligația de a realiza implementarea codului sursă conform principiilor de secure coding, utilizând standarde și bune practici de securitate în dezvoltarea software, în scopul reducerii riscurilor de vulnerabilități și al asigurării unui nivel adecvat de securitate al aplicației cu respectarea minimal a următoarelor cerințe:

- Security by Design: Platforma va fi proiectată incorporând principii de securitate încă de la început, pentru a asigura că toate funcțiile și modulele sunt construite cu considerații de securitate integrate, minimizând astfel riscurile și vulnerabilitățile. Furnizorul va demonstra că securitatea nu este tratată ca un element adițional, ci ca parte fundamentală a arhitecturii sistemului.
- Secure Coding: Dezvoltarea aplicației se va realiza respectând practici de codare sigură, recunoscute la nivelul industriei, incluzând standarde precum OWASP. Codul sursă va fi supus proceselor de revizuire și analiză de securitate, atât statică, cât și dinamică, pentru identificarea și eliminarea vulnerabilităților înainte de punerea în producție.
- Validarea Inputului: Toate datele primite de sistem prin API-uri, indiferent de sursă, vor fi validate și sanitizate riguros. Sistemul va preveni atacuri de tip SQL Injection, Cross-Site Scripting (XSS), command injection sau alte vulnerabilități asociate procesării inputului nesecurizat. Validarea va fi realizată atât la nivel de structură, cât și la nivel de conținut, utilizând reguli stricte și scheme de validare definite explicit pentru fiecare API.
- Protecția Datelor Sensibile: Datele sensibile și datele cu caracter personal vor fi protejate prin mecanisme de criptare atât în tranzit, cât și la stocare. Toate comunicațiile dintre componentele sistemului, precum și între clienți și backend, vor utiliza protocoale criptografice securizate (TLS).
- Măsuri de securitate aplicate bazelor de date: vor fi implementate măsuri sporite de securitate la nivelul bazelor de date, pentru a evita accesarea directă a acestora prin eludarea aplicațiilor web și a interfețelor de acces (control acces, criptare date, monitorizare și audit, back-up regulat, actualizări permanente etc.).

2. **Securitate operațională și protecția datelor sensibile**

Securitatea trebuie să fie integrată în mod transversal în toate componentele platformei, de la gestionarea secretelor și a credențialelor până la controlul accesului și protecția lanțului software.

Scopul acestui capitol este să detalieze cerințele de securitate operațională care completează principiile arhitecturale și cerințele funcționale descrise în capitolele anterioare.

Platforma trebuie sa aibă capabilitatea să asigure:

- protecția centralizată a secretelor și a informațiilor sensibile utilizate în infrastructură, în clusterele Kubernetes și în fluxurile de lucru;
- verificarea continuă a imaginilor container și a componentelor software utilizate, pentru reducerea riscului de vulnerabilități;
- guvernanța accesului pe baza de politici și roluri, cu procese automatizate de acordare și retragere a drepturilor.

Aceste capabilități sunt esențiale pentru instituțiile publice care operează medii hibride și complexe, în care atât conformitatea, cât și reducerea riscului operațional sunt critice.

3. Gestionarea centralizată a secretelor

Platforma are capabilitatea să gestioneze centralizat secretele și datele sensibile (chei API, parole, token-uri de acces, certificate, string-uri de conexiune la baze de date) prin intermediul unui serviciu dedicat de tip „vault”, integrat direct în interfața de lucru și în motorul de orchestrare.

Soluția trebuie să asigure că:

- secretele sunt stocate criptat, folosind algoritmi moderni și chei gestionate în condiții de siguranță;
- accesul la secrete este controlat pe baza de roluri și scopuri (workspaces, proiecte, clustere), astfel încât fiecare utilizator sau flux de lucru are acces doar la informațiile strict necesare;
- secretelor le sunt asociate metadate (nume, descriere, categorie, scop, proprietar), pentru a permite o administrare clară și o auditare eficientă.

În cadrul platformei, secretele sunt:

- expuse operatorilor și proiectanților de fluxuri printr-un mecanism controlat de selecție (de exemplu, secțiunea de „Variables”/„Secrets” în editorul de workflow), fără a afișa valoarea în clar;
- organizate pe grupuri și scopuri (de exemplu: secrete pentru conectarea la un anumit cluster Kubernetes, secrete pentru un sistem de baze de date, secrete pentru un anumit furnizor de cloud), permițând reutilizarea controlată și evitarea duplicării inutile;
- disponibile în mod standardizat în pașii de execuție (scripturi, apeluri de API, acțiuni DevOps), prin funcții predefinite sau variabile de mediu, fără ca utilizatorii să fie nevoiți să copieze manual valori sensibile.

Platforma trebuie să permită revocarea rapidă a unor chei sau credențiale compromise, cu propagarea imediată a schimbărilor în fluxurile de lucru și în componentele dependente.

Prin utilizarea gestionării centralizate a secretelor, platforma reduce riscul expunerii datelor sensibile în cod, fișiere de configurare sau scripturi și asigură un model de securitate compatibil cu cerințele stricte ale sectorului public.

4. **Access governance automatizat și control al privilegiilor**

Pe lângă autentificare și autorizare (gestionate prin modulele de identitate și RBAC descrise în capitolele dedicate), platforma trebuie să asigure și o guvernanță automatizată a accesului, astfel încât drepturile utilizatorilor și ale sistemelor să fie aliniate constant la principiul „least privilege”.

Platforma are capabilitatea să:

- aplice politici centralizate de acces pentru utilizatori, grupuri și aplicații, definind clar ce operațiuni sunt permise asupra resurselor (workflows, clustere, șabloane, secrete);
- implementeze procese de grant/revoke automatizat pentru acces, pe baza unor evenimente de tip onboarding/offboarding, schimbare de rol sau de apartenență la un grup organizațional;
- integreze politicile de acces cu mecanismele de audit și cu modulul de identitate, astfel încât orice modificare de drepturi să fie urmărită și justificată.

În contextul instituțiilor publice, access governance înseamnă:

- definirea de roluri standardizate (administrator de platformă, operator de infrastructură, dezvoltator, utilizator de business) cu seturi de permisiuni predefinite;
- implementarea unor fluxuri de aprobare pentru atribuirea unor drepturi sensibile (de exemplu, acces la secrete, drept de modificare a fluxurilor critice, acces la medii de producție);
- posibilitatea de a efectua recertificări periodice ale drepturilor, prin revizuirea și confirmarea de către responsabili a faptului că utilizatorii mai au nevoie de accesul acordat.

Platforma trebuie să sprijine aceste procese prin:

- interfețe clare pentru vizualizarea permisiunilor și a rolurilor alocate;
- rapoarte privind utilizarea efectivă a drepturilor (de exemplu: roluri neutilizate, conturi inactive, acces rareori folosit la resurse sensibile);
- integrare cu modulul de audit, astfel încât fiecare decizie de acordare sau retragere a accesului să fie documentată.

Prin access governance automatizat, instituția poate demonstra, în fața auditorilor interni și externi, că are un control ferm asupra accesului la resursele critice și asupra modului în care sunt utilizate cpabilitățile platformei.

5. **Securitate la nivel de rețea: instalarea unui echipament de tip firewall care să realizeze:**

- Filtrarea Traficului: Blochează traficul nedorit și permite traficul legitim prin reguli prestabilite și tehnologii de tip whitelisting/blacklisting.
- Protecție împotriva Atacurilor: Previne atacurile de tip DDoS, malware, și alte tipuri de intruziuni.

- Monitorizare și Logare: Înregistrează activitățile de rețea și ajută la detectarea comportamentelor suspecte.
- VPN: Permite accesul securizat la rețea prin tuneluri criptate.
- Controlul Accesului: Gestionarea accesului utilizatorilor și dispozitivelor la diferite părți ale rețelei.
- Web application firewall.
- Să dispună de tehnologii de securitate utilizate pentru a detecta și preveni accesul neautorizat sau activitățile malițioase într-o rețea sau un sistem informatic (IDS/IPS).

6. **Web Application Firewall (WAF):**

- Va fi implementat un firewall pentru aplicații web, configurat pentru a detecta și bloca atacuri cibernetice specifice aplicațiilor web, cum ar fi SQL Injection și Cross-Site Scripting (XSS).

7. **DDOS Protection:**

- Platforma va include protecție împotriva atacurilor de tip Distributed Denial of Service (DDOS), utilizând soluții avansate pentru a asigura disponibilitatea și performanța în fața acestor amenințări.

8. **Securitate la nivel de servere și sisteme de operare:**

- Actualizări Regulate: Se vor instala toate actualizările de securitate și patchurile sistemelor de operare și aplicațiilor instalate, oferite de producătorii/furnizorii acestora.
- Antivirus și Anti-malware: Se vor utiliza soluții antivirus și anti-malware actualizate.
- Firewall: Va fi activat și configurat firewall-ul pentru a bloca accesul neautorizat.
- Controlul Accesului: Se vor utiliza controale stricte de acces și permisiuni pe fișiere și directoare.
- Politici de Parole: Se vor implementa politici stricte de parole, incluzând complexitate și rotație regulată.
- Autentificare Multi-factor: Va fi activată autentificarea mulți-factor pentru conturi critice.
- Criptare: Se va utiliza BitLocker sau soluții similare pentru criptarea hard diskurilor.
- Audit și Monitorizare: Se vor configura auditarea și monitorizarea logurilor de securitate.
- Dezactivarea Serviciilor Neutilizate: Se vor dezactiva și elimina serviciile și aplicațiile neutilizate.
- Backup-uri Regulate: Se vor efectua backup-uri regulate și testa restaurarea datelor.

9. **Securitate la nivelul soluției de virtualizare, prin abordarea următoarelor:**

- Izolare și Segregare: Se asigură izolarea mașinilor virtuale pentru a preveni accesul neautorizat între ele.
- Managementul Patch-urilor: Se actualizează regulat hipervizorul și VM-urile pentru corectarea vulnerabilităților.

- Autentificare și Autorizare: Se utilizează autentificarea mulți-factor și controlul strict al accesului.
- Monitorizare și Logare: Se implementează sisteme de monitorizare și logare pentru detectarea activităților suspecte.
- Criptare: Se criptează datele în tranzit și la rest pentru protejarea informațiilor sensibile.
- Back-up: Se realizează copii de siguranță periodice și se testează procedurile de recuperare.

10. **Securitate la nivelul endpoint (stațiilor desktop/laptop)**

- Achiziția și instalarea unei soluții de tip endpoint security, care să poată fi instalată atât pe servere (Windows, Linux, CentOS) cât și pe sisteme endpoint (desktop/laptop). Soluția trebuie să ofere protecție antimalware împotriva atacurilor de tip 0-day, exploiturilor cunoscute, amenințărilor web, atacurilor de phishing și ransomware. T
- rebuie să utilizeze machine learning pentru detecție atacuri cibernetice și să includă protecție împotriva atacurilor fără fișiere (fileless), precum și un Sandbox Analyzer pentru a combate atacurile avansate. Soluția trebuie să dispună de un firewall la nivel de host și să dispună de un dashboard centralizat în care să fie disponibile toate alertele la nivel de instituție. Specificațiile complete ale acestei soluții vor fi realizate în faza de scriere a caietului de sarcini.

11. **Soluție pentru identificarea vulnerabilităților din infrastructură pentru a detecta, analiza și gestiona vulnerabilitățile de securitate dintr-un sistem informatic, rețea sau aplicație.**

- Aceasta va fi folosită pentru identificarea periodică a vulnerabilităților în vederea remedierii acestora.

Sistemul va respecta Regulamentul (UE) 2016/679 și legislația națională aplicabilă. Vor fi implementate mecanisme de anonimizare, clasificare și identificare automată a documentelor care conțin date cu caracter personal.

Soluția va fi considerată conformă din punct de vedere al securității doar dacă toate măsurile descrise în prezentul capitol sunt implementate și funcționale, iar sistemul demonstrează reziliență la atacuri și conformitate cu cerințele legale și tehnice aplicabile.

4.10.1 Managementul utilizatorilor si accesul la sistem – 1 pachet

Platforma va asigura guvernanța completă a identităților digitale, a drepturilor de acces și a modului în care utilizatorii, aplicațiile și serviciile interacționează cu resursele IT ale instituției.

Soluția trebuie să includă un serviciu centralizat de tip Identity Provider (IdP), care oferă Single Sign-On (SSO), autentificare multiplă (MFA), managementul ciclului de viață al utilizatorilor și grupurilor, precum și integrare cu directoare și furnizori de identitate existenți (ex. LDAP/Active Directory, IdP extern, furnizori cloud de identitate).

Prin acest modul de identificare și control al accesului, platforma va permite:

- administrarea centralizată a identităților și rolurilor;
- aplicarea unificată a politicilor de securitate asupra aplicațiilor și resurselor;

- trasabilitatea completă a autentificărilor, a modificărilor de drepturi și a operațiunilor administrative;
- conformitatea cu standarde și bune practici (ex. ISO/IEC 27001) și cu cerințele legale aplicabile (inclusiv din perspectiva protecției datelor)
- autentificarea participanților prin soluția **ROeID**, conform cerințelor naționale privind identificarea electronică.
- Implementarea de principii **Zero Trust**, fără încredere implicită pentru niciun utilizator sau dispozitiv.

Soluția de management a identității utilizatorilor, va fi furnizată ca platformă unificată de **Management al Identității și Accesului.**

Soluția va îndeplini următoarele cerințe tehnico-funcționale minimale si obligatorii:

- va permite implementarea în regim on-premises, în cloud privat sau în cloud public controlat de autoritatea contractantă, fără dependență funcțională obligatorie de servicii SaaS externe pentru funcțiile de autentificare, autorizare, federare și provisioning.
- va suporta instalarea și operarea în regim containerizat, inclusiv în Docker/Compose și Kubernetes, cu scalare orizontală, componente server/worker de tip stateless, toleranță la defecte și funcționare în arhitecturi de înaltă disponibilitate bazate pe PostgreSQL, cu mecanisme de redundanță și replicare.
- va asigura, în cadrul aceleiași soluții și al aceluiași plan de administrare, gestionarea identităților, a politicilor, a componentelor edge, a fluxurilor din ciclul de viață și a resurselor de integrare/operaționalizare, cu model unitar de RBAC, audit și configurare declarativă.
- va permite administrarea declarativă, versionabilă și transportabilă a configurației, prin fișiere structurale, cu aplicare atomică, reconciliere automată și reutilizarea configurațiilor între medii.
- va include o bibliotecă versionată de șabloane reutilizabile pentru fluxuri, politici, formulare, integrări și resurse de implementare, cu posibilitatea de export și import între proiecte sau medii, actualizări în bloc sau punctuale, istoric al versiunilor și rollback.
- va permite instalarea, actualizarea și operarea declarativă a componentelor de control și edge în platforme de orchestrare containerizată, cu implementare etapizată controlată, administrare multi-locație și suport pentru practici de tip GitOps.
- va suporta administrarea în regim multi-cluster și multi-mediu, cu separarea mediilor de dezvoltare, test, staging și producție, definirea clusterelor țintă, actualizări controlate și trasabilitate completă a implementărilor.
- va permite operaționalizarea dependențelor sale și a resurselor asociate și prin mecanisme de tip Infrastructure as Code, cu șabloane parametrizabile, versionare, reluarea controlată a execuțiilor eșuate și rollback.
- va integra un mecanism centralizat de management al secretelor și credențialelor, utilizabil în mod unitar de fluxuri, componente edge, implementări și operațiuni runtime, cu rotație controlată, token-uri de serviciu cu privilegii minime și audit.

- va permite audit tehnic independent al componentelor critice, al configurațiilor de securitate și al interfețelor expuse, inclusiv exportul artefactelor necesare verificării.
- va funcționa nativ ca furnizor de identitate/autentificare pentru cel puțin următoarele protocoale și mecanisme: OAuth 2.0 / OpenID Connect, SAML 2.0, LDAP, RADIUS, SCIM 2.0 și application proxy / forward-auth pentru aplicații fără suport nativ de federare.
- va putea funcționa și ca hub de federare / sursă externă de identitate pentru cel puțin: Kerberos, LDAP, OAuth/OIDC, SAML și SCIM, inclusiv sincronizarea utilizatorilor și grupurilor din sisteme externe.
- va putea funcționa atât în rol de Identity Provider / OpenID Provider, cât și în rol de Service Provider / Relying Party, în funcție de scenariul de integrare.
- În zona OAuth 2.0 / OIDC, CMIU va suporta cel puțin fluxurile authorization code, client_credentials, implicit, hybrid și device code, precum și PKCE, rotația refresh token-urilor și validarea strictă a redirect URI, inclusiv pe bază de expresii regulate controlate administrativ.
- În zona SAML 2.0, CMIU va suporta semnarea răspunsurilor și a aserțiunilor, criptarea aserțiunilor, precum și binding-urile HTTP-Redirect și HTTP-POST.
- va suporta Single Logout centralizat pentru aplicații OIDC și SAML, inclusiv variante front-channel și back-channel, precum și logout administrativ forțat prin terminarea sesiunilor.
- va suporta SCIM 2.0 atât pentru provisioning și sincronizare către aplicații externe, cât și pentru provisioning dinspre clienți SCIM către platformă, pentru obiecte de tip Users și Groups, inclusiv autentificare la endpoint-urile țintă prin token static sau token dinamic de tip OAuth cu durată scurtă de viață.
- va permite protejarea aplicațiilor fără suport nativ SSO printr-o componentă integrată de tip reverse proxy/forward-auth, cu propagarea identității către aplicația protejată prin antete HTTP, JWT, JWKS și atribute configurabile în funcție de utilizator, grup sau context.
- va include capabilități native de integrare la marginea infrastructurii pentru validarea și aplicarea politicilor de acces pe JWT/JWKS, OAuth 2.0, CORS, ACL, cote și mTLS între punctul de control și aplicațiile protejate.
- va putea integra protecția aplicațiilor web prin principalele reverse proxy-uri, controlere de ingress și service mesh-uri utilizate în infrastructuri moderne.
- va include componente edge implementabile separat în rețele, zone de securitate sau locații distincte, inclusiv on-premises, DMZ și Kubernetes, pentru funcții de tip proxy, LDAP, RADIUS și alte funcții conexe, cu conectare securizată la planul de control, configurare centralizată, actualizare controlată și token-uri de serviciu cu privilegii minime.
- va permite centralizarea accesului la resurse de administrare și operare la distanță prin protocoale RDP, SSH și VNC, utilizând același motor de politici și aceeași platformă de identitate.

- va include un furnizor LDAP cu suport pentru LDAPS, StartTLS, compatibilitate extinsă de schemă, direct bind, cached bind, direct search și cached search, precum și control RBAC asupra accesului de căutare în director.
- va permite aplicarea MFA inclusiv în fluxurile LDAP bind.
- va include un furnizor RADIUS cu suport pentru PAP și EAP-TLS, reutilizând același motor de fluxuri și politici ca pentru autentificarea web, precum și definirea dinamică a atributelor vendor-specific.
- va suporta autentificarea de tip Machine-to-Machine (M2M) prin conturi tehnice și token-uri dedicate, nu exclusiv prin secret static de client.
- va implementa un motor de orchestrare a fluxurilor de identitate bazat pe fluxuri, etape și politici, configurabile fără dezvoltări intruzive în aplicațiile protejate.
- va suporta distinct cel puțin următoarele tipuri de fluxuri: Authentication, Authorization, Enrollment, Invalidation/Logout, Recovery, User settings / self-service și Unenrollment.
- va permite atașarea de politici la nivel de flux, etapă, aplicație, furnizor, sursă externă, utilizator și grup.
- va suporta politici programabile și mapări configurabile pentru transformarea atributelor, a claim-urilor, a grupurilor și a altor date de identitate, atât la intrarea din surse externe, cât și la expunerea către aplicațiile consumatoare.
- va permite aplicarea de acces condiționat pe baza contextului de autentificare, incluzând cel puțin utilizator, grup, aplicație, sursă, domeniu, orar, adresă IP, locație, ASN și nivel de risc, precum și politici standard pentru GeoIP/ASN.
- va permite modelarea vizuală a fluxurilor identitare și din ciclul de viață prin apeluri API, transformări, condiții, ramificații, bucle, execuții paralele și reutilizarea componentelor.
- va putea consuma surse și mecanisme declanșatoare configurabile de evenimente, inclusiv webhook-uri, mesaje și sisteme externe, cu corelare și filtrare în timp real pentru declanșarea automată a fluxurilor identitare.
- va permite formulare electronice dinamice pentru cereri identitare în regim self-service, cu validări, mecanisme de aprobare, transmitere automată a datelor către fluxuri și posibilitatea de includere în portaluri sau aplicații externe.
- va suporta fluxuri în regim self-service pentru înrolare, recuperare credențiale, administrare profil utilizator, ștergere/dezactivare cont și inițiere de cereri de acces sau modificare de drepturi.
- CMIU-36. Fluxurile publice de identificare și autentificare vor include mecanisme care să prevină enumerarea utilizatorilor, astfel încât interfața să nu confirme explicit existența sau inexistența unui cont.
- va permite definirea de experiențe distincte pentru fiecare domeniu sau wildcard de domeniu, inclusiv branding, localizare, fluxuri implicite și redirecționare către aplicația implicită după autentificare.

- va permite administrarea centralizată a utilizatorilor, grupurilor, rolurilor, permisiunilor, conturilor tehnice și token-urilor, cu model RBAC și principiul privilegiului minim.
- va permite sincronizarea utilizatorilor, grupurilor și apartenențelor la grupuri din surse externe, inclusiv prin LDAP, Kerberos, OAuth/OIDC, SAML și SCIM, cu reguli de mapare personalizabile.
- va permite provisioning și deprovisioning automate de utilizatori și grupuri pe baza standardelor și a API-urilor suportate, inclusiv prin SCIM și surse federate.
- va include capabilități native de automatizare a ciclului de viață al identităților, declanșabile pe bază de evenimente, pentru minimum: onboarding, offboarding, aprobare, creare, actualizare sau dezactivare de cont, atribuire și revocare de grupuri/roluri, remediere și cleanup.
- va permite conturi de serviciu neinteractive, bazate exclusiv pe token, cu expirare configurabilă, rotație automată, revocare explicită și separarea clară între token-uri API și parole de aplicație.
- va permite propagarea către aplicațiile consumatoare a datelor de autorizare relevante, inclusiv grupuri, entitlements, atribute și claim-uri personalizate.
- va permite, în cadrul fluxurilor identitare, execuții operaționale securizate prin apeluri API, scripturi Bash/Shell, PowerShell și comenzi SSH, cu izolare a execuțiilor, management securizat al secretelor și audit detaliat per execuție.
- va expune API-uri REST atât pentru administrarea funcțiilor identitare, cât și pentru interogarea detaliilor operaționale privind fluxurile, execuțiile și deployment-urile, în vederea integrării cu sisteme externe de monitorizare, audit sau ITSM.
- va suporta MFA prin cel puțin: TOTP, WebAuthn/FIDO2/U2F, passkeys, OTP prin e-mail, SMS, coduri statice/de rezervă și integrare cu factori externi de autentificare, acolo unde este necesar.
- va permite administratorului controlul tipurilor de autentificatori acceptați, aplicarea de politici de tip step-up, frecvența de revalidare MFA și definirea situațiilor în care autentificarea cu passkey este suficientă sau trebuie completată cu un factor suplimentar.
- Implementarea WebAuthn/FIDO2 va suporta chei hardware, autentificatori de platformă și autentificatori de pe dispozitive mobile, precum și restricții configurabile privind tipurile de dispozitive admise.
- va permite controlul sesiunilor pe baza mecanismelor de network binding și GeoIP binding, terminarea automată a sesiunilor care își schimbă nejustificat contextul de rețea sau geolocație și revocarea sesiunilor anterioare ale aceluiași utilizator la autentificare.
- va include mecanisme de detecție a autentificărilor suspecte pe baza țării, a ASN și a scenariilor de tip impossible travel.
- va permite, pentru scenarii cu cerințe ridicate de confidențialitate, criptarea token-urilor OAuth/OIDC, nu doar semnarea acestora.
- va suporta impersonarea administrativă controlată, cu posibilitatea dezactivării globale și cu obligativitatea introducerii unui motiv justificativ.

- va înregistra toate evenimentele relevante de utilizator și de sistem, fără salvarea în clar a parolelor sau a altor credențiale sensibile în loguri.
- va asigura audit trail la nivel de câmp pentru modificările de configurație și ale obiectelor de identitate, cu valorile anterioare și cele noi, precum și cu mascarea valorilor sensibile.
- va permite definirea de reguli de notificare pentru evenimente, cu transport prin interfață locală, e-mail și webhook.
- va permite căutare avansată, export și păstrare configurabilă a jurnalelor și evenimentelor.
- va permite exportul logurilor, metricilor și traselor către ecosistemul de monitorizare al autorității contractante, cu trasabilitate pe cereri și sesiuni și compatibilitate cu standarde de observabilitate de tip OpenTelemetry.
- va asigura observabilitate și audit end-to-end, în cadrul aceluiași model de trasabilitate, pentru autentificări, provisioning, formulare, fluxuri, execuții operaționale, implementări și componente edge, cu corelarea contextului de tip cerere–sesiune–execuție.

4.10.2 Securitate și conformitate – 1 pachet

Securitatea și conformitatea sunt elemente centrale ale platformei de orchestrare, având în vedere mediul specific al instituțiilor publice, în care sunt procesate date sensibile și sunt operate sisteme critice pentru funcționarea administrației.

Platforma trebuie să trateze securitatea nu ca pe un modul separat, ci ca pe o proprietate transversală a întregii arhitecturi: de la autentificarea utilizatorilor și autorizarea accesului, până la protejarea secretelor, auditarea acțiunilor și integrarea cu procesele de management al vulnerabilităților.

Soluția va asigura:

- autentificare unificată a utilizatorilor, prin integrare cu sursele de identitate deja existente (ex. LDAP, Active Directory sau alți furnizori compatibili), cu suport pentru Single Sign-On (SSO) și autentificare multifactor (MFA);
- control granular al accesului prin mecanisme de tip Role-Based Access Control (RBAC), în care drepturile sunt configurate pe roluri și grupuri;
- gestionarea centralizată și securizată a secretelor (chei, parole, token-uri) printr-un serviciu dedicat de tip vault, integrat cu workflows-urile și conectorii platformei;
- audit și trasabilitate completă a acțiunilor efectuate în platformă, pentru a permite demonstrarea conformității în fața organismelor de control;

Prin acest set de capabilități, platforma oferă un cadru coerent pentru implementarea principiilor „security by design” și „defense in depth”, în acord cu cerințele standardelor de securitate (ex. ISO/IEC 27001) și ale reglementărilor privind protecția datelor (ex. GDPR).

4.10.2.1 Autentificare unificată și Single Sign-On (SSO)

Platforma trebuie să asigure un **mecanism unificat de autentificare** pentru toți utilizatorii, tehnici și non-tehnici, astfel încât identitatea să fie gestionată central, iar accesul la resursele administrate de platformă să fie coerent și controlabil.

a) Integrare cu surse de identitate existente

Soluția trebuie să permită integrarea cu sursele de identitate deja utilizate de instituție, cum ar fi:

- directoare de tip LDAP;
- servicii de Active Directory (AD);
- alți furnizori compatibili cu standarde de identitate moderne (ex. SAML 2.0, OpenID Connect).

Platforma va permite:

- configurarea unuia sau mai multor furnizori de identitate;
- actualizarea periodică a informațiilor de identitate, astfel încât modificările operate în sistemele centrale (angajări, plecări, schimbări de rol) să se propage automat în drepturile de acces la platformă.

În acest fel, nu se definesc utilizatori „paraleli” în platformă, ci se reutilizează infrastructura de identitate existentă a instituției.

b) Single Sign-On (SSO)

Platforma trebuie să ofere Single Sign-On (SSO), astfel încât utilizatorii să se poată autentifica folosind un singur set de credențiale și să acceseze:

- interfața web a platformei;
- eventualele module suplimentare expuse prin același mecanism de identitate;
- API-urile platformei (indirect, prin token-uri emise de furnizorul de identitate).

Cerințele funcționale includ:

- suport pentru protocoale standard de SSO, cum ar fi SAML 2.0 și/sau OpenID Connect (OIDC), pentru a asigura interoperabilitatea cu soluțiile existente în instituție;
- posibilitatea de a configura politici de sesiune (durata sesiunii, reautentificare periodică, logout global), astfel încât comportamentul să respecte regulile interne de securitate;
- suport pentru SSO atât pentru interfață, cât și pentru API-uri, astfel încât aplicațiile terțe integrate să poată utiliza token-uri emise de furnizorul central de identitate.

Implementarea SSO reduce semnificativ numărul de parole gestionate de utilizatori, simplifică experiența de acces și scade riscul asociat gestionării necorespunzătoare a datelor de autentificare.

c) Autentificare multifactor (MFA)

Platforma trebuie să permită și/sau să respecte politicile de autentificare multifactor (MFA) definite în infrastructura de identitate a instituției.

Din punctul de vedere al platformei, aceasta înseamnă:

- acceptarea fluxurilor de autentificare în care utilizatorului i se cere, pe lângă parolă, un al doilea factor (cod temporar, aplicație de autentificare, token hardware etc.);

- asigurarea faptului că, după validarea MFA de către furnizorul de identitate, sesiunea rezultată este recunoscută și acceptată de platformă fără solicitarea unui factor suplimentar;
- posibilitatea de a defini politici prin care anumite roluri, grupuri de utilizatori sau operațiuni critice sunt tratate ca „sensibile”. Pentru aceste categorii, fluxurile de autentificare și autorizare vor impune utilizarea autentificării multifactor (MFA) ca pas obligatoriu, înainte de acordarea accesului sau aprobarea acțiunilor.

În acest mod, instituția poate aplica MFA diferențiat:

- pentru toți utilizatorii;
- sau, cel puțin, pentru utilizatorii cu roluri privilegiate (administratori de sistem, administratori de securitate, operatori ai platformei).

d) Managementul sesiunilor și al accesului

Platforma trebuie să asigure o gestionare clară a sesiunilor de utilizator, incluzând:

- închiderea automată a sesiunilor inactive după un interval configurabil (idle timeout);
- posibilitatea de a invalida sesiuni active atunci când:
  - sunt modificate drepturile unui utilizator;
  - se suspectează compromiterea contului;
- propagarea evenimentelor de logout dinspre furnizorul central de identitate către platformă, pentru a evita sesiuni „orfane”.

În plus, platforma trebuie să permită:

- vizualizarea, pentru utilizatorii autorizați (de exemplu, administratori de securitate), a sesiunilor active și a ultimelor momente de acces;
- restricționarea autentificării din anumite intervale de adrese IP sau zone de rețea, acolo unde politicile instituției o cer (de exemplu, acces administrativ doar din rețeaua internă).

Prin aceste mecanisme, autentificarea nu este doar un pas singular de acces, ci un proces continuu de gestionare a identității și a sesiunilor, integrat în practicile de securitate ale instituției publice.

4.10.2.2 Autorizare bazată pe roluri (RBAC) și politici de acces

Platforma trebuie să asigure un **mecanism centralizat de autorizare**, bazat pe roluri (Role-Based Access Control – RBAC) și politici de acces configurabile, astfel încât fiecare utilizator să aibă acces doar la resursele și acțiunile strict necesare rolului său în instituție („least privilege”).

Scopul acestui sub-sistem este:

- să ofere o **structură clară de roluri și drepturi**, ușor de explicat și auditat;
- să permită **maparea directă** a rolurilor interne (departamente, direcții, echipe) în permisiunile platformei;
- să facă posibilă **separarea responsabilităților** (segregation of duties) și controlul fin al acțiunilor critice.

a) Model de roluri și grupuri

Platforma trebuie să utilizeze un model RBAC în care:

- **rolurile** definesc seturi de permisiuni (ce acțiuni sunt permise);
- **grupurile / unitățile organizaționale** (importate din sistemul de identitate) pot fi mapate la unul sau mai multe roluri;
- utilizatorii pot avea **unul sau mai multe roluri**, în funcție de responsabilități.

Exemple de roluri care pot fi definite în platformă, adaptabile la structura instituției:

- roluri de administrare:
  - *Administrator platformă* (configurare globală, integrare, securitate);
  - *Administrator infrastructură* (gestionare conectori, medii, clustere);
- roluri operaționale:
  - *Operator DevOps* (gestionare workflows, deployment-uri, monitorizare);
  - *Operator suport* (vizualizare stări, relansare fluxuri, consultare loguri);
- roluri de business:
  - *Aprobator de servicii / manager de linie*;
  - *Utilizator final de portal self-service*.

Platforma trebuie să permită definirea de roluri, orientate pe scenarii comune, dar și roluri personalizate, create și ajustate de instituție, fără a fi necesară modificarea codului sursă.

b) Domenii de aplicare a permisiunilor (scopes)

Permisiunile nu trebuie să fie doar globale „tot sau nimic”, ci să poată fi aplicate pe **domenii de lucru** (scopes), astfel încât accesul să fie granulat. Platforma va permite configurarea permisiunilor cel puțin la nivel de:

- **instanță globală a platformei** – drepturi care afectează configurația generală (ex. definire conectori, configurare SSO, politici globale);
- **spații logice / workspaces / proiecte** – drepturi limitate la un subset de resurse sau un anumit proiect sau departament;

Astfel, platforma permite scenarii precum:

- un operator DevOps poate gestiona workflows doar într-un anumit workspace, fără acces la configurația globală;
- un administrator de departament poate aproba doar cereri din aria sa, fără a vedea resursele altor direcții.

c) Tipuri de permisiuni (read / write / execute / administrare)

Pentru fiecare tip de obiect administrat de platformă (ex: workflows, conectori, formulare, medii, etc.), modelul RBAC trebuie să susțină diferențierea pe **tipuri de acțiuni**, de exemplu:

- **citire (read / view)** – vizualizarea configurațiilor, a rapoartelor, a stărilor;
- **modificare (write / edit)** – crearea, editarea sau ștergerea configurațiilor, în limitele rolului;

- **execuție (execute / run)** – dreptul de a lansa workflows, de a declanșa manual procese, de a relansa execuții;
- **administrare (admin / manage)** – drepturi complete asupra unui obiect sau domeniu (inclusiv delegarea altor drepturi).

Platforma trebuie să permită asocierea acestor permisiuni la:

- roluri globale (ex. Administrator platformă are drepturi complete);
- roluri limitate (ex. Operator poate doar vizualiza și lansa, dar nu poate modifica definițiile).

Această separare este esențială pentru a preveni situațiile în care aceeași persoană definește, aprobă și execută operațiuni critice, fără control încrucișat.

d) Model de permisiuni granulare pe obiecte

Platforma implementează modelul RBAC printr-un **sistem de permisiuni granulare**, aplicate pe fiecare tip de obiect administrat. Rolurile sunt, în esență, **colecții de permisiuni** de forma „Create / Read / Update / Delete / Execute" aplicate pe domenii funcționale distincte.

