Aprobat,
Președinte
Cătălin RAIU

Semnatar: Raiu Catalin-Valentin
Data si ora semnarii: 2026.03.10 12:56:02 +0200

CAIET DE SARCINI

pentru Implementarea ”Sistemului Informatic Integrat pentru Servicii Publice de Combatere a discriminării (SIISPECD)” în cadrul proiectului „Sistem Informatic Integrat pentru Servicii Publice Electronice de Combatere a Discriminării (SIISPECD)”, Cod SMIS 335331.

Cuprins

1. Introducere 6

2. Contextul realizării acestei achiziții 6

2.1. Informații despre beneficiar 6
2.2. Informații despre contextul care a determinat achiziția 8
2.3. Informații despre beneficiile anticipate de către beneficiar 8
2.4. Factori interesați și rolul acestora, dacă este cazul 9
2.5. Obiectivele generale și specifice ale proiectului 9

3. Obiectul contractului 10

4. Descrierea situației actuale la nivelul beneficiarului 10

5. Cerințe privind soluția tehnică solicitată 12

5.1. Cerințe generale 12
5.2. Prevederi de securitate 15
5.3. Cerințele funcționale ale sistemului 17
5.3.1. Cerințe funcționale privind managementul documentelor 17
5.3.2. Cerințe funcționale privind gestiunea solicitărilor de acces la informații de interes public 21
5.3.3. Cerințe funcționale privind gestiunea petițiilor și autosesizărilor 23
5.3.4. Cerințe funcționale privind avizarea de legalitate a documentelor 25
5.3.5. Cerințe funcționale privind întocmirea și avizarea proiectelor de acte normative 25
5.3.6. Cerințe funcționale privind reprezentarea în instanță și expertizare judiciară 26
5.3.7. Cerințe funcționale privind Portalul de Servicii Electronice Publice (PSEP) 26
5.3.8. Cerințe funcționale privind sistemul de management al documentelor 31
5.4. Arhitectura funcțională a sistemului 33
5.4.1. Arhitectura logică a SIISPECD 33
5.4.2. Arhitectura fizică SIISPECD 36
5.4.3. Compunerea infrastructurii de comunicații, terminale, management și Securitate a SIISPECD 39
5.4.4. Interoperabilitate 40
5.4.5. Performanța sistemului 41
5.5. Securitatea sistemului 42
5.6. Confidențialitatea datelor 43
5.7. Cerințe hardware și software de infrastructură 43
5.7.1. Echipament WAN 43
5.7.2. Switch Agregare LAN 47
5.7.3. Echipamente extindere rețea locală prin acces WiFi 50
5.7.4. Scaner registratură 56
5.7.5. Scaner arhivă 57
5.7.6. Computere de birou 58
5.7.7. Computere portabile 66

5.7.8. Sistem de videoconferință 73
5.7.9. Aplicație de administrare centralizată a infrastructurii de rețea 85
5.7.10. Aplicație de administrare centralizată a stațiilor de lucru 86
5.7.11. Software de realizare a copiilor de siguranță 89
5.7.12. Actualizarea soluției software existente de gestiune și securizare a accesului 92
5.7.13. Software de jurnalizare de audit 92
5.7.14. Pachet BYOL CPG Azure Hub Stack 98
5.8. Cerințe software 104
5.8.1. Platforma de dezvoltare și administrare aplicații web (LCAP) 104
5.8.2. Platforma de managementul documentelor 115
5.8.3. Software de gestiune a bazelor de date relaționale 134
5.8.4. Platforma software de videoconferință 135
5.8.5. Platforma software de transcriere audio în text 137
5.9. Cerințe privind serviciile 138
5.9.1. Livrarea, instalarea și configurarea echipamentelor 138
5.9.2. Livrarea, instalarea și configurarea produse software 139
5.9.3. Analiză și proiectare 140
5.9.4. Implementare 142
5.9.5. Instruire 144
5.9.6. Punerea în producție 153
5.9.7. Servicii de asigurare a securității cibernetice a rețelei și sistemului informatic 153
5.9.8. Graficul de prestare al serviciilor 156

6. Cerințe privind garanția și suportul tehnic 157

6.1. Garanția echipamentelor 157
6.2. Suportul tehnic pentru produsele software 158
6.3. Servicii de mentenanță a SIISPECD 158
6.3.1. Descrierea generală a serviciilor de mentenanță solicitate 159
6.3.2. Definirea şi prezentarea modelului general de prestare al serviciilor 159
6.3.3. Serviciile de suport Nivel 1 - Centrul de suport unic 160
6.3.4. Serviciile de suport Nivel 2 – Servicii de mentenanță preventivă și analiză a performanței 163
6.3.5. Serviciile de suport Nivel 3 – Servicii de mentenanță corectivă și evolutivă 165
6.3.6. Nivelul de asigurare a serviciilor (SLA) 167
6.3.7. Abordarea serviciilor de mentenanță evolutivă 171
6.3.8. Raportare 172
6.4. Predare sistem 173
6.5. Cerințele generale predare coduri sursă 174

7. Locul și durata desfășurării activităților 174

7.1. Locul desfășurării activităților 174
7.2. Durata contractului 175

8. Resurse umane necesare/expertiza necesară pentru realizarea activităților contractului și obținerea rezultatelor 175

8.1. Experți cheie solicitați pe categorie de expertiză 175
8.1.1. Expert cheie nr. 1: Manager de proiect 176
8.1.2. Expert cheie nr. 2: Arhitect de sistem 177
8.1.3. Expert cheie nr. 3: Analist Coordonator 178
8.1.4. Expert cheie nr. 4: Expert îmbunătățire procese de business 178
8.1.5. Expert cheie nr. 5: Expert coordonator dezvoltare aplicații web 179
8.1.6. Expert cheie nr. 6: Expert coordonator implementare sistem de management documente 180
8.1.7. Expert cheie nr. 7: Expert coordonator testare 181
8.1.8. Expert cheie nr. 8: Coordonator instruire pentru utilizare și administrare 182
8.1.9. Expert cheie nr. 9: Expert stocare și protecție copii de siguranță 183
8.2. Alte condiții referitoare la calificarea experților 184
8.2.1. Personalul administrativ și personalul suport/backstopping pentru activitatea experților cheie în cadrul Contractului 185
8.2.2. Alte cerințe legate de personalul direct implicat în prestarea serviciilor 185
8.2.3. Infrastructura Contractantului necesară pentru desfășurarea activităților Contractului 186
8.2.4. Infrastructura și resursele disponibile la nivel de Autoritate Contractantă pentru îndeplinirea Contractului 187
9. Cadrul legal care guvernează relația dintre Autoritatea Contractantă și Contractant (inclusiv în domeniile mediului, social și al relațiilor de muncă) 187
10. Managementul/Gestionarea Contractului și activități de raportare în cadrul Contractului 188
10.1. Plan de livrare produse și prestări servicii 188
10.2. Abordare și metodologie în cadrul Contractului 189
10.2.1. Organizarea 189
10.2.2. Monitorizare și control 189
10.2.3. Registrul riscurilor 189
10.3. Atribuțiile și responsabilitățile părților 189
10.4. Gestionarea relației dintre Contractant și Achizitor 191
10.5. Raportarea în cadrul contractului 191
10.6. Evaluarea performanței Contractantului 192
11. Recepția produselor și serviciilor 193
11.1. Recepția produselor 193
11.2. Recepția serviciilor 194
12. Modalități și condiții de plată 195
13. Metodologia de evaluare a Ofertelor prezentate 196
13.1. Modul de prezentare al ofertelor tehnice 196
13.2. Aplicarea criteriului de atribuire 204
13.2.1. Factor de evaluare 1 - Valoarea propunerii financiare, fără TVA 205
13.2.2. Factor de evaluare 2 - Experiența personalului desemnat pentru executarea

contractului 205
13.2.3. Factor de evaluare 3 - Demonstrarea unei abordări, înțelegeri și metodologii adecvate pentru implementarea contractului, precum și o planificare adecvată a resurselor umane și a activităților 209
13.2.4. Factor de evaluare 4 – Specificații tehnice extinse pentru echipamente 213
13.2.5. Factor de evaluare 5 – Criterii ecologice privind echipamentele care au impact asupra mediului pe durata întregului ciclu de viaţă 214

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 furnizarea produselor și prestarea serviciilor care fac obiectul Contractului ce rezultă din această procedură.
În cadrul acestei proceduri, **Consiliul Național pentru Combaterea Discriminării**, îndeplinește rolul de Autoritate Contractantă, respectiv Achizitor în cadrul Contractului.
Pentru scopul prezentei secțiuni a Documentației de Atribuire, orice activitate descrisă întrun 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.
Acolo unde sunt menționate produse de o anumită origine, sursa, producție, un procedeu special, o marca de fabrica sau de comerț, un brevet de invenție, o licență de fabricație, se citește "sau echivalent". Aceste specificații 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 tipului de produs și NU au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor produse din cadrul procedurii.
Ofertanții trebuie să răspundă integral cerințelor minime incluse în Caietul de sarcini și întro formă care nu limitează aria sau serviciile solicitate.
În acest sens, orice ofertă prezentată care se abate de la prevederile Caietului de sarcini, va fi luată în considerare numai în măsura în care Propunerea Tehnică presupune asigurarea unui nivel calitativ superior cerințelor minime obligatorii din Caietul de sarcini.
În cadrul prezentei achiziții, produsele si materialele încorporate ce vor fi furnizate trebuie să fie noi și nefolosite. De asemenea, vor fi oferite cele mai recente modele. Produsele și materialele încorporate ce vor fi furnizate ar trebui să încorporeze cele mai recente îmbunătățiri în proiectare și materiale.
Nu se admit oferte parțiale din punct de vedere cantitativ și calitativ, ci numai oferte integrale, care corespund tuturor cerințelor minime stabilite prin prezentul Caiet de sarcini.

2. Contextul realizării acestei achiziții

2.1. Informații despre beneficiar

Consiliul Național pentru Combaterea Discriminării (denumită în continuare “CNCD și “beneficiar”) este organizată și funcționează în temeiul Hotărârii Guvernului nr.1194 din 2001 privind organizarea și funcţionarea Consiliului Naţional pentru Combaterea Discriminării.
Consiliul Național pentru Combaterea Discriminării este autoritatea de stat autonomă, sub control parlamentar, care își desfașoară activitatea în domeniul discriminării. Este garant al respectării și aplicării principiului nediscriminării, în conformitate cu legislația internă în vigoare și cu documentele internaționale la care România este parte.
CNCD își exercită atribuțiile în următoarele domenii:

- Prevenirea faptelor de discriminare prin realizarea de campanii de informare, de conștientizare privind drepturile omului, efectele discriminării, principiul egalității, cursuri de formare, de informare, proiecte și programe la nivel local, regional și național, realizarea de studii, rapoarte etc.;
- Medierea faptelor de discriminare a părților implicate în cazul de discriminare, în prezența reprezentanților Consiliului Național pentru Combaterea Discriminării. Consiliul Național pentru Combaterea Discriminării urmărește reducerea și eliminarea faptelor de discriminare și nicidecum să aplice amenzi.
- Investigarea, constatarea și sancționarea faptelor de discriminare. Pentru analizarea cât mai corectă a cazurilor și pentru luarea deciziilor în cazul petițiilor primite sau autosesizărilor, Colegiul Director dispune de măsuri pentru a investiga cazurile, în urma cărora acesta constată existența sau nu a faptei de discriminare și după caz, sancționarea acesteia.
- Monitorizarea cazurilor de discriminare în urma constatării unor cazuri de discriminare de către CNCD, prin supravegherea ulterioară a părților implicate.
- Acordarea de asistență de specialitate victimelor discriminării prin explicarea legislației celor interesați de către consilierii juridici ai CNCD, prin îndrumarea asistată în ceea ce privește activitatea de depunere a petiției și informații suplimentare ce decurg din această procedură.
- Cadrul legal care reglementează înființarea, organizarea și funcționarea CNCD:
- Ordonanţa Guvernului nr. 137/2000 privind prevenirea și sancționarea tuturor formelor de discriminare, republicată, cu modificările și completările ulterioare;
- Hotărârea Guvernului nr.1194 din 2001 privind organizarea și funcţionarea Consiliului Naţional pentru Combaterea Discriminării.
- Ordinul Președintelui CNCD nr. 27 din 7 februarie 2024 privind aprobarea Procedurii interne de soluționare a petițiilor și sesizărilor
- Ordonanţa Guvernului nr. 27/2002 privind reglementarea activităţii de soluţionare a petiţiilor;
- Legea nr. 233/2002 pentru aprobarea Ordonanţei Guvernului nr. 27/2002 privind reglementarea activităţii de soluţionare a petiţiilor;
- Legea 544/2001 privind liberul acces la informaţiile de interes public.
- Legea nr. 514/2003 privind organizarea și exercitarea profesiei de consilier juridic, actualizată
- H.G. 561/2009 pentru aprobarea Regulamentului privind procedurile, la nivelul Guvernului, pentru elaborarea, avizarea si prezentarea proiectelor de documente de politici publice, a proiectelor de acte normative, precum si a altor documente, in vederea adoptării/ aprobării.
- Regulament de organizare și funcționare al Consiliului Național pentru Combaterea Discriminării – Anexă la Ordinul Președintelui CNCD nr. 225 din 23 August 2023 .

2.2. Informații despre contextul care a determinat achiziția

Conform analizei efectuate la nivelul instituției, funcționarii implicați în furnizarea serviciilor publice de combaterea discriminării, se confruntă cu următoarele situații:

- gestionarea unui număr mare de dosare - încărcarea suplimentara a angajaților generata de multe activități redundante care sunt gestionate manual datorita absenței unor sisteme/ instrumente/aplicații specifice care să permită diminuarea timpilor morți și a activităților care nu aduc o reala valoare adăugată;
- în situația primirii de formulare completate electronic, prin email, nu exista nicio metoda de a prelua automat datele din formulare și de a le transfera în aplicațiile back-office, fiind deci necesară reintroducerea manuală a datelor din formulare;
- arhivarea documentelor se realizează prin metode tradiționale, cu dificultățile aferente în situațiile în care este necesară consultarea arhivei fizice;
- imposibilitatea de automatizare a proceselor repetitive, datorata lipsei de sisteme/instrumente/ aplicații specifice, ce consuma o parte importantă din activitatea funcționarilor, care ar trebui sa se concentreze mai mult pe activități specifice cu semnificativa valoare adăugată;
- imposibilitatea de a asigura servicii de prevenire a faptelor de discriminare prin realizarea de cursuri de formare privind drepturile omului, efectele discriminării, principiul egalității, datorită lipsei de personal și a mijloacelor tehnice necesare.

De asemenea, exista mulți beneficiari ai serviciilor publice de combaterea discriminării care nu au domiciliul în București, dar trebuie să interacționeze cu instituția pentru constatarea și sancționarea faptelor de discriminare.

Toate aceste realități impun nevoia de a îmbunătăți accesul cetățenilor la informație și de a pune la dispoziție servicii electronice.

În concluzie, prin intermediul Programului Creștere Inteligentă, Digitalizare și Instrumente Financiare 2021-2027 (PCIDIF), Măsura 1: Servicii publice destinate cetățenilor și/sau firmelor identificate în CSP gestionat de ADR și/sau în concordață cu Politica eGuv, Acțiunea 2.2 Eguvernarea și digitalizarea în beneficiul cetățenilor - 2.2.1: E-guv în administrația/instituțiile publice, **CNCD își propune să digitalizeze procesele de activitate aferente serviciilor publice de combatere a discriminării** în următoarele domenii:

a. prevenirea faptelor de discriminare;
b. medierea faptelor de discriminare;
c. investigarea, constatarea și sancționarea faptelor de discriminare;
d. monitorizarea cazurilor de discriminare;
e. acordarea de asistență de specialitate victimelor discriminării.

În acest sens este nevoie de achiziționarea unui Sistem Informatic Integrat pentru Servicii Publice Electronice pentru Combaterea Discriminării (în continuare denumit prescurtat ”SIISPECD”).

2.3. Informații despre beneficiile anticipate de către beneficiar

Beneficiile implementării Sistemului Informatic Integrat pentru Servicii Publice de Combatere a

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

discriminării (SIISPECD) constau în optimizarea proceselor de lucru în cadrul Consiliului Național pentru Combaterea Discriminării, pentru reducerea timpului de procesare a sesizărilor și a petițiilor privind acte sau fapte de discriminare și pentru asigurarea accesului online la serviciile publice de combatere a discriminării.

Pentru a produce schimbări majore în indicatorii de performanță este nevoie de digitalizarea fluxurilor de lucru de bază din cadrul CNCD, în scopul eficientizării proceselor de activitate specifice, evitării întreruperilor ce pot apărea în fluxurile informaționale ale instituției, reducând astfel întârzierile în prestarea serviciilor publice de combatere a discriminării, precum și asigurarea accesului online la acestea pentru beneficiari.

Astfel, beneficiile anticipate de către CNCD sunt:

- creșterea gradului/nivelului de transparența privind activitatea instituției;
- creșterea eficienței în gestionarea proceselor interne de lucru în cadrul CNCD;
- creșterea productivității individuale a funcționarilor SPCD;
- diminuarea costurilor operaționale;
- îmbunătățirea procesului de luare a deciziilor;
- optimizarea proceselor de interacțiune cu beneficiari ai serviciilor de combatere a discriminării;
- creșterea performanțelor instituționale.

2.4. Factori interesați și rolul acestora, dacă este cazul

Factorii interesați în implementarea Contractului sunt:

- Consiliul Național pentru Combaterea Discriminării în calitate de beneficiar al finanțării;
- Angajații din Consiliul Național pentru Combaterea Discriminării care vor utiliza SIISPECD;
- Cetățenii, organizațiile non-guvernamentale, instanțele și instituțiile publice beneficiari ai serviciilor de combatere a discriminării prestate de CNCD.

2.5. Obiectivele generale și specifice ale proiectului

Obiectivul general al proiectului este digitalizarea serviciilor de combatere a discriminării pentru beneficiarii Consiliului Național pentru Combaterea Discriminării (CNCD prin optimizarea proceselor de activitate.

Obiectivele specifice ale proiectului sunt:

1. Implementarea unor procese de digitalizare a serviciilor publice de combatere a discriminării.
2. Adaptarea resurselor umane CNCD la noile procese digitale prin dezvoltarea competențelor în TIC.

Obiectivul general și obiectivele specifice ale proiectului vor fi îndeplinite prin implementarea ”la cheie” a unui Sistem Informatic Integrat pentru Servicii Publice Electronice de Combatere a

Discriminării (SIISPECD) în cadrul Consiliului Național pentru Combaterea Discriminării, prin:

- Furnizare de Echipamente, în conformitate cu cerințele din prezentul document.
- Furnizarea de Licențe software, în conformitate cu cerințele din prezentul document;
- Prestarea de Servicii IT, în conformitate cu cerințele din prezentul document;
- Prestarea de Servicii de instruire, în conformitate cu cerințele din prezentul document.

3. Obiectul contractului

Prin intermediul contractului care va fi atribuit prin prezenta procedură de achiziție publică, se va realiza implementarea „la cheie” a unui Sistem Informatic Integrat pentru Servicii Publice Electronice de Combatere a Discriminării (SIISPECD) în cadrul Consiliului Național pentru Combaterea Discriminării, prin:

- Furnizare de Echipamente, în conformitate cu cerințele din prezentul document.
- Furnizarea de Licențe software, în conformitate cu cerințele din prezentul document;
- Prestarea de Servicii IT, în conformitate cu cerințele din prezentul document;
- Prestarea de Servicii de instruire, în conformitate cu cerințele din prezentul document.

4. Descrierea situației actuale la nivelul beneficiarului

În prezent, CNCD dispune de o infrastructură hardware și software de bază precară și uzată moral. Instituția nu dispune de aplicații dedicate aferente serviciilor publice de combaterea discriminării, software-ul de aplicație comercial existent fiind următorul:

- Program de legislație – Indaco Lege5, varianta de rețea, 1 licență
- Sistem informatic integrat financiar contabil și de gestiune pentru instituții bugetare SIMEC (CTCE), 1 licență
- Aplicație pentru calcularea și administrarea salariilor SALARII (CTCE), 1 licență

Toate aplicațiile sunt în mentenanță evolutivă iar instituția nu deține codul sursă.
Instituția nu utilizează baze de date relaționale sau sisteme de management ale acestora.
Conectarea la internet este realizată prin fibră optică iar furnizorul de servicii de acces la internet este Serviciul de Telecomunicații Speciale (STS). Viteza maximă a conexiunii este de 1 Gbps.
CNCD dispune a un singur server (Dell PowerEdge T110 II, Intel Xeon E3-1220 V2 @3.10 GHz), instalat din anul 2019, servind ca mediu de stocare pentru fișiere, respectiv programul de legislație (Indaco Lege5). Sistemul de operare al serverului este Windows Server 2016 Standard, pentru care Microsoft mai asigură suport până în Ianuarie 2027 doar pentru vulnerabilități de securitate. 10
Atât serverul cât și echipamentele principale de rețea (router-ul de instituție, switch-ul principal și centrala telefonică) dispun de UPS-uri care le asigură o funcționare de 15 minute.
Nu există echipamente de tip SAN/NAS instalate, serverul îndeplinind și funcția de stocare de fișiere.
Nu există o procedură elaborată pentru realizarea copiilor de siguranță și recuperarea în caz de

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

dezastru. Nu se realizează copii de siguranță ale datelor, cu excepția anumitor fișiere de pe serverul instituției, ale căror duplicate (copii) sunt salvate (manual) pe un HDD suplimentar instalat tot pe server.
Volumul stocat aferent fișierelor cu documentele înregistrate pe serverul de fișiere este de aproximativ 200 Gb.
Instituția nu deține echipamente de tip Firewall/Gateway
Instituția nu deține echipamente de tip Firewall de aplicații WEB
Instituția nu dispune de o cameră dedicată a serverelor.
CNCD dispune de cablare structurată, o rețea cu 140 de prize RJ45 cat. 5e duble (Internet/telefonie) și un număr de 7 patch panel-uri.
Rutarea în cadrul rețelei LAN a instituției se realizează printr-un echipament TP-Link ER7206 Omada Gigabit Multi-WAN VPN Router, cu o vechime în exploatare de aproximativ 3 ani.
Echipamentele active de rețea sunt următoarele:

- Cisco SG220-50, gigabit, 50 de porturi
- Zyxel GS1900-24, gigabit, 24 de porturi
- Zyxel ES-1124, megabit, 24 de porturi
- Zyxel GS1100-16, gigabit, 16 porturi
- TP-Link TL-SG1008D, gigabit, 8 porturi (2 echipamente)
- Cisco SG-1110D-08, gigabit, 8 porturi (2 echipamente)
- Cisco SG-110D-05, gigabit, 5 porturi (2 echipamente)
- TP-Link TL-SG105, gigabit, 5 porturi (3 echipamente)
- Netgear GS305E, gigabit, 5 porturi (2 echipamente)

CNCD dispune de 9 echipamente de tip multifuncțională de rețea:

- Canon iR2630i - 1 echipament
- Canon iR2530i – 2 echipamente
- Canon iR1435i – 3 echipamente
- Minolta Bizhub 284e - 2 echipamente
- Minolta Bizhub - 1 echipament

Echipamentele sunt folosite pentru copiere, scanare și imprimare de documente și au o vechime cuprinsă între 2-7 ani.
CNCD dispune de 2 echipamente de tip scanner:

- Canon DR-C225
- Canon DR-M140

Echipamentele sunt folosite pentru scanarea și prelucrarea de documente și au o vechime cuprinsă între 5-7 ani.
CNCD dispune de 65 echipamente de tip Desktop PC cu monitor în stare de funcționare. Din cele 65 calculatoare, 14 rulează versiuni vechi de OS (Microsoft Windows 7 Pro), iar 47 dintre ele utilizează suita Office (Micorsoft Oficce 2013 sau mai veche), introducându-se astfel în instituție vulnerabilăți la amenințări cibernetice sau neputând asigura nivelul adecvate de securitate a datelor.

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

CNCD dispune de doar 2 echipamente de tip laptop (ASUS VivoBook 15" A1504ZA cu procesor Intel® Core™ i3-1215U până la 4.4 GHz, 8GB RAM, 256GB SSD) și 2 echipamente de tip tabletă (Samsung Galaxy Tab A7 Lite Lenovo P10).
Relația CNCD cu beneficiarii este caracterizată, în general, de proceduri complexe, fluxuri ale documentelor în format letric și termene din ce în ce mai lungi de rezolvare.
Pentru funcționarii instituției implicați în furnizarea serviciilor publice, principalele situații cu care se confruntă și care se doresc a fi eliminate sau ameliorate în urma implementării proiectului sunt următoarele:

- gestionarea unui număr mare de dosare - încărcarea suplimentara a angajaților generata de multe activități redundante care sunt gestionate manual datorita absenței unor sisteme/ instrumente/aplicații specifice care să permită diminuarea timpilor morți și a activităților care nu aduc o reala valoare adăugată;
- în situația primirii de formulare completate electronic, prin email, nu exista nicio metoda de a prelua automat datele din formulare și de a le transfera în aplicațiile back-office, fiind deci necesară reintroducerea manuală a datelor din formulare;
- arhivarea documentelor se realizează prin metode tradiționale, cu dificultățile aferente în situațiile în care este necesară consultarea arhivei fizice;
- imposibilitatea de automatizare a proceselor repetitive, datorata lipsei de sisteme/instrumente/ aplicații specifice, ce consuma o parte importantă din activitatea funcționarilor, care ar trebui sa se concentreze mai mult pe activități specifice cu semnificativa valoare adăugată.

De asemenea, exista mulți beneficiari ai serviciilor publice de combaterea discriminării care nu au domiciliul în București, dar trebuie sa interacționeze cu instituția pentru constatarea și sancționarea faptelor de discriminare.
Toate aceste realități impun nevoia de a îmbunătăți accesul cetățenilor la informație și de a pune la dispoziție servicii electronice.

5. Cerințe privind soluția tehnică solicitată

5.1. Cerințe generale

Sistemul Informatic Integrat pentru Servicii Publice de Combatere a discriminării (SIISPECD) se va implementa în Cloudul Privat Guvernamental (CPG), unitatea de Cloud Dedicat bazată pe tehnologia Azure Hub Stack și va fi dezvoltat pe baza componentelor software solicitate prin prezentul document și prezentate în capitolele 5.7 și 5.8, astfel încât să se îndeplinească cerințele funcționale prezentate în capitolul 5.3 în vederea digitalizării serviciilor publice de combatere a discriminării pentru cetățeni, cu respectarea cerințelor privind arhitectura sistemului din capitolul 5.4 și cele privind performanța sistemului din capitolul 5.4.5.

Sistemul va fi proiectat astfel încât să acopere obiectivele Beneficiarului, atât din punct de vedere al finanțării cât și a cadrului legislativ ce guvernează activitatea acestuia realizat utilizând standarde

deschise și în linie cu cadrul național de interoperabilitate, scalabil și înalt disponibil.
Sistemul se va implementa în Cloudul Privat Guvernamental (CPG), unitatea de Cloud Dedicat bazată pe tehnologia Azure Hub Stack, care va asigura infrastructura de mașini virtuale/containere necesară, precum și soluția de disaster recovery întrun centru de date diferit de cel de producție.
La proiectarea, realizarea și implementarea SIISPECD trebuie să se țină cont de respectarea următoarele principii generale:

a. *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. Sistemul informatic propus nu va include nici o caracteristică ce este incompatibilă cu legislația națională în vigoare și a normelor și standardelor internaționale recunoscute în domeniu.

b. Principiul divizării arhitecturii pe niveluri: constă în proiectarea independentă a componentelor sistemului în conformitate cu standardele de interfață dintre nivele. Arhitectura sistemului va fi organizată pe 3 niveluri, respectiv:

- Nivel prezentare
- Nivel aplicativ și integrare
- Nivel de date

c. Principiul arhitecturii bazate pe servicii (SOA): constă în distribuirea funcționalității platformelor software în unități mai mici, distincte - numite servicii - care pot fi distribuite întro rețea și pot fi utilizate împreună pentru a crea aplicații destinate implementării funcțiilor de business ale sistemului informatic. Soluția propusă pentru SIISPECD va dispune de o arhitectură deschisă, va respecta cerințele de scalabilitate și interoperabilitate și va fi bazată pe standarde și protocoale de comunicație deschise, bazate pe tehnologie SOA.

d. Principiul datelor sigure: stipulează introducerea datelor în sistem doar prin canalele autorizate și autentificate. Componentele sistemului din zona privată vor implementa facilități de securizare a accesului la date bazat pe autentificarea si autorizarea utilizatorilor prin intermediul soluției Active Directory implementată în cadrul CNCD și actualizată prin prezentul proiect.

e. Principiul securității informaționale: presupune asigurarea unui nivel adecvat de integritate, selectivitate, accesibilitate și eficiență pentru protecția datelor de pierderi, alterări, deteriorări și de acces nesancționat.

f. Principiul transparenței: presupune proiectarea și realizarea conform principiului modular, cu utilizarea standardelor transparente în domeniul tehnologiilor informatice și de telecomunicații. Datorită arhitecturii SOA și protocoalelor deschise publice acestor servicii, coroborat cu descrierea prin intermediul descriptorilor WSDL a semnăturii funcțiilor oferite de fiecare serviciu web, devine transparenta modalitatea prin care SIISPECD va realiza integrarea cu sisteme externe, indiferent de limbajele de implementare și platformele pe care rulează acestea, singurele constrângeri fiind doar cele de logica impuse de operarea cu funcțiile SIISPECD.

g. Principiul expansibilității: stipulează posibilitatea extinderii și completării sistemului informatic cu noi funcții sau îmbunătățirea celor existente. SIISPECD va fi construit pe o arhitectură

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

scalabilă şi centralizată, care va răspunde eventualelor cerințe de dezvoltări ulterioare. De asemenea, va fi extensibil prin crearea unei arhitecturi modulare, cu posibilități de extindere a funcționalităților, interfețelor sau a opțiunilor, care va permite integrarea de API-uri sau de noi componente, în vederea extinderii funcționalităților.

h. Principiul scalabilității: presupune asigurarea unei performanțe constante a SIISPECD la creșterea volumului de date și a solicitării sistemului informatic. Prin arhitectura să modularizată, SIISPECD va suporta scalabilitate atât pe verticală cât şi pe orizontală, atât în totalitatea lui cât şi selectiv, la nivelul anumitor componente a căror selecție poate fi efectuată pe parcursul utilizării sistemului în funcție de necesitățile punctuale. Soluția va avea un grad mare de parametrizare şi va face față independent la modificările de structura organizatorică şi de proces din partea beneficiarului. Sistemul informatic, cu toate componentele sale va fi dezvoltat pe tehnologie web, pe o platformă modernă, suficient de flexibilă încât să permită, în cazul în care va fi necesar, încorporarea cu minim de efort a eventualelor schimbări şi a modurilor diferite de interpretare a acestora.

i. Principiul ”Once only” presupune că: odată ce o instituție a statului a preluat sau creat date despre cetățean sau companie, nicio altă instituție a statului nu mai are voie să le ceară;
o informație existentă deja în cadrul sistemului informatic al CNCD să fie accesată în mod direct de către utilizatori sau alte aplicații/sisteme informatice, fără a fi necesară implicarea cetățeanului.

j. 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. Soluția va oferi utilizatorului un mediu de lucru facil și o interfață de prezentare sugestivă, ce se va distinge prin capabilități de navigare ușor de folosit, claritate în gruparea și separarea elementelor, afișarea unui meniu de acțiuni dinamic în funcție de contextul curent și permisiunile utilizatorului.

k. 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. Menținerea integrității datelor sistemului va fi realizată printr-un cumul de componente și acțiuni după cu urmează:

- Controlul acțiunilor asupra datelor - toate componentele SIISPECD vor fi integrate cu soluția de gestiune și securizare a accesului Active Directory implementată în cadrul CNCD astfel încât să fie realizat un control robust, unitar și de nivel sporit de granularitate astfel încât să fie eliminate acțiunile intenționate sau neintenționate, neautorizate de alterare a conținutului;
- Jurnal de audit - Orice acțiune menită să altereze starea datelor sistemului este înregistrată sub formă de jurnal de audit. Pe baza acestuia, în situații excepționale, poate fi refăcută starea anterioară a înregistrării alterate.

Jurnalul de audit este consultabil de către utilizatori cu rol de administrator din cadrul sistemului:

- Jurnalizarea Operațiunilor Utilizatorilor: Toate acțiunile realizate de către utilizatori în cadrul sistemului trebuie să fie înregistrate întrun jurnal de activități. Informațiile înregistrate trebuie să includă, dar să nu se limiteze la, data și ora operațiunii, utilizatorul care a efectuat operațiunea, natura acțiunii (ex. creare, modificare, ștergere), și detaliile relevante asociate acțiunii.
- Jurnalizarea Accesului: Orice încercare de acces la sistem, reușită sau nereușită, trebuie să fie înregistrată în jurnalul de acces. Detaliile înregistrate ar trebui să includă, dar să nu se limiteze la, IP-ul utilizatorului, tipul de acces (autentificare, autorizare), rezultatul accesului (reușit, eșuat), și orice alte informații relevante.
- Jurnalizarea Erorilor de Sistem: Orice eroare sau excepție generată de sistem trebuie să fie înregistrată întrun jurnal dedicat erorilor de sistem. Informațiile înregistrate ar trebui să includă, dar să nu se limiteze la, data și ora erorii, natura erorii (ex. eroare de autentificare, eroare de acces la bază de date), și orice alte detalii relevante care pot ajuta la diagnosticarea și remedierea erorii.
- Formatul și Retenția Jurnalelor: Jurnalele trebuie să fie păstrate întrun format sigur și nealterabil pentru o perioadă specificată de timp, conform cerințelor legale și de conformitate. Toate jurnalele trebuie să fie ușor accesibile pentru administrare și auditare, iar informațiile să poată fi extrase și interpretate eficient.

5.2. Prevederi de securitate

Sistemul Informatic Integrat pentru Servicii Publice Electronice de Combatere a Discriminării (SIISPECD) va fi proiectat pentru a asigura conformitatea deplină cu Regulamentul (UE) 2016/679 privind protecția datelor cu caracter personal (GDPR), în special în contextul prelucrării datelor sensibile, precum cele referitoare la originea rasială sau etnică. Măsurile tehnice și organizatorice detaliate în prezentul capitolvor fi implementate pentru a garanta confidențialitatea, integritatea și disponibilitatea datelor, respectând principiile GDPR de minimizare a datelor, limitare a scopului și securitate a prelucrării. Aceste prevederi asigură protecția drepturilor și libertăților persoanelor vizate, aliniind SIISPECD cu cerințele legale și cu obiectivele Consiliului Național pentru Combaterea Discriminării (CNCD) ca operator de date.

În cadrul sistemului vor trebui să fie implementate măsuri de securitate care să faciliteze implementarea unor politici de securitate, conform cerințelor Regulamentului General privind Protecția Datelor (GDPR), cel puțin referitoare la:

- Securitate adecvată – protecția împotriva prelucrării neautorizate sau ilegale, împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin măsuri tehnice sau organizatorice;

- Protecția datelor cu caracter personal care dezvăluie originea rasială sau etnică, confesiunea religioasă şi prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice;
- Pseudonimizare și criptare – prelucrarea datelor cu caracter personal în zona de testare întrun asemenea mod încât acestea să nu mai poată fi atribuite unei anumite persoane vizată, fără a se utiliza informații suplimentare;
- Capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;
- Capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
- Un proces pentru testarea, evaluarea și aprecierea periodică a eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării;

O caracteristică esențială este conceptul de „data protection by design și by default” în sensul implementării de soluții și măsuri tehnice de securitate adecvate la momentul implementării mijloacelor și modalităților de prelucrare a datelor cu caracter personal.
Implementarea unui proiect de o asemenea anvergură și complexitate impune următoarele politici de securitate, în funcție de nivelul logic, astfel:

- La nivel de server, se vor folosi sisteme de virtualizare sau partiționare astfel încât mașinile virtuale/partițiile să poată fi utilizate similar serverelor fizice, în sensul că se va permite comunicarea între două mașini virtuale/partiții doar prin canalele special definite în acest scop;
- La nivel de comunicații, prin folosirea tehnicilor specifice de izolare a traficului;
- La nivel de aplicație, prin logarea tuturor activităților efectuate asupra datelor.
- În cadrul proiectului se va asigura că sunt implementate minim urmatoarele principii:
- abordarea securității prin concepție pentru a asigura securitatea modulelor și a infrastructurii lor complete;
- că serviciile nu sunt vulnerabile la atacurile care ar putea să le întrerupă funcționarea și ar putea provoca furtul sau deteriorarea datelor;
- utilizarea unor servicii calificate de asigurare a încrederii în conformitate cu regulamentul eIDAS pentru a asigura integritatea, autenticitatea, confidențialitatea și nerepudierea datelor.

Datorită riscului ridicat asociat prelucrării datelor cu caracter personal sensibile în cadrul SIISPECD, furnizorul va sprijini realizarea unei Evaluări a Impactului asupra Protecției Datelor (DPIA), conform Articolului 35 din GDPR. Aceasta va implica identificarea și evaluarea riscurilor pentru drepturile și libertățile persoanelor vizate, generate de operațiunile de prelucrare, și propunerea de măsuri tehnice suplimentare pentru mitigarea acestora, complementare celor specificate în prezentul capitol, dacă este cazul. DPIA va fi elaborată în colaborare cu beneficiarul, pentru a asigura conformitatea cu cerințele legale și compatibilitatea cu arhitectura sistemului

implementat în Cloudul Privat Guvernamental, și va fi supusă, dacă este cazul, consultării Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP).

5.3. Cerințele funcționale ale sistemului

5.3.1. Cerințe funcționale privind managementul documentelor

SIISPECD va permite factorilor de interes externi CNCD cu acces la dispozitive electronice de tip calculator, mobil etc să se autentifice și să depună documente principale (cum ar fi cererea, reclamația, sesizarea, propunerea etc) prin intermediul unui formular electronic, precum și să atașeze alte documente anexe, justificative aflate în format electronic direct în Portalul de Servicii Electronice Publice (PSEP) al CNCD. Acesta va prelua datele și documentele introduse și le va transfera automat sistemului intern de management a documentelor (DMS). În cazul depunerii documentelor prin alt mijloc legal - poștă, email etc, soluția va permite introducerea informațiilor privitoare la factorul de interes extern și conținutul documentului principal în DMS de către angajatul responsabil cu activitatea de Registratură, angajat care va scana eventualele documente fizice și le va atașa la documentul principal.

SIISPECD va permite realizarea activitatilor de înregistrare a petiţiilor, a documentelor oficiale şi a oricăror alte documente în sistemul de management al documentelor DMS de către angajatul responsabil cu activitatea de registratură precum și repartizarea acestora în cadrul instituției, în funcţie de obiectul de activitate, sau către diferite alte instituţii în a căror sferă de competenţă intră problematica din cuprinsul lor;

SIISPECD va asigura evidenţa petiţiilor repartizate pe compartimentele din instituție urmărind soluţionarea acestora în termenul legal.

SIISPECD va permite administrarea numerelor de inregistrare in cadrul institutiei, respectiv se va implementa în cadrul sistemului DMS, posibilitatea de gestiune, definire si alocare de către un utilizator cu drepturi stabilite de administrare a unei plaje de numere per Compartiment / Proiect la începutul anului. Orientativ, alocarea numerelor de înregistrare se realiza in conform modelului:

- Secretariat: 1 – 10.000
- DJ – Citații: 10.001 – 18.500
- DJ – Achiziții: 18.501 – 20.250

SIISPECD va permite stocarea, inregistrarea si distribuirea documentelor in cadrul institutiei, respectiv se va implementa urmatorul set de cerinte / functionalitati:

- Soluția va permite stocarea, înregistrarea si distribuirea Petițiilor depuse fizic personal, prin intermediul Poștei Romane, Poștei Militare sau prin mijloace electronice precum email sau client Active Fax.
- Documentele primite vor fi scanate daca sunt primite in format fizic si încărcate in Sistem completând meta datele necesare in cadrul unor formulare prestabilite. Înregistrarea petițiilor se va realiza cronologic, in ordinea primirii acestora, in aceeași zi in care au fost primite.

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

- Documentele primite vor fi înregistrate electronic in Registrul intrări / ieșiri al Serviciului Comunicare, Secretariat și Relații cu Publicul (SCRSRP) sau in Registrul
- Compartimentului responsabil in funcție de caz. Câmpurile (minime) utilizate in cadrul Registrului de intrări / ieșiri sunt enumerate mai după cum urmează: Menționarea numărului la care a fost înregistrat documentul;
    - Data înregistrării;
    - Nr. și data cu care emitentul a expediat documentul în cauză;
    - Nr. total al filelor documentului;
    - Nr. anexelor documentului;
    - Emitentul;
    - Conținutul documentului în rezumat;
    - Menționarea Compartimentului căruia i-a fost repartizată lucrarea;
    - Data expedierii;
    - Modul rezolvării;
    - Destinatar;
    - Nr. de înregistrare la care se conexează și indicativul dosarului după nomenclator;
    - Observații.
- Documentele vor putea fi înregistrate în Sistem în funcție de rolul acestora, după caz: informare, analiză, solicitare, sinteză, fundamentare a politicilor, programelor și proiectelor din domeniu.
- În funcție de caz, respectiv flux, anumite documente vor putea fi înregistrate de către solicitant în cadrul Portalului de Servicii Electronice Publice (PSEP) sau de către funcționarul responsabil în sistemul DMS (în situația în care solicitantul nu are posibilitatea de a utiliza un cont în Portal).
- Soluția va permite gestionarea următoarelor tipologii de documente în cadrul fluxurilor implementate:
    - Corespondenta externă:
        - Petiții / solicitări / puncte de vedere / invitații în formă electronică - internet (support@cncd.ro, contact.cncd@gmail.com);
        - Petiții / solicitări / puncte de vedere / invitații / facturi, transmise prin poștă sau fax sau depuse personal la sediul instituției.
    - Corespondenta internă:
        - Note de fundamentare, alte documente emise de către departamentele instituție;
        - Registrul special de înregistrare a documentelor care intră și ies din instituție (registru intrări / ieșiri);
        - Condică de corespondență a fiecărui departament.

- Soluția va permite salvarea borderourilor scanate ce conțin corespondenta plicurilor returnate si a confirmărilor de primire, borderouri aferente Poștei Romane sau Poștei Militare. După scanare si stocare, acestea vor fi distribuite fără a primi număr de înregistrare către Serviciul Asistenta Colegiul Director (SACD). In scop informativ, un set al câmpurilor aferente borderourilor se poate regăsi mai jos după cum urmează:
    - Poșta Română
        - Data;
        - Nr. Crt;
        - Felul trimiterii;
        - Subunitatea e prezentare;
        - Număr de prezentare;
        - Servicii suplimentare;
        - Destinatar;
        - Semnătura de primire;
        - Calitatea primitorului (grad de rudenie, delegat, etc.).
    - Poșta Militară:
        - Expeditor;
        - Destinatar;
        - Serie;
        - Nr. Borderou;
        - Data;
        - Nr. crt;
        - Destinatar;
        - Nr. de înregistrare al corespondentei si nr. anexelor;
        - Semnătura;
        - Ora;
        - Întocmit / Primit (Nume, Prenume, Semnătura).
- Soluția va permite scanarea și stocarea citațiilor emise de către instanțele de judecată (primite prin intermediul Poștei Romane) și distribuirea acestora către Direcția Juridică, compartiment care va furniza numărul de înregistrare utilizând registrul propriu.
- Soluția va permite înregistrarea facturilor în Registrul Intrări / Ieșiri și transmiterea acestora către Direcția Juridică corelând informațiile cu Condica de corespondență.
- Soluția va permite utilizarea Registrului de Intrări / Ieșiri și de către direcțiile care nu dețin un registru propriu de înregistrare. Registrele electronice vor respecta următoarele cerințe de business:
    - În situația răspunsurilor la solicitări ce au fost deja înregistrate se va utiliza același număr de înregistrare realizând corelarea între documente.

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

- În situația documentelor emise de către Serviciul Asistentă Colegiul Director (SACD) se va identifica dacă este primul răspuns către petentul din dosar realizând corelarea între documente.
- În situația în care este emisa prima adresa adresată petentului, aceasta primește același număr de înregistrare (data curenta) cu cel alocat petiției sale realizând corelarea în registru cu înregistrările anterioare.
- În situația primei adrese către reclamant sau alta persoana / instituție din dosar se va atribui un număr în ordine cronologică.
- În situația primei adrese către petent, se vor popula câmpurile („Data expedierii”, „Modul rezolvării’, „Destinatar”, „Nr. de înregistrare la care se conexează și indicativul dosarului după nomenclator”) din Registrul de intrări / ieșiri. Aceeași situație se aplică și în cazul adreselor primite din exterior și a celor la care vor răspunde alte departamente din cadrul instituției.
- În situația documentelor cu circuit intern, pentru direcțiile / serviciile ce nu dețin registru propriu, se va atribui număr de înregistrare, apoi se vor corela electronic întro maniera similara Condicii de Corespondență a direcției / serviciului către care este adresat documentul, condica ce conține (minimal) următoarele câmpuri in momentul de fata:
  - Număr document din registrul de intrare – ieșire;
  - Nume persoana;
  - Semnătura;
  - Termen de realizare a lucrării.
- În situația documentelor ce au fost repartizate și înregistrate în mod eronat la un alt departament, redirecționarea documentului / petiției de la un departament la altul se va face pe baza Condicii de Corespondență pe care fiecare structură organizatorică o va deține electronic in cadrul Sistemului. Departamentul care a redirecționat in sistem un document spre un alt departament va notifica tot prin intermediul sistemului Secretariatul care va face aceasta mențiune în rubrica „Observații” din Registrul de Intrare-Ieșire.

- Soluția va permite definirea termenelor legale de soluționare a documentelor în cadrul fluxurilor documentelor. În acest scop se vor implementa notificările necesare persoanelor implicate.

SIISPECD va permite directionarea pe fluxul electronic al documentelor în funcție de responsabili, stabilirea rezolutiilor și generarea documentelor de răspuns, respectiv se va implementa urmatorul set de cerințe / funcționalități:

- Soluția va permite transmiterea documentelor înregistrate în ”mapa electronică” a Președintelui sau în absenta acestuia către Secretarul General si Vicepreședinte.
- Soluția va permite configurarea și definirea responsabililor pe fluxul electronic al documentelor.
- Soluția va permite utilizarea semnăturilor electronice în avizarea documentelor pe flux.

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

- Soluția va permite stabilirea rezoluțiilor pe fluxul electronic.

SIISPECD va permite preluarea pe fluxul electronic al documentelor cu rezolutie în funcție de responsabilii configurați, respectiv se va implementa următorul set de cerințe / funcționalități:

- Soluția va permite direcționarea documentelor cu rezoluție către responsabili din cadrul instituției pe flux, realizând corelarea cu condica de corespondenta electronica a departamentului / serviciului către care a fost direcționat prin rezoluție spre rezolvare.
- Documentele interne din „mapa” electronică a Președintelui care necesitau doar semnătura acestuia în calitate de reprezentant al instituției se vor direcționa pe flux persoanei emitente fără a mai fi trecute în condica de corespondență electronică a departamentului respectiv.

SIISPECD va permite elaborarea, înregistrarea și transmiterea răspunsului către instituția / persoana în cauza, respectiv se va implementa următorul set de cerințe / funcționalitați:

- Documentul de răspuns va primi același număr de ieșire cu care a fost înregistrat inițial în Registrul intrări / ieșiri electronic, dar cu data curentă închizându-se numărul respectiv. În cazul adreselor noi emise de instituție se va aloca un număr de ieșire nou cu menționarea destinatarului, de asemenea.
- Sistemul va notifica persoanele implicate.

SIISPECD va permite corelarea informatiilor înregistrate electronic cu Arhiva fizică a Instituției.

- Sistemul va permite corelarea documentației înregistrata in sistem cu Arhiva fizica a Instituției.
- Sistemul va permite păstrarea trasabilității și a istoricului în cadrul circuitului electronic al documentelor.

Registraturile electronice vor respecta cerințele menționate mai sus, detalii concrete ale modalității prin care acestea vor fi implementate urmează a fi detaliate în etapa de analiză și proiectare din cadrul proiectului.

5.3.2. Cerințe funcționale privind gestiunea solicitărilor de acces la informații de interes public

SIISPECD va permite primirea, înregistrarea și transmiterea solicitărilor de informații de interes public către departamentele cu atribuții în soluționarea solicitărilor de la persoane fizice, persoane juridice, instituții publice.

Sintetizat, SIISPECD va permite:

- Înregistrarea de intrare a documentelor și a anexelor aferente solicitărilor informațiilor de interes public;
- Transmiterea acestora pe flux în funcție de responsabili;
- Elaborarea documentelor de răspuns și transmiterea acestora prin metode electronice;
- Elaborarea reclamațiilor administrative de către solicitanți și înregistrarea acestora;
- Stabilirea rezolutiilor utilizand semnaturi electronice;

- Elaborarea răspunsurilor la reclamații de către responsabili și transmiterea acestora către solicitant;
- Arhivarea (corelarea cu Arhiva fizica), păstrarea trasabilitații și istoricul documentației pe fluxul electronic în Sistem.

SIISPECD va permite solicitantului să se autentifice în sistem și să depună solicitarea de informații de interes public în cadrul unui formular (Cererea de informații de interes public) precum și alte documente justificative prin intermediul Portalului de Servicii Electronice Publice (PSEP), care va prelua solicitarea electronica și o va transfera sistemului interne de management a documentelor (DMS). În cazul depunerii solicitarilor prin alte mijloace (solicitari formulate în scris, pe suport de hârtie sau pe suport electronic (e-mail)), soluția va permite introducerea informațiilor privitoare la solicitant și conținutul solicitarii în DMS de către angajatul responsabil cu activitatea de Registratură SCSRP, angajat care va scana eventualele documente fizice și le va atașa la documentul principal. Sistemul va permite in acest caz generarea, printarea si eliberarea catre solicitant a unei confirmari scrise conţinând data şi numărul de înregistrare a solicitarii.

SIISPECD va permite înregistrarea solicitării de informații de interes public în Registrul electronic de corespondență din DMS de către Secretariat precum si in Registrul pentru înregistrarea cererilor si răspunsurilor privind accesul la informațiile de interes public fiind urmata de direcționarea automată a acesteia către următorul actor pe fluxul de lucru, respectiv responsabilul L544/2001 sau compartimentul vizat. În cazul în care solicitarea a fost introdusă prin intermediul PSEP, atunci sistemul DMS va transmite solicitantului în contul său confirmarea înregistrării. Registrul pentru înregistrarea cererilor si răspunsurilor privind accesul la informațiile de interes public conține (minimal) următoarele câmpuri:

- Nr. si data cererii;
- Numele si prenumele solicitantului;
- Informațiile solicitate;
- Răspunsul (Valori: Da, acces liber / Termen de 30 de zile / Trimis la ..... (alta instituție) / Nu, informație exceptată / Nu, informație inexistentă);
- Nr. si data răspunsului;

SIISPECD va permite responsabilului L544/2001 formularea răspunsului la solicitarea adresată CNCD în termen de 10 zile, solicitantul primind informațiile in cadrul sistemului PSEP:

- În situația in care solicitarea de informații de interes public are în vedere una din informațiile de interes public comunicate din oficiu, responsabilul L544/2001 va indica în răspunsul electronic elaborat in DMS locul unde se află informația solicitată și posibilitatea de a o consulta la sediul instituției sau pe site-ul oficial al acesteia.
- În situația in care solicitarea de informații de interes public are ca obiect una din informațiile exceptate de la accesul liber al cetățenilor responsabilul L544/2001 va formula răspunsul în sensul că informația nu poate fi furnizată întrucât este exceptată de la comunicare.

- În situația în care cererea de informații de interes public este respinsă, solicitantul poate face o reclamație administrativă prin completarea unui formular electronic ce va fi prevăzut în cadrul sistemului PSEP:

SIISPECD va permite ca reclamațiile administrative să poată fi înregistrate în DMS și alocate Președintelui CNSC în vederea dispunerii rezoluției de reanalizare. În cadrul sistemului DMS, Președintele dispune rezoluția de reanalizare urmând realocarea automată către responsabilul inițial căruia i-a fost repartizată reclamația.
SIISPECD va permite ca persoană responsabilă căreia i-a fost repartizată reclamația să poată să completeze electronic formularul și transmite răspunsul privind modul de soluționare în cadrul Sistemului DMS (Răspuns la reclamație), solicitantul fiind notificat prin intermediul sistemului PSEP și având posibilitatea de a descarca răspunsul.
Modulul va respecta cerințele menționate mai sus, detalii concrete ale modalității prin care acestea vor fi implementate urmează a fi detaliate în etapa de analiză și proiectare din cadrul proiectului.

5.3.3. Cerințe funcționale privind gestiunea petițiilor și autosesizărilor

SIISPECD va permite petentului să se autentifice și să depună cererea, reclamația, sesizarea sau propunerea formulată în scris, precum și alte documente justificative prin intermediul Portalului de Servicii Electronice Publice (PSEP), care va prelua petiția și o va transfera sistemului intern de management a documentelor (DMS). În cazul depunerii acesteia prin alt mijloc legal - poștă, email, sau oral (urmarea unei note de audiență), soluția va permite introducerea informațiilor privitoare la petent și conținutul petiției în DMS de către angajatul responsabil cu activitatea de Registratură, angajat care va scana eventualele documente fizice și le va atașa la documentul principal. În cazul autosesizării, aceasta va putea fi inițiată intern direct în DMS de către persoana abilitată.
SIISPECD va permite înregistrarea petiției sau autosesizării în Registrul electronic de corespondență din DMS de către angajatul responsabil cu activitatea de Registratură și direcționarea automată a acesteia către următorul actor pe fluxul de lucru. În cazul în care petiția a fost introdusă prin intermediul PSEP, atunci sistemul DMS va transmite petentului în contul său confirmarea înregistrării.
SIISPECD va permite Președintelui CNCD să analizeze, introducă rezoluție și să repartizeze petiția către serviciul competent (Serviciul Asistență Colegiu Director - SACD).
SIISPECD va permite Manager / Șef SACD să analizeze, introducă rezoluție și să repartizeze petiția către un angajat nominalizat.
SIISPECD va permite Consilierului:

- Să redirecționeze documentele către o altă instituție în cazul direcționării petiției în mod greșit către CNCD.
- Să procedeze la tratarea inadmisibilității în cazul unor excepții precizate de lege.
- Să completeze informațiile prin intermediul petentului întrun interval de 15 zile, altfel să claseze petiția. În cazul în care Petentul a introdus petiția / sesizarea prin intermediul PSP, soluția va permite notificarea petentului în portal, urmând ca acesta să introducă informațiile

lipsă tot prin intermediul acestuia.

- Să constituie dosarul electronic al cazului și să îl înregistreze în Baza de Date a Serviciului. Conținutul Bazei de Date va fi detaliat separat (pct. p).
- Să comunice petiția la reclamat și să înregistreze punctul său de vedere.
- Să direcționeze dosarul către un Membru al Colegiului Director.

SIISPECD va permite unui Membru al Colegiului Director să verifice cazul și să introducă o rezoluție cu cel puțin 20 de zile înainte de termenul stabilit pentru audierea părților.
SIISPECD va permite Managerului / Șefului SACD să analizeze și să dispună modalități de soluționare:

- În cazul unei plângeri penale, să dispună suspendare și / sau reanalizare;
- În cazul unei aceleiași fapte, să dispună conexarea dosarelor;
- În cazul aceleiași cauze, să aplice rezoluție;
- Să dispună investigarea actelor sau faptelor de discriminare.

SIISPECD va permite Consilierului să introducă Raportul de investigație și a documentelor suport.
SIISPECD va permite generarea citațiilor și urmărirea răspunsului la acestea.
SIISPECD va permite introducerea de către Consilier a dezbaterilor și declarațiilor înregistrate, dovezi, precum și a concluziilor în urma desfășurării audierilor.
SIISPECD va permite administrarea de către Consilier a probelor documentate pe tot parcursul investigației, precum și a altor documente care pot surveni și întrerupe procesul: dispoziție instanță judecată (adoptare și emitere hotărâre), înțelegere amiabilă.
SIISPECD va permite gestiunea adoptării hotărârilor (în toate formele sale) de către Colegiul Director și semnarea acestora după motivarea juridică în maxim 30 de zile realizată de către Consilier și verificată de către Manager / Șef SACD.
SIISPECD va permite distribuirea în vederea comunicării a hotărârii și trimiterea acesteia pe bază de adresă înregistrată prin intermediul Registraturii.
SIISPECD va permite legătura cu Arhiva fizică prin includerea nomenclatorului arhivistic al instituției, generarea și plasarea de coduri QR care să facă legătura între documentele electronice și cele fizice corespondente.
SIISPECD va permite mutarea cazului la Contencios în cazul prezenței unei contestații și eventuala reluare a ciclului (reanalizare conform Art. 75) de la pasul d.
SIISPECD va permite pe tot parcursul procesului de tratare a petițiilor și autosesizărilor gestionarea Bazei de date, care va cuprinde cel puțin următoarele informații: nr petiție, an dosar, nr dosar, titular dosar, dosare anexate, nr. dosare anexate, titular inițial (preluat / conexat), nr. hotărâre / dosar deliberat, data hotărâre, data comunicare hotărâre, reintroducere dosar, petent, reclamat, obiect, soluție, detalii etc.
SIISPECD va permite pe tot parcursul procesului de tratare a petițiilor și autosesizărilor gestionarea Arhivei în lucru SACD, care va cuprinde cel puțin următoarele informații: an dosar, nr. dosar, nr. petiție, status, citații, consilier, predare / primire, încrucișare etc.

SIISPECD va permite pe tot parcursul procesului de tratare a petițiilor si autosesizărilor transmiterea din DMS în PSEP a oricăror notificări destinate petentului pentru a fi recepționate de către acesta în contul său, în cazul în care acesta a introdus petiția în sistem prin portal.
Modulul va respecta cerințele menționate mai sus, detalii concrete ale modalității prin care acestea vor fi implementate urmează a fi detaliate în etapa de analiză și proiectare din cadrul proiectului.

5.3.4. Cerințe funcționale privind avizarea de legalitate a documentelor

SIISPECD va permite prin intermediul sistemului DMS accesul consilierului juridic responsabil de la nivelul Compartimentului Avizări, Contracte și Achiziții (C.A.C.A.) aplicarea vizei de legalitate sub forma de ștampilă electronică sau / și semnătură electronică pe documentele supuse avizării în cadrul următoarelor acțiuni realizate pe fluxul de documente:

- avizarea documentelor în legătură cu activitatea CNCD, care angajează răspundere patrimonială, contractuală, civilă, penală, disciplinară.
- vizare de legalitate a ordinelor emise de Președinte.
- avizare asupra legalității documentelor și a măsurilor ce urmează a fi luate de conducerea instituției sau de către celelalte compartimente în desfășurarea activității și care pot angaja răspunderea patrimonială a instituției, inclusiv a contractelor de achiziție publică.
- avizarea privind legalitatea proiectelor de contracte, protocoale, acorduri sau a oricăror alte acte care produc efecte juridice, ce privesc activitățile Consiliului Național pentru Combaterea Discriminării.
- formularea de puncte de vedere în scris cu privire la neregulile semnalate în documentele supuse avizării juridice și comunicarea acestora celor ce întocmesc respectivele documente, în vederea îndreptării acelor nereguli.
- acordarea de consultanță celorlalte compartimente din CNCD.
- semnalarea către Președinte a cazurilor de aplicare defectuoasă a prevederilor legale în domeniul prevenirii și combaterii discriminării și întocmirea de propuneri pentru rezolvarea cazurilor respective.

Modulul va respecta cerințele menționate mai sus, detalii concrete ale modalității prin care acestea vor fi implementate urmează a fi detaliate în etapa de analiză și proiectare din cadrul proiectului.

5.3.5. Cerințe funcționale privind întocmirea și avizarea proiectelor de acte normative

SIISPECD va permite prin intermediul sistemului DMS accesul și lucrul colaborativ al consilierului juridic responsabil de la nivelul Biroului Avizări, Contracte și Structuri Teritoriale (BACST) și a altor membri ai unui grup de lucru constituit prin dispoziția Președintelui CNCD la documentele electronice premergătoare proiectelor de acte normative.
SIISPECD va permite gestiunea în formă electronică a proiectului de act normativ și a instrumentelor de prezentare și motivare (expuneri de motive - în cazul proiectelor de legi, note de fundamentare - în cazul ordonanțelor de urgență și al hotărârilor Guvernului, referate de aprobare – pentru celelalte acte normative), precum și fluxurile de aprobare ale acestora prin aplicarea semnăturii electronice.

5.3.6. Cerințe funcționale privind reprezentarea în instanță și expertizare judiciară

SIISPECD va permite primirea și introducerea chemării în judecată a entității în DMS direct prin intermediul Portalului de Servicii Electronice Publice (PSEP) sau indirect prin intermediul scanării documentelor fizice sosite la Registratură.

SIISPECD va permite înregistrarea, gestionarea și direcționarea documentelor electronice reprezentând actele procedurale necesare reprezentării intereselor instituției în fața instanțelor de judecată sau a altor organe administrativ-jurisdicționale (întâmpinare, cerere de chemare în judecată / contestație administrativă, alte lucrări de specialitate, precizări etc.) pe fluxuri predefinite, la actori predefiniți.

SIISPECD va asigura gestiunea și monitorizarea stării acțiunilor în curs prin mecanisme de vizualizare și urmărire în timp.

SIISPECD va permite formularea, gestionarea și direcționarea documentelor reprezentând puncte de vedere cadru privind obiectul acțiunii de chemare în judecată, precum și opinii juridice de specialitate cu valoare de expertiză sau consultanță judiciară, menite să sprijine în concret instanțele cu privire la acțiunile judecătorești al cărora obiect îl formează răspunderea delictuală civilă în materia nediscriminării.

Modulul va respecta cerințele menționate mai sus, detalii concrete ale modalității prin care acestea vor fi implementate urmează a fi detaliate in etapa de analiza si proiectare din cadrul proiectului.

5.3.7. Cerințe funcționale privind Portalul de Servicii Electronice Publice (PSEP)

Portalul de servicii electronice publice se va implementa pe Platforma de dezvoltare și administrare aplicații web (LCAP) și va asigura digitalizarea serviciilor de combaterea discriminării prestate de către CNCD pentru persoanele fizice și juridice, prin preluarea electronică a solicitărilor.

PSEP va putea fi accesat de beneficiari prin intermediul computerelor personale, precum și a dispozitivelor mobile cu sistem de operare de tip android sau ios.

În acest sens, PSEP va prezenta serviciile de combaterea discriminării prestate de către CNCD, întro manieră unitară și structurată, astfel încât utilizatorul să poată regăsi ușor serviciul dorit și informațiile asociate despre obținerea acestuia.

Pentru fiecare serviciu prestat se va prezenta o secțiune ce include o descriere a acestuia, documentele necesare, cât și o secțiune pentru accesarea serviciului în formă electronică.

Portalul va pune la dispoziția utilizatorilor un asistent virtual pentru furnizarea de răspunsuri personalizate privind întrebările legate de serviciile de combaterea discriminării prestate de către instituție.

Accesarea unui serviciu în formă electronică presupune parcurgerea de către utilizator a unei succesiuni de activități asistate de Portal. Serviciile electronice vor fi centrate pe activități și pe finalitatea acestora, constând întro succesiune de pași care includ, după caz:

- ecrane de informare;
- ecrane care conțin formulare web care trebuie completate, cu atașarea de fișiere (fotografii, documente scanate);

- ecrane care permit încărcarea de fișiere structurate de tip xml sau csv;
- ecrane de vizualizare a unor documente generate automat de către Portal, în baza informațiilor furnizate până la acel moment.

Formularele web care compun serviciile electronice vor include pentru unele câmpuri controale de culegere a informației de tip text simplu, text multilinie, lista de selecție valori dintr-un nomenclator, bifă (checkbox).

Formularele web vor realiza, pentru unele câmpuri, validări ale datelor introduse de utilizator, pentru verificarea respectării unor constrângeri referitoare la: localizarea spațială a utilizatorului, tipul informațiilor care trebuie completate, lungimea minimă sau maximă a textului, la limite ale valorilor numerice sau ale datelor calendaristice.

Asistentul virtual va asigura totodată asistarea utilizatorilor în completarea formularelor web oferind răspunsuri contextuale pe baza datelor colectate.

Formularele web completate de utilizator vor fi interpretate în timp real de sistem, indicând utilizatorului următoarea activitate necesară în vederea finalizării demersului dorit, activitate care poate include:

- completarea altui formular;
- încărcarea de fișiere de tip imagine;

Vor fi implementate reguli referitoare la obligativitatea atașării anumitor tipuri de documente. Regulile vor fi dependente de tipul de demers (serviciu electronic) şi de opțiunile selectate de către utilizator în cadrul formularului web.

În procesul de completare a formularelor web, sistemul va inițializa formularul (sau câmpuri ale acestuia) cu unele dintre informațiile structurate salvate în cadrul profilului utilizatorului.

Utilizatorii autentificați vor putea accesa și vizualiza în mod organizat istoricul solicitărilor trimise către instituție și stadiul procesării acestora.

În cazul serviciilor electronice prin care se depune o solicitare, la finalizarea procesului aferent depunerii cererii, Portalul va genera un document electronic (pdf) care cuprinde toate informațiile completate de către solicitant în formularele web aferente pașilor de proces deja urmați, pentru a permite solicitantului să verifice toate informațiile introduse înainte de transmiterea solicitării. Generarea documentelor electronice în baza informațiilor structurate completate de către solicitant în formularele web se va baza pe șabloane configurabile, în care vor fi incluse atât informații structurate culese din formularele aferente serviciului electronic cât şi paragrafe formatate de text predefinit.

Ulterior transmiterii unei solicitări, utilizatorul este notificat automat de către Portal prin email despre stadiul procesării şi poate vizualiza online stadiul acesteia, utilizând un link inclus în mesajul email primit.

PSEP va putea, după caz, să fie configurat să solicite ca anumite documente atașate de către utilizatori să fie semnate electronic, caz în care se va verifica validitatea semnăturii electronice. Portalul va semnala utilizatorului dacă semnătura nu este validă și nu permite parcurgerea pașilor următori ai serviciului electronic.

PSEP va permite prezentarea serviciilor de combaterea discriminării, într-o manieră unitară și structurată, astfel încât utilizatorul să poată regăsi ușor serviciul dorit și informațiile asociate acestuia.

În acest sens, serviciile de combaterea discriminării vor fi proiectate și implementate în cadrul Portalului astfel încât să fie îndeplinite liniile generale de implementare definite mai jos:

a. Portalul va asigura preluarea solicitărilor și direcționarea automată către alte module aplicative din back-end, prin intermediul serviciilor web, în vederea procesării acestora.

b. Transmiterea unei solicitări în formă electronică va presupune parcurgerea de către utilizator a unei succesiuni de activități asistate de Portal. Portalul va asigura transmiterea solicitărilor de către utilizatori prin completarea de formulare web și încărcarea de fișiere (pdf)

c. În cazul, completării formularelor web, Portalul va asigura și precompletarea unor câmpuri prin integrarea cu alte sisteme informatice, precum și validarea preliminară a datelor completate în unele câmpuri pe baza regulilor configurate;

d. Utilizatorii autentificați vor avea acces și vor putea vizualiza în mod organizat istoricul solicitărilor trimise către CNCD.

e. Utilizatorii PSEP vor putea primi notificări referitoare la solicitările transmise, precum și la solicitările de informații transmise de CNCD, etc.

f. Notificările se vor trimite prin mesaje email pe adresa utilizatorului. Mesajele vor conține un text informativ personalizat cu date specifice fiecărui utilizator.

SIISPECD va implementa un set de reguli clare și auditabile privind identificarea persoanelor fizice și juridice care solicită serviciile instituției.

Se va asigura o evidență certă a identităților persoanelor fizice, o evidență consistentă a identității persoanelor juridice și/sau a reprezentanților acestora, o evidență exactă a identităților profesionale asociate identităților persoanelor fizice și a fiecărui rol asociat oricăreia dintre aceste tipuri de identități.

Sub aspectul implementării în cadrul instituției, a nivelului de asigurare necesar pentru dovedirea si verificarea identității persoanelor fizice sau persoanelor juridice și pentru gestionarea mijloacelor de identificare electronică, se va implementa un mecanism de autentificare de nivel substanțial ce constă în:

a. Depunerea solicitărilor de către persoanele fizice și juridice nu se poate realiza decât după autentificarea acestora în contul propriu, creat și activat în PSEP;

b. Crearea contului de către persoana fizică presupune completarea unui formular electronic prin care se introduc datele de identificare (inclusiv număr de telefon și adresa de email pentru corespondență), încărcarea unei copii a cărții de identitate și acordarea consimțământului pentru prelucrarea datelor cu caracter personal. În urma transmiterii cererii de creare a contului, persoana fizică primește un mesaj prin care este invitat să valideze adresa de email și/sau numărul de telefon și să urmeze instrucțiunile pentru identificare;

c. Contul creat este activat doar după ce se face identificarea persoanei fizice și se verifică corectitudinea datelor introduse în formularul electronic de deschidere a contului;

d. Identificarea persoanei fizice se va realiza pentru activarea contului creat, prin unul din următoarele mecanisme la alegerea persoanei fizice solicitante:

- Prin prezentarea la sediul CNCD cu cartea de identitate, unde un funcționar va efectua identificarea, va verifica informațiile din contul creat și va activa contul. Sistemul va permite funcționarului să valideze identitatea persoanei fizice prin preluarea datelor din SNIEP.
    - Prin încărcarea unui unui document electronic semnat cu certificat calificat emis de un furnizor de servicii de încredere, caz în care sistemul va verifica valabilitatea certificatului calificat (prin integrarea cu serviciile OCSP - Online Certificate Status Protocol, în conformitate cu RFC 6960) și corespondența dintre informațiile asociate acestuia cu cele din cartea de identitate încărcată în sistem și va valida contul;
    - Prin înrolarea persoanei în ROeID din cadrul Platformei Software Centralizate pentru Identificare Digitală (PSCID) implementată de către Autoritatea pentru Digitalizarea României (https://www.adr.gov.ro/proiecte-in-implementare/platforma-software-centralizata-pentru-identificare-digitala-pscid/)

e. Autentificarea persoanei fizice în contul activat se realizează, de fiecare dată, prin:

- Utilizarea unui mecanism de autentificare propriu al SIISPECD ce va consta din doi factori:

    i. Nume utilizator și parolă = ceva ce știu

    ii. Cod unic (OTP=one time password) transmis pe emailul/telefonul persoanei fizice declarate la crearea contului=ceva ce dețin (un dispozitiv prin care se va primi codul unic prin email sau telefon.
- Utilizarea mecanismului de autentificare delegată, pus la dispoziție de către ROeID prin Platforma Software Centralizată pentru Identificare Digitală (PSCID) implementată de către Autoritatea pentru Digitalizarea României

O persoană fizică, care are un cont activ în PSEP, poate opta să se asocieze cu o persoană juridică pe care o reprezintă, pentru a putea depune solicitări în numele acesteia. În acest caz, va completa un formular electronic de solicitare cu datele de identificare a persoanei juridice și va încărca o copie a împuternicirii de reprezentare legală. Completarea datelor de identificare ale persoanei juridice se va realiza automat prin introducerea CUI și preluarea datelor de la ONRC. În urma transmiterii solicitării de asociere cu persoana juridică, se va verifica corectitudinea datelor introduse în solicitarea transmisă de către un funcționar al CNCD, care va valida solicitarea sau o va respinge, după caz.

Având în vedere prevederile art. 5 alin (2) din OUG 38/2020, prin care Autoritățile și instituțiile publice stabilesc tipul de semnătură electronică aplicabilă pentru utilizarea de către persoanele fizice sau juridice a unui serviciu disponibil online prestat de respectivele autorități, cu respectarea dispozițiilor Regulamentului nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe

piața internă și de abrogare a Directivei 1999/93/CE, și mecanismul de autentificare de nivel substanțial ce va fi implementat în cadrul PSEP, solicitările/rapoartele în formă electronică depuse de către aceștia prin Portal nu necesită semnarea cu un certificat digital. Documentele asociate solicitărilor, pe care persoanele fizice sau juridice sunt obligate să le prezinte, vor fi încărcate în formă electronică (rezultată în urma scanării sau emise în această formă).
Documentele de răspuns (dacă este cazul), pentru solicitările primite în formă electronică, vor fi emise de către CNCD în formă electronică, semnate de reprezentantul legal cu certificat digital calificat (respectând astfel prevederile Art.3 alin (1) din OUG38/2020) și vor fi transmise către solicitant în contul acestuia din PSEP.
Portalul de servicii electronice va putea fi accesat prin intermediul unei aplicații mobile native dedicată dispozitivelor mobile cu sistem de operare de tip android sau ios, ce va putea fi descărcată din magazinele online ale producătorilor sistemelor de operare mobile (Google Play, Apple Store).
Aplicațiile mobile vor putea fi instalate gratuit de orice persoană care dorește accesarea serviciilor puse la dispoziția publicului de către instituție.
Aplicațiile vor permite autentificarea utilizatorilor cu aceleași credențiale utilizate pentru autentificarea în Portalul de servicii electronice.
Utilizatorii vor putea accesa prin aplicația mobilă funcționalitățile disponibile în Portal.
Solicitările depuse prin intermediul aplicațiilor mobile se vor gestiona în Portal, oferind atât beneficiarilor cât şi funcționarilor o experiență de utilizare unitară, indiferent de modul de accesare a Portalului de servicii electronice.
Portalul de servicii electronice publice trebuie să permită accesarea de către utilizatori prin intermediul următoarelor browsere Chrome, Edge, Firefox, Safari sau echivalent, compatibile cu standardele HTML5, CSS și JavaScript.
Paginile web ale PSEP trebuie să îndeplinească cerinţele de compatibilitate şi accesibilitate pentru persoane cu dizabilități, în concordanţă cu specificaţiile W3C (World Wide Web Consortium, 5 Mai 1999) şi recomandările WAI (Web Accessibility Initiative), acceptate la nivel mondial drept standarde internaţionale în domeniul accesibilităţii web: Web Content Accessibility Guidelines (WCAG) 2.0 – minimum nivel AA.
Interfața portalului web de servicii va fi proiectată asfel încât să respecte prevederile OUG 112/2018 privind transpunerea Directivei 2102/2016 privind accesibilitatea site-urilor web și a aplicațiilor mobile ale organismelor din sectorul public, precum și respectarea prevederilor Directivei (UE) 2019/882 a Parlamentului European și a Consiliului din 17 aprilie 2019 privind cerințele de accesibilitate aplicabile produselor și serviciilor.
Portalul de Servicii Electronice Publice va facilita totodată implementarea serviciului public de prevenire a faptelor de discriminare (ce vizează un număr estimat de circa 30.000 de persoane anual) prin integrarea unei aplicații software specializate mature prin care se va asigura furnizarea de cursuri de formare privind drepturile omului, efectele discriminării, principiul egalității, prin formare asistată de calculator (Computer Based Training), asigurând în acest sens procesele de organizare, desfășurare și analiză a cursurilor, prin următoarele funcționalități:

- Încărcarea cursurilor create și configurarea sesiunilor de curs;
- Furnizează cursanților informații generale despre curs: descriere, compunere (capitole, subcapitole, test, etc.), formatul cursului (document, video, listă întrebări, etc.), procentajul de parcurgere, etc.
- Asigură descărcarea materialelor de curs (documente și fișiere video) de către participanții la curs;
- Susținerea examinării de către cursanți după finalizarea cursurilor în vederea certificării competențelor dobândite;
- Emiterea și difuzarea automată a certificatelor ce atestă parcurgerea cu succes a cursurilor;
- Elaborarea și diseminarea participanților la sesiunile de formare a unui chestionar de evaluare care să aibă în vedere aspecte precum: suportul de curs, exercițiile și studiile de caz, funcționalitățile platformei, integrarea cunoștințelor și abilităților dobândite în activitatea curentă. Rezultatele obținute vor fi centralizate și analizate, urmând a fi utilizate la elaborarea analizei de impact;
- Generarea raportului cuprinzând cursurile parcurse de către cursanți;
- Posibilitatea de urmărire a progresului la nivel de cursant;
- Realizarea de rapoarte în timp real privind stadiul formării (persoane repartizate, sesiuni începute, sesiuni terminate, număr certificări, etc.) raportate la număr de persoane, grupe, sesiuni;
- Generarea de rapoarte privind persoanele participante la cursuri, care să cuprindă: numele și prenumele, instituție, datele de contact, domeniul/domeniile în care s a efectuat formarea; competențele dobândite; certificatul obținut, care să ateste că programele de instruire au fost absolvite;
- Generarea registrului participanților la cursurile de formare ce va conține minim următoarele:
    - date privind participanții la cursurile de formare (nume și prenume, CNP/cod unic participant, tipul funcției, unitatea organizatorică)
    - date privind modulele urmate de către fiecare participant,
    - date privind certificatele obținute de către participanți în urma examinării;

5.3.8. Cerințe funcționale privind sistemul de management al documentelor

Se va implementa în activitatea instituției o arhitectură de stocare electronică a documentelor bazată pe structuri logice relaționale (dosare electronice) conectate direct în fluxurile de lucru.

Se va implementa o soluție în care stocarea documentelor electronice va permite o gestiune riguroasă a drepturilor de scriere și de citire. Vor fi putea fi realizate relații ale aceluiași document electronic în mai multe dosare electronice (fără a fi necesară multiplicarea sa – practic documentul va fi unic în continuare însă el va putea face parte în același timp din mai multe dosare electronice)

fapt ce va permite ca fiecare unitate organizatorică, în funcție de specificul activității sale să poată percepe actul respectiv întro manieră contextuală.
În cazul unor documente primite de la alte aplicații, se va putea realiza declanșarea automată a fluxurilor pre-configurate pentru distribuirea documentelor primite direct la grupurile de utilizatori asociate unităților organizatorice competente, în funcție de tipul documentului și notificarea personalului acestor unități via email și în aplicație.
În cazul documentelor primite în format letric sau pe conturile de email configurate în aplicație, personalul registraturii instituției care le-a primit și a realizat înregistrarea, inițiază declanșarea fluxurilor ad-hoc pentru distribuirea documentelor la grupurile de utilizatori asociate unităților organizatorice competente de la primul nivel ierarhic. Aplicația va fi configurată să notifice automat personalul acestor unități via email și în aplicație, la declanșarea fluxurilor.
Personalul unităților organizatorice de la primul nivel ierarhic, va putea prelua sarcina primită și direcționa mai departe fluxurile primite sub formă de sarcini, către grupurile de utilizatori asociate unităților organizatorice de nivel ierarhic imediat inferior, și procesul continuă până când sarcina este distribuită/preluată unui/de către angajat/utilizator.
Comunicarea formală internă între unitățile organizatorice din cadrul instituției se va realiza prin transmiterea de documente prin intermediul fluxurilor ad-hoc. Utilizatorii vor elabora documentul (fie generându-l din șablon, fie încărcându-l în depozit de pe stația locală), îl vor înregistra în Registrul unic general electronic și apoi vor iniția transmiterea pe flux ad-hoc prin: stabilirea activităților asociate (avizare, aprobare, semnare, etc.), tipul distribuției (secvențial sau paralel), prioritatea, participanții implicați (la nivel de grup), definirea de escaladări (termenul de declanșare, grupul către care se escaladează). Utilizatorul va putea să salveze fluxul astfel definit (ca șablon) pentru utilizarea ulterioară.
Documentele atașate pe flux vor putea fi semnate electronic cu semnătură calificată de către actorii participanți la flux.
Toate documentele emise de instituție, indiferent de canalul pe care au fost adresate solicitările, vor fi produse în format electronic. Avizarea și aprobarea documentelor emise se realizează prin intermediul fluxurilor digitale din aplicație. Personalul din unitățile organizatorice inițiază fluxul de aprobare a documentelor, atașând pe acesta documentele electronice. Documentele vor fi semnate electronic cu semnătură calificată de către actorii participanți la flux și stocate în depozitul de documente electronice. Actorii participanți la flux vor putea respinge documentul, condiționat de completarea motivelor respingerii/descrierea modificărilor solicitate. În cazul respingerii, fluxul se întoarce la inițiator, care în baza motivelor respingerii, întreprinde modificările necesare și trimite documentul revizuit din nou pe flux.
Soluția va permite semnarea electronică a documentelor, utilizând certificate digitale calificate. Se va lua în considerare inclusiv scenariul în care, în funcție de natura documentului (intern sau care iese din instituție) și a persoanei semnatare, se va folosi un tip de semnătură sau altul pe un flux.
Documentele emise de instituție, indiferent de canalul pe care au fost adresate solicitările, sunt produse în format electronic, semnate cu semnătură electronică calificată și stocate în depozitul de

documente electronice.

Fluxurile de aprobare a documentelor (de răspuns-ieșire) includ după ultimul pas de aprobare/semnare, întoarcerea fluxului la inițiator.

Pentru documentele care trebuie transmise în format letric conform unor norme legale explicite (cu putere de lege)/prevederi procedurale specifice sau pentru care solicitanții au solicitat explicit eliberarea în format letric, fluxurile întoarse la inițiator, vor fi prevăzute cu pași suplimentari care să faciliteze inițiatorului tipărirea documentului în două exemplare, exemplarul 2 va fi păstrat în instituție pentru arhivare. Ambele exemplare originale vor fi semnate olograf doar de către reprezentantul legal al instituției, exemplarul 1 va fi expediat destinatarului.

Pentru răspunsurile care trebuie transmise în format electronic via email, acest lucru se va putea realiza direct din aplicație de către inițiator, după finalizarea fluxului de aprobare și avizare a documentului.

5.4. Arhitectura funcțională a sistemului

5.4.1. Arhitectura logică a SIISPECD

Arhitectura logică a SIISPECD este prezentată în figura următoare:

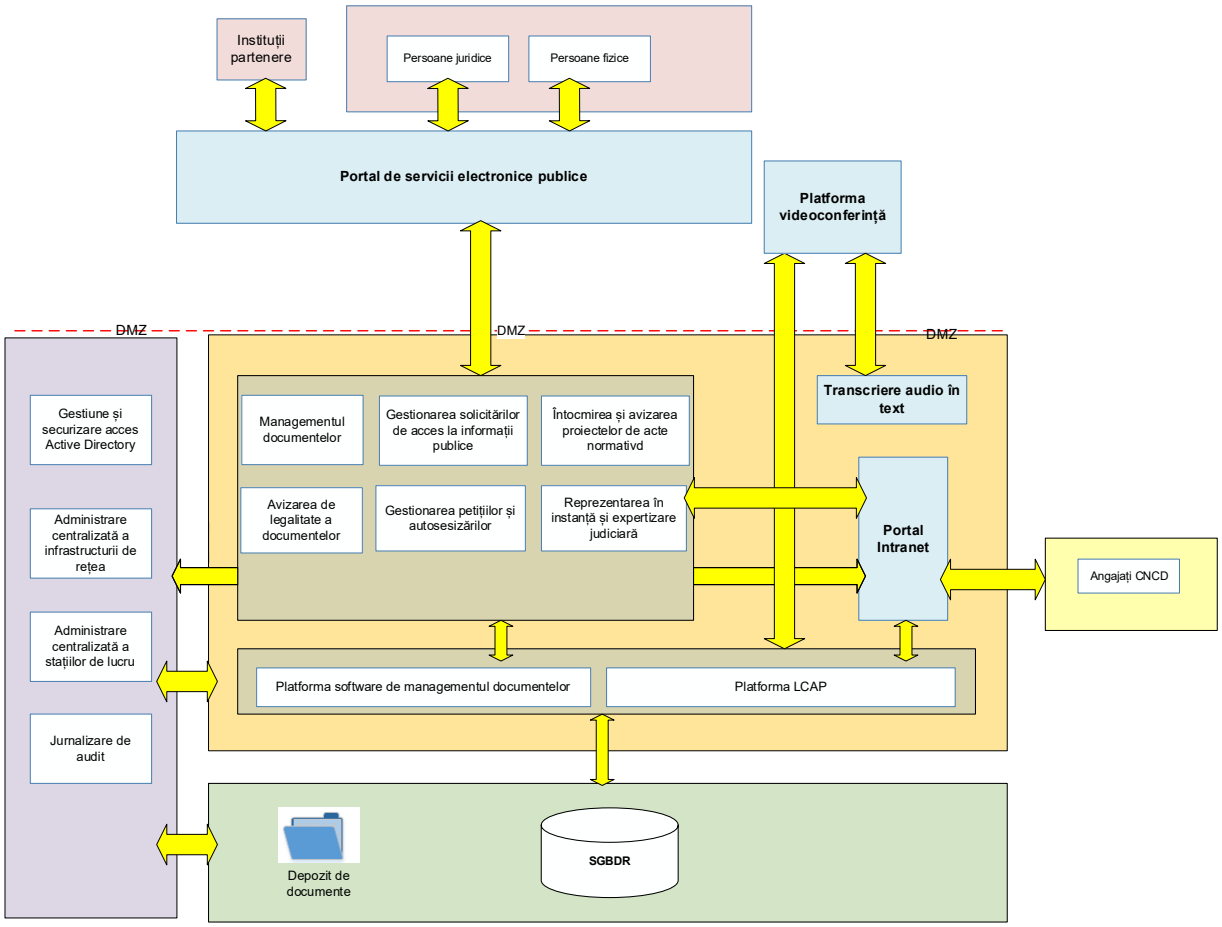


Figura 1: Arhitectura logică a SIISPECD

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

Pentru asigurarea unei securități adecvate a SIISPECD, pentru a proteja informația și subsistemele componente împotriva utilizării lor neautorizate sau a divulgării informației cu caracter personal sau a celei cu accesibilitate limitată, arhitectura sistemului va implementa două zone de securitate, ce asigură compartimentarea sistemului astfel încât dacă o parte din el este compromisă de către un potențial atac, acesta nu poate compromite și cealaltă zonă. În acest sens, se va realiza izolarea zonei de securitate PUBLICE de cea PRIVATĂ astfel încât:

- Să nu existe interacțiuni directe în sensul ZONA PUBLICĂ → ZONA PRIVATĂ;
- Doar ZONA PRIVATĂ accesează recurent ZONA PUBLICĂ pentru alimentarea proceselor de business interne, respectiv pentru remiterea rezultatelor acestora.

În acest sens, figura de mai sus ilustrează cele două zone distincte:

- Zona publică (DMZ) - Găzduiește componentele software cu care vor interacționa utilizatorii publici ai sistemului (e.g. persoanele fizice și cele juridice) prin intermediul rețelei Internet.
- Zona privată - Găzduiește componentele software dedicate utilizatorilor interni ai instituției, respectiv expune API-urile necesare integrării cu sisteme informatice ale altor instituții.

Componentele arhitecturii logice evidențiate în figura de mai sus sunt:

1. **Portalul de servicii electronice publice** va fi găzduit în DMZ (zona publică) și va asigura servicii de acces pentru persoanele fizice și juridice la serviciile publice de combatere a discriminării atât în regim autentificat (pentru accesul la solicitări și notificări), cât și neautentificat (pentru accesul la date publicate din oficiu de către CNCD). Portalul de servicii electronice publice va fi accesibil utilizatorilor autentificați doar prin intermediul zonei DMZ, care va funcționa în regim de proxy și va aplica regulile de securitate ce se impun la nivel de sursă a conexiunilor. De asemenea conexiunile cu serverul proxy vor fi executate doar prin protocol securizat HTTPS (SSL). Metadatele și documentele preluate (aferente solicitărilor și notificărilor) sunt transmise prin servicii web securizate către platformele aplicative din zona privată în vederea procesării.
2. **Platforma de managementul documentelor** va fi o aplicație de back-office prin intermediul căreia CNCD va realiza gestionarea documentelor și a metadatelor asociate, a versiunilor acestora, a tuturor fluxurilor de lucru și a obiectelor, facilitând astfel ținerea evidenței activității instituției în sistem informatizat și circulația electronică a documentelor în cadrul acesteia. Va fi accesibilă utilizatorilor angajați ai CNCD doar din rețeaua internă.
3. **Modulele aplicative funcționale ale SIISPECD** vor asigura optimizarea proceselor de lucru ale CNCD asociate serviciilor publice de combatere a discriminării, fiind implementate pe baza Platformei de dezvoltare aplicații web din categoria Enterprise Low-Code Application Platform (Platforma LCAP) și Platformei software de managementul documentelor (DMS), ambele utilizând același sistem unitar de gestiune a bazelor de date.
4. **Platforma de videoconferință** va permite comunicarea la distanță între funcționarii CNCD și petenți/reclamați în cadrul procesului de constatare și sancționare a faptelor de discriminare.
5. **Platforma software de transcriere audio în text** va asigura transcrierea, în timp real, a audierilor în cadrul CNCD.