În interfața de administrare, pentru fiecare rol se pot configura explicit permisiuni asupra unor categorii de resurse, cum ar fi, fără a se limita la:

- resurse de orchestrare și execuție:
  - deployment-uri și reguli de deployment;
  - joburi programate;
  - funcții serverless și execuția acestora;
- resurse legate de infrastructură:
  - clustere și grupuri de clustere;
  - template-uri Terraform și deployment-uri Terraform;
  - configurări operaționale (config);
- resurse legate de aplicații și formulare:
  - formulare de business utilizate în portal;
  - artefacte și modele AI;
- resurse de guvernanță și administrare:
  - licențe;
  - grupuri și roluri;
- resurse de observabilitate:
  - loguri și audit;
  - componente de monitorizare și notificări.

Pentru fiecare astfel de categorie, platforma permite configurarea granulară a permisiunilor de tip:

- Create – dreptul de a crea noi obiecte (ex. un nou deployment, un nou template Terraform, un nou formular);

- Read – dreptul de a vizualiza configurația și starea obiectelor existente (ex. vizualizare loguri, vizualizare configurații de deployment);
- Update – dreptul de a modifica obiectele existente (ex. actualizarea unui workflow, modificarea unui formular, schimbarea configurației unui cluster group);
- Delete – dreptul de a șterge obiecte (ex. eliminarea unui job, dezafectarea unui template);
- Execute (acolo unde este relevant) – dreptul de a lansa sau relansa execuții (ex. rularea unei funcții, declanșarea unui deployment, pornirea unui job).

Prin asocierea acestor permisiuni la roluri:

- se pot crea roluri cu drepturi complete asupra unui set de obiecte (de exemplu un rol de tip „global admin”, care are Create/Read/Update/Delete/Execute pe toate domeniile);
- se pot crea roluri restrictive, care permit doar citirea sau doar execuția unor obiecte, fără posibilitatea de modificare (de exemplu, roluri pentru operatori sau pentru utilizatori de suport).

Acest model bazat pe permisiuni pe obiecte permite:

- adaptarea foarte fină a drepturilor la structura organizațională;
- demonstrarea clară, în fața auditorilor, a faptului că fiecare rol are exact permisiunile necesare și nimic în plus;
- ajustarea rapidă a accesului pe măsură ce apar noi tipuri de resurse în platformă, fără a schimba mecanismul de bază.

e) Roluri și operațiuni „sensibile” și legătura cu MFA

Pentru anumite categorii de roluri și acțiuni, instituția poate impune cerințe suplimentare de securitate. Platforma trebuie să permită, prin integrarea cu furnizorul de identitate, **definirea de politici prin care anumite roluri, grupuri de utilizatori sau operațiuni critice sunt tratate ca „sensibile”**.

Pentru aceste categorii, fluxurile de autentificare și autorizare vor impune:

- utilizarea autentificării multifactor (MFA) ca pas obligatoriu înainte de acordarea accesului;
- reluarea unui pas MFA atunci când se inițiază o acțiune cu impact major (de exemplu, modificarea politicilor de securitate, aprobarea unui deployment în producție, acces la date cu caracter personal).

Această funcționalitate se realizează prin mecanisme de tip **flow / stage / policy** la nivelul soluției de management al identității, astfel încât:

- utilizatorii cu roluri privilegiate (administrare platformă, securitate, administratori de infrastructură) să fie supuși obligatoriu autentificării MFA;
- pentru operațiuni sensibile, execuția să fie condiționată de trecerea printr-un pas suplimentar de verificare MFA, chiar dacă utilizatorul are deja o sesiune activă.

În acest fel, nu doar că se controlează „cine are dreptul să facă ceva”, ci se impune și **un nivel suplimentar de încredere** atunci când acel „ceva” este deosebit de critic.

f) Integrare cu sursa de identitate și guvernanță continuă

Platforma trebuie să poată **corela modelul RBAC intern cu structura de identitate a instituției**, astfel încât:

- grupurile, unitățile organizaționale și atributele utilizatorilor din LDAP / Active Directory sau alți provideri să fie reutilizate în definirea rolurilor;
- schimbările din sistemul de identitate (intrări/ieșiri din organizație, schimbări de departament, modificări de funcție) să se reflecte în mod coerent în drepturile de acces din platformă;
- să fie posibilă implementarea unor procese de revizuire periodică a accesului (recertificare de roluri), în colaborare cu departamentele de resurse umane, securitate și IT.

Prin acest model, RBAC nu rămâne un mecanism static, ci devine parte din **guvernanța continuă a identităților și accesului**, aliniat cu practicile de securitate ale instituției.

4.10.2.3 Gestionarea secretelor

Platforma trebuie să includă un **serviciu centralizat de gestionare a secretelor** (tip „vault”), utilizat pentru stocarea și folosirea în siguranță a informațiilor sensibile necesare orchestrării: parole, token-uri, chei API, certificate, date de conectare la baze de date sau sisteme interne/extern.

Scopul acestui serviciu este:

- să elimine expunerea secretelor în clar în workflows, template-uri sau cod;
- să permită reutilizarea controlată a secretelor în multiple fluxuri, fără a le replica în mai multe locuri;

a) Serviciu centralizat de tip vault

Platforma va include un modul dedicat de tip **vault**, accesibil prin interfață grafică și prin API, care:

- stochează toate valorile marcate ca „secret” în formă **criptată** la nivel de infrastructură;
- permite definirea de variabile atât de tip **secret**, cât și de tip **configurație** (valori non-secrete reutilizabile, cum ar fi adrese de endpoint, nume de baze de date, constante folosite în workflows).

Platforma va permite administrarea acestor variabile prin:

- listarea și filtrarea lor în funcție de denumire, scop și tip;
- definirea unei descrieri pentru fiecare intrare, astfel încât utilizatorii să poată înțelege contextul și utilizarea așteptată;
- operarea de acțiuni specifice (creare, actualizare, ștergere) doar de către utilizatori cu permisiuni corespunzătoare din modelul RBAC.

b) Domenii logice și compartimentarea variabilelor

Pentru a respecta principiul „least privilege” și pentru a evita amestecarea necontrolată a secretelor între proiecte sau zone funcționale, platforma va organiza variabilele și secretele în domenii logice.

Exemple de domenii logice care trebuie suportate:

- **Cluster** – variabile legate de un anumit cluster (de exemplu fișiere de tip *kubeconfig*, subdomenii, parametri de conectare), utilizabile în workflows care operează pe acel cluster;
- **DevOps** – variabile generale utilizate de echipele DevOps (ex. token-uri pentru sisteme de CI/CD, endpoint-uri interne, valori comune pentru mai multe fluxuri);
- **Integrari** – secrete și configurații pentru conectori către sisteme externe (baze de date, aplicații de business, servicii cloud, sisteme de mesagerie etc.);

Această compartimentare asigură atât **securitatea datelor sensibile**, cât și **organizarea clară** a configurațiilor în infrastructuri complexe.

c) Integrare directă în editorul de fluxuri de lucru

Platforma trebuie să expună serviciul de tip vault **direct în editorul de workflows**, astfel încât utilizatorii să poată folosi secrete și variabile în definițiile de flux.

Pentru fiecare nod / pas / acțiune din workflow, interfața va pune la dispoziție o zonă prin care:

- utilizatorul poate vizualiza lista variabilelor disponibile în domeniul logic relevant (de exemplu, variabile de spațiu de lucru și, acolo unde este cazul, variabile de cluster sau integrare);
- poate insera referințe la variabile în câmpurile de configurare ale pasului (ex. câmpuri de tip URL, credențiale, parametri de interogare), utilizând o sintaxă de interpolare standard (de tip ${…} sau echivalent);

În execuție, platforma va rezolva automat variabilele referențiate, extrăgând valorile din vault și injectându-le în contextul pasului.

d) Funcții predefinite și variabile derivate

Pe lângă stocarea de secrete și valori statice, platforma include și un set de **funcții predefinite** care pot fi utilizate ca variabile speciale în workflows, pentru a genera sau transforma valori la runtime, fără a scrie cod suplimentar.

Exemple de funcționalități care trebuie acoperite:

- funcții de timp și dată:
  - data curentă;
  - timestamp curent (ex. UNIX timestamp);
  - conversii între formate de dată;
- funcții de generare:
  - generare de identificatori aleatori (UUID);
  - numere sau șiruri aleatoare;
- funcții de conversie și transformare:
  - conversii între tipuri (string → int, string → float etc.);
  - transformări de text (majuscule/minuscule);
  - codare/decodare (ex. base64).

Aceste funcții sunt disponibile în platformă și pot fi inserate în câmpurile workflow-urilor, similar secretelor și variabilelor clasice.

Astfel, utilizatorii pot:

- genera token-uri temporare sau identificatori unici pentru fiecare execuție;
- construi parametri dinamici de interogare sau mesaje;
- evita scrierea de scripturi suplimentare pentru operațiuni de bază de transformare.

Operațiunile sensibile asupra secretelor (creare, modificare, ștergere) vor fi limitate la roluri dedicate (ex. administratori de securitate, administratori de integrare), în acord cu modelul RBAC descris anterior.

e) Integrare cu guvernanța și procesele de securitate

Platforma trebuie să permită integrarea gestionării secretelor în procesele de guvernanță ale instituției, prin:

- posibilitatea de a utiliza API-ul vault-ului în workflows pentru:
    - actualizarea automată a unor secrete (de exemplu, token-uri obținute din sisteme externe).

Prin acest mecanism, platforma nu doar stochează secretele în siguranță, ci oferă și **un cadru de control și trasabilitate**, esențial pentru demonstrarea conformității cu politicile interne de securitate, standardele ISO și cerințele specifice mediului public.

4.10.2.4 Audit și trasabilitate acțiuni

Platforma trebuie să asigure un **mecanism complet de audit și trasabilitate** pentru toate acțiunile relevante din punct de vedere operațional și de securitate, astfel încât instituția să poată demonstra în orice moment:

1. cine a făcut o anumită acțiune;
2. când a avut loc acțiunea;
3. asupra cărui obiect (resursă, workflow, secret, rol etc.) s-a acționat.

Scopul acestui modul este să furnizeze **dovada tehnică necesară** pentru investigații, controale interne, audit extern (inclusiv conformitate ISO 27001, GDPR) și pentru reconstituirea cronologiei unor incidente.

a) Domeniul de acoperire al jurnalizării

Platforma trebuie să colecteze evenimente de audit cel puțin pentru următoarele categorii de acțiuni:

- autentificare și autorizare
    - autentificări reușite și refuzate (SSO, MFA);
    - inițierea și rezultatul pașilor MFA;
    - acordarea, modificarea și revocarea rolurilor sau permisiunilor pentru utilizatori sau grupuri;
- configurare și guvernanță

- modificări ale configurațiilor globale ale platformei (setări de securitate, integrare cu IdP, SMTP, notificări etc.);
- crearea, modificarea și ștergerea rolurilor și grupurilor de acces;
- operațiuni asupra secretelor și variabilelor din vault (creare, actualizare, ștergere, schimbare scope);
- definirea și modificarea conectorilor, mediilor, clusterelor, grupurilor de clustere, template-urilor și formularelor;

- orchestrare și execuții operaționale
  - crearea, modificarea, activarea/dezactivarea și ștergerea workflows-urilor;
  - declanșarea execuțiilor (manual, prin triggere, cron, surse de evenimente);
  - rezultatul execuțiilor: reușite, eșecuri, anulări, time-out;
  - lansarea sau ștergerea de deployment-uri;
- procese de aprobare și guvernanță business
  - trimiterea, aprobarea, respingerea sau anularea cererilor inițiate prin formularele de business;
  - schimbarea stării unui workflow sau serviciu în urma unei aprobări

Prin această acoperire extinsă, orice modificare semnificativă de configurare sau execuție poate fi urmărită în detaliu.

b) Structura evenimentelor de audit

Platforma trebuie să înregistreze evenimentele de audit într-un format structurat, astfel încât să poată fi căutate, filtrate și corelate ușor. Pentru fiecare eveniment, vor fi memorate cel puțin următoarele câmpuri:

- **identitatea actorului**: utilizator autentificat, serviciu tehnic sau API key care a inițiat acțiunea;
- **momentul exact al acțiunii**: timestamp cu precizie de cel puțin o secundă, sincronizat la nivel de platformă;
- **tipul acțiunii**: autentificare, modificare configurare, execuție workflow, actualizare secret, creare rol etc.;
- **obiectul asupra căruia s-a acționat**: tip (workflow, secret, rol, cluster, formular etc.) și un identificator clar (nume, ID);
- **rezultatul acțiunii**: succes / eșec / parțial, împreună cu un mesaj explicativ sau cod de eroare;

Structura standardizată a evenimentelor permite instituției să utilizeze atât interfața platformei, cât și instrumente externe (de tip SIEM) pentru analiză.

c) Interfață de vizualizare, căutare și filtrare

Platforma trebuie să pună la dispoziție un **modul dedicat de vizualizare a jurnalelor de audit**, accesibil utilizatorilor cu roluri adecvate (de exemplu, securitate, audit intern, administratori de platformă).

Interfața va permite:

- filtrare după:
  - perioadă de timp;
  - tip de acțiune (login, modificare, execuție);
  - utilizator / grup;
  - tip de obiect (workflow, secret, rol etc.);
  - rezultat (reușit/eșuat);
- sortare după dată, utilizator, tip de eveniment;
- afișarea detaliată a unui eveniment individual, incluzând toate câmpurile relevante și eventualele mesaje de eroare;
- exportul selecțiilor de evenimente în formate standard (de exemplu CSV, JSON) pentru analiză ulterioară sau atașare la rapoarte de audit.

Astfel, echipele de control pot identifica rapid, de exemplu:

- cine a modificat un anumit workflow și când;
- ce utilizator a revocat sau a acordat un rol privilegiat;
- ce execuții au eșuat într-un anumit interval și care a fost cauza.

Corelare cu logurile operaționale și execuțiile workflows

Pentru a asigura **trasabilitate end-to-end**, evenimentele de audit trebuie corelate cu logurile operaționale ale platformei și cu execuțiile workflows-urilor.

Platforma va utiliza identificatori comuni (de tip **run ID**) astfel încât:

- o execuție de workflow să poată fi urmărită de la:
  - inițiere (de exemplu, un trigger dintr-un formular sau un eveniment Kafka),
  - la fiecare pas intern (acțiuni, apeluri de integrare),
  - până la finalizare (succes sau eșec);
- modificarea unei configurații (de exemplu a unui conector sau a unui secret) să poată fi pusă în relație cu execuțiile care au utilizat respectiva configurație.

Această abordare ajută la:

- analiza cauzelor rădăcină pentru incidente (root cause analysis);
- demonstrarea faptului că un anumit comportament al sistemului a fost determinat de o schimbare concretă, realizată de un anumit utilizator, la un moment clar identificat.

d) Integrare cu soluții externe de monitorizare și SIEM

Pentru instituțiile care utilizează platforme centralizate de monitorizare și analiză de securitate (SIEM), platforma trebuie să ofere:

- posibilitatea de **export continuu** sau periodic al jurnalelor de audit către sisteme externe, utilizând protocoale și formate standard (de exemplu, syslog, HTTP, mesagerie);
- configurarea de **destinații multiple** pentru evenimente (de exemplu, un SIEM intern, un sistem de log management, o platformă de raportare);
- însoțirea fiecărui eveniment exportat cu metadatele necesare pentru corelarea cu alte surse (loguri de sistem, loguri de aplicație etc.).

Această integrare permite echipelor de securitate să:

- coreleze evenimentele de pe platformă cu alte evenimente din infrastructură;
- definească alerte centralizate pentru acțiuni critice (de exemplu, modificarea unui rol privilegiat, ștergerea unui secret, multiple autentificări eșuate);
- includă platforma în tabloul general de risc și conformitate al instituției.

4.10.2.5 Fluxuri de autentificare configurabile

Platforma trebuie să permită configurarea flexibilă a fluxurilor de autentificare, astfel încât instituția să poată adapta mecanismele de acces la specificul fiecărei aplicații, fiecărui tip de utilizator și fiecărui nivel de sensibilitate al datelor sau operațiunilor. Scopul este asigurarea unui echilibru între securitate, ușurința în utilizare și cerințele de conformitate (inclusiv politici interne, ISO 27001, GDPR).

Soluția va funcționa în strânsă integrare cu un serviciu central de identitate (IdP), permițând definirea, versionarea și aplicarea unor fluxuri de autentificare configurabile, fără a fi necesară modificarea aplicațiilor integrate.

Platforma trebuie să asigure cel puțin următoarele capabilități:

- posibilitatea de a defini mai multe fluxuri de autentificare (authentication flows) care pot fi asociate cu:
    - aplicații sau zone funcționale diferite;
    - tipuri de utilizatori (ex. personal tehnic, utilizatori de business, conturi privilegiate);
    - scenarii speciale (ex. acces de la distanță, acces din rețele neîncredere, acces pentru parteneri);
- suport pentru autentificare unificată (SSO) prin furnizorul de identitate, cu posibilitatea de a combina:
    - autentificare bazată pe directoare corporative (ex. LDAP / Active Directory);
    - autentificare cu furnizori de identitate federată (OIDC/SAML, după caz);
    - autentificare locală sau pe bază de conturi gestionate în sistem, acolo unde este justificat.

Fluxurile de autentificare trebuie să fie configurabile astfel încât:

- să includă pași succesivi sau condiționali, de exemplu:

- verificare credențiale de bază (user/parolă sau token);
- verificare suplimentară prin MFA pentru anumite roluri sau acțiuni sensibile;
- afișarea unor ecrane de informare sau consimțământ (de exemplu, politici de utilizare acceptate de utilizator);

- să permită activarea obligatorie a autentificării multifactor (MFA) pentru:
  - anumite roluri privilegiate (ex. administratori de platformă, operatori DevOps, conturi cu drept de modificare a politicilor);
  - operațiuni sensibile (ex. modificarea configurației unui cluster, a unui flux de lucru sau a politicilor de acces);
  - acces din anumite rețele, locații sau contexte (în funcție de politicile instituției și capabilitățile IdP).

Platforma va permite instituției să:

- aleagă și să asocieze fluxul de autentificare potrivit în momentul integrării unei noi aplicații sau la configurarea unui nou workspace / spațiu logic în interiorul platformei;
- modifice fluxurile de autentificare fără a afecta codul aplicațiilor, prin ajustări la nivelul furnizorului de identitate și prin setări în platformă (de exemplu, asocierea unei noi politici de MFA unui anumit grup de utilizatori);
  - diferențieze politica de autentificare între: accesul la interfața de administrare;
  - accesul la interfața de utilizator final;
  - accesul programatic (de exemplu, token-uri de service pentru API-uri, chei de acces pentru automatizări).

Pentru asigurarea trasabilității și a conformității, platforma trebuie să se integreze cu jurnalul de audit, astfel încât:

- fiecare autentificare să fie înregistrată cu:
  - identitatea utilizatorului;
  - fluxul de autentificare folosit;
  - factorii de autentificare utilizați (ex. parolă + MFA);
  - rezultatul autentificării (reușită/eșec) și cauza eșecului (parolă incorectă, MFA refuzat, cont blocat etc.);
- modificările aduse fluxurilor de autentificare (creare, editare, activare/dezactivare) să fie logate, incluzând:
  - cine a efectuat modificarea;
  - momentul modificării;
  - configurația veche vs. nouă.

Prin aceste mecanisme, platforma va permite instituției să implementeze politici de autentificare diferențiate, să crească nivelul de securitate pentru zonele critice și să demonstreze, în fața

organelor de audit, modul în care este controlat accesul la infrastructură și la fluxurile operaționale critice.

4.10.3 Firewall cloud – 2 buc.

Furnizarea, instalarea și configurarea unei soluții de tip **firewall virtual (Next Generation Firewall - NGFW)**, implementată în mediul cloud, pentru asigurarea securității traficului de rețea, controlului accesului și protecției comunicațiilor.

Soluția trebuie livrată în configurație redundantă (minim 2 instanțe).

1. **Cerințe generale**
   - Soluția trebuie să fie disponibilă sub formă de **appliance virtual**, compatibilă cu:
     - medii virtualizate
     - infrastructuri cloud private / guvernamentale
   - Trebuie să permită:
     - alocarea flexibilă a resurselor (CPU, RAM)
     - scalare în funcție de necesități
   - Se vor implementa:
     - **minimum 2 instanțe firewall**, posibil de configurat independent sau în mod activ-pasiv sau echivalent (HA)
2. **Cerințe funcționale – securitate rețea**

Filtrarea traficului

- Soluția trebuie să permită:
  - filtrarea traficului pe bază de reguli
  - politici de tip whitelist / blacklist
- Filtrare la nivel:
  - L3 / L4 (IP, port)
  - L7 (aplicație)

Protecție împotriva atacurilor

- Soluția trebuie să includă mecanisme pentru:
  - prevenirea atacurilor de tip DDoS / DoS
  - detecția și blocarea malware
  - prevenirea intruziunilor
- Trebuie să includă:
  - sisteme IDS/IPS integrate
  - actualizări regulate ale semnăturilor

Monitorizare și logare

- Soluția trebuie să permită:
  - înregistrarea traficului și evenimentelor de securitate
  - exportul logurilor către sisteme externe (ex: SIEM)
- Trebuie să includă:
  - mecanisme de alertare
  - vizualizare centralizată

VPN

- Soluția trebuie să suporte:
  - VPN site-to-site
  - VPN remote access
- Trebuie să includă:
  - criptare IPsec și/sau SSL VPN
  - autentificare securizată (user/parolă, certificat sau echivalent)
- Soluția trebuie să permită:
  - **minimum 25 conexiuni VPN remote simultane**
- În cazul în care soluția necesită licențiere suplimentară pentru utilizatori VPN:
  - ofertantul va include **licențe pentru minimum 25 utilizatori VPN**

Controlul accesului

- Soluția trebuie să permită:
  - definirea politicilor pe utilizatori, grupuri sau dispozitive
  - integrare cu LDAP / Active Directory sau echivalent

Protecția aplicațiilor web (WAF)

- Soluția trebuie să includă capabilități de:
  - protecție a aplicațiilor web la nivel de firewall
  - detectarea și blocarea atacurilor web cunoscute
- Trebuie să permită:
  - identificarea atacurilor de tip:
    - SQL injection
    - cross-site scripting (XSS)
    - alte tipuri comune de atacuri web

IDS/IPS

- Soluția trebuie să includă:
  - mecanisme IDS și IPS

- Trebuie să permită:
    - analiză trafic în timp real
    - blocarea automată a amenințărilor

3. **Funcționalități avansate de securitate**
    - Soluția trebuie să includă:
        - control aplicații (Application Control)
        - protecție anti-malware
        - filtrare trafic web (URL filtering sau echivalent)
    - Trebuie să beneficieze de:
        - servicii de securitate actualizate periodic (threat intelligence)
4. **Cerințe performanță și resurse**
    - Fiecare instanță firewall trebuie să suporte:
        - minimum 1 vCPU
        - alocare flexibilă de memorie RAM
    - Soluția trebuie să permită:
        - scalare verticală prin alocare resurse suplimentare
5. **Cerințe disponibilitate**
    - Soluția trebuie implementată în:
        - configurație redundantă (minimum 2 instanțe)
    - Trebuie să suporte:
        - failover automat
        - sincronizare configurație între instanțe
6. **Cerințe integrare**
    - Soluția trebuie să permită:
        - integrarea cu platforme SIEM/XDR
        - export loguri în formate standard
7. **Cerințe licențiere și subscripție**
    - Soluția trebuie să includă:
        - licențiere pentru minimum 2 instanțe firewall virtual
    - Trebuie să includă subscripție pentru o perioadă de:
        - **minimum 36 luni (3 ani)**, pentru ambele instanțe cu funcționare independentă
    - Subscripția trebuie să acopere:
        - servicii de prevenire a intruziunilor (IPS)

- protecție anti-malware
- control aplicații
- actualizări de securitate (semnături, reputație, threat intelligence)
- suport tehnic

4.10.4 Web Application Firewall (WAF) – 2 buc.

Furnizarea, instalarea și configurarea unei soluții de tip **Web Application Firewall (WAF) enterprise**, destinată protejării aplicațiilor web împotriva atacurilor cibernetice specifice.

Soluția trebuie să fie implementată în mediul cloud și livrată în configurație redundantă.

Cerințe minime:

- Soluția trebuie să fie livrată sub formă de appliance virtual sau software dedicat.
- Trebuie să permită:
  - integrarea cu infrastructura existentă
  - protejarea aplicațiilor web publice
- Se vor implementa **minimum 2 instanțe**, în configurație de înaltă disponibilitate (HA).

1. **Cerințe funcționale WAF**

- Soluția trebuie să permită:
  - detectarea și blocarea atacurilor web, inclusiv:
    - SQL Injection
    - Cross-Site Scripting (XSS)
    - alte tipuri de atacuri specifice aplicațiilor web
- Trebuie să includă:
  - reguli predefinite de securitate (bazate pe bune practici, ex: OWASP sau echivalent)
  - mecanisme de actualizare a regulilor
- Soluția trebuie să permită:
  - definirea de politici personalizate
  - protecție la nivel HTTP/HTTPS

2. **Funcționalități avansate**

- Soluția trebuie să includă:
  - protecție împotriva atacurilor de tip:
    - brute force
    - session hijacking
  - validarea și filtrarea input-urilor
- Trebuie să permită:

- terminare SSL/TLS
- inspecția traficului criptat

3. **Funcționalități de tip load balancing**
   - Soluția trebuie să includă capabilități de distribuție a traficului către mai multe instanțe aplicație.
   - Trebuie să permită:
     - algoritmi de load balancing configurabili
     - verificarea stării serviciilor (health checks)
4. **Performanță și capacitate**
   - Fiecare instanță trebuie să suporte trafic de minimum **1 Gbps.**
   - Soluția trebuie să permită scalare prin adăugarea de instanțe suplimentare.
5. **Disponibilitate**
   - Soluția trebuie implementată în configurație redundantă (minimum 2 instanțe).
   - Trebuie să suporte:
     - failover automat
     - sincronizare configurații
6. **Monitorizare și raportare**
   - Soluția trebuie să ofere:
     - vizibilitate asupra traficului web
     - detalii despre atacurile detectate și blocate
   - Trebuie să permită:
     - generare de rapoarte
     - export date către sisteme externe (SIEM/XDR)
7. **Integrare**
   - Soluția trebuie să permită:
     - integrarea cu soluții de securitate existente
     - export de loguri în formate standard
8. **Cerințe licențiere și subscripție**
   - Soluția trebuie să includă licențiere pentru minimum 2 instanțe.
   - Fiecare instanță trebuie să includă:
     - capabilități WAF
     - capabilități load balancing
   - Soluția trebuie să includă:

- servicii de securitate și suport pentru o perioadă de **minimum 36 luni (3 ani)**.

- Subscripția trebuie să acopere:
  - actualizări reguli WAF
  - suport tehnic

4.10.5 Servicii protecție DDoS (Distributed Denial of Service)

Furnizarea unui serviciu de tip cloud pentru **protecția împotriva atacurilor DDoS, securizarea aplicațiilor web și optimizarea livrării conținutului**, destinat protejării serviciilor expuse pe internet.

Serviciul va fi livrat sub formă de subscripție pentru o perioadă de minimum 36 de luni.

1. **Cerințe generale**
   - Soluția trebuie să fie:
     - livrată ca serviciu (SaaS)
     - operată de furnizor (fără necesitatea instalării de echipamente locale)
   - Soluția trebuie să funcționeze:
     - la nivel global, printr-o rețea distribuită de centre de date
   - Trebuie să permită:
     - protejarea aplicațiilor web publice și serviciilor expuse în internet
2. **Protecție DDoS**
   - Soluția trebuie să asigure protecție împotriva atacurilor:
     - volumetrice (L3/L4)
     - la nivel aplicație (L7)
   - Trebuie să includă:
     - detectarea automată a atacurilor
     - mitigarea automată, fără intervenție manuală
   - Soluția trebuie să fie capabilă să:
     - absoarbă și filtreze trafic malițios la scară largă
     - mențină disponibilitatea serviciilor protejate
3. **Web Application Firewall (WAF - nivel cloud)**
   - Soluția trebuie să includă un WAF integrat care:
     - protejează aplicațiile web împotriva atacurilor cunoscute și emergente
   - Trebuie să includă:
     - reguli predefinite (inclusiv bazate pe OWASP Top 10 sau echivalent)
     - actualizări automate ale regulilor

- Soluția trebuie să permită:
    - definirea de reguli personalizate
    - filtrarea traficului HTTP/HTTPS

4. **Protecție DNS**
    - Soluția trebuie să includă:
        - servicii DNS gestionate
        - protecție împotriva atacurilor DNS (DNS flood, amplification etc.)
    - Trebuie să permită:
        - disponibilitate ridicată a serviciilor DNS
5. **CDN și optimizare trafic**
    - Soluția trebuie să includă:
        - rețea de distribuție a conținutului (CDN)
    - Trebuie să permită:
        - cache pentru conținut static și dinamic (unde este aplicabil)
        - optimizarea livrării conținutului către utilizatori
6. **Control acces și politici de securitate**
    - Soluția trebuie să permită:
        - definirea de politici de acces pe bază de:
            - IP
            - locație geografică
            - reputație trafic
    - Trebuie să includă:
        - mecanisme de protecție împotriva bot-urilor
        - limitarea ratei de trafic (rate limiting)
7. **Monitorizare și raportare**
    - Soluția trebuie să ofere:
        - dashboard-uri în timp real
        - vizibilitate asupra:
            - traficului legitim
            - atacurilor blocate
    - Trebuie să permită:
        - generarea de rapoarte
        - exportul datelor

8. **Disponibilitate și SLA**
   - Soluția trebuie să ofere:
     - disponibilitate ridicată (minim 99,9% sau echivalent)
   - Trebuie să fie bazată pe:
     - infrastructură distribuită global
9. **Integrare**
   - Soluția trebuie să permită:
     - integrarea cu sisteme existente de securitate (ex: SIEM/XDR)
     - acces prin API (REST sau echivalent)
10. **Cerințe licențiere și subscripție**
    - Serviciul trebuie să fie furnizat sub formă de:
      - subscripție pe **minimum 36 luni (3 ani)**
    - Subscripția trebuie să includă:
      - toate funcționalitățile de protecție DDoS
      - WAF cloud cu reguli actualizate
      - servicii CDN și DNS
      - suport tehnic

4.10.6 Soluție tip MDR Plus (Managed Detection and Response) cu servicii incluse de monitorizare 24/7

Cerințe minime:

- Prestatorul va livra o soluție integrata pentru managementul securității, de tip EDR pentru minimum 120 echipamente/VM-uri, cu licență valabilă 36 luni.
- Soluția trebuie să fie compatibilă cu Windows și Linux (dacă este cazul).
- Soluția trebuie să fie certificată sau recunoscută în topurile independente (Gartner, Forrester, AV-Test etc.).
- Soluția va conține următoarele module:
  A. O consola de management care asigura funcționalități de administrare.
  B. Protecție antimalware pentru stații fizice/virtuale, laptop-uri si servere
  C. Monitorizare și răspuns 24x7

A. CONSOLA DE MANAGEMENT

1. Instalare si configurare:

- Mașinile de scanare (pentru tipul de scanare centralizata) pentru mediile virtuale se descarcă din interfața web a produsului.

2. Cerințe generale:

- Interfața consolei de management va fi in limba romana.
- Interfața clientului de securitate, care se instalează pe stații si servere, va fi in limba romana.
- Soluția va permite activarea/dezactivarea actualizărilor de produs/semnături.
- Actualizări automate a consolei de management făcute de către producătorul soluției, fără intervenția utilizatorului.
- Notificările – prezente in interfața, notificările necitite sunt evidențiate, trimise către una sau mai multe adrese de email, alertează administratorul in cazul unor probleme majore: licențiere, detecție virusi, actualizări de produs disponibile).
- Consola de management este accesibila de oriunde in lume (soluție de tip Cloud), fără a fi nevoie de setări suplimentare din partea utilizatorului.

3. Panou de monitorizare si raportare (Dashboard):

- Rapoartele din panoul de monitorizare vor putea fi configurate specificând numele raportului, tipul raportului, ținta raportului, opțiuni specifice pentru orice tip de raport (de exemplu pentru raportul de actualizare - care este intervalul după care o stație este considerata neactualizata).
- Panoul central conține rapoarte pentru toate modulele suportate.
- Rapoartele din panoul central de comanda permit: adăugarea altor rapoarte, ștergerea lor si rearanjarea.

4. Inventarierea rețelei – managementul securității:

- Soluția se va integra cu domeniul Active Directory si va putea importa inventarul.
- Se permite descoperirea stațiilor fizice neintegrate in Active Directory (Workgroup) cu ajutorul Network discovery.
- Soluția va oferi opțiuni de căutare, sortare si filtrare după numele sistemului, sistem de operare, adresa IP, politica aplicata, ultima data când s-a conectat (online si/sau offline) si FQDN.
- Soluția va permite crearea unui pachet unic pentru toate sistemele de operare, de stații sau servere. Astfel, administratorul va putea descarcă pachetele pentru protecția stațiilor si serverelor pe care rulează sistemul de operare Windows, Linux, Mac.
- Soluția va permite instalarea la distanta sau manual a clienților antimalware pe mașini fizice/virtuale.
- Soluția va permite selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe mașinile fizice/virtuale.
- Soluția va permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanta pentru clientul antimalware.
- Soluția va oferi posibilitatea de repornire a mașinilor fizice de la distanta.

- Soluția va oferi informații detaliate despre fiecare task si se fișează daca task-ul s-a finalizat sau nu cu succes.
- Soluția va permite configurarea centralizata a clienților antimalware prin intermediul politicilor
- Se vor oferi in consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizare, Versiunea produsului, Versiunea de semnături.

5. Politici:

- Soluția va permite configurarea setărilor clientului antimalware prin intermediul unei singure politici ce conține setări pentru toate module
- Politica va conține opțiuni specifice de activare/dezactivare si configurarea funcționalităților precum scanarea antimalware la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, power user.
- Soluția permite aplicarea politicilor pe mașini client, grupuri de mașini, domeniu, unități organizaționale.
- Politica sa poate fi schimbata automat in funcție de:
    - IP sau clasa de IP al stației
    - Gateway-ul alocat
    - DNS serverul alocat
    - WINS serverul alocat
    - Sufix DNS pentru conexiunea dhcp
    - Clientul este/nu este in accesai rețea cu infrastructura de management (stația de lucru poate soluționa implicit numele gazdei)
    - Tipul rețelei (lan, wireless)

6. Rapoarte:

- Soluția va conține rapoarte care prezinta statusul mașinilor clienților din punct de vedere al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate.
- Rapoartele programate pot fi trimise către un număr nelimitat de adrese de email (nu este nevoie sa aibă un cont in consola de management).
- Soluția va permite vizualizarea rapoartelor curente programate de administrator.
- Soluția va permite exportarea rapoartelor in format .pdf si detaliile ca format .csv. sau arhiva.
- Soluția include un generator de rapoarte care oferă posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menținând informațiile concise si ordonate corespunzător. Astfel, Soluția include interogări precum: starea terminalului, evenimente terminal, evenimente Exchange.