Accesul angajaților CNCD la datele și funcționalitățile SIISPECD, se va realiza din Intranet, pe bază de roluri strict definite pentru a evita accesul neautorizat la date.
Platforma de management documente se va integra cu soluția gestiune și securizare a accesului Active Directory ce va fi implementată la nivelul CNCD pentru asigurarea autentificării și autorizării utilizatorilor.
Platforma de dezvoltare și administrare aplicații web (LCAP) va asigura acces selectiv la date și aplicații către instituțiile cu care se realizează schimb de date, prin intermediul API, asigurând totodată și managementul API-urilor.
Din punct de vedere tehnic, arhitectura sistemului va include un mediu de producție și unul de disaster-recovery ce vor fi găzduite în Cloud-ul Privat Guvernamental - componenta de Cloud Dedicat bazat pe tehnologia Azure Hub Stack.
Arhitectura sistemului va fi constituită din soluții redundante, cu asigurarea disponibilității și balansarea încărcării (cluster HA) pentru componentele funcționale critice ale sistemului conform tabelului de mai jos.
Pentru asigurarea funcționării în bune condiții a performanței sistemului vor fi asigurate următoarele medii:

a. Mediul de producție - asigură funcționarea în producție a sistemului și reprezintă mediul care va fi utilizat în mod direct de către anagajații instituției pentru furnizarea serviciilor electronice expuse către cetățeni;
b. Mediul de disaster-recovery – va fi folosit pentru restabilirea funcționarii sistemului în urma unui dezastru în cadrul componentei de Cloud Dedicat a Cloud-ului Privat Guvernamental si va avea rolul de a minimiza impactul nefuncționării centrului de date de producție și de a asigura continuitatea operațiunilor.

Mediul de disaster-recovery va fi dimensionat pentru a permite restaurarea rapida a funcționării sistemului și pentru funcționarea acestuia pentru o perioadă scurtă de timp, până la repunerea în funcțiune a mediului de producție. În acest sens se va utiliza, soluția Software de realizare a copiilor de siguranță solicitată a fi livrată în cadrul proiectului.
Ținând cont de sensibilitatea datelor și nivelului de securitate solicitat în cadrul proiectului, cât și de asigurarea de către producători a suportului tehnic pentru toate componentele funcționale, de securitate și suport ale platformei, furnizorul este solicitat să ofere versiunea comercială (COTS) pentru toate componentele software.
Sistemul informatic va fi proiectat astfel încât să funcționeze în regim de înaltă performanță şi disponibilitate şi va fi structurat pe trei niveluri, conform celor mai bune practici în domeniu: stocarea datelor, prelucrare şi prezentare.
Dimensionarea componentelor funcționale și a celor de suport ale mediului de producție va trebui să asigure minimul de resurse de procesare după cum urmează:

Nr. crt.	Componenta	Număr minim de noduri pentru Mediul de productie	Disponibilitate minima	Număr minim vCPU/nod
1.	Portal de servicii electronice publice	2	HA (activ-activ)	16
2.	Software de gestiune bazelor de date relaționale zona publică	2	HA (activ-pasiv)	8
3.	Platforma de managementul documentelor	2	HA (activ-activ)	16
4.	Software de gestiune bazelor de date relaționale zona privată	2	HA (activ-pasiv)	8
5.	Software de gestiune și securizare a accesului	2	HA (activ-activ)	8
6.	Web Apllication firewall	2	HA (activ-activ)	8
7.	Software realizare copii de siguranță	1		8
8.	Software de jurnalizare de audit	1		4
9.	Administrare centralizată a stațiilor de lucru	1		16
10.	Software de videoconferința	1		20
11.	Software de monitorizare a performanței aplicațiilor	2	HA (activ-activ)	4

Este responsabilitatea ofertantului să prezinte în cadrul ofertei o soluție care să îndeplinească cerințele arhitecturale, de înaltă disponibilitate a serviciilor oferite utilizatorilor, de continuitate în funcționare, în condițiile de performanță și încărcare solicitate prin prezentul document.

Ofertanții vor prezenta în cadrul ofertei lista mașinilor virtuale/containerelor necesare pentru soluția propusă, indicând pentru fiecare: tipul (conform specificațiilor Azure), rolul, sistemul de operare necesar, software-ul instalat, numărul de nuclee virtuale de procesare necesare, memoria RAM, spațiu de stocare necesar.

5.4.2. Arhitectura fizică SIISPECD

Arhitectura fizică a SIISPECD este prezentată în figura următoare:

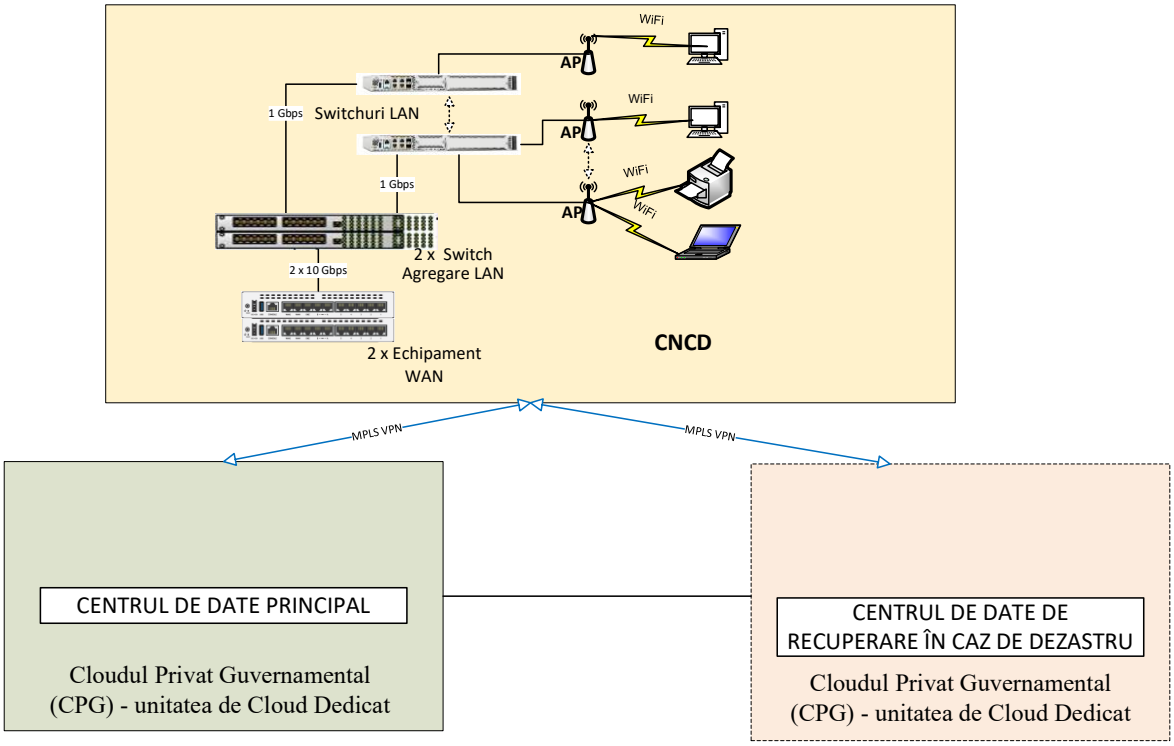


Figura 2: Arhitectura fizică a SIISPECD

În Figura 2 echipamentele nominalizate trebuie furnizate în cadrul acestui proiect. În sub-capitolele următoare sunt descrise pe larg componentele infrastructurii SIISPECD.

5.4.2.1 Infrastructura de comunicații a SIISPECD

Conectivitatea securizată prin MPLS VPN a CNCD la CPG se va realiza prin **Echipamente de comunicații WAN**.

Infrastructura de comunicații LAN a CNCD va fi realizată, în cadrul proiectului, prin extindere organică, prin utilizarea ultimelor tehnologii disponibile în materie de switching, acces wirelss și securitate, cu:

Echipamente de tip Switch LAN care să asigure, în cadrul locației CNCD, conectivitatea LAN a echipamentelor de tip Acces Point;

Echipamente de tip Access Point care să asigure conectivitatea LAN WiFi a stațiilor de lucru de pe care se va realiza accesul utilizatorilor din cadrul sediului CNCD la aplicațiile din compunerea sistemului;

În cadrul sediului CNCD conectivitatea Switch-urilor LAN se va realiza prin **Echipamente de tip Switch Agregare LAN.**

Totodată, soluția implementată trebuie să asigure posibilitatea să se monitorizeze și să se intervină, în mod proactiv, în identificarea și rezolvarea problemelor de conectivitate ale utilizatorilor pentru a reduce la minim timpii de inactivitate.

5.4.2.2 Infrastructura de terminale pentru utilizatori

Infrastructura de terminale pentru utilizatori a SIISPECD, va include:

- Stații de lucru;
- Calculatoare portabile;
- Scanere

5.4.2.3 Infrastructura de management și administrare a SIISPECD

Infrastructura de management, monitorizare și administrare a SIISPECD, va include:

- **Aplicație de administrare centralizată a infrastructurii de rețea**, facilitând configurarea, provizionarea, monitorizarea și depânărea AP-urilor, switch-urilor și echipamentelor WAN;
- **Aplicație de administrare centralizată a stațiilor de lucru,** facilitând monitorizarea și managementul calculatoarelor și a sesiunilor utilizatorilor în infrastructura sistemului, inclusiv implementarea sistemului de operare și a actualizărilor, precum și preluarea controlului de la distanță pentru depanare;

5.4.2.4 Infrastructura de securitate a informațiilor SIISPECD

Infrastructura de securitate a informațiilor SIISPECD, va include a**ctualizarea soluției existente de gestiune și securizare a accesului Active Directory,** incluzând atât licențele software necesare cât și operațiunile de actualizare a serviciilor ActiveDirectory, DNS, WSUS, FileServer și Print Server spre sistem de operare Windows Server 2022.

5.4.2.5 Platforma de procesare, stocare și securitate a SIISPECD

Platforma de procesare, stocare și securitate necesară funcționării SIISPECD va fi implementată prin utilizarea **Cloudului Privat Guvernamental (CPG), unitatea de Cloud Dedicat bazată pe tehnologia Azure Hub Stack**.
Platforma de procesare, stocare și securitate va asigura resursele de procesare și stocare necesare astfel încât SIISPECD să respecte cerințele tehnice, funcționale și de performanță din prezentul document.
Soluția va fi configurată astfel încât, să asigure realizarea copiilor de siguranță (mașini virtuale, baze de date și fișiere aferente documentelor electronice) și stocarea acestora în centrul de date de recuperare în caz de dezastru, astfel încât să permită restaurarea în cel mult 30 de minute, după restabilirea serviciilor în centrul de date principal.
Accesul personalului din cadrul CNCD la platforma de procesare, stocare și securitate (respectiv la aplicațiile ce vor rula pe aceasta) se va realiza prin linii de comunicație securizată de tip MPLS VPN.

5.4.3. Compunerea infrastructurii de comunicații, terminale, management și Securitate a SIISPECD

5.4.3.1 Infrastructura hardware a SIISPECD

SIISPECD va include o infrastructură de comunicații, terminale, management și securitate compusă din următoarele echipamente:

Nr.	Descriere	Cantitate	Observații
1	Echipament WAN	2	CNCD Sediul Central
2	Switch Agregare LAN	2	CNCD Sediul Central
3	Switch Acces LAN	4	CNCD sediul central
4	Acces Point	15	CNCD sediul central
5	Scaner registratură	4	Unul la registratură/secretariat, unul la SACD, unul la Direcția Juridică și unul la Direcția Economică
6	Scaner arhivă	1	
6	Computere de birou	65	
7	Computere portabile	2	

5.4.3.2 Infrastructura software a SIISPECD

SIISPECD va include o infrastructură de software de management, administrare, precum și securitate a informației, compusă din următoarele soluții software:

Nr.	Descriere	Unitate de măsură	Cantitate	Observații privind licențierea
1	Aplicație de administrare centralizată a infrastructurii de rețea	Set	1	Acoperă AP-urile, switch-urile LAN și echipamentele WAN
2	Aplicație de administrare centralizată a stațiilor de lucru	Set	1	Acoperă stațiile de lucru și calculatoarele portabile din cadrul SIISPECD
3	Software de realizare a copiilor de siguranță	Set	1	Asigură o capacitate de date de protejată pentru minim 5 TB, indiferent de numărul de mașini fizice sau virtuale protejate
4	Software de jurnalizare de audit	Set	1	Soluția trebuie să asigure colectarea evenimentelor de audit din toate aplicațiile, bazele de date și

Nr.	Descriere	Unitate de măsură	Cantitate	Observații privind licențierea
				echipamentele din compunerea SIISPECD
5	Actualizarea soluției Active Directory existente	Set	1	Se va include licența Microsoft Windows Server 2022 pentru 16 nuclee și 79 bucăți Microsoft Windows Server 2022 user CAL. Aceste licențe sunt necesare pentru actualizarea serviciilor ActiveDirectory, DNS, WSUS, FileServer și Print Server la nivel de ediție 2022
6	Pachet BYOL CPG Azure Hub Stack	Set	1	Va include licențele necesare pentru funcționarea soluției în Cloudul Privat Guvernamental (CPG), unitatea de Cloud Dedicat bazată pe tehnologia Azure Hub Stack

5.4.4. Interoperabilitate

Toate aplicațiile software din compunerea SIISPECD vor dispune de mecanisme de interfațare necesare pentru integrarea cu alte aplicații și sisteme informatice.

Astfel, sistemul trebuie dezvoltat pe baza unei strategii API ready (API ready - un set de definiții de sub-programe, protocoale și unelte pentru programarea de aplicații și software. Un API poate fi utilizat pentru un sistem web, sistem de operare, sistem de baze de date, hardware sau biblioteci software). API-urile si formatul datelor trebuie să fie compatibile cu OpenAPI2 si DCAP elaborat de DGEurope, (https://www.w3.org/TR/vocab-dcat-2/ si https://www.openapis.org/)

În plus față de integrările solicitate în mod explicit în cerințele din prezentul document, Furnizorul va avea în vedere ca API-urile aplicațiilor furnizate să permită integrarea prin servicii web cu:

a. Sistemul informatic al Oficiul Național al Registrului Comerțului (ONRC), pentru preluarea datelor de identificare ale persoanelor juridice;

b. Sistemul informatic al Direcției Generală pentru Evidența Persoanelor (DGEP), pentru preluarea datelor de identificare ale persoanelor fizice;

c. Sistemul Informatic al Registrului Național al persoanelor juridice fără scop lucrativ constituite cf. OG 26/2000, pentru preluarea pentru preluarea datelor de identificare ale persoanelor jurdice fără scop lucrative.

d. PJN - Platforma de jurnalizare şi notificare (Hotărârea Guvernului nr. 112/2023)

e. Portalul Digital Unic al României (PDURo) în vederea facilitării preluării de petiții

privind discriminarea.
Sistemul se va implementa în conformitate cu legea nr. 242 din 20 iulie 2022 privind schimbul de date între sisteme informatice și crearea Platformei naționale de interoperabilitate, și, subsecvent, ale OMCID nr. 21.286/26.10.2023 privind Normele de Referință pentru Realizarea Interoperabilității (NRRI). În acest sens, sistemul va fi proiectat pentru a fi pregătit să gestioneze/ schimbe date cu Platforma Națională de Interoperabilitate (PNI) prin:

- Definirea la nivel de serviciu/flux de lucru, a seturilor de date necesare platformei de interoperabilitate, conforme cu legislația ce guvernează instituția în cauză - Legea nr.242/2022 privind schimbul de date între sisteme informatice şi crearea Platformei naţionale de interoperabilitate, OUG nr. 89/2022 privind înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizate de autoritățile și instituțiile publice, HOTĂRÂRE nr. 112 din 8 februarie 2023 privind aprobarea Ghidului de guvernanță a platformei de cloud guvernamental
- furnizare standardizare pentru datele ce vor fi furnizate în NNRI (RNR)

Pentru realizarea integrărilor necesare cu sistemele externe nominalizate mai sus, în etapa de analiză și proiectare, Contractantul va identifica informațiile necesare implementării integrărilor cu acestea și va documenta mecanismele tehnologice (REST API) în vederea unei potențiale implementări. Este responsabilitatea autorității contractante să faciliteze schimbul de informații cu instituțiile nominalizate și să încheie protocoale de schimb de informații cu acestea.
Contractantul va livra sistemul cu interfețele (API) pregătite tehnic pentru conectare, conform specificațiilor, chiar și în absența disponibilității serviciilor instituțiilor partenere la momentul recepției.
În cadrul sistemului nou implementat se vor defini schemele de mesaje care vor fi schimbate cu alte instituții. Aceste mesaje vor sta la baza comunicării digitale inter-instituționale, vor reține autorul și destinatarul, datele solicitate si datele transmise, data și ora la care au fost cerute si soluționate precum si protocolul prin care instituțiile cooperează și fac schimb de date.
Viitorul contractant va avea obligația de a asigura conformitatea SIISPECD cu prevederile Regulamentului eIDAS 2 (propus ca actualizare a Regulamentului UE 910/2014), pe toată durata implementării, în măsura în care acesta devine aplicabil. Aceasta poate include, integrarea cu Portofelul Digital European (EUDI Wallet) pentru autentificare și semnături electronice, precum și suportul pentru servicii de încredere extinse (ex. semnături avansate bazate pe EUDI Wallet), în conformitate cu standardele și obligațiile aplicabile autorităților publice.

5.4.5. Performanța sistemului

SIISPECD va fi implementat astfel încât să asigure următorii parametri de performanță și încărcare:

a. Portal de servicii electronice publice

i. Număr estimat de utilizatori ce vor transmite solicitări anual: 49.500

ii. Timpul mediu de răspuns pentru 500 utilizatori standard concurenți în Portalul de servicii electronice publice nu va depăși 3 secunde pentru încărcarea unei pagini web,

corespunzătoare unor operații standard;

b. Sistemul intern de management documente:

i. Număr estimat de utilizatori (angajați CNCD): 79

ii. Timpul mediu de răspuns pentru 30 de utilizatori standard concurenți nu va depăși 3 secunde pentru încărcarea unei pagini web, corespunzătoare unor operații standard;

Timpii de răspuns prevăzuți mai sus, trebuie obținuți în condiții ideale (de pe stații de lucru conectate prin interfață wired 10/100 MBs, direct la serverul pe care rulează aplicația).

5.5. Securitatea sistemului

Pentru asigurarea unui nivel adecvat al securității informaționale soluția informatică livrată trebuie să permită realizarea de conexiuni securizate între terminalele utilizatorilor CNCD și serverele de aplicație pentru asigurarea siguranței informației expediate (prin intermediul sesiunilor SSL).

SIISPECD trebuie să asigure mecanisme de protecție împotriva încercărilor deliberate sau accidentale de acces neautorizat la datele pe care acesta le gestionează. Soluția de securitate trebuie sa asigure securitatea si confidențialitatea datelor cu caracter personal preluate, procesate și stocate în bazele de date. Astfel, utilizatorii vor putea accesa numai acele secțiuni și acel conținut care le sunt permise prin apartenenta la un profil sau la o macheta de securitate.

Soluția de securitate va fi configurată astfel încât:

a. să nu permită persoanelor neautorizate să modifice sau să șteargă informațiile din sistem;

b. să nu permită persoanelor neautorizate să acceseze sistemul pentru a proteja integral și în permanență informațiile;

c. să permită controlul complet al accesului utilizatorilor la aplicații prin înregistrarea datei și orei la care a fost executată fiecare tranzacție, precum și identitatea utilizatorului care a inițiat-o;

d. în caz de avarii să existe înregistrate informații de diagnosticare necesare pentru identificarea și soluționarea problemei.

e. Accesul la date al utilizatorilor (cu excepția celor cu rol de administrator) să se facă doar prin intermediul serviciilor oferite de componentele informatice, pe baza drepturilor deținute de către utilizatori, accesul direct la datele din bazele de date nefiind permis. Acest acces trebuie să poată fi reglementat prin politici de securitate, aferente fiecărui tip de utilizator.

SIISPECD trebuie sa includă mecanisme pentru asigurarea următoarelor definiții de securitate:

a. confidențialitatea, care asigură că datele sunt accesibile, vizibile sau disponibile doar utilizatorilor autorizați atât pentru datele stocate cât și pentru cele care tranzitează sistemul;

b. integritatea, care asigură nealterarea datelor sau distrugerea acestora de către o acțiune neautorizata;

c. disponibilitatea, asigura ca resursele de informații sa fie accesibile si utilizabile la cererea personalului autorizat atunci când le sunt necesare;

d. autentificarea, este mecanismul prin care un utilizator demonstrează că este cine spune că este; autorizarea definește ce resurse de sistem va putea accesa utilizatorul autentificat;

e. nonrepudierea, este un serviciu care nu permite unui utilizator participant la introducerea, modificarea sau manipularea datelor prin sistem să decline faptul că el a fost inițiatorul unei anumite acțiuni.

Prevederile de securitate vor fi implementate la următoarele niveluri ale soluției informatice propuse:

a. Nu se permite acces neautentificat la date și informații. Orice acces în aplicații, atât la nivelul utilizatorilor cât și la nivelul unor module, este precedat de identificarea, autentificarea și autorizarea accesului;
b. Sesiunile de lucru inactive trebuie să expire după o perioadă de timp configurabilă;
c. Serviciile și porturile de comunicație folosite vor fi documentate întro listă a serviciilor utilizate. Serviciile și porturile neutilizate vor fi dezactivate;

Sistemul informatic și componentele acestuia se vor livra doar cu ultimele patch-uri de securitate aplicate.

Viitorul contractant va avea obligația de a asigura conformitatea deplină a SIISPECD cu prevederile Directivei NIS 2 (Directiva UE 2022/2555), transpusă prin OUG nr. 155/2024, pe toată durata implementării. Aceasta include, dar nu se limitează la, implementarea măsurilor tehnice pentru gestionarea riscurilor cibernetice și asigurarea securității lanțului de aprovizionare, precum și configurarea platformei pentru a permite continuitatea serviciilor.

5.6. Confidențialitatea datelor

În cadrul proiectului se vor respecta următoarele principii:

a. abordarea **confidențialității prin concepție** pentru a asigura securitatea modulelor și a infrastructurii lor complete;

b. respectarea cerințelor și obligațiilor juridice privind **protecția și confidențialitatea datelor** recunoscând riscurile la adresa confidențialității care reies din analiza și prelucrarea avansată a datelor.

5.7. Cerințe hardware și software de infrastructură

5.7.1. Echipament WAN

Echipamentul WAN este un echipament de rutare Layer3 cu capabilități integrate de protecție în rețea și cu funcționalitățile de baza accelerate folosind procesoare specializate (ASIC-uri). Echipamentele trebuie să suporte configurarea atât în modul Transparent, cât și în modul NAT.

Echipamentul trebuie să îndeplinească următoarele cerințe și necesar de echipare:

- Minim 16 interfețe GE RJ45
- Minim 8 interfete GE SFP
- Minim 4 interfete 10 GE SPF+
- 1 port GE RJ45 pentru management/înaltă disponibilitate
- 1 port USB
- 1 port consola RJ-45

Echipamentul trebuie să dispună de următoarele capabilități rutare Layer3:

a. IPSec VPN Throughput (512 bytes): 12 Gbps
b. SSL-VPN Throughput: 1,5 Gbps
c. Tunele IPSec VPN concurente de tip gateway-to-gateway: 2000
d. Tunele IPSec VPN concurente de tip client-to-gateway: 500
e. Sesiuni concurente (TCP): 700 000
f. Sesiuni noi/Sec: 35 000
g. Va fi instalat în pereche în configurație redundantă activ-activ / activ-pasiv

Echipamentul trebuie să dispună de următoarele capabilități de protecție rețea: 49

a. Firewall Throughput (pachete UDP de 64 bytes): 10 Gbps
b. Firewall Throughput (pachete pe secunda) : 15 Mpps
c. IPS Throughput (Enterprise Mix): 1.4 Gbps
d. Throughput cu urmatoarele functionalități activate simultan: Firewall, IPS și Application Control - 3 Gbps
e. Inspecție SSL: 3000 Mbps

Licențierea echipamentului nu trebuie să limiteze numărul de utilizatori protejați

Echipamentul trebuie să se alimenteze de la rețeaua cu energie electrică având următorii parametrii 100-240V, 50-60Hz.

Echipamentul trebuie să asigure următoarele servicii de rutare/rețea:

a. Suport WAN multiplu – posibilitatea de a folosi minim 4 interfețe pentru conexiuni cu furnizorii de servicii de Internet (ISP);
b. Suport PPPoE
c. Client/Server DHCP
d. Rutare pe baza de politici
e. Rutare dinamica IPv4/IPv6- RIP, OSPF ,BGP, IS-IS, Multicast(IPv4)
f. Suport multi-zone
g. Rutare între zone
h. VLAN Tagging(802.1q)
i. Link aggregation (802.3ad)
j. Rutare intre VLAN-uri
k. Suport IPv6 (Firewall, AntiVirus, Web-Filtering, IPS, DNS, Transparent Mode, SIP, rutare dinamica, Admin access, Management)

Echipamentul trebuie să asigure următoarele capabilități de modelare a traficului:

a. Pe baza de politici
b. Suport DiffServ
c. Bandă Garantată/Maximă/Prioritară
d. Modelare pe bază de IP, pe bază de politici, pe bază de aplicații, pe bază de URL

Echipamentul trebuie să asigure următoarele capabilități privind domeniile virtuale:

a. Domenii Firewall/Rutare separate

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

b. Posibilitatea de folosire mixta a domeniilor virtuale in modul Transparent/NAT
c. Interfețe VLAN separate

Echipamentul trebuie să asigure următoarele capabilități de înaltă disponibilitate:

a. Activ/Activ, Activ/Pasiv
b. Statefull Failover
c. Link status monitor
d. Link failover

Echipamentul trebuie să asigure următoarele capabilități de VPN:

a. PPTP, IPSec, SSL
b. Suport criptare DES, , AES
c. Autentificare SHA-l *I* MD5
d. PPTP, L2TP, VPN Client pass through
e. Suport VPN "Hub and Spoke"
f. Autentificare IKE cu Certificate (x.509 v1 și v2)
g. IPSec NAT Traversal
h. Să dispună de client de VPN propriu, atât pentru PC-uri cât și pentru dispozitive mobile
i. Să includă SSLVPN cu suport pentru minim 500 tunele

Echipamentul trebuie să suporte următoarele servicii de securitate:

A. Firewall:

- NAT, PAT, Transparent
- VLAN Tagging (802.1q)
- SIP/H.323/SCCP NAT Traversal
- Suport session helpers (DCE-RPC, DNS, FTP, H.245, H.323, MGCP, ONC-RPC, PPTP, RSH, RTSP, SIP, TFTP, TNS)
- Profiluri granulare de protecție per politica
- Suport proxy explicit
- Suport pentru autentificarea userilor la nivel de politici firewall:
  - baza locala de utilizatori
  - Windows AD
  - External RADIUS/LDAP/TACACS+
  - XAUTH over RADIUS (IPSEC)
  - RSA Secure ID

B. Prevenirea intruziunilor:

- Suport Anomalii de protocoale
- Suport Semnaturi definite de utilizator
- Suport Ipv6

C. Antivirus:

- Suport Antispyware
- Worm Prevention

- Blocarea fișierelor in funcție de tip sau dimensiune
- Suport Ipv6

D. Antispam:

- Inspecție SMTP/SMTPS, IMAP/IMAPS, POP/POPS

E. Application control:

- Identificarea și controlul la nivel de aplicație cu identificarea aplicații de uz comun (control Layer 7 indiferent de port/protocol), baza de date de aplicații trebuie sa fie întreținută de producător și actualizata periodic
- Traffic shaping (per aplicație)
- Suport inspecție trafic SS

F. Suport Data Loss Prevention:

- Identificarea și controlul datelor sensitive
- Suport actiuni configurabile (block/log/archive)
- Opțional, suport document fingerprinting

G. Filtrare WEB

- Blocarea accesului utilizatorilor la site-uri de tip malițios sau cu conținut nepotrivit folosind o baza de date globala cu certificare recunoscut
- Posibilitatea definirii de liste statice cu URL-uri permise/blocate
- Posibilitatea de customizare a categoriilor globale prin suprascriere

H. Filtrare DNS

- Blocarea traficului către domenii malițioase sau cu conținut nepotrivit folosind o baza de date globala cu certificare recunoscuta.
- Posibilitatea definirii de liste statice cu domenii permise/blocate

Echipamentul trebuie să asigure următoarele capabilități de management:

- Consola, Telnet, SSH, HTTP/HTTPS, CLI
- Toate functionalitatile Să poată fi configurate exclusiv pe echipamentul propus, fără necesitatea suplimentara a unui echipament/ unei platfome de management
- Nu se accepta echipamente de tip “cloud-based”.
- Utilizatori/ Administratori cu drepturi configurabile
- Syslog, SNMP, log-uri interne, grafice, notificări email
- System software rollback
- Autentificare pentru administratori:
  - Baza de date locala
  - Integrare Active Directory
  - Integrare LDAP/RADIUS/Tacacs+
  - IP/MAC address binding

Echipamentele vor beneficia de garanție prin care care să se garanteze diagnosticarea echipamentului/modulului defect și înlocuirea acestuia, fără costuri suplimentare pentru beneficiar, în termen de 24 de ore în regim de 24 ore pe zi, 7 zile pe săptămână, pe o perioadă de 60 luni.

Echipamentele vor beneficia de suport software pe o perioadă de 60 luni, acoperind dreptul beneficiarului de a face update–uri precum și access direct la site-ul producatorului pentru a deschide direct cazuri de suport cu acesta.
Echipamente vor beneficia de licențierea tututor funcționalităților solicitate pe o perioada de 60 luni.
După expirarea serviciilor de garanție și suport tehnic, echipamentele trebuie să continue să funcționeze, să permită atât administrarea, cât și fluxurile de date.

5.7.2. Switch Agregare LAN

CARACTERISTICĂ	SPECIFICAŢII TEHNICE MINIME
Numar port-uri	Minim 24 port-uri SFP+ autosensing 1 Gbps/ 10Gbps Minim: 4 port-uri SFP 1Gbps/10Gbps/25Gbps/50Gbps 1 port consola de tip USB-C 1 port USB-A pentru memorii flash
Format	Rackabil
Memorie și Procesor	Minim 8 GB DDR4 Packet buffer size: 8 MB 32GB flash (eMMC) Procesor Quad Core ARM Cortex A72 sau echivalent cu frecvența de minim 1.8Ghz
Performanță	Latenta la 1000 Mb mai mică de 4,3 µs (64-byte packets) Latenta la 10 Gb mai mică de 1.6 µs (64-byte packets) Latenta la 25 Gb mai mică de 3 µs (64-byte packets) Latenta la 50 Gb mai mică de 3.5 µs (64-byte packets) Throughput: minim 650 Mpps Capacitate routing/switching: minim 850 Gbps Posibilitatea de front plane stacking Doua surse de alimentare redundante cu capacitate de minim 250W
Layer 2 switching	Suport pentru IEEE 802.1Q cu 4094 VLAN ID simultane Suport pentru IEEE 802.1D STP Suport pentru IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) Suport pentru IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) Suport pentru BPDU filter Suport pentru encapsulare VXLAN Suport pentru RPVST+ Support pentru BPDU Tunnelling
Layer 3 services	DHCP relay DHCP server

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

CARACTERISTICĂ	SPECIFICAŢII TEHNICE MINIME
	Static ARP, gratuituos ARP, proxy ARP Bidirectional Forwarding Detection GRE Tunnelling
Layer 3 routing	Static IP routing Static Routing IPv4, IPv6 OSPFv2, OSPF v3 mDNS Gateway ECMP Dual IP Stack BGP BGP-4 Policy Based Routing IP Performance Optimization
Management	Interfata de management Web HTTP si HTTPS Interfata de management de tip CLI (cu acces complet la configurarea echipamentului) Posibilitatea de a restrictiona acesul cu niveluri diferite de prvilegii pentru diversi utilizatori Posibilitatea de a face managementul din aplicatie mobila pusa la dispozitie de producatorul echipamentului Posibilitatea de syslogging remote si local SNMP v1, v2c, v3 Doua imagini flash Suport pentru port mirroring Suprot pentru 802.1AB LLDP Suport pentru RMON Mecanism integrat pentru diagnosicarea cablurilor conectate IP SLA for Voice Programabilitate si REST API SNMP v2c/v3 Nu se acceptă echipamente al căror management se realizează exclusiv în cloud-uri publice. Toate funcționalitățile echipamentului trebuie să poată fi configurate exclusiv pe echipamentul ofertat. Toate porturile de pe echipament vor fi la viteza maximă. Toate functionalitățile tip Layer 2 sau Layer 3 vor fi disponibile „out of the box” fără necesitatea de a achiziționa licențe adiționale
Securitate	Switch-ul va avea integrat modul de tip TPM "trusted platform

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

CARACTERISTICĂ	SPECIFICAŢII TEHNICE MINIME
	module" Enrolment over Secure Transport Control Plane Policing DHCP Protection Switch CPU Protection MACSec WANSec Dynamic IP Lockdown
Alte caracteristici	Sistem de operare bazat pe baze de date cu acces prin REST API la configurarea si monitorizarea echipamentului. Suport pentru multiple checkpoint-uri pentru salvarea configuratiei si starii echipamentului. Suport pentru QoS de tip 802.1p si DSCP Link aggregation (suport pentru 128 LAGs a cate 8 port-uri grupate prin LACP) LLDP-MED (Media Endpoint Discovery) Auto voice VLAN Suport pentru ACL-uri bazate pe adrese MAC si adrese IP Suport pentru autentificare 802.1X si RADIUS Suport pentru alocare automata de VLAN-uri Mecanism integrat de protectie ARP pentru a preveni atacurile de tip spoofing Mecanism de izolare a port-urilor fara a utiliza VLAN-uri Suport pentru Jumbo frame Suport pentru 802.3x flow-control Echipamentul va avea functionalitati avansate de visibilitate si procesare precum: Application Recognition, Datapoint Collection (cu functionalitati de sortare si cautare), Policy Control bazat pe roluri si aplicatii, WAN MACSec, Reflexive Policy

Echipamentul trebuie să se alimenteze de la rețeaua cu energie electrică având următorii parametrii 200-240V, 50-60Hz.

Echipamentele vor beneficia de garanție prin care care să se garanteze diagnosticarea echipamentului/modulului defect și înlocuirea acestuia, fără costuri suplimentare pentru beneficiar, în termen de 24 de ore în regim de 8 ore pe zi, 5 zile pe săptămână, pe o perioadă de 60 luni.

Echipamentele vor beneficia de suport software pe o perioadă de 60 luni, acoperind dreptul beneficiarului de a face update–uri precum și access direct la site-ul producatorului pentru a deschide direct cazuri de suport cu acesta.

5.7.3. Echipamente extindere rețea locală prin acces WiFi

Pachetul de echipamente și materiale pentru extinderea rețelei locale prin acces WiFi va fi format din următoarele componente:

Nr. Crt.	Denumire tip echipament	Cantitate
1	Switch acces LAN	4
2	Wireless Access Point	15
3	Set accesorii și cablaj	1

5.7.3.1 Switch acces LAN

CARACTERISTICĂ	SPECIFICAŢII TEHNICE MINIME
Numar port-uri	Minim 24 port-uri RJ-45 autosensing 10/100/1000Mbps PoE+ Minim 2 port-uri SFP+ fixed 1000 Mbps / 10Gbps 1 port consola de tip USB-C 1 port USB-A pentru memorii flash 1 port consola RJ 45
Alimentare PoE	Da, standard PoE+ Class 4 pentru toate port-urile Sursa de alimentare cu capacitate de minim 370W pentru PoE+ Suport pentru Quick PoE: Alimentarea echipamentului prin portul PoE incepe din momentul in care Switch-ul este bagat in priza
Format	Rackabil
Memorie si Procesor	Minim 8 GB DDR4 Packet buffer size: minim 6 MB Minim 16MB flash (eMMC) Procesor Quad Core ARM Cortex A72 sau echivalent cu frecvența de minim 1.8Ghz
Performanta	Latenta 1000 Mb < 3.4 µs (64-byte packets) Latenta 10 Gb < 24. µs (64-byte packets) Throughput: minim 95.2 Mpps Capacitate routing/switching: minim 128 Gbps Posibilitatea de front plane stacking prin porturile existente SFP+
Layer 2 switching	Suport pentru IEEE 802.1Q cu 4094 VLAN ID simultane Suport pentru IEEE 802.1D STP Suport pentru IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) Suport pentru IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) Suport pentru BPDU filter Suport pentru encapsulare VXLAN

CARACTERISTICĂ	SPECIFICAȚII TEHNICE MINIME
	Suport pentru RPVST+
Layer 3 services	DHCP relay DHCP server Static ARP, gratuituos ARP, proxy ARP
Layer 3 routing	Static IP routing Static Routing IPv4, IPv6 OSPFv2, OSPF v3 mDNS Gateway ECMP Dual IP Stack
Management	Interfata de management Web HTTP si HTTPS Interfata de management de tip CLI (cu acces complet la configurarea echipamentului) Posibilitatea de a restrictiona acesul cu niveluri diferite de prvilegii pentru diversi utilizatori Posibilitatea de syslogging remote si local SNMP v1, v2c, v3 Doua imagini flash Suport pentru port mirroring Suprot pentru 802.1AB LLDP Suport pentru RMON Mecanism integrat pentru diagnosicarea cablurilor conectate Programabilitate si REST API Posibilitatea de a face managementul din aplicatie mobila pusa la dispozitie de producatorul echipamentului Nu se acceptă echipamente al căror management se realizează exclusiv în cloud-uri publice. Toate funcționalitățile echipamentului trebuie să poată fi configurate exclusiv pe echipamentul ofertat. Toate porturile de pe echipament vor fi la viteza maximă. Toate functionalitățile tip Layer 2 sau Layer 3 vor fi disponibile „out of the box” fără necesitatea de a achiziționa licențe adiționale
Securitate	Switch-ul va avea integrat modul de tip TPM "trusted platform module"
Alte caracteristici	Sistem de operare bazat pe baze de date cu acces prin REST API la configurarea si monitorizarea echipamentului. Suport pentru multiple checkpoint-uri pentru salvarea configuratiei si starii echipamentului.

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

CARACTERISTICĂ	SPECIFICAŢII TEHNICE MINIME
	Suport pentru QoS de tip 802.1p si DSCP Link aggregation (suport pentru 32 trunks a cate 8 port-uri grupate prin LACP) LLDP-MED (Media Endpoint Discovery) Auto voice VLAN Suport pentru ACL-uri bazate pe adrese MAC si adrese IP Suport pentru autentificare 802.1X si RADIUS Suport pentru alocare automata de VLAN-uri Mecanism integrat de protectie ARP pentru a preveni atacurile de tip spoofing Mecanism de izolare a port-urilor fara a utiliza VLAN-uri Suport pentru Jumbo frame Suport pentru 802.3x flow-control

Echipamentul trebuie să se alimenteze de la rețeaua cu energie electrică având următorii parametrii 200-240V, 50-60Hz.

Echipamentele vor beneficia de garanție prin care care să se garanteze diagnosticarea echipamentului/modulului defect şi înlocuirea acestuia, fără costuri suplimentare pentru beneficiar, în termen de 24 de ore în regim de 8 ore pe zi, 5 zile pe săptămână, pe o perioadă de 60 luni.

Echipamentele vor beneficia de suport software pe o perioadă de 60 luni, acoperind dreptul beneficiarului de a face update–uri precum și access direct la site-ul producatorului pentru a deschide direct cazuri de suport cu acesta.

5.7.3.2 Acces Point

CARACTERISTICĂ	SPECIFICAŢII TEHNICE MINIME
Porturi	Minim 1 interfete SmartRate (RJ-45, viteza maximă negociată 2,5Gbps), cu capabilitati de Auto-sensing link speed (100/1000/2500BASE-T) si MDI/MDX Minim 1 port USB 2.0 – conector tip A, cu posibilitatea de a transmite 5W/1A catre un dispozitiv atasat Port consola dedicat (Micro-B USB)
Antene wireless	Minim 2 antene integrate tri-band, omnidirectionale pentru 2x2 MIMO in banda de 6Ghz cu castig de minim 4.5 dbi, 2x2 MIMO in banda de 5GHz cu castig de minim 4.5 dBi si 2x2 MIMO in banda 2.4GHz cu castig de minim 2.8 dBi. Optimizate pentru montarea orizontala pe tavan. Bluetooth 5.0 Low Energy (BLE5.0) Zigbee (802.15.4) radio (2.4GHz) GNSS L1 (1575.42 Mhz) cu support pentru GPS, Galileo, GLONASS si BeiDou

CARACTERISTICĂ	SPECIFICAŢII TEHNICE MINIME
Wireless	IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.11ax
Rate de transfer	802.11g: 6/9/12/18/24/36/48/54 Mbps 802.11b: 1/2/5.5/11Mbps 802.11a: 6/9/12/18/24/36/48/54 Mbps 802.11n de la 6.5 până la 400 Mbps 802.11ac de la 6.5 până la 1083 Mbps 802.11ax (5Ghz) de la 3.6 până la 1200 Mbps 802.11ax (6Ghz) de la 3.6 până la 2400 Mbps
Moduri de operare radio	Acces client, retea mesh, captura de pachete;
Caracteristici radio	Echipamentul trebuie sa suporte: - OFDMA: gestionarea simultana a mai multor clienți capabili de Wi-Fi 6 pe fiecare canal, indiferent de tipul dispozitivului sau al traficului - Advanced Cellular Coexistence: Functionalitate care minimizeaza impactul interferentelor retelelor GSM
Moduri de operare AP	- Autonom (functionare independenta pentru fiecare AccesPoint in parte); - Cluster (administrare centralizata pentru mai multe echipamente conectate in acelasi domeniu Layer 2); - Cloud-based (sa suporte administrarea centralizata din cloud); - Controller-based (sa suporte administrarea centralizata prin intermediul unui controller wireless); - Punct de acces remote (administrarea realizata de catre un controller dedicat pe baza unui tunel IPSec) Modul de functionare trebuie Să poată fi schimbat de catre autoritatea contractanta la nevoie fara a fi necesara înlocuirea echipamentului sau demontarea acestuia.
Funcționalități ale AP-ului	- Să poată functiona in cluster local, cloud public sau privat - Sa poată sa deservi până la 2048 de clienti simultan - Sa nu necesite produse sau servicii aditionale de management - AP-ul trebuie sa contina o intefata web pentru configurare - Configurarea AP-ului se poate face fara o conexiune fizica in retea; de ex prin o tableta sau un smart phone - Sa ofere posibilitatea de configurare in mod bridge fara controller si optiunea unei integrari cu un controller dedicat

CARACTERISTICĂ	SPECIFICAŢII TEHNICE MINIME
	- Sa nu necesite licente software adtionale pentru firmware - Trebuie sa suporte MESH - Să poată oferi suport pentru acesul de tip guest, integrat, fara software sau licente aditionale - Să poată oferi functii de detectie ale AP-ul rogue fara necesitatea unei solutii 3rd party - AP-ul trebuie sa detecteze si sa auto-prioritizeze aplicatiile de voce si video - Tehnologie ce poate rezolva problema clientilor “sticky”; in cazul in care se afla intr-un cluster mai multe AP-uri de la acelasi vendor, clientul va fi mutat automat catre AP-ul care ofera cel mai bun semnal - Tehnologie care maximizeaza eficienta AP-ului prin minimizarea interferentei de la retelele 3G/4G, sisteme distribuite de antene sau echipamente celulare mici - Localizare interioară a AP-urilor, cu ajutorul GPS-ului integrat, astfel încât serviciile de localizare pot fi implementate
Funcții de management	- AP-ul trebuie sa contina o solutie de management integrat si firmware special pentru un controller virtual - Aceasta solutie trebuie sa permita formarea de cluster-uri de cel puțin 128 de AP-uri si sa sustina minim 1800 de clienti - Soluția sa fie scalabila fara configurari sau licente aditionale - Soluția va functiona prin alegerea unui AP din cluster ca și controller virtual - AP-urile aditionale adaugate cu ajutorul acestei solutii trebuie suporte configurari de tip plug-n-play - AP-urile din acelasi cluster se vor organiza automat fara a fi nevoie de a alege un main si un backup - Soluția trebuie sa includa management automat al radiourilor: schimbarea automata a setarilor de putere si canal, atat in banda de 2.4 GHz cat si in cea de 5 GHz - Soluția trebuie sa includa metode de redundanta: in cazul in care AP-ul care deserveste ca și controller virtual cade, un alt AP din cluster va prelua automat functiile de controller - Sistemul trebuie să poată distribui automat firmware-ul catre toate AP-urile din acelasi cluster/grup - Soluția trebuie să poată împinge configuratii/modificari de configuratii catre toate AP-urile aflate in cluster

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

CARACTERISTICĂ	SPECIFICAŢII TEHNICE MINIME
Securitate	Să permită autentificare prin WPA3, WPA2, WPA, WPA Enterprise, Enhanced Open (OWE) Să permita autentificare perin WEP dinamic cu 802.1X Să permita autentificare prin IEEE 802.1X Proxy RADIUS pentru clienti NAS RADIUS cu redundanta integrata (Dynamic RADIUS Proxy) Suport pentru o tehnologie care face deep packet inspection si web content filtering pentru a putea bloca acesul utilizatorilor de la anumite aplicatii sau tipuri de aplicatii cat timp sunt legati la reteaua wireless
Certificare	• Marcaj CE • UL2043 plenum rating • Wi-Fi Alliance: - Wi-Fi CERTIFIED a, b, g, n, ac - Wi-Fi CERTIFIED 6E (ax, 6 GHz) WPA, WPA2 and WPA3 – Enterprise with CNSA option, Personal (SAE), Enhanced Open (OWE) - WMM, WMM-PS, W-Fi Agile Multiband - Passpoint (release 2) - Wi-Fi CERTIFIED Location™ • Bluetooth SIG
Alimentare	Port compliant PoE IEEE 802.3at sau alimentare directa de la sursa AC Puterea PoE va putea fi preluată fie de la un singur port (sursă unică sau setată să prioritizeze), fie de la ambele porturi simultan (setată să le combine).
Caracteristici mecanice	Temperatura de functionare: 0 - +50 Celsius. Umiditate: 5% - 95% fara condens

Echipamentul se va livra împreună cu accesoriile de montaj (tavan). Suportul de montare trebuie să fie prevazut din fabrica (de producator) cu posibilitate de blocare mecanica pentru a preveni căderea accidentală sau accesul neautorizat la echipament.