- Interogarea legata de starea terminalului include informații precum:
  - tip mașină
  - infrastructura rețelei căreia ii aparține terminalul
  - datele agentului de securitate
  - starea modulelor de protecție
  - rolurile terminalelor.
- Interogarea legata de evenimente terminal include informații precum:
  - calculatorul țintă pe care a avut loc evenimentul
  - tipul starea si configurația agentului de securitate instalat
  - starea modulelor si rolurilor de protecție instalate pe agentul de securitate
  - utilizatorul autentificat in timpul evenimentului

7. Utilizatori:

- Administrarea se va putea face pe baza de roluri.
- Roluri multiple predefinite: Administrator companie, Administrator rețea, Reporter sau rol personalizat.
  - Administrator companie: administrează arhitectura consolei de management;
  - Administrator rețea: administrează serviciile de securitate;
  - Reporter: monitorizează si generează rapoarte.
- Utilizatorii pot fi importați din Microsoft Active Directory sau creați in consola de management.
- Se va permite configurarea detaliata a drepturilor administrative, permițând selectarea serviciilor si obiectelor pentru care un utilizator poate face modificări.
- Se va permite deconectarea automata a oricărui tip de utilizator după un anumit timp pentru o protecție sporita a datelor afișate in consola de administrare. Acest interval se poate personaliza de administratorul soluției.

8. Log-uri:

- Înregistrarea acțiunilor utilizatorilor.
- Se vor oferi informații detaliate pentru fiecare acțiune a unui utilizator.
- Se va permite filtrarea acțiunilor utilizator după numele utilizatorului, acțiune.

9. Actualizare:

- Se permite definirea de locații de actualizare multiple.
- Se permite activarea/dezactivarea actualizărilor de produs si semnături.
- Orice client antivirus sa poată fi configurat sa livreze update-urile către alt client antivirus

B. PROTECTIE STATII SI SERVERE FIZICE/VIRTUALE

1. Caracteristici generale minimale si eliminatorii:

- Pentru reducerea la minim a consumului de resurse, soluția antimalware trebuie sa permită instalarea personalizata a modulelor deținute (de exemplu, sa permită instalarea soluției antimalware fără modulul de control al accesului web, modul de control al dispozitivelor sau modulul firewall).
- Pentru o mai buna protecție a stațiilor si serverelor, Soluția include un vaccin anti-ransomware. Acest vaccin asigura protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor si serverelor, chiar daca sunt infectate si prin blocarea procesului de criptare.
- Vaccinul anti-ransomware primește actualizări de la producător, odată cu actualizarea semnăturilor produsului Antimalware.
- Pentru o mai buna protecție a stațiilor si serverelor, soluția include protecție împotrivă atacurilor zero-day de tip exploit avansate (atacuri direcționate) bazata pe tehnologii de învățare automata (machine learning).
- Pentru o mai buna protecție a a stațiilor si serverelor, Soluția include un modul integrat de tip ERA (Endpoint Risk Analytics – Analiza de risc a endpoint-ului) capabil sa identifice si remedieze in mod automatizat sau manual un număr mare de riscuri existente la nivel de rețea sau sistem de operare ce pot afecta funcționalitatea si nivelul de securizare al endpoint-ului
- Pentru o mai buna protecție a stațiilor si serverelor, Soluția include un modul avansat de securitate – HyperDetect, bazat pe tehnologii de tip „machine learning tunabil” proiectat special pentru a detecta atacuri avansate si activități suspecte in faza pre-execuție.
- Acest modul avansat de securitate va proteja împotrivă: atacurilor direcționate (Targeted Attack - APT), fișierelor suspecte si traficului la nivel de rețea suspect, exploit-urilor, ransomware si grayware. Fiecărui tip de amenințare menționat, i se vor putea stabili, independent, un nivel de protecție dorit: permisiv, normal, agresiv.
- Modulul avansat de securitate are posibilitatea de a raporta, bloca accesul, dezinfecta, șterge sau muta in carantina pentru fiecare din categoriile descrise. Astfel, administratorul va putea decide daca dorește întâi monitorizare sau dorește si blocarea amenințărilor. Aceste acțiuni menționate, vor putea fi stabilite independent, pentru fișiere sau pentru traficul din rețea, cu posibilitatea extinderii nivelului de raportare pentru a include nivelurile superioare (vor putea fi raportate amenințările care ar fi fost detectate daca nivelul de protecție era stabilit mai agresiv).
- Pentru a oferi un nivel adițional de protecție a stațiilor si serverelor, soluția include un sandbox in cloud-ul public al producătorului acesteia.
- Modulul de Sandbox va putea trimite automat fișiere in Sandbox-ul din cloud-ul producătorului unde vor putea fi „detonate” pentru o analiza in profunzime.
- Modulul de Sandbox include doua variante de analiza: doar monitorizare sau blocare. In modul monitorizare utilizatorul va putea accesa fișierul dorit, pe când in modul blocare, utilizatorului i se va bloca rularea fișierului până când Sandbox-ul din cloud-ul producătorului va da verdictul.

- Modulul de Sandbox include doua tipuri de acțiuni remediere: implicită și de siguranță. Pentru acțiunea implicită se va putea stabili: doar raportare, dezinfecție, ștergere si carantinare. Pentru acțiunea de siguranță se va putea stabili: ștergere sau carantinare.
- Modulul de Sandbox include si posibilitatea de trimitere manuală a fișierelor in Sandbox-ul din cloud-ul producătorului. Astfel, daca administratorul suspectează un fișier ca fiind malitios, îl poate trimite manual in Sandbox pentru a fi „detonat" si a afla verdictul. Va putea trimite mai multe fișiere de odată, cu posibilitate de a specifica daca vor fi „detonate" individual sau toate in același timp.
- Modulul de Sandbox poate suporta „detonarea" următoarelor tipuri de fișiere: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.
- Fișierele menționate anterior, vor putea fi detectate corect chiar daca sunt incluse in arhive de tipul: : 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ.
- Modul de detectare, corelare si răspuns la evenimente de tip EDR („endpoint detection and response") capabil sa identifice amenințări avansate sau atacuri in curs de desfășurare.
- Acest modul cuprinde colectare de date si evenimente despre hardware si software aferent fiecărei stații de lucru aducând informații detaliate referitoare la incidentele detectate, o harta detaliata a acestora precum si acțiuni de remediere automate si integrare cu modulele de Sandbox si modulul avansat de securitate - – HyperDetect. Din punct de vedere funcțional modulul EDR cuprinde 2 componente distincte: senzorul ce colectează si procesează datele respectiv partea de analiza de securitate care are ca obiect interpretarea acestora.
- Modulul EDR are capacitatea de a evalua activitatea tipica a unui endpoint din perspectiva securității acestuia conform tehnicilor de atac MITRE („baselining") si poate raporta orice deviație de la acest comportament sub forma unui incident
- Modulul EDR permite filtrarea incidentelor din interfață grafică in funcție intervalul de timp, pe baza unui scor de încredere („confidence score"), indicatori de atac, tehnici de atac (ATT&CK) respectiv sistem de operare afectat cat si după IP, nume fișier, nume stație.
- Modulul permite vizualizarea detaliata a incidentelor incluzând detalii specifice fiecărui nod afectat după cum urmează: tabul „rezumat" generează o harta de principiu a incidentului, tabul „timeline" detaliază incidentul in functie de amprenta de timp a fiecărei acțiuni aferente incidentului, respectiv butonul „acționează" care poate genera un set de masuri specifice fiecărui element din harta incidentului (kill, carantina – la nivel de nod, investigați – virus total, sandbox, google – la nivel de fișier, adăugare in lista de blocare – la nivel de rețea sau instalare patch – la nivel de nod).
- Modulul poate excepta fișiere non-malițioase de la acțiunea de investigare sau poate genera/adăuga un set de fișiere malițioase într-o lista neagra pentru a preveni mișcarea laterala a fișierelor/proceselor malițioase.

2. Cerințe de sistem:

- Sisteme de operare pentru stații de lucru: Windows 11, Windows 10, macOS 12 Monterey și toate versiunile ulterioare
- Sisteme de operare embedded: Windows 10 IoT Enterprise
- Sisteme de operare pentru servere: Windows Server 2016; Windows Server 2019 (inclusiv Core); Windows Server 2022 (inclusiv Core); Windows Server 2025
- Sisteme de operare Linux – distribuții și versiuni live:
    - Red Hat / CentOS / derivate:
    - RHEL 8.x și 9.x
    - CentOS 7.x, CentOS Stream 8, 9, 10
    - AlmaLinux 8.x, 9.x, 10.x
    - Rocky Linux 8.x, 9.x, 10.x
    - Oracle Linux 7.x–10.x (UEK și RHCK)
    - CloudLinux 7.x, 8.x
    - Miracle Linux 8.x
    - Kylin v10 (RHEL-based)
- Debian / Ubuntu & derivate:
    - Debian 9, 10, 11, 12
    - Ubuntu 18.04.x, 20.04.x, 22.04.x, 23.04.x, 24.04.x
    - Pop!_OS 22.04.x, 24.04.x
    - Linux Mint 20.x, 21.x, 22.x
    - Zorin OS (versiunile actuale suportate)
    - Linux Mint Debian Edition 6
    - TUXEDO OS
- SUSE & altele:
    - SUSE Linux Enterprise Server 12 SP4+ și 15.x
    - openSUSE Leap 15.x, MicroOS (versiunile listate)
    - Fedora 37–43 (până la expirarea fiecărei versiuni)
    - Amazon Linux 2 și Microsoft Azure Linux 3
    - openEuler 24.x

3. Administrare si instalare remote:

- Înainte de instalare, administratorul va putea particulariza pachetele de instalare cu modulele dorite: firewall, content control, device control, power user.
- Instalarea se va putea face in mai multe moduri:

- prin descărcarea directa a pachetului pe stația pe care se va face instalarea;
- prin instalarea la distanta, direct din consola de management
- trimiterea pe email (oricâte adrese) a linkului cu pachetul de instalare pentru Windows, Linux, Mac.

- Instalarea clienților la distanta in alte locații decât cele in care este instalata consola de management se va face prin intermediul unui alt client antivirus existent in locațiile respective pentru a minimiza traficul in WAN.
- In consola vor fi disponibile informații despre fiecare stație: numele stației, IP, sistem de operare, module instalate, politica aplicata, informații despre actualizări etc.
- Din consola se va putea trimite o singura politica pentru configurarea integrala a clientului de pe stații/servere.
- Consola va include o secțiune, „Audit”, unde se vor menționa toate acțiunile întreprinse fie de administratori fie de reporteri, cu informații detaliate: logare, editare, creare, delogare, mutare etc.
- Posibilitatea creării unui singur pachet de instalare, utilizabil atât pentru sistemele de operare pe 32 de biți cat si pentru cele pe 64 de biți.
- Posibilitatea creări unui singur pachet de instalare, utilizabil pentru stații (fizice si/sau virtuale), servere (fizice si/sau virtuale), exchange.
- Posibilitatea de a crea pachetele de instalare de tip web installer sau kit full.
- Administratorul va putea crea grupuri sau chiar subgrupuri, unde va putea muta stațiile/serverele din rețea pentru cele care nu sunt integrate domeniu.
- Permite selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decât cele integrate in domeniu.

4. Caracteristici si funcționalități principale ale modulului antimalware:

- Soluția permite administratorului sa stabilească acțiunea luată de produsul Antimalware la detectarea unei amenințări noi. Astfel administratorul va putea alege intre următoarele acțiuni:
  - Acțiune implicită pentru fișiere infectate:
    - interzice accesul
    - dezinfectează
    - ștergere
    - muta fesierele in carantina
    - nicio acțiune
  - Acțiune alternativa pentru fesierele infectate:
    - interzice accesul
    - dezinfectează

        - ștergere
        - mută fesierele in carantină
    - Acțiune implicită pentru fesierele suspecte:
        - interzice accesul
        - ștergere
        - muta fișierele in carantina
        - nicio acțiune
    - Acțiune alternativa pentru fișierele suspecte:
        - interzice accesul
        - ștergere
        - muta fișierele in carantina
- Scanarea automata in timp real va putea fi setata sa nu scaneze arhive sau fișiere mai mari de « x » MB, mărimea fișierelor putând fi definita de administratorul soluției,
- Definirea pana la 16 nivele de profunzime pentru scanarea in arhive.
- Scanarea euristica comportamentala prin simularea unui calculator virtual in interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătura nu a fost lansata încă.
- Scanarea oricărui suport de stocare a informației (CD-uri, harduri externe, unități partajate etc). De asemenea, se va putea anula scanarea in cazul in care sunt detectate unități care au informații stocate mai mult de « x » MB.
- Configurarea cailor ce urmează a fi scanate la cerere.
- Clienții antimalware pentru workstation să permită definirea unor liste de excludere de la scanarea in timp real si la cerere a anumitor directoare, discuri, fișiere, extensii sau procese.
- Cu ajutorul unei baze de date complete cu semnături de spyware si a euristicii de detecție a acestui tip de programe, produsul va trebui sa ofere protecție anti-spyware.
- Abilitatea de a detecta atacuri fără fișiere, inclusiv cele care folosesc instrumente legitime ale sistemului de operare, cum ar fi Powershell sau interpreții de script. Soluția nu va bloca global scripturile pentru a realiza acest lucru.
- Oferă tehnologia Anti-Ransomware.
- Posibilitatea de configura scanarile programate sa se execute cu prioritate redusa
- Produsul antimalware poate fi configurat să folosească scanarea in cloud, și parțial scanarea locala. Pentru stațiile ce nu au suficiente resurse hardware, scanarea se poate face cu o mașina de scanare instalata in rețea (scanare centralizata).
- Administratorul poate personaliza și motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare:

- Scanare locală, când scanarea se efectuează pe stația de lucru locală. Modul de scanare locală este potrivit pentru mașinile puternice, având toate semnăturile și motoarele stocate local.
- Scanarea hibrid cu motoare light (Cloud public), cu o amprentă medie, folosind scanarea în cloud și, parțial, semnături locale. Acest mod de scanare oferă avantajul unui consum mai bun de resurse, fără să implice scanarea locală.
- Scanarea centralizată în Cloud-ul privat, cu o amprentă redusă, necesitând un server de securitate pentru scanare. În acest caz, nu se stochează local nicio semnătură, iar scanarea este transferată către serverul de securitate.
- Scanare centralizată (Scanare în cloud privat cu server de securitate) cu fallback* pe Scanare locală (motoare full)
- Scanare centralizată (Scanare în cloud privat cu server de securitate) cu fallback* pe Scanare hibrid (cloud public cu motoare light)

- Pentru o protecție sporită, soluția antimalware trebuie sa aibă 3 tipuri de detecție: bazata pe semnături, bazată de comportamentul fișierelor si bazata pe monitorizarea proceselor.
- Pentru o protecție sporită, soluția antimalware trebuie sa poată scana paginile HTTP.
- Pentru o mai buna gestionare a antimalware instalat pe stații, produsul va include opțiunea de setare a unei parole pentru protecția la dezinstalare.
- Pentru siguranța utilizatorului, clientul va include un modul de antiphishing.
- Soluția oferă protecție in timp real pe mașinile cu sistem de operare Linux in conformitate cu versiunea de kernel instalată.

5. Anti-Exploit-Avansat:

- Posibilitatea de a opri atacurile avansate de tip „zero-day” efectuate prin intermediul unor exploit-uri evazive
- Depistarea in timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare.
- Protejarea aplicațiilor utilizate frecvent si a celor de tip „sistem” cum ar fi browserele, aplicațiile de tip office sau reader, procesele critice aferente sistemelor de operare.

6. Firewall:

- Posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate.
- Modulul poate fi instalat/dezinstalat in funcție de preferința administratorului.
- Posibilitatea de a defini rețele de încredere pentru mașina destinație.
- Abilitatea de a detecta scanarea de porturi.
- Posibilitatea de a seta diferite profiluri de rețea (Home/Office, Trusted, Public, Untrusted sau Let the Windows decide)
- Abilitatea de a crea reguli personalizate bazate pe aplicație și/sau conexiune

7. Carantina:

- Produsul antimalware să permită trimiterea automată a fișierelor din carantina către laboratoarele antimalware ale producătorului.
- Trimiterea conținutului carantinei va putea fi expediat in mod automat, la un interval definit de administrator.
- Produsul antimalware sa permită ștergerea automata a fișierelor carantinate mai vechi de o anumita perioada, pentru a nu încarcă inutil spațiul de stocare.
- Posibilitatea de a restaura un fișier din carantina in locația lui originala.
- Modulul de carantina va permite rescanarea obiectelor după fiecare actualizare de semnături.

8. Controlul dispozitivelor:

- Modulul poate fi instalat/dezinstalat in funcție de preferința administratorului.
- Modulul va permite controlul următoarelor tipuri de dispozitive:
    - Bluetooth Devices
    - CDROM Devices
    - Floppy Disk Drives
    - Security Policies 153
    - IEEE 1284.4
    - IEEE 1394
    - Imaging Devices
    - Modems
    - Tape Drives
    - Windows Portable
    - COM/LPT Ports
    - SCSI Raid
    - Printers
    - Network Adapters
    - Wireless Network Adapters
    - Internal and External Storage
- Modulul va permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client.
- Modulul va permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli.

9. Power User:

- Modulul poate fi instalat/dezinstalat in funcție de preferința administratorului.

- Modulul permite posibilitatea de a acorda utilizatorilor drepturi de Power User. Utilizatorii vor putea accesa si modifica setările clientului antimalware dintr-o consola disponibila local pe mașina client.
- Modificările efectuate din modulul Power User vor fi active local, pe mașina pe care s-au făcut respectivele modificări.
- Administratorul va putea suprascrie din consola setările aplicate de utilizatorii Power User.

10. Actualizare:

- Posibilitatea efectuării actualizării la nivel de stație in mod silențios (fără avertizare).
- Sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate).
- Actualizarea pentru locațiile remote prin intermediul unui client antimalware care are si rol de server de actualizare.
- Abilitatea de a împiedica punctele finale să iasă pe internet pentru a descărca actualizări.

C. Monitorizare și răspuns 24x7

- Serviciul va oferi monitorizare și răspuns 24x7 pentru a elimina cheltuielile operaționale de gestionare a alertelor și evenimentelor de securitate.
- Trebuie incluse cel puțin servicii precum: investigații incidente, răspunsuri / reacții la posibile atacuri, recomandări in caz ca sunt observate sau detectate anumite vulnerabilități cat si servicii de tip “threat hunting” pentru eventualele amenințați care nu sunt neapărat vizibile.
- Informații despre amenințări prin cercetarea amenințărilor cibernetice, a activităților geopolitice și tendințele globale ale datelor.
- Control al organizației pentru acțiuni pre aprobate (spre exemplu, organizația poate controla daca stațiile protejate pot fi izolate de rețea automat sau nu, daca procesele pot fi oprite, fișierele infectate pot fi șterse automat, etc).
- Soluția trebuie sa permită definirea de contacte de urgenta (email si telefon) in cazul in care echipa SoC MDR trebuie sa ia legătura urgent cu organizația in anumite situații (e.g., incident critic).
- Monitorizare Darkweb pentru a descoperi informații “scurse” din organizație (spre exemplu, monitorizare daca anumite informații senzitive ale organizației sunt “vândute” pe aceste platforme).
- Notificări personalizate pe email la momentul unui eveniment (spre exemplu, un raport de acțiune a fost generat si poate fi accesat).
- Rapoarte lunare de service incluzând raport după fiecare incident de tip critic sau major, si rapoarte lunare cu statistici serviciu.
- Access la consola de tip web MDR unde se poate observa activitatea echipei SoC de MDR, investigațiile in curs, activitățile de tip threat hunting, recomandările primite, rapoartele generate, deschiderea unui ticket cu echipa de suport, etc.

4.10.7 Soluție SIEM (Security Information and Event Management) - 1 pachet

Soluție software pentru **monitorizare de securitate, identificare vulnerabilități și detecție / răspuns la incidente**, implementată într-un mediu virtualizat din cloud guvernamental.

Soluția trebuie sa respecte minimal următoarele cerințe tehnice și funcționale :

1. **Cerințe generale**
   - Soluția trebuie să fie:
     - modulară și scalabilă
     - implementabilă în medii virtualizate
   - Soluția trebuie să includă:
     - componente de colectare date
     - analiză și corelare
     - interfață de vizualizare web
2. **Cerințe funcționale - Vulnerability Management**
   - Identificarea vulnerabilităților pe baza bazelor de date publice (ex: CVE sau echivalent)
   - Scanare:
     - periodică configurabilă
     - la cerere
   - Clasificare vulnerabilități după severitate
   - Corelare cu:
     - pachete software instalate
     - configurații sistem
   - Generare rapoarte și notificări
3. **Cerințe funcționale - SIEM**
   - Colectarea logurilor din:
     - sisteme Windows și Linux
     - echipamente de rețea (syslog sau echivalent)
   - Corelare evenimente pe bază de reguli
   - Definire reguli personalizate
   - Dashboard-uri și vizualizare evenimente
   - Stocare și căutare în date istorice
4. **Cerințe funcționale - XDR**
   - Monitorizarea endpoint-urilor prin agenți
   - Detectarea:

- modificărilor de fișiere
- execuțiilor suspecte

- Corelare între:
  - endpoint-uri
  - servere
- Capabilități de răspuns:
  - colectare informații pentru investigații

5. **Cerințe integrare și arhitectură**
   - Implementare în mediu virtualizat
   - Arhitectură distribuită (agent + server)
   - Compatibilitate cu LDAP / Active Directory sau echivalent
   - Interfață web pentru administrare
6. **Cerințe securitate**
   - Criptare comunicații (TLS sau echivalent)
   - Autentificare și control acces
   - Jurnalizare acțiuni administrative
7. **Cerințe performanță și scalabilitate**
   - Soluția trebuie să suporte minimum:
     - **120 surse de loguri monitorizate simultan**
   - Trebuie să permită:
     - extindere ulterioară fără reinstalare completă
   - Procesarea evenimentelor trebuie să fie:
     - near real-time (în funcție de resursele alocate)
8. **Cerințe dimensionare resurse hardware**

Pentru funcționarea soluției la capacitatea minimă de 120 de surse de loguri, ofertantul trebuie să propună o arhitectură care să respecte următoarele cerințe minime:

Nod central (management + analiză)

- CPU: maxim 8 vCPU
- RAM: maxim 16 GB
- Storage:
  - maxim 500 GB pentru stocare loguri și date analiză
  - tip: SSD
- Sistem de operare suportat:

- Linux sau echivalent

Nod colectare / indexare (dacă este separat)

- CPU: naxim 4 vCPU
- RAM: maxim 8 GB
- Storage: maxim 250 GB

Endpoint-uri monitorizate

- Agenții trebuie să funcționeze pe:
  - Windows (stații și servere)
  - Linux
- Consum resurse endpoint:
  - redus, fără impact semnificativ asupra utilizatorului

Cerințe generale resurse

- Soluția trebuie să permită:
  - ajustarea resurselor alocate (scalare verticală)
  - distribuirea componentelor pe mai multe mașini virtuale
- Trebuie să funcționeze în medii:
  - virtualizate
  - cloud privat / guvernamental

9. Cerințe raportare

- Dashboard-uri configurabile
- Rapoarte:
  - vulnerabilități
  - incidente de securitate
- Export:
  - PDF, CSV sau echivalent

10. Cerințe implementare

- Instalare și configurare inițială
- Integrare în infrastructura existentă
- Documentație tehnică
- Instruire personal

11. Cerințe suport

- Suport tehnic conform SLA
- Actualizări:

- reguli de detecție
- baze de vulnerabilități

4.10.8 Scanner vulnerabilități – 1 pachet

Soluție dedicată pentru scanarea externă a vulnerabilităților, independentă de alte platforme de monitorizare, implementată în mediul cloud.

1. **Cerințe generale**
   - Soluția trebuie să funcționeze:
     - independent de agenți instalați pe endpoint-uri
     - utilizând protocoale standard de rețea
   - Scanarea trebuie să poată fi realizată:
     - din interiorul infrastructurii
     - din segmente de rețea definite
2. **Cerințe funcționale de scanare**
   - Scanare pe bază de:
     - IP individual
     - intervale IP
     - hostname
   - Identificare:
     - porturi deschise
     - servicii active
   - Detectare vulnerabilități la nivel:
     - sistem de operare
     - servicii
     - aplicații
3. **Politici și configurare**
   - Politici predefinite de scanare
     Profiluri personalizabile
   - Suport pentru:
     - scanări autentificate
     - scanări neautentificate
4. **Baze de date și actualizări**
   - Utilizare baze de date actualizate (CVE sau echivalent)
   - Trebuie să includă:

- actualizări regulate ale plugin-urilor
- mecanisme automate de update

5. **Cerințe raportare**
   - Rapoarte detaliate cu:
     - vulnerabilități
     - severitate
     - impact
     - recomandări
   - Clasificare pe niveluri de risc
   - Export:
     - CSV
     - JSON sau echivalent
6. **Cerințe licențiere și subscripție**
   - Soluția trebuie să includă:
     - drept de utilizare pentru minimum 36 luni
   - Subscripția trebuie să acopere:
     - actualizări baze vulnerabilități
     - actualizări motor scanare
     - suport tehnic
7. **Cerințe suplimentare**
   - Nu se acceptă soluții care:
     - nu oferă actualizări regulate
     - necesită costuri suplimentare pentru funcționalități de bază

4.10.9 Servicii monitorizare tip MDR/SOC – 1 pachet

Prestarea de servicii de tip **monitorizare, suport și asistență tehnică pentru incidente de Securitate** de tip Managed Detection & Response (MDR) și Security Operations Center (SOC), aferente infrastructurii implementate în cadrul proiectului.

1. **Cerințe generale**
   - Prestatorul va asigura servicii de tip:
     - monitorizare și analiză evenimente de securitate
     - suport în investigarea incidentelor
     - recomandări de remediere
   - Serviciile vor acoperi:

- întreaga infrastructură de securitate implementată în proiect
- Serviciile vor fi furnizate:
  - la cerere și/sau pe baza alertelor generate de sistemele existente

2. **Program de operare și disponibilitate**
   - Program de disponibilitate:
     - **8 ore/zi, 5 zile/săptămână (8x5)**
     - Timp de răspuns, Next Business Day (NBD)
   - Serviciile prestate vor include:
     - analiză incidente
     - investigații
     - recomandări tehnice
     - suport operațional
3. **Monitorizare și analiză alerte**
   - Prestatorul va asigura monitorizarea alertelor generate de infrastructura existentă.
   - Surse de date monitorizate:
     - firewall
     - WAF
     - soluții de protecție DDoS
     - IDS/IPS
     - servere și sisteme de operare
     - endpoint-uri
     - aplicații web
   - Monitorizarea se va realiza:
     - pe baza datelor disponibile în platformele existente
4. **Investigarea incidentelor**
   - Prestatorul va asigura analiza și investigarea incidentelor de securitate identificate.
   - Activitățile includ:
     - analiza alertelor generate
     - corelarea evenimentelor
     - identificarea cauzelor probabile
   - Vor fi investigate inclusiv:
     - tentative de acces neautorizat
     - atacuri web

- atacuri de tip DDoS
- alerte IDS/IPS
- blocări de cont
- anomalii de acces

5. **Recomandări de remediere**
   - Prestatorul va furniza recomandări tehnice pentru remedierea incidentelor.
   - Recomandările vor include:
     - acțiuni propuse
     - prioritizarea acestora în funcție de impact
   - Implementarea măsurilor:
     - rămâne în responsabilitatea beneficiarului (cu suport la cerere)
6. **Raportare**
   - Prestatorul va furniza un **raport lunar de securitate**.
   - Raportul va include:
     - incidente detectate
     - acțiuni de analiză efectuate
     - recomandări
     - tendințe și riscuri identificate
     - sumar analiză loguri
7. **Escaladare incidente**
   - Prestatorul va asigura notificarea beneficiarului în cazul incidentelor critice.
   - Escaladarea va include:
     - descriere incident
     - impact estimat
     - recomandări imediate

4.11 Confidențialitatea datelor

4. Contextul GDPR

Soluția informatică dezvoltată în cadrul proiectului va procesa volume semnificative de date cu caracter personal, conformitatea cu GDPR și Legea nr. 190/2018 fiind obligatorie. Autoritatea Contractantă rămâne operatorul de date, iar Prestatorul acționează ca împuternicit exclusiv pentru activitățile tehnice aferente soluției..

Legislația GDPR în România se aplică prin intermediul Regulamentului General privind Protecția Datelor (Regulamentul (UE) 2016/679), cunoscut sub numele de GDPR, care este direct aplicabil în toate statele membre ale Uniunii Europene, inclusiv România. Pe plan național, Legea nr. 190/2018

completează și clarifică aplicarea GDPR în România, specificând aspecte legate de prelucrarea datelor personale, desemnarea responsabilului cu protecția datelor și sancțiunile aplicabile.

5. **Cerințe GDPR - Responsabilitatea Prestatorului (strict tehnică)**

2.1. Analiza tehnică a fluxurilor de date

Prestatorul va:

- Identifica și documenta fluxurile de date personale strict în cadrul soluției informatice.
- Evidenția punctele de intrare, stocare, prelucrare și ieșire a datelor.
- Furniza Beneficiarului documentația necesară pentru evaluările GDPR pe care acesta le realizează.

2.2. Implementarea măsurilor tehnice de securitate

Prestatorul va implementa în soluție:

- Controlul accesului pe roluri (RBAC).
- Jurnalizare și audit trail.
- Mecanisme de backup și restaurare.
- Criptare în tranzit și, unde este necesar, criptare la stocare.
- Mecanisme de protecție împotriva accesului neautorizat.

2.3. Funcționalități pentru exercitarea drepturilor persoanelor vizate

Prestatorul va asigura ca Soluția să permită:

- Exportul datelor personale asociate unui utilizator.
- Rectificarea datelor.
- Ștergerea datelor conform politicilor Beneficiarului.
- Restricționarea prelucrării, acolo unde este aplicabil.

Notă: Decizia când și cum se aplică aceste drepturi aparține exclusiv Autorității Contractante.

2.4. Mecanisme pentru gestionarea consimțământului (dacă este necesar)

Prestatorul va implementa în aplicație:

- Funcționalități de colectare, retragere și evidență a consimțământului.
- Interfețe pentru gestionarea preferințelor utilizatorilor.

Notă: Autoritatea Contractantă stabilește temeiul legal al fiecărei prelucrări.

2.5. Suport tehnic pentru documentația GDPR

Prestatorul va furniza Beneficiarului:

- Descrierea tehnică a sistemului.
- Descrierea măsurilor tehnice și organizatorice implementate în soluție.

- Informații necesare pentru DPIA, registre de prelucrare și alte documente GDPR elaborate de Beneficiar.

Notă: Prestatorul nu elaborează politici GDPR interne ale instituției și nu desemnează DPO.

3. Cerințe GDPR – Responsabilitatea Autorității Contractante (operatorul de date)

Autoritatea Contractantă este responsabilă pentru:

- Stabilirea temeiurilor legale ale prelucrării.
- Elaborarea politicilor și procedurilor GDPR interne.
- Desemnarea DPO.
- Realizarea DPIA (cu suport tehnic din partea Prestatorului).
- Gestionarea solicitărilor persoanelor vizate.
- Monitorizarea conformității la nivel organizațional.

4. Proprietatea asupra datelor

- Datele generate de utilizatorii interni sunt proprietatea exclusivă a Achizitorului.
- Datele introduse de utilizatorii externi sunt proprietatea exclusivă a acestora.
- Prestatorul nu dobândește niciun drept asupra datelor și nu le poate utiliza în alte scopuri decât cele contractuale.

5 Ipoteze și riscuri

5.1 Ipoteze

Următoarele ipoteze vor sta la baza întocmirii ofertelor:

- Începerea activităților contractului se va realiza în perioada preconizată;
- Nu se prevăd schimbări ale cadrului instituțional și legal care să afecteze major implementarea și desfășurarea în bune condiții a Contractului;
- Autoritatea contractantă va nominaliza o echipă de experți care vor colabora cu prestatorul pentru implementarea cu succes a proiectului.
- Autoritatea contractantă va nominaliza un manager de proiect care va fi împuternicit să ia decizii cu privire la implementarea proiectului.
- Toate solicitările de informații adresate autorității contractante vor primi răspuns în termen de 3-5 zile lucrătoare, în funcție de complexitatea problematicii.
- Se vor putea realiza recepții parțiale pentru diferite livrabile ale proiectului.

5.2 Riscuri

La elaborarea ofertelor, operatorii economici trebuie să ia în calcul următoarele riscuri, care pot interveni în derularea contractului:

- Surse de ordin instituțional - factori care aparțin organizației.
- Surse de mediu legislativ - factori care provin din contextul legislativ național (legislația actuală aplicabilă).
- Surse externe (la nivel național/european) - factori ce sunt determinați de specificul reglementărilor și regulilor în domeniul fondurilor europene.
- Surse de ordin financiar - factori care provin din constrângeri (limitări) de tip financiar, cu privire la nivelul și disponibilitatea resurselor necesar a fi alocate.

În ceea ce privește riscurile de mediu și legate de schimbările climatice, precizăm că nu există o vulnerabilitate a proiectului referitor la aceste aspecte.

Principalele riscuri identificate de către autoritatea contractantă, precum și strategiile de gestionare a acestor riscuri, sunt prezentate în continuare.

Tabel 5 - Riscuri

Nr. crt.	Riscul identificat	Măsurile de atenuare a riscului
1.	Nerespectarea termenelor de livrare/furnizare a bunurilor/serviciilor de către subcontractori Posibile consecințe: Prelungirea perioadei de implementare față de cea preconizată inițial;	Impact: mare Probabilitate de apariție: medie Măsurile de atenuare: • Definirea și respectarea unei metodologii de implementare corespunzătoare;

Nr. crt.	Riscul identificat	Măsurile de atenuare a riscului
	Întârzierile în finalizarea proiectului ar putea conduce la pierderi financiare	• Stabilirea unui plan de comunicare coerent cu furnizorii la nivelul proiectului; • Prevederea in realizarea graficului de implementare a unor durate acoperitoare pentru activitățile prevăzute in cererea de finanțare
2.	Erori în definirea specificațiilor echipamentelor Posibile consecințe: Neprevederea anumitor specificații minime necesare pentru buna funcționare a echipamentelor	Impact: mare Probabilitate de apariție: mica Înainte de inițierea proiectului, una din problemele ce intră în atribuțiile managerului de proiect este de a planifica în detaliu toate etapele de desfășurare ale proiectului, între care este inclusă și etapa de specificații tehnice Măsurile de atenuare: • Planificarea detaliată a activității de cercetare și proiectare în ceea ce privește echipamentele ce se doresc a se achiziționa • Actualizarea periodica a riscurilor împreuna cu echipa de proiect; • Urmărirea periodica a riscurilor; • Alocarea in echipa de proiect a unor resurse umane înalt calificate; • Remedierea disfuncționalităților; • Stabilirea mai multor soluții tehnologice astfel încât fiecare componenta sa aibă si o alternativa de backup;
3.	Insuficiente resurse umane si financiare alocate pentru susținerea proiectului Posibile consecințe: Întreruperea unor activități inițiate, pierderea continuității	Impact: mare Probabilitate de apariție: medie În funcție de severitatea modificărilor și a gradului de afectarea a desfășurării proiectului se vor lua măsuri suplimentare, inclusiv redefinirea unor activități/cu acordul corespunzător al finanțatorului. Măsurile de atenuare: • Prevederea unor intervale suplimentare de timp pentru reorganizarea activităților în funcție de schimbările apărute • Realizarea unei planificări clare pentru

Nr. crt.	Riscul identificat	Măsurile de atenuare a riscului
		fiecare etapa, inclusiv nivelul de încărcare pentru fiecare persoana; • Asigurarea personalului necesar si definirea personalului cu rol de back-up pentru situațiile când aceasta este necesar; • Stabilirea clara a rolurilor pe care le dețin fiecare dintre persoanele implicate; • Monitorizarea constanta a gradului de încărcare a resurselor precum si disponibilitatea continua a resurselor back-up, asigurându-se astfel continuitatea in desfășurarea activităților proiectului; • Aplicarea cailor de escaladare stabilite prin planul de comunicare in cazul in care se constata gap-uri in fluxul de comunicare/colaborare
4.	Schimbări legislative Posibile consecințe: Redefinirea unor activități, includerea unor elemente noi în funcție de schimbările legislative.	Impact: mare Probabilitate de apariție: medie Modificările legislative pot afecta derularea proiectului, prin schimbări care pot impune modificarea planurilor activităților/bugetului, ceea ce poate duce la întârzieri datorate reorganizărilor necesare pentru implementarea in continuare a proiectului. Măsurile de atenuare: • Prevederea unor intervale suplimentare de timp pentru reorganizarea activităților în funcție de schimbările apărute; • Departament juridic responsabil de monitorizarea legislației, procedura de conformitate legislativa; flexibilitatea organizațională, aplicarea procedurii de change management pentru orice astfel de schimbare; • Acte adiționale care vor reflecta schimbările impuse de modificările legislative;
5.	Planificarea nerealista a resurselor de care este nevoie Posibile consecințe: Prelungirea perioadei de implementare față	Impact: mare Probabilitate de apariție: medie Măsurile de atenuare:

Nr. crt.	Riscul identificat	Măsurile de atenuare a riscului
	de cea preconizată inițial; Întârzierile în finalizarea proiectului ar putea conduce la pierderi financiare;	• Metodologie de proiect corect stabilita; • Alocarea de fonduri proprii pentru achiziția resurselor necesare in vederea îndeplinirii obiectivelor proiectului;
6.	Modificarea structurii de personal Posibile consecințe: Pot să apară întârzieri în realizarea activităților	Impact: mediu Probabilitate de apariție: medie Fluctuațiile de personal pot afecta derularea proiectului. Atragerea pe parcurs a unor persoane care să cunoască activitățile proiectului și să se familiarizeze cu acestea ar putea conduce la preluarea rapidă a responsabilităților, după caz. Măsurile de atenuare: • Pregătirea unor persoane care să poată prelua din responsabilitățile celor care au părăsit instituția; • Efectuarea unor schimbări de personal; • Realizarea unei biblioteci de documente de proiect, ce va facilita înțelegerea rapidă a contextului de către persoanele implicate în proiecte pe parcursul desfășurării acestuia;
7.	Gradul de încărcare prea mare al persoanelor din echipa de proiect Posibile consecințe: Întârzieri sau calitate necorespunzătoare a rezultatelor preconizate	Impact: mare Probabilitate de apariție: medie Antrenarea unor angajați care să participe la activitățile proiectului Măsurile de atenuare: • Gestionarea corespunzătoare a timpilor de lucru
8.	Depășirea bugetului prevăzut în proiect Posibile consecințe: Duratele prevăzute pentru derularea diverselor etape ale proiectului sau modificările cerințelor, întârzierile în proiect pot conduce la situația în care costurile prevăzute în proiect să fie depășite fapt care ar putea produce întârzieri in implementare	Impact: mare Probabilitate de apariție: mică Măsurile de atenuare: • Respectarea termenelor prevăzute în proiect, prin desfășurarea adecvată a proceselor de monitorizare și control impuse de metodologiile de management al proiectului.
9.	Lipsa comunicării eficiente in cadrul echipei	Impact: mic/mediu

Nr. crt.	Riscul identificat	Măsurile de atenuare a riscului
	de proiect Posibile consecințe: Lipsa comunicării eficiente poate produce întârzieri in proiect, sau crea cerințe neclare si/sau incomplete	Probabilitate de apariție: mica/medie Măsurile de atenuare: • Realizare și respectare plan de comunicare • Realizarea unui plan de ședințe periodice • Stabilire responsabilități clare a membrilor echipelor de proiect
10.	Întârzieri în verificarea și avizarea de către Autoritatea Contractantă a variațiilor decizionale Posibile consecințe: Pot să apară întârzieri în realizarea activităților	Impact: mare Probabilitate de apariție: mare Măsurile de atenuare: • Minimizare risc (pregătirea tuturor informațiilor necesare pentru luare unei decizii rapide și corecte).
11.	Întârzieri rezultate la stabilirea unor decizii pe parcursul derulării procedurilor de atribuire (contestații, clarificări solicitate asupra anumitor aspecte ale ofertelor etc.); Posibile consecințe: Pot să apară întârzieri în realizarea activităților	Impact: mare Probabilitate de apariție: medie Măsurile de atenuare: • Prin planul de proiect realizat de Consultant se vor descrie circumstanțele luării deciziilor decisive si impactul acestora
12.	Propunerea unei soluții tehnice diferite față de cea descrisă in proiectul inițial Posibile consecințe: Pot să apară întârzieri în realizarea activităților Poate fi reziliat contractul de finanțare	Impact: mare Probabilitate de apariție: mica Măsurile de atenuare: • Selectarea atentă de specialiști IT cu experiență vastă în domeniile proiectului • Planificarea unui număr suficient de variante intermediare pentru soluțiile tehnice astfel încât orice abatere de la obiectivele proiectului să fie identificată din timp și eliminată înainte de a se propaga în cadrul soluțiilor tehnice propuse • Implicarea experților ITC în alegerea soluției tehnice; Definirea clară a specificațiilor tehnice introduse în documentația de atribuire și impunerea unor condiții contractuale clare • Analizarea împreună cu Beneficiarul a oportunității de modificare a soluției tehnice, prin încheierea unui act adițional la

Nr. crt.	Riscul identificat	Măsurile de atenuare a riscului
		contractul de finanțare
13.	Dificultăți de colaborare și comunicare intre factorii interesați implicați (inclusiv personal insuficient sau diferențe de înțelegere a noțiunilor din caietul de sarcini)	• Se va urmări in mod continuu fluxul de comunicare între personalul Autorității Contractante și a Prestatorului. • Atât Autoritatea Contractantă cât și Prestatorului vor avea permanent in vedere o lista de rezerva a personalului responsabil cu implementarea proiectului.
14.	Datele și informațiile necesare desfășurării serviciilor, comunicate de către autoritatea contractantă, nu sunt suficiente pentru îndeplinirea cerințelor solicitate prin Caietul de Sarcini la nivelul de calitate așteptat;	Impact: mare Probabilitate de apariție: medie Măsurile de atenuare: • Managerul de proiect al Autorității Contractante va monitoriza continu fluxul de lucru, cu scopul de a remedia deficientele, sau, după caz va suplimenta cu informații necesare pentru îndeplinirea cerințelor solicitate prin Caietul de Sarcini la nivelul de calitate așteptat, conform graficului de prestare a activităților.
15.	Apariția necesității de adăugare a unor activități/ solicitări de informații noi, in funcție de progresul activităților.	Impact: mare Probabilitate de apariție: medie Măsurile de atenuare: • alocarea de personal instruit care sa răspundă conform termenelor asumate prin caietul de sarcini; • asumarea responsabilității pe calitatea datelor puse la dispoziție; • consecințele unor solicitări de modificare făcute de către autoritatea contractantă.

Ofertantul va identifica și alte riscuri față de cele principale, relevate mai sus, în special riscuri de natură tehnică specifice soluției ofertate.

În cadrul ofertei sale, Ofertantul va prezenta obligatoriu comentarii și puncte de vedere cu privire la toate riscurile, va prezenta modul în care își va organiza activitatea și strategiile pe care le va utiliza pentru a realiza gestiunea acestor riscuri și va identifica alte riscuri pe care le consideră relevante din punctul său de vedere, inclusiv riscuri aferente organizării și soluției tehnice propuse, riscuri pentru care va realiza analiza impactului și va identifica măsurile optime de gestiune și responsabilitatea gestiunii acestora. Analiza riscurilor va include o componentă cantitativă (listă de riscuri, măsuri de prevedere/planificare, măsuri corective, măsuri de rezervă) și una calitativă

(evaluarea probabilității și a impactului).

5.3 Indicatori de performanță

Indicatorii de performanță stabiliți pentru activitățile proiectului prin raportare la cerințele din Caietul de Sarcini și clauzele din Contract:

Tabel 6 - Indicatori de performanță

Indicator de performanță	Nivelul de performanță așteptat (conform contract / Caiet de Sarcini)	Ce se măsoară	Modalitate de evaluare	Scop
Raportul de analiză și proiectare detaliat complet și adecvat pentru scopul utilizării	Raportul este livrat conform cerințelor stabilite în Caietul de Sarcini	Nivelul de acuratețe al raportului livrat după o "evaluare reciprocă" (pondere informații inexacte / sub nivelul de calitate agreat în informațiile furnizate)	Excelentă (5 puncte) – Raportul livrat include îmbunătățiri semnificative față de cerințele minime stabilite în Caietul de Sarcini în special prin luarea în considerare a noilor tendințe din industrie. Documentația a fost folosită pentru etapa următoare așa cum a fost prezentată. Foarte bună (4 puncte) – Raportul livrat include unele îmbunătățiri și nu include neconformități/inexactități față de nivelul agreat. Documentația a fost folosită pentru etapa următoare așa cum a fost prezentată. Au fost necesare doar ajustări nemateriale. Bună (3 puncte) - Raportul livrat nu include neconformități/inexactități față de nivelul agreat însă nu include nici elemente suplimentare care să aducă o valoare adăugată semnificativă proiectului. Raportul a putut fi folosit pentru etapa următoare după ce a fost corectat de câteva ori.	Evaluarea completitudinii aplicabilității și relevanței raportului de analiză detaliată

Indicator de performanță	Nivelul de performanță așteptat (conform contract / Caiet de Sarcini)	Ce se măsoară	Modalitate de evaluare	Scop
			Nu au existat întârzieri semnificative ca urmare a corecturilor. Satisfăcătoare (2 puncte) – Raportul transmis a inclus neconformități / inexactități față de nivelul agreat sau a folosit tehnologii/metode complet învechite care erau în principal abandonate de industrie, iar aceste aspecte nu au putut fi corectate în totalitate într-o perioadă rezonabilă (ex. au cauzat întârzieri semnificative în realizarea activităților din calendarul general al proiectului), dar cu toate acestea au fost corectate, fără costuri suplimentare pentru Autoritatea Contractantă. Nesatisfăcătoare (1 punct) – Raportul livrat a inclus neconformități / inexactități majore față de nivelul agreat sau a folosit tehnologii/metode complet învechite care erau, în principal, abandonate de industrie, iar aceste aspecte nu au putut fi corectate. Autoritatea Contractantă a trebuit să mobilizeze alte resurse pentru a remedia problemele, ceea ce a condus la costuri suplimentare semnificative pentru Autoritatea Contractantă și/sau a cauzat întârzieri semnificative în realizarea activităților din	

Indicator de performanță	Nivelul de performanță așteptat (conform contract / Caiet de Sarcini)	Ce se măsoară	Modalitate de evaluare	Scop
			calendarul general al proiectului.	
Livrabil adecvat pentru scopul utilizării	Aplicația este dezvoltată și implementată conform cu specificațiile, inclusiv din punct de vedere al migrării datelor	Nivelul de corelare între cerințele pentru aplicație și implementarea lor în aplicația finală, inclusiv cu privire la migrarea datelor	**Excelentă(5 puncte)** - Aplicația livrată a inclus toate cerințele din caietul de sarcini. Acestea au fost implementate într-un mod eficient și a adus îmbunătățiri semnificative față de cerințele minime stabilite în Caietul de Sarcini în special prin luarea în considerare a noilor tendințe din industrie. Datele au fost migrate complet și corect. Aplicația a fost folosită în producție așa cum a fost prezentată. **Foarte bună (4 puncte)** - Aplicația livrată a inclus toate cerințele din Caietul de sarcini. Acestea au adus unele îmbunătățiri față de cerințele minime stabilite în Caietul de Sarcini. Datele au fost migrate complet și corect. Aplicația a fost folosită în producție așa cum a fost prezentată. **Bună (3 puncte)** - Aplicația livrată nu include neconformități/inexactități față de cerințele din caietul de sarcini însă nu include nici elemente suplimentare care să aducă o valoare adăugată semnificativă proiectului. Datele au fost migrate complet și corect după mici ajustări. Aplicația a putut fi folosită după ce au fost necesare câteva runde de	Evaluarea conformității aplicației implementate cu specificațiile

Indicator de performanță	Nivelul de performanță așteptat (conform contract / Caiet de Sarcini)	Ce se măsoară	Modalitate de evaluare	Scop
			ajustări, dar acestea nu au generat întârzieri semnificative. **Satisfăcătoare (2 puncte)** - Aplicația livrată a inclus neconformități/inexactități semnificative față de cerințele din caietul de sarcini sau a folosit tehnologii/metode complet învechite care erau în principal abandonate de industrie, iar aceste aspecte nu au putut fi corectate în totalitate într-o perioadă rezonabilă (ex. au cauzat întârzieri semnificative în realizarea activităților din calendarul general al proiectului), dar cu toate acestea au fost corectate de către Prestator, fără costuri suplimentare pentru Autoritatea Contractantă. Datele nu au fost migrate complet sau corect decât după reluarea procesului, dar au putut fi migrate corect și complet fără costuri suplimentare pentru Autoritatea Contractantă. **Nesatisfăcătoare (1 punct)** - Aplicația livrată a inclus neconformități/inexactități majore față de cerințele din caietul de sarcini sau a folosit tehnologii/metode complet învechite care erau în principal abandonate de industrie sau datele nu au fost migrate corect sau complet, iar aceste aspecte nu au putut fi corectate de	

Indicator de performanță	Nivelul de performanță așteptat (conform contract / Caiet de Sarcini)	Ce se măsoară	Modalitate de evaluare	Scop
			către Prestator, fără costuri suplimentare pentru Autoritatea Contractantă. Autoritatea Contractantă a trebuit să mobilizeze alte resurse pentru a remedia problemele, ceea ce a condus la costuri suplimentare semnificative pentru Autoritatea Contractantă și/sau a cauzat întârzieri semnificative în realizarea activităților din calendarul general al proiectului.	
Livrabile intermediare și finale predate în termenul agreat	Fără depășiri de termene și fără reveniri asupra acceptanțelor	Livrarea la timp și conform parametrilor specificați a rezultatelor	**Excelentă (5 puncte)** - Livrabilele au fost furnizate în termenele convenite în contract **Foarte bună (4 puncte)** - Livrabilele au fost furnizate imediat după încheierea termenelor convenite în Contract însă fără întârzierea activităților din calendarul general al proiectului **Bună (3 puncte)** - Livrabilele au fost furnizate după încheierea termenelor convenite în Contract conducând la întârzieri ale activităților din calendarul general al proiectului ce pot fi neglijate **Satisfăcătoare (2 puncte)** - Livrabilele au fost furnizate cu mult după încheierea termenelor convenite în Contract conducând la întârzieri ale activităților din	**Evaluarea eficientei managementului de proiect prin finalizarea la timp a punerii în funcțiune a aplicației**

Indicator de performanță	Nivelul de performanță așteptat (conform contract / Caiet de Sarcini)	Ce se măsoară	Modalitate de evaluare	Scop
			calendarul general al proiectului (mai mult de 60 de zile) **Nesatisfăcătoare (1 puncte)** - Livrabilele au fost furnizate cu mult după încheierea termenelor convenite în Contract conducând la întârzieri majore ale activităților din calendarul general al proiectului (mai mult de 120 de zile)	

6 Abordare și metodologie în cadrul contractului

Agenția Națională pentru Sport dorește implementarea unei platforme de servicii publice digitale care să schimbe informații în mod nativ între diversele componente care urmează să fie implementate și soluțiile existente în acest moment în cadrul instituției.

Se vor furniza soluții software existente pe piață, de tip **COTS (Commercial Off-The-Shelf)**, cu excepția cazului în care Caietul de sarcini prevede în mod explicit altfel. Aceste soluții vor fi instalate, configurate, personalizate și, după caz, dezvoltate în cadrul proiectului, astfel încât să permită implementarea integrală a aplicațiilor și funcționalităților solicitate prin Caietul de sarcini.

Toate licențele COTS ofertate vor avea caracter **perpetuu**, **nelimitat în timp** și **pentru un număr nelimitat de utilizatori**, cu excepția situațiilor în care, pentru o anumită licență, Caietul de sarcini prevede în mod explicit alte condiții.

Ofertanții vor preciza explicit în cadrul ofertelor numele produselor software ofertate.

Având în vedere faptul că strategia de implementare a proiectului implică achiziționarea unor platforme/soluții software standard, ale căror funcționalități standard de administrare vor fi utilizate in cadrul contractului pentru configurarea unor fluxuri de lucru specifice în funcție de specificul activității Beneficiarului, fapt ce necesită derularea unei etape de analiză/studiere proceduri interne/implementare proceduri de lucru, in cadrul scenariilor demonstrative se va verifica un set restrâns de funcționalități de bază ale platformelor software ofertate, care este obligatoriu să existe in platformele/soluțiile ofertate (platforme/soluții software standard de tip COTS), care vor fi configurate generic. Nu vor face obiectul în cadrul scenariilor demonstrative aspecte care țin de configurarea/dezvoltarea specifică a platformelor ofertate pentru Autoritatea Contractantă.

Pentru demonstrarea conformității propunerilor tehnice prezentate cu solicitările caietului de sarcini, ofertanții au obligația de a depune până la data și ora limită de depunere a ofertelor în anunțul de participare, o înregistrare audio-video a sesiunii demonstrative prin care vor prezenta modalitatea prin care soluțiile ofertate incluse în soluția tehnică răspund la funcționalitățile prezentate în scenariile care sunt detaliate în prezentul Caiet de sarcini.

Condiții de licențiere

Oferta tehnică și financiară va include toate licențele necesare pentru toate sub-sistemele și componentele software ofertate (aplicații software standard de tip COTS – commercial of-the-shelf), necesare funcționării în condiții normale, pe termen nedeterminat, a acestora.

Funcționarea platformelor software cu toate funcționalitățile solicitate prin Caietul de sarcini nu trebuie să implice costuri suplimentare de licențiere, ulterior acceptanței sistemului. Dacă nu este specificat altfel în cadrul secțiunilor aferente specificațiilor detaliate pentru componentele software, licențierea software-ului de aplicație ofertat va fi de tip perpetuu, irevocabil și nelimitat în timp pentru număr nelimitat de utilizatori dacă în Caietul de sarcini nu se prevede altfel pentru o anume licență.

În vederea asigurării continuității soluției și independentei Beneficiarului fata de Prestator, se va avea în vedere respectarea următoarelor aspecte:

- Pentru toate aplicațiile customizate/configurate/dezvoltate specific pentru Beneficiar va fi livrat inclusiv codul sursă și documentația aferentă conform Art.12 din OUG 41/2016. Codurile sursă vor fi livrate în format editabil / prelucrabil;
- Drepturile de autor asupra soluțiilor și aplicațiilor software dezvoltate specific pentru Beneficiar vor fi transferate integral și vor deveni proprietatea acestuia, la recepția sistemului;

6.1 Cadrul activităților

Pentru implementarea cu succes a proiectului TIC, Prestatorul va aloca o echipă proprie de coordonare și va utiliza o metodologie și unelte de management de proiect care să permită un proces eficient de planificare și monitorizare, un control eficient al riscurilor și management contractual. Astfel, Prestatorul va nominaliza un Manager de Proiect responsabil pe întreaga durată a implementării, care va asigura coordonarea tuturor activităților și va raporta periodic către echipa de management de proiect a Beneficiarului.

6.1.1 Localizarea proiectului

Proiectul se va implementa la sediul al ANS, situat în Str. Vasile Conta, Nr.16, Sector 2, Municipiul București, București, Cod poștal 020954, reprezentând locația principală pentru activitățile de analiză, proiectare, dezvoltare, instruire testare și recepție.

Soluția TIC dezvoltată va deservi întreg ecosistemul sportiv la nivel național, indiferent de locația fizică a implementării.

6.1.2 Durata de implementare a proiectului TIC

Durata de implementare a proiectului TIC: **24 luni**

Se vor avea în vedere următoarele termene maximale pentru finalizarea activităților de implementare:

- Livrare si preluare echipamente hardware - 3 luni (L1-L3), incluzând minimum 7 zile lucrătoare pentru recepția calitativă.
- Analiza fluxurilor de activitate din cadrul ANS și Proiectarea sistemului – 8 luni (L1-L8), , incluzând minimum 7 zile lucrătoare pentru recepția livrabilelor.
- Dezvoltare soluție TIC integrată și testare internă Prestator – 13 luni (L1-l13), , incluzând minimum 7 zile lucrătoare pentru recepția livrabilelor.
- Implementarea măsurilor de securitate cibernetică - 8 luni (L8-L15), incluzând minimum 7 zile lucrătoare pentru recepția livrabilelor.
- Implementare sistem integrat - 8 luni (L13-L20), incluzând minimum 7 zile lucrătoare pentru recepția livrabilelor.
- Testare finală – 6 luni (L19-L24), incluzând minimum 7 zile lucrătoare pentru recepția livrabilelor.
- Instruire administratori si utilizatori – 5 luni (L19-L23), incluzând minimum 7 zile lucrătoare pentru recepția livrabilelor.

Nerespectarea termenelor aferente etapelor și a recepțiilor de mai sus dă dreptul autorității contractante de a aplica penalități conform contractului.

În cazul în care, în urma recepției calitative, sunt formulate observații ce necesită completări sau corecții, etapa se consideră finalizată numai după predarea versiunilor finale, complete și conforme ale livrabilelor.

Ofertantul are obligația de a include în graficul de implementare:

- perioade suficiente pentru elaborarea livrabilelor,
- perioade pentru recepția calitativă (conform termenelor din caietul de sarcini),
- perioade pentru remedierea neconformităților,
- perioade pentru retestarea și reverificarea livrabilelor.

Autoritatea contractantă va avea la dispoziție:

- **minimum 2 zile lucrătoare** pentru retestarea/reverificarea unui livrabil pentru care a transmis observații,
- **minimum 3 zile lucrătoare** pentru verificarea documentelor uzuale,
- **maximum 5 zile lucrătoare** pentru verificarea documentelor complexe.

Termenele maximale pentru finalizarea etapelor includ:

- predarea versiunilor draft,
- predarea versiunilor finale,
- timpul de analiză al autorității contractante,
- timpul necesar prestatorului pentru remedierea neconformităților,
- timpul necesar autorității contractante pentru reverificare și recepție.

6.2 Servicii și livrabile specifice proiectului TIC

În cadrul procesului de implementare, lansare în producție și apoi garanție și suport se vor presta minimal următoarele servicii:

6.2.1 Livrare si preluare echipamente hardware

În cadrul acestei activități Prestatorul va livra, instala și pune în funcțiune echipamentele hardware furnizate în cadrul proiectului.

Prestatorul este responsabil în totalitate de livrarea produselor (hardware și de comunicații), respectiv activități legate de furnizarea produselor, cum ar fi: transportul, asigurarea, instalarea, punerea în funcțiune, asistență tehnică în perioada de garanție și orice alte asemenea obligații care revin acestuia prin contract.

Toate cheltuielile legate de activitățile echipelor de instalare vor fi suportate integral de Ofertant.

Pentru livrarea și implementarea infrastructurii hardware solicitate vor trebui asigurate următoarele activități:

- Livrarea echipamentelor;

- Servicii de livrare, etichetare, instalare și punere în funcțiune echipamentelor;
- Derularea activităților corespunzătoare recepției cantitative a echipamentelor;
- Derularea activităților corespunzătoare recepției calitative a echipamentelor;
- Livrarea documentației tehnice a echipamentelor recepționate.

Se vor efectua următoarele operații în vederea punerii în funcțiune a echipamentelor hardware:

- Transportul echipamentelor de către Prestator la sediul Beneficiarului în vederea instalării și punerii în funcțiune, respectând normele de transport impuse de către producător și de ambalare (în cazul în care echipamentele livrate nu sunt ambalate în ambalajul original);
- Instalarea fizică a echipamentelor la pozițiile de lucru indicate de Beneficiar (birouri, spații de lucru, zone administrative);
- Conectarea echipamentelor la rețeaua existentă (prin cablu sau Wi-Fi), în limitele infrastructurii puse la dispoziție de Beneficiar;
- Conectarea echipamentelor la sursele de electroalimentare;
- Interconectarea noilor echipamente cu sistemul de comunicații existent, daca este cazul;
- Configurarea conexiunii la rețea conform politicilor Beneficiarului (nume dispozitiv, domeniu, profil utilizator, politici de securitate);
- Inițializarea echipamentelor;
- Verificarea funcționării echipamentelor (pornire, conectivitate, funcționalitate periferice, imprimare/test scanare);
- Remedierea eventualelor neconformități constatate în timpul verificărilor;
- Marcarea cu etichete a fiecărui echipament conform cu procedura de etichetare agreată. Modul concret de realizare, inscripționare și fixare a etichetelor pe echipamente se va propune de către Prestator și se va accepta de către Autoritatea Contractantă după intrarea în vigoare a contractului, dar înainte de începerea instalării acestora.

Activitățile de instalare a produselor hardware se vor realiza de către reprezentanții Ofertantului sub supravegherea personalului Autorității Contractante.

Echipamentele trebuie livrate împreună cu toate accesoriile necesare punerii în funcțiune, chiar daca acestea nu au fost solicitate în mod explicit în caietul de sarcini, dar sunt necesare pentru operaționalizarea și integrarea echipamentelor în infrastructura existentă la Achizitor.

Livrabile:

- Avize de însoțire a mărfii
- Certificate de garanție și conformitate
- Raport de instalare și punere în funcțiune echipamente

6.2.2 Analiza fluxurilor de activitate din cadrul ANS și proiectarea sistemului

În cadrul acestei activități Prestatorul va identifica și adapta fluxurilor de lucru și procesele operaționale din cadrul ANS pentru integrarea soluțiilor digitale ce urmează a fi implementate.

Transformarea digitală impune ajustări în modul de desfășurare a activităților, optimizarea proceselor și redefinirea modului de interacțiune între structurile instituției și stakeholderi.

Procesul de analiză și adaptare a fluxurilor de activitate va include următoarele etape:

- Analiza specificului activității fiecăruia dintre entitățile/compartimentele vizate de proiect stabilirea modulului în care sistemul va fi implementat astfel încât să sprijine activitățile specifice ale acestora.
- Cartografierea fluxurilor de lucru actuale – documentarea proceselor existente la nivelul ANS și identificarea punctelor cheie în care digitalizarea va aduce îmbunătățiri. Identificarea etapelor critice supuse digitalizării – analiza proceselor care necesită transformare digitală și stabilirea priorităților pentru eficientizarea acestora.
- Evaluarea impactului soluțiilor digitale – determinarea modului în care noile tehnologii influențează procesele curente și ce ajustări sunt necesare pentru integrarea eficientă a acestora.
- Elaborarea unei strategii de tranziție – definirea pașilor pentru implementarea schimbărilor, astfel încât procesul de adaptare să fie fluent și să minimizeze impactul asupra activităților curente. Această activitate va asigura alinierea proceselor instituționale la cerințele impuse de digitalizare și va facilita implementarea eficientă a noilor tehnologii la nivelul sportului românesc. Analiza și documentarea fluxurilor adaptate va reprezenta un element esențial în integrarea soluțiilor digitale și în optimizarea performanței administrative a ANS.
- Documentarea modalității de configurare/customizare/integrare a sistemului informatic astfel încât acesta să sprijine în mod eficient desfășurarea activităților specifice ale utilizatorilor, precum și documentarea tipurilor de fluxuri de lucru care vor fi utilizate, cu pregătirea diagramelor de activități, indicarea modalității concrete de operare în sistemul informatic.

Raportul de analiză și proiectare va include lista completă a funcționalităților sistemului (plecând de la specificațiile caietului de sarcini, cu clarificările obținute în etapa de analiză) și detalierea grupurilor/rolurilor de utilizatori ai sistemului și a drepturilor acestora.

Ofertantul trebuie să descrie în detaliu metodologia după care va derula activitățile de analiză și proiectare. Ofertantul trebuie să descrie instrumentele pe care le vor utiliza în etapa de analiză și proiectare astfel încât să poată asigura:

- Colectarea și evidența cerințelor;
- Trasabilitatea cerințelor pornind de la obiectivele proiectului până la specificațiile tehnice pentru demonstrarea acoperirii integrale a tematicii proiectului;

Ofertantul trebuie să prezinte detaliat livrabilele care vor rezulta în urma prestării serviciilor corespunzătoare etapei de analiza și proiectare. Descrierea trebuie să conțină cel puțin următoarele informații:

- Formularul/formularele care vor fi utilizate pentru fiecare livrabil;
- Descrierea conținutului fiecărui livrabil;
- Modul în care va fi interpretat conținutul livrabilelor.

Serviciile de analiza și proiectare vor acoperi cel puțin următoarele aspecte:

- Analiza contextului existent;
- Înțelegerea structurii organizatorice a Achizitorului;
- Analiza situației din momentul de față din cadrul instituției Achizitorului prin ședințe de analiza, chestionare etc. Se vor identifica procesele operaționale (la nivelul instituției) care vor fi impactate prin implementarea soluției proiectului;
- Definirea cerințelor de configurare a noului sistem informatic;
- Stabilirea actorilor care vor interacționa în viitorul sistem.

Se vor evidenția activitățile care urmează a fi automatizate dacă este cazul, astfel încât să se identifice clar funcțiile viitorului sistem și modul în care acesta va ajuta la îndeplinirea obiectivelor proiectului.

Datele de intrare sunt:

- Contractul, pentru termene și condiții;
- Propunerea tehnică, pentru aria de acoperire a proiectului;
- Cerințele clientului colectate și evaluate în timpul acestei faze.

Livrabile:

Raport de analiză de business și proiectare ce va include cel puțin următoarele:

- fluxuri de lucru/procese specifice, cazuri de utilizare, surse și categorii de date, nomenclatoare, cerințe de configurare, integrare etc.);
- arhitectura de sistem și modul în care se propune configurarea componentelor de sistem astfel încât să se obțină funcționalitățile solicitate în proiectul tehnic și/sau identificate/detaliate în etapa de analiză – arhitectura hardware de rețea și securitate, software și funcțională;
- interfețe;
- module;
- funcționalități;
- specificații tehnice fluxuri; tipuri/categorii de formulare/template-uri care vor fi gestionate;
- model de date (logic și fizic);
- scenarii de testare funcțională si non-funcțională;
- specificații de securitate și de integrare.

6.2.3 Dezvoltare soluție TIC integrată

6.2.3.1 Livrare, instalare, punere în funcțiune software

În cadrul acestei activități Prestatorul va livra, instala și și configura software-ul furnizat în cadrul proiectului.

Prestatorul este responsabil de livrarea, instalarea infrastructurii software de sistem.

Activitățile de instalare și configurare a software-ului se vor realiza de către reprezentanții Ofertantului sub supravegherea personalului Autorității Contractante.

Livrabile:

- Kituri de instalare și chei de acces (unde este cazul)
- Certificate de garanție și conformitate (unde este cazul)
- Documentație tehnică
- Raport de instalare, configurare și testare a componentelor software, ce va conține obligatoriu:
    - Tabel cu produsele software livrate și instalate
    - Tabel cu mașinile virtuale configurate
    - Descrierea modului de instalare a fiecărei componente software
    - Lista de verificare a instalării și configurării preliminare a componentelor software (scenarii de testare și raport de testare)

6.2.3.2 Dezvoltare soluție TIC integrată

În cadrul acestei etape se vor realiza serviciile de dezvoltare și integrare ale platformei informatice.

Prestatalul va avea în vedere dezvoltarea și integrarea componentelor/modulelor soluției software integrate după cum urmează: Portal Public ANS, Modul Registratură – management documente, Modul registrul Sportiv – Federații și Cluburi, Modul Registrul Sportivilor și Antrenorilor, Modul Registrul Bazelor Sportive, Modul Anuarul Sportului, Modul Galeria Marilor Sportivi, Modul CNFPA, Modul Arhiva, Modul Administrativ, Chatbot/Asistent Virtual, Rapoarte Business Intelligence.

Având ca referință documentele rezultate în etapa analiză și proiectare, Prestatorul va dezvolta și asambla componentele software într-un sistem integrat, conform cu specificațiile de analiză și proiectare.

Produsele livrate vor fi instalate în locația indicată de Autoritatea Contractantă, în infrastructura menționată în cadrul Caietului de sarcini (CGP și echipamente achiziționate în cadrul proiectului), după care se vor realiza dezvoltările/configurările/integrările necesare pentru îndeplinirea în totalitate a cerințelor caietului de sarcini detaliate și documentate sub forma unor proceduri de instalare, configurare și integrare pentru toate componentele livrate în cadrul proiectului.

Se vor implementa fluxurile electronice de lucru prin derularea următoarelor activități:

- se vor defini metadatele generale ale fluxurilor electronice;
- se vor defini seturi de activități și condiții specifice proceselor și metadatelor asociate;
- se vor configura seturile de decizii cu opțiune pentru semnătura digitală;

Se va finaliza procesul iterativ de rafinare a componentelor configurate/customizate pentru satisfacerea cerințelor funcționale, integrarea și documentarea tuturor componentelor soluției, instalarea aplicație informatice integrate și integrarea în sistem a arhivei digitale.

Această etapă se va finaliza cu activitățile de testare internă derulate de Prestator, atât la nivel de componente cât și la nivelul sistemului integrat.

Livrabile:

- Raport de dezvoltare/configurare/customizare
- Raport de testare internă
- Cod sursă
- Documentație tehnică
- Documentație de utilizare
- Release notes

6.2.4 Implementarea măsurilor de securitate cibernetică

Această activitate are ca obiectiv implementarea măsurilor tehnice de securitate cibernetică în cadrul soluției TIC, în vederea asigurării funcționării în condiții de siguranță și a respectării cerințelor tehnice stabilite de Beneficiar.

Prestatorul va implementa exclusiv măsurile tehnice de securitate aferente soluției TIC, conform cerințelor din prezentul caiet de sarcini și în strânsă legătură cu documentațiile și cerințele transmise de consultanții externi ai Beneficiarului.

1. **Implementarea mecanismelor de autentificare și control al accesului:**

Prestatorul va implementa următoarele măsuri tehnice:

- mecanisme de autentificare multi-factor (MFA);
- gestionarea drepturilor de acces pe baza rolurilor (RBAC);
- politici tehnice de parole și sesiuni;
- auditarea și jurnalizarea accesului utilizatorilor;
- configurarea restricțiilor de acces la nivel de aplicație și API.

2. **Criptarea și protecția datelor:**

Prestatorul va implementa:

- criptarea datelor în tranzit (TLS 1.2/1.3);
- criptarea datelor în repaus la nivelul bazelor de date și al fișierelor;
- mecanisme de protecție împotriva accesului neautorizat la date;
- gestionarea cheilor de criptare conform politicilor Beneficiarului.