Echipamentele vor beneficia de garanție prin care care să se garanteze diagnosticarea echipamentului/modulului defect şi înlocuirea acestuia, fără costuri suplimentare pentru beneficiar, în termen de 24 de ore în regim de 8 ore pe zi, 5 zile pe săptămână, pe o perioadă de 60 luni.

Echipamentele vor beneficia de suport software pe o perioadă de 60 luni, acoperind dreptul beneficiarului de a face update–uri precum și access direct la site-ul producatorului pentru a deschide direct cazuri de suport cu acesta.

5.7.3.3 Set accesorii și cablaj

Setul de accesorii și cablaj va include toate materialele și componentele necesare pentru serviciile accesorii echipamentelor de extindere rețea LAN, astfel:

- Montarea Wireless Access Point-urilor pe perete sau tavan. Locurile de instalare vor fi stabilite în prealabil cu beneficiarul final;
- Montarea Switch-urilor în rack-urile existente;
- Conectarea Wireless Access Point-urilor la Switch-uri prin cablu UTP Categorie 6 folosind montarea aparentă cu canal de cablu;
- Conectorizare şi conectare la reţeaua de date conform cu arhitectura stabilită şi verificarea comunicaţiei între componentele instalate;
- Instalarea, activarea şi verificarea legăturii (uplink) de management pentru echipamentele instalate;
- Instalarea/actualizarea ultimelor versiuni de sistem de operare/firmware și verificarea bunei funcționări în urma operațiunilor de instalare/actualizare;
- Configurarea de bază a echipamentelor şi a modulelor astfel încât să se realizeze conectivitatea primară între componentele rețelei LAN.

Din analiza preliminară a Autorității Contractante, Setul de accesorii și cablaj trebuie să includă următoarele cantități estimate:

Denumire echipament	**UM**	**Cant**
Patch cord UTP Cat 6	buc	70
Canal cablu PVC 40x25	ml	50
Canal cablu PVC 25x16	ml	100
Cablu UTP Cat 6	ml	1200

5.7.4. Scaner registratură

Tip: ADF
Tehnologie scanare: Color CCD sau CIS, minim 2 senzori
Iluminare: minim 2 lămpi LED albe (1 față și 1 spate)
Modalitati de scanare:

a. Simplex / Duplex;
b. Monocrom / Color

Viteza de scanare ADF:

a. Simplex: minim 80 ppm A4 la o rezolutie de minim 200/300 dpi
b. Duplex: minim 160 ppm A4 la o rezolutie de minim 200/300 dpi

Capacitate ADF: minim 100 coli A4 80 g/m2
Rezoluție optică: 600 dpi
Rezoluție ieșire: minim 50 și minim 600 dpi (ajustabilă cu increment de minim 1dpi)
Format ieșire:

a. Color (24 bit),

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

b. tonuri de gri (8 bit),
c. monocrom (1 bit)

Dimensiune document ADF:

a. Maximum: A4
b. Minimum: A8

Panou control: Prevăzut cu ecran de tip LCD și butoane funcții: cel puțin pornire/oprire, meniu, start, stop, derulare etc.

Funtionalități minime procesare imagine:

a. Detectarea automată a culorii
b. Detectare și eliminare pagini albe
c. Eliminare găuri perforator
d. Eliminare dungi verticale
e. Eliminare culoare
f. Repoziționare imagine și text pe orizontală și verticală
g. Trunchiere imagine

Volum zilnic de scanare: Minimum 12.000 pagini

Interfață: minim USB 3.2 Gen 1

5.7.5. Scaner arhivă

Echipamentul trebuie să îndeplinească următoarele cerințe:

a. Tehnologie de scanare de tip V și plat, cu un unghi de 100 grade respective 180 de grade, cu sistem de sticlă presoare interschimbabilă intre V si plat având funcția de a copia digital documente legate de până la 15 kg;
b. Tehnologie de scanare manuala cu automatizarea întregului flux de scanare cu excepția întoarcerii paginilor;
c. Dimensiunea de scanare in mod plat să fie de până la 63 x 45 cm , iar in V 45 x 31 cm per pagina;
d. Rezoluția de scanare să fie de 300 dpi cu posibilitatea de upgrade până la 1000 dpi fără intervenția producătorului. Înlocuirea unității optice ale echipamentului de scanare să poată să fie realizată de către Beneficiar (plug and play), fără pierderea garanției;
e. Posibilitatea scanării materialelor cu o grosime de până la 150 mm;
f. Captura imaginilor să se efectueze cu ajutorul tastaturii, mouse-ului sau a declanșatoarelor de tip pedală;
g. Posibilitatea de ajustare a luminii in funcție de modul de scanare (V sau plat) pentru o dispersie uniforma a luminii
h. Echipamentul de scanare nu trebuie să forțeze legătura dosarelor (care pot determina ruperea legăturii sau a filelor);
i. Echipamentul de scanare trebuie să fie conceput cu un sistem de iluminare bazat pe tehnologie LED cu temperatura de culoare cuprinsă în intervalul de 5200 și 5600 grade Kelvin și care să

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

nu producă radiații ultraviolete sau infraroșii cu un indice CRI98;

j. Posibilitatea de scanare a coperților fără necesitatea utilizării unui echipament suplimentar (exemplu scaner flat-bed);
k. În situația în care documentele au nevoie de o scanare delicată, mult mai atentă sau o revenire la paginile anterioare echipamentul de scanare trebuie să ofere posibilitatea de scanare fără sticla presoare;
l. Durata maximă a unui flux complet (scanare – transfer imagine) trebuie să fie de 2 secunde per imagine (pagină);
m. Echipamentul de scanare trebuie să asigure o viteza zilnică de scanare de minim la 10.000 pagini;
n. Imaginea preluată, color, trebuie să nu prezinte deformări fizice sau optice ale originalului de natură să afecteze lizibilitatea conținutului (ex.: probleme de încadrare, claritatea imaginii, luminozitate, lizibilitate detalii, zone întunecate sau pete care nu există pe original), nici alterări de succesiune a cadrelor. În acest sens se va furniza o platforma software de scanare şi indexare integrată nativ cu echipamentele de scanare. Platforma software trebuie să conţină minim următoarele funcţionalităţi:
    i. Scanarea să se realizeze într-o singură sesiune;
    ii. Funcţie de preview;
    iii. Îndreptarea imaginilor, atât pentru fiecare imagine, dar şi pentru întreaga lucrare;
    iv. Lipirea de pagini în mod automat, dar şi manual;
    v. Tăierea şi separarea unei pagini scanate în mai multe imagini distincte, atât manual, pentru fiecare pagină sau pentru o lucrare în mod automat. Posibilitatea de a păstra imaginile sursă (dupa procesare/tăiere/separare în structura de imagini iniţială;
    vi. Definirea fluxurilor de digitizare şi conversie în funcţie de tipul de document scanat;
    vii. Crearea de profile.

5.7.6. Computere de birou

Computerele de birou trebuie să îndeplinească următoarele specificații:

Specificații tehnice minime	Specificații tehnice extinse
Chipset: Intel Q670 sau echivalent	Chipset: Intel B860 sau echivalent.
Procesor: Intel Core generatia 13 sau echivalent, frecvența minim 2.5 GHz, turbo până la 4.8 GHz, minim 24MB cache, minim 14 nuclee, minim 20 fire de execuție, TDP maxim 65W	Procesor: Intel generația 15 sau echivalent, cu minim 10 nuclee fără HT, frecvență turbo de minim 4.9 GHz, minim 20MB cache
Placa de bază: să facă parte din nomenclatorul de subansamble al firmei producătoare a calculatorului;	Placa de bază: să facă parte din nomenclatorul de subansamble al firmei producătoare a calculatorului;
Memorie: minim 2 sloturi DIMM	Memorie: minim 2 sloturi DIMM
Minim 3 sloturi SATA 3.0 pentru 3.5-inch/2.5-	Minim 1 slot SATA pentru 3.5-inch hard drive

Specificații tehnice minime	Specificații tehnice extinse
inch hard drive si slim optical drive	și 2 sloturi M.2 SSD
Porturi minime: - 4 x USB 3.2 Gen 1 (5 Gbps) – minim doua în față - 4 x USB 2.0 (480Mbps) - minim 2 în față, minim 2 porturi care să permită revenirea din hibernare (Sleep), precum și pornirea cu ajutorul tastaturii sau mouse-ului conectat - 1 x RJ45 - 2 x DisplayPort l.4 - 1 x Serial Port - 1 x HDMI - 1 x port audio universal - 1 x security cable slot - 1 x padlock ring Nu se acceptă adaptoare pentru porturile minime de mai sus.	Porturi minime: - 4 x USB 3.2 Gen 1 (5 Gbps) - 2 x USB 2.0 (480Mbps) - 1x USB-C 3.2 Gen 1 cu suport pentru transfer de date si incarcare la minim 15W - 1 x RJ45 - 1 x DisplayPort l.4 - 1 x HDMI - 1x port pentru microfon - 1x port combo de tip jack casti/microfon - 1x line-out (3.5mm) Nu se acceptă adaptoare pentru porturile minime de mai sus.
Memorie RAM instalată: minim 1 x 16GB, DDR4	Memorie RAM instalată: minim 16 GB, DDR5 de tip DIMM
Placă video integrată, Intel UHD Graphics 770 sau echivalent	Placă video integrată, Intel UHD Graphics 770 sau echivalent
Unitati de stocare: a. M.2 de minim 512GB PCIe NVMe MTBF minim 1.4 milioane ore sau echivalent b. 3.5 inch de minim 1TB 7200rpm Hard Disk Drive sau echivalent	Unitati de stocare: a. M.2 de minim 512GB PCIe NVMe MTBF minim 1.4 milioane ore sau echivalent b. 3.5 inch de minim 1TB 7200rpm Hard Disk Drive sau echivalent
Audio: Integrat Realtek ALC3246 sau echivalent	High Definition (HD) Audio
Conectivitate: a. 10/100/1000, Gigabit Ethernet LAN b. Wi-Fi 6E 802.11ax, 2 antene pentru TX și 2 pentru RX, cu Bluetooth încorporat	Conectivitate: a. 10/100/1000, Gigabit Ethernet LAN b. Wi-Fi 6E 802.11ax, 2 antene pentru TX și 2 pentru RX, cu Bluetooth încorporat
Carcasa echipament: - Tip tower	Carcasa echipament: - Tip tower sau SFF

Specificații tehnice minime	Specificații tehnice extinse
- Accesul la componentele interioare se va face fara a necesita instrumente (tool-less)	- Accesul la componentele interioare se va face fara a necesita instrumente (tool-less)
Sloturi minime: a. un conector M.2 2230 pentru placa Wi-Fi b. un conector M.2 2230/2280 pentru SSD c. un slot Half-height Gen3 PCIe x16 d. două sloturi Half-height Gen3 PCIe x1 slot	Sloturi minime: a. un slot M.2 pentru placa Wi-Fi b. două sloturi M.2 pentru SSD c. un slot PCIe 4.0 x16 d. un slot PCIe 3.0 x1
Sursa de alimentare: - Putere: de minim 300W, - Eficiență: minim 92% (certificată 80 PLUS Platinum) - Conformitate cu ENERGY STAR - cu cablu de alimentare.	Sursa de alimentare: - Putere: de minim 200W, - Eficiență: minim 90% (certificată 80 PLUS Platinum) - Conformitate cu ENERGY STAR - cu cablu de alimentare.
Computerul de birou va fi livrat cu monitor cu următoarele specificații: a. Minim 23.8 inch diagonala utilizabila a ecranului, IPS widescreen 16:9, antiglare, FullHD (minim1920x1080) la 60Hz,	Computerul de birou va fi livrat cu monitor cu următoarele specificații: a. Minim 23.8 inch diagonala utilizabila a ecranului, IPS widescreen 16:9, antiglare, rezoluție minim1920x1080 cu o rata de refresh de mai mare sau egala cu 120Hz,
b. Rata de contrast minim 1000:1	b. Rata de contrast minim 1000:1
c. Strălucire minim 250 cd/mp, timp de răspuns maxim 8ms (5 ms gtg fast mode),	c. Strălucire minim 250 cd/mp, timp de răspuns maxim 8ms (5 ms gtg fast mode),
d. Unghi de vizualizare minim 178 grade vertical și 178 grade orizontal, pixel 0.2745 mm,	d. Unghi de vizualizare minim 178 grade vertical și 178 grade orizontal
e. Conectivitate: • 1 x DP (ver 1.2) • 1 x HDMI (ver 1.4) • 1 x VGA • 1 x SuperSpeed USB 5Gbps (USB3.2 Gen1) upstream	e. Conectivitate: • 1 x DP • 1 x HDMI • 1 x VGA • 1 x SuperSpeed USB 5Gbps (USB3.2 Gen1) upstream • 4 x SuperSpeed USB 5Gbps

Specificații tehnice minime	Specificații tehnice extinse
• 4 x SuperSpeed USB 5Gbps (USB3.2 Gen1)	(USB3.2 Gen1) • 1x USB-C cu 15W power delivery
f. Monitorul va fi dotat cu cablu DP, SuperSpeed USB 5Gbps.	- Monitorul va fi dotat cu cablu DP, SuperSpeed USB 5Gbps
Monitorul va fi dotat cu minim 2 difuzoare cu puterea de ieșire continuă de minim 3,5 W și o gama de frecvențe ca acoperă spectru audio tipic de la 200 Hz la 20 kHz. Sunt acceptate și soluții de tip soundbar, caz în care dispozitvul soundbar trebuie prevăzut cu sistem de prindere pe partea de jos a ecranului monitorului;	Monitorul va fi dotat cu minim 2 difuzoare cu puterea de 2 W și o gama de frecvențe ca acoperă spectru audio tipic pentru întâlniri virtuale și sesiuni online. Sunt acceptate și soluții de tip soundbar, caz în care dispozitvul soundbar trebuie prevăzut cu sistem de prindere pe partea de jos a ecranului monitorului
Securitate: Monitorul trebuie prevazut cu un slot fizic de securitate	Securitate: Monitorul trebuie prevazut cu un slot fizic de securitate
Monitorul va permite:	Monitorul va permite:
Înclinare (Tilt): minim între -5 grade și 21 grade, pentru a permite poziționarea monitorului în sus sau în jos pentru a găsi un unghi optim de vizualizare pentru confort și vizibilitate.	Înclinare (Tilt): minim între -5 grade și 21 grade, pentru a permite poziționarea monitorului în sus sau în jos pentru a găsi un unghi optim de vizualizare pentru confort și vizibilitate.
Ajustare pe înălțime: minim 150 mm,	Ajustare pe înălțime: minim 150 mm,
Pivotare 90°, pentru schimbarea monitorului între orientarea peisaj și cea portret, în cazul anumitot tipuri de sarcini sau fluxuri de lucru.	Pivotare 90°, pentru schimbarea monitorului între orientarea peisaj și cea portret, în cazul anumitot tipuri de sarcini sau fluxuri de lucru.
Rotire: pe orizontală 45° stânga-dreapta, pentru partajarea ecranului cu alții sau pentru ajustarea orientării în funcție de configurația spațiului de lucru;	Rotire: pe orizontală 45° stânga-dreapta, pentru partajarea ecranului cu alții sau pentru ajustarea orientării în funcție de configurația spațiului de lucru;
Cerințe privind eficiența energetică și mediu ce trebuie îndeplinite de monitor:	Cerințe privind eficiența energetică și mediu ce trebuie îndeplinite de monitor:
Îndeplinește criterii specifice de eficiență energetică, contribuind la reducerea consumului de energie și a impactului asupra mediului): Certificare ENERGY STAR;	Îndeplinește criterii specifice de eficiență energetică, contribuind la reducerea consumului de energie și a impactului asupra mediului): Certificare ENERGY STAR;
Monitorul va avea un consum în modul Standby de cel mult 0,5 W conform cerințelor Programului Energy Star pentru Display-uri versiunea 8.0	Monitorul va avea un consum în modul Standby de cel mult 0,5 W conform cerințelor Programului Energy Star pentru Display-uri versiunea 8.0

Specificații tehnice minime	Specificații tehnice extinse
Monitorul va avea un consum în modul Oprit de cel mult 0,3 W conform cerințelor Programului Energy Star pentru Display-uri versiunea 8.0	Monitorul va avea un consum în modul Oprit de cel mult 0,3 W conform cerințelor Programului Energy Star pentru Display-uri versiunea 8.0
Îndeplinește criterii stricte de mediu, inclusiv eficiență energetică, selecție de materiale și gestionare a sfârșitului de viață: Înregistrare EPEAT Gold;	Îndeplinește criterii stricte de mediu, inclusiv eficiență energetică, selecție de materiale și gestionare a sfârșitului de viață: Înregistrare EPEAT Gold;
Respectă restricțiile privind utilizarea anumitor materiale periculoase, cum ar fi plumbul, mercurul, cadmiul și altele, contribuind la reducerea impactului asupra mediului: Conformitate RoHS (Restriction of the Use of Certain Hazardous Substances);	Respectă restricțiile privind utilizarea anumitor materiale periculoase, cum ar fi plumbul, mercurul, cadmiul și altele, contribuind la reducerea impactului asupra mediului: Conformitate RoHS (Restriction of the Use of Certain Hazardous Substances);
Îndeplinește standarde ridicate de mediu și responsabilitate socială: Certificare TCO;	Îndeplinește standarde ridicate de mediu și responsabilitate socială: Certificare TCO;
Nu conține substanțe ignifuge bromurate (BFR) și clorură de polivinil (PVC), cu excepția cablurilor externe.	Nu conține substanțe ignifuge bromurate (BFR) și clorură de polivinil (PVC), cu excepția cablurilor externe.
Monitorul va avea sursa de energie electrica integrată în carcasa acestuia.	Monitorul va avea sursa de energie electrica integrată în carcasa acestuia.
Computerul de birou va fi livrat cu următorul software instalat cu licență: a. Windows 11 Pro 64bit preinstalat, furnizat împreună cu atributele sale originale de legalitate, cum ar fi etichetele GML (Genuine Microsoft Label) sau etichetele COA (Certificate of Authenticity) folosite de producătorul hardware-ului sau alte modalități de certificare a autenticității cerute de producătorul software-ului, în funcție de versiunea furnizată; b. Microsoft Office Home & Business 2021 preinstalat cu licență.	Computerul de birou va fi livrat cu următorul software instalat cu licență: a. Windows 11 Pro 64bit preinstalat, furnizat împreună cu atributele sale originale de legalitate, cum ar fi etichetele GML (Genuine Microsoft Label) sau etichetele COA (Certificate of Authenticity) folosite de producătorul hardware-ului sau alte modalități de certificare a autenticității cerute de producătorul software-ului, în funcție de versiunea furnizată; b. Microsoft Office Home & Business 2021 preinstalat cu licență.
Computerul de birou va avea cheia sistemului de operare încorporată în BIOS pentru a permite reinstalarea sistemului de operare sau partiție de	Computerul de birou va avea cheia sistemului de operare încorporată în BIOS pentru a permite reinstalarea sistemului de operare sau

Specificații tehnice minime	Specificații tehnice extinse
recovery originale fără a mai fi necesară introducerea cheii de produs.	partiție de recovery originale fără a mai fi necesară introducerea cheii de produs.
Licentele sa fie verificabile pe site-ul producatorului dupa seria echipamentului livrat in configuratia de baza.	Licentele sa fie verificabile pe site-ul producatorului dupa seria echipamentului livrat in configuratia de baza.
Autoritatea contractantă își rezervă dreptul de a solicita producătorului sistemelor de operare și Office confirmarea că ofertanții sunt autorizați să comercializeze licențele ofertate în România.	Autoritatea contractantă își rezervă dreptul de a solicita producătorului sistemelor de operare și Office confirmarea că ofertanții sunt autorizați să comercializeze licențele ofertate în România.
Computerul de birou va avea instalată o soluție ce va oferi următoarele funcționalități de salvare (backup) și recuperare în caz de dezastru:	Computerul de birou va avea instalată o soluție ce va oferi următoarele funcționalități de salvare (backup) și recuperare în caz de dezastru:
Permite backup complet al sistemului de operare ofertat, incluzând automat partițiile necesare pentru boot și funcționare.	Permite backup complet al sistemului de operare ofertat, incluzând automat partițiile necesare pentru boot și funcționare.
Suportă backup la nivel de disc, volum și fișiere/foldere.	Suportă backup la nivel de disc, volum și fișiere/foldere.
Trebuie să funcționeze fără a necesita partiții ascunse dedicate OEM pentru backup sau recovery.	Trebuie să funcționeze fără a necesita partiții ascunse dedicate OEM pentru backup sau recovery.
Suportă backup Full, Incremental și Differential.	Suportă backup Full, Incremental și Differential.
Permite backup programat (one-time, zilnic, săptămânal, lunar sau la eveniment).	Permite backup programat (one-time, zilnic, săptămânal, lunar sau la eveniment).
Asigură funcționalitate de Smart Backup, cu backup automat la intervale de 30 de minute pentru fișiere modificate frecvent.	Asigură funcționalitate de Smart Backup, cu backup automat la intervale de 30 de minute pentru fișiere modificate frecvent.
Permite versionarea backup-urilor și restaurarea la un punct anterior în timp.	Permite versionarea backup-urilor și restaurarea la un punct anterior în timp.
Permite salvarea backup-urilor pe:	Permite salvarea backup-urilor pe:
discuri locale,	discuri locale,
unități USB,	unități USB,
locații de rețea,	locații de rețea,
Suportă copiere offsite automată prin FTP a imaginilor de backup.	Suportă copiere offsite automată prin FTP a imaginilor de backup.
Permite criptarea backup-urilor folosind	Permite criptarea backup-urilor folosind algoritm AES-256 .

Specificații tehnice minime	Specificații tehnice extinse
algoritm AES-256 .	
Dispune de funcție de verificare automată a integrității imaginilor de backup (Image Check).	Dispune de funcție de verificare automată a integrității imaginilor de backup (Image Check).
Include un mecanism de protecție a fișierelor de backup împotriva modificărilor neautorizate (Backup Protection).	Include un mecanism de protecție a fișierelor de backup împotriva modificărilor neautorizate (Backup Protection).
Permite recuperarea rapidă a sistemului (BareMetal Recovery;	Permite recuperarea rapidă a sistemului (BareMetal Recovery;
Permite restaurarea pe hardware diferit (System Transfer);	Permite restaurarea pe hardware diferit (System Transfer);
Permite montarea imaginilor de backup ca drive virtual, pentru recuperare granulară de fișiere;	Permite montarea imaginilor de backup ca drive virtual, pentru recuperare granulară de fișiere;
Oferă posibilitatea de creare mediu bootabil WinPE / Pre-OS pentru recuperare în caz de sistem nefuncțional.	Oferă posibilitatea de creare mediu bootabil WinPE / Pre-OS pentru recuperare în caz de sistem nefuncțional.
Soluția va fi oferită sub formă de licență (drept de utilizare) perpetuă sau de tip abonament, caz în care dreptul de utilizare trebuie să fie pentru minim 3 ani.	Soluția va fi oferită sub formă de licență (drept de utilizare) perpetuă sau de tip abonament, caz în care dreptul de utilizare trebuie să fie pentru minim 3 ani.
Computerul de birou va fi dotat cu mouse USB cu scroll, 2 butoane și tastatura silenţioasa USB, 104 taste - US Layout.	Computerul de birou va fi dotat cu mouse USB cu scroll, 2 butoane și tastatura silenţioasa USB, 104 taste - US Layout.
Computerul de birou va fi dotat cu camera web – 2k QHD cu următoarele specificații: a. rezolutie minim 2K QHD / 24, 30 fps b. HD Digital ZOOM minim 2x c. Functie de autofocus d. Video Noise Reduction (3D + 2D) e. Privacy cap integrat f. Certificata Microsoft Teams și Zoom	Computerul de birou va fi dotat cu camera web –QHD cu următoarele specificații: a. rezolutie minim QHD, 30 fps b. Functie de autofocus c. Privacy cap integrat d. Certificata Microsoft Teams și/sau Zoom e. Microfon direcțional
Computerul de birou va dispune de următoarele capabilități de securitate și management: a. Posibilitatea de blocare fizica a accesului în carcasa, standard security slot Data Protection and Encryption Microsoft Windows Bitlocker	Computerul de birou va dispune de următoarele capabilități de securitate și management: a. Posibilitatea de blocare fizica a accesului în carcasa b. Parole pentru BIOS și sistem,

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

Specificații tehnice minime	Specificații tehnice extinse
b. Ștergerea datelor de pe hard diskul local prin BIOS („Secure Erase") c. Comutator de protecție împotriva intervenției neautorizate în șasiu d. Parole pentru BIOS și sistem, securitatea interfețelor de intrare/ieşire e. Tehnologie Intel Trusted Execution sau echivalent f. Tehnologie Intel Identity Protection sau echivalent g. Compatibilitate BIOS optionala pentru Computrace h. Intel Software Guard Extensions sau echivalent i. Senzor pentru detectarea intruziunii neautorizate in carcasa, TPM 2.0	securitatea interfețelor de intrare/ieşire c. Compatibilitate BIOS optionala pentru Computrace d. Chip de securitate integrat de tip discrete TPM 2.0 certificat
Computerul de birou va dispune de următoarele certificări și va respecta următoarele standarde privind:	Computerul de birou va dispune de următoarele certificări și va respecta următoarele standarde privind:
Îndeplinește criterii specifice de eficiență energetică, contribuind la reducerea consumului de energie și a impactului asupra mediului: Certificare ENERGY STAR versiunea 8.0;	Îndeplinește criterii specifice de eficiență energetică, contribuind la reducerea consumului de energie și a impactului asupra mediului: Certificare ENERGY STAR versiunea 8.0;
Consum maxim în modul Pornit (E_{TEC_MAX}) prin care să îndeplinească cerințele Programului Energy Star pentru Computere versiunea 8.0	Consum maxim în modul Pornit (E_{TEC_MAX}) prin care să îndeplinească cerințele Programului Energy Star pentru Computere versiunea 8.0
Îndeplinirea unor criterii de siguranță pentru a proteja utilizatorii de pericole electrice și alte riscuri: certificare IEC 60950-1;	Îndeplinirea unor criterii de siguranță pentru a proteja utilizatorii de pericole electrice și alte riscuri: certificare IEC 60950-1;
Îndeplinirea cerințelor de a gestiona și recicla produsele electronice la sfârșitul ciclului lor de viață pentru a reduce impactul asupra mediului conform Directivei 2012/19/EU privind Deșeurile de Echipamente Electrice și Electronice;	Îndeplinirea cerințelor de a gestiona și recicla produsele electronice la sfârșitul ciclului lor de viață pentru a reduce impactul asupra mediului conform Directivei 2012/19/EU privind Deșeurile de Echipamente Electrice și Electronice;
Îndeplinirea condițiilor de funcționare în ceea ce privește temperatura, umiditatea, vibrațiile și	Îndeplinirea condițiilor de funcționare în ceea ce privește temperatura, umiditatea, vibrațiile

Specificații tehnice minime	Specificații tehnice extinse
șocurile: conformitate cu standardul MIL-STD 810H;	și șocurile: conformitate cu standardul MIL-STD 810H;
Îndeplinirea cerințelor de securitate privind modulele criptografice: certificare FIPS 140-2;	Îndeplinirea cerințelor de securitate privind modulele criptografice: certificare FIPS 140-2;
Computerul de birou va fi furnizat cu ambalaj cu o proporție de material reciclat de minim 10%.	Computerul de birou va fi furnizat cu ambalaj cu o proporție de material reciclat de minim 10%.
Temperatura de funcționare a sistemului de la +5° la +35°C.	Temperatura de funcționare a sistemului de la +5° la +35°C.
Computerul de birou trebuie să conțină service tag, pentru a facilita accesul la informațiile de service și garanție direct pe website-ul producătorului, prin care se asigură următoarele: - Suport pentru monitorizarea furnizării rezoluțiilor necesare și coordonarea pro-activa a managementului evenimentelor și a comunicării; - Managementul cazurilor, inclusiv escaladarea evenimentelor pentru o rezoluție rapidă; - Raportarea telefonică a defectelor 24 de ore pe zi, 7 zile pe săptămână. - Suport tehnic pentru hardware-ul și software-ul OEM achiziționat cu dispozitivul, livrat de la distanță sau la locul de instalare a dispozitivului, în funcție de tipul de defecțiune raportat; - Posibilitatea de a descărca versiunile curente ale driverelor și firmware-ului dispozitivului - Descărcarea de software gratuit pentru diagnosticarea automata și raportarea de la distanță a defecțiunilor.	Computerul de birou trebuie să conțină service tag sau echivalent, pentru a facilita accesul la informațiile de service și garanție, prin care se asigură următoarele: - Suport pentru monitorizarea furnizării rezoluțiilor necesare și coordonarea pro-activa a managementului evenimentelor și a comunicării; - Managementul cazurilor, inclusiv escaladarea evenimentelor pentru o rezoluție rapidă; - Raportarea telefonică a defectelor 24 de ore pe zi, 7 zile pe săptămână. - Suport tehnic pentru hardware-ul și software-ul OEM achiziționat cu dispozitivul, livrat de la distanță sau la locul de instalare a dispozitivului, în funcție de tipul de defecțiune raportat; - Posibilitatea de a descărca versiunile curente ale driverelor și firmware-ului dispozitivului - Descărcarea de software gratuit pentru diagnosticarea automata și raportarea de la distanță a defecțiunilor.

5.7.7. Computere portabile

Computerele portabile trebuie să îndeplinească următoarele specificații:

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

Specificații tehnice minime	Specificații tehnice extinse
Chipset: Intel sau echivalent	Chipset: Intel sau echivalent
Procesor: minim Intel Core I5 sau echivalent, frecventa de baza minim 1.9GHz, minim12MB cache, minim 12 core-uri, minim16 fire de execuție (turbo 4.7 GHz), maxim 28W	Procesor: Intel sau echivalent de generația nouă cu AI Boost, cu minim 12 nuclee, frecvență turbo de minim 4.9 GHz, minim 12MB Cache și care poate procesa minim 12 trilioane de operații pe secundă dedicate sarcinilor AI.
Memorie: minim 2 sloturi DIMM	Memorie: minim 2 sloturi DIMM
Memorie RAM instalată: minim 1 x 16GB, DDR4, minim 3200MT/s	Memorie RAM instalată: minim 1 x 16GB, DDR5, minim 3200MT/s
Porturi minime: a. 1 x HDMI minim1.4b b. 1 x LAN RJ-45 c. 1 x USB 3.2 Gen1 (5 Gbps) d. 1 x USB 3.2 Gen1 (5 Gbps) care asigură furnizarea de energie pentru alimentarea dispozitivelor conectate chiar și atunci când computerul este oprit e. 1x Thunderbolt 4 cu DisplayPort Alt Mode/ Power Delivery f. 1 x headphone and microphone combo port g. 1 x security cable slot	Porturi minime: a. 1 x HDMI minim1.4b b. 1 x LAN RJ-45 c. 1 x USB 3.2 Gen1 (5 Gbps) d. 1 x USB 3.2 Gen1 (5 Gbps) care asigură furnizarea de energie pentru alimentarea dispozitivelor conectate chiar și atunci când computerul este oprit e. 1x Thunderbolt 4 cu DisplayPort Alt Mode/ Power Delivery f. 1 x headphone and microphone combo port g. 1 x security cable slot
Nu se acceptă adaptoare pentru porturile minime de mai sus.	Nu se acceptă adaptoare pentru porturile minime de mai sus.
Placă video integrată, Intel Graphics sau echivalent	Placă video integrată, Intel Graphics sau echivalent
Unitati de stocare: M.2 de minim 512GB PCIe NVMe MTBF minim 1.4 milioane ore sau echivalent	Unitati de stocare: M.2 de minim 512GB SSD PCIe Gen 4
Audio Integrat Realtek ALC3204 (minim 2 x 2W) sau echivalent	Audio integrat HD, difuzoare stereo (minim 2 x 2W), Dolby Audio sau echivalent
Conectivitate: a. placa de retea integrata Gigabit (10/100/1000 Mbps) b. Intel AX211 WiFi 6e 2x2 AX sau	Conectivitate: a. placa de retea integrata Gigabit (10/100/1000 Mbps) b. Intel AX211 WiFi 6e 2x2 AX sau

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

Specificații tehnice minime	Specificații tehnice extinse
echivalent, cu capabilitate BlueTooth integrată.	echivalent, cu capabilitate BlueTooth integrată.
Baterie cu următoarele caracteristici: - capacitate minimă de 51 watt-ore; - capabilitate de încărcare rapidă; - încărcare prin adaptor de minim 65W curent alternativ prin port USB Type-C; livrat cu cablu de alimentare.	Baterie cu următoarele caracteristici: - capacitate minimă de 51 watt-ore; - capabilitate de încărcare rapidă; - încărcare prin adaptor de minim 65W curent alternativ prin port USB Type-C; - livrat cu cablu de alimentare.
Display cu următoarele caracteristici: - minim 15.6 inch Non-Touch full HD cu rezoluția de minim 1920 x1080, tehnologie IPS; - Anti-Glare, minim 400 nits, contrast minim 800:1, pixel pitch 0.179 x 0.179 mm, - Dotat cu camera web full HD cu capabilitate IR ce asigură login prin recunoaștere facială, cu Camera Shutter; Microfon încorporat și Temportal Noise Reduction	Display cu următoarele caracteristici: - minim 15.6 inch Non-Touch full HD cu rezoluția de minim 1920 x1080, tehnologie IPS; - Anti-Glare, minim 400 nits, contrast minim 800:1, pixel pitch 0.179 x 0.179 mm, - Dotat cu camera web full HD cu capabilitate IR ce asigură login prin recunoaștere facială, cu Camera Shutter; - Microfon încorporat și Temportal Noise Reduction
Computerul portabil va dispune de: - Tastatură încorporată cu layout US (QWERTY); - Dispozitiv de navigare încorporat care va fi utilizat pentru a mișca cursorul pe ecran și pentru a executa funcții de clic; - Cititor încorporat de Smart Carduri; Cititor de amprentă care respectă standardul FIPS și asigură stocarea protejată a datelor biometrice.	Computerul portabil va dispune de: - Tastatură încorporată cu layout US (QWERTY); - Dispozitiv de navigare încorporat care va fi utilizat pentru a mișca cursorul pe ecran și pentru a executa funcții de clic; - Cititor încorporat de Smart Carduri; - Cititor de amprentă care respectă standardul FIPS și asigură stocarea protejată a datelor biometrice.
Computerul portabil va avea un chip/modul de securitate integrat pe placa de baza tip TPM 2.0 care oferă posibilitatea criptarii datelor atat hardware cat si software, precum și un cititor de amprenta capacitiv cu rezolutie senzor de	Computerul portabil va avea un chip/modul de securitate integrat pe placa de baza tip TPM 2.0 care oferă posibilitatea criptarii datelor atat hardware cat si software, precum și un cititor de amprenta capacitiv cu rezolutie senzor de

Specificații tehnice minime	Specificații tehnice extinse
minim 500 dpi.	minim 500 dpi.
Computerul portabil va fi livrat cu următoarele accesorii: i. Geantă de umăr/Rucsac cu următoarele specificații: - Dimensiune compatibilă cu laptopul - buzunar frontal cu fermoar; - rezistentă la apă; - compartiment pentru laptop captusit cu spuma; Mouse USB cu fir cu minim 3 butoane și minim 1000 dpi	Computerul portabil va fi livrat cu următoarele accesorii: i. Geantă de umăr/Rucsac cu următoarele specificații: - Dimensiune compatibilă cu laptopul - buzunar frontal cu fermoar; - rezistentă la apă; - compartiment pentru laptop captusit cu spuma; ii. Mouse USB cu fir cu minim 3 butoane și minim 1000 dpi
Cerințe privind eficiența energetică și mediu ce trebuie îndeplinite de computerul portabil:	Cerințe privind eficiența energetică și mediu ce trebuie îndeplinite de computerul portabil:
Este eficient energetic, contribuind la reducerea consumului de energie și a impactului asupra mediului: Certificare ENERGY STAR versiunea 8.0;	a. Este eficient energetic, contribuind la reducerea consumului de energie și a impactului asupra mediului: Certificare ENERGY STAR versiunea 8.0;
b. Îndeplinește criterii stricte de mediu, inclusiv eficiență energetică, selecție de materiale și gestionare a sfârșitului de viață: Înregistrare EPEAT Gold;	c. Îndeplinește criterii stricte de mediu, inclusiv eficiență energetică, selecție de materiale și gestionare a sfârșitului de viață: Înregistrare EPEAT Gold;
d. Respectă restricțiile privind utilizarea anumitor materiale periculoase, cum ar fi plumbul, mercurul, cadmiul și altele, contribuind la reducerea impactului asupra mediului: Conformitate RoHS (Restriction of the Use of Certain Hazardous Substances);	e. Respectă restricțiile privind utilizarea anumitor materiale periculoase, cum ar fi plumbul, mercurul, cadmiul și altele, contribuind la reducerea impactului asupra mediului: Conformitate RoHS (Restriction of the Use of Certain Hazardous Substances);
f. Îndeplinește standarde ridicate	g. Îndeplinește standarde ridicate

Specificații tehnice minime	Specificații tehnice extinse
de mediu și responsabilitate socială: Certificare TCO Generația 9.;	de mediu și responsabilitate socială: Certificare TCO Generația 9.;
h. Nu conține substanțe ignifuge bromurate (BFR) și clorură de polivinil (PVC), cu excepția cablurilor externe.	i. Nu conține substanțe ignifuge bromurate (BFR) și clorură de polivinil (PVC), cu excepția cablurilor externe.
Computerul portabil va fi livrat cu următorul software instalat cu licență: a. Windows 11 Pro 64bit preinstalat, furnizat împreună cu atributele sale originale de legalitate, cum ar fi etichetele GML (Genuine Microsoft Label) sau etichetele COA (Certificate of Authenticity) folosite de producătorul hardware-ului sau alte modalități de certificare a autenticității cerute de producătorul software-ului, în funcție de versiunea furnizată; b. Office Home & Business 2021 preinstalat cu licență.	Computerul portabil va fi livrat cu următorul software instalat cu licență: a. Windows 11 Pro 64bit preinstalat, furnizat împreună cu atributele sale originale de legalitate, cum ar fi etichetele GML (Genuine Microsoft Label) sau etichetele COA (Certificate of Authenticity) folosite de producătorul hardware-ului sau alte modalități de certificare a autenticității cerute de producătorul software-ului, în funcție de versiunea furnizată; b. Office Home & Business 2021 preinstalat cu licență.
Computerul portabil va avea cheia sistemului de operare încorporată în BIOS pentru a permite reinstalarea sistemului de operare sau partiție de recovery originale fără a mai fi necesară introducerea cheii de produs.	Computerul portabil va avea cheia sistemului de operare încorporată în BIOS pentru a permite reinstalarea sistemului de operare sau partiție de recovery originale fără a mai fi necesară introducerea cheii de produs.
Licentele sa fie verificabile pe site-ul producatorului dupa seria echipamentului livrat in configuratia de baza.	Licentele sa fie verificabile pe site-ul producatorului dupa seria echipamentului livrat in configuratia de baza.
Autoritatea contractantă își rezervă dreptul de a solicita producătorului sistemelor de operare și Office confirmarea că ofertanții sunt autorizați să comercializeze licențele ofertate în România.	Autoritatea contractantă își rezervă dreptul de a solicita producătorului sistemelor de operare și Office confirmarea că ofertanții sunt autorizați să comercializeze licențele ofertate în România.
Computerul de birou va avea instalată o soluție ce va oferi următoarele funcționalități de salvare (backup) și recuperare în caz de	Computerul de birou va avea instalată o soluție ce va oferi următoarele funcționalități de salvare (backup) și recuperare în caz de

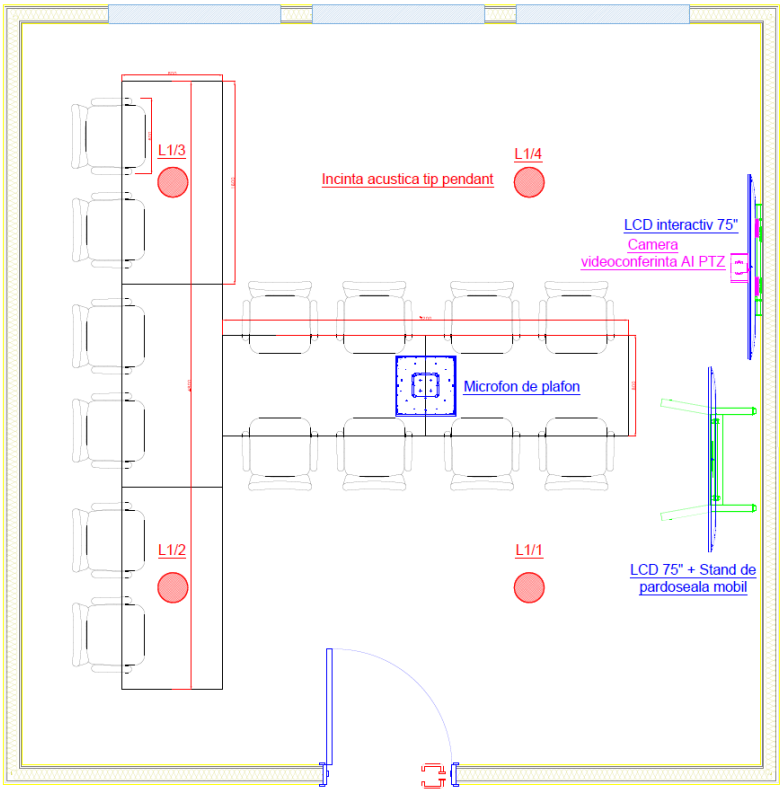
Specificații tehnice minime	Specificații tehnice extinse
dezastru:	dezastru:
• Permite backup complet al sistemului de operare ofertat, incluzând automat partițiile necesare pentru boot și funcționare.	• Permite backup complet al sistemului de operare ofertat, incluzând automat partițiile necesare pentru boot și funcționare.
• Suportă backup la nivel de disc, volum și fișiere/foldere.	• Suportă backup la nivel de disc, volum și fișiere/foldere.
• Trebuie să funcționeze fără a necesita partiții ascunse dedicate OEM pentru backup sau recovery.	• Trebuie să funcționeze fără a necesita partiții ascunse dedicate OEM pentru backup sau recovery.
• Suportă backup Full, Incremental și Differential.	• Suportă backup Full, Incremental și Differential.
• Permite backup programat (one-time, zilnic, săptămânal, lunar sau la eveniment).	• Permite backup programat (one-time, zilnic, săptămânal, lunar sau la eveniment).
• Asigură funcționalitate de Smart Backup, cu backup automat la intervale de 30 de minute pentru fișiere modificate frecvent.	• Asigură funcționalitate de Smart Backup, cu backup automat la intervale de 30 de minute pentru fișiere modificate frecvent.
• Permite versionarea backup-urilor și restaurarea la un punct anterior în timp.	• Permite versionarea backup-urilor și restaurarea la un punct anterior în timp.
• Permite salvarea backup-urilor pe:	• Permite salvarea backup-urilor pe:
• discuri locale,	• discuri locale,
• unități USB,	• unități USB,
• locații de rețea,	• locații de rețea,
• Suportă copiere offsite automată prin FTP a imaginilor de backup.	• Suportă copiere offsite automată prin FTP a imaginilor de backup.
• Permite criptarea backup-urilor folosind algoritm AES-256 .	• Permite criptarea backup-urilor folosind algoritm AES-256 .
• Dispune de funcție de verificare automată a integrității imaginilor de backup (Image Check).	• Dispune de funcție de verificare automată a integrității imaginilor de backup (Image Check).
• Include un mecanism de protecție a fișierelor de backup împotriva modificărilor neautorizate (Backup Protection).	• Include un mecanism de protecție a fișierelor de backup împotriva modificărilor neautorizate (Backup Protection).