3. **Analiza de risc, definirea politicilor de securitate, testele de penetrare și auditul tehnic**

- Analiza de risc, definirea politicilor de securitate, testele de penetrare (black box și white box) și auditul tehnic nu fac parte din prezentul contract și sunt realizate în cadrul unor achiziții separate derulate de Autoritatea Contractantă.
- Prestatorul va colabora cu consultanții externi ai Beneficiarului pentru implementarea măsurilor tehnice rezultate din documentațiile elaborate în cadrul acestor achiziții, asigurând integrarea corespunzătoare a cerințelor de securitate în soluția TIC.

4. **Monitorizarea și detectarea proactivă a amenințărilor**:

Prestatorul va asigura:

- **Implementarea unei soluții SIEM** (Security Information and Event Management) pentru monitorizarea în timp real a activităților suspecte și asigurarea unui răspuns rapid la incidente.
- **Integrarea sistemelor de protecție împotriva atacurilor cibernetice**, inclusiv DDoS, malware, phishing și alte tipuri de amenințări.
- **Continuitatea activității și recuperării în caz de dezastru**, prin dezvoltarea și implementarea planurilor de backup și recuperare a datelor, pentru minimizarea impactului incidentelor asupra funcționării platformei.

5. Teste de penetrare și audit tehnic

- Prestatorul va pune la dispoziție soluția livrată, în forma complet integrată, pentru efectuarea testelor de penetrare (black box și white box) și a auditului tehnic, realizate de terțe părți contractate de Autoritatea Contractantă prin proceduri separate de achiziție.
- Prestatorul va asigura, fără costuri suplimentare, toate elementele necesare desfășurării acestor activități, incluzând, dar fără a se limita la: acces la mediile de test și producție (după caz); conturi dedicate; documentație tehnică; -arhitectură și diagrame; cod sursă (acolo unde este aplicabil); suport tehnic pe durata derulării testelor și auditului. Rezultatele testelor vor fi documentate, iar vulnerabilitățile identificate vor fi remediate și retestate.
- Recepția finală a soluției se va realiza numai după remedierea integrală a tuturor vulnerabilităților, neconformităților sau deficiențelor identificate în cadrul testelor de penetrare și al auditului tehnic, confirmarea remedierii fiind realizată de entitatea terță care a efectuat verificările.

Livrabile:

- Documentația privind mecanismele de autentificare și control al accesului
- Documentația privind criptarea și protecția datelor
- Documentația soluției SIEM
- Planul de continuitate a activității și planul de recuperare în caz de dezastru

6.2.5 Implementarea sistemului integrat

Această activitate are ca obiectiv configurarea, personalizarea și integrarea soluției TIC, **se va face fazat in următoarea ordine**:

- Faza 1 – Implementarea și adoptarea soluției la nivelul ANS
- Faza 2 – Implementarea și adoptarea soluției la nivelul Federațiilor Sportive
- Faza 3 – Implementarea și adoptarea soluției la nivelul Cluburilor Sportive
- Faza 4 – Implementarea și adoptarea soluției la nivelul Sportivilor
- Faza 5 – Implementarea și adoptarea soluției la nivelul altor structuri sportive

Pentru fiecare fază, Prestatorul va realiza configurările și personalizările necesare pentru a asigura o adaptare optimă la nevoile specifice ale utilizatorilor platformei.

Faza de implementare va preceda testarea și simularea platformei integrate.

Livrabile:

- Planul de implementare etapizată
- Configurările și personalizările soluției TIC
- Rapoarte de implementare pe fiecare fază
- Documentația de integrare a sistemului
- Mediul de testare și simulare
- Manuale și ghiduri pentru utilizatori și administratori
- Plan de adoptare a soluției

6.2.6 Testarea platformei digitale

Testarea platformei digitale este un proces esențial pentru asigurarea funcționalității, performanței și conformității acesteia cu cerințele stabilite.

Această etapă va include verificarea corectitudinii implementării funcționalităților, evaluarea interoperabilității între module, testarea timpilor de răspuns și identificarea eventualelor erori sau neconformități.

Procesul de testare va acoperi atât scenarii uzuale de utilizare, cât și situații extreme, pentru a evalua rezistența platformei la sarcini mari și posibile disfuncționalități. Vor fi utilizate metode de testare automată și manuală, pentru a garanta funcționalitatea optimă a sistemului.

Testarea va include, de asemenea, verificarea conformității cu cerințele de accesibilitate, securitate și protecția datelor, precum și desfășurarea de sesiuni de testare de tip User Acceptance Test (UAT) cu utilizatorii finali. Aceștia vor evalua platforma din perspectiva experienței de utilizare și vor oferi feedback pentru îmbunătățiri suplimentare. În funcție de rezultatele testelor, vor fi efectuate ajustări și optimizări pentru a garanta integrarea eficientă a soluției digitale în fluxurile de lucru ale ANS.

Testarea sistemului livrat se va realiza de către Prestator împreună cu reprezentanții beneficiarului utilizând scenarii de testare agreate în prealabil în vederea validării modalității corecte de implementare a funcționalităților solicitate.

După finalizarea testării funcționale și a UAT, Prestatorul va realiza o testare de penetrare de tip greybox asupra întregului sistem, în vederea identificării vulnerabilităților de securitate și

a validării configurărilor aplicației și infrastructurii. Prestatorul va remedia toate vulnerabilitățile identificate înainte de transmiterea sistemului către auditul extern.

Întregul sistem informatic va fi supus, înainte de recepția finală, testării de către Consultanti externi, prin efectuarea de audituri tehnice, teste de penetrare (black box și white box) și simulări de atacuri, pentru a valida eficiența măsurilor implementate. Prestatorul are obligația de a remedia integral neconformitățile identificate de aceștia înainte de recepția finală.

Este necesar ca Prestatorul să planifice, să pregătească și să efectueze toate testele necesare pentru confirmarea îndeplinirii cerințelor funcționale și non-funcționale, precum și a compatibilității sistemului cu specificațiile de interfațare cu sistemele externe.

6.2.6.1 Testarea

În cadrul propunerii tehnice Ofertantul trebuie să prezinte:

- Modalitatea în care va realiza testarea infrastructurii hardware și software de sistem
- Modalitatea în care se va realiza testarea sistemului informatic și testele de acceptanță specifice;
- Metodologia de testare după care se vor realiza activitățile de testare în timpul desfășurării contractului, inclusiv cea pentru testarea funcțională, testarea de performanță și securitate;
- Instrumentele de testare folosite;
- Livrabilul/livrabilele rezultate și formularul/formularele care vor fi utilizate;

Beneficiarul (cu asistența Prestatorului) va rula toate scenariile pentru testele de acceptanță ale întregului sistem (infrastructură hardware, software de bază, sistem informatic) sau componente livrate.

Ofertantul va include în planul de testare metodologia de testare a corectitudinii și consistenței datelor migrate, iar pe parcursul derulării testelor de acceptanță va derula procedurile de migrare a informațiilor, dacă este cazul.

În cadrul testării de acceptanță se vor efectua teste de performanță cel puțin pentru a demonstra capabilitățile sistemului de a susține numărul de utilizatori solicitați în Caietul de sarcini și performanțele de accesare/răspuns a sistemului definite în analiză și proiectare.

Planul de testare pentru acceptanță va cuprinde toate testele necesare pentru a demonstra acoperirea în întregime a cerințelor din prezentul proiect tehnic.

Astfel, se va avea în vedere faptul că infrastructura hardware și software, precum și sistemul informatic funcționează corect din punct de vedere al respectării cerințelor, consistenței datelor, al constrângerilor de timp, al validărilor de date și al gestiunii erorilor, inclusiv pentru funcționalitățile existente care au fost extinse sau modificate. Criteriul de succes – sistemul trece toate testele definite în planul de testare agreat împreună cu Beneficiarul.

Planurile de testare trebuie să includă cel puțin următoarele elemente:

- descrierea componentei de sistem testat
- obiectivele de testare

- descrierea mediului de testare
- rezultatele așteptate ale testului
- test de abordare
- datele de test
- descrierea procedurilor de test
- cazuri de testare
- instrumente folosite de testare
- persoanele responsabile
- cerințe de intrare / ieșire

Prestatorul trebuie să precizeze toate instrumentele de testare (aplicații, scripturi, etc), destinate a fi utilizate în timpul procedurilor de testare, dacă este cazul. Prestatorul trebuie să furnizeze instrumentele de testare, dacă este cazul. Toate rezultatele testelor trebuie înregistrate și furnizate Beneficiarului după fiecare test.

Coordonarea testelor - Testele vor fi coordonate de către Beneficiar/Utilizatori, care vor revizui și aproba planul și specificațiile de testare înainte de execuția efectivă a testelor, vor controla că mediul de testare e conform cu cerințele, vor monitoriza efectuarea testelor și se vor asigura de aplicarea procedurilor de management ale testării.

Livrabile:

- Plan și documentație de testare
- Rapoarte de testare

6.2.6.2 Asigurarea Calității

- Prestatorul trebuie să prezinte un plan pentru Asigurarea Calității acceptabil pentru Beneficiar, ca parte a planului de proiect;
- Prestatorul trebuie să aloce timp suficient, în cadrul planului de proiect, pentru verificare și validare în termeni de calitate, pentru serviciile prestate în cadrul contractului și pentru livrabilele/documentele/rapoartele rezultate;
- Prestatorul va elabora procedurile standard de operare pentru toate aplicațiile livrate, cu instrucțiuni detaliate pentru sprijinirea angajaților în diferite procese de lucru;
- Prestatorul va pune la dispoziție manuale, documentații, proceduri complete privind concepția, implementarea si administrarea in integralitate a sistemului informatic;

Livrabile:

- Plan de asigurare a calității

6.2.7 Instruirea personalului

Scopul instruirii

Pentru a asigura o tranziție eficientă și o utilizare optimă a soluțiilor informatice livrate, personalul ANS va beneficia de sesiuni de pregătire specializate. Aceste sesiuni vor include instruiri detaliate

privind utilizarea și administrarea platformei digitale dezvoltate prin proiect, astfel încât personalul să poată opera în condiții de siguranță și eficiență noile tehnologii.

În urma instruirii, personalul ANS va putea asigura nivelul 1 de suport, redirecționând către furnizorii de servicii aferenți (software, hardware, rețea etc.) problemele care depășesc acest nivel.

Prestatorul va asigura instruirea unui număr de 130 persoane din cadrul ANS, prin module separate pentru utilizatori și administratori. Managementul instituției va fi instruit în utilizarea aplicației pentru obținerea analizelor și rapoartelor de tip managerial. De asemenea, utilizatorii vor beneficia de instruire de bază în domeniul IT, tip ECDL.

Categorii de instruire

Instruirea se va realiza în cadrul a trei categorii de cursuri specifice:

- Instruire competențe digitale de bază;
- Instruire utilizatori platformă informatică integrată;
- Instruire administratori platforma informatică integrată.

Obiectivele instruirii

- instruirea de bază în domeniul IT, tip ECDL;
- cunoașterea sistemului integrat în ansamblul său;
- învățarea modului de operare a funcționalităților sistemului;
- învățarea modului de rezolvare a problemelor curente;
- învățarea modului de administrare a componentelor sistemului;
- instruirea pentru conștientizarea securității utilizatorilor;
- înțelegerea implicațiilor sistemului propus și a avantajelor acestuia.

Evaluarea participanților

La finalul cursului, participanții vor fi evaluați prin teste grilă care acoperă întregul conținut al instruirii. Răspunsurile corecte vor fi comunicate la final, urmate de discuții și clarificări.

Evaluarea generală și certificarea participanților se vor baza pe:

- rezultatul testului
- implicarea activă pe durata instruirii

Participanții vor primi **certificat de participare** sau **certificat de absolvire**, în funcție de rezultatele evaluării.

La finalul sesiunilor, Prestatorul va întocmi un **Raport de instruire** pentru fiecare sesiune.

Cerințe transversale obligatorii

Sesiunile de instruire vor respecta cerințele Ghidului solicitantului, Contractului de finanțare, prevederile Manualul de Identitate Vizuala si regulile interne ale ANS, și vor include:

- o secțiune privind dezvoltarea durabila - masuri privind importanta protecției mediului si dezvoltării durabile, problemele de mediu si tema schimbărilor climatice,
- o secțiune cu privire la egalitatea de șanse si nediscriminarea si egalitatea de gen - masuri privind promovarea egalității de șanse intre femei si bărbați, a egalității de șanse pentru toți, fără discriminare in funcție de gen, rasa, origine etnica, religie, handicap, vârsta, orientare sexuală.

Fiecare sesiune va fi susținută de 2 traineri formatori, certificați de către producătorul soluțiilor informatice ofertate.

Ofertanții vor include în propunerea tehnică **metodologia de instruire**, **programa și planul de formare** (calendar) propus pentru atingerea obiectivului activității.

Livrabile:

- Plan de instruire;
- Materiale de instruire utilizatori soluție;
- Materiale de instruire administratori soluție ;
- Raport de instruire:
  - Liste de prezență,
  - Chestionare de evaluare a cursului,
  - Chestionare de testare și evaluare cunoștințe,
  - Lista de înmânare a certificatelor de participare,
  - Certificate de participare cursanți.

Notă:

- Lista livrabilelor nu este limitativă;
- Beneficiarul va aproba fiecare document în parte, având dreptul de a solicita completări sau, acolo unde este justificat, noi documente.

Prestatorul va furniza sesiuni de instruire conform cerințelor detaliate mai jos:

6.2.7.1 Instruire competențe digitale de bază

Această instruire este destinată personalului ANS, în vederea formării competențelor digitale de bază, în conformitate cu standarde recunoscute la nivel european (ex.: ICDL/ECDL, IC3, DigComp sau echivalent).

Cursul trebuie:

- să fie furnizat de un furnizor autorizat conform legislației în vigoare (Autoritatea Națională pentru Calificări sau organisme echivalente);
- să aibă programa aliniată la standarde recunoscute (ICDL/ECDL, IC3, DigComp sau echivalent).

Structura programului:

- Grup țintă **- 130 persoane**

Organizare:

- Sesiunile de instruire se vor desfășura în sistem online, prin intermediul unei platforme de învățare (e-Learning);
- Suportul de curs va fi disponibil în format electronic;
- Instruirea se va realiza în limba română.
- Participanții vor primi certificate de absolvire și/sau certificări recunoscute, emise de furnizor sau de organisme acreditate, care atestă competențele dobândite.

6.2.7.2 Instruire utilizatori platformă informatică integrată

Această instruire este destinată utilizatorilor sistemului și se va desfășura după finalizarea testării funcționale.

Managementul instituției va fi instruit pentru utilizarea aplicației în vederea generării și interpretării analizelor și rapoartelor de tip managerial.

Conținut minim:

- Prezentarea sistemului, a modulelor și funcționalităților generale;
- Autentificare, roluri și drepturi;
- Utilizarea fiecărui modul funcțional;
- Utilizarea aplicației în vederea obținerii de analize de tip managerial;
- Utilizarea documentației tehnice și modalitatea de solicitare a suportului tehnic.

Structura programului:

- utilizatori finali - **110 persoane**
  - grupă: max. 20 persoane
  - durată: 3 zile
- Management instituție - **15 persoane**
  - grupă: max. 15 persoane
  - durată: 3 zile

Organizare:

- Achizitorul va asigura următoarele resurse:
  - sală de curs;
  - telecomunicații;
  - stații de lucru/laptopuri;
- Prestatorul va asigura următoarele resurse:
  - mediul de s identic cu mediul de producție
  - date de test semnificative
  - Suportul de curs în format electronic

- Instruirea se va realiza în limba română.
- Participanții vor primi certificate, emise de furnizorul instruirii, care atestă competențele de dobândite.

6.2.7.3 Instruirea administratorilor

Această instruire este destinată administratorilor platformei (personalului tehnic.

Conținut minim:

- Administrarea platformei software și cloud;
- Back-up și recuperare date;
- Administrare și configurare soluție;
- Securitate sistem;
- Modalități de asigurare suport tehnic.

Instruirea va avea caracter practic, bazat pe studii de caz și exerciții.

Prestatorul va furniza și procedurile necesare întreținerii sistemului.

Structura programului:

- administratori - **5 persoane**
  - grupă: max. 5 persoane
  - durată: 5 zile

Organizare:

- Achizitorul va asigura următoarele resurse:
  - sală de curs;
  - telecomunicații;
  - stații de lucru/laptopuri;
- Prestatorul va asigura următoarele resurse:
  - mediul de instruire identic cu mediul de producție
  - date de test semnificative
  - Suportul de curs în format electronic
- Instruirea se va realiza în limba română.
- Participanții vor primi certificate, emise de furnizorul instruirii, care atestă competențele de dobândite.

6.2.8 Garanția sistemului

În cadrul proiectului sunt avute în vedere avute in vedere următoarele servicii de garanție:

- servicii de garanție pentru echipamentele hardware;.
- servicii de garanție pentru soluția software dezvoltată și implementată.

Prin perioadă de garanție se înțelege perioada în care Prestatorul are obligația de a asigura în mod gratuit remedierea defectelor constatate de către Beneficiar pe parcursul exploatării sistemului.

Prin „defecte" se înțeleg toate neconformitățile față de cerințele caietului de sarcini, precum și eventualele funcționalități suplimentare agreate de comun acord între Beneficiar și Prestator în perioada implementării și documentate corespunzător.

Perioada de garanție pentru echipamentele hardware, de comunicație și pentru licențele de sistem este precizată în secțiunea aferentă caracteristicilor tehnice ale acestora și se acordă de la momentul recepției calitative.

Garanția pentru întregul sistem de aplicații este de 36 luni de la data recepției finale, prin garanție înțelegând menținerea funcționalităților existente la momentul recepției calitative, certificate prin testele realizate.

Orice costuri aferente menținerii garanției produselor software licențiate, conform politicilor producătorilor, vor fi în sarcina Prestatorului, în măsura în care acestea sunt necesare pentru menținerea garanției sistemului software integrat sau a componentelor sale.

În cazul disfuncționalităților apărute în perioada de garanție, ofertantul devenit Prestator va trebui să respecte următoarele criterii de calitate a serviciilor:

1. Defecte hardware

În cazul componentelor hardware și de comunicație centralizate, care susțin operarea tuturor utilizatorilor:

- Timpul de intervenție pentru diagnosticare va fi de cel mult 8 ore, cel de soluționare temporară (work-around, care permite continuarea activității, chiar dacă aceasta nu se face la nivelul maxim de performanță) va fi de cel mult 24 ore, iar cel de remediere de cel mult 72 de ore. Toți timpii se măsoară de la momentul semnalării incidentului, în intervalul orar 08:00-17:00, în zilele lucrătoare.

În cazul componentelor hardware descentralizate, care susțin operarea unuia unui grup de utilizatori:

- Timpul de intervenție pentru diagnosticare în caz de defect va fi de cel mult 12 ore, cel de soluționare temporară (work-around, care permite continuarea activității, chiar dacă aceasta nu se face la nivelul maxim de performanță) va fi de cel mult 48 de ore, iar cel de remediere de cel mult 96 de ore. Toți timpii se măsoară de la momentul semnalării incidentului, în intervalul orar 08:00-17:00, în zilele lucrătoare.

2. Defecte software

Criteriile de performanță ale serviciilor furnizate în perioada de garanție sunt (în funcție de gravitatea incidentului apărut) următoarele:

Tabel 7 - Timpii de răspuns

Gravitate	Timp de răspuns	Timp soluționare temporară	Timp remediere
Critic	4 ore	8 ore	24 ore
Mediu	8 ore	24 ore	48 ore
Minor	48 ore	72 ore	96 de ore

Tipul incidentelor:

- **Critic**: una sau mai multe resurse din mediul productiv sunt nefuncționale sau profund degradate, iar impactul acestui incident duce la imposibilitatea utilizării integrale a întregului sistem sau a unei componente majore a acestuia.
- **Mediu**: impactul produs de degradarea uneia sau mai multor resurse duce la scăderea performanței sau afectarea parțială a unor funcționalități ale sistemului. Sistemul este funcțional pentru cea mai mare parte a scenariilor de utilizare.
- **Minor**: impactul produs de degradarea uneia sau mai multor resurse este redus sau există soluție temporară.

Prestatorul are obligația de a asigura serviciile de remediere a eventualelor defecte (bug fixing) în perioada de garanție în intervalul orar 8-17, în toate zilele lucrătoare. **Prin ore/zile aferente timpilor de răspuns, soluționare temporară sau remediere se înțeleg ore consecutive în intervalul zilelor lucrătoare.**

3. Procedura de notificare a incidentelor

Înștiințarea cu privire la o disfuncționalitate a sistemului informatic implementat va fi realizată de către beneficiar prin următoarele metode puse la dispoziție de către Prestator:

- utilizând sistemul de poștă electronică (la o adresa de poștă electronică dedicată pusă la dispoziție de către Prestator).
- printr-un apel telefonic al Beneficiarului la un număr dedicat pus la dispoziție de către Prestator.
- printr-o aplicație de gestionare a incidentelor.

4. Documentarea intervențiilor

La finalizarea fiecărei intervenții în cadrul perioadei de garanție se va întocmi o fișă de intervenție care va conține următoarele detalii: data intervenției, descrierea intervenției, modalitatea de rezolvare a intervenției (reparație/înlocuire), durata de intervenție și confirmarea recepției prin semnăturile Prestatorului și Beneficiarului.

Perioada de garanție se prelungește cu timpul de nefuncționare al echipamentelor/subsistemelor informatice în intervalul de reparare a acestora.

Livrabile:

- Fișe de intervenție
- Raport de garanție și suport (trimestrial)

6.3 Grafic de execuție

Ofertantul va prezenta împreună cu oferta un grafic de execuție (plan de proiect) în care se vor detalia toate activitățile planificate în cadrul proiectului, milestone-urile aferente furnizării livrabilelor și ale acceptării acestora de către Autoritatea Contractantă, responsabilitățile asociate fiecărei activități și persoanele responsabile din cadrul echipei de proiect pentru realizarea fiecărei activități.

Fiecare activitate din graficul de proiect va fi detaliată în partea descriptivă a ofertei. Activitățile se vor planifica prin respectarea dependențelor logice între ele și nu prin stabilirea arbitrară a unei date de start și de finalizare, fără o legătură logică vizibilă cu alte activități. Dependențele și ipotezele de planificare vor fi detaliate în oferta tehnică.

Planul de proiect va fi prezentat în format Gantt, realizat cu un instrument software de planificare (Microsoft Project, Primavera sau similar) și va conține obligatoriu, condiție obligatorie pentru validarea ofertei, următoarele elemente:

- Codificarea activităților (cod WBS)
- Denumirea activităților
- Durata activităților (cu precizarea zilelor lucrătoare sau calendaristice)
- Dependențele de alte activități, prin indicarea codului activităților respective
- Reprezentarea grafică a activității printr-o bară orizontală, plasată în zona care indică perioada de derulare a proiectului, cu marcarea grafică a dependențelor de alte bare ale altor activități
- Marcarea milestone-urilor (jaloanelor) proiectului, la finalul principalelor etape ale procesului de implementare, la finalizarea recepțiilor cantitative și calitative, cu ocazia transmiterii rapoartelor periodice.

Activitățile prezentate în graficul Gantt nu vor avea durate mai lungi de 14 zile calendaristice. În cazul unor activități principale mai lungi de 14 zile calendaristice, acestea vor fi descompuse în sub activități cu obiective măsurabile, cu durată mai scurtă de 14 zile calendaristice.

Această cerință este formulată pentru evitarea situației în care activitățile sunt planificate generic pe întreaga durată a proiectului, sau activități care de fapt reprezintă etape de proiect. Prezentarea graficului de activități la un nivel granular va permite atât evaluarea abilității ofertanților de a transforma strategia de implementare prezentată într-un plan fezabil și realist, cât și ulterior va permite (pe perioada implementării) un proces eficient de evaluare a progresului implementării.

Activitățile incluse în plan vor avea rezultate și/sau livrabile identificate clar și măsurabile. Toate activitățile incluse în graficul de implementare vor fi descrise în detaliu în cadrul ofertei scrise.

Graficul de execuție reprezintă un element de bază al strategiei ofertantului, arată modul în care acesta își va organiza activitatea, motiv pentru care lipsa sa sau a informațiilor solicitate nu poate face obiectul clarificărilor sau completărilor ulterioare pe durata evaluării ofertelor.

Ofertanții vor evidenția toate milestone-urile și activitățile importante, duratele acestora și resursele ce vor fi alocate execuției fiecărei activități, în cadrul graficului de execuție ce va fi inclus în oferta tehnică.

6.4 Recepția

În planul de proiect se va avea în vedere realizarea următoarelor recepții:

- **Cantitative** - prin intermediul cărora se livrează echipamentele HW, pachetele SW și livrabilele serviciilor prestate din punct de vedere cantitativ.
- **Calitative** - prin intermediul cărora Beneficiarul verifică parametrii de calitate ai livrărilor cantitative. Acestea pot fi:

Recepții calitative parțiale - sunt recepții calitative ce privesc anumite componente și/sau servicii ce fac obiectul contractului de achiziție. Sunt acceptate recepții calitative parțiale pentru:

- Livrarea și instalarea echipamentelor HW - în urma testelor de acceptanță a instalării echipamentelor HW și software de bază.
- Livrarea și instalare software - în urma testelor de acceptanță a instalării software-ului.
- Servicii de analiză și proiectare - în urma aprobării documentului de analiză și proiectare.
- Servicii de dezvoltare și testare - în urma testării funcționale, de integrare și de performanță a sistemului.
- Servicii de instruire – în urma acceptării serviciilor de instruire prestate.

Recepție finală - care este realizată după finalizarea tuturor activităților pentru implementarea sistemului informatic și punerea în funcțiune a întregului sistem informatic.

Livrabilele se predau beneficiarului pe baza unor procese verbale de recepție cantitativă. Recepțiile calitative se realizează pe baza proceselor verbale de recepție cantitativă aferente livrabilelor menționate mai sus și a inspecțiilor/verificărilor realizate de către beneficiar în conformitate cu prevederile prezentului document.

Recepția serviciilor se va efectua pe baza de proces verbal semnat de Contractant și Autoritatea contractantă. Recepția serviciilor se va realiza în mai multe etape, în funcție de progresul contractului, respectiv:

Recepția cantitativă se va realiza după prestarea serviciilor și predarea livrabilului scris aferent respectivei etape a implementării (raport de analiză și proiectare, scenarii de testare, raport de testare, raport de instalare și configurare infrastructură și software de sistem, raport de instruire).

Recepția calitativă se va realiza după instalarea, punerea în funcțiune și testarea rezultatelor obținute în urma prestării serviciilor și a configurării aplicațiilor și echipamentelor (acolo unde este cazul) și după ce, dacă este cazul, toate neconformitățile constatate au fost remediate.

Ofertantul va prezenta în cadrul propunerii tehnice planul de recepții și acceptanță care va fi utilizat în cadrul proiectului pentru recepțiile/acceptanțele parțiale și recepția/acceptanța finală, în concordanță cu graficul general de implementare pregătit și cu respectarea termenelor maximale solicitate pentru finalizarea principalelor etape ale implementării. Se va prezenta planul împărțit pe etape, precum și formularele aferente recepțiilor/acceptanțelor parțiale și recepțiilor/acceptanțelor finale.

6.5 Grafic de plăți

Autoritatea Contractantă va efectua plățile conform etapelor de recepție prevăzute în prezentul document:

- Pe baza procesului verbal de acceptanță parțială, după finalizarea livrării și instalării echipamentelor hardware și în urma testelor de acceptanță aferente instalării echipamentelor hardware și a licențelor software standard.
- Pe baza procesului verbal de acceptanță parțială după finalizarea livrării și instalării licențelor software – in urma instalării produselor și a verificării funcționalităților standard ale acestora, conform ofertei tehnice;
- Pe baza proceselor verbale de acceptanță parțială, după finalizarea principalelor etape ale implementării sistemului informatic integrat și în urma testelor de acceptanță aferente etapelor de analiză și proiectare, dezvoltare/configurare și testare, instruire și punere în producție.

Procesul Verbal de Recepție a Produselor/Serviciilor reprezintă singurul temei în baza căruia Contractantul este îndreptățit să primească plata pentru Produsele furnizate și pentru Serviciile prestate în conformitate cu prevederile prezentului Contract.

Termenul stabilit pentru plata facturii este de 30 de zile de la data transmiterii facturii în sistemul național privind factura electronică RO e-Factura, factura fiind emisă după acceptarea fără obiecțiuni, prin Proces-Verbal de Recepție, a bunurilor și a serviciilor facturate.

6.6 Strategia de organizare și coordonare a proiectului

Metodologia de organizare, coordonare și implementare a proiectului se bazează pe următoarele strategii:

a) Strategia de organizare și coordonare a proiectului

Proiectul va fi condus la nivel strategic de un Comitet de Conducere care va stabili și va controla direcția în care evoluează proiectul. Includerea în Comitetul de Conducere a unor persoane cu funcții de răspundere va asigura atât respectarea intereselor tuturor celor afectați de proiect, cât și o alocare corespunzătoare a resurselor pe durata proiectului.

b) Strategia de achiziție a produselor și a serviciilor

Strategia de achiziție include încheierea contractului printr-o procedură de achiziție realizată conform legislației în vigoare. În cadrul acestei licitații, **ANS** va avea rol de Autoritate Contractantă și va pregăti documentația necesară în vederea selecționării unor firme care vor asigura realizarea proiectului.

c) Strategia de implementare a proiectului

Din punctul de vedere al strategiei de implementare a proiectului, aceasta va respecta modelul standard al unui proiect de tip IT, în domeniul administrațiilor publice, prin care sunt puse în aplicare prevederi legale incidente instituției.

Structura organizațională a proiectului va fi pe trei niveluri ierarhice:

- **Nivelul 1** – Comitetul de conducere – cu rol de decizie în cadrul proiectului, compus din minim 3 membri:

Președinte Comitet – Reprezentant Autoritate Contractantă

Reprezentant Prestator care realizează implementarea proiectului;

- **Nivelul 2** – Nivelul de coordonare – cu rol de planificare, urmărire și control în cadrul proiectului. Acest nivel raportează către Comitetul de Conducere.

Este compus din:

Responsabil proiect din partea Autorității Contractante

Lider/manager de proiect din partea Prestatorului de produse și servicii IT;

- **Nivelul 3** – Nivelul de execuție – cu rol de execuție a activităților din cadrul proiectului. Acest nivel este constituit din echipele de proiect ale Autorității Contractante și Contractantului de produse și servicii IT, numit și contractor. Fiecare echipă de proiect raportează către Lidear-ul/ Managerul de proiect /responsabil proiect corespunzător.

6.7 Metodologia de implementare a proiectului

Ofertantul va descrie metodologia de implementare a proiectului, precum și fiecare fază a proiectului în conformitate cu metodologia de proiect propusă.

Ofertantul va detalia metodele și instrumentele folosite pentru:

- Managementul proiectului.
- Monitorizarea evoluției proiectului.
- Managementul calității.
- Managementul riscurilor.
- Managementul schimbării.
- Managementul comunicării.

6.7.1 Monitorizarea evoluției proiectului

Strategia de monitorizare a evoluției proiectului va include în mod obligatoriu cel puțin următoarele elemente, care vor fi incluse în strategia și graficul de prestare și care vor fi prezentate în cadrul ofertei:

- Întâlnire de kick-off, în cadrul căreia se vor realiza: prezentarea echipelor, a responsabilităților experților, punctele de contact din partea celor două echipe, informațiile necesare pentru demararea activităților, prezentarea graficului de prestare actualizat în funcție de data de semnare a contractului, prezentarea principalelor componente ale soluției tehnice care va fi implementată, strategia de derulare a proiectului (etape, livrabile), instrumente de lucru și de colaborare.
- Întâlniri de planificare la începutul fiecărei etape din cadrul ciclului de viață al implementării sistemului informatic, în cadrul căreia se vor prezenta: obiectivele etapei, activitățile care se vor desfășura și calendarul acestora, dependențele de echipa autorității contractante (inclusiv informații necesare), formatul livrabilelor de final de etapă. Ședința de kick-off va avea de asemenea rolul de ședință de început pentru etapa de analiză.
- Întâlniri de confirmare a rezultatelor obținute în cadrul unei etape finalizate a procesului de implementare. În cazul în care se va considera oportun, ședințele de confirmare a

finalizării unei etape se pot desfășura împreună cu cele de planificare a demarării următoarei etape a procesului de implementare.

- Ședințe lunare de management pentru prezentarea de către Managerul de proiect al Prestatorului a stadiului proiectului, a activităților întârziate și a măsurilor de recuperare a întârzierii, pentru discutarea problemelor și a riscurilor apărute și care sunt de competența echipei de management. Se va prezenta în mod obligatoriu graficul de execuție Gantt actualizat (format tracking Gantt, cu vizualizarea simultană a versiunii aprobate la demararea proiectului, comparativ cu varianta care include datele reale de start și finalizare a tuturor activităților, inclusiv cu eventualele replanificări de durate și activități suplimentare necesare).
- Rapoarte lunare de progres prezentate de Prestator responsabilului de contract al autorității contractante.
- Registru de acțiuni - document întreținut de către managerul de proiect al Prestatorului și care va include toate acțiunile, responsabilii și termenele stabilite în cadrul ședințelor de management și a întâlnirilor de planificare sau al ședințelor tehnice.
- Ședințe tehnice - acest tip de ședințe vor fi programate și vor avea loc ori de câte ori va fi necesară clarificarea unor aspecte de ordin tehnic între membrii celor două echipe (Prestator și Beneficiar). Deciziile luate și acțiunile stabilite vor fi documentate de către Prestator și transmise autorității contractante. Aceste tipuri de ședințe pot avea loc și on-line, pentru eficiență.
- Ședințe ad-hoc, ori de câte ori este necesară rezolvarea sau clarificarea unei probleme punctuale. Aceste tipuri de ședințe pot avea loc și on-line, pentru eficiență.

6.7.2 Managementul calității

Calitatea în mediul de proiect se definește ca fiind totalitatea cerințelor de ordin tehnic, funcțional, a obiectivelor cantitative și calitative ale proiectului, precum și metodologia și procedurile de management de proiect stabilite la nivelul proiectului, care trebuie atinse și respectate pentru finalizarea cu succes a proiectului.

Ofertantul va avea în vedere cel puțin furnizarea următoarelor livrabile pe durata implementării proiectului:

- Livrabile de management (planuri, proceduri, rapoarte):
  - Echipa de proiect;
  - Planul proiectului;
  - Rapoarte de monitorizare și control al proiectului:
- Livrabile tehnice ale proiectului:
  - Conform capitolului 6.2.

Procedura de management al calității va prevedea metodele concrete prin care se va monitoriza și controla evoluția calității livrabilelor, pe întreaga durată a proiectului. În mod concret, se va realiza la nivelul proiectului o strategie de testare și acceptanță care va indica, pentru fiecare tip de livrabil în parte, etapele procesului de verificare a calității (testare), criteriile de acceptanță și modalitatea de documentare a acestui proces.

6.7.3 Managementul riscurilor

Riscurile la adresa obiectivelor proiectului vor fi identificate și documentate în Registrul Riscurilor, împreună cu modul în care acestea pot fi ținute sub control.

De asemenea, se vor prevedea măsuri de rezervă pentru situația în care riscul devine activ. Registrul Riscurilor și planurile asociate pentru controlul acestor riscuri vor fi revăzute în mod regulat în timpul ședințelor de evaluare a riscurilor.

Pe durata derulării proiectului, în momentul identificării unui nou risc sau al manifestării unui risc planificat, persoana din echipa de proiect care a identificat riscul îl comunică managerului de proiect. Acesta realizează o analiză preliminară și, dacă riscul este real, întocmește un Raport de Risc pe care îl transmite Comitetului de Conducere al proiectului în vederea aprobării măsurilor propuse în cadrul Raportului. Managerul de Proiect al prestatorului va fi responsabil de actualizarea Registrului de Riscuri.

Prestatorul va fi responsabil pentru livrarea unui sistem informatic perfect integrat, care să includă toate funcționalitățile și care să permită atingerea tuturor obiectivelor specifice ale proiectului, conform cerințelor din Caietul de Sarcini.

De asemenea, la finalizarea implementării tehnice a proiectului și înainte de testarea finală a soluției, prestatorul va trebui să realizeze teste de securitate și să prezinte un raport cu privire la problemele identificate. Acestea vor fi analizate, se vor stabili acțiuni de remediere care vor fi implementate și ulterior se va face o nouă verificare a securității.

Ofertantul va prezenta procedura de management a riscurilor, registrul inițial al riscurilor care conține cele mai importante riscuri identificate de acesta și măsurile propuse de remediere, precum și formularele care vor fi utilizate în cadrul acestui proces pe durata contractului.

Se vor identifica riscuri din categorii diferite, care necesită abordări diferite, inclusiv pe baza experienței proprii. Se vor analiza cu precădere riscuri de ordin tehnic, riscuri de integrare, riscuri aferente migrării de date, riscuri aferente caracterului centralizat al sistemului.

6.7.4 Managementul schimbării

Schimbările survenite sau propuse vor fi analizate din punct de vedere al implicațiilor asupra diferitelor elemente ale proiectului (obiective, cerințe, buget, resurse, termene de implementare, riscuri) și se vor stabili cele mai bune strategii pentru gestionarea lor. Schimbările care au implicații asupra livrabilelor proiectului vor fi documentate și supuse aprobării Conducerii Autorității Contractante, sau persoanelor desemnate în acest sens.

Ofertantul va prezenta în cadrul propunerii tehnice modalitatea de tratare a schimbărilor în cadrul contractului. Se va prezenta procedura de management al schimbărilor precum și formularele care vor fi utilizate în cadrul acestui proces pe durata contractului.

6.7.5 Managementul comunicării

Ofertantul trebuie să prezinte în cadrul proiectului modalitatea (metodologia) prin care se va realiza comunicarea între participanții la contract.

6.8 Evaluarea rezultatelor proiectului

Evaluarea rezultatelor proiectului este procesul prin care se obțin informații asupra calității proiectului, măsurând rezultatele în raport cu obiectivele stabilite, în vederea luării deciziilor strategice pentru a susține implementarea și managementul proiectului. Se va realiza atât evaluarea permanentă (concomitentă proiectului), cât și evaluarea finală, conform schemei de evaluare.

Evaluarea permanentă, realizată pe parcursul duratei proiectului va fi axată pe următoarele aspecte:

- Încadrarea în timpul alocat.
- Încadrarea în buget.
- Stadiul realizărilor.
- Efectele implementării proiectului pentru instituție.
- Cooperarea în rândul membrilor echipei de proiect.

În cazul evaluării permanente se vor folosi multe dintre datele obținute în urma procesului de monitorizare, însă examinarea acestor date va fi analitică. Rezultatele acestui tip de evaluare sunt cruciale, deoarece ele determină modalitatea de continuare a proiectului.

Evaluarea finală se va realiza la sfârșitul perioadei de implementare a proiectului, moment în care toate componentele proiectului (proces, relevanță și coerență măsurilor luate, activitățile, valoarea adăugată) vor fi luate în considerare în vederea examinării rezultatelor. Evaluarea va fi atât cantitativă, cât și calitativă și va viza:

- Resursele investite.
- Activitățile desfășurate.
- Rezultatele obținute.
- Atingerea nivelului de performanță propus la planificare.
- Schimbările intervenite și consecințele lor
- Efectele implementării proiectului pentru instituție
- Nivelul de proprietate locală asupra rezultatelor proiectului.

Activitatea de evaluare este responsabilitatea beneficiarului finanțării nerambursabile. În scopul unei analize eficiente și imparțiale, se va desfășura și o evaluare externă (audit financiar), comandată pentru a evita dezavantajele folosirii unui singur tip de evaluare, deseori subiectivă, și anume aceea a evaluării interne.

6.9 Raportarea

Prestatorul trebuie să elaboreze și să transmită Autorității Contractante cel puțin următoarele rapoarte:

- **Rapoarte periodice (lunare)** prezentate de Managerul de Proiect Autorității Contractante, în care să prezinte: stadiul implementării în baza planului de proiect contractual, activitățile realizate, cele întârziate și motivul, activitățile planificate pentru următoarea perioadă, riscuri și probleme, situația financiară a proiectului, cereri de schimbare, alte probleme care necesită o decizie din partea Autorității Contractante
- **Rapoarte de etapă**, la finalizarea principalelor etape din ciclul de implementare: analiză, instalare și configurare echipamente și software standard, testare, instruire, suport pentru operarea în producție.
- **Rapoarte ad-hoc** elaborate de către Managerul de proiect, ori de câte ori acest lucru este necesar, la solicitarea Autorității Contractante.
- **Raport Final** (la finalizarea contractului), cuprinzând un sumar al activităților desfășurate, al rezultatelor obținute, al problemelor întâmpinate și al soluțiilor găsite, precum și eventuale aspecte importante în perioada post-implementare;

6.10 Atribuțiile și responsabilitățile Părților

6.10.1 Responsabilitățile Contractantului

Contractantul va fi responsabil pentru:

1. asigurarea planificării resurselor în raport cu graficul estimat pentru derularea contractului și prezentat în cadrul acestui document;
2. îndeplinirea obligațiilor sale, cu respectarea celor mai bune practici din domeniu, a prevederilor legale și contractuale relevante precum și cu deplina înțelegere a complexității legate de derularea cu succes a Contractului;
3. asigurarea valabilității tuturor autorizațiilor și certificatelor, care sunt necesare (conform legislației în vigoare) pentru prestarea serviciilor;

4. prestarea serviciilor în conformitate cu cerințele Caietului de Sarcini;
5. prezentarea rezultatelor în formatul/formatele care să respecte cerințele Autorității Contractante;
6. colaborarea cu personalul Autorității Contractante alocat pentru serviciile desfășurate conform Contractului (monitorizarea progresului activităților în cadrul Contractului, coordonarea activităților în cadrul Contractului, feedback).
7. respectarea prevederilor legale în domeniul achizițiilor publice cu privire la evitarea conflictului de interese. Prestatorul nu are dreptul de a angaja sau de a încheia orice alte înțelegeri privind prestarea serviciilor ce fac obiectul prezentului contract, direct ori indirect, în scopul îndeplinirii contractului, cu:
    a. persoane fizice sau juridice care au fost implicate în procesul de evaluare a ofertelor depuse în cadrul procedurii de achiziție ce a stat la baza atribuirii acestui contract;
    b. angajați/foști angajați ai Achizitorului implicați în procedura de atribuire cu care autoritatea contractantă a încetat relațiile contractuale ulterior atribuirii prezentului contract, pe parcursul unei perioade de cel puțin 12 (douăsprezece) luni de la încheierea contractului, sub sancțiunea rezilierii contractului.

6.10.2 Responsabilitățile Autorității Contractante

Autoritatea Contractantă va fi responsabilă pentru:

1. punerea la dispoziția Contractantului a tuturor informațiilor disponibile pentru obținerea rezultatelor așteptate, cum ar fi: date de intrare, raportări, situații specifice;
2. desemnarea echipei implicate și responsabile cu interacțiunea și suportul oferit Contractantului;
3. asigurarea tuturor resurselor care sunt în sarcina sa pentru buna derulare a Contractului.
4. efectuarea plăților conform prevederilor contractuale.

7 Cerințe privind echipa de proiect a ofertantului

7.1 Numărul de experți pe categorie de expertiză necesară

Având în vedere complexitatea si specificitatea contractului ce urmează a fi atribuit, precum și necesitatea ca Ofertantul să gestioneze contractul într-un mod metodologic și organizat, au fost formulate cerințele minimale și obligatorii de mai jos cu privire la componența și responsabilitățile echipei de proiect a Ofertantului, după cum urmează:

7.2 Experți cheie

7.2.1 Manager de proiect - 1 persoană

Responsabilități:

- Activități specifice de management de proiect (legat de obiectul contractului, implementare sistem informatic).
- Punct principal de contact in relația cu beneficiarul.
- Managementul contractului.
- Managementul proiectului in ansamblul sau, managementul ariei de cuprindere, managementul schimbărilor, planificarea generala a proiectului, managementul riscurilor, managementul problemelor, managementul comunicării.
- Asigurarea resurselor proiectului.
- Managementul, organizarea, alocarea și planificarea echipei de proiect.
- Identificarea riscurilor și propunere de soluții pentru diminuarea/evitarea riscurilor.
- Rezolvarea problemelor in scopul evitării situațiilor de criza.
- Urmărirea respectării tuturor termenelor conform planului de proiect.
- Analiza modalității prin care livrabilele proiectului corespund cerințelor de business.
- Realizarea rapoartelor de progres ale proiectului.
- Elaborarea planurilor de calitate.

Cerințe minimale:

- Studii superioare finalizate cu diplomă de licență sau echivalent.
- Minimum 5 ani de experiență specifică în managementul proiectelor IT, dovedită prin participarea în calitate de manager de proiect / coordonator într-un proiect de implementare a unui sistem informatic cu valoare de minimum 1.000.000 EUR (fără TVA), demonstrată prin documente justificative relevante.
- Competențe privind metodologia de management de proiect pe care Prestatorul o va utiliza în cadrul proiectului, dovedite prin cel puțin o certificare recunoscută la nivel național/internațional.

7.2.2 Expert analiză de business - 1 persoană

Responsabilități:

- Analiza cerințelor beneficiarului.
- Identificarea proceselor interne ale beneficiarului.
- Colectarea datelor documentate de la beneficiar.
- Coordonarea interviurilor de analiză cu persoanele implicate.
- Validarea datelor colectate de la beneficiar.
- Identificare riscuri asociate implementării sistemului.
- Identificare procese și proceduri afectate de implementarea sistemului.
- Furnizarea către echipa prestatorului a informațiilor specifice domeniului de activitate al beneficiarului, inclusiv a restricțiilor procedurale și legale, precum și a recomandărilor privind implementarea.

Cerințe minimale:

- Studii superioare finalizate cu diplomă de licență sau echivalent.
- Minimum 3 ani experiență specifică în analiză de business în proiecte IT, dovedită prin participarea în cel puțin un proiect similar.
- Competențe privind analiza de business dovedite prin certificare recunoscută la nivel național și/sau internațional ca standard în materie de tip CBAP® (Certified Business Analysis Professional) sau echivalent.
- Experiență specifică de participare în cel puțin un proiect sau contract în care a îndeplinit activități similare cu cele pe care urmează să le îndeplinească în viitorul contract, dovedită prin documente justificative relevante.

7.2.3 Expert arhitect software - Full Stack - 1 persoană

Responsabilități:

- Definirea arhitecturii generale a soluției informatice;
- Definire cerințe funcționale, non-funcționale și de integrare, proiectare model de date și procese;
- Proiectarea și documentarea arhitecturii, a specificațiilor funcționale, respectiv a specificațiilor de integrare.
- Sprijinirea echipei tehnice de implementare pentru găsirea de soluții tehnice
- Identificare riscurilor tehnice și a măsurilor de minimizare/eliminare a acestora prin soluții de arhitectură
- Dezvoltarea de servicii autonome (adaptoare custom), incluzând mapări de date, transformări, validări si gestionarea securității specifice fiecărui sistem;
- Implementează pattern-uri critice precum Retry policies, Circuit Breaker și gestionarea cozilor de mesaje (Message Queues)
- Monitorizarea activităților care includ containerizarea (Docker)

- Configurează si (la nevoie) dezvoltă componente în cadrul platformei pentru a implementa fluxuri de lucru complexe.

Cerințe minimale:

- Studii superioare finalizate cu diploma de licență sau echivalent.
- Experiență specifică de minimum 3 ani în dezvoltarea de aplicații software de tip backend/web, demonstrată prin participarea în calitate de arhitect/dezvoltator în cel puțin un proiect de dezvoltare platformă web sau aplicație enterprise care include componente server-side (API REST/SOAP, microservicii, baze de date sau echivalent).
- Experiență dovedită în gestionarea de baze de date relaționale, scriere de interogări complexe și proceduri stocate.
- Experiență specifică de participare în cel puțin un proiect sau contract în care a îndeplinit activități similare cu cele pe care urmează să le îndeplinească în viitorul contract, dovedită prin documente justificative relevante.

7.2.4 Expert securitate informatică - 1 persoană

Responsabilități:

- Identificarea potențialelor vulnerabilități de securitate ale sistemului și proiectarea măsurilor de securitate necesare în vederea atingerii obiectivului de siguranță a datelor și a operării solicitat.
- Definirea procedurilor de asigurare și monitorizare a securității sistemului implementat.
- Verificarea/testarea securității sistemului informatic, la finalizarea implementării.

Cerințe minimale:

- Studii superioare finalizate cu diploma de licență sau echivalent.
- Minimum 3 ani experiență specifică în securitate informatică, testare sau audit de securitate, dovedită prin participarea în cel puțin un proiect similar.
- Competente în domeniul testării/auditării securității sistemelor informatice dovedite prin certificare recunoscuta la nivel național și/sau internațional.
- Experiență specifică de participare în cel puțin un proiect sau contract în care a îndeplinit activități similare cu cele pe care urmează să le îndeplinească în viitorul contract, dovedită prin documente justificative relevante.

7.2.5 Expert integrare - 1 persoană

Responsabilități:

- Dezvoltă și configurează componente modulare reutilizabile pentru orchestrarea API-urilor în workflow-uri complexe.
- Realizează mapări și transformări de date între sisteme eterogene, asigurând validarea acestora prin reguli predefinite în formulare dinamice.
- Implementează logica de integrare inter-instituțională, utilizând API-uri expuse de entități diferite pentru a crea un motor unitar de guvernanță.

- Gestionează securitatea integrărilor prin utilizarea Vault pentru managementul secretelor, cheilor și variabilelor de mediu.
- Configurează politici de Retry, gestionarea erorilor și mecanisme de alertare pentru a asigura fiabilitatea execuțiilor paralele și izolate.
- Implementează arhitecturi event-driven, configurând surse (webhook-uri, mesaje) și triggere care reacționează în timp real la evenimente specifice.
- Utilizează planificarea de tip cron-like pentru execuția programată a fluxurilor de mentenanță și administrare.
- Proiectează vizual workflow-uri care includ ramificații, condiții, bucle și execuții paralele.
- Dezvoltă scripturi de automatizare în limbaje diverse (Python, Node.js, PHP, Java, C#, Go) pentru a extinde funcționalitățile platformei.

Cerințe minimale:

- Studii superioare finalizate cu diploma de licență sau echivalent.
- Minimum 3 ani experiență specifică în integrarea sistemelor informatice (API REST/SOAP, ESB, middleware), dovedită prin participarea în cel puțin un proiect de integrare multi-sistem.
- Cunoștințe aprofundate de RBAC (Role-Based Access Control) și auditare detaliată a execuțiilor. Cunoașterea și aplicarea practică a modelului Role-Based Access Control (RBAC), demonstrată prin:
    - prezentarea în propunerea tehnică a arhitecturii de control al accesului propuse pentru sistem (roluri, permisiuni, granularitate, mecanisme de auditare); și/sau
    - referința la cel puțin un proiect anterior în care expertul a implementat un mecanism RBAC, descris succint în CV. Nu se solicită certificare separată.
- Experiență dovedită în cadrul unor proiecte similare de a lucra cu versiuni multiple de runtime (ex: PHP 5.6 - 8.3, Java 8 - 21).

7.2.6 Expert dezvoltare software - Full Stack - 1 persoană

Responsabilități:

- Activități specifice de dezvoltare de aplicații software, pe baza documentelor de analiza, specificații funcționale, specificații tehnice, arhitectura sistem
- Dezvoltarea de soluții custom pentru integrarea sistemelor legacy sau third-party, asigurând fluxul de date între Frontend și Backend.
- Realizarea mapărilor complexe de date și transformări (ETL la nivel de serviciu), implementarea validărilor stricte de tip schemă și gestionarea protocoalelor de securitate (OAuth2, mTLS, API Keys).
- Implementarea logică a politicilor de Retry (cu exponential backoff) și a mecanismelor de Circuit Breaker (ex. folosind biblioteci precum Resilience4j, Polly sau la nivel de Service Mesh) pentru a preveni căderile în lanț.

- Utilizarea cozilor de mesaje (Message Queues precum RabbitMQ, Kafka sau AWS SQS) pentru procesarea asincronă a task-urilor grele, asigurând o experiență de utilizare fluidă în Frontend.
- Implementarea fluxurilor de lucru complexe care combină interfețele vizuale cu logica de business backend via Webhooks și API-uri REST.

Cerințe minimale:

- Studii superioare finalizate cu diploma de licență sau echivalent.
- Experiență specifică de minimum 3 ani în dezvoltarea de aplicații software de tip backend/web, demonstrată prin participarea în calitate de arhitect/dezvoltator în cel puțin un proiect de dezvoltare platformă web sau aplicație enterprise care include componente server-side (API REST/SOAP, microservicii, baze de date sau echivalent).
- Experiență dovedită în gestionarea de baze de date relaționale, scriere de interogări complexe și proceduri stocate.
- Experiență specifică de participare în cel puțin un proiect sau contract în care a îndeplinit activități similare cu cele pe care urmează să le îndeplinească în viitorul contract, dovedită prin documente justificative relevante.

7.2.7 Expert baze de date - 1 persoană

Responsabilități:

- Proiectează și realizează structura de date sau a modelului de date și a designului logic și fizic al bazelor de date prin transpunerea fluxului informațional și a schemelor logice, specifice sistemului în baze de date relaționale.
- Realizează documentațiile de administrare a bazelor de date;
- Gestionează aspectele de securitate a bazelor de date, inclusiv controlează permisiunile de acces și privilegiile utilizatorilor.
- Contribuie la elaborarea documentației aplicației și a livrabilelor proiectului.
- Stabilește funcționalități de backup și recover a datelor în caz de dezastru.

Cerințe minimale:

- Studii superioare finalizate cu diplomă de licență sau echivalent.
- Minimum 3 ani experiență specifică în administrarea sau proiectarea bazelor de date, dovedită prin participarea în cel puțin un proiect similar.
- Competențe în domeniul bazelor de date, dovedite prin cel puțin o certificare recunoscută la nivel național/ internațional.
- Experiență specifică de participare în cel puțin un proiect sau contract în care a îndeplinit activități similare cu cele pe care urmează să le îndeplinească în viitorul contract, dovedită prin documente justificative relevante.

7.2.8 Expert testare software - 1 persoană

Responsabilități:

- Activități specifice testării de aplicații software
- Realizarea planurilor, a scenariilor și a cazurilor de test
- Activități de testare componente și testare funcțională
- Întocmirea și livrarea rapoartelor de testare
- Asigurare suport tehnic în perioada de garanție
- Crearea/ actualizarea documentațiilor

Cerințe minimale:

- Studii superioare finalizate cu diplomă de licență sau echivalent.
- Minimum 3 ani experiență specifică în testare software, dovedită prin participarea în cel puțin un proiect similar.
- Competente privind testarea, dovedite prin certificare recunoscuta la nivel național și/sau internațional.
- Participare in cel puțin un proiect sau contract în care a îndeplinit activități similare cu cele pe care urmează să le îndeplinească în viitorul contract, dovedită prin prezentarea de contracte, recomandări sau orice alte documente justificative relevante din care să reiasă experiența specifică.

7.2.9 Expert instruire - 1 persoană

Responsabilități:

- Susținerea sesiunilor de formare a personalului
- Evaluarea personalului
- Pregătirea materialelor de instruire

Cerințe minimale:

- Studii superioare finalizate cu diploma de licență sau echivalent.
- Minimum 3 ani experiență specifică în instruirea utilizatorilor în proiecte IT, dovedită prin participarea în cel puțin un proiect similar.
- Competente privind formarea personalului, dovedite prin certificare recunoscută la nivel național și/sau internațional.
- Participare in cel puțin un proiect sau contract în care a îndeplinit activități similare cu cele pe care urmează să le îndeplinească în viitorul contract, dovedită prin prezentarea de contracte, recomandări sau orice alte documente justificative relevante din care să reiasă experiența specific.

Pe lângă echipa de experții cheie, ofertanții vor avea obligația de a asigura forța de muncă calificată/autorizată și vor purta întreaga responsabilitate pentru îndeplinirea corectă a activităților descrise, conform specificului soluțiilor informatice pe care le vor oferta.

În cazul în care, pentru realizarea serviciilor, este necesar personal în plus față de cel specificat în ofertă și mai apoi în contract, pentru dezvoltarea corespunzătoare a proiectului, prestatorul va fi

responsabil pentru asigurarea acestor resurse adiționale, fără costuri suplimentare din partea Autorității contractante.

Prestatorul este liber să-și stabilească propria strategie de personal, astfel încât să acopere toată durata contractului, în conformitate cu prevederile caietului de sarcini.

Pentru fiecare rol de expert cheie din echipa de proiect solicitată se va prezenta în cadrul ofertei un CV detaliat al persoanei propuse, din care să rezulte modalitatea de îndeplinire a tuturor cerințelor minimale aferente expertului respectiv. În acest sens, se va prezenta o matrice detaliată de corespondență între cerințele minimale ale fiecărui rol de expert cheie solicitat și modalitatea concretă de îndeplinire a cerinței respective de către persoana propusă.

În oferta se va prezenta modalitatea de organizare a echipei (diagramă organizațională a proiectului) precum și rolurile și responsabilitățile propuse (cele minimale plus altele, considerate necesare de către fiecare ofertant în parte).

Având în vedere importanța echipei de experți a ofertantului în vederea asigurării atingerii obiectivelor contractului, cerințele cu privire la experiența și expertiza membrilor echipei sunt cerințe tehnice obligatorii ale Caietului de sarcini, iar echipa de Experți ofertată este parte integrantă a Ofertei Tehnice. Nerespectarea cerințelor minimale obligatorii ale Caietului de Sarcini referitoare la echipa de experți cheie duce la respingerea ofertei tehnice ca neconformă.

Certificările profesionale solicitate pot fi demonstrate și prin prezentarea unor diplome de absolvire a unor studii de învățământ superior care să dea dreptul, potrivit prevederilor Registrului Național al Calificărilor din învățământul Superior- RNCIS, ca absolventul să practice respectiva activitate.

Participarea la activitățile de implementare a experților cheie nominalizați în ofertă este obligatorie, sub sancțiunea rezilierii contractului din culpa exclusivă a prestatorului. În cazul absenței unui expert cheie nominalizat de la mai mult de două activități programate în cadrul proiectului, autoritatea contractantă va notifica prestatorul cu privire la acest aspect și va solicita fie înlocuirea expertului, fie reluarea activității numai în prezența acestuia.

Autoritatea contractantă poate solicita înlocuirea unui expert nominalizat cheie, în cazul în care acesta nu performează corespunzător în cadrul proiectului.

Înlocuirea unui expert nominalizat se va putea realiza numai în cazuri în afara controlului prestatorului (de exemplu boală, cazuri de forță majoră, demisie)/înlocuirea unui expert se va face în cel mult 2 săptămâni de la momentul identificării indisponibilității acestuia, fără a afecta calendarul de implementare și integral pe cheltuiala prestatorului, care va avea obligația de a gestiona procesul de tranziție, astfel încât noul expert să fie la curent cu activitățile proiectului și să nu genereze ineficientă și/sau întârzieri.

Înlocuirea unui expert identificat în ofertă se va putea face numai cu un alt expert care deține cel puțin același nivel de cunoștințe și experiență astfel încât, dacă ar fi fost nominalizat în cadrul ofertei, ar fi obținut cel puțin același punctaj cu expertul pe care îl înlocuiește, astfel încât rezultatul evaluării ofertelor să nu fie afectat.

Pentru demonstrarea îndeplinirii cerințelor minimale aferente experților, se vor avea în vedere următoarele tipuri de documente pentru studiile și cursurile de formare absolvite, se vor furniza copii ale diplomelor obținute.

În urma verificării exactității informațiilor și a dovezilor furnizate de către ofertanți, autoritatea contractantă poate solicita și alte documente/informații care să clarifice experiența profesionala

solicitata. De asemenea, autoritatea contractantă își rezervă dreptul de a contacta beneficiarii finali ai proiectelor prezentate la experiența profesionala, în vedere confirmării celor prezentate de către ofertanți.

Un expert nominalizat poate îndeplini un singur rol în cadrul echipei de implementare.

Orice înlocuire a experților cheie, se poate face doar cu notificarea și acceptul prealabil al Autorității contractante și după și acceptarea de către autoritatea contractantă a propunerii unui nou expert care întrunește toate cerințele tehnice minimale solicitate prin prezentul caiet de sarcini pentru expertul care urmează să fie înlocuit, precum și pe cele care au dus la acordarea punctajului tehnic.

7.3 Experți cheie pentru serviciile de arhivare

Rolurile aferente arhivării fizice sunt necesare exclusiv pentru implementarea Modulului Arhivă și au caracter accesoriu. Aceste roluri nu reprezintă cerințe de calificare pentru operatorul economic, ci cerințe tehnice aferente execuției contractului.

Pentru serviciile de arhivare solicitate în cadrul Caietului de sarcini va fi desemnat următoarele tipuri de personal:

7.3.1 Coordonator tehnic echipa arhivare fizică – 1 persoană

Pentru această poziție se va nominaliza o persoană care va fi responsabilă în principal cu gestiunea din punct de vedere tehnic al activităților de arhivare fizică a documentelor.

Responsabilități:

- Coordonarea echipei de arhivare și gestiunea activităților de arhivare din punct de vedere tehnic;
- Întocmirea planului metodic pentru selecționarea documentelor în vederea eliminării definitive din arhivă și a tuturor documentelor necesare în acest sens;
- Participarea în cadrul Comisiei de selecționare a documentelor în vederea eliminării definitive din arhivă;
- Asigurarea că activitatea de arhivare fizica se desfășoară conform metodologiei;
- Participă la întocmirea rapoartelor privind activitățile de arhivare fizica;
- Coordonarea activităților de arhivare fizica a documentelor, asigurarea calității, etc.;
- Supravegherea îndeplinirii planului de desfășurare a activităților;
- Identificarea riscurilor și problemelor tehnice și a soluțiilor de rezolvare;
- Verificarea documentelor întocmite de echipă.

Cerințe minime:

- Studii superioare într-unul din domeniile prevăzute în Standardul ocupațional de arhivist (limbă și literatură, limbi moderne aplicate, istorie, studii culturale) finalizate prin diplomă de licență sau echivalent;
- Experiență profesională generala de minim 5 ani;

- Participarea la cel puțin un contract de servicii de arhivare a documentelor în condițiile prevăzute în Legea 16/1996 Legea Arhivelor Naționale, în care să fi deținut o poziție similară celei pentru care este propus.

7.3.2 Coordonator tehnic echipa de digitizare – 1 persoană

Coordonatorul echipei de digitizare va fi responsabil în principal cu gestiunea din punct de vedere tehnic al activităților de scanare.

- Coordonarea echipei de scanare și gestiunea activităților de scanare din punct de vedere tehnic;
- Asigurarea că activitatea de scanare se desfășoară conform metodologiei;
- Participă la întocmirea rapoartelor privind activitățile de scanare;
- Coordonarea activităților de pregătirea și scanarea documentelor, asigurarea calității, etc.;
- Supravegherea îndeplinirii planului de desfășurare a activităților;
- Identificarea riscurilor și problemelor tehnice și a soluțiilor de rezolvare;
- Verificarea documentelor întocmite de echipă.

Cerințe minime:

- Studii superioare finalizate prin diplomă de licență sau echivalent;
- Experiență profesională generala de minim 5 ani;
- Participarea la cel puțin un contract în care s-au prestat servicii arhivare digitală (scanare) similare cu cele care fac obiectul contractului ce urmează a fi atribuit, în care să fi deținut o poziție similară celei pentru care este propus.

7.3.3 Coordonator tehnic procesare date – 1 persoană

Coordonatorul echipei de procesare va fi responsabil în principal cu gestiunea din punct de vedere tehnic al activităților de procesare date.

Responsabilități:

- Coordonarea echipei de procesare date și gestiunea activităților de procesare date din punct de vedere tehnic;
- Asigurarea că activitatea de procesare date se desfășoară conform metodologiei;
- Livrarea rapoartelor privind activitățile de procesare date;
- Coordonarea activităților de procesarea datelor de intrare, verificarea și validarea datelor colectate, obținerea metadatelor, scrierea media, etc..
- Supravegherea îndeplinirii planului de desfășurare a activităților;
- Identificarea riscurilor și problemelor tehnice și a soluțiilor de rezolvare;
- Verificarea documentelor întocmite de echipă.

Cerințe minime:

- Studii superioare finalizate prin diplomă de licență sau echivalent;
- Experiență profesională generală de minim 5 ani;
- Participarea la cel puțin un contract în care s-au prestat servicii arhivare digitală constând în digitizarea documentelor cu extragere meta-descriptori și structurarea documentelor în unei baze cu acestea acestora similare cu cele care fac obiectul contractului ce urmează a fi atribuit.

7.4 Experți non-cheie pentru serviciile de arhivare

Rolurile aferente arhivării fizice sunt necesare exclusiv pentru implementarea Modulului Arhivă și au caracter accesoriu. Aceste roluri nu reprezintă cerințe de calificare pentru operatorul economic, ci cerințe tehnice aferente execuției contractului.

Echipa de proiect va trebui să cuprindă inclusiv următorii experți non-cheie care să asigure prestarea serviciilor aferente contractului la nivelul calitativ minim solicitat:

7.4.1 Arhiviști atestați – minim 5 persoane;

Responsabilități:

- Realizarea de operațiuni arhivistice de prelucrare a documentelor
- Administrarea documentelor in depozitul de arhiva
- Verificarea condițiilor de conservare a documentelor din depozit

Cerințe minime:

- Deținerea de competențe privind arhivarea, dovedite prin prezentarea unei diplome/certificări sau orice alt document echivalent din care să reiasă îndeplinirea cerinței

7.4.2 Arhivari atestați – minim 5 persoane;

Responsabilități:

- Realizarea de operațiuni arhivistice de prelucrare a documentelor
- Administrarea documentelor in depozitul de arhiva
- Verificarea condițiilor de conservare a documentelor din depozit.

Cerințe minime:

- Deținerea de competențe privind arhivarea, dovedite prin prezentarea unei diplome/certificări sau orice alt document echivalent din care să reiasă îndeplinirea cerinței

7.4.3 Legători manuali – minim 2 persoane;

Responsabilități:

- Pregătirea documentelor pentru constituirea unităților arhivistice;
- Legarea documentelor aferente unităților arhivistice constituite conform prevederilor legale .

Cerințe minime:

- Deținerea de competențe privind legătoria de arhivă, dovedite prin prezentarea unei diplome/certificări sau orice alt document echivalent din care să reiasă îndeplinirea cerinței

7.4.4 Operatori scanare – minim 5 persoane;

Responsabilități:

- Scanarea documentelor utilizând echipamentele din dotare și instrumentele software de scanare și arhivare disponibile la nivelul prestatorului.

7.4.5 Operatori procesare date – minim 3 persoane;

Responsabilități:

- Procesarea datelor/documentelor/informațiilor în vederea constituirii arhivei digitizate potrivit cerințelor prezentului caiet de sarcini.

Modalitatea în care se va face dovada îndeplinirii cerințelor stabilite pentru experții solicitați prin documentația de atribuire vor fi aceleași ca cele pentru experții cheie și non cheie implicați în procesul de implementare a soluțiilor informatice din cadrul proiectului.

7.5 Personal administrativ și personal suport pentru activitatea experților principali în cadrul Contractului

Contractantul va asigura personalul administrativ care este necesar pentru desfășurarea activității echipei sale. În plus, Contractantul va asigura (după caz și dacă se consideră necesar) pentru serviciile din contract, personal de suport pentru prestarea serviciilor.

7.6 Alte cerințe legate de personalul direct implicat în prestarea serviciilor

Este responsabilitatea Contractantului să se asigure și să urmărească cu strictețe ca oricare dintre experții principali propuși să cunoască foarte bine și să înțeleagă cerințele, scopul și obiectivele Contractului, cerințele legislației românești relevante, specificul activităților pe care urmează să le desfășoare în cadrul Contractului precum și a responsabilităților atribuite.

7.7 Infrastructura Contractantului necesară pentru desfășurarea activităților Contractului

Ofertantul devenit Contractant trebuie să se asigure că personalul care își desfășoară activitatea în cadrul Contractului, dispune de sprijinul material și de infrastructura necesară pentru a permite acestuia să se concentreze asupra realizării activităților din cadrul Contractului.

Infrastructura prezentată de Ofertant în Propunerea Tehnică trebuie să fie corespunzătoare scopului Contractului și să îndeplinească toate cerințele de funcționalitate și pentru utilizare (inclusiv aspecte legate de protecția mediului) stabilite prin legislația în vigoare sau va avea acces la infrastructura/sprijinul material necesar(ă), demonstrând asta prin prezentarea aranjamentelor întreprinse în acest sens.

8 Scenariu sesiune demonstrativă

Având în vedere complexitatea sistemului ce trebuie implementat și importanța respectării termenului de implementare menționat în prezentul document, asumat și prin contractul de finanțare, Autoritatea Contractantă solicită ofertanților prezentarea și demonstrarea principalelor capabilități ale soluției tehnice propuse în cadrul unei sesiuni demonstrative. Obiectivul acestei sesiuni va fi acela de a demonstra faptul că platformele tehnologice pe care se bazează soluția software propusă respectă unele dintre cerințele tehnice și funcționale majore ale proiectului, conform specificațiilor minimale ale caietului de sarcini.

Astfel, obiectul sesiunii demonstrative constă în demonstrarea modalității de îndeplinire a unora dintre cerințele tehnice minimale care se regăsesc în caietul de sarcini, cerințe considerate de bază de către autoritatea contractantă, care nu pot face obiectul dezvoltării în cadrul contractului și care trebuie să fie respectate de către platformele tehnice ofertate.

În cazul în care un Ofertant nu poate demonstra în cadrul sesiunii demonstrative îndeplinirea uneia sau mai multor cerințe minimale ale caietului de sarcini, incluse în scenariul de verificare, conform modalității prezentate în oferta scrisă, atunci oferta acestuia va fi respinsă ca neconformă.

Ofertele care vor prezenta înregistrări video cu caracter de prezentare generală a soluției propuse și care nu demonstrează scenariile solicitate punct cu punct, vor fi declarate neconforme.

Ofertantul va realiza o înregistrare video a întregului scenariu de verificare prezentat în cadrul prezentului capitol pentru toate produsele indicate.