Specificații tehnice minime	Specificații tehnice extinse
• Permite recuperarea rapidă a sistemului (BareMetal Recovery;	• Permite recuperarea rapidă a sistemului (BareMetal Recovery;
• Permite restaurarea pe hardware diferit (System Transfer);	• Permite restaurarea pe hardware diferit (System Transfer);
• Permite montarea imaginilor de backup ca drive virtual, pentru recuperare granulară de fișiere;	• Permite montarea imaginilor de backup ca drive virtual, pentru recuperare granulară de fișiere;
• Oferă posibilitatea de creare mediu bootabil WinPE / Pre-OS pentru recuperare în caz de sistem nefuncțional.	• Oferă posibilitatea de creare mediu bootabil WinPE / Pre-OS pentru recuperare în caz de sistem nefuncțional.
Soluția va fi oferită sub formă de licență (drept de utilizare) perpetuă sau de tip abonament, caz în care dreptul de utilizare trebuie să fie pentru minim 3 ani.	Soluția va fi oferită sub formă de licență (drept de utilizare) perpetuă sau de tip abonament, caz în care dreptul de utilizare trebuie să fie pentru minim 3 ani.
Computerul portabil va dispune de următoarele certificări și va respecta următoarele standarde privind: - Îndeplinirea unor criterii de siguranță pentru a proteja utilizatorii de pericole electrice și alte riscuri: certificare IEC 60950-1; - Îndeplinirea cerințelor de a gestiona și recicla produsele electronice la sfârșitul ciclului lor de viață pentru a reduce impactul asupra mediului conform Directivei 2012/19/EU privind Deșeurile de Echipamente Electrice și Electronice; Îndeplinirea cerințelor de securitate privind modulele criptografice: certificare FIPS 140-2;	Computerul portabil va dispune de următoarele certificări și va respecta următoarele standarde privind: - Îndeplinirea unor criterii de siguranță pentru a proteja utilizatorii de pericole electrice și alte riscuri: certificare IEC 60950-1; - Îndeplinirea cerințelor de a gestiona și recicla produsele electronice la sfârșitul ciclului lor de viață pentru a reduce impactul asupra mediului conform Directivei 2012/19/EU privind Deșeurile de Echipamente Electrice și Electronice; - Îndeplinirea cerințelor de securitate privind modulele criptografice: certificare FIPS 140-2;
Computerul portabil va avea o greutate de cel mult 1,65 Kg ± 10%.	Computerul portabil va avea o greutate de cel mult 1,65 Kg ± 10%.
Computerul portabil va fi furnizat cu ambalaj cu o proporție de material reciclat de minim 10%.	Computerul portabil va fi furnizat cu ambalaj cu o proporție de material reciclat de minim 10%.

5.7.8. Sistem de videoconferință

Sala de consiliu din cadul CNCD va fi dotată cu un sistem de videoconferință.

Sala de conferință va fi dotată cu 5 mese aranjate în formă de T conform următorului plan de amplasament:



Mesele și scaunele vor fi prevăzute cu roți pentru a permite re-aranjarea sălii pentru activități specifice CNCD.

Pentru desfășurarea ședințelor consiliului, sistemul de videoconferință va fi compus din cel puțin următoarele elemente:

Nr. crt.	Descriere	U/M	Cantitate
1	Display interactiv	Buc.	1
2	Suport de prindere pe perete pentru ecranul LCD interactiv	Buc.	1
3	Accesoriu tip pull-out pentru acces facil la ecranului LCD	Buc.	1
4	Ecran LCD profesional	Buc.	1
5	Kit Videoconferință	Buc.	1
6	Camera Video PTZ	Buc.	1
7	Microfon de plafon	Buc.	1

8	Procesor audio	Buc.	1
9	Amplificator Audio	Buc.	1
10	Difuzor tip pendant	Buc.	4
11	Switch PoE	Buc.	1
12	Distribuitor amplificator 1:2	Buc.	1
13	Echipament inregistrare	Buc.	1
14	Masă conferință	Buc.	5
15	Scaun conferință	Buc.	20

Acestea trebuie să îndeplinească cerințele minimale descrise în continuare.

5.7.8.1 Display interactiv

Caracteristică	**Cerință minimală**
Diagonala	Minim 75"
Tip ecran	LCD
Raport de aspect	16:9
Culori de afisare	Minim 1,07 miliarde (10 biti)
Rezolutie	Minim 4K UHD (3840x2160 @60Hz)
Timp de raspuns	Maxim 5ms
Refresh	Minim 60Hz
Unghi de vizualizare	Minim 178˚
Luminozitate	Minim 500cd/m²
Contrast	Minim 4000:1
Duritatea sticlei	Sticla temperată AG cu Nivel Mohs 7 astfel încât să ofere protecție împotriva zgârieturilor, cu avantajul suplimentar de a reduce reflexiile și amprentele.
Tip de sticla	- Design al ecranului tactil în care nu există spațiu de aer între ecranul tactil și ecranul LCD - Anti-reflexie si anti-amprente pentru durabilitate - Suprafata Antibacteriana
Durata de viata a ecranului	Minim 50.000 de ore
Specificatii tehnice interactivitate Tehnologie de scriere	 Tehnologie IR de inalta precizie + Senzor de clasificare a materialelor
Puncte de atingere	Minim 50
Rezoluție de atingere	32768 x 32768pixeli
Timp de raspuns	Maxim 5ms
Precizie la atingere	±1mm

Caracteristică	**Cerință minimală**
Dimensiunea minima a obiectului	2mm
Instrument de atingere	Deget, pen pasiv, obiecte opace
Scriere simultana	Da
Pen incluse	Minim 2
Tipul pen	Pen cu recunoastere duala
Suport pentru pen	Suport magnetic integrat pentru pen
Diametru varf pen	3mm/7mm
Diferentiere intre pen si atingere	Da
Adnotare peste orice sursa	Da
Aplicații incluse	Tabla virtuala, Adnotare, Cronometru, Player media, Browser, Cititor PDF, Inregistrare ecran, Spinner, Votare, Instrumente matematice.
Compatibilitate	Windows, Linux, Mac, Android, Chrome
Rata de urmarire	1m/s
Rata de scanare	100 Hz
Conectivitate	Minim 3x Intrari HDMI; Minim 1x Iesire HDMI; Minim 3x USB-A 2.0; Minim 3x USB Touch (tip B); Minim 4x USB A 3.0; Minim 2x USB-C (Video, Audio, Touch si Retea) Minim 1x USB-C pentru transfer de date; Minim 1x Iesire USB-C (Video, Audio, Touch si Retea); Minim 1x Intrare DisplayPort; Minim 1x Intrare LAN (RJ45); Minim 1x Iesire LAN (RJ45); Minim 1x RS-232; Wake-on-LAN: Da; Adaptor wireless 2.0 + Punct de acces wireless (WAP): Da; Modul WiFi: Da Bluetooth: 5.2; Minim 1x Intrare audio 3.5mm; Minim 1x Iesire audio pe conector optic; Minim 1x Iesire casti 3.5mm; Minim 3x Iesiri Touch; Cititor NFC integrat; Senzor de proximitate; WIFI: IEEE 802.11a/b/g/n/ac/ax (benzi de frecventa 2,4 si 5 GHz) Capabil de viteze de pana la 1GB.

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

Caracteristică	Cerință minimală
Sistem de operare	Minim Android 13sau similar
RAM	Minim 8GB
Stocare interna	Minim 128GB
CPU	Minim 4 nuclee de înaltă performanță de tip Arm Cortex -A76 sau similar și 4 nuclee proiectate pentru eficiență și consum redus de tip ARM Cortex-A55 sau similar
GPU	ARM Mali G610 MC4 sau similar
Rezolutie Android	4K
Certificare Google	EDLA (Acord de Licenta pentru Dispozitive Enterprise)
Acces la aplicatiile din Google Play Store	Da (certificat)
Acces la aplicatiile Microsoft	Da (certificat)
Acces la serviciile Google Cloud	Da (certificat)
Difuzoare	Minim 2x20W + 2x10W Subwoofer
Tensiune de alimentare	100-240V ~ 50/60Hz
VESA	800x400
Caracteristici integrate	Mirroring - oricarui dispozitiv pe tabla: Gratuit pe durata de viata a ecranului; Profile de conturi personalizate integrate; Adnotare pe tabla alba; Trimitere directa de email de pe ecranul tactil; Actualizari over-the-air;
Accesorii incluse	Cablu HDMI lungime 1.5m, Cablu USB (A-B) lungime 3m, Cablu USB-C lungime 1.5m, Cablu de alimentare lungime 3m, Telecomanda, Baterii pentru telecomanda, 2x Pen, Ghid pentru Utilizator, Ghid de Instalare Rapida, Adaptor WiFi 2.0 + WAP.
Certificari	CE, FCC, UL, Energy Star & EEC

5.7.8.2 Suport de prindere pe perete pentru ecranul LCD interactiv

Caracteristică	Cerință minimală
Tip	Suport perete pentru display-uri cu diagonala 55” – 100”;
Orientare	Landscape
Adjustabilitate	Fixa, Micro-ajustabila, Reglabila pe inaltime, Deplasare lateral;
Greutatea suportata	Cel puțin dublu față de greutatea display-ului interactiv propus
VESA	100 x 100 mm - 1070 x 600 mm

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

Culoare	Negru
Certificari	OSHPD, TUV, UL Listed

5.7.8.3 Accesoriu tip pull-out pentru acces facil la ecranului LCD

Caracteristică	**Cerință minimală**
Tip	Accesoriu tip pull-out
Aplicatie	Perete
Tip solutie	Universal
Caracteristici speciale	Multi-Display
Adancime	Maximum 39mm
Ajustare	+0.5° / -2°
Culoare	Negru

5.7.8.4 Ecran LCD profesional

Caracteristică	**Cerință minimală**
Tip	Ecran LCD profesional
Diagonala	Minim 75”
Tip panou	VA
Haze	25% (Anti-Glare)
Raport de aspect	16:9
Rezolutie	Minimum 3840 × 2160pixeli
Refresh	Minimum 60Hz
Luminozitate	Minimum 800niti
Tip iluminare de fundal	DLED
Contrast	Minimum 6000:1
Unghi de vizualizare (H × V)	178°
Timp de raspuns	Maximum 6.5ms
Durata de viata	Minimum 50000 de ore
Orientare	Landscape si Portret
Player intern	Procesor: Minimum A55 × 4 nuclee similar; Grafica: Minimum Mali-G52 × 2 sau similar; Memorie: Minimum 4GB; Stocare: Minimum 32GB.
Conectivitate	Minimum 3x Intrari HDMI 2.1, HDMI 1 suporta ARC; Minimum 1x USB 2.0; Minimum 1x USB 3.0; Minimum 1x USB Tip C;

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

Caracteristică	Cerință minimală
	Minimum 1x RS-232; Minimum 1x Intrare RJ45 10M / 100M / 1000Mbps; Minimum 1x Iesire HDMI; Minimum 1x Iesire Audio pe conector mini jack 3.5mm’ Minimum 1x Iesire SPDIF; Minimum 1x Iesire RJ45 10M / 100M / 1000Mbps; 1x Slot OPS; 1x Slot modul Wi-Fi; Wi-Fi: Suporta Wi-Fi 6, 802.11ac/b/g/n/a/ax, 2.4GHz/5GHz; Bluetooth: Minimum 5.2
Difuzoare	Minimum 2x 16W
VESA	800x600mm
Certificari	Siguranta: IEC 62368-1; EMC: Clasa B; Erp: Da; Energy Star: Da.
Accesorii incluse	Cablu de alimentare, 1x Cablu HDMI, 1x Modul Wi-Fi, Telecomanda, Stand mobil de pardoseala.

5.7.8.5 Kit Videoconferință

Caracteristică	Cerință minimală
Tip	Kit videoconferinta alcătuit din mini PC cu Windows 10 IoT si touchpanel pentru controlul sesiunilor de videoconferinta cu diagonala de 10.1"
Specificatii tehnice mini PC Procesor	Procesor Intel Core i5 cu minim 4 nuclee, 8 fire de execuție, frecventa turbo de minim 4 GHz, minim 8MB Cache sau echivalent; interfata grafica integrata
Chipset	Intel SoC (System on Chip) sau echivalent
Capacitate de stocare	Minim 256GB SSD M2 PCIe
Memorie	Minim 8GB DDR4-3200 dual-channel
Minim intrari/iesiri (nu se accepta adaptoare):	2x USB 3.2 Gen 2 (unul pentru dispozitivului de captare si transmisie audio, respectiv unul pentru conectarea camerei video) 1x USB 3.2 Gen1 1x Thunderbolt™ 4 1x USB-C 3.2 Gen 1 (pentru conectarea tabletei de control) 1x HDMI-in 2x HDMI-out 1.4

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

Caracteristică	Cerință minimală
	1x Ethernet * Nu se accepta adaptoare sau improvizatii pentru pentru interfetele echipamentului
Comunicatii/ conectivitate	1 port conectare in reteaua LAN de tip Gigabit Ethernet, Intel Ethernet Connection I219-LM sau echivalent, cu suport WoL (Wake-on-LAN) Adaptor combo wireless si bluetooth: 11ac wireless, M.2 Card, Intel Wireless-AC 9560 (dual band), Wi-Fi + Bluetooth 5.0 combo, cu suport Intel vPro technology, 2x2
Carcasa	Format cu dimensiuni reduse; kit VESA mount inclus
Alimentare	Adaptor cu putere de 90 Watti, 100V - 240V autosensing, sursa de putere cu eficienta de minim 88%
Sistem de operare	Windows 10 IoT Enterprise SAC 64 bit sau echivalent, preinstalat
Administrare	Echipamentul va asigura suport pentru administrare prin Intel Active Management Technology 15.0 (Intel AMT 15.0) sau echivalent
Securitate	Chip de securitate integrat TPM 2.0, certificat TGP Posibilitatea de a bloca / debloca individual porturile USB – protectie de tip Smart USB Power-on password; Administrator password; Hard disk password Slot pentru cablu de tip Kensington lock sau echivalent
Specificatii tehnice touchpanel Diagonala	Display cu diagonala de minim 10", rezolutie minima de 1280x800 pixeli, luminozitate de minim 320 nits, aspect ratio 16:10, Anti-Glare
Rezolutie	Minimum 1280x800pixeli
Suprafata	Suprafata display-ului trebuie sa fie tratata contra urmelor de degete.
Multi-touch	Suport multi-touch in 10-puncte
Senzori	Flexibilitate în pozitionare pe echipamentul de gestiune a videoconferintei la 30° sau 60°; Tableta va fi prevazuta cu senzori infra-rosu pentru detectia miscarii la o distanta de minim 3 metri si la un unghi de minim 90°.
Conectivitate	Tableta de control va fi prevazuta cu urmatoarele porturi: 1x Port Ethernet Gigabit RJ45; 1x Slot de securitate de tip Kensington lock sau echivalent, 1x Intrare HDMI, 1x Conector de alimentare (pe Cutia de conexiune), 1x Port Ethernet Gigabit RJ45 (pe Cutia de conexiune), 1x Iesire HDMI (pe Cutia de conexiune), 1x USB-B (pe Cutia de conexiune)
Accesorii	Accesoriu montare touchpanel pe perete

5.7.8.6 Camera Video PTZ

Caracteristică	Cerință minimală
Tip	Camera Video PTZ
Senzor Imagine	1/2.8 Sony CMOS sau similar
Zoom Optic	Minim 12x
Unghi de vizualizare orizontal(PTZ)	Minim 67º
Unghi de vizualizare vertical(PTZ)	Minim 53 º
Unghi de vizualizare orizontal(Referinta)	Minim 102º
Unghi de vizualizare vertical(Referinta)	Minim 56 º
Functii video inteligente	Incardare a participantilor si urmarire a prezentatorului prin intermediul AI, posibilitate comutare multi-camera
Iesiri video	3G-SDI, HDMI, USB, ONVIF, RTSP
Comunicatie	USB-B 3.0, RJ-45, RS-232, RS-485, VISCA/TCP, VISCA/UDP, PELCO-D, PELCO-P, ONVIF
Alimentare	PoE, IEEE 802.3af sau prin alimentator suplimentar
Format semnal	SDI sau HDMI: 1080p60/59.94/50/30/29.94/25, 720p60/59.95/50; USB: 1080p30/25, 720p30/25, 360p30.
Accesorii	Echipamentul trebuie sa fie livrat cu suport universal de montare

5.7.8.7 Microfon de plafon

Caracteristică	Cerință minimală
Tip	Microfon de plafon
Tip acoperire	Automata sau directionabila
Tensiunea de alimentare	PoE, Clasa 0
Software de control	Designer sau aplicatie web
Protectie impotriva prafului	IP5X conform IEC 60529
Cerinte pentru cabluri	Cat5e sau mai mare (cabluri ecranate)
Tip conector	RJ45
Audio	Iesire digitala AES67 sau Dante; Acoperire automata activata: 2 canale in total (1 iesire, 1 canal pentru referinta AEC); Acoperire automata dezactivata: 10 canale in total (8 canale de

Caracteristică	Cerință minimală
	transmitere independente, 1 iesire pentru automix, 1 canal pentru referinta AEC); Rata de esantionare: 48 kHz; Adancimea de biti: 24
Sensibilitatea la 1kHz	−1.74 dBFS/Pa
SPL Maximum	95.74 dBSPL
Raport semnal-zgomot	Maximum 76 dB
Dinamica	77.5 dB
Procesare digitala a semnalului	Mixare automata, anulare ecou acustic (AEC), reducere de zgomot, control automat al amplificarii, compresor, intarziere, egalizator (parametric cu 4 benzi), functie de intrerupere (mute), amplificare (interval de 140 dB)
Raspuns in frecventa	Minimum intervalul 126Hz – 19000Hz
Accesorii	Kit instalare microfon plafon

5.7.8.8 Procesor audio

Caracteristică	Cerință minimală
Tip	Procesor audio
Intrare	Minimum 2x conector bloc cu 3 pini (Balansat activ)
Iesire	Minimum 2x conector bloc cu 3 pini (Impedanta balansata)
Mobil	Minimum 1x TRRS 3.5mm
Conexiuni USB	Minimum 1x USB 2.0 Tip B Un singur port transporta 2 canale de intrare si 2 canale de iesire (mono sumat)
Conexiuni de retea (Audio Digital Dante)	Minimum 1x RJ45 Minimum 10 intrari Dante, 8 iesiri Dante
Tensiune de alimentare	802.3 at Type 2 (PoE Plus), Clasa 4
Software de control	Da
Audio digital Dante	Raspuns in frecventa: Minimum intervalul 21-19000Hz; Rata de esantionare: 48 kHz; Adancimea de biti: 24
Audio USB	Rata de esantionare: 48 kHz; Adancimea de biti: 16, 24
Distorsiune armonica totala @ 1 kHz, intrare 0 dBV, amplificare analogica 0dB	<0.05%
Impedanta de intrare	9.6kΩ

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

Caracteristică	Cerință minimală
Impedanta de iesire	80Ω
Cerinte pentru cabluri	Cat5e sau mai mare (cabluri ecranate)

5.7.8.9 Amplificator Audio

Caracteristică	Cerință minimală
Tip	Amplificator Audio
Configurari	4x canale 75W; 2x canale 150W; 1x canal 300W(bridged); 2x canale 75W + 1x canal 150W(bridged).
Tipuri semnal intrare	Analog balansat sau nebalansat
Raspuns in frecventa	Intre 20 Hz si 20 kHz ±0.5 dB la 1 W
THD+N	<0.1% la 1 kHz @ -3 dB
Raport semnal zgomot	>103 dBA, intre 20 Hz si 20 kHz, balansat
Conectori	Minim 2 iesiri pe 4 pini 5.08mm; Minim 4 intrari RCA nebalansate; Minim 4 intrari 3 pini 3.5mm balansate.

5.7.8.10 Difuzor tip pendant

Caracteristică	Cerință minimală
Tip	Difuzor tip pendant
Trepte transformator	70V: 3.75W/7.5W/15W/30W/60W; 100V: 7.5W/15W/30W/60W.
Raspuns in frecventa	Intre 50 Hz si 20 kHz ±3 dB
Putere	Minim 125W, 8 Ohmi
Acoperire	Minim 100º conic
Intrare	4 pini 5mm

5.7.8.11 Switch PoE

Caracteristică	Cerință minimală
Tip	Switch PoE+

Caracteristică	Cerință minimală
Porturi Gigabit PoE+	Minim 8 porturi RJ45
Porturi Gigabit	Minim 2 porturi RJ45
Porturi 10GBASE-X	Minim 2 porturi SFP
Viteza de transfer	Minim 24Gbps
Buget PoE	Minim 125W
Control	RS-232 prin intermediul porturilor USB-C si RJ45
Functii	Recunoasterea echipamentelor conectate in retea prin intermediul IGMP Plus; Posibilitate de montare pentru a avea porturile accesibile in partea frontala a rack-ului; Rutare statica, RIP si PIM; Server DHCP si PTPv2.

5.7.8.12 Distribuitor amplificator 1:2

Caracteristică	Cerință minimală
Tip	Distribuitor amplificator 1:2 HDMI
Conectivitate	1x Intrare HDMI; 2x Iesiri HDMI; 1x RS-232 pentru actualizare firmware.
Video	Latimea de banda de pana la 17,82 Gbps (5,94 Gbps per canal grafic); Rezolutie de pana la 4K@60Hz (4:4:4); Conformitate cu semnalul HDR10, HDCP 2.2; Suporta culori profunde, x.v.Color, lip sync, PCM 7.1, Dolby TrueHD, DTS–HD, 2K, 4K și 3D.
LED-uri indicatoare	Pornit, Intrare, Iesiri 1 la 2
Accesorii incluse	Sursa de alimentare

5.7.8.13 Echipament înregistrare

Caracteristică	Cerință minimală
Tip	Echipament înregistrare
Intrari video	Minim: 1x HDMI, 1x 12G SDI
Intrari retea	SRT, RTSP
Intrari audio	Minim: 2x XLR, 1x USB, 1x SDI, 1x HDMI, 1x RCA

Caracteristică	Cerință minimală
Iesiri video	Minim: 2x HDMI
Codec-uri	H.264/AVC, H.265/HEVC
Rezolutie culoare	4:2:0
Rezolutie video	Minim 1920x1200
Protocoale streaming	RTMP/RTMPS, SRT, HLS, MPEG-DASH, RTSP, MPEG-TS, UPnP
Encodare audio	MP3, PCM, si AAC (sampling intre 16 si 48 kHz cu bitrate pana la 320 kbps)
Retea	Minim: 1× 10/100/1000 Ethernet port (RJ45); 802.1x.
Stocare	FTP, SFTP, SCP, RSYNC, CIFS, AWS, sau WebDav servers
Format inregistrare	AVI, MP4, MOV, sau MPEG-TS
Control	Panou Admin bazat pe browser; Ecran LCD cu butoane pentru control integrat.

5.7.8.14 Masă conferință

Masa de conferință de tip FLIP TOP cu următoarele specificații:
Dimensiuni minime: Lungime 1600 x Lățime 800 x Înălțime 735 mm
Roți: cu diametrul de minim 60 mm, prevăzute cu frâne
Material Blat: Melamină

5.7.8.15 Scaun conferință

Scaun de conferință cu patru picioare prevăzute cu roți, cu următoarele specificații:
Dimensiuni minime:

- Lățime: 570 mm
- Adâncime: 600 mm
- Înălțime totală: 865 mm
- Înălțime șezut: 645 mm

Tapițerie:

- Șezut tapițat cu material textil pentru confort.
- Spătar din plasă pentru respirabilitate.

Cadru din oțel pentru durabilitate.
Cotiere:

- Cotiere integrate pentru confort sporit.
- Finisaj din plastic pentru o curățare ușoară.

5.7.9. Aplicație de administrare centralizată a infrastructurii de rețea

Aplicația de administrare centralizată a infrastructurii de rețea va asigura managementul rețelei LAN și a celei wireless.

Aplicația va asigura o vizibilitate extinsă asupra întregii rețele, traficul, performanța și securitatea, astfel încât să ofere administratorilor o imagine de ansamblu clară a rețelei în vederea luării unor decizii informate.

Aplicația va oferi capacități extinse de generare a rapoartelor și istoric detaliat al activității rețelei, ceea ce ajută la evaluarea performanței în timp și la respectarea regulamentelor sau standardelor de securitate;

Aplicația va oferi suport atât pentru rețelele cablate, cât și pentru cele wireless. Acest lucru face posibilă gestionarea și monitorizarea întregii infrastructuri IT dintr-un singur punct de control.

Aplicația va asigura posibilitatea de a proviziona în manieră de tip zero-touch AP-urile achiziționate în cadrul acestui proiect.

Aplicația trebuie să permită (și să fie licentiată pentru) integrarea de hărti și localizarea în timp real a clienților conectati la infrastructura wireless pe baza informatiilor primite de la Acces Point-uri.

Aplicația trebuie să permită integrarea și a altor echipamente de rețea disponibile în infrastructura beneficiarului (indiferent de producatorul acestora) în scop de monitorizare.

Aplicația trebuie să poată identifica și clasifica automat clientii și echipamentele de tip rogue.

Aplicația trebuie să ofere posibilitatea de a folosi search engine inclus, prin limbaj natural, folosind tehnologie tip AgenticAI

Aplicația trebuie să ofere proactiv recomandări pentru optimizarea infrastructurii și mitigarea problemelor in infrastrucutura, derivate din contextul rețelei

Aplicația trebuie să suporte monitorizarea, analiza și blocarea traficului la nivel de aplicație, tip de aplicație, pe bază de semnături ale aplicațiilor diferite, categorie web sau reputatia website-ului.

Aplicația trebuie să suporte mai mulți administratori simultani cu posibilitate de acces granular asupra facilitatilor puse la dispoziție.

Aplicația trebuie să suporte monitorizarea, analiza și blocarea traficului la nivel de aplicatie, tip de aplicatie, categorie web sau reputația website-ului

Accesul la aplicația trebuie să fie securizat prin traffic HTTPS și autentificare bazată pe certificat

Aplicația trebuie să suporte funcționalități pentru autentificarea utilizatorilor și definirea de politici pentru segregarea acesului în retea (NAC)

Aplicația trebuie să suporte funcționalități de tip guest precum: configurarea și customizarea unui landing page cu banner propriu, logo și culori.

Aplicația trebuie să poată analiza prezența utilizatorilor folosind datele primite de la echipamentele wireless. Acestea vor aduce informații despre numarul de utilizatori dintr-o anumita locație, retenția lor și frecvența cu care revin.

Aplicația va fi asigurată cu drept de utilizare pentru autoritatea contractantă pentru o perioadă de

cel puțin 5 (cinci) ani, acoperind și dreptul beneficiarului de a face update–uri.

5.7.10. Aplicație de administrare centralizată a stațiilor de lucru

Pentru a asigura managementul securizat al calculatoarelor precum și mijloacele tehnice necesare pentru auditul acțiunilor realizate în sistem, Aplicația de administrare centralizată a stațiilor de lucru va realiza monitorizarea și managementul calculatoarelor și a sesiunilor utilizatorilor în infrastructura sistemului, asigurând în acest sens funcționalitățile descrise în acest capitol.

Aplicația va asigura descoperirea, monitorizarea și gestionarea calculatoarelor (cu sisteme de operare Windows și Linux) conectate în rețea.

Aplicația va fi instalată în mediu virtual în infrastructura implementată prin proiect.

Aplicația va asigura gestionarea parolei pentru accesarea calculatoarelor Windows (sharing account).

Aplicația va asigura gestionarea parolei pentru accesarea calculatoarelor Linux (sharing account).

Aplicația va asigura gestionarea parolelor pentru accesarea sistemelor web-based (sharing account).

Aplicația va asigura suport pentru modul de lucru partajat – multi-tenant.

Aplicația va asigura suport pentru utilizatori multipli cu posibilitatea de a configura drepturile de acces al acestora prin permisiuni.

Aplicația va asigura criptarea bazei de date cu toate datele sensibile.

Aplicația va asigura posibilitatea de a monitoriza activitatea utilizatorilor în sesiuni locale și la distanță.

Aplicația va dispune de o interfață unică pentru monitorizarea activității utilizatorilor din mai multe instanțe ale soluției.

Aplicația va asigura posibilitatea înregistrării numai a ferestrei active a utilizatorului.

Aplicația va asigura posibilitatea de a naviga cu ușurință la sesiunea utilizatorului unde a fost utilizată o parolă.

Aplicația va asigura realizarea automată a inventarului hardware și software al calculatoarelor din rețeaua Beneficiarului, astfel:

a. Inventarul software va include cel puțin: sistemul de operare și patch-uri/service pack-uri de sistem instalate, aplicațiile software instalate și versiunea lor împreună cu funcții de monitorizare a nivelului de utilizare a aplicațiilor instalate.
b. Inventarul hardware al calculatoarelor trebuie să includă cel puțin: producător și model, procesor instalat, memorie RAM instalată, HDD (capacitate și serie), interfețe rețea instalate și setări de rețea.

Opțional, aplicația va asigura interogări prin care să recunoască calculatoarele și profilurile de utilizator ca tipuri individuale. Astfel, în funcție de opțiunile selectate, o interogare trebuie să poată returna fie un set de calculatoare, fie un set de profiluri de utilizator.

Aplicația va asigura monitorizarea utilizării dispozitivelor USB pe stații de lucru cu sistem de operare Windows și controlul dispozitivelor USB cu posibilitatea de a bloca anumite clase de dispozitive.

Aplicația va asigura posibilitatea de a instala clienții de la distanță pe calculatoarele utilizatorilor.

Aplicația va asigura scanarea setărilor de rețea, cel puțin configurația TCP/IPv4, TCP/IPv6, WINS și DNS, configurată pe sistemele gestionate.

Aplicația va asigura conectarea de la distanță la stațiile gestionate de soluție. Conectarea trebuie să poată fi realizata atât pe profilul utilizatorului stației cât și folosind credențiale de tip ”administrator” (conectarea cu profil de administrator trebuie să poată fi realizată doar de utilizatorii cu drepturi de acces la consola de administrare a soluției oferite).

Soluția trebuie să detecteze automat orice modificare a configurației calculatoarelor (modificare configurație hardware, instalare / dezinstalare software etc) cu generarea automată a unei alerte;

Aplicația va asigura alertarea automată a administratorului soluției în caz de încălcări de securitate și / sau potențiale pierderi de date.

Aplicația va include șabloane de alertă predefinite pentru detectarea încălcărilor de securitate.

Aplicația va asigura monitorizarea site-urilor web vizitate și înregistrarea tastelor introduse în orice aplicație și/sau pe orice site web cu posibilități de căutare.

Aplicația va include un motor de raportare încorporat pentru generarea de rapoarte cu mai mulți parametri.

Aplicația va include opțiunea de a primi / transmite rapoarte pe baza unei planificări.

Aplicația va asigura protecție împotriva întreruperii / opririi proceselor aplicației Client și împotriva schimbării / ștergerii fișierelor generate de aplicația Client chiar și pentru utilizatorii cu privilegii de administrator.

Aplicația va asigura autentificarea suplimentară (cu doi factori – 2FA) a utilizatorilor care se conectează la sistemul monitorizat cu credențiale de access suplimentare pentru protecția avansată a sistemului.

Aplicația va asigura posibilitatea de a bloca utilizatorii manual sau automat la detectarea acțiunilor interzise.

Opțional, aplicația va asigura posibilitatea de a opri procesele nepermise începute de un utilizator.

Aplicația va asigura posibilitatea de a permite / interzice accesul utilizatorilor la sistemul monitorizat

Opțional, Aplicația va asigura posibilitatea de a acorda acces la sistemul monitorizat numai după ce utilizatorul furnizează informațiile necesare.

Aplicația va asigura căutarea multi-parametri în rezultatele monitorizării.

Aplicația va asigura monitorizarea IP-urilor de la care a fost accesat sistemul monitorizat. Filtrarea sesiunilor monitorizate după adresa IP.

Aplicația va asigura vizualizarea sesiunilor live în timp real.

Aplicația va asigura analiza frecvenței de utilizare a aplicațiilor și a frecvenței de vizitare a site-urilor web.

Aplicația va asigura compararea numărului de licențe deținut de Beneficiar pentru o anumită aplicație cu numărul de utilizatori activi ai aplicației respective cu blocarea utilizării aplicației de către noi utilizatori în cazul depășirii numărului de licențe existente. În situația blocării utilizării datorită depășirii numărului de licențe, soluția trebuie să creeze o coadă de așteptare și să permită accesul atunci când unul dintre utilizatorii care foloseau aplicația nu o mai utilizează (în cazul în care modelul de licențele o permite).

Aplicația va asigura posibilitatea de a arhiva rezultatele monitorizării și de a vizualiza datele din arhivă.

Aplicația va asigura posibilitatea de a șterge capturile de ecran în timp ce metadatele rămân intacte.

Aplicația va asigura posibilitatea de export a rezultatelor monitorizării pentru vizionarea viitoare ca videoclip.

Aplicația va asigura posibilitatea de exporta capturi de ecran separate.

Aplicația va asigura validarea rezultatelor monitorizării pentru a garanta integritatea datelor monitorizate.

Aplicația va asigura posibilitatea filtrării utilizatorilor în timpul monitorizării.

Aplicația va asigura posibilitatea filtrării aplicațiilor / site-urilor web în timpul monitorizării.

Aplicația va asigura posibilitatea de a monitoriza activitatea utilizatorului numai în intervalele de timp specificate (ore de lucru).

Aplicația va asigura detectarea deviațiilor în utilizarea sistemelor / autentificărilor – de exemplu: sisteme / credențiale de autentificare utilizate rar.

Aplicația va asigura detectarea sistemelor folosite în afara programului normal de lucru.

Aplicația va asigura detectarea automată a stării de repaus a sistemelor monitorizate și afișarea în rapoarte a timpului de repaus al utilizatorului comparativ cu timpul activ al utilizatorului.

Aplicația va asigura controlul utilizării lățimii de bandă prin funcții specifice de configurare a dimensiunii capturilor de ecran înregistrate.

Aplicația va pune la dispoziție o componentă API prin care să se poată dezvolta integrări cu sistemele existente în organizația Beneficiarului

Aplicația va asigura vizualizarea sesiunilor prin API, utilizând API inclus în soluție.

Soluția trebuie să asigure distribuirea și instalarea automată, de la distanță de pachete software: patch-uri de securitate și actualizări ale sistemelor de operare, inclusiv a unei imagini de sistem de operare preconfigurat, pe întreg parcul de calculatoare gestionate, cu mențiunea că, dacă un calculator nu este deschis la momentul transmiterii pachetului, job-ul rămâne în așteptare (un interval de timp configurabil) până la deschiderea și conectarea acestuia în rețea și apoi să se execute. Aceste job-uri de instalare pachete software trebuie să poată fi programate să se execute întrun anumit interval de timp.

Soluția trebuie să permită instalări software simultane (software deployment) la distanță atât pentru instalări ce nu necesită intervenții (unattended) cât și folosind parametrii stabiliți anterior, fără întreruperea activității utilizatorilor, sau acțiunile de deployment să poată să fie programate în afara programului de lucru, în măsura în care calculatoarele rămân deschise, utilizatorul fiind înștiințat de momentul în care se produce restart-ul si să i se poată permite selecția acestui moment.

Suplimentar față de instalarea de software, soluția trebuie să permită inițierea diverselor proceduri de a activa, dezinstala sau configura un anumit produs, inclusiv inițierea de proceduri de instalare software complet noi, complet personalizate.

Aplicația va asigura auto-învățarea în timp a comportamentului normal al utilizatorilor și detectarea automată a unui comportament anormal al acestora

În timpul înregistrării sesiunii unui utilizator, soluția trebuie să asigure afișarea unui icon care să anunțe utilizatorul ca acțiunile sale sunt înregistrate. Utilizatorii autorizați ai soluției pot activa / dezactiva afișarea icon-ului de informare a utilizatorului privind înregistrarea.

Soluția oferită trebuie să fie o aplicație sau o suită de aplicații COTS (Commercial Off-the-Shelf) licențiate pentru utilizare on-premise, la sediul Beneficiarului.

Produsul va beneficia de suport tehnic pe o perioadă de 5 (cinci) ani, acoperind dreptul beneficiarului de a face update–uri precum și access direct la site-ul producătorului pentru a deschide direct cazuri de suport cu acesta.

5.7.11. Software de realizare a copiilor de siguranță

Soluția trebuie să fie flexibilă și scalabilă și să permită instalarea pe două și trei nivele de arhitectură; prin nivele de arhitectură se înțelege nivelul agent de backup, nivelul server de management și nivelul de server media de realizare și stocare a backup-urilor.
Soluția trebuie sa permită administrarea din interfața GUI, CLI si RestfulAPI;
Soluția trebuie să poată funcționa independent de o anumită tehnologie hardware.
Soluția trebuie să poată fi instalată pe medii fizice, virtuale cât și pe medii cloud.
Soluția trebuie să permită instalarea cel puțin pe urmatoarele sisteme de operare: Windows și Linux.
Soluția trebuie să suporte integrarea cu discuri DAS, NAS, SAN pentru stocarea fisierelor de backup.
Soluția trebuie să suporte integrarea cu echipamente de stocare, în mod nativ sau prin protocolul

OST (OpenStorage).
Soluția trebuie să identifice segmentele de date unice la nivelul agenților de backup, pentru optimizarea traficului prin rețea.
Soluția trebuie să suporte transferul datelor prin LAN și SAN.
Soluția trebuie să permită reluarea unui backup nefinalizat cu succes de la ultimul checkpoint.
Soluția trebuie să permită reluarea unei restaurări nefinalizate de la ultimul checkpoint.
Soluția trebuie să ofere capabilități pentru efectuarea de backup-uri sintetice.
Soluția trebuie să automatizeze crearea de multiple copii ale backup-urilor pe diferite medii de stocare cu politici diferite de retenție.
Soluția trebuie să permită crearea de backup-uri prin politici sau manual.
Soluția trebuie să asigure asistență pentru operațiile importante: instalare, creare activități de salvare / restaurare, formatare medii de stocare, etc.
Soluția trebuie să ofere posibilitatea de a efectua Bare Metal Restore (functionalitati de restaurare complet automatizate care includ sistemul de operare, configuratia, aplicatiile si datele) pentru Windows și Linux (RHEL, SUSE) fără a necesita integrarea cu soluții terte, instrumente native ale sistemului de operare sau instrumente pentru crearea de imagini.
Soluția trebuie să ofere toate tipurile de backup: full, incremental si diferențial.
Soluția trebuie să permită integrarea cu sisteme de tip LDAP pentru autentificarea utilizatorilor.
Soluția trebuie să asigure suport pentru protecția containerelor Docker.
Soluția trebuie să asigure suport pentru protecția aplicațiilor care ruleaza în containere Docker pe volume de date persistente.
Soluția trebuie să asigure suport pentru Kubernetes.
Soluția trebuie să asigure suport pentru multiplexing si multistreaming.
Soluția trebuie să asigure agenți dedicați pentru protecția sistemelor de baze de date, minim Microsoft SQL Server, Oracle RAC, IBM DB2, MySQL, PostgreSQL, precum și bazele de date propuse;
Soluția trebuie să asigure protectie pentru urmatoarele sisteme de operare: Windows cu distributii pentru 32 bit si 64 bit, RHEL, SUSE Linux Enterprise Server, CentOS, Ubuntu;
Soluția de backup trebuie să asigure suport pentru efectuarea de snapshot-uri la nivel de storage.
Soluția trebuie să suporte utilizarea protocolului Network Data Management Protocol (NDMP) pentru a iniția și controla salvarea/restaurarea sistemelor Network Attached Storage (NAS)
Soluția trebuie să suporte NDMP v2, v3 si v4.
Soluția trebuie să suporte salvari NDMP local și 3-way, functionalitatea Direct Access Recovery (DAR).
Soluția trebuie să permită actualizarea automată a tuturor clienților.
Soluția să asigure un modul de monitorizare și administare centralizat. Acesta trebuie să asigure functionalități de alertare și raportare pentru soluția propusă. Rapoartele și alertele trebuie să fie predefinite, dar să existe și posibilitatea de a crea rapoarte noi, prin utilizarea interfeței vizuale de tip point and click, sau drag and drop, dar și prin executia de fraze SQL custom peste baza de date

de tip repository sau catalog a soluției de backup.
Soluția trebuie să permită posibilitatea de a salva medii virtuale ca VMware, Hyper-V, Red Hat Virtualization, Open Stack, precum și mediul virtual oferit în proiect.
Soluția nu trebuie să necesite instalarea niciunui agent (permanent sau temporar) pentru salvarea masinilor virtuale.
Soluția trebuie să permită pornirea pe serverul de backup de mașinii virtuale direct din fisierele de backup aflate pe disc;
Soluția trebuie să permită salvarea completă și restaurarea granulară pentru Active Directory fără a fi necesară integrarea cu mecanismele native de backup ale acestor aplicații.
Soluția trebuie să permită backup de tipul “Incremental Forever”, astfel încât să salveze doar blocurile modificate. Aceste blocuri să poată fi ulterior combinate cu backup-ul anterior pentu a sintetiza un nou full backup, pentru o restaurare mult mai rapidă.
Procesul de deduplicare a datelor să poată fi efectuat inline sau post proces de backup.
Procesul de deduplicare trebuie să folosească segmente de dimensiuni variabile, pentru eficientizarea factorului de deduplicare.
Pentru a facilita protectia sistemelor pentru care nu există agenți dedicați, să permită crearea de mount point-uri de tip NFS si CIFS direct din sistemul de deduplicare al datelor, iar datele salvate în mount point-uri să fie deduplicate și protejate în sistemul de deduplicare.
Soluția trebuie să asigure suport pentru aplicarea procesului de deduplicare atât la sursa datelor de protejat cât și la nivelul sistemului de stocare al backup-urilor.
Soluția trebuie să asigure suport pentru deduplicare globală.
Soluția trebuie să asigure replicare de tip „one-to-one”, „one-to-many”, „many-to-one” și topologii de replicare cascadata a datelor deduplicate.
Soluția trebuie să asigure criptarea datelor replicate, în vederea securizării acestora pe perioada transferului între locații.
Soluția trebuie să permită prevenirea accesului neautorizat la aplicația de backup prin mecanisme de control acces bazate pe roluri.
Soluția trebuie să asigure suport pentru criptarea datelor, atât cele aflate în tranzit, cât și celor salvate. Soluția trebuie să includă propriile mecanisme pentru administrarea cheilor de criptare.
Soluția trebuie să asigure suport pentru autentificare în interfața Web de administrare folosind mecanisme 2 Factor Authentication.
Soluția trebuie să asigure mecanisme de protectie împotriva Ransomware, la nivel de client și la nivelul stocării backup-urilor, pentru a determina dacă nu cumva datele au fost deja afectate de ransomware. Acest mecanism trebuie să funcționeze în momentul rulării backup-ului, în momentul salvării pe disc și imediat înainte de orice tentativă de restaurare.
Soluția trebuie să asigure mecanisme de obfuscare a datelor sensibile salvate.
Soluția trebuie să permita scanarea anti-malware a datelor salvate cu cel puțin două motoare de scanare.
Soluția trebuie să permită instalarea unui numar nelimitat de clienți de backup indiferent de tipul

acestora.
Soluția va fi licențiată astfel încât să asigure o capacitate de date de protejată pentru minim 5 TB, indiferent de numărul de procesoare ale serverelor și de numarul de mașini fizice sau virtuale protejate.
Suport pentru software pe o perioadă de 60 luni, acoperind dreptul beneficiarului de a face update–uri precum și access direct la site-ul producatorului pentru a deschide direct cazuri de suport cu acesta. De asemenea, se va asigura dreptul de a face update-uri și upgrade-uri la toate componentele software propuse.
Furnizorul are obligația de a elabora o politică detaliată de backup pentru Sistemul Informatic Integrat pentru Servicii Publice Electronice de Combatere a Discriminării (SIISPECD), care să fie supusă aprobării beneficiarului, și de a implementa această politică în soluția propusă. Politica de backup va respecta bunele practici din industrie, incluzând, dar fără a se limita la: menținerea mai multor copii ale datelor pe suporturi de stocare diverse, cu cel puțin o copie stocată întro locație separată fizic, criptarea datelor pentru asigurarea confidențialității, programarea automată a backup-urilor cu frecvență adecvată pentru minimizarea pierderii de date, și testarea periodică a procedurilor de restaurare pentru garantarea integrității și disponibilității datelor. Implementarea politicii va asigura continuitatea operațională și protecția datelor sistemului în conformitate cu specificațiile tehnice ale prezentului document.

5.7.12. Actualizarea soluției software existente de gestiune și securizare a accesului

SIISPECD va dispune de mecanisme unificate și integrate pentru gestiunea și securizarea accesului utilizatorilor la infrastructura și aplicațiile sistemului. Soluția existentă de gestiune și securizare a a accesului, Microsoft Active Directory va actualizată la ultima versiune.
Se va include o licența Microsoft Windows Server 2022 pentru 16 nuclee și 79 bucăți Microsoft Windows Server 2022 user CAL. Aceste licențe sunt necesare pentru actualizarea serviciilor ActiveDirectory, DNS, WSUS, FileServer și Print Server la nivel de ediție 2022. Operațiunile de actualizare a serviciilor ActiveDirectory, DNS, WSUS, FileServer și Print Server spre sistem de operare Windows Server 2022, precum și migrarea/actualizarea profilelor de utilizator pe toate calculatoarele din dotarea CNCD, intră în scopul proiectului.

5.7.13. Software de jurnalizare de audit

SIISPECD va include o soluție de jurnalizare de audit bazată pe bazat pe o aplicație software introdusă deja în circuitul comercial. Nu se accepta dezvoltări, ci doar configurări sau personalizări, pentru a se putea permite implementarea soluției pentru a răspunde cerințelor tehnice din cadrul proiectului.
Aplicația trebuie să asigure monitorizarea SIISPECD, din punct de vedere al auditului. Astfel, soluția trebuie să asigure colectarea evenimentelor de audit din toate aplicațiile, bazele de date și

echipamentele din compunerea SIISPECD.
Interfața de operare și administrare a aplicației trebuie să fie de tip WEB, asigurând totodată compatibilitate cu orice browser modern (Chrome, Microsoft Edge, Opera, Firefox etc.)
Aplicația trebuie să includă următoarele module funcționale:

- Modul afișare – asigură afișarea în format tabelar a tuturor evenimentelor colectate. Interfața va putea fi configurabilă din punctul de vedere al câmpurilor ce pot fi vizualizate și va permite filtrări avansate precum și ordonări ale evenimentelor;
- Modul panouri de bord – asigură vizualizări grafice pentru evenimentele colectate, sub formă de tablouri de bord. Acestea vor putea fi configurabile în funcție de nevoile de business. De asemenea, întrun grup, pot fi asociate tablouri pentru tehnologii diferite și va permite căutarea în toate tablourile relativ la un criteriu sau set de criterii comune;
- Modul Raportare – va asigura intrinsec rularea și vizualizarea de rapoarte de tip ”best practices” pentru diverse tehnologii precum și de conformitate pentru GDPR și pentru standardele ISO 27001. De asemenea, permite crearea de noi rapoarte, editarea rapoartelor existente, va conține funcții de planificare a rulării și transmiterii rapoartelor și funcții de export a rezultatelor rapoartelor.
- Modul Alertare - include implicit afișarea de alerte de tip ”best practices” pentru diverse tehnologii. Alertele vor fi definite/editate întro interfață grafică, intuitivă. Alertele predefinite trebuie să acopere o gamă largă de tehnologii.
- Managementul incidentelor – permite personalului să desfășoare în mod colaborativ activități de investigare a evenimentelor.
- Depozite de date - Aplicația va stoca datele cel puțin în două moduri (depozite):
    - Arhiva – datele sunt depozitate pentru păstrare pe termen lung, comprimate
        - Rata compresie – minim 1 la 20
        - Va oferi mecanisme anti-repudiere: criptare și semnare digitală a datelor
    - Online – datele sunt depozitate indexat cu accesare rapidă pentru nevoi investigaționale, de raportare etc.

Nu se acceptă tehnologii proprietare pentru depozitele de date – datele sunt ale Autorității Contractante și accesarea/utilizarea acestora nu trebuie să fie dependentă de soluția propusă.
Administrarea aplicației se va realiza folosind sisteme de permisiuni tip RBAC (Role Based Access Control), atât pentru accesul la date cât și pentru configurările sistemului. Operatorii soluției nu trebuie să poată modifica datele sistemului.
Aplicația trebuie să se integra cu sistemul Active Directory ce se va implementa în cadrul proiectului pentru autentificare unitară.
Aplicația trebuie să asigure colectarea evenimentelor din segmente diferite de rețea.
Aplicația trebuie să asigure colectarea datelor prin intermediul agenților sau direct din sistemele sursă.
Aplicația trebuie să asigure capacități de colectare fluxuri de evenimente de tip Syslog, NetFlow, sFlow sau direct prin sisteme tip TAP.

Agenții vor transmite datele colectate către serverul de procesare, în format comprimat și criptat.
Agenții de colectare vor putea efectua colectare filtrată și vor furniza capacități de procesare / preprocesare / postprocesare a datelor.
Agenții vor asigura mecanisme de protecție împotriva alterării datelor colectate la colecție, în tranzit sau repaus.
Aplicația trebuie să asigure instalarea, dezinstalarea precum și configurarea parametrilor de funcționare a agenților.
Operațiunile de administrare a agenților se vor putea efectua pentru fiecare agent în parte sau pentru mai mulți agenți în același timp.
Aplicația trebuie să asigure adăugarea surselor de date din interfața grafică.
Aplicația trebuie să dispună de capacități de tip autodiscovery pentru identificarea automată a tipurilor de evenimente comune.
Aplicația trebuie să asigure colectarea de evenimente prin intermediul conectorilor predefiniți din cel puțin următoarele surse de date:

- Microsoft Windows Server 2016 sau superior
- Microsoft Windows 8 sau superior
- Windows Hyper-V și VMware vCenter
- Cisco SourceFire, ASA, ISE, FirePower, Prime
- Cisco Netflow v5, v9
- distribuții comerciale Linux
- Balansoare de rețea F5
- Microsoft DNS, Linux DNS
- DHCP
- Servicii web Apache, Tomcat, Microsoft IIS sau cele construite pe tehnologie NodeJS
- SQL Server Log, Oracle Audit, alte sisteme de baze de date cu conector ODBC
- Sisteme de baze de date No-SQL
- Evenimente de aplicații generate sub forma de înregistrări text sau tabele de audit în baze de date MS SQL, Oracle, etc.
- Mesaje syslog generate de echipamente de rețea, echipamente de tipărire, sisteme de control al accesului sau alte echipamente
- Colectarea evenimentelor de securitate la nivel de sistem de fișiere, pentru tehnologii Linux și Windows
- Colectarea de metadate din sisteme terțe (Active Directory, informații WMI, SNMP, sisteme de management al identităților), pentru utilizarea lor în procesul de corelare

Aplicația trebuie să includă funcționalități avansate de configurare a conectorilor, astfel încât să acomodeze fișiere aparent neparsabile:

- Fișiere cu evenimente multiline (număr dinamic de linii, evenimente separate prin newline / datetime)
- Fișiere XML

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

- Fișiere free text

Aplicația trebuie să asigure capacități avansate de filtrare a evenimentelor la destinație. Filtrarea poate fi efectuată astfel:

- Filtrare tip „drop event”
- Filtrare cu trimiterea evenimentelor doar în arhiva
- Filtrare fără trecerea evenimentelor prin motorul de corelare, cu trimiterea acestora doar în baza de date on-line și arhivă.

Aplicația trebuie să asigure capacități de filtrare a evenimentelor la sursă

Aplicația trebuie să permită exportul evenimentelor din arhivă în baze de date on-line pentru activități investigaționale, de raportare etc.

Aplicația trebuie să permită ca exportul să se facă imediat sau programat.

Aplicația trebuie să asigure exportul filtrat al evenimentelor pentru investigații.

Activitățile de export vor fi efectuate din interfața grafică a soluției, fără a fi necesară instalarea sau folosirea unor elemente sau aplicații terțe

Depozitul on-line trebuie să poată fi scalat în funcție de nevoie, oricând pe durata de utilizare a soluției, fără a implica niciun cost de licențiere pentru baza de date

Arhiva poate fi scalată în funcție de nevoie, oricând pe durata de utilizare a soluției, fără a implica niciun cost de licențiere pentru baza de date.

Aplicația trebuie să permită configurarea redirecționării de evenimente către soluții terțe, astfel:

- în format brut sau în format normalizat (syslog, .json, CEF)
- filtrate (doar de la anumite surse, doar de un anumit tip etc.)

Aplicația trebuie să permită exportul alertelor, în mod manual, una câte una sau selecție, precum și în mod automat. Se vor putea defini criteriile de export pentru alerte, pentru fiecare alerta în parte sau bulk în formate și pe medii diferite: Email, call-uri de API-uri, syslog.

Configurările pentru redirecționarea evenimentelor se vor face din interfața grafică a platformei cu granularitate până la nivel de tip de eveniment, alertă etc.

Aplicația va include capacități de alertare asupra statusului serviciilor componente precum și de restaurare automată a acestora în caz de oprire

Aplicația trebuie să permită configurarea de alerte inclusiv pentru praguri de ingestie evenimente/număr de evenimente care așteaptă să fie ingerate/procesate de soluție

Aplicația va dispune de funcții de tip self-audit. Astfel, vor fi auditate toate operațiunile efectuate de utilizatorii și de serviciile componente ale soluției

Aplicația trebuie să pună la dispoziția utilizatorului un API de integrare pentru surse de date noi sau includerea de logica în procesele de colectare, corelare sau alertare a datelor pentru a putea acomoda cele mai exigente cerințe de securitate.

Aplicația trebuie să permită afișarea grafică de agregări de evenimente sub forma de panouri de bord.

Panourile de bord vor putea fi asociate (grupate) în grupe de panouri

Aplicația trebuie să asigure posibilitatea de filtrare și afișare în toate panourile relativ la un singur

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

criteriu.
Aplicația va dispune de alerte pre-configurate pe multiple tehnologii, în baza scenariilor de bună practică.
Toate evenimentele ingerate în soluție trebuie să poată fi incluse în motorul de corelare
Aplicația trebuie să asigure posibilitatea de a exclude evenimente din fluxul de corelare. Filtrarea se va face per sursa de date sau pe identificator de tip de eveniment
Procesele de corelare vor putea fi executate în mai mulți pași – corelări din 1 sau mai multe evenimente/secvențe de evenimente cu praguri de activare reguli individuale.
În urma alertelor declanșate aplicația trebuie să poată rula acțiuni automate. Acțiunile vor putea fi implicite, pe tehnologii sau vor putea fi personalizate.
În procesul de configurare/personalizare a acțiunilor automate trebuie să poată fi incluse elemente/câmpuri din evenimentele ce au generat alerta
Aplicația va putea transmite notificări pentru alerte cel puțin prin:

- Email
- consola soluției

Aplicația trebuie să permită definirea de noi reguli de alertare în baza unor criterii singulare, corelate sau de excludere, inclusiv:

- Eveniment singular – când un singur eveniment indică situația care necesita remediere
- Evenimente corelate – când trebuie detectată o situație specifică, definită în termeni de evenimente care survin în aproximativ același timp
- Cumul de evenimente – când trebuie detectată o situație în care acțiuni similare se derulează întro succesiune rapidă
- Lipsa unui eveniment – când se așteaptă evenimente specifice întrun anumit interval de timp sau întro anumită situație dată, dar acest sau aceste evenimente nu mai au loc
- Lipsa unui eveniment corelat – când trebuie urmărite situații sau procese în care acțiunile subsecvente nu mai au loc
- Reguli particularizate – când se dorește detectarea unei situații care nu poate fi definită prin celelalte modele de reguli

Aplicația trebuie să asigure următoarele funcționalități privind managementul alertelor:

- marcarea alertelor (acknowledge) de tip one-by-one sau bulk;
- marcare automată a alertelor – în funcție de scorul de gravitate;
- notare rezoluție pentru alerte. Notarea se va putea efectua one-by-one sau bulk.

Aplicația va include un feed propriu de securitate ce trebuie să ofere minim informații tip: IP-uri, domenii și url-uri malițioase, dar va permite și integrare de feeduri de securitate de tip open source / subscription based.
Aplicația trebuie să asigure capacități de corelare automată pentru informațiile din evenimentele de securitate în funcție de informațiile conținute în feedurile de securitate.
Aplicația trebuie să includă modul de afișare tabelară a evenimentelor cu posibilități avansate pentru filtrare și ordonare

Viteza de răspuns pentru filtrări și căutări în baza de date online trebuie să asigure o bună experiență de utilizare. Astfel, o căutare simpla, după un singur criteriu, în toata baza de date online va returna rezultate în mai puțin de 10 secunde
Filtrele aplicate pot fi salvate pentru o utilizare ulterioara. De asemenea, filtrele trebuie să poată fi salvate ca și rapoarte/alerte/tablouri de bord.
Utilizatorii vor putea selecta informațiile (coloanele) ce vor fi vizibile în interfață
Utilizatorii vor putea accesa vizualizare detaliata pentru fiecare eveniment.
Interfața de căutare a sistemului de audit va oferi posibilitatea de combinare a operatorilor logici de căutare ("AND", "OR", “NOT”) și vor putea fi definite expresii complexe cu operatori paranteză (inclusiv paranteze imbricate)
Aplicația trebuie să asigure corelarea jurnalelor pentru toate seturile de date, indiferent de sursă și/sau tipul de jurnal
Aplicația trebuie să permită detectarea automată a autentificărilor suspecte
Aplicația trebuie să asigure, în cadrul modului de raportare, un set complet de rapoarte pentru standarde conformitate uzuale: ISO 27001, GDPR
Vor fi disponibile în mod implicit rapoarte de tip bună practică pentru multiple tehnologii.
Toate rapoartele predefinite trebuie să poată fi personalizate astfel:

- Titlurile rapoartelor trebuie să poată fi modificate.
- Rapoartele vor include pe prima pagina informații succinte despre perioada evenimentelor din raport/ce evenimente sunt cuprinse etc.

Rapoartele vor conține grafice relativ la informația afișată în acestea.
Rezultatul rapoartelor trebuie să poată fi exportat ca și fișier în următoarele formate: PDF, HTML, XLSX, XLS, CSV, XML.
Toate serviciile și componentele aplicației vor fi instalate pe aceeași mașină virtuală.
Soluția trebuie să includa posibilitatea de management al tuturor agenților: Windows / Linux /etc.
Soluția trebuie să ridice evenimente/alerte de modificare de configurație
Soluția trebuie să poată monitoriza în timp real modificarile de parole, adăugările de utilizatori pe orice sistem de operare monitorizat: Windows / Linux cu ajutorul agenților nativi.
Soluția trebuie să includă cel puțin 450 de scenarii de monitorizare / alertare built-in.
Soluția trebuie să ofere posibilitatea de a integra nativ un LLM local pentru ajutorul investigatorilor.
Soluția trebuie să ofere funcționalitate de investigare automată a incidentelor.
Soluția trebuie să ofere posibilitatea crearii personalizate de incidente cu câmpuri dinamice în funcție de tipul de incident și să ofere intrumente de vizualizare rapidă de management a acestora.
Aplicația va avea posibilitatea de a distribui pe orizontala serviciile și componentele astfel încât, pentru o eventuala nevoie de scalare, să permită utilizarea infrastructurii existente a beneficiarului.
Aplicația trebuie să asigure un volum de minim 2.000 EPS (events per second) sau 50 GB date/zi.
Nu va exista nicio limitare de licență pentru volumul de date întreținut de soluție (volumul bazelor de date online și arhiva) iar acesta va putea fi scalat, pe parcursul sau după încheierea proiectului, în funcție de nevoile beneficiarului, fără niciun cost suplimentar de licențiere pentru dimensiunea

depozitelor de date.
Contractorul va asigura activarea controalelor astfel încât să fie generate și colectate evenimente de audit din toate componentele furnizate în proiect.

5.7.14. Pachet BYOL CPG Azure Hub Stack

Acest pachet va include licențele necesare pentru funcționarea soluției în Cloudul Privat Guvernamental (CPG), unitatea de Cloud Dedicat bazată pe tehnologia Azure Hub Stack, după cum urmează:

5.7.14.1 Software de protecție a aplicațiilor

Soluția de protecție a aplicațiilor web trebuie să fie furnizată sub forma unui appliance virtual, configurat cu 8 vCPU și implementat în mașini virtuale pe platforma Azure Stack Hub, îndeplinind cerințele funcționale și de performanță de mai jos.
Soluția trebuie să poată gestiona traficul IPv4 și IPv6.
Sistemul de securitate trebuie să poată fi configurat în modul reverse-proxy, în care tot traficul către și dinspre aplicație circulă prin WAF. Trebuie să existe suport obligatoriu pentru protocoalele HTTP/S 1.0/1.1/2.0 și opțional WebSocket și FTP/S.
Soluția trebuie să permită terminarea conexiunilor SSL la client și la serverul de aplicații. Pentru a reduce timpul de răspuns al serverului, trebuie să fie posibilă menținerea unui pool de conexiuni către serverul de aplicații, reutilizabil pentru cererile clienților.
Soluția trebuie să ofere un mod care să permită criptarea protocolului HTTP în numele serverului de aplicații, convertind toate cererile și răspunsurile HTTP în HTTPS, fără modificări la nivelul aplicației sau al serverului de aplicații.
Soluția trebuie să utilizeze tehnologia de pooling de conexiuni pentru a optimiza conexiunile dintre WAF și serverele de aplicații, menținând un număr specific de conexiuni reutilizabile pentru interogarea aplicației fără inițierea de noi conexiuni.
Soluția trebuie să ofere un mod de detectare (înregistrarea informațiilor despre amenințările detectate fără blocare), în care regulile politicii de securitate sunt identice cu cele din modul de prevenire. Sistemul trebuie să permită configurarea detaliată a modului pentru părți individuale ale aplicației (ex. URL, parametri de formular).
Soluția trebuie să suporte capabilități de blocare precum: resetarea conexiunii, trimiterea unui cod de eroare selectat, redirecționarea cererii, modificarea corpului răspunsului sau blocarea adreselor IP ale clienților pentru o perioadă specificată. Sunt acceptate și soluții care suportă capabilități de blocare folosind codurile de eroare HTTP.
Soluția trebuie să ofere funcționalitate de rescriere HTML, inclusiv adăugarea, eliminarea și editarea anteturilor de cereri și răspunsuri HTML, traducerea codificărilor de caractere în URL-uri, rescrierea și redirecționarea adreselor URL în cereri și rescrierea părților corpului în răspunsuri.

Expresiile regulate trebuie să fie disponibile pentru manipulările de text necesare.
Soluția trebuie să permită administratorului să restricționeze accesul la metode HTTP și WEBDAV (ex. HEAD, CONNECT, TRACE) pentru URL-uri individuale.
Soluția trebuie să poată aplica reguli de restricție diferitelor părți ale cererii, inclusiv aplicații, URL-uri, parametri de interogare, parametri FORM, anteturi sau cookie-uri.
Soluția trebuie să impună restricții de protocol asupra cererilor, specifice fiecărui URL, incluzând: a. Lungimea metodei HTTP, b. Lungimea șirului de interogare, c. Lungimea protocolului, d. Numele, valoarea și numărul de anteturi transferate în cererea HTTP, e. Lungimea răspunsului, f. Numele, valoarea și numărul cookie-urilor, g. Numele parametrului, valoarea și numărul, h. Lungimea maximă (per fișier) și numărul de fișiere transferate (prin metoda POST).
Soluția trebuie să poată ascunde informații sensibile în corpul și anteturile răspunsului serverului.
Soluția trebuie să analizeze corpul răspunsului, indiferent de codul de răspuns, pentru a bloca complet răspunsul sau a ascunde datele sensibile dacă sunt detectate, utilizând modele definite prin expresii regulate.
Soluția trebuie să suporte un model de securitate negativ, în care atacurile sunt detectate prin potrivirea expresiilor regulate cu cererile primite la URL-uri.
Soluția trebuie să permită specificarea expresiilor regulate pentru toate părțile cererii (URI, parametri, anteturi, cookie-uri) pentru a selecta URL-urile la care se aplică regulile corespunzătoare.
Soluția trebuie să suporte un model de securitate pozitiv, care să permită o „listă albă” de valori în diferite elemente ale politicii de securitate, respingând toate celelalte valori (de exemplu: Lista valorilor permise pentru parametrii FORM/interogare (tipuri de date, liste etc.), Lista de meta-caractere/cuvinte cheie permise în URL-uri, parametri, Profil de aplicație valid (URL-uri și parametri permisi pentru fiecare adresă URL cu profiluri de securitate individuale), Metode HTTP permise pentru fiecare adresă URL, Tipuri de conținut permise pe adresă URL, Extensii de fișiere permise pentru fișierele încărcate, etc.)
Soluția trebuie să permită crearea de site-uri/servicii virtuale corespunzătoare aplicațiilor țintă, cu profiluri de configurare individuale pentru fiecare aplicație, incluzând setări pentru URL-uri și parametri.
Soluția trebuie să suporte integrarea cu sistemele SIEM.
Soluția trebuie să suporte următoarele mecanisme de autentificare: obligatoriu LDAP/RADIUS și opțional Kerberos, SAML, RSA SecurID, coduri SMS, certificate.
Soluția trebuie să ofere protecție împotriva atacurilor asupra disponibilității aplicațiilor (DoS/DDoS), incluzând blocarea atacurilor DDoS, protecție împotriva atacurilor Low-and-Slow (ex. SlowLoris), detectarea nodurilor de ieșire anonime din rețeaua TOR și protecție împotriva atacurilor volumetrice.
Soluția trebuie să suporte integrarea cu scanere de vulnerabilități ale aplicațiilor, permițând importarea listei de vulnerabilități detectate și crearea automată a regulilor de securitate pentru blocarea acestora.
Soluția trebuie să fie livrată sub forma a două instanțe de appliance care funcționează întrun cluster

de înaltă disponibilitate (HA) în Azure Stack Hub, asigurând redundanța și continuitatea operațiunilor.
Parametrii minimi de performanță necesari pentru fiecare instanță virtuală din cluster, configurată cu 8 vCPU: a. Lățime de bandă: minim 1 Gbps; b. Număr de conexiuni simultane: minim 500.000; c. Număr de tranzacții HTTP pe secundă: minim 50.000 d. Număr de conexiuni HTTP noi pe secundă: minim 20.000.
Soluția trebuie să fie livrată cu licențe și suport de producător în modelul 24x7 pentru o perioadă de 5 ani. Licențele trebuie să includă toate funcționalitățile legate de protecția aplicațiilor, protecția DDoS și protecția avansată împotriva boturilor.

5.7.14.2 Sisteme de operare

Pentru a asigura o infrastructură robustă, sigură și compatibilă în Componenta de Cloud Dedicat a Cloudului Privat Guvernamental bazată pe Azure Stack Hub, sistemele de operare ofertate pentru mașinile virtuale (VM) trebuie să fie Windows Server și/sau RHEL.
Această cerință se bazează pe necesitatea critică de a beneficia de suport de la producător ca măsură fundamentală de securitate, precum și pe compatibilitatea optimă cu Azure Stack Hub, în contextul în care Cloudul Privat Guvernamental se bazează pe modelului BYOL (Bring Your Own License). Securitatea infrastructurii IT depinde în mod direct de capacitatea de a răspunde rapid la vulnerabilități și amenințări emergente. Atât Windows Server, cât și RHEL beneficiază de suport extins de la producătorii lor (Microsoft, respectiv Red Hat), care garantează actualizări de securitate, patch-uri pentru vulnerabilități și asistență tehnică pe o perioadă de minim 5 ani de la data implementării. Acest suport pe termen lung este esențial pentru:

- Protecția împotriva atacurilor cibernetice prin aplicarea promptă a actualizărilor de securitate.
- Menținerea conformității cu standardele de securitate (ex. ISO 27001, GDPR), prin utilizarea unui OS activ suportat.
- Reducerea riscurilor asociate utilizării unui OS nesuportat, care ar expune infrastructura la vulnerabilități necorectate.

Având în vedere aceste aspecte, soluția ofertată trebuie să utilizeze exclusiv Windows Server și RHEL ca sisteme de operare pentru VM-urile gazdă, cu excepția cazurilor în care software-ul specific (ex. Web Application Firewall) necesită un OS proprietar. Aceste sisteme de operare trebuie să fie compatibile cu toate rolurile VM-urilor din soluția ofertată și trebuie să suporte rularea ca VM gazdă în Azure Stack Hub, utilizând Hyper-V.
Sistemele de operare ofertate trebuie să beneficieze de suport complet (inclusiv actualizări de securitate și suport tehnic) pentru o perioadă de minim 5 ani, de la livrare, fiind esențial pentru securitatea infrastructurii, deoarece:

- Asigură protecția împotriva vulnerabilităților noi prin actualizări regulate de securitate.
- Menține conformitatea cu standardele de securitate (ex. ISO 27001, GDPR).

- Previne riscurile asociate utilizării unui OS nesuportat, cum ar fi exploatarea vulnerabilităților necorectate.
- Garantează stabilitatea și continuitatea operațiunilor pentru toate rolurile VM-urilor

Sistemele de operare ofertate trebuie să fie licențiate corespunzător în conformitate cu modelul BYOL (Bring Your Own License), pentru a asigura utilizarea legală și accesul la suport și actualizări pe întreaga perioadă de 5 ani:

- Licențele trebuie să acopere toate mașinile virtuale ale soluției ofertate și să fie valabile pentru implementarea în cloud privat pe Azure Stack Hub, respectând termenii de licențiere ai Microsoft și Red Hat.
- Windows Server: Licențele trebuie să includă drepturi de utilizare în Azure Stack Hub (ex. licențe Windows Server Standard sau Datacenter Edition, cu Software Assurance sau un contract de suport echivalent activ pentru a garanta accesul la patch-uri și asistență tehnică).
- RHEL 8: Licențele trebuie să fie sub forma unui abonament Red Hat Enterprise Linux activ, care include acces la Red Hat Customer Portal pentru actualizări, patch-uri și suport tehnic. Abonamentul trebuie să acopere toate VM-urile gazdă și să fie compatibil cu Azure Stack Hub.
- Licențele trebuie să permită accesul la actualizări de securitate și suport tehnic 24x7 pe întreaga perioadă de 5 ani;
- Licențele trebuie să fie conforme cu reglementările aplicabile (ex. audituri de licențiere) și să acopere toate scenariile de utilizare (ex. failover, DR), pentru a evita riscurile legale și operaționale.

5.7.14.3 Software de balansare a aplicațiilor

Soluția de balansare a cererilor utilizatorilor trebuie să fie implementată sub forma unui appliance virtual în cluster active-active HA (High Availability) pe platforma **Azure Stack Hub**, pentru a distribui eficient cererile utilizatorilor către servere, asigurând disponibilitate, scalabilitate și performanță.

Appliance-ul virtual trebuie să fie compatibil cu platforma de virtualizare Hyper-V utilizată de Azure Stack Hub.

Soluția trebuie să poată gestiona traficul IPv4 și IPv6.

Soluția trebuie să poată fi configurată în modul reverse-proxy, în care tot traficul către și dinspre aplicațiile backend circulă prin soluția de load balancing. Trebuie să existe suport pentru protocoalele HTTP/S 1.0/1.1/2.0, TCP/UDP și opțional WebSocket.

Soluția trebuie să permită terminarea conexiunilor SSL la nivelul soluției de load balancing și la serverele backend. Pentru a optimiza performanța, trebuie să fie posibilă menținerea unui pool de conexiuni către serverele backend, reutilizabile pentru cererile clienților.

Soluția trebuie să ofere un mod care să permită criptarea protocolului HTTP în numele serverelor backend, convertind toate cererile și răspunsurile HTTP în HTTPS, fără modificări la nivelul

aplicațiilor sau al serverelor backend.
Soluția trebuie să utilizeze tehnologia de pooling de conexiuni pentru a optimiza conexiunile dintre soluția de load balancing și serverele backend, menținând un număr specific de conexiuni reutilizabile pentru a reduce latența.
Opțional, soluția trebuie să ofere un mod de monitorizare pasivă (log-only), în care cererile suspecte sunt înregistrate fără a fi blocate, pentru a permite analiza traficului înainte de aplicarea politicilor de blocare. Configurarea trebuie să fie granulară, aplicabilă la nivel de URL sau aplicație.
Soluția trebuie să suporte capabilități de gestionare a traficului suspect, inclusiv: redirecționarea cererilor, trimiterea unui cod de eroare selectat, resetarea conexiunii sau limitarea temporară a accesului pentru adrese IP suspecte.
Soluția trebuie să ofere funcționalitate de rescriere a cererilor și răspunsurilor HTTP, inclusiv modificarea anteturilor, rescrierea URL-urilor și gestionarea codificărilor de caractere. Expresiile regulate trebuie să fie disponibile pentru manipularea textului.
Opțional, soluția trebuie să permită administratorului să restricționeze accesul la metode HTTP (ex. HEAD, CONNECT, TRACE) pentru URL-uri individuale.
Opțional, soluția trebuie să poată aplica reguli de restricție diferitelor părți ale cererii, inclusiv aplicații, URL-uri, parametri de interogare, anteturi sau cookie-uri.
Soluția trebuie să impună restricții de protocol asupra cererilor, specifice fiecărui URL, incluzând: a. Lungimea metodei HTTP, b. Lungimea șirului de interogare, c. Lungimea protocolului, d. Numele, valoarea și numărul de anteturi transferate în cererea HTTP, e. Lungimea răspunsului, f. Numele, valoarea și numărul cookie-urilor, g. Numele parametrului, valoarea și numărul.
Soluția trebuie să poată ascunde informații sensibile în anteturile și corpul răspunsurilor serverului (ex. headere de server, versiuni software).
Soluția trebuie să analizeze corpul răspunsurilor pentru a bloca sau masca datele sensibile, utilizând modele definite prin expresii regulate, indiferent de codul de răspuns HTTP.
Soluția trebuie să suporte un mecanism de protecție bazat pe rate limiting, în care cererile excesive sunt detectate și limitate prin configurarea pragurilor de trafic.
Soluția trebuie să permită specificarea expresiilor regulate pentru toate părțile cererii (URI, parametri, anteturi, cookie-uri) pentru a aplica reguli de filtrare sau balansare.
Opțional, soluția trebuie să suporte un model de balansare bazat pe liste albe, care să permită doar cereri conforme cu valorile predefinite: a. Lista valorilor permise pentru parametrii de interogare (tipuri de date, liste etc.). b. Lista de meta-caractere/cuvinte cheie permise în URL-uri, parametri. c. Metode HTTP permise pentru fiecare adresă URL. d. Tipuri de conținut permise pe adresă URL.
Soluția trebuie să permită definirea de servicii virtuale corespunzătoare aplicațiilor backend, cu profiluri de configurare, incluzând setări pentru URL-uri și parametri.
Soluția trebuie să suporte integrarea cu sisteme SIEM pentru monitorizarea și raportarea evenimentelor de trafic.
Soluția trebuie să suporte mecanisme de autentificare: obligatoriu LDAP, RADIUS și opțional Kerberos, SAML și certificate.

Soluția trebuie să ofere protecție împotriva atacurilor asupra disponibilității aplicațiilor (DoS/DDoS), incluzând limitarea ratei cererilor, verificarea traficului prin metode precum JavaScript challenge sau echivalent, protecție împotriva atacurilor Low-and-Slow și detectarea traficului suspect (ex. noduri TOR).
Soluția trebuie să suporte integrarea cu sisteme de monitorizare a sănătății aplicațiilor, permițând verificarea activă a stării serverelor backend și ajustarea automată a distribuției traficului în funcție de disponibilitatea acestora.
Soluția trebuie să fie livrată sub forma a două instanțe de appliance virtual care funcționează întrun cluster active-active HA în Azure Stack Hub, utilizând Azure Standard Load Balancer pentru distribuția traficului între instanțe, asigurând redundanță și continuitatea operațiunilor. În cazul în care, Azure Standard Load Balancer nu se poate utiliza, distribuția traficului între instanțe trebuie să fie realizată prin DNS round-robin, combinat cu un mecanism de monitorizare externă (ex. script de health check) care actualizează DNS-ul în caz de eșec al unei instanțe, asigurând redundanță și continuitatea operațiunilor.
Fiecare instanță virtuală din cluster va fi configurată cu minim 2 vCPU.
Soluția trebuie să fie livrată cu licențe și suport de producător în modelul 24x7 pentru o perioadă de 5 ani. Licențele trebuie să includă toate funcționalitățile legate de load balancing, protecția DDoS și monitorizarea sănătății aplicațiilor.

5.7.14.4 Software de monitorizare a performanței aplicațiilor

Având în vedere complexitatea tehnică și funcțională a sistemului, precum și importanța acestuia, este necesara implementarea unei soluții care să detecteze și să faciliteze remedierea problemelor de funcționare care afectează performanța și disponibilitatea aplicațiilor critice ale SIISPECD, respective Platforma de management documente, PSEP și Software-ul de gestiune a bazelor de date.
Soluția trebuie să monitorizeze performanța funcționării aplicațiilor oferind următoarele funcționalități minime:

- Monitorizează întreaga stivă de aplicații din cadrul sistemului
- Urmărește metrici cheie (timp de răspuns, utilizare CPU/RAM, rate de eroare) în timp real;.
- Oferă trasabilitate end-to-end a tranzacțiilor pentru identificarea blocajelor în fluxurile de lucru (e.g., procesarea petițiilor).
- Utilizează algoritmi AI pentru a detecta anomalii și a prevedea probleme.
- Trimite alerte prin email sau se integrează cu Azure Monitor pentru notificări proactive.
- Evaluează performanța PSEP, urmărind metrici precum latența formularelor și timpul de încărcare a paginilor.
- Suportă monitorizare sintetică pentru simularea interacțiunilor utilizatorilor, asigurând o experiență consistentă.

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

- Generează tablouri de bord personalizabile și rapoarte lunare privind incidentele și performanța.
- Facilitează analiza cauzelor rădăcină pentru rezolvarea rapidă a incidentelor
- Înregistrează evenimentele de performanță și se integrează cu Software-ul de jurnalizare pentru gestionarea centralizată a auditului, respectând cerințele de jurnalizare.

Soluția trebuie să fie compatibilă cu Azure, putând fi implementată pe mașini virtuale Windows Server sau RHEL.
Soluția se va integra cu Active Directory pentru controlul accesului securizat.
Oferă API-uri REST pentru integrarea cu Platforma de management documente, PSEP și Software-ul de gestiune a bazelor de date, respectând principiile SOA.
Exportă date de performanță către Software-ul de jurnalizare de audit pentru corelarea auditului și către Software-ul de realizare a copiilor de siguranță pentru backup.
Permite realizarea de extensii personalizate pentru monitorizarea fluxurilor, facilitând mentenanța evolutivă.
Înregistrează securizat activitățile de monitorizare, îndeplinind cerințele de jurnalizare
Se va licenția astfel încât să acopere aplicațiile monitorizate și/sau hosturile, optimizat pentru toate mașinile virtuale ale SIISPECD și aplicațiilor cheie.

5.8. Cerințe software

5.8.1. Platforma de dezvoltare și administrare aplicații web (LCAP)

Portalul de servicii electronice publice se va implementa pe baza unei platforme de dezvoltare aplicații web din categoria Enterprise Low-Code Application Platform (LCAP). Platforma LCAP trebuie să fie o soluție matură și specializată, introdusă deja în circuitul comercial. Maturitatea soluției presupune îndeplinirea tuturor următoarelor condiții:

a. existența referințelor publice pe website-ul producătorului din care să rezulte trecerea prin cel puțin 2 iterații/versiuni majore prin care s-au îmbunătățit funcționalitățile și performanța.
b. existența unui roadmap publicat de producător privind dezvoltarea produsului;
c. motivată de obligativitatea implementării cu succes a unei soluții informatice, autoritatea contractantă apreciază că este necesar să se asigure că platforma ofertată este funcțională și eficientă, iar utilizarea acesteia în cadrul instituției nu va conduce la blocarea activității. Pe cale de consecință, solicităm prezentarea de recomandări din partea a cel puțin 2 beneficiari finali din care să rezulte utilizarea cu succes a acesteia pentru implementarea de aplicații web. Apreciem că dovada implementării și utilizării cu succes a platformei de către 2 beneficiari finali, va genera instituției un beneficiu prin utilizarea unei platforme a cărei inadvertențe și/sau eventuale probleme au fost deja cunoscute și remediate.
d. existența unui portal al comunității cu utilizatori activi, ce include documentație tehnică de produs, resurse de formare și bune practici, precum și un forum pentru depanare;

Produsul software trebuie să pună la dispoziție un mediu unificat integrat de configurare și

administrare (Integrated Development Environment), asigurând o experiență fără întreruperi pentru dezvoltare și administrare. Acest mediu trebuie să permită colaborarea în timp real și în cadrul său să ofere o interfață de tip drag-and-drop pentru dezvoltare și administrare

Pentru a asigura performanță, stabilitate și securitate soluția propusă trebuie să permită implementarea întro arhitectură de înaltă disponibilitate în configurații de tip activ-activ.

Pentru scopul acestui proiect, Achizitorul solicită implementarea unei configurații de tip activ-activ pentru aplicații în ambele centre de date. Toate nodurile vor participa activ la deservirea cererilor utilizatorilor.

Conţinutul aplicațiilor dezvoltate pe platforma LCAP va fi introdus şi afişat în format Unicod (UTF-8) – lucru care va permite afişarea concomitentă a textelor în caractere latine (inclusiv diacriticele româneşti).

Din punctul de vedere al licențierii, Platforma de dezvoltare și administrare aplicații web (LCAP) trebuie să acopere un număr nelimitat de utilizatori, pentru toate instanțele de server web necesare respectării cerințelor de arhitectură a sistemului (i.e. separarea între mediul de back-office și cel de front-office, clusterizarea serverelor de aplicatie, compatibilitatea cu celelalte componente software ale arhitecturii SIISPECD) și cerințelor de performanță.

Licențierea platformei LCAP va asigura un drept de utilizare perpetuu pentru beneficiar și nu va impune limite privind numărul de utilizatori ce vor accesa aplicațiile web dezvoltate pe aceasta, în mod autentificat sau neautentificat.

Produsul va beneficia de suport tehnic pe o perioadă de 5 (cinci) ani, acoperind dreptul beneficiarului de a face update–uri precum și access direct la site-ul producătorului pentru a deschide direct cazuri de suport cu acesta.

Pentru asigurarea neutralității tehnologice pe termen lung, Platforma de dezvoltare și administrare aplicații web (LCAP) va permite modificarea/ actualizarea/ extinderea aplicațiilor implementate (Portal de servicii de electronice publice, modulele aplicative ale SIISPECD) dintr-o interfață grafică, fără a necesita scrierea de cod, dispunând în acest sens de următoarele categorii de funcționalități:

a. Managementul rolurilor
b. Managementul permisiunilor
c. Managementul utilizatorilor
d. Interfațare API și administrare
e. Automatizare
f. Fluxuri de lucru
g. Funcții predefinite
h. Managementul entităților
i. Managementul meniurilor
j. Managementul paginilor
k. Managementul formularelor
l. Managementul listelor

m. Managementul funcțiilor de chatbot

Funcționalitățile de managementul rolurilor trebuie să includă:

a. Adăugarea, editarea sau ștergerea rolurilor;
b. Configurarea rolurilor pentru restricționarea accesului la nivel de pagină, componentă, acțiune, flux de lucru sau entitate;

Funcționalitățile de managementul permisiunilor trebuie să asigure definirea schemei de permisiuni astfel:

a. Configurarea permisiunilor la nivel de pagină (de acces sau de editare) în funcție de rol;
b. Configurarea permisiunilor la nivel de entitate, determinând astfel operațiunile disponibile utilizatorului prin interfață, cum ar fi Creare, Citire, Actualizare sau Ștergere;
c. Configurarea permisiunilor la nivel de modul pentru a restricționa accesul sau pentru a acorda opțiuni de editare rolurilor;
d. Configurarea permisiunilor la nivel de acțiuni și butoane, astfel încât acestea să fie disponibile doar pentru anumite roluri;
e. Configurarea permisiunilor la nivel de căutare prin stabilirea de reguli care să restricționeze afișarea rezultatelor în funcție de roluri;
f. Configurarea permisiunilor de utilizare a resurselor API.

Funcționalitățile de managementul utilizatorilor trebuie să includă:

a. Crearea utilizatorilor și asocierea acestora la cel puțin un rol;
b. Modificarea utilizatorilor, acordarea sau revocarea rolurilor;
c. Ștergerea utilizatorilor.

Funcționalitățile de interfațare API trebuie să includă:

a. Crearea de interfețe REST API;
b. Crearea metodelor API (GET, POST, PUT, DELETE) pentru execuția logicii (acțiunilor) la nivel de server sau pentru preluarea datelor;
c. Securizarea API-urilor prin chei API și token web JSON;
d. Mecanisme de partajare a resurselor restricționate ale unei pagini web dintr-un alt domeniu aplicativ.

Funcționalitățile de automatizare trebuie să includă:

a. Posibilitatea programării execuției automate de joburi/acțiuni, periodic la anumite momente/intervale (declanșatoare de timp, declanșatoare de interval) sau când are loc un eveniment (la lansarea/închiderea aplicației, la începutul/sfârșitul fiecărei solicitări);
b. Programarea execuției automate a următoarelor job-uri/acțiuni:
    i. rulare interogări SQL;
    ii. rulare executabile;
    iii. rulare scripturi;
    iv. postarea de date;
    v. transmiterea de e-mailuri;

Funcționalitățile asociate fluxurilor de lucru trebuie să includă:

a. Posibilitatea definirii unei liste de acțiuni, ce trebuie efectuate întro anumită succesiune, care poate include o logică condiționată;
b. Posibilitatea definirii fluxurilor de lucru prin utilizarea a cel puțin următoarelor elemente BPMN: eveniment de start, eveniment de stop, activități, poartă de decizie (XOR);
c. Posibilitatea testării fluxurilor de lucru prin rularea acestora și indicarea erorilor prin mesaje de eroare;
d. Posibilitatea clonării fluxurilor de lucru cu logică similară și editarea acestora în scopul creării unui flux nou;
e. Posibilitatea adăugării activităților în fluxul de lucru prin intermediul funcțiilor predefinite (secvențe de cod) cu variabile/parametrii de intrare și de ieșire.