Fișierele video vor fi încărcate odată cu oferta, în cadrul platformei SEAP. În situația în care, din motive strict tehnice (de exemplu, dimensiunea fișierelor video), încărcarea acestora în SEAP nu este posibilă, ofertantul va depune fișierele video pe suport fizic, în plic închis, la registratura autorității contractante, până la data și ora-limită de depunere a ofertelor.

Nu se acceptă link-uri către platforme de streaming, servicii externe de partajare video sau orice alt mecanism de accesare a conținutului în afara SEAP.

.

Înregistrarea video se va realiza astfel încât să respecte următoarele criterii de calitate:

- în cazul produselor software, se va filma (sau captura) întregul ecran, astfel încât să fie vizibile și lizibile câmpurile și butoanele;
- mișcările mouse-ului vor fi suficient de lente încât să se poată urmări operațiunile realizate pe ecran;
- executarea scenariului va fi în mod obligatoriu însoțită de descrierea audio, sincronizată cu imaginea video, a acțiunilor pe care operatorul le execută pe ecran.

Înregistrarea video va fi realizată astfel încât să poată fi redată utilizând un PC standard cu Windows 10, utilizând Windows Media Player.

Ulterior, în cadrul etapei de evaluare tehnică a ofertelor, Autoritatea Contractantă poate solicita ofertanților reluarea sesiunii demonstrative, pentru clarificarea unor eventuale aspecte tehnice. în acest caz, sesiunea demonstrativă va fi susținută de către fiecare Ofertant online, în urma invitației de participare primite din partea Autorității Contractante.

Pe durata sesiunii demonstrative, Autoritatea Contractantă va solicita realizarea de capturi de ecran cu interfețele aplicațiilor utilizate pentru demonstrarea fiecărei funcționalități care face obiectul sesiunii demonstrative. Aceste capturi de ecran vor fi incluse în anexa procesului verbal aferent sesiunii demonstrative ce va fi încheiat de către Autoritatea Contractantă și Ofertanți la finalul sesiunilor demonstrative.

În scopul susținerii sesiunii demonstrative, nu se solicită configurarea unor platforme software conform cerințelor de proces specifice Autorității contractante, ci doar demonstrarea unor funcționalități de bază care trebuie să facă parte din platformele software standard ofertate.

Astfel, în timpul sesiunii demonstrative va fi demonstrată modalitatea de îndeplinire a următoarelor cerințe minimale ale caietului de sarcini pentru aplicațiile solicitate:

8.1 Scenariul DEMO I – Managementul cererilor, registratură electronică și fluxuri de lucru cu documentele

Acest scenariu validează funcționalitățile de bază ale platformei integrate de management documente: configurarea dinamică a formularelor, integrarea Portal–Back-Office, registratura electronică, motorul de workflow, colaborarea pe documente, generarea de răspunsuri oficiale și semnarea electronică.

Cerințe tehnice de demonstrat:

Se va demonstra accesarea interfeței de administrare a platformei și crearea unui formular nou prin intermediul unui modulul de tip Form Builder (Smart Form Builder), validând configurarea dinamică a formularelor și interfața de administrare aferentă;

Se va demonstra definirea logicii condiționale în cadrul unui formular, prin adăugarea unui câmp selector (ex: Tip solicitant: Persoană Fizică/Juridică) care activează dinamic câmpuri suplimentare în funcție de selecția utilizatorului (ex: CUI, nr. Registrul Comerțului pentru persoane juridice), validând capacitatea Smart Form de a ghida utilizatorul și de a colecta date minimal dar complet;

Se va demonstra maparea câmpurilor formularului public pe entitatea internă „Cerere” din Aplicația de Management (minim trei câmpuri critice — ex: Nume, E-mail, CUI), validând integrarea datelor din formular cu structura internă de tip Back-Office;

Se va demonstra publicarea instantanee a formularului configurat pe Portalul Web, asigurând sincronizarea în timp real între Back-Office și Portal;

Se va demonstra accesarea Portalului și localizarea formularelor publicate, cu diferențierea comportamentului pentru utilizatorii autentificați și neautentificați (formularele cu vizibilitate restricționată nu vor fi accesibile utilizatorilor neautentificați);

Se va demonstra parcurgerea fluxului asistat de completare de către utilizatorul final, cu declanșarea logicii condiționale configurate, eliminarea câmpurilor redundante, validarea câmpurilor obligatorii cu mesaje de eroare clare și trimiterea formularului, asigurând controlul calității datelor la nivelul Portalului;

Se va demonstra integrarea nativă Portal → Back-Office în timp real, prin crearea automată a entității „Cerere” în aplicația de management ca urmare a submiterii din Portal, maparea corectă a datelor pe câmpurile interne corespunzătoare (validând integritatea și securitatea în tranzit) și generarea automată a notificărilor sau task-urilor interne asociate;

Registratură Electronică. Se va demonstra funcționarea modulului de Registratură Electronică integrat nativ cu Portalul, cu vizualizarea listei de documente/cereri nou primite, generarea automată a numărului de înregistrare, datei/orei, tipului documentului și sursei (ex: „Portal Web”), validarea numerotării automate și a trasabilității legale;

Se va demonstra completarea și validarea metadatelor suplimentare la nivelul registraturii (categorie, domeniu, termen legal), precum și asocierea documentelor atașate de utilizator la dosarul cererii fără descărcare locală, în logica content management unitar;

Se va demonstra inițierea fluxului de lucru direct din registratură, prin selectarea acțiunii „Inițiază Workflow” pe cererea înregistrată, validând legătura Registratură → Workflow;

Se va demonstra motorul de workflow cu selectarea automată a fluxului de lucru predefinit în funcție de tipul documentului, alocarea automată a task-urilor către compartimentul responsabil (ex: Direcție Tehnică/Juridică), calculul automat al termenelor de soluționare cu excluderea zilelor nelucrătoare, precum și vizualizarea grafică a diagramei de workflow și a stării curente a cererii pentru managerul de proces, asigurând transparența și controlul procesului;

Se va demonstra accesul securizat la conținut direct din aplicație fără descărcare locală, cu deschiderea documentelor atașate în viewer/editor web (PDF/Word) și editarea colaborativă simultană a documentelor de lucru (track changes, comentarii) direct în platformă de către doi sau mai mulți utilizatori;

Se va demonstra comunicarea contextuală în sistem prin adăugarea de comentarii și mențiuni (@user) pe documentele de lucru;

Se va demonstra generarea răspunsului oficial pe baza unui template standard, cu completarea automată a câmpurilor dinamice (ex: nr. înregistrare, date solicitant) și reutilizarea șabloanelor predefinite;

Se va demonstra fluxul decizional de aprobare, prin trimiterea automată a răspunsului în etapa de aprobare, aprobarea sau respingerea/returnarea cu observații de către manager, validând ciclurile de feedback intern;

Semnare electronică și ieșiri oficiale. Se va demonstra integrarea cu mecanismul de semnătură electronică, semnarea documentului aprobat de către conducere, înregistrarea automată a documentului semnat în registratura de ieșire, precum și publicarea răspunsului în contul utilizatorului din Portal cu notificare prin email, asigurând conformitatea legală și ciclul complet intrare–ieșire.

8.2 Scenariul DEMO II – Business Intelligence (BI)

Acest scenariu validează funcționalitățile de analiză și raportare de bază ale soluției de Business Intelligence: dashboard-urile analitice cu indicatori de performanță, capacitatea de interogare în limbaj natural (NL2SQL) și reutilizarea rezultatelor obținute din analize ad-hoc.

Cerințe tehnice de demonstrat:

Dashboard-uri analitice. Se va demonstra prezentarea a cel puțin 3–4 dashboard-uri analitice relevante, acoperind minim următoarele domenii: conformitatea și încălcările tipilor de răspuns (inclusiv trend sau breakdown pe departament/unitate), fluxul și volumul documentelor (pe status, pe tip sau pe perioadă), precum și sarcina de lucru / workload (volum pe utilizator sau pe echipă,

inclusiv vechime/backlog). Fiecare dashboard va conține grafice clare (bar, line, pie etc.) și indicatori de performanță (KPI) numerici unde este cazul; datele pot fi demonstrate/simulate;

Interogare în limbaj natural (NL2SQL). Se va demonstra capacitatea unui utilizator de a pune intrebari in limba romana direct in interfata aplicatiei (ex: 'Care departament are cele mai multe întârzieri?', 'Cate documente au intrat saptamana trecuta?'), iar sistemul va genera (sau sugera) automat o interogare pe date (ex: SQL) și va afișa rezultatul sub formă de tabel și/sau grafic. Se acceptă și variante în care generarea este semi-automată (completare, sugestii), cu condiția explicării mecanismului de funcționare;

Reutilizarea rezultatelor. Se va demonstra capacitatea de a salva rezultatele și graficele obținute din interogări (ex: din interfața de chat/NL2SQL) și de a le include in dashboard-uri existente sau intr-o zona dedicata de 'rapoarte / widget-uri salvate', asigurând astfel reutilizarea și persistența analizelor ad-hoc efectuate de utilizatori.

8.3 Scenariul DEMO III - Chatbot

Acest scenariu validează implementarea și funcționarea unui sistem de asistent virtual de tip chat bazat pe inteligență artificială, conceput pentru a înțelege intenția utilizatorului, a procesa limbaj natural și a genera răspunsuri relevante: autentificarea și gestionarea utilizatorilor cu sistem de roluri și a documentelor, crearea template-urilor cu variabile, gestionarea conversațiilor cu suport pentru fișiere și voce, generarea de documente prin conversație și conversia text-în-voce.

Cerințe tehnice de demonstrat:

Autentificarea și gestionarea utilizatorilor. Se va demonstra funcționalitatea completă de înregistrare și autentificare: crearea unui cont nou prin completarea formularului de înregistrare (nume, prenume, adresă de email, parolă), salvarea datelor în baza de date, autentificarea ulterioară cu email și parolă, crearea sesiunii active și redirecționarea către interfața principală a aplicației;

Sistemul de roluri. Se va demonstra funcționarea sistemului de roluri prin crearea a două tipuri de conturi: un cont cu rol de administrator și un cont cu rol de utilizator standard. Se va verifica că administratorul are acces la funcționalitățile de configurare ale sistemului (gestionarea clienților, managementul documentelor, configurarea comportamentului AI în chat), iar utilizatorul standard are acces doar la conversațiile cu AI, gestionarea propriului profil și setările interfeței;

Managementul documentelor. Se va demonstra gestionarea documentelor de către administrator: accesarea secțiunii documentelor, încărcarea unui document în sistem (tipuri acceptate: PDF, DOC/DOCX, alte documente text), procesarea automată a documentului de către sistem și disponibilizarea sa pentru utilizarea de către AI în procesul de răspuns sau de generare de documente;

Crearea template-urilor de documente. Se va demonstra transformarea unui document într-un template editabil care conține variabile (ex: {{NUME}}, {{ADRESA}}, {{CNP}}), indicând locurile unde Asistentul va introduce automat datele furnizate de utilizator, precum și salvarea template-ului și disponibilizarea sa pentru generarea ulterioară a documentelor;

Gestionarea variabilelor. Se va demonstra funcționalitatea de administrare a variabilelor: crearea unei variabile noi (cu introducerea numelui variabilei), salvarea și utilizarea ei în template-uri, editarea variabilelor existente și ștergerea variabilelor;

Gestionarea conversațiilor. Se va demonstra funcționarea completă a sistemului de conversații: autentificarea utilizatorului, crearea unei conversații noi, trimiterea mesajelor către asistentul virtual cu salvarea conversației în baza de date, redenumirea conversației, ștergerea conversației și căutarea conversațiilor din trecut;

Încărcarea fișierelor în conversație. Se va demonstra capacitatea utilizatorului de a încărca fișiere pentru analiză în cadrul unei conversații active (tipuri acceptate: PDF, imagine PNG/JPG, document text), iar chatbot-ul va analiza fișierul și va extrage informațiile relevante din acesta;

Introducerea mesajelor vocale. Se va demonstra funcționalitatea de introducere a mesajelor vocale în chat: selectarea opțiunii de înregistrare vocală, înregistrarea mesajului, trimiterea către chat-ul AI, conversia automată a mesajului vocal în text și transmiterea către AI pentru procesare;

Generarea documentelor prin conversație. Se va demonstra capacitatea chat-ului AI de a identifica template-ul corespunzător la solicitarea unui document de către utilizator, afișarea unui preview al documentului solicitat (structura documentului, secțiunile principale, câmpurile care trebuie completate) pentru confirmarea de către utilizator, solicitarea datelor necesare completării variabilelor (ex: nume, adresă, CNP) direct în interfața de chat și generarea documentului final;

Gestionarea documentelor suplimentare. Se va demonstra capacitatea sistemului de a informa utilizatorul atunci când documentul solicitat necesită documente suplimentare (ex: copie carte de identitate, documente justificative, alte fișiere relevante), precum și posibilitatea utilizatorului de a încărca aceste documente direct în conversație;

Conversia textului în voce (Text-to-Speech). Se va demonstra funcția de redare vocală a răspunsurilor: trimiterea unei întrebări către chatbot, generarea răspunsului, activarea opțiunii de redare audio și conversia automată a textului în voce cu redare către utilizator.

8.4 Scenariul DEMO IV – Managementul identității, accesului și securitatea platformei

Acest scenariu validează mecanismele de securitate și administrare a identității la nivelul întregii platforme integrate: serviciul unificat de identitate, fluxurile de autentificare configurabile, controlul granular al accesului, jurnalele de audit și gestionarea centralizată a secretelor.

Cerințe tehnice de demonstrat:

Se va demonstra existența și funcționarea unui serviciu de identitate unificat pentru administrarea centralizată a utilizatorilor și a grupurilor, cu posibilitatea de creare, modificare, suspendare și ștergere a conturilor, precum și gestionarea apartenenței utilizatorilor la grupuri;

Se va demonstra configurabilitatea fluxurilor de autentificare, incluzând suportul pentru multiple metode de autentificare (nume utilizator/parolă, autentificare cu doi factori – 2FA prin cod SMS sau aplicație OTP, integrare cu sisteme naționale de identitate de tip eIDAS / ROeID), precum și parametrizarea politicilor aferente (durata sesiunii, complexitatea parolei, blocarea după tentative eșuate);

Se va demonstra un mecanism granular de control al accesului bazat pe roluri (RBAC), aplicabil la nivel de resurse și acțiuni specifice, cu posibilitatea definirii de roluri predefinite și personalizate (ex: Super Admin, Admin Instituție, Moderator, Evaluator, Autor, Co-autor, Utilizator standard) și a limitării accesului utilizatorilor strict la resursele pentru care au permisiuni explicite;

Se va demonstra funcționarea jurnalului de audit (audit trail) detaliat și imuabil, cu înregistrarea evenimentelor precum autentificări (reușite și eșuate), modificări de politici, creări/modificări/ștergeri de resurse, schimbări de roluri și operațiuni administrative, inclusiv filtrarea și căutarea avansată a jurnalelor după utilizator, acțiune sau interval de timp;

Se va demonstra gestionarea centralizată și securizată a secretelor (chei API, certificate, credențiale de servicii) destinate utilizării în implementările de infrastructură și Kubernetes, precum și în cadrul fluxurilor de lucru aplicative, folosind servicii de tip Secret Manager.

8.5 Scenariul DEMO V – Platforma de Learning Management System (LMS)

Acest scenariu validează platforma de Learning Management System (LMS) integrată în soluție: asistentul de învățare bazat pe AI, managementul conținutului (CMS), administrarea accesului și a motorului AI, monitorizarea și securitatea, crearea și colaborarea pe materiale didactice, compatibilitatea mobilă, parcurgerea conținutului de către cursant și interacțiunea cu evaluările.

Cerințe tehnice de demonstrat:

Prezentarea asistentului de învățare dotat cu interfață hibridă voce-text în limba română. Se va demonstra adresarea unei întrebări în limbaj natural în limba română către asistent și obținerea răspunsului, precum și crearea unei baze de cunoștințe din interfața web a platformei și interogarea acesteia la nivel de lecție;

Se va demonstra configurarea setărilor de bază ale chatbot-ului, incluzând limba și preferințele de interacțiune;

Se va demonstra încărcarea și adaptarea modelului de limbaj, prin setarea unui model de limbaj preantrenat și adaptarea lui la specificul conversației prin adăugarea de terminologie specifică domeniului în fișierele de antrenament;

Se va demonstra crearea și personalizarea intențiilor (intents) bazate pe scenariile de utilizare comune (ex: „resetare parolă”, „programare întâlnire”);

Se va demonstra configurarea răspunsurilor și a fluxurilor conversaționale ale chatbot-ului, astfel încât utilizatorii să fie ghidați spre soluții eficiente;

Se va demonstra testarea și optimizarea interacțiunilor chatbot, cu verificarea înțelegerii corecte a intențiilor și ajustarea configurărilor și a modelului de antrenament în funcție de rezultatele testelor;

Gestionarea accesului și a utilizatorilor (RBAC). Se va demonstra accesarea panoului de administrare, crearea unui utilizator administrat cu atribuirea unui rol specific (ex: Autor sau Evaluator) și funcția de blocare/deblocare instantanee a unui cont de utilizator (modificarea stării de acces în timp real);

Configurarea motorului AI. Se va demonstra accesarea secțiunii de setări AI din panoul de administrare, configurarea securizată a cheii API prin Secret Manager și selectarea modelului de limbaj implicit pentru platformă;

Monitorizare și Securitate (Analytics). Se va demonstra accesarea tab-ului de Audit & Securitate, filtrarea și vizualizarea jurnalelor de audit pentru a valida trasabilitatea acțiunilor (cine a creat un utilizator, cine a modificat un proiect), precum și prezentarea log-urilor de securitate prin simularea sau vizualizarea unor evenimente (ex: încercări eșuate de autentificare, declanșarea limitărilor de rată);

Crearea și structurarea conținutului (CMS). Se va demonstra accesarea Organizatorului (tabloul de bord) și crearea unui proiect nou, utilizarea asistentului AI pentru generarea automată a structurii unui material pe baza unui subiect scris sau a unui fișier încărcat, precum și interfața de editare de tip drag-and-drop a materialului;

Asistență AI integrată. Se va demonstra selectarea unui element de text din zona de lucru și utilizarea funcției de AI din panoul dedicat pentru a rescrie/adapta/extinde/rezuma textul, precum și generarea unui fișier audio dintr-un text prin funcționalitatea Text-to-Speech;

Colaborare și Feedback. Se va demonstra invitarea unui alt utilizator ca și Co-autor la proiect, deschiderea panoului de revizuire, adăugarea unui comentariu contextual pe un element specific din curs, rezolvarea unui comentariu și utilizarea unei rubrici de evaluare pentru a oferi feedback structurat;

Compatibilitate mobilă și previzualizare. Se va demonstra funcționalitatea de comutare a vizualizării între Desktop, Tabletă și Mobil pentru materialele didactice, rearanjarea automată a elementelor (responsive design) și lansarea modului de Previzualizare pentru a vedea cursul exact așa cum îl va vedea cursantul final;

Accesarea și parcurgerea conținutului de către cursant. Se va demonstra autentificarea securizată în platformă, accesarea unui curs publicat din tabloul de bord al cursantului și reluarea cursului exact de la secțiunea la care a rămas la sesiunea anterioară (sincronizarea progresului între dispozitive);

Interacțiunea cu evaluările și barierele logice. Se va demonstra parcurgerea unei secțiuni de testare, răspunsul la întrebări cu feedback vizual imediat (corect/greșit) și funcționarea unei „Bariere Logice” care împiedică avansarea cursantului până la obținerea scorului necesar la testul anterior.

9 Modalitatea de întocmire și prezentare a ofertei

9.1 Oferta tehnică

Oferta tehnică se va prezenta la rubrica special prevăzută în S.E.A.P. în acest sens, respectiv „Documente de calificare și propunere tehnică”, și va include:

1) **Formularul de Propunere Tehnică** - se va completa de ofertant în baza cerințelor din caietul de sarcini, incluzând toate informațiile solicitate, conform formularul aferent din secțiunea Formulare a Documentației de atribuire;

2) Matricea de corespondență care va conține pentru fiecare cerință sau grup de cerințe din caietul de sarcini (capitolele 3 integral, 4 integral, 5 integral și 6 integral) un răspuns descriptiv clar, iar pentru fiecare modul va conține cât mai multe exemple de capturi de ecran, în vederea explicitării modului în care acesta răspunde cerințelor autorității contractante.

3) Documente tehnice care nu conțin informații legate de prețuri (broșuri/ cataloage/ manuale utilizare/ fișe tehnice/ etc.) pentru produsele ofertate.

Documentele aferente propunerii tehnice trebuie prezentate și în format electronic (fișiere compatibile Microsoft Office sau PDF, editabile), pentru înlesnirea procesului de evaluare.

La redactarea ofertei se va avea în vedere ca aceasta să fie structurată astfel încât sa conțină următoarele:

I. **Considerații generale:**

- Viziunea proprie asupra realizării proiectului. Se așteaptă comentariile ofertantului din care sa reiasă modul în care a înțeles Caietul de sarcini, specificul activității beneficiarului și al proiectului, precum și principalele aspecte care vor asigura succesul proiectului.
- Enumerarea și explicarea principalelor riscuri și ipoteze privind execuția proiectului, plecând de la specificul proiectului și pe baza experienței similare a ofertantului. Se vor trata obligatoriu toate riscurile identificate în Caietul de sarcini, precum și riscurile de ordin tehnic relevante (legate de integrare, de performanță).
- Identificarea și prezentarea unor soluții de preîntâmpinare a riscurilor și de restrângere a efectelor acestora.

II. **Soluția tehnică propusă:**

- Ofertantul va prezenta pe larg soluția propusă pentru proiect, în vederea atingerii obiectivelor acestuia și a rezultatelor așteptate. Se vor identifica produsele propuse (hardware și software), avantajele acestora, proiecte similare în care acestea au fost utilizate (pentru produsele software), principalele aspecte legate de specificul acestora și de avantajele pe care le vor oferi autorității contractante.
- Ofertantul va prezenta arhitectura fizică și logică a sistemului propus. Se vor evidenția toate componentele arhitecturii software, realizându-se și o corespondență cu produsele software ofertate (pentru fiecare element al arhitecturii logice se vor prezenta produsele software cu care se va implementa componenta respectivă).

- Ofertantul va prezenta arhitectura tehnică a sistemului, cu identificarea infrastructurii hardware și a produselor software care vor fi instalate pe fiecare echipament în parte). Se va prezenta lista și configurația fiecărei mașini virtuale care se va configura.
- Ofertantul va prezenta arhitectura de înaltă disponibilitate pe care o propune, din punctul de vedere al infrastructurii de echipamente, al clusterului bazelor de date și al balansării serverelor de aplicație, precum și al componentei de comunicație.
- Se va descrie modalitatea de implementare a fiecărei cerințe funcționale aferente aplicațiilor specializate solicitate.
- Sunt așteptate răspunsuri concrete care să demonstreze înțelegerea cerinței și modalitatea concretă propusă pentru atingerea ei (descriere a funcționalității și capturi de ecrane din aplicațiile propuse, care să demonstreze modalitatea de îndeplinire a cerinței). Având în vedere faptul că se solicită ofertarea unor soluții software disponibile comercial, nu se acceptă doar o declarație de confirmare a conformității, ci o demonstrare concretă a modului concret în care soluția ofertată răspunde cerințelor, inclusiv (în cazul cerințelor pentru platformele software) prin includerea unor capturi de ecran care să dovedească modul în care soluția ofertată răspunde fiecărei cerințe a caietului de sarcini. Simpla declarare a respectării cerințelor sau copierea cerințelor fără personalizarea răspunsului în funcție de soluția ofertată și fără prezentarea capturilor de ecran relevante din aplicațiile propuse nu se va considera că este o dovadă a modalității în care cerințele sunt respectate, iar oferta tehnică va fi respinsă ca neconformă.
- În cazul în care anumite funcționalități specifice nu sunt prezente în aplicațiile ofertate și vor fi dezvoltate în cadrul proiectului, ofertantul va preciza explicit acest lucru în ofertă și va descrie strategia pe care o va aborda pentru implementarea funcționalităților respective (descrierea contextului aplicației, a modulului funcțional unde se va implementa funcționalitatea, ecranul care va fi personalizat etc.). Toate funcționalitățile pentru care nu se va preciza explicit faptul că vor fi dezvoltate în cadrul proiectului se va presupune că fac parte din aplicația standard ofertată și este obligatorie prezentarea capturilor de ecran justificative, sub sancțiunea respingerii ofertei. Pentru toate funcționalitățile dezvoltate în cadrul proiectului se va furniza obligatoriu codul sursă la finalul proiectului. Toate funcționalitățile care au fost indicate în cadrul ofertei ca fiind incluse în produsele standard ofertate se vor verifica în etapa de instalare a aplicațiilor, iar cele care au rezultat în urma personalizării se vor verifica în etapa de recepție a serviciilor de dezvoltare/configurare.

III. Strategia abordării:

a. Metodologii folosite:

- Ofertantul va descrie metodologia de implementare a sistemului informatic pe care o va utiliza, adaptată specificului acestui proiect și cuprinzând detalierea activităților din cadrul fiecărei etape a implementării, conform solicitărilor caietului de sarcini. Pentru fiecare etapă de implementare se vor identifica livrabilele fizice și scrise, iar pentru acestea din urmă se va prezenta structura conținutului și sursa informațiilor.
- Ofertantul va descrie metodologia de management de proiect folosită, care va fi adaptată specificului proiectului. Se vor descrie cel puțin strategiile de organizare, de planificare, de monitorizare și de control, managementul calității și al riscurilor (identificare, analiză,

planificare, monitorizare riscuri), managementul schimbării și al configurației livrabilelor proiectului (produse și livrabile scrise – documente)

- Ofertantul va descrie strategia de testare care va fi utilizată în cadrul proiectului, incluzând tipurile de teste care vor fi realizate asupra tuturor tipurilor de livrabile (echipamente, aplicații și servicii), etapele testării, modalitatea de planificare și de urmărire, inclusiv documentarea rezultatelor testării, modalitatea de gestionare a neconformităților. Se va descrie modalitatea de realizare a testelor funcționale, de securitate, de performanță, precum și uneltele care vor fi utilizate, acolo unde este cazul.
- Se vor prezenta răspunsuri la toate cerințele secțiunilor 4 și 5 din cadrul caietului de sarcini.

b. Organizarea proiectului:

- Ofertantul va prezenta în detaliu, în raport cu specificul organizației acestuia si cu metodologia propusa, modalitatea în care proiectul va fi organizat, incluzând cel puțin următoarele elemente: Reprezentantul său în cadrul Comitetului de Conducere al Proiectului, Manager de Proiect, Șefi de Echipă, Experții cheie și alte roluri importante din cadrul echipei tehnice de proiect, Echipa de Suport administrativ.
- Ofertantul va prezenta organizarea și responsabilitățile fiecărei părți implicate în proiect, inclusiv propunerile pentru organizarea: Beneficiarului/Utilizatorilor în scopul derulării corespunzătoare a proiectului.
- Ofertantul trebuie să-si asume în întregime efectuarea activităților care concură la atingerea rezultatelor, ținând seama de resursele umane limitate ale Beneficiarului/ Utilizatorilor.
- În cazul în care ofertantul reprezintă o asociere, ofertantul trebuie să descrie modalitatea în care fiecare membru al asocierii intervine în proiect, distribuirea și interacțiunea sarcinilor și responsabilităților. Aceeași descriere a rolurilor și a responsabilităților va fi prezentată și pentru eventualii subcontractori.
- Oferta va include o organigramă a echipei de proiect a prestatorului. Se va prezenta componența echipei prestatorului pentru fiecare dintre rolurile cheie solicitate în Caietul de sarcini. Se vor descrie responsabilitățile detaliate ale fiecăruia dintre experții solicitați, având în vedere prevederile caietului de sarcini și se va indica alocarea experților la diferitele activități ale proiectului.
- Oferta va conține un tabel în care, pentru fiecare dintre experții solicitați, se va descrie modalitatea concretă prin care expertul nominalizat îndeplinește fiecare dintre cerințele tehnice minimale solicitate, precum și cerințele pentru care se acordă punctaj (fără trimitere la alte documente atașate, cum ar fi CV-uri). Pentru demonstrarea perioadelor de experiența similară se vor prezenta datele de start și de finalizare (luna/an) pentru fiecare proiect în parte. Experiența similară trebuie să rezulte explicit și din CV-urile atașate ofertei tehnice. Se vor prezenta copii ale diplomelor pentru cursurile relevante absolvite, precum și documente justificative relevante pentru experiența similară prezentată în CV. Pentru fiecare expert nominalizat în parte se va prezenta o declarație de disponibilitate semnată de către expert și contrasemnată de către ofertant.

IV. Planificarea activităților

- Ofertantul va prezenta planificarea activităților propuse, în interdependența logică a acestora - un grafic în format Gantt.
- Planul trebuie să includă termenele cheie (milestones) pe care ofertantul și-a propus să le respecte pentru atingerea obiectivelor.
- Ofertantul va detalia care sunt resursele (experții cheie și numiți generic prin competențele lor) pe care le va aloca pentru fiecare etapă și activitate a proiectului.
- Graficul de proiect nu va cuprinde activități cu o durată individuală mai mare de 1 lună (30 de zile calendaristice, pentru demonstrarea înțelegerii complete și concrete a complexității proiectului și a activităților concrete pe care ofertantul le va avea de derulat, precum și pentru a permite ulterior o monitorizare eficientă a progresului implementării. în cazul în care graficul de implementare prezentat nu va respecta acest criteriu de calitate, oferta tehnica va fi respinsa.
- Ofertantul va prezenta o descriere detaliată a abordării pentru implementarea proiectului, prin detalierea fiecăreia dintre activitățile incluse în graficul Gantt pe care îl va prezenta. Pentru fiecare activitate se vor prezenta durata, experții implicați, rezultatul așteptat și eventualele dependențe de activități/resurse ale beneficiarului. Se vor identifica livrabilele principale ale serviciilor de implementare prestate, precum și acceptanțele parțiale.
- Ofertantul va realiza o prezentare detaliată din care să reiasă clar modul în care se desfășoară întregul proces care reglementează manipularea, pregătirea, scanarea indexarea, refacerea documentelor.
- Se va elabora și prezenta o planificare a activităților, a echipamentelor și a personalului alocat pentru prestarea serviciilor, astfel încât finalizarea serviciilor să se realizeze în termen, pornind de la estimările de volum din prezenta documentație.

V. Prezentarea serviciilor de garanție

- Ofertantul va prezenta o descriere detaliată a serviciilor de garanție și a metodologiei utilizate.

VI. Sesiune demonstrativă

- În cadrul ofertei tehnice se va include o înregistrare video a sesiunii demonstrative, conform scenariului de verificare din capitolul 8.

De asemenea, oferta va fi însoțită și de:

- **Declarație pe propria răspundere** - din care să rezulte faptul că la elaborarea ofertei ofertantul a ținut cont de obligațiile care sunt în vigoare în România referitoare la condițiile de mediu, sociale și cu privire la relațiile de muncă pe toată durata de îndeplinire a contractului de servicii, precum și că le va respecta în vederea implementării contractului. Informații detaliate privind reglementările care sunt în vigoare la nivel național și se referă la condițiile de muncă și protecția muncii, securității și sănătății în muncă, se pot obține de la Inspecția Muncii sau pe site-ul http://www.inspectmun.ro/legislatie/legislatie.html. Informații privind reglementările care sunt în vigoare la nivel național și se referă la condițiile de mediu, se pot obține de la Agenția Națională pentru Protecția Mediului sau de pe site-ul: http://www.anpm.ro/web/quest/legislatie.

- **Declarație privind partea/părțile din propunerea tehnica si financiara care au caracter confidențial**. Având în vedere prevederile art. 217 alin.(6) din Legea nr. 98/2016, operatorul economic trebuie sa elaboreze oferta în conformitate cu prevederile din documentația de atribuire si sa indice în cuprinsul acesteia, informațiile din cadrul documentelor de calificare, propunerii tehnice si/sau din propunerii financiare care sunt confidențiale, clasificate sau protejate de un drept de proprietate intelectuala. Caracterul confidențial trebuie demonstrat prin orice mijloace de proba.
- **Declarație prin care Ofertantul își asumă obligația de a prezenta toate informațiile/documentele solicitate** de către persoanele autorizate și/sau de către: autoritățile naționale cu atribuții de monitorizare, verificare, control și audit, serviciile Comisiei Europene, ale Curții Europene de Conturi, reprezentanții serviciului specializat al Comisiei Europene - Oficiul European pentru Lupta Antifraudă - OLAF, reprezentanții Departamentului pentru Lupta Antifraudă -DLAF. Accesul reprezentanților Comisiei Europene, Oficiului European pentru Lupta Antifraudă -OLAF sau Curții Europene de Conturi le va fi acordat cu respectarea regulii confidențialității, fără ca prin acest lucru să se încalce obligațiile de drept public ce îi revin Prestatorului, conform legii statului a cărui naționalitate o are. Declarația va confirma faptul că Ofertantul va permite accesul neîngrădit al persoanelor/instituțiilor mai sus menționate în cazul în care aceștia efectuează verificări/controale/audit la fața locului și solicita declarații, informații, documente, precum și ofițerului de proiect și/sau oricăror altor persoane desemnate de către Beneficiar, precum și personalului/agenților desemnați de instituțiile din România abilitate conform legii să deruleze astfel de verificări și controale.
- **Declarație privind respectarea aplicării principiului DNSH** pentru produsele ofertate.
- **Draft contract** asumat sau declarație privind acceptarea clauzelor contractuale.

Neprezentarea în cadrul ofertei a tuturor informațiilor solicitate în cadrul acestei secțiuni va face imposibilă evaluarea conformității ofertelor și se va considera o încălcare a cerințelor explicite ale Autorității contractante privind tratarea obligatorie a unor elemente de conținut din cadrul ofertei, ceea ce va conduce la respingerea ofertei.

Perioada de valabilitate a ofertelor: 90 de zile.

9.2 Oferta financiară

Oferta financiară va cuprinde prețul total ofertat, valoare fără TVA care se completează în sistemul electronic SEAP rubrica special dedicată „Oferta financiară", precum si următoarele documente.

I. Formularul de ofertă financiară;

II. Anexa la Formularul de Oferta;

III. Documentele de fundamentare a prețului, daca este cazul.

Ofertantul va include, în cadrul propunerii financiare, toate si orice costuri legate de: transport, ambalare, manipulare, montaj, punere în funcțiunea a produselor/echipamentelor, analiză, proiectare, customizare/dezvoltare soluție, testare si instruire a personalului autorității contractante.

Propunerea financiară are caracter obligatoriu, din punctul de vedere al conținutului pe toata perioada de valabilitate stabilita de către autoritatea contractanta si asumata de ofertant.

Cu excepția erorilor aritmetice, astfel cum sunt acestea definite la art. 134 alin. (10) din Anexa la H.G. nr. 395/2016/ art. 140 alin. (9) din Anexa la H.G. nr. 394/2016, nu vor fi permise alte omisiuni, necorelări sau ajustări ale propunerii financiare.