Platforma va dispune de următoarele funcții predefinite:

- Adăugarea unei casete de verificare (checkbox) prin care să se afișeze/ascundă un câmp dinamic în urma verificării condiției adevărat/fals;
- Adăugarea unui selector de dată și oră;
- Adăugarea unui câmp derulant (dropdown);
- Adăugarea unui câmp de tip text;
- Adăugarea de elemente de tip opțiuni multiple (multiple choice) cu casete de verificare (checkboxes);
- Adăugarea de elemente de tip opțiuni multiple (multiple choice) cu câmpuri derulante (dropdown);
- Adăugarea de elemente de tip opțiuni multiple (multiple choice) cu butoane de opțiune (radio button);
- Adăugarea unei casete de text pentru introducerea unui număr;
- Adăugarea unui element de tip glisor (slider);
- Adăugarea de text static;
- Încărcarea unui câmp dinamic dintr-un JSON;
- Transmitere email către unul sau mai mulți recipienți;
- Transmitere email cu fișier atașat
- Crearea unei entități noi;
- Crearea unui obiect JSON;
- Crearea unei pagini noi;
- Crearea unui portal nou;
- Crearea unui rol;
- Crearea unui thumbnail;
- Adăugarea, ștergerea, vizualizarea sursei de date;
- Afișare mesaje (de eroare, de confirmare, etc.);
- Descărcare fișier;
- Executare cod Javascript;
- Adăugare modul la o pagină;

- Criptare/decriptare date AES și RSA;
- Modificarea permisiunilor pentru foldere;
- Autorizarea utilizatorilor;
- Închidere formulare pop-up;
- Închidere ferestre pop-up;
- Conversia datelor HTML în Microsoft Word;
- Copiere fișier întrun alt folder;
- Ștergere entitate, fișier, folder, modul, pagină, portal, rol, utilizator;
- Executare listă de acțiuni;
- Generare cod de bare;
- Generare PDF din șablon HTML;
- Îmbinare (merge) fișiere PDF;
- Injectarea unei imagini în PDF;
- Generare credențiale;
- Interogare date în sursa de date;
- Creare folder nou;
- Conversia unei liste de entități în format CSV și/sau Excel;
- Conversia în format Excel a unei liste de rezultate obținute printr-o căutare (query) în baza de date;
- Încărcare listă de entități din conținutul unui fișier CSV, XLSX, JSON, precum și dintr-o interogare SQL;
- Încărcare conținut dintr-un modul HTML;
- Încărcare pagină în contextul de execuție;
- Încărcare portal în contextul de execuție;
- Creare arhivă de fișiere specificate;
- Dezarhivare fișiere dintr-o arhivă;
- Parsare valori multiple din aceeași sursă;
- Parsare JSON pentru extragerea valorilor parametrilor;
- Parsare XML pentru extragerea valorilor parametrilor;
- Redirecționarea utilizatorului către o altă pagină din portal sau către un URL, după transmiterea unui formular;
- Rulare SQL Query
- Actualizare modul, pagina, portal, rol, profil utilizator, nume utilizator;
- Încărcare fișier(e) pe un FTP;
- Validare utilizator/parolă;
- Înregistrare utilizator;

Funcționalitățile de managementul entităților trebuie să includă:

a. Adăugarea, editarea, ștergerea și vizualizarea entităților;

b. La crearea unei entități trebuie:
   i. să se genereze automat tabelele în baza de date, cu chei index pe baza relațiilor definite cu alte entități;
   ii. să se genereze o pagină ce va apare în meniul principal al aplicației, existând totuși posibilitatea dezactivării afișării paginii entității în meniul principal (fiind accesată de exemplu la completarea unui formular); Pagina trebuie să poată fi definită ca o pagină de nivel superior sau ca un copil al unei pagini existente;
   iii. să se genereze un formular pentru introducerea datelor cu câmpuri bazate pe proprietățile definite la crearea entității;
   iv. să se poată genera o listă de valori pentru a afișa înregistrările asociate entității;
   v. să se poată defini o sursă de date pentru entitate;
   vi. să se genereze automat butoane în interfață prin care să se ofere posibilitatea de a crea, edita, șterge și vizualiza înregistrările;
   vii. să se poată defini funcții predefinite care să fie utilizate pentru operațiuni de creare, ștergere, actualizare parțială, actualizare și citire;
   viii. să se poată defini/utiliza API-uri pentru crearea, preluarea, actualizarea și ștergerea înregistrărilor;
   ix. să se poată genera un tablou de bord vizual în care să se definească KPI-uri pe baza datelor din entitate;
c. Reprezentarea vizuală a relației dintre entități;
d. Posibilitatea definirii relațiilor dintre entități;
e. Configurarea permisiunilor pentru restricționarea accesului la nivel de entitate: vizualizare, adăugare, editare, ștergere;

Funcționalitățile de managementul meniurilor trebuie să includă:

a. Posibilitate grupării paginilor pentru crearea de sub-meniuri;
b. Posibilitatea organizării meniului prin funcții de tip drag-and-drop a paginilor definite;
c. Posibilitatea organizării meniului pentru diferite profiluri de utilizator;

Funcționalitățile de managementul paginilor trebuie să includă:

a. Posibilitatea restricționării accesului la nivel de pagină în funcție de rol: vizualizare, adăugare pagină, editare proprietăți pagină, mutare pagină și ștergere pagină ;
b. Posibilitatea definirii ca pagină copil a unei pagini părinte;
c. Posibilitate definirii de cuvinte cheie pentru o pagină;
d. Posibilitatea publicării programate (sau scoaterii din publicare) la o anumită dată și oră;
e. Afișarea paginii în meniul principal, existând totuși posibilitatea dezactivării afișării (fiind accesată de exemplu la completarea unui formular).
f. Posibilitatea așezării conținutului, în fiecare pagină, prin componente de tip HTML (text), formulare, liste și tab-uri;

Funcționalitățile de managementul formularelor trebuie să includă:

a. Posibilitatea definirii unui formular pe oricare pagină în vederea colectării de date;

b. Definirea de formulare cu următoarele tipuri de câmpuri:
c. Casetă de text – permite introducerea de conținut de tip text pe o singură linie sau pe mai multe, permițând condiționarea numărului de caractere sau introducerea unei validări personalizate;
d. Număr întreg;
e. Email – permite introducerea de conținut de tip text. Validează conținutul pentru a fi o adresa de email validă.
f. Telefon - permite introducerea de conținut de tip text sub forma de număr de telefon în formatul definit de standardul internațional E.164. Permite realizarea automată a preselecției prefixului în funcție de țară;
g. Casetă de text cu editor WYSIWYG - permite introducerea de conținut de tip text și formatarea acestuia prin următoarele opțiuni:
    i. Alegerea stilului caracterelor: bold, italic, subliniat, superscript, subscript;
    ii. Alegerea dimensiunii caracterelor;
    iii. Alegerea de liste numerotate automat sau cu bullet-uri;
    iv. Alegerea spațierii între rânduri;
    v. Alegerea alinierii textului la stânga, la centru, la dreapta;
h. Text static – permite afișarea de informații ce nu pot modificate de către utilizator, cum ar fi mesaje de informare sau mesaje de ajutor. Permite formatarea/stilizarea textului;
i. Dropdown - permite alegerea unei opțiuni dintr-o listă predefinită sau dinamică;
j. Dropdown cu autocompletare - permite alegerea unei opțiuni dintr-o listă predefinită sau dinamică, permițând filtrarea listei de opțiuni pe măsură de textul este introdus;
k. Dropdown cu casete de verificare - permite alegerea unei opțiuni dintr-o listă predefinită sau dinamică, prin bifarea acesteia;
l. Alegere multiplă cu casete de verificare - permite alegerea uneia sau mai multor opțiuni dintr-o listă predefinită sau dinamică.
m. Casete cu butoane de opțiune (radio button) - permite alegerea unei opțiuni dintr-o listă predefinită sau dinamică de tip radio button;
n. Caseta de dată și oră – permite alegerea unei date și ore sau a unui interval de date sau date și ore. Formatul afișat trebuie să se poată configura, putându-se dezactiva date din viitor sau din trecut, precum și personalizarea în funcție de criterii dinamice;
o. Caseta de Încărcare a unui singur fișier - Permite încărcarea unui fișier, cu o extensie ce se validează printr-o listă de extensii valide (sigure), configurabile. Permite limitarea dimensiunii unui document care poate fi încărcat. Asigură gestionarea fișierelor duplicate prin suprascriere sau redenumire;
p. Caseta de Încărcare fișiere multiple - Permite încărcarea mai multor fișiere, cu extensii ce se validează printr-o listă de extensii valide (sigure), configurabile. Permite limitarea dimensiunii unui document care poate fi încărcat. Asigură gestionarea fișierelor duplicate prin suprascriere sau redenumire;

q. Parolă/Confirmare parolă - permite introducerea parolelor. Parolele nu sunt vizibile la tastare și sunt criptate.
r. Valută - Permite introducerea de sume de bani prin configurarea: monedei, definirea poziția însemnului distinctiv la monedei, definirea separatorului de zecimale, definirea separatorului de mii;
s. Posibilitatea definirii direcției etichetelor pentru fiecare câmp (sus, stânga, dreapta);
t. Posibilitatea adăugării de instrucțiuni de completare pentru fiecare câmp;
u. Posibilitatea definirii de validatori personalizați pentru orice câmp. Aplicația va dispune de următorii validatori predefiniți:
    i. Număr întreg;
    ii. Număr întreg pozitiv;
    iii. Email;
    iv. Dată;
    v. Obligatoriu;
v. Posibilitatea condiționării validatorilor în funcție de alte câmpuri pentru a putea permite crearea logicii afișării sau validării câmpurilor unui formular;
w. Generarea listei de opțiuni pentru câmpurile cu alegere multiplă de tip dropdown sau cu casete de verificare, trebuie să se poată realiza prin:
    i. Listă statică de formă cheie/valoare;
    ii. Interogări ale bazei de date prin care se aduc datele;
    iii. API ce returnează format JSON;
x. Posibilitatea de a construi formulare dinamice prin utilizarea de expresii de legătură, care pot controla afișarea sau activarea câmpurilor.

Funcționalitățile de managementul listelor trebuie să includă:

i. Posibilitatea definirii afișării listelor de date, sub formă tabelară, din următoarele surse de date: formulare, tabele din baza de date, interogări SQL și solicitări JSON de la un API;
ii. Posibilitatea adăugării de noi surse de date;
iii. Permite definirea pentru fiecare coloană a funcționalităților de filtrare, ordonare, sortare și căutare;

Funcționalitățile de management al funcțiilor de chatbot trebuie să includă:

a. mecanisme de inteligență artificială care să permită interacțiunea naturală a actorilor aplicațiilor web implementate;
b. motor NLU multi-language care să identifice intențiile utilizatorului, sentimentele și entitățile de sistem;
c. posibilitatea antrenării asistentului inteligent pentru a răspunde la întrebări simple sau complexe, atât cu fraze introduse manual, dar și prin integrarea cu surse de date din aplicațiile implementate;
d. posibilitatea configurării trimiterii de notificări;
e. generarea de rapoarte avansate în format PDF, MS Word sau Excel. Să asigure un generator

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

PDF încorporat;

f. asistarea utilizatorilor în completarea unor documente;
g. detectarea intenției utilizatorului;
h. extragerea automată a entităților;
i. motor NLP cu suport pentru limba română;
j. colectarea de date din informațiile introduse de utilizator, din acțiuni și din aplicații;
k. utilizarea datelor colectate pentru a oferi răspunsuri contextuale;
l. filtrarea conversațiilor.
m. functionalități built-in de OCR
n. Suport nativ în limba română, cu diacritice
o. Configurarea de fluxuri conversaționale (fără scriere de cod)
p. configurarea comportamentului chatbotului în cazul în care acesta nu înțelege cerința utilizatorului;
q. monitorizarea calității modelului de antrenament;
r. stocarea istoricului de conversații.

Funcționalitățile de management al funcțiilor de chatbot pot fi asigurate de către Ofertant prin oricare dintre următoarele două modalități tehnice, cu condiția respectării integrale a specificațiilor funcționale și de securitate solicitate:

a. nativ, prin utilizarea componentelor și modulelor incluse direct în arhitectura Platformei de dezvoltare și administrare aplicații web (LCAP) propuse;
b. prin integrare cu soluție software terță, specializată și matură. În acest caz, Ofertantul are obligația de a asigura interfațarea completă și transparentă a soluției de chatbot cu Platforma LCAP, utilizând mecanisme de tip API sau conectori dedicați. Toate costurile aferente licențierii și integrării soluției de chatbot (inclusiv eventualele costuri pentru instrumente AI terțe) vor fi incluse în propunerea financiară în prețul Platformei de dezvoltare și administrare aplicații web (LCAP) , fără a genera costuri suplimentare pentru Achizitor pe durata contractului

Pentru implementarea funcționalităților serviciului public de prevenire a faptelor de discriminare în cadrul Portalului de Servicii Electronice Publice, Platforma de dezvoltare și administrare aplicații web (LCAP) va fi livrată împreună cu o aplicație software specializată și matură, ce va facilita implementarea cerințelor funcționale privind furnizarea de cursuri de formare, îndeplinind, în acest sens, următoarele cerințe:

- aplicația va fi instalată pe infrastructura proiectului în mașină virtuală;
- aplicația permite personalizarea interfeței la nivel de grafică (logo, culori, pagină de login) conform identității vizuale a beneficiarului
- aplicația permite personalizarea la nivel de interfață și funcționalități, incluzând cel puțin: modul de afișare grupat/negrupat al cursurilor, afișarea/ascunderea cursurilor inactive, utilizarea unei adrese personalizate de email pentru comunicare

- aplicația va afișa toate meniurile și informațiile afișate în timpul lucrului minim în limba română
- aplicația permite activarea/dezactivarea de măsuri suplimentare de securitate, incluzând minim autentificare în doi pași
- aplicația dispune de un sistem de securitate de tip reCAPTCHA sau similar
- aplicația dispune de un sistem de securitate ce trece minim testele de securitate OWASP Top 10
- aplicația permite activarea/dezactivarea posibilității ca utilizatorii să își creeze singur conturi (self-registration)
- aplicația permite ca în baza valorii câmpurilor existente la înregistrare, utilizatorii să fie alocați automat către grupe diferite de studiu
- aplicația dispune de cel puțin patru roluri implicite pentru utilizatori: Cursant, Instructor, Manager și Administrator
- aplicația este de tip multirol, fiecare utilizator putând să acceseze toate drepturile care îi sunt alocate pe baza unui singur nume de utilizator și a unei parole, fără să trebuiască să se logheze/delogheze cu fiecare rol pentru a beneficia de drepturile/funcționalitățile respectivului rol
- aplicația permite utilizatorior cu rol de Administrator să creeze roluri noi, pe baza drepturilor celorlalte tipuri de utilizatori
- soluția include o aplicație de mobil (atât pentru iOS cât și pentru Android) pentru utilizatorii de tip Cursant, ce este oferita ca parte din soluție.
- Aplicația de mobil oferă utilizatorilor de tip Cursant posibilitatea de a stoca local (pe mobil/tableta unde este instalata) cursurile alocate și de a le parcurge chiar și în lipsa unei conexiuni active la internet
- Aplicația de mobil sincronizează automat progresul înregistrat de utilizatorii de tip Cursant în cursurile consumate asincron atât dinspre dispozitivul mobil, cat si dinspre platforma, la reconectarea dispozitivului mobil la internet
- aplicația permite definirea de câmpuri suplimentare în profilul utilizatorilor sau descrierea cursurilor care să fie folosite în procese de gestionare a utilizatorilor sau cursurilor, respectiv în diferite tipuri de rapoarte
- aplicația permite realizarea de conturi prin importul informațiilor din fișiere .xls sau .csv
- aplicația dispune de modele de fișiere pentru importul informațiilor pentru crearea de conturi
- aplicația asigura posibilități multiple de a căuta, filtra și sorta informațiile despre utilizatori și cursuri, în funcție de gradul de acces acordat de rolul sau rolurile deținute de fiecare utilizator
- aplicația asigura posibilitatea utilizatorilor cu rol de Instructor și Administrator să formeze grupe de studiu, în care să aloce utilizatorii la care respectivele roluri au acces

- aplicația permite alocarea automată a utilizatorilor la grupele existente, în baza criteriilor stabilite pentru acestea, pe baza informațiilor despre utilizatori existente în platformă sau completate la momentul înregistrării
- aplicația asigura organizarea de cursuri sincron prin integrarea nativa (conector) cu un sistem de video-conferință consacrat Google Meet/ Microsoft Teams sau Zoom (care se va putea integra prin parametrii conectorului)
- aplicația trebuie să fie compatibilă cu standardul SCORM, putând rula minim pachete SCORM 2004, versiunea 3
- aplicația asigura organizarea de cursuri asincron, pentru care utilizatorii cu rol de Instructor și Administrator pot încărca suporturi de învățare minim în următoarele formate: .zip (SCORM), .pdf, .pptx, .mp3, .mp4, .xlsx, .docx.
- aplicația asigura posibilitatea Administratorilor să creeze categorii de suporturi de învățare, astfel încât acestea să poată fi organizate
- aplicația asigura posibilitatea utilizatorului care a încărcat un material să îl previzualizeze fără ca acesta să îi fie alocat și fără înregistrarea în platformă a activității acestuia (mod sand-box)
- aplicația asigura alocarea de elemente de identificare pentru materialele încărcate, minim autor, imagine reprezentativă, descriere și categorie
- aplicația asigura vizualizarea numărului de conectări ale utilizatorilor, precum și a numărului de accesări ale cursurilor întro anumită perioadă de timp
- Pentru materialele SCORM aplicația permite modificări limitate ale materialului încărcat, prin suprascriere a acestuia cu forma actualizată, fără a se pierde datele privind progresul, timpul sau scorul utilizatorilor care au parcurs deja respectivul material in forma sa anterioara si fără a trebui realocat cursanților materialul în forma actualizată
- aplicația asigura administrarea procesului de formare, oferind minim limitarea timpului de accesare al materialelor digitale și al examenelor/probelor de evaluare, numărul de accesări pentru finalizarea cursului
- aplicația permite utilizatorilor de tip Cursant sa încarce teme de lucru aferente fiecărui curs asincron, respectiv utilizatorilor de tip Instructor sa vadă respectivele teme încărcate de fiecare Cursant
- aplicația asigura configurarea de trasee de învățare, adică organizarea întro ordine stabilită a cursurilor ce trebuie parcurse de către cursanți
- Întrun traseu de învățare aplicația permite introducerea unei descrieri, a unei imagini reprezentative si a autorului traseului respectiv
- Aplicația software permite vizualizarea și extragerea rapoartelor în format minim .xlsx privind progresul utilizatorilor cu rol de Cursant atât la nivel individual, cât și la nivel de grupă, de curs sau de categorie de cursuri
- Aplicația software permite vizualizarea și folosirea informațiilor (câmpurilor noi) introduse pentru utilizatori sau cursuri ca filtre în vizualizarea rapoartelor

- Aplicația software permite vizualizarea și extragerea răspunsurilor individuale date de utilizatori la întrebările din chestionarele parcurse
- Aplicația software permite vizualizarea și extragerea răspunsurilor date de utilizatorii cu rol de Cursant la întrebările de tip sondaj, în mod anonimizat
- Aplicația software permite vizualizarea sub formă grafică a situației generale privind stadiul de parcurgere a unui curs, incluzând minim informații despre numărul de cursanți alocați, procentul celor care l-au accesat, procentul celor care l-au finalizat, timpul total și mediu petrecut în curs, precum și, dacă există, situația scorului obținut
- Aplicația software permite generarea și descărcarea unui raport care să reflecte performanța înregistrată întrun curs în mod cumulat și subsecvent pe fiecare dintre structurile organizatorice create. Raportul include minim informații despre scorul mediu, timpul total, gradul de finalizare și numărul de Cursanți pentru fiecare dintre nivelurile selectate
- Aplicația software permite utilizatorilor cu rol de Instructor sau Administrator să vadă detalii despre mesajele transmise cu ajutorul sistemului de mesagerie integrat, per canal de transmitere
- Pe toata perioada de licențiere a soluției se va asigura mentenanță si update-uri, fiind necesară prezentarea în acest sens a unei declarații asumate de către producător, pentru prezentul proiect

Toate costurile aferente licențierii și integrării aplicației software specializate de furnizare de cursuri de formare vor fi incluse în propunerea financiară în prețul Platformei de dezvoltare și administrare aplicații web (LCAP), fără a genera costuri suplimentare pentru Achizitor pe durata contractului.

5.8.2. Platforma de managementul documentelor

5.8.2.1 Cerințe generale

Platforma software de management al documentelor va fi bazată pe o soluție „Low code/No code”, introdusă în circuitul comercial pentru a garanta fiabilitatea și performanța necesare gestionării fluxurilor critice de documente și arhivare electronică ale instituției, conform cerințelor de disponibilitate înaltă și securitate din prezentul caiet de sarcini.

Maturitatea soluției presupune îndeplinirea tuturor următoarelor condiții:

a. existența referințelor din care să rezulte trecerea prin cel puțin 2 iterații/versiuni majore prin care s-au îmbunătățit funcționalitățile și performanța.
b. existența unui roadmap emis de producător privind dezvoltarea produsului;
c. motivată de obligativitatea implementării cu succes a unei soluții informatice, autoritatea contractantă apreciază că este necesar să se asigure că aplicația ofertată este funcțională și eficientă, iar utilizarea acesteia în cadrul instituției nu va conduce la blocarea activității. Pe cale de consecință, solicităm prezentarea de recomandări din partea a cel puțin 2 beneficiari finali din care să rezulte utilizarea cu succes a acesteia. Apreciem că dovada implementării și utilizării cu succes a aplicației de către 2 beneficiari finali, va genera

insituției un beneficiu prin aplicarea unei soluții ale căror inadvertențe și/sau eventuale probleme au fost deja cunoscute și remediate.

d. existența unui portal al producătorului, ce include documentație tehnică de produs;

Platforma software trebuie să pună la dispoziție un mediu unificat integrat de configurare și administrare, asigurând implementarea soluției prin utilizarea unei metodologii de tip prototip evolutiv, oferind astfel utilizatorilor o imagine concretă asupra modului de gestionare a documentelor și a metadatelor asociate, a versiunilor acestora, precum și a fluxurilor de lucru cu documente.

Platforma va asigura gestionarea documentelor și a metadatelor asociate, a versiunilor acestora, a tuturor fluxurilor de lucru și a obiectelor, facilitând astfel ținerea evidenței activității instituției în sistem informatizat și circulația electronică a documentelor în cadrul acesteia.

Platforma va asigura înregistrarea, scanarea şi stocarea în forma electronica a oricărui document, alături atributele, metadatele și datele descriptive conexe, care să ajute la o rapidă organizare și regăsire ulterioară a informației;

Platforma va asigura trasabilitatea circuitului documentelor în cadrul instituției, punând la dispoziție instrumente prin care să asigure în orice moment vizualizarea traseului documentelor, utilizatorul la care se află documentul, starea asociată etc..

Platforma va asigura automatizarea proceselor de lucru existente în cadrul instituției prin implementarea de fluxuri de lucru electronice.

Platforma software de management al documentelor trebuie să fie o soluție complet integrată, scalabilă, deschisă și extensibilă, pentru asigurarea interoperabilității cu alte aplicații/sisteme informatice, atât prin API cât și prin interfețe și/sau conectori dedicați.

5.8.2.2 Cerințe privind tipurile de utilizatori

Platforma software de managementul documentelor va fi implementată astfel încât să asigure utilizarea de către următoarele categorii de utilizatori:

a. Utilizatori standard (ce vor utiliza clienți web și clienți mobili) – minim 75;
b. Utilizatori avansați (ce vor utiliza clienți desktop) – personal responsabil de primirea și înregistrarea documentelor: minim 4
c. Utilizatori de tip administrator – specialiști IT: minim 1

Utilizatorii avansați vor dispune de toate funcționalitățile oferite de Platforma software de managementul documentelor, accesibile la nivelul utilizatorului.

Utilizatorii standard vor dispune de toate funcționalitățile oferite de Platforma software de managementul documentelor, mai puțin cele referitoare la scanare.

Utilizatorii de tip administrator vor dispune de toate funcționalitățile oferite de Platforma software de managementul documentelor și, în plus, vor putea efectua următoarele acțiuni:

a. configurarea funcțiilor, a serviciilor și a meniurilor platformei;

b. configurarea depozitelor de documente și a registrelor;
c. definirea fluxurilor;
d. configurarea integrării cu soluții de management a utilizatorilor și accesului;
e. gestionarea locațiilor de stocare a documentelor, a tipurilor de obiecte, cheilor de criptare, precum și definirea și gestionarea profilurilor de backup ale soluției, vizualizarea și editarea fișierelor de configurare, instalarea și managementul componentelor soluției;
f. configurarea directoarelor de rețea monitorizate pentru declanșarea automată a unor fluxuri de lucru ori de câte ori se importă un fișier;
g. configurarea interfațării cu server de email pentru transmiterea mesajelor generate de aplicație;
h. configurarea conturilor de email monitorizate pentru declanșarea automată a unor fluxuri de lucru ori de câte ori se importă un fișier;
i. configurarea interfațării prin servicii web de tip REST cu alte aplicații informatice, în vederea facilitării accesului la documentele stocate precum și pentru preluarea documentelor care trebuie stocate;
j. configurarea task-urilor pre-programate care trebuie declanșate le momente de timp pre-fixate;
k. monitorizarea conexiunii între diferitele componente ale soluției;
l. monitorizarea tuturor operațiilor și evenimentelor din soluție;
m. monitorizarea mesajelor legate erori survenite și/sau de blocarea unor fluxuri (de exemplu datorită unor erori de concepere a acestora în faza de proiectare);

5.8.2.3 Cerințe privind accesul și interfața platformei

Platforma trebuie să asigure accesul utilizatorilor la funcționalități, în funcție de rol și locație, prin intermediul mai multor tipuri de clienți dedicați, după cum urmează:

a. Client de tip Web;
b. Client de tip mobil;
c. Client de tip desktop (rich-client).

Accesarea platformei de către utilizatorii standard ce utilizează client de tip web, se va realiza prin intermediul unui browser web, fără a fi necesară instalarea pe stația de lucru de utilitare sau plugin-uri. Browser-ele web prin care se va realiza accesarea vor fi Chrome, Edge, Firefox, Safari, compatibile cu standardele HTML5, CSS și JavaScript;
Accesarea platformei de către utilizatorii standard ce utilizează client de tip mobil, se va realiza printr-o aplicație mobilă, care să permită gestionarea activităților și a documentelor prin intermediul unui dispozitiv mobil de tip telefon inteligent sau tableta.
Aplicația mobilă trebuie să fie disponibilă pentru descărcare din magazinele Google și Apple.
Prin intermediul aplicației mobile, utilizatorii vor avea acces la cel puțin următoarele funcționalități:

a. Adăugare/modificare/ștergere directoare noi;
b. Adăugare/modificare/ștergere fișiere;
c. Încărcare versiuni noi de documente;
d. Vizualizare fișiere;
e. Adăugarea de notițe de margine generale, personale și permanente atât la nivel de folder cat și la nivel de document;
f. Formulare electronice;
g. Captura de date și arhivarea documentelor on-the-go;
h. Opțiuni de căutare și afișare a informației;
i. Inițierea și implicarea în fluxuri de lucru.

Prin intermediul aplicației mobile, utilizatorii vor avea posibilitatea de a participa activ pe fluxurile de lucru cu documente și informații, utilizând cel puțin funcționalități de tipul: pornire flux de lucru, transmitere documente pe fluxurile de lucru spre aprobare/informare, delegare fluxuri, fluxuri de lucru bazate pe formulare electronice.

Prin intermediul aplicației mobile, utilizatorii vor putea efectua căutări și vor putea salva căutările favorite.

Accesarea platformei de către utilizatorii avansați ce utilizează client de tip Desktop, se va realiza prin intermediul unei aplicații de tip ”rich client” ce se va instala pe stațiile de lucru ale acestora.

Pentru asigurarea unui acces centralizat și controlat, Platforma va asigura identificarea fiecărui utilizator în sistem prin utilizarea de conturi unice și personalizate de acces.

În funcție de autorizarea conferită utilizatorului, acesta va avea acces doar la documentele, fluxurile, registrele și funcționalitățile platformei, în conformitate cu drepturile de acces stabilite, în raport cu rolul și locul din organizație;

Interfața platformei prezentată utilizatorului va fi în limba română, inclusiv meniurile platformei și mesajele de eroare;

Interfața platformei trebuie să prezinte informațiile prin utilizarea de meniuri, sub-meniuri și meniuri contextuale.

Platforma trebuie să permită utilizatorului modificarea și personalizarea modului de afișare, a schemelor de culoare, a casetelor de dialog, precum și configurarea accesului rapid la funcții sau ascunderea acestora.

Platforma trebuie să permită utilizatorului configurarea afișării sarcinilor active după diverse criterii, precum ordonare ascendenta/descendenta, tipul sarcinii, termene limita, etc.

Platforma trebuie să permită utilizatorului configurarea zonei de afișare a sarcinilor de lucru prin posibilitatea de definire a unor profile de vizualizare care să secționeze ecranul astfel încât utilizatorul să aibă acces la toate zonele necesare pentru desfășurarea activității în mod centralizat – în urma definirii acestor profile de vizualizare va avea acces minim la lista de sarcini active, formularul atașat fluxului de lucru și structura de directoare asociată sarcinii.

Interfața grafică a platformei trebuie să fie dinamică, în sensul adăugării sau ascunderii automate a datelor și funcționalităților la care un utilizator/grup de utilizatori are/nu are acces;

Interfața grafică a platformei trebuie să asigure utilizatorului facilități avansate de vizualizare a documentelor de tip imagine: scalarea imaginii, încadrare pe înălțime, încadrare pe lățime, full-screen, mărire imagine în funcție de procent, previzualizare document, rotire pagina etc.;
Câmpurile din interfața platformei vor asigura introducerea și afișarea textului în format Unicode (UTF-8) – lucru care va permite afișarea textelor în caractere latine (inclusiv diacriticele românești).

5.8.2.4 Cerințe privind organizarea, încărcarea și căutarea documentelor

Platforma trebuie să permită definirea unei structuri arborescente pentru depozitele de documente electronice (arhive), organizată pe directoare și sub-directoare, pre-configurate sau generate dinamic în funcție de metadatele asociate documentelor.
Platforma nu trebuie să limiteze tipul de format de fișier ce poate fi arhivat/stocat, fiind permise atât fișierele de tip text, imagine, cât și orice alt tip de fișier;
Platforma trebuie să dispună de un motor de recunoaștere optică a caracterelor prin care se va realiza extragerea automată a textului din documentele electronice (inclusiv pentru fișiere de tip imagine), pentru a facilita căutarea avansată de tip full-text în toate documentele din depozit (pentru care exista drepturile de acces relevante).
Platforma nu va limita posibilitatea de adăugare a metadatelor pe documente în funcție de tipul de document/fișier.
Platforma trebuie să dispună de funcționalitatea de anulare (Undo) a următoarelor acțiuni efectuate în interfață asupra dosarelor și/sau documentelor: mutare dosar/document, ștergere dosar/document, utilizare ca referință dosar/document, editarea metadatelor la nivel de dosar/folder;
Platforma trebuie să dispună de mecanisme de sincronizare a documentelor și metadatelor asociate din depozit cu un sistem extern de fișiere de date (file-system);
Platforma trebuie să permită desfășurarea activităților de căutare la nivelul întregului depozit de documente, sau la nivelul unor zone restrânse din acesta, în funcție de drepturile de acces ale utilizatorului și de necesitățile acestuia de căutare;
Platforma trebuie să permită ordonarea elementelor din structura de organizare a depozitului în funcție de mai multe criterii: sortare manuală, alfabetică crescătoare sau descrescătoare, în funcție de data arhivării etc;
Platforma trebuie să asigure trasabilitatea modificărilor efectuate pe documente prin jurnalizarea acțiunilor realizate de utilizator în acest sens.
Platforma trebuie să permită afișarea unui document în mai multe locații din depozit prin crearea de referințe sau copii ale acestuia.
Platforma trebuie să pună la dispoziție un mecanism de căutare complex care să permită identificarea rapidă și facilă a informației pe baza unor criterii multiple și a unor opțiuni de căutare avansata, în toate depozitele de documente electronice în care utilizatorul deține dreptul de a caută documente.

Platforma trebuie să permită realizarea căutărilor în funcție de metadate, comentarii, versiuni, adnotări asupra documentelor, precum și căutare în conținutul documentelor;
Platforma trebuie să asigure facilitați avansate de căutare full-text în toate documentele din depozit (pentru care există drepturile de acces relevante) utilizând operatori logici, funcții de autocompletare în baza caracterelor deja introduse, auto-corecție a termenilor în cazul în care aceștia au fost introduși greșit, opțiunea de evidențiere a termenilor căutați, posibilitatea de excludere a unor termeni de căutare etc.
Platforma va pune la dispoziție funcționalități de listare a celor mai recente căutări, precum și opțiunea de căutări preferate.
Platforma trebuie să permită salvarea de profile de căutare și definirea de căutări personalizate;
Rezultatele căutărilor vor putea fi rafinate prin filtrări și ordonări suplimentare;
Platforma trebuie să asigure limitarea apariției duplicatelor în cadrul depozitului verificând astfel, automat, la fiecare încărcare, nu doar denumirea noului fișier, ci și conținutul acestuia (CRC sau similar). În cazul detectării duplicatelor, Platforma va notifica utilizatorul și îi va oferi posibilitatea de a realiza referință către un obiect existent în depozit.
Platforma trebuie să dispună de capabilități intrinseci de transfer de tip batch pentru importul rapid al volumelor mari de documente în depozite, asigurând cel puțin următoarele funcționalități:

a. Încărcarea documentelor în depozite în locațiile corespunzătoare, asigurând totodată atașarea metadatelor din fișierele cu metadescriptorii asociați;
b. Monitorizarea unuia sau mai multor directoare în vederea detectării unui flux de date;
c. Să permită ca structura de stocare să fie definită în funcție de anumite metadate ale documentelor, dar să asigure și posibilitate personalizării structurii.

Platforma trebuie să asigure transformarea în format electronic a documentelor în format letric, precum și preluarea acestora direct în aplicație prin integrarea cu dispozitive scanner ce dispun de drivere ISIS și/sau TWAIN.
Platforma trebuie să asigure transformarea în format electronic a documentelor în format letric, folosind echipamente de scanare de rețea, asigurând preluarea automată a acestora în aplicație prin monitorizarea unui sistem de fișiere.
Platforma trebuie să permită unirea paginilor întrun document electronic (Merge PDF) .
Platforma trebuie să permită împărțirea documentului electronic în pagini (Split PDF).

5.8.2.5 Cerințe privind înregistrarea documentelor

Platforma trebuie să permită transpunerea în formă electronică a proceselor de registratură și secretariat din instituție, asigurând în acest sens cel puțin următoarele funcționalități:
Platforma va permite definirea de noi registre de către administratorul de sistem.
Generarea numerelor de înregistrare și alocarea datei și orei de înregistrare se va realiza în mod automat, la introducerea unui document în sistem, în conformitate cu regulile de registratura

specifice instituției.
Platforma va permite înregistrarea documentelor de intrare, ieșire și interne, precum și eliberarea către solicitant a unei reciSIISPECD cu privire la preluarea și înregistrarea documentelor. Recipisa trebuie să fie configurabilă și să conțină minim elemente precum numărul, data și ora înregistrării, emitentul și conținutul pe scurt al documentului.
Platforma va permite utilizatorilor avansați ce utilizează client de tip Desktop să încarce documente în depozit și dacă nu dispun de conectivitate cu serverul – operare offline;
Platforma va asigura gestionarea tuturor tipurilor de documente de intrare/ieșire/interne ale instituției, indiferent de forma de intrare/ieșire: letric, electronic, e-mail, poștă sau fax;
Platforma va permite identificarea informațiilor despre stadiul de rezolvare al unui document, având posibilitatea de a puncta în orice moment locul în care acesta a ajuns şi starea acestuia.
Platforma va permite ca numerele de înregistrare să fie personalizate în funcție de specificul instituției și în conformitate cu regulile de registratura ale acesteia. Vor putea fi alocate sufixe și prefixe configurabile, se vor putea aloca inclusiv plaje de numere, în funcție de necesitățile autorității;
Platforma va permite configurarea fiecărui registru din punct de vedere al structurii – tip de coloane, tipul de documente ce pot fi înregistrate, precum și drepturile de acces pe care le pot avea utilizatorii asupra acestuia. Exemple de coloane pentru registre: data înregistrării, numărul, sursa, solicitant, destinatar, unitate organizatorică competentă, etc.
Platforma va permite definirea drepturilor de editare/vizualizare de către utilizatori/grupuri de utilizatori, pentru fiecare registru.
Platforma va permite alocarea unuia sau mai multor numere de înregistrare unui document, în funcție de circuitul documentului în cadrul instituției și în conformitate cu regulile de registratura.
Platforma va permite completarea registrelor manual sau automat, prin preluarea metadatelor specifice din documentele înregistrate.
Platforma va impune atașarea fișierelor în format electronic la numere de înregistrare, precum și atașarea automată a documentelor scanate în sistem la numărul de înregistrare aferent.
În vederea înregistrării, Platforma va asigura importul automat al documentelor, sub formă de sarcini, direct dintr-unul sau mai multe conturi de email configurabile în aplicație.
Platforma va asigura posibilitatea utilizatorilor, direct din interfața unui registru, să distribuie documente înregistrate (inclusiv cu metadatele aferente) către unitățile organizatorice din instituție.
Platforma va asigura posibilitatea configurării distribuirii automate a unor documente înregistrate către unitățile organizatorice competente din instituție.
Platforma va asigura resetarea pentru fiecare registru (an, lună etc), cu salvarea valorilor care au fost introduse anterior resetării.
Platforma va asigura jurnalizarea și generarea rapoartelor cu privire la activitatea de înregistrare a documentelor.
Platforma va asigura accelerarea proceselor de scanare a documentelor în format letric în vederea înregistrării, asigurând cel puțin următoarele funcționalități:

a. Să permită tipărirea de etichete cu coduri de bare care să fie aplicate pe documentele în format letric, în sprijinul identificării automate a acestora la scanare;
b. Să recunoască codurile de bare în momentul scanării documentelor și să asocieze automat documentele la înregistrările din registre fără necesitatea unei procesări manuale;
c. Să asigure alăturarea în același document a paginilor cu coduri de bare identice;
d. Să asigure injectarea de coduri de bare pe documentele electronice la momentul înregistrării acestora.

Platforma trebuie să permită conexarea mai multor documente întrun grup de documente (dosar/colecție de documente).
Platforma trebuie să permită atașarea unor documente la un document din depozit (ex. adăugarea unor anexe la un contract).
Platforma trebuie să permită implementarea Nomenclatorului Arhivistic al instituției, astfel încât la încărcarea unui document în depozit și selectarea tipului documentului, să populeze automat metadata referitoare la termenul de păstrare al respectivului document.

5.8.2.6 Cerințe privind lucrul colaborativ

Platforma trebuie să asigure lucrul colaborativ pe documente prin mecanism de Check-în/Check-out, cu blocarea la editare a documentului de către alți utilizatori.
Platforma trebuie să asigure controlul versiunilor pentru documente și trasabilitatea fiecărui document în parte. Vor fi stocate în sistem versiunile pentru fiecare document după realizarea modificărilor de către utilizatorii cu drepturile de acces corespunzătoare.
Platforma trebuie să asigure posibilitatea de a reveni la o versiune anterioara – „roll back”, precum și posibilitatea de comparare a versiunilor.
Platforma trebuie să asigure posibilitatea marcării versiunilor blocate la ștergere.
Platforma trebuie să asigure inclusiv păstrarea de versiuni pentru metadatele asociate documentelor.
Platforma trebuie să asigure utilizarea șabloanelor de documente și crearea de documente noi pe baza acestor șabloane.
Platforma trebuie să permită utilizatorilor să creeze alerte atât la nivel de folder cât și la nivel de document prin configurarea următorilor parametri: denumire, prioritate, dată, informații, utilizatori/grupuri de utilizatori care vor fi notificați.
Platforma trebuie să asigure instrumente de lucru pentru utilizatori, ce vor facilita comunicarea acestora prin mesaje și vor permite schimbul de fișiere, direct din interfața platformei.
Platforma trebuie să asigure utilizatorilor un cadru integrat de colaborare pe documente și fluxuri de lucru, prin posibilitatea schimbului de mesaje de colaborare pe document și păstrarea istoricului acestei corespondențe.
Pentru gestionarea informației din instituție, documentarea anumitor procese și gestionarea know-how-ului instituțional, Platforma va include următoarele funcționalități integrate de tip forum,

parametrizabile, care vor permite schimbul de informații rapid între utilizatori și va asigura trasabilitatea și transparenta:

a. Definirea de către utilizatori a unor spații de lucru de tipul: domenii sau subiecte de interes general, etc;
b. Spațiile de lucru vor fi evidențiate vizual în interfața platformei;
c. La accesarea unui spațiu de lucru, utilizatorul va putea vizualiza lista de postări;.
d. Posibilitatea ca utilizatorii să realizeze postări care să includă text, linkuri, imagini, documente;
e. Posibilitatea ca utilizatorii să posteze comentarii;
f. Posibilitatea utilizatorilor de a se abona la spațiile de lucru pentru a primi notificări cu privire la noutăți;

Platforma trebuie să permită utilizatorilor cu drepturi corespunzătoare, crearea (configurarea) unor comisii/echipe de lucru pentru un anumit document sau proiect, prin definirea utilizatorilor care vor avea posibilitatea să încarce documente și să modifice/editeze documentele distribuite.

5.8.2.7 Cerințe privind fluxurile electronice

Fluxurile de lucru pre-configurate prezentate utilizatorului vor fi cele pentru care acesta are drept de utilizare în conformitate cu rolul său în instituție.
Pentru implementarea proceselor aferente circulației documentelor, Platforma trebuie să permită utilizatorilor să creeze fluxuri ad-hoc, prin stabilirea activităților asociate (avizare, aprobare, semnare, etc.), definirea unuia sau mai multor participanți și a tranzițiilor dintre activități. La definirea unui astfel de flux se va putea stabili: tipul distribuției (secvențial sau paralel), prioritatea, participanții implicați (la nivel de utilizator sau grup), definirea de escaladări (termenul de declanșare, utilizatorul către care se escaladează). Utilizatorul va putea să salveze fluxul astfel definit (ca șablon) pentru utilizarea ulterioară.
Platforma trebuie să asigure posibilitatea monitorizării fluxurilor de lucru prin vizualizarea datelor relevante sub forma grafică (diagramă), tabelară și listă.
Platforma trebuie să asigure afișarea diagramei fluxului de lucru, cu indicarea poziției documentului în cadrul fluxului.
Platforma trebuie să asigure afișarea sarcinilor primite de utilizatori prin intermediul fluxurilor de lucru, precum și posibilitatea filtrării sarcinilor după o perioada de timp selectată de utilizator.
Platforma trebuie să asigure marcarea sarcinilor ca citite/necitite.
Platforma trebuie să asigure posibilitatea unui utilizator de a redirecționa o sarcină de lucru către un alt utilizator.
Platforma trebuie să asigure posibilitatea filtrării listei sarcinilor de lucru, în funcție de utilizatorii implicați pe flux sau starea în care se găsește fluxul de lucru: activ, finalizat, cu termen limită depășit, etc.

Platforma trebuie să asigure definirea și transmiterea alertelor și notificărilor în platformă cât și via email către utilizatorii participanți la flux, în funcție de evenimentele de pe flux (activitate nouă pe flux, apropierea unui termen limită, depășirea unui termen limită, etc). Utilizatorul va avea posibilitatea de a accesa sarcina/evenimentul direct de pe email.
Platforma trebuie să asigure posibilitatea repartizării sarcinilor între utilizatori și clasificarea acestora pe nivele de prioritate.
Platforma trebuie să asigure un mecanism de management al delegărilor pentru sarcinile asociate fluxurilor de lucru. Fiecare utilizator va putea să-și delege sarcinile către unul sau către multipli utilizatori pe o anumită perioada de timp.
Platforma trebuie să asigure escaladarea în funcție de criterii flexibil predefinite, asigurând ca minim:

a. escaladare în funcție de tipul maxim normat pentru realizarea unui pas din flux;
b. escaladare în funcție de timpul maxim normat pentru finalizarea derulării întregului flux;
c. escaladare graduală către diferitele nivele de superiori ierarhici pentru la atingerea unor praguri de întârziere predefinite.