Reprezintă erori aritmetice, respectiv aspecte care pot fi clarificate cu respectarea principiilor prevăzute la art. 2 alin. (2) din Lege, elementele propunerii financiare urmând a fi corectate, implicit alături de prețul total al ofertei, prin refacerea calculelor aferente.

In vederea comparării unitare a ofertelor, se solicită ca toate preturile sa fie exprimate în cifre cu cel mult două zecimale.

10 Metodologia de evaluare a Ofertelor prezentate

10.1 Criteriu de atribuire

În cadrul prezentei proceduri de achiziție urmează să fie aplicat criteriul de atribuire **„cel mai bun raport calitate-preț"**, în conformitate cu prevederile art. 187 alin. (3), lit. C din legea nr. 98/2016 privind achizițiile publice, cu modificările și completările ulterioare.

ALGORITM DE CALCUL:

Evaluarea ofertelor se va face în ordinea descrescătoare a punctajului total obținut din punctajul tehnic și financiar, pe baza ponderilor prezentate în fișa de date a achiziției, pentru fiecare dintre criteriile respective.

Oferta care obține cel mai mare număr de puncte va fi declarată câștigătoare.

Evaluarea ofertelor se va realiza pe baza următoarelor criterii și a punctajul aferent obținut de fiecare ofertă evaluată.

Punctajul total acordat pentru fiecare ofertă se calculează pe baza formulei:

Punctaj Total Ofertant A = Punctaj „Prețul ofertei" Ofertant A + Punctaj „Propunerea tehnică - Experiența profesională a experților-cheie" Ofertant A + Punctaj „Propunerea tehnică - Demonstrarea unei metodologii adecvate de implementare a contractului, precum și o planificare adecvată a resurselor umane și a activităților" Ofertant A .

Criteriile de evaluare propuse sunt:

	Factori de evaluare	**Punctaj**
	Punctaj financiar	
1	FACTORUL DE EVALUARE 1: “Prețul ofertei (fără TVA)”	40
	Punctaj tehnic	
2	FACTORUL DE EVALUARE 2: “Experiența profesională a experților-cheie”	40
3	FACTORUL DE EVALUARE 3: “Demonstrarea unei metodologii adecvate de implementare a contractului, precum și o planificare adecvată a resurselor umane și a activităților”	20
TOTAL (puncte)		**100**

Toate calculele se vor face cu 4 zecimale, iar rotunjirile se vor face la 2 zecimale, conform funcției ROUND din Microsoft Excel – ROUND(formula, 2) - pentru fiecare din calculele aferente evaluării ofertelor. Funcția ROUND se va aplica pentru întreaga formulă de calcul, pentru fiecare etapă a calculului.

Punctajul tehnic total al ofertei se calculează prin însumarea punctajelor tehnice obținute în urma aplicării fiecărui sub-factor de evaluare. Punctajul aferent unui sub-factor de evaluare va fi obținut prin acordarea notei corespunzătoare calificativului obținut de oferta respectivă la evaluarea acelui sub-factor.

În conformitate cu prevederile art. 139 alin (3) din HG 395/2016 cu modificările si completările ulterioare, în cazul în care două sau mai multe oferte eligibile sunt clasate pe primul loc, cu punctaj total egal (tehnic + financiar), departajarea se va face având în vedere punctajul obținut la factorii de evaluare în ordinea descrescătoare a ponderilor acestora. În situația în care egalitatea se menține, autoritatea contractantă are dreptul să solicite noi propuneri financiare, iar oferta câștigătoare va fi desemnată cea cu propunerea financiară cea mai mică.

FACTORUL DE EVALUARE 1. Descrierea modalității de punctare a factorului de evaluare "Prețul ofertei"

Factor de evaluare	**Modalitate de punctare**	**Punctaj maxim**
1. Prețul ofertei	Punctajul financiar se acordă astfel: a. Pentru cel mai mic dintre preturile ofertate se acordă punctajul maxim alocat = 40 de puncte; b. Pentru alt preț decât cel prevăzut la litera a) se acordă punctaj astfel: **Punctaj Financiar Ofertant A = (Preț minim ofertat/ Preț Ofertant A)** x **40** Se vor compara preturile fără TVA prezentate în propunerea financiară.	**40 puncte** **(pondere 40%)**

FACTORUL DE EVALUARE 2. Descrierea modalității de punctare a factorului de evaluare "Propunerea tehnică - Experiența profesională a experților cheie"

Prin acest factor se va realiza evaluarea experienței profesionale a persoanelor propuse pentru anumite poziții de experți. Persoanele pentru care se va face evaluarea vor avea responsabilitatea realizării efective a activităților și proceselor de execuție aferente derulării contractului. Factorul de evaluare este Experiența profesionala a personalului ofertantului concretizata în numărul de proiecte în care personalul a îndeplinit sarcini similare.

Număr maxim de puncte: 40 (pondere 40%).

Acordarea punctajului „Experiența profesionala a experților-cheie" se va face în felul următor:

Expert cheie	Număr maxim de puncte
Factorul de evaluare „Experiența Manager de proiect"	5
Factorul de evaluare „Experiența Arhitect software – Full stack"	5
Factorul de evaluare „Experiența Analist de business"	5
Factorul de evaluare „Experiența Expert securitate informatică"	5
Factorul de evaluare „Experiența Dezvoltator software – Full Stuck"	5
Factorul de evaluare „Experiența Expert baze de date"	5
Factorul de evaluare „Tester software"	5
Factorul de evaluare „Instructor aplicații"	5
Total	**40**

Se va puncta numai Experiența similară superioară celei minim solicitate prin caietul de sarcini (1 proiect).

Punctajul aferent experienței persoanelor propuse ca experți-cheie se va acorda pentru fiecare în parte, astfel:

Manager de proiect: punctaj maxim acordat - 5 puncte

- pentru Experiența constând în implicarea între 2 și 3 proiecte sau contracte (in care a realizat activități similare celor pe care urmează să le îndeplinească în viitorul contract) a persoanei propuse se acordă 1 punct;
- pentru Experiența constând în implicarea între 4 și 5 proiecte sau contracte (in care a realizat activități similare celor pe care urmează să le îndeplinească în viitorul contract) a persoanei propuse - se acordă 3 puncte;
- pentru Experiența constând în implicarea în minim 6 proiecte sau contracte (in care a realizat activități similare celor pe care urmează să ie îndeplinească în viitorul contract) a persoanei propuse - se acordă 5 puncte.

Expert arhitect software - full stuck: punctaj maxim acordat - 5 puncte

- pentru Experiența constând în implicarea între 2 și 3 proiecte sau contracte (in care a realizat activități similare celor pe care urmează să le îndeplinească în viitorul contract) a persoanei propuse se acordă 1 punct;
- pentru Experiența constând în implicarea între 4 și 5 proiecte sau contracte (in care a realizat activități similare celor pe care urmează să le îndeplinească în viitorul contract) a persoanei propuse - se acordă 3 puncte;
- pentru Experiența constând în implicarea în minim 6 proiecte sau contracte (in care a realizat activități similare celor pe care urmează să ie îndeplinească în viitorul contract) a persoanei propuse - se acordă 5 puncte.

Expert analiză de business: punctaj maxim acordat - 5 puncte

- pentru Experiența constând în implicarea între 2 și 3 proiecte sau contracte (in care a realizat activități similare celor pe care urmează să le îndeplinească în viitorul contract) a persoanei propuse se acordă 1 punct;
- pentru Experiența constând în implicarea între 4 și 5 proiecte sau contracte (in care a realizat activități similare celor pe care urmează să le îndeplinească în viitorul contract) a persoanei propuse - se acordă 3 puncte;
- pentru Experiența constând în implicarea în minim 6 proiecte sau contracte (in care a realizat activități similare celor pe care urmează să ie îndeplinească în viitorul contract) a persoanei propuse - se acordă 5 puncte.

Expert securitate informatică: punctaj maxim acordat - 5 puncte

- pentru Experiența constând în implicarea între 2 și 3 proiecte sau contracte (in care a realizat activități similare celor pe care urmează să le îndeplinească în viitorul contract) a persoanei propuse se acordă 1 punct;
- pentru Experiența constând în implicarea între 4 și 5 proiecte sau contracte (in care a realizat activități similare celor pe care urmează să le îndeplinească în viitorul contract) a persoanei propuse - se acordă 3 puncte;
- pentru Experiența constând în implicarea în minim 6 proiecte sau contracte (in care a realizat activități similare celor pe care urmează să ie îndeplinească în viitorul contract) a persoanei propuse - se acordă 5 puncte.

Expert dezvoltare software – full stuck: punctaj maxim acordat - 5 puncte

- pentru Experiența constând în implicarea între 2 și 3 proiecte sau contracte (in care a realizat activități similare celor pe care urmează să le îndeplinească în viitorul contract) a persoanei propuse se acordă 1 punct;
- pentru Experiența constând în implicarea între 4 și 5 proiecte sau contracte (in care a realizat activități similare celor pe care urmează să le îndeplinească în viitorul contract) a persoanei propuse - se acordă 3 puncte;
- pentru Experiența constând în implicarea în minim 6 proiecte sau contracte (in care a realizat activități similare celor pe care urmează să ie îndeplinească în viitorul contract) a persoanei propuse - se acordă 5 puncte.

Expert baze de date: punctaj maxim acordat - 5 puncte

- pentru Experiența constând în implicarea între 2 și 3 proiecte sau contracte (in care a realizat activități similare celor pe care urmează să le îndeplinească în viitorul contract) a persoanei propuse se acordă 1 punct;
- pentru Experiența constând în implicarea între 4 și 5 proiecte sau contracte (in care a realizat activități similare celor pe care urmează să le îndeplinească în viitorul contract) a persoanei propuse - se acordă 3 puncte;

- pentru Experiența constând în implicarea în minim 6 proiecte sau contracte (in care a realizat activități similare celor pe care urmează să ie îndeplinească în viitorul contract) a persoanei propuse - se acordă 5 puncte.

Expert testare software: punctaj maxim acordat - 5 puncte

- pentru Experiența constând în implicarea între 2 și 3 proiecte sau contracte (in care a realizat activități similare celor pe care urmează să le îndeplinească în viitorul contract) a persoanei propuse se acordă 1 punct;
- pentru Experiența constând în implicarea între 4 și 5 proiecte sau contracte (in care a realizat activități similare celor pe care urmează să le îndeplinească în viitorul contract) a persoanei propuse - se acordă 3 puncte;
- pentru Experiența constând în implicarea în minim 6 proiecte sau contracte (in care a realizat activități similare celor pe care urmează să ie îndeplinească în viitorul contract) a persoanei propuse - se acordă 5 puncte.

Expert instruire: punctaj maxim acordat - 5 puncte

- pentru Experiența constând în implicarea între 2 și 3 proiecte sau contracte (in care a realizat activități similare celor pe care urmează să le îndeplinească în viitorul contract) a persoanei propuse se acordă 1 punct;
- pentru Experiența constând în implicarea între 4 și 5 proiecte sau contracte (in care a realizat activități similare celor pe care urmează să le îndeplinească în viitorul contract) a persoanei propuse - se acordă 3 puncte;
- pentru Experiența constând în implicarea în minim 6 proiecte sau contracte (in care a realizat activități similare celor pe care urmează să ie îndeplinească în viitorul contract) a persoanei propuse - se acordă 5 puncte.

Punctajul tehnic se va acorda numai experților care respectă cerințele tehnice minimale.

Nu va fi punctată Experiența profesionala a unor persoane propuse pe poziții de experți, suplimentar față de rolurile solicitate. Nu se vor indica mai multe persoane pentru același rol, considerându-se o ofertă alternativă.

Pentru demonstrarea experienței profesionale solicitate, Ofertanții trebuie sa prezinte în cadrul ofertei tehnice documente relevante cum ar fi: recomandări emise de beneficiarul final al proiectului, semnate sau contrasemnate de către autoritatea contractantă/beneficiarul privat în calitate de beneficiar final al proiectului, documente de proiect contrasemnate de beneficiarul final al proiectului, alte documente oficiale similare din care să reiasă informațiile solicitate.

Nu se vor lua în considerare proiectele implementate în cadrul organizației ofertantului și care au ca beneficiar final însuși ofertantul, ci doar acele proiecte implementate pentru instituții/beneficiari privați ca entități terțe, în baza unor contracte de furnizare/prestare de servicii similare.

Pentru fiecare document propus, se va prezenta o persoana de contact din partea beneficiarului final al proiectului (nume, poziție, adresa de mail, număr de telefon), în măsura sa confirme cele prezentate în recomandări (sau alte documente justificative relevante)sau aceste informații trebuie să reiasă din evaluarea documentului propus. Documentele de recomandare care nu dețin numele în clar, calitatea/poziția din cadrul organizației din postura în care semnează persoana respectivă documentul, precum și datele de identificare și de contact ale Autorității contractante/beneficiarului privat, nu vor fi luate în considerare.

In urma verificării exactității informațiilor și a dovezilor furnizate de către ofertanți, autoritatea contractantă poate solicita și alte documente/informații care să clarifice Experiența profesionala solicitata. De asemenea, autoritatea contractantă își rezerva dreptul de a contacta beneficiarii finali ai proiectelor prezentate la Experiența profesionala, în vedere confirmării celor prezentate de către ofertanți.

Punctajul va fi acordat numai pentru proiectele sau contractele pentru care documentele prezentate dovedesc Experiența similară solicitata pentru fiecare persoana propusa pentru o anumita poziție de expert.

Factorul de evaluare 3. Descrierea modalității de punctare a factorului de evaluare "Propunerea tehnică - Demonstrarea unei metodologii adecvate de implementare a contractului, precum și o planificare adecvată a resurselor umane și a activităților

Punctajul total maxim ce poate fi acordat pentru acest criteriu este de 20 puncte (pondere 20%), obținute prin însumarea punctajelor celor 3 subcriterii care sunt prezentate în continuare.

F3.1 Abordarea metodologica propusă pentru implementarea contractului		
Linii directoare: se va analiza informația furnizată în Formularul de propunere tehnica - secțiunea 2	Calificative	Punctaj
Abordarea propusă se bazează în mare măsură pe o serie de metodologii, metode și/sau instrumente testate, recunoscute și care demonstrează o foarte bună înțelegere a contextului, respectiv a particularității sarcinilor stabilite în caietul de sarcini, în corelație cu aspectele-cheie, precum si cu riscurile si ipotezele identificate.	foarte bine	8 pct
Abordarea propusa se bazează parțial pe metodologii, metode și/sau instrumente testate, recunoscute și care demonstrează înțelegerea contextului, respectiv a particularității sarcinilor stabilite în caietul de sarcini, în corelație cu aspectele-cheie, precum si cu riscurile și ipotezele identificate.	bine	4 pct
Abordarea propusă nu are la baza metodologii, metode și/sau instrumente testate, recunoscute și arată o înțelegere limitată a contextului, respectiv a particularității sarcinilor stabilite în caietul de sarcini.	acceptabil	1 pct
F3.2 Resursele (umane si materiale) și realizările corespunzătoare fiecărei activități, inclusiv atribuțiile membrilor echipei în implementarea activităților contractului		
Linii directoare: se va analiza informația furnizată în Formularul de propunere tehnică - secțiunea 3 și secțiunea 4.	Calificative	Punctaj
Resursele identificate și realizările indicate sunt deplin corelate cu complexitatea fiecărei activități propuse. Sunt indicate responsabilitățile în execuția contractului și interacțiunea între membrii echipei în cadrul tuturor etapelor implementării contractului și, dacă este cazul, distribuirea și interacțiunea sarcinilor și responsabilităților între operatorii din cadrul grupului. În abordarea metodologică propusă sunt indicate toate activitățile și sarcinile experților cheie și non-cheie implicați, interacțiunea între membrii echipei de experți, volumul de muncă estimat pe fiecare expert cheie și pe echipa de experți non-cheie, în relație cu activitățile prevăzute și sarcinile acestora, inclusiv cele referitoare la managementul contractului și activitățile suport.	foarte bine	6 pct
Resursele identificate și realizările indicate sunt parțial corelate cu complexitatea fiecărei activități propuse. Sunt indicate parțial responsabilitățile în execuția contractului și interacțiunea între membrii echipei în cadrul tuturor etapelor implementării contractului și, daca este cazul, distribuirea și interacțiunea sarcinilor și responsabilităților între operatorii economici din cadrul grupului. În abordarea metodologică propusă sunt indicate majoritatea activităților și sarcinile experților cheie și non-cheie implicați, interacțiunea între membrii echipei de experți, volumul de muncă estimat pe fiecare expert cheie și pe echipa de experți non-cheie, în relație cu activitățile prevăzute și sarcinile acestora, inclusiv cele referitoare la managementul contractului și activitățile suport.	bine	3 pct

Resursele identificate sau realizările indicate sunt corelate într-un mod limitat cu complexitatea activităților propuse. Sunt indicate în mod limitat responsabilitățile în execuția contractului sau interacțiunea între membrii echipei în cadrul tuturor etapelor implementării contractului și, dacă este cazul, distribuirea și interacțiunea sarcinilor și responsabilităților între operatorii economici din cadrul grupului. în abordarea metodologică propusă, sunt indicate în mod limitat/parțial activitățile și sarcinile experților cheie și non-cheie implicați, interacțiunea între membrii echipei de experți, volumul de muncă estimat pe fiecare expert cheie și pe echipa de experți non-cheie în relație cu activitățile prevăzute și sarcinile acestora, inclusiv cele referitoare la managementul contractului și activitățile suport.	acceptabil	1 pct
F3.3 încadrarea în timp, planificarea, succesiunea și durata activităților propuse		
Linii directoare: se va analiza informația furnizată în Formularul de propunere tehnica - secțiunea 3.	Calificative	Punctaj
Graficul de execuție este foarte detaliat și permite identificarea exactă a tuturor etapelor și a logicii activităților, sunt identificate toate jaloanele proiectului, este prezentată calea critică a proiectului și se prezintă măsurile care vor fi luate pentru protejarea duratei activităților de pe calea critică. Durata activităților corespunde deplin complexității acestora, iar succesiunea dintre acestea, inclusiv perioada de desfășurare, este stabilită în funcție de logica relației dintre acestea. Durata prevăzută pentru fiecare activitate necesară a ofertantului furnizor este corelată cu activitățile proiectului prevăzute a fi realizate în lunile respective și cu resursele identificate pentru desfășurarea acestora.	foarte bine	6 pct
Durata activităților corespunde parțial complexității acestora, iar succesiunea dintre acestea, inclusiv perioada de desfășurare este corelată doar parțial cu logica relației dintre acestea. Graficul de execuție este parțial detaliat, calea critică nu identifică întrutotul corect activitățile relevante ale proiectului, strategiile de minimizare a riscurilor care pot afecta durata activităților de pe calea critică sunt doar parțial relevante. Nu sunt identificate corect toate jaloanele proiectului. Durata prevăzută pentru fiecare activitate necesara a ofertantului furnizor este corelata parțial cu activitățile proiectului prevăzute a fi realizate în lunile respective și cu resursele estimate pentru desfășurarea acestora.	bine	3pct
Durata activităților corespunde în mică măsură complexității acestora sau succesiunea dintre acestea, inclusiv perioada de desfășurare, este stabilită într-un mod foarte puțin adecvat în raport cu logica relației dintre acestea sau durata prevăzută pentru fiecare operațiune principală necesară este corelată în mică măsură cu activitățile prevăzute a fi realizate în lunile respective și cu resursele estimate pentru desfășurarea acestora. Nu este identificată calea critică sau nu sunt detaliate activitățile care o compun sau nu sunt analizate strategiile de minimizare a riscurilor care pot afecta activitățile de pe calea critică.	acceptabil	1 pct

10.2 Alte prevederi

Toate cerințele din prezentul Caiet de sarcini sunt minimale și obligatorii. Specificațiile tehnice care indică o anumită origine, sursă, producție, un procedeu special, o marcă de fabrică sau de comerț, un brevet de invenție, o licență de fabricație, sunt menționate doar pentru identificarea cu ușurință a caracteristicilor produsului și NU au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor produse. Aceste specificații vor fi considerate ca având mențiunea de ”sau echivalent” iar ofertantul are obligația de a demonstra echivalența produselor ofertate cu cele solicitate (acolo unde este cazul).

Propunerea tehnică va fi însoțită de materialul documentar suport ce va dovedi caracteristicile fiecărui produs (de exemplu: file de catalog, desene, schițe, etc.) și va include o descriere detaliată a caracteristicilor/performanțelor acestuia. În Propunerea tehnică se va indica, dacă este cazul, adresa paginii web producătorului/ distribuitorului/ furnizorului pe care pot fi găsite caracteristicile produselor ofertate, și care să demonstreze îndeplinirea specificațiilor tehnice din Caietul de sarcini.

În vederea asigurării continuității soluției și independentei Beneficiarului fata de furnizori, se va avea în vedere respectarea următoarelor aspecte:

- Pentru toate aplicațiile dezvoltate specific pentru Beneficiar va fi livrat inclusiv codul sursă și documentația aferentă conform Art.12 din OUG 41/2016. Codurile sursă vor fi livrate în format editabil / prelucrabil;
- Drepturile de autor asupra soluțiilor și aplicațiilor software dezvoltate specific pentru Beneficiar vor fi transferate integral și vor deveni proprietatea acestuia, la recepția sistemului;
- Pachetele de licențe incluse în obiectul achiziției trebuie să asigure îndeplinirea cerințelor din cadrul prezentului caiet de sarcini.

Prin transmiterea unei oferte Ofertanții își asumă direct și explicit îndeplinirea în totalitate a cerințelor formulate de autoritatea contractantă în caietul de sarcini și respectarea acestora.

11 Cadrul legal care guvernează relația dintre Autoritatea Contractantă și Contractant

Contractantul trebuie să respecte toate prevederile legale, aplicabile la nivel național, dar și regulamentele aplicabile la nivelul Uniunii Europene (acolo unde se impune).

Pe perioada realizării tuturor activităților din cadrul Contractului, Contractantul este responsabil pentru implementarea celor mai bune practici, în conformitate cu legislația și regulamentele existente la nivel național și la nivelul Uniunii Europene. Contractantul va fi ținut deplin responsabil pentru subcontractanții săi în furnizarea produselor si realizarea operațiunilor cu titlu accesoriu prevăzute în Caietul de Sarcini, urmând să răspundă față de Autoritatea Contractantă, pentru orice nerespectare sau omisiune a respectării oricăror prevederi legale și normative aplicabile. Autoritatea Contractantă nu va fi ținută responsabilă pentru nerespectarea sau omisiunea respectării de către Contractant sau de către subcontractanții acestuia a oricărei prevederi legale sau a oricărui act normativ aplicabil precum și atât pentru furnizarea produselor cât și pentru rezultatele generate de furnizarea produselor.

În cazul în care intervin schimbări legislative, Contractantul are obligația de a informa Autoritatea Contractantă cu privire la consecințele asupra activităților care fac obiectul Contractului și de a-și adapta activitatea în funcție de decizia Autorității Contractante în legătură cu schimbările legislative.

11.1 Obligații aplicabile în domeniul mediului, social și al muncii

Ofertantul devenit Contractant are obligația de a respecta în executarea Contractului, obligațiile aplicabile în domeniul mediului, social și al muncii instituite prin dreptul Uniunii, prin dreptul național, prin acorduri colective sau prin dispozițiile internaționale de drept în domeniul mediului, social și al muncii enumerate în anexa X la Directiva 2014/24, respectiv:

- Convenția nr. 87 a OIM privind libertatea de asociere și protecția dreptului de organizare;
- Convenția nr. 98 a OIM privind dreptul de organizare și negociere colectivă;
- Convenția nr. 29 a OIM privind munca forțată;
- Convenția nr. 105 a OIM privind abolirea muncii forțate;
- Convenția nr. 138 a OIM privind vârsta minimă de încadrare în muncă;
- Convenția nr. 111 a OIM privind discriminarea (ocuparea forței de muncă și profesie);
- Convenția nr. 100 a OIM privind egalitatea remunerației;
- Convenția nr. 182 a OIM privind cele mai grave forme ale muncii copiilor;
- Convenția de la Viena privind protecția stratului de ozon și Protocolul său de la Montreal privind substanțele care epuizează stratul de ozon;
- Convenția de la Basel privind controlul circulației transfrontaliere a deșeurilor periculoase și al eliminării acestora (Convenția de la Basel);
- Convenția de la Stockholm privind poluanții organici persistenți (Convenția de la Stockholm privind POP);

- Convenția de la Rotterdam privind procedura de consimțământ prealabil în cunoștință de cauză, aplicabilă anumitor produși chimici periculoși și pesticide care fac obiectul comerțului internațional (UNEP/FAO) (Convenția PIC), 10 septembrie 1998, și cele trei protocoale regionale ale sale.

Actele normative și standardele indicate mai sus sunt considerate indicative și nelimitative; enumerarea actelor normative din acest capitol este oferită ca referință și nu trebuie considerată limitativă.

11.2 Organizare și funcționare

- Constituția României: http://legislatie.just.ro/Public/DetaliiDocument/47355
- ORDONANȚĂ DE URGENȚĂ nr. 57/2019 privind Codul administrativ: http://legislatie.just.ro/Public/DetaliiDocument/28009
- Legea nr.188/1999 privind statutul funcționarilor publici, republicată, cu modificările și completările ulterioare: http://legislatie.just.ro/Public/DetaliiDocument/20173
- Legea nr.7/2004 privind Codul de conduită a funcționarilor publici, cu modificările și completările ulterioare: http://legislatie.just.ro/Public/DetaliiDocument/49915
- Legea nr.393/2004 privind statutul aleșilor locali, cu modificările și completările ulterioare: http://legislatie.just.ro/Public/DetaliiDocument/55664
- OUG 21/2004 privind Sistemul National de Management al Situațiilor de Urgență, cu modificările și completările ulterioare:http://legislatie.just.ro/Public/DetaliiDocument/51410
- Legea nr.481/2004 privind protecția civilă, republicată: http://legislatie.just.ro/Public/DetaliiDocument/95836
- Legea nr.52/2003 privind transparența decizională în administrația publică: http://legislatie.just.ro/Public/DetaliiDocument/153210
- Legea nr.24/2000 republicată (r2), privind normele de tehnică legislativă pentru publicarea actelor normative, modificată și completată: http://legislatie.just.ro/Public/DetaliiDocument/118116
- Codul civil al României aprobat prin Legeanr.287/2009: http://legislatie.just.ro/Public/DetaliiDocumentAfis/205332
- Legea nr.50/1991 privind autorizarea executării lucrărilor de construcții: http://legislatie.just.ro/Public/DetaliiDocument/55794
- Legea nr.416/2001 privind venitul minim garantat: http://legislatie.just.ro/Public/DetaliiDocument/29731
- Legea nr.98/2016 privind achizițiile publice: http://legislatie.just.ro/Public/DetaliiDocument/178667
- Legea nr.333/2003 cu privire la paza obiectivelor, bunurilor, valorilor și protecția persoanelor: http://legislatie.just.ro/Public/DetaliiDocument/156432

- Legea nr.176/2010 privind integritatea în exercitarea funcțiilor și demnităților publice, pentru modificarea și completarea Legii nr.144/2007 privind înființarea, organizarea și funcționarea Agenției Naționale de Integritate, precum și pentru modificarea și completarea altor acte normative: http://legislatie.just.ro/Public/DetaliiDocument/201185
- Legea nr.161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției: http://legislatie.just.ro/Public/DetaliiDocument/43323#id_artA511
- Legea fondului funciar nr.18/1991 republicată, modificată și completată:http://legislatie.just.ro/Public/DetaliiDocument/203359
- OG nr.28/2008 privind registrul agricol, modificată și completată: http://legislatie.just.ro/Public/DetaliiDocument/96993
- Legea nr. 145/2014 pentru stabilirea unor masuri de reglementare a pieței produselor din sectorul agricol: http://legislatie.just.ro/Public/DetaliiDocument/162616
- Legea nr.17/2014 privind unele măsuri de reglementare a vânzării-cumpărării terenurilor agricole situate în extravilan și de modificare a Legii nr. 268/2001 privind privatizarea societăților comerciale ce dețin în administrare terenuri proprietate publică și privată a statului cu destinație agricolă și înființarea Agenției Domeniilor Statului: http://legislatie.just.ro/Public/DetaliiDocument/156290
- Legea nr.190/2018 privind masuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European si al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal si privind libera circulație a acestor date si de abrogare a Directivei 95/46/CE: http://legislatie.just.ro/Public/DetaliiDocument/203151

11.3 Acte normative cu impact asupra activității

- Legea nr. 544/2001 privind liberul acces la informațiile de interes public, cu modificările și completările ulterioare: http://legislatie.just.ro/Public/DetaliiDocument/31413
- Hotărârea nr. 123/2002 de aprobare a Normelor metodologice de aplicare a Legii nr. 544/2001 privind liberul acces la informațiile de interes public: https://legislatie.just.ro/Public/DetaliiDocument/34416
- O.G. nr. 27/2002 privind reglementarea activității de soluționare a petițiilor: https://legislatie.just.ro/Public/DetaliiDocument/33817
- Ordonanța Guvernului nr. 27/2002 privind reglementarea activității de soluționare a etițiilor: http://legislatie.just.ro/Public/DetaliiDocument/33817
- Ordonanța Guvernului nr.80/2003 privind concediul de odihnă anual și alte concedii ale președinților și vicepreședinților consiliilor județene, precum și ale primarilor și viceprimarilor, cu modificările și completările ulterioare: http://legislatie.just.ro/Public/DetaliiDocument/45932

- Hotărârea Guvernului nr. 432/2004 privind dosarul profesional al funcționarilor publici: http://legislatie.just.ro/Public/DetaliiDocument/51282
- Hotărârea Guvernului nr. 905/2017 privind registrul general de evidență a salariaților: http://legislatie.just.ro/Public/DetaliiDocument/195770
- Hotărârea Guvernului nr.250/1992 privind concediul de odihnă și alte concedii ale salariaților din administrația publică, din regiile autonome cu specific deosebit și din unitățile bugetare, republicată, cu modificările și completările ulterioare: http://legislatie.just.ro/Public/DetaliiDocument/2566
- Ordinul nr.289/147/7325/2017/437/1136/2018/1588/2017/2018 din 17 august 2017 privind aprobarea Normelor tehnice de completare a registrului agricol pentru perioada 2015 – 2019: http://legislatie.just.ro/Public/DetaliiDocument/196888

11.4 Organizare servicii publice oferite cetățenilor

- Legea nr. 9 din 2023 pentru modificarea si completarea Ordonanței de Urgentă a Guvernului nr. 41/2016 privind stabilirea unor masuri de simplificare la nivelul administrației publice centrale si pentru modificarea si completarea unor acte normative: https://legislatie.just.ro/Public/DetaliiDocument/263706
- Legea nr. 242 din 20 iulie 2022 privind schimbul de date intre sisteme informatice si crearea platformei naționale de interoperabilitate: https://legislatie.just.ro/Public/DetaliiDocumentAfis/257856
- Legea nr. 179 din 2022 privind datele deschise si reutilizarea informațiilor din sectorul public
- Ordonanța de Urgenta nr. 38 din 30 martie 2020 privind utilizarea înscrisurilor în forma electronică la nivelul autorităților si instituțiilor publice: https://legislatie.just.ro/Public/DetaliiDocumentAfis/256414
- Ordonanța de Urgenta nr. 39 din 2020 pentru completarea Legii nr. 455 din 2001 privind semnătura electronică: https://legislatie.just.ro/Public/DetaliiDocumentAfis/224645
- Hotărârea Guvernului nr. 922 din 2010 privind organizarea si funcționarea Punctului de Contact Unic Electronic: https://legislatie.just.ro/Public/DetaliiDocumentAfis/122181
- Legea nr. 350 din 6 iulie 2001 privind amenajarea teritoriului și urbanismul: https://legislatie.just.ro/Public/DetaliiDocumentAfis/29453
- Legea-CADRU nr. 195 din 22 mai 2006 a descentralizării: https://legislatie.just.ro/Public/DetaliiDocumentAfis/72024
- Legea nr. 101 din 25 aprilie 2006 (*republicată*) serviciului de salubrizare a localităților: https://legislatie.just.ro/Public/DetaliiDocument/71304
- Legea nr. 241 din 22 iunie 2006 (*republicată*)privind serviciul de alimentare cu apă și de canalizare: https://legislatie.just.ro/Public/DetaliiDocument/73044
- Legea nr. 325 din 14 iulie 2006 (*republicată*)serviciului public de alimentare cu energie termică: https://legislatie.just.ro/Public/DetaliiDocument/73837
- Legea nr. 230 din 7 iunie 2006 a serviciului de iluminat public: https://legislatie.just.ro/Public/DetaliiDocument/72642

- Legea nr. 92 din 10 aprilie 2007 serviciilor publice de transport persoane în unitățile administrativ-teritoriale: https://legislatie.just.ro/Public/DetaliiDocument/81267
- Legea nr. 92 din 10 aprilie 2007 serviciilor publice de transport persoane în unitățile administrativ-teritoriale: https://legislatie.just.ro/Public/DetaliiDocument/81267
- Legea nr. 155 din 12 iulie 2010 - Legea poliției locale: https://legislatie.just.ro/Public/DetaliiDocumentAfis/120615
- Legea nr. 292 din 20 decembrie 2011 - Legea asistenței sociale: https://legislatie.just.ro/Public/DetaliiDocumentAfis/133913

11.5Achiziții publice

- Legea privind achizițiile publice nr. 98/2016, cu modificările și completările ulterioare: https://legislatie.just.ro/Public/DetaliiDocument/178667
- Legea privind remediile si căile de atac in materie de atribuire a contractelor de achiziție publica a contractelor sectoriale si a contractelor de concesiune de lucrări si concesiune de servicii, precum si pentru organizarea si funcționarea Consiliului de Soluționare a Contestațiilor nr. 101/2016: https://legislatie.just.ro/Public/DetaliiDocument/178680
- Normele metodologice de aplicare a prevederilor referitoare la atribuirea contractului de achiziție publică /acordului cadru din Legea 98/2016 privind achizițiile publice HG nr. 395/2016: https://legislatie.just.ro/Public/DetaliiDocument/179009
- www.anap.gov.ro;
- Alte acte normative, standarde si norme tehnice specifice in vigoare.

Notă privind respectarea legislației în domeniul protecției datelor cu caracter personal, inclusiv a directivei GDPR:

Toate sistemele de aplicații software ofertate și care vor fi implementate vor furniza toate funcționalitățile care să permită respectarea cerințelor și exigențelor legislației în domeniul protecției datelor cu caracter personal, inclusiv ale directivei GDPR.

Ofertanții vor descrie în mod obligatoriu în cadrul ofertelor tehnice, sub sancțiunea respingerii acestora, funcționalitățile de ordin tehnic ale produselor ofertate care implementează cerințele Directivei GDPR, în principal respectarea principiilor „privacy by design" și „privacy by default", precum și implementarea de mecanisme tehnice care să asigure respectarea drepturilor persoanelor vizate sub aspectul protecției datelor cu caracter personal.

Verificat,

Direcția Economică, Achiziții, Investiții, Patrimoniu și Proiecte Fonduri Nerambursabile

Director/Manager Proiect, Alexandru-Bogdan DRAGOMIR

Întocmit,

Paul TUDOSE, S.C. PERFORM SOFT DEVELOPMENT S.R.L.