Platforma trebuie să asigure asignarea drepturilor de acces în mod diferențiat în ceea ce privește accesarea/utilizarea fluxurilor de lucru – de exemplu, un utilizator va avea acces doar la anumiți pași de flux.
Platforma trebuie să asigure managementul fluxurilor de lucru definite și va acorda posibilitatea ca utilizatorii cu drept de acces în acest sens, să realizeze modificări asupra fluxurilor de lucru de tipul: versionări, export, creare sau ștergere șabloane de fluxuri de lucru.
Platforma trebuie să asigure posibilitatea configurării preluării în pașii de flux a documentelor și metadatelor din alte aplicații informatice.
Platforma trebuie să asigure posibilitatea configurării în pașii de flux a formularelor web (create prin intermediului designer-ului inclus în aplicație). Anumite câmpuri ale formularelor web vor fi completate automat de către aplicație, iar altele vor fi completate de utilizatori.
Platforma trebuie să permită implementarea de mecanisme de distribuire automată a sarcinilor din fluxurile de lucru către utilizatorii dintr-un grup în funcție de următoarele criterii:

a. Încărcarea utilizatorilor
b. Round robin
c. Valori ale unor indecși

Platforma trebuie să permită utilizatorilor participanți la fluxurile de lucru să întreprindă acțiuni de aprobare/respingere. În cazul respingerii, să oblige utilizatorul să motiveze respingerea.

5.8.2.8 Cerințe privind semnarea electronică a documentelor

Platforma trebuie să dispună de mecanisme de aplicare a semnăturii electronice calificate asupra documentelor.

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

Platforma trebuie să asigure posibilitatea marcării poziției de aplicare a semnăturii electronice calificate.
Platforma nu va condiționa semnarea documentelor cu semnătură electronică calificată prin mecanisme de check-out/check-in. Cu alte cuvinte, Platforma va asigura semnarea fără descărcare/încărcare pe/de pe stația de lucru a utilizatorului, a documentelor transmise pe fluxurile de lucru electronice sau stocate în depozit, și fără a fi nevoie de instalarea manuală de utilitare (programe de calculator) pe stațiile locale, în cazul clienților de tip web.
Platforma trebuie sa permită ca un document ce se afla pe flux să fie semnat multiplu cu diferite certificate calificate (emise de furnizori de servicii de încredere diferiți), de către utilizatori.

5.8.2.9 Cerințe privind transmiterea și exportul documentelor

Platforma trebuie să asigure posibilitatea utilizatorilor de a genera referințe (shortcut-uri) ale documentelor și directoarelor din depozit, pentru a facilita accesul controlat și temporar la documente ce nu pot fi transmise prin email din motive diverse (de exemplu: dimensiune prea mare).
Utilizatorii vor putea transmite referințele (shortcut-urile) documentelor și directoarelor din depozit, prin email sau prin alte mijloace de comunicare electronică, direct din interfața de acces a platformei.
Referințele (shortcut-urile) generate de utilizatori pentru documentele și directoarele din depozit, vor putea fi configurate de către aceștia pentru a se limita la un număr de descărcări sau pentru o anumită perioadă de valabilitate.
Platforma trebuie să asigure posibilitatea exportului documentelor dintr-un folder, direct din interfața platformei, în format zip cu posibilitatea configurarea următorilor parametri: intervalul de timp în care au fost încărcate documentele, tipurile de documente, export structura directoare cu documente, export doar documente, export doar structura de directoare, directoare fără documente, versiuni documente, lista metadate.
Platforma trebuie să permită utilizatorilor exportul unei colecții de documente din depozit, împreună cu toate atributele lor sau doar o parte din acestea, pentru a fi puse la dispoziția unei entități terțe, prin care aceasta, direct dintr-un browser web, fără a fi nevoie de instalarea de programe de calculator de tip utilitar sau plug-in, să poată:

a. Vizualiza organizarea documentelor în structura de directoare stabilită la configurarea exportului;
b. Previzualiza documentele direct din browser;
c. Căuta documente după cuvinte din denumirea fișierului;
d. Descărca documentele.

5.8.2.10 Cerințe privind protecția datelor cu caracter personal

Din punct de vedere al alinierii și respectării cerințelor referitoare la protecția datelor cu caracter personal, Platforma va asigura îndeplinirea următoarelor cerințe minimale:

a. Să permită definirea și utilizarea de metadate dedicate pentru datele cu caracter personal, prin intermediul cărora să se marcheze existența datelor cu caracter personal în documente;
b. Să pună la dispoziție o funcție automatizată de export pentru documente și metadate asociate, care să permită exportul datelor cu caracter personal în forma mascată, cu excepția fișierelor de tip imagine (pentru care este necesară prelucrarea manuală);
c. Să permită căutarea și filtrarea datelor cu caracter personal;
d. Să pună la dispoziție un tablou de bord centralizat pentru managementul datelor relevante din punct de vedere GDPR;

Platforma trebuie să dispună de un mecanism de clasificare a datelor cu caracter personal cu următoarele funcționalități:

a. identificarea automată a datelor cu caracter personal (CNP, e-mail) în documentele încărcate în depozit și marcarea acestora printr-o metadată ce evidențiază un document ce conține date cu caracter personal;
b. evidențierea vizuală automată a denumirii documentelor care conțin date cu caracter personal.

5.8.2.11 Cerințe privind raportarea

Platforma trebuie să includă funcționalități integrate de raportare sub formă de tablouri de bord agregate, pentru a oferi o imagine clară a performanței proceselor derulate în cadrul instituției. Modulul de raportare va îndeplini cel puțin următoarele funcționalități:
Platforma trebuie să permită vizualizări diferite ale datelor, prezentându-le în formă grafică (bar charts, line graphs și pie charts, etc), ușor de construit pe baza instrumentelor disponibile.
Platforma trebuie să permită agregarea rapidă și ușoară a datelor pentru a crea și a combina vizualizări combinate cât și statistici pe datele din sistem.Platforma trebuie să permită filtrarea rapidă din interfața grafică a datelor reprezentate pentru interpretarea rapidă a datelor relevante.
Platforma trebuie să permită salvarea acestor vizualizări pentru refolosire ulterioară cât și popularea automată și dinamică a acestor vizualizări pe măsură ce noi date apar în aplicație.
Platforma trebuie să permită utilizatorilor să creeze propriile rapoarte, fără scriere de cod, în care să utilizeze seriile de date puse la dispoziție de aplicație. În acest sens. Utilizatorii trebuie să poată să creeze formule, totaluri sumarizatoare, să afișeze informațiile analizate în diverse formate.
Rapoartele vor putea fi generate pe intervale de timp definite și pe utilizator.
Platforma trebuie să permită parametrizarea rapoartelor prin posibilitatea de adăugare a unor filtre

suplimentare pentru afișarea datelor de interes.
Platforma trebuie să permită afișarea numărului de documente dintr-un depozit prin punerea la dispoziție a unor rapoarte predefinite care să afișeze cel puțin următoarele:

a. numărul de documente dintr-un depozit;
b. numărul de documente dintr-un depozit per utilizator;
c. numărul de documente încărcate întrun depozit pe un anumit interval de timp;
d. numărul de documente încărcate întrun depozit de un utilizator pe un anumit interval de timp.

5.8.2.12 Cerințe privind interoperabilitatea

Depozitele de documente electronice din cadrul platformei de managementul documentelor vor constitui arhiva electronică operațională (mediul de activitate curentă al CNCD), în care vor fi stocate temporar documentele electronice ale CNCD, până când acestea vor fi supuse operațiunilor de prelucrare arhivistică reglementate prin Legea Arhivelor Naționale nr. 16/1996, cu modificările și completările ulterioare, respectiv vor fi transferate întrun depozit de arhivă electronică al unui furnizor acreditat de servicii de arhivare electronică.
Pentru cazul în care CNCD decide să contracteze printr-o procedură de achiziție distinctă, astfel de servicii de arhivare electronică furnizate de un terț acreditat conform OMCID nr. 20717/2024, soluția propusă trebuie să asigure următoarele funcționalități:

a. Trebuie să dispună de capabilități de interfațare prin servicii web de tip REST API cu sistemul informatic al prestatorului de servicii de arhivare electronică legală, în vederea transmiterii documentelor electronice care trebuie arhivate, fără ca implementarea serviciilor web să necesite scrierea de cod;
b. Să permită utilizatorilor autorizați să selecteze unul sau mai multe documente din depozitul Platformei software de managementul documentelor și să le transmită către sistemul informatic al prestatorului de servicii de arhivare electronică legală, printr-o simplă comandă disponibilă în interfață;
c. Înainte de apelarea serviciilor web pentru transferul documentelor către sistemul informatic al prestatorului de servicii de arhivare electronică legală, Platforma software de managementul documentelor trebuie să verifice dacă documentele selectate sunt semnate electronic cu semnătură calificată și să semnaleze utilizatorului, în interfață dacă este cazul;
d. Odată cu fișierele asociate documentelor, Platforma software de managementul documentelor va transmite și metadatele obligatorii conform Legii 135/2007 privind arhivarea documentelor în formă electronică, cu modificările și completările ulterioare, respectiv:
    i. proprietarul documentului în formă electronică;

ii. emitentul documentului în formă electronică;
iii. titularul dreptului de dispoziție asupra documentului;
iv. data emiterii documentului;
v. tipul documentului în formă electronică;
vi. nivelul de clasificare a documentului în formă electronică;
vii. cuvintele-cheie necesare identificării documentului în formă electronică;
viii. termenul de păstrare a documentului (poate fi relativ calculat la o metadata/cuvant-cheie)

Platforma software de managementul documentelor trebuie să permită integrarea cu Microsoft Teams, punând la dispoziție funcționalități de lucru cu documentele direct din MS Teams precum: creare folder documente, încărcare documente, încărcare de versiuni, pornire de fluxuri de lucru, căutare, ștergere intrare, vizualizare fișiere existente în arhiva etc.

Platforma trebuie sa pună la dispoziție un serviciu Web de tip REST API care să permită autentificarea pe baza de nume_utilizator și parola și care în urma autentificării să genereze un token/ticket care să se utilizeze la apelarea altor servicii web; perioada de valabilitate a tichetelor trebuie să fie configurabilă de către un administrator.

Toate serviciile web sa se poată apela doar pe baza de autentificare.

Platforma trebuie să pună la dispoziție un serviciu web care să permită încărcarea unui document în depozit, folosind standardul multipart/form-data și completarea metadatelor aferente acestuia și asocierea unui context de securitate (grup/utilizator).

Platforma trebuie să pună la dispoziție un serviciu web care să permită generarea de numere de înregistrare din toate registrele configurate.

Platforma trebuie să pună la dispoziție un serviciu web care să permită căutarea full text (în conținut), returnând o listă de documente care corespund parametrilor de căutare împreună cu metadatele acestora.

Platforma trebuie să pună la dispoziție un serviciu web care să permită căutarea la nivel de metadate, returnând o listă de documente care corespund parametrilor de căutare împreuna cu metadatele acestora.

Platforma trebuie să pună la dispoziție un serviciu web care să permită actualizarea metadatelor unui document aflat in depozit.

Platforma trebuie să pună la dispoziție un serviciu web care să permită încărcarea unei noi versiuni a unui document.

Platforma trebuie să pună la dispoziție un serviciu web care să permită afișarea metadatelor unui document.

Platforma trebuie sa pună la dispoziție un serviciu web care sa permită afișarea tuturor versiunilor unui document.

Platforma trebuie să pună la dispoziție un serviciu web care să permită afișarea tuturor documentelor dintr-un folder.

Platforma trebuie să pună la dispoziție un serviciu web care să permită descărcarea unui document

din depozit, prin specificarea identificatorului unic.
Platforma trebuie să pună la dispoziție un serviciu web care să permită modificarea drepturilor unui document.
Toate serviciile web puse la dispoziție trebuie să se poată testa dintr-o interfața prietenoasa și trebuie sa respecte standardul OpenAPI 3.
Platforma trebuie să asigure integrarea cu soluțiile Microsoft Office utilizate de beneficiar, oferind facilități de salvare în depozit direct din editorul de texte.
Platforma trebuie să fie integrată cu soluțiile Microsoft Office astfel încât pentru documente editabile de tip Microsoft Word va fi permisă editarea în paralel, fiecare utilizator putând vizualiza în timp real modificările efectuate de alți utilizatori.
Platforma trebuie să fie integrată cu soluțiile Microsoft Outlook, astfel încât să asigure, direct din aplicația de mesagerie electronică Outlook, să încarce documente în depozit (prin salvare) și să completeze metadatele acestora.
Platforma trebuie să permită integrarea cu soluții de management al utilizatorilor prin LDAP, astfel încât utilizatorii să nu necesite un set de credențiale dedicat, iar accesul să se facă pe baza drepturilor de acces la infrastructura instituției, așa cum e aceasta definită în LDAP.

5.8.2.13 Cerințe privind administrarea și configurarea

Platforma trebuie să permită vizualizarea tuturor utilizatorilor conectați și permite deconectarea unui anumit utilizator.
Platforma trebuie să permită configurarea perioadei de inactivitate a utilizatorilor în vederea deconectării automate a acestora.
Platforma trebuie să permită configurarea politicii de parole, referitor la:

a. complexitatea parolei (trebuie să se poată utiliza minim opțiunile : majuscule, litere mici, un număr minim de caractere al parolei);
b. schimbarea forțată a parolei la următoarea logare în sistem;
c. permite definirea politicilor de parolare pentru utilizatori individuali, pentru grupuri, la nivel global din interfața de administrare;
d. schimbarea forțată a parolei la data menționată;
e. schimbarea parolei cu solicitarea de modificare a acesteia – cu opțiunea utilizatorului de a refuza acest lucru și să continue logarea cu parola originală, situație în care cererea de modificare va fi afișată la fiecare încercare noua de logare în sistem, până la modificarea acesteia.

Platforma trebuie să permită configurarea mecanismelor de securitate bazate pe grupuri, roluri, utilizatori și funcții din organigramă. Drepturile de securitate și permisiunile vor fi special proiectate astfel încât să permită controlarea accesului utilizatorilor la documente și tipul drepturilor de acces.
Platforma trebuie să permită organizarea utilizatorilor în grupuri. Un utilizator poate face parte din

unul sau mai multe grupuri. Permisiunile de securitate și drepturi de acces se vor putea asocia cu grupurile de utilizatori (aplicându-se tuturor utilizatorilor membri la momentul controlului accesului).
Platforma trebuie să permită definirea și administrarea drepturilor multiple de acces în cadrul soluției, adăugarea utilizatorilor noi și gruparea/alocarea acestora în grupuri predefinite și moștenirea de drepturi.
Platforma trebuie să permită definirea drepturilor de acces pe tipurile de fluxuri de lucru pe care un utilizator le va avea disponibile. La nivelul fiecărei activități din flux se vor putea defini drepturi pentru cine va avea acces la acea activitate și drepturi referitoare la acțiunile care se vor putea desfășura de către utilizator.
Platforma trebuie să permită posibilitatea de asociere de drepturi în mod granular, pe diferite nivele (directoare, documente, tipuri de documente, atribute ale documentelor, grad clasificare, etc), până la nivel de obiect și câmp index.
Platforma trebuie să permită administratorului să definească și să întrețină un set general de atribute la nivelul organizației din care să se poată selecta ce atribute să apară pe fiecare tip de document.
Platforma trebuie să permită administratorului să definească mai multe depozite de documente, ce pot fi utilizate în același timp. Fiecare depozit de documente va avea propriile date primare (utilizatori, grupuri de utilizatori, parole, formulare, liste de valori), cât și tranzacționale (foldere, drepturi, restricții aferente obiectelor, informații ierarhice, referințe logice, documente, activități).
Platforma trebuie să includă un designer dedicat pentru definirea formularelor electronice pentru unele tipuri de documente gestionate, care să fie utilizate ca șabloane de documente.
Designerul de formulare electronice va asigura cel puțin:

a. crearea de formulare dinamice de tip responsiv și interactive;
b. crearea de formulare cu tab-uri și metadate dinamice cu afișare de metadate în funcție de condiționalități;
c. completarea automată a anumitor câmpuri;
d. includerea pe câmpuri a unor formule de calcul;
e. Posibilitatea definirii a câmpurilor de tip: dată, text, casetă de verificare, semnături, imagine, link, de tip buton pentru adăugarea sau ștergerea liniilor;
f. introducerea de reguli și validări pe câmpurile formularului;
g. preluarea de date din surse externe de informație, cum sunt alte sisteme software sau baze de date externe;
h. definirea modului de vizualizare în funcție de echipament: desktop, telefon, tableta.

Platforma trebuie să asigure definirea și utilizarea de nomenclatoare de documente.
Platforma trebuie să asigure jurnalizarea tuturor operațiilor, evenimentelor și acțiunilor desfășurate în aplicație. Aceste informații vor putea fi accesate de administratorul de sistem prin intermediul rapoartelor de audit.
Platforma trebuie să includă un designer de fluxuri care să permită utilizatorilor cu rol de administrator definirea vizuală, direct în aplicație a fluxurilor de lucru aplicabile documentelor.

Designerul de fluxuri va pune la dispoziție cel puțin următoarele instrumente predefinite prin care să se realizeze configurarea pașilor fluxurilor de lucru prin metoda drag-and-drop: nod de tip start, nod de tip end, activitate, conectori, porți logice (noduri de decizie), porți paralele (noduri de distribuție și respectiv noduri de colectare);
Platforma trebuie să dispună de mecanisme de administrare a fluxurilor electronice de lucru dintr-o interfață grafică, precum acțiuni de definire, configurare, activare, dezactivare butoane de acțiuni, organizare dinamica a secțiunilor din interfață, profile de vizualizare/colecții de teme, posibilitatea de asociere a activităților către utilizatori și roluri din organizație.
Platforma trebuie să permită modificarea fluxurilor de lucru predefinite prin intermediul designerului grafic, prin operații de drag and drop și asignare de relații. Modificarea nu trebuie să presupună scriere de cod.
Platforma trebuie să permită configurarea fluxurilor de lucru atât prin intermediul designerului grafic, cât și prin dezvoltarea de scripturi pentru realizarea unor automatizări suplimentare sau implementarea regulilor de proces specifice instituției.
Platforma trebuie să permită administratorului să configureze funcțiile, a serviciile și meniurile platformei în conformitate cu rolul, apartenența la grupuri și drepturile utilizatorului. Parametrizările se vor realiza fără a fi necesara dezvoltarea de cod;
Platforma trebuie să permită administratorului să configureze locațiile de stocare a documentelor, a tipurilor de obiecte, precum și definirea și gestionarea profilurilor de backup ale sistemului, vizualizarea și editarea fișierelor de configurare, instalarea și managementul modulelor soluției, etc;
Platforma trebuie să permită administratorului să configureze să monitorizeze toate operațiile și evenimentele realizate în sistem, cu evidențierea de date relevante și posibilitatea de a exporta rapoartele de audit;
Platforma trebuie să permită administratorului să configureze să configureze reguli pentru migrarea automată a conținutului pentru optimizarea stocării, păstrând accesibilitatea și nevoile de conformitate în decursul timpului;
Platforma trebuie să permită administratorului să configureze să configureze mecanismele pentru asigurarea continuității activității în caz de dezastru, prin care să asigure:

i. Sincronizarea bidirecțională a două sau mai multe depozite de documente atât în ceea ce privește datele primare (utilizatori, grupuri de utilizatori, parole, formulare, liste de valori), cât și a celor tranzacționale (foldere, drepturi, restricții aferente obiectelor, informații ierarhice, referințe logice, documente, activități);
ii. Sincronizarea totală sau parțială a unor părți din depozit;

Platforma trebuie să permită administratorului să configureze integrarea cu soluții de management a utilizatorilor și accesului;
Platforma trebuie să permită administratorului să configureze noi registre electronice și totodată să definească drepturile de editare/vizualizare pentru acestea la nivel de rol sau de utilizator;
Platforma trebuie să permită administratorului să definească tipurile de documente;
Platforma trebuie să permită administratorului să asigure personalizarea interfeței de utilizare în

funcție de rolul utilizatorilor, permițând astfel o standardizare a prezentării funcționalităților disponibile;
Platforma trebuie să permită administratorului să definească chei de criptare prin intermediul interfeței de administrare și să configureze utilizarea de chei de criptare diferite pentru diferite tipuri de documente și/sau pentru diferite depozite de documente;
Platforma trebuie să permită administratorului să configureze joburi pentru exportul automat de documente din depozit către un spațiu de stocare, în vederea salvării copiilor de siguranță ale documentelor;
Platforma trebuie să permită administratorului să creeze filtre de căutare care să se aplice fluxurilor de lucru în funcție de:

a. Starea fluxurilor de lucru: active, finalizate, toate fluxurile, fluxurile cu termen depășit
b. Utilizatorii implicați pe fluxurile de lucru: inițiatori, prezenți pe pașii de flux, prezenți pe pașii încă activi
c. Data de start, intervalul de timp

Platforma trebuie să permită administratorului să creeze formulare electronice printr-un un designer de formulare electronice.
Designer-ul de formulare electronice va permite adăugarea următoarelor tipuri de câmpuri/atribute specifice:

a. Câmpuri de introducere informații (string, numeric, etc)
b. Câmpuri de tip dată
c. Câmpuri de tip text
d. Câmpuri de tip area text
e. Câmpuri de tip check-box
f. Câmpuri de tip radio button
g. Câmpuri de tip combo box
h. Câmpuri de tip semnătură
i. Câmpuri de tip buton, inclusiv adăugare linie sau ștergere linie
j. Câmpuri de tip imagine
k. Câmpuri de tip link

Designer-ul de formulare electronice va permite configurarea parametrilor câmpurilor
Designer-ul de formulare electronice va permite introducerea unor reguli de validare cu privire la numărul de caractere din fiecare câmp
Designer-ul de formulare electronice va permite preluarea de date din surse externe de informație (sisteme software, baze de date externe, etc)
Designer-ul de formulare electronice va permite completarea automată a anumitor câmpuri,
Designer-ul de formulare electronice va permite implementarea formule de calcul,
Designer-ul de formulare electronice va permite posibilitatea de adăugare sau ștergere de câmpuri din formulare,
Designer-ul de formulare electronice va permite utilizarea de script-uri pentru implementarea

diverselor automatizări,
Designer-ul de formulare electronice va permite implementarea de liste de valori dinamice
Platforma trebuie să permită administratorului să expună formulare electronice în exteriorul platformei prin intermediul API;
Platforma trebuie să permită administratorului să configureze reguli pentru migrarea automată a conținutului pentru optimizarea stocării, păstrând accesibilitatea și nevoile de conformitate în decursul timpului;

5.8.2.14 Cerințe privind arhitectura și performanța

În vederea eliminării riscului de creștere a dimensiunii sistemului de gestiune a bazelor de date relaționale și creșterea timpului de răspuns, documentele vor fi păstrate independent de sistemul de gestiune a bazelor de date relaționale. În sistemul de gestiune a bazelor de date relaționale se vor păstra doar legăturile către fișierele din depozit, alături de metadatele acestora.
Platforma trebuie să permită funcționarea cu cel puțin trei din următoarele sisteme de gestiune a bazelor de date relaționale: MySQL, PostgreSQL, Oracle și Microsoft SQL.
Platforma trebuie să permită funcționarea pe cel puțin două sisteme de operare server diferite (Windows și Linux), fără degradarea performanțelor sau limitarea funcționalităților solicitate prin prezentul caiet de sarcini.
Platforma va fi implementată astfel încât să asigure următorii parametri de performanță și încărcare
- Timpul mediu de răspuns pentru 125 de utilizatori standard concomitenți nu va depăși:
    a. 3 secunde pentru încărcarea unei pagini web, corespunzătoare unor operații standard;
    b. 3 secunde pentru returnarea unei liste cu 1000 de obiecte (documente) la căutarea în depozit la nivel de indecși;
    c. 3 sec pentru rapoartele rulate pe 5000 de obiecte (documente)

Platforma software de managementul documentelor se va implementa printr-o arhitectură bazată pe servicii, care să asigure o disponibilitate de 99,96 % pentru mediul de producție pentru serviciile aplicative oferite utilizatorilor, în condițiile de performanță și încărcare solicitate mai sus, printr-o combinație de mecanisme care să includă:

a. Gruparea serviciilor aplicative nucleu, din punct de vedere logic și funcțional pe mai multe servere de aplicații (instanțe virtualizate) care să îndeplinească roluri diferite;
b. Clusterizare la nivelul serverelor de aplicații și a celor de baze de date
c. Componentizarea/modularizarea soluției prin descompunerea în microservicii și instalarea în containere sau mașini virtuale, asigurându-se astfel scalabilitatea și portabilitatea soluției. Containerele vor putea fi agregate întro platformă de orchestrare ce facilitează automatizarea și crearea de configurații declarative (de ex. Kubernetes etc.).

La definirea arhitecturii soluției se va lua în considerare necesitatea configurării următoarelor medii:

a. Mediul de producție: asigură funcționarea în producție a soluției informatice și reprezintă

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

mediul care va fi utilizat efectiv de întreg personalul instituției;

b. Mediul de testare – dezvoltare, va fi utilizat pentru:
   - dezvoltarea de module/funcționalități noi;
   - dezvoltarea de modificări ce vor fi aduse mediului principal de producție;
   - testarea și validarea modificărilor, înaintea promovării acestora pe mediul de producție;
   - validarea integrării cu diverse aplicații și sisteme informatice.

c. Mediul de recuperare în caz de dezastru – asigură stocarea copiilor de siguranță a mașinilor virtuale, bazei de date și depozitelor de documente din centrul de date principal.

Mediul de producție și cel de testare-dezvoltare vor fi găzduite în centrul de date principal.

Pe parcursul implementării se vor elabora proceduri/procese dedicate atât pentru migrarea dezvoltărilor (testate și acceptate) de pe mediul de dezvoltare/testare pe mediul de producție cât și de pe mediul de producție pe mediul de dezvoltare/testare.

5.8.3. Software de gestiune a bazelor de date relaționale

Software-ul de Gestiune a Bazelor de date Relaționale trebuie să asigure necesarul de persistență operațională pentru aplicațiile din cadrul SIISPECD (Portal de servicii de electronice publice și platforma de managementul documentelor), prin satisfacerea cerințelor descrise în acest capitol.

Software-ul de Gestiune a Bazelor de date Relaționale trebuie să fie un sistem de gestiune a bazelor de date de tip relațional.

Software-ul de Gestiune a Bazelor de date Relaționale trebuie să aibă posibilitatea rulării pe arhitecturi cu procesoare pe 64 biți.

Software-ul de Gestiune a Bazelor de date Relaționale trebuie să permită instalarea bazei de date pe mai multe noduri (arhitectură de tip cluster) pentru a asigura toleranța la căderi de noduri, fără a necesita achiziția de componente adiționale.

Software-ul de Gestiune a Bazelor de date Relaționale trebuie să aibă posibilitatea definirii de indecși pentru accesarea rapidă a datelor.

Software-ul de Gestiune a Bazelor de date Relaționale trebuie să ofere posibilitatea de a face salvare și restaurare automate de date.

Software-ul de Gestiune a Bazelor de date Relaționale trebuie să includă capabilități de căutare complexă la nivel de text, folosind indecși specializați și efectuarea rapidă a căutărilor în acest tip de date.

Software-ul de Gestiune a Bazelor de date Relaționale trebuie să permită în mod nativ stocarea și gestiunea de structuri de date de tip XML.

Software-ul de Gestiune a Bazelor de date Relaționale trebuie să ofere suport pentru proceduri stocate și triggeri.

Software-ul de Gestiune a Bazelor de date Relaționale trebuie să ofere suport pentru tranzacții.

Software-ul de Gestiune a Bazelor de date Relaționale trebuie să permită execuția operațiilor de tip

SELECT, INSERT, UPDATE, DELETE.
Software-ul de Gestiune a Bazelor de date Relaționale trebuie să permită definirea de tabele de tip index sau indecși de tip „cluster” pentru acces rapid la anumite tabele.
Software-ul de Gestiune a Bazelor de date Relaționale trebuie să ofere suport pentru replicarea datelor între două instanțe ale bazei de date.
Software-ul de Gestiune a Bazelor de date Relaționale trebuie să permită restricționarea accesului la nivelul obiectelor bazei de date.
Software-ul de Gestiune a Bazelor de date Relaționale trebuie să ofere mecanisme native de restricționare a accesului utilizatorilor.
Software-ul de Gestiune a Bazelor de date Relaționale trebuie să permită efectuarea de backup automat întro formă unitară, centralizată și ușor de administrat.
Software-ul de Gestiune a Bazelor de date Relaționale trebuie să permită instalarea bazei de date pe mai multe noduri (arhitectură de tip cluster) pentru a asigura toleranța la defecte hardware sau nefuncționare planificată și disponibilitatea crescută a sistemului. Bazele de date ale SIISPECD (atât pentru aplicațiile din DMZ, cât și pentru cele din zona privată) vor fi configurate în regim de înaltă disponibilitate.
Software-ul de Gestiune a Bazelor de date Relaționale trebuie să ofere securitate tranzacțională în cazul apariției unor erori hardware sau software în clusterul de bază de date.
Software-ul de Gestiune a Bazelor de date Relaționale trebuie să ofere suport nativ pentru setul de caractere pe mai mulți octeți – în special: UTF-8.
Soluția propusă va fi licențiată astfel încât nodurile active din cluster să totalizeze cel puțin 16 nuclee de procesare.
Produsul va beneficia de suport tehnic pe o perioadă de 5 (cinci) ani, acoperind dreptul beneficiarului de a face update–uri precum și access direct la site-ul producătorului pentru a deschide direct cazuri de suport cu acesta.

5.8.4. Platforma software de videoconferință

SIISECD va include o platformă software de videoconferință care va permite comunicarea la distanță între funcționarii CNCD și petenți/reclamați în cadrul procesului de constatare și sancționare a faptelor de discriminare
Se solicită implementarea unei soluții mature care să asigure funcționarea simultană pentru minim 5 de participanți concurenți, rezoluție HD.
Soluția propusă trebuie sa dispună de un design de natura moderna si sa aiba un plan de dezvoltare bine conturat cel putin pe termen mediu.
Soluția trebuie sa respecte standardele din domeniul securitatii referitoare la ciclul de dezvoltare si sa respecte practicile internationale referitoare la scrierea codului pentru a asigura securitate si acces la informatii si care sa respecte in mod strict cerintele de confidentialitatea si integritatea datelor.
Beneficiarul va deține controlul deplin asupra locatiilor de implementare pentru a se conforma cu ușurință oricăror cerinte regionale de stocare și tranzit de date, păstrând astfel controlul deplin

asupra tuturor înregistrărilor cu detaliile apelurilor (CDR), iar detaliile și modelele întâlnirilor nu sunt niciodată expuse tertilor.
Soluția trebuie sa ofere support pentru o gama larga de codecuri audio, de la G711 – narrow band pana la codecuri moderne de voce HD de cel putin 17khz – G722, Opus, Silk etc
Codurile video suportate trebuie sa acopere, pentru interoperabilitate, cel putin H.261, H.263 si H.264, VP8 si VP9 pentru comunicatia WebRTC
Soluția va asigura compatibilitate cu producatorii majori de sisteme de videoconferinta SIP si H.323, integrare cu sisteme de telefonie PSTN/IP PBX precum si terminale de voce.
Produsul va oferi interoperabilitate pentru cel putin urmatorii producatori de sisteme de videoconferinta: Cisco, Poly, Avaya, Yealink respectiv urmatoarele servicii cloud si/sau self-hosted: Webex, Zoom (cu CRC), Poly, BlueJeans, Pexip, Lifesize, Skype for Business, TEAMS, Google Meet.
Soluția trebuie integrată cu echipamentul pentru înregistrarea conferințelor (a se vedea cap. 5.7.8.13) precum si posibilitatea de live streaming. Soluția va asigura integrarea cu protocolul RTMP pentru recording precum si streaming catre minim client iOS, Android, Windows 10+, Linux si Mac folosind doar un browser web (Chrome, Edge, Firefox, Safari)
Serverul de recording va oferi si un portal in care inregistrarile videoconferintelor vor putea fi redate în baza RBAC oferite de integrare LDAP.
Soluția va suporta minim urmatoarele rezolutii: SD, HD 720p30 and Full HD 1080p30.
În cazul în care calitatea retelei fluctuează, soluția va oferi protocoale automate pentru reducerea vitezei apelului si implicit a nivelului de pachete pierdute.
Soluția va oferi optiuni de aranjare a participantilor pe ecran atat in mod static cat si in mod automat, cu optiuni inteligente de a promova vorbitorii activi in ferestre mai mari, detectarea faciala automata și zoom automat (framing) pe vorbitor/grupuri de personae.
Soluția va detecta de asemenea fluxurile video cu camera inchisa (privacy shutter) sau unde nu exista persoane in campul vizual al camerei si le vor elimina din layoutul prezentat celorlalti participanti – in acelasi timp va oferi informatii vizuale tuturor participantilor video cate persoane se afla in conferinta in total, cate sunt pe telefon precum si cate persoane au camera inchisa.
Pentru soluțiile cu terminale cu 2 ecrane, in timpul in care nu este partajat continut, Soluția va utiliza si al doilea ecran pentru a putea vizualiza participanti.
Soluția va oferi o interfata REST API atat client cat si server ce vor permite integrarea cu sisteme de management ce pot configura si obtine un status al funtionarii platformei in timp real
În contextul actual al creșterii exponențiale a atacurilor de cybersecuritate, soluțiile de securizare a unei camere de conferinta prin PIN si/sau un link generat aleatoriu trebuie augmentate cu mijloace suplimentare, cum ar fi:

- Restricționare access pe baza adresei IP sursa a sistemului/gateway-ului de audio/video
- Prin acces in conferinta pe baza autentificarii fiecarui participant prin SSO folosind SAML2.0 sau OpenID Connect (ADFS, Entra ID, Okta...) – in acest caz se poate folosi aditional si MFA cu SMS/Authenticator

- Prin PIN dinamic aleator generat si trimis prin SMS la momentul în care utilizatorul intra in conferință

Pentru auditarea accesului administrativ in Soluția de videoconferinta, se vor folosi standarde de jurnalizare, de exemplu syslog pe o instanta externa. In mod similar, accesul in videoconferinte va fi jurnalizat.

Pentru analiza calitativa si proactivitate in descoperirea eventualelor nefunctionalitati, platforma trebuie sa inregistreze si

1. evenimente de calitate a apelului (rezolutie sub-optima, pachete pierdute)
2. cauze anormale de deconectare pe parte de:
   - participanti, cum ar fi procente peste 20% de pachete pierdute sau deconectari provocate de sisteme firewall remote – TTL TCP expirat)
   - infrastructura de conferinta, cum ar fi conexiune intre servere pierduta, restart neprogramat partial al unui server/unor servere, servicii defectuoase, limita capacitate atinsa, lipsa resurse hardware etc
3. evenimente de brute-force PIN sau destinatie de videoconferinta (friendly scanners) si platforma va bloca automat sursele acestor anomalii. Pentru protectia utilizatorilor interni (sursa IP) se va oferi totusi posibilitatea de whitelisting (false positives)

Pentru a asigura o comunicare cat mai facila si lipsita de stress, platforma de videoconferinta trebuie sa ofere si urmatoarele posibilitati/functii:

1. interfata web catre participantii in conferinta trebuie sa fie editabila cu mesaje audio (IVR), text (mesaje vizuale scrise) precum si culori/logo-uri, imagini de fundal
2. sa ofere participantilor la conferinta functii de "testare" in prealabil a calitatii conexiunii precum si testarea camerei web, microfonului si a difuzoarelor (casti)

Soluția software de videoconferință va rula pe infrastructura furnizorului și va fi oferită ca serviciu pe o perioadă de 60 de luni.

5.8.5. Platforma software de transcriere audio în text

Platforma software de transcriere audio în text va asigura transcrierea, în timp real, a audierilor în cadrul CNCD.

Platforma trebuie să permită flexibil extragerea automată a textului din fișiere audio/video de formate diverse, asigurându-se ca minim compatibilitate pentru următoarele formate: aac, aiff, asf, avi, flac, flv, mpeg, mp3, mp4, m4a, mkv, ts, webm.

Platforma trebuie să permită transcrierea audierilor în text din limba română cu un randament superior sau egal valorii de 95% când înregistrarea este de calitate similară transmisiunilor media radio/tv. Notă: Prin calitate similară transmisiunilor media radio/tv se înțelege o înregistrare audio-video de tipul celei care se poate regăsi la https://www.romania-actualitati.ro/live/.

Platforma trebuie să dispună de caracteristici adaptive care să permită transcrierea audierilor în transmisiuni realizate în condiții care nu sunt ideale (de exemplu microfoane puțin performante, înregistrări din conferințe online, vorbitori aflați la distanță de microfon, discursuri realizate în

încăperi cu ecou etc.) precum și în medii zgomotoase, cum ar fi de exemplu înregistrări cu zgomote de bruiaj.
Platforma trebuie să permită exportul textului în formate flexibile, asigurându-se minim formatele: srt, pdf, docx, txt.
Platforma va asigura editor text cu sincronizare între audio și text, ceea ce înseamnă că în momentul în care se apasă pe un cuvânt din transcript se dă play automat în audio/video în momentul de timp în care a fost spus acel cuvânt;
Platforma trebuie sa dispună de un vocabular de minim 20.000 cuvinte pentru limba română.
Platforma va permite adăugarea de cuvinte noi.
Platforma trebuie să dispună atât de un model acustic cât și de un model lingvistic. Platforma va dispune de posibilitatea de îmbunătățire a algoritmului de recunoaștere vocală pe un anumit domeniu specific, care să poată fi făcută în două moduri: fie prin introducere de înregistrări audio ale cuvintelor specifice domeniului sau prin introducerea unui vocabular text personalizat domeniului.
Platforma software de transcriere audio în text, va fi oferită ca serviciu și se va instala pe Cloud-ul Privat Guvernamental - componenta de Cloud Dedicat bazat pe tehnologia Azure Hub Stack sau va fi găzduită întrun centru de date localizat în Uniunea Europeană, pentru asigurarea respectării cerințelor privind protecția datelor cu caracter personal.
Platforma trebuie să permită integrarea cu alte aplicații folosind servicii de tip REST API
Se vor asigura minim 50 de ore de transcriere pe lună, pentru o durată de minim 60 de luni. Orele de transcriere ne-consumate în cadrul unei luni se vor reporta, putând fi consumate oricând până la sfârșitul perioadei contractate.

5.9. Cerințe privind serviciile

5.9.1. Livrarea, instalarea și configurarea echipamentelor

Livrarea, instalarea și configurarea echipamentelor se va realiza în termenul prevăzut conform ”Planului de livrare produse și prestări servicii” întocmit pe baza prevederilor din capitolul 10.1 al prezentului document.
Produsele vor fi livrate cantitativ și calitativ la locul indicat de Achizitor pentru fiecare produs în parte. Fiecare produs va fi însoțit de toate subansamblele/ părțile componente necesare punerii și menținerii în funcțiune.
Contractantul va ambala și eticheta produsele furnizate astfel încât să prevină orice daună sau deteriorare în timpul transportului acestora către destinația stabilită.
Ambalajul trebuie prevăzut astfel încât să reziste, fără limitare, manipulării accidentale, expunerii la temperaturi extreme, sării și precipitațiilor din timpul transportului și depozitării în locuri deschise. În stabilirea mărimii și greutății ambalajului Contractantul va lua în considerare, acolo unde este cazul, distanta față de destinația finală a produselor furnizate și eventuala absență a facilităților de manipulare la punctele de tranzitare.
Transportul și toate costurile asociate sunt în sarcina exclusivă a Contractantului. Produsele vor fi

asigurate împotriva pierderii sau deteriorării intervenite pe parcursul transportului și cauzate de orice factor extern.
Contractantul, în condițiile legii, va prezenta, la livrare, următoarele:

- documentele de însoțire a mărfii (aviz de însoțire a mărfii/aviz de expediție etc.)
- documentația tehnică
- certificat de garanție;

Contractantul este responsabil pentru livrarea în termenul solicitat și se consideră că a luat în considerare toate dificultățile pe care le-ar putea întâmpina în acest sens și nu va invoca nici un motiv de întârziere sau costuri suplimentare.
Furnizorul este responsabil de instalarea și punerea în funcțiune a echipamentelor, precum și pentru asigurarea suportului tehnic în perioada de garanție și orice alte asemenea obligații care revin.
Furnizorului prin contract. Instalarea și punerea în funcțiune va cuprinde cel puțin următoarele operațiuni:

- instalare fizică a echipamentelor în rack;
- instalare componente hardware și software necesare infrastructurii IT;
- realizare conexiuni date echipamente;
- configurare console management și update firmware la ultima versiune;
- configurare transport VLAN-uri la nivelul switch-uri LAN;
- configurare echipamente de stocare
- instalare și configurare soluție virtualizare;
- instalare soluție de backup și configurare job-uri backup și replicare;
- instalare platforme administrare centralizată;
- instalare și configurare echipamente WAN, switch-uri LAN și AP-uri în CNCD și unitățile subordonate;

Toate cheltuielile legate de activitățile echipelor de instalare vor fi suportate integral de Furnizor.
Furnizorul va include toate elementele de conectică necesare instalării în mod redundant al echipamentelor, materialele necesare etichetării și cosmetizării conexiunilor din rack.
Livrabilele aferente activităților de instalare și configurare a echipamentelor sunt:
#L1.1 Raport de instalare și configurare a echipamentelor

5.9.2. Livrarea, instalarea și configurarea produse software

Instalarea și configurarea produselor software se va realiza în termenul prevăzut conform ”Planului de livrare produse și prestări servicii” întocmit pe baza prevederilor din capitolul 10.1 al prezentului document.
Pentru asigurarea livrării cu succes a componentelor software ale sistemului vor trebui asigurate următoarele activități:

a. Finalizarea arhitecturii funcționale;
b. Instalarea componentelor software;

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

c. Configurarea preliminară a componentelor software.

La finalizarea activității, Contractantul va elabora un Raport de instalare și configurare a componentelor software, ce va conține obligatoriu informații privind:

a. Tabel cu produsele software livrate și instalate
b. Tabel cu mașinile/containerele virtuale configurate
c. Descrierea modului de instalare a fiecărei componente software (inclusiv cu capturi de ecran)
d. Lista de verificare a instalării și configurării preliminare a componentelor software

Livrabilele aferente activităților de instalare și configurare a produselor software sunt:

Livrabil #L2.1 Raport de instalare și configurare a produselor software.

5.9.3. Analiză și proiectare

Rolul principal al Fazei de analiză și proiectare este de a înțelege corect nevoile utilizatorilor și de a descrie la un nivel suficient de detaliu sistemul care urmează a fi implementat.

Contractantul trebuie să execute activități de analiză a cerințelor care să asigure premisele unei implementări eficiente. Informațiile care stau la baza procesului de analiză sunt:

a. Contractul, pentru termene și condiții;
b. Caietul de sarcini și propunerea tehnică;
c. Cerințele clientului colectate și evaluate în timpul acestei faze.

Activitățile desfășurate în această fază se vor concentra inițial pe completarea informațiilor prezentate în caietul de sarcini, astfel încât Contractantul să poată avea o imagine corectă și completă a domeniilor de aplicabilitate.

Contractantul trebuie să deruleze activități de colectare date necesare pentru definirea în detaliu a cerințelor aferente noului sistem. Trebuie colectate informațiile necesare în vederea:

a. Identificării legislației și a procedurilor operaționale care reglementează procesele din scopul proiectului aferente serviciilor de combaterea discriminării prestate de către CNCD persoanelor fizice și juridice;
b. Identificarea automatizărilor care se pot implementa din perspectiva suportului informatic asigurat prin implementarea sistemului;
c. Mapării grafice a proceselor viitoare aferente serviciilor de combaterea discriminării prestate de către CNCD persoanelor fizice și juridice, în contextul îndeplinirii cerințelor funcționale solicitate de către soluțiile software din scopul proiectului (se va utiliza un instrument software de modelare BPMN);
d. Analizei situației existente a infrastructurii de securitate și a infrastructurii serviciilor IT

Achizitorul va acorda tot sprijinul necesar pentru înțelegerea cât mai bună și completă a contextului în care va fi implementat sistemul.

În cadrul acestei faze este obligatorie abordarea de tip prototip evolutiv, prin configurarea preliminară a produselor software din contract, asigurând astfel un suport vizual concret pentru

Achizitor în procesul de validare a modului de implementare a proceselor viitoare aferente serviciilor prestate de către CNCD persoanelor fizice și juridice.
Propunerea tehnică trebuie să cuprindă următoarele:

a. Metodologia detaliată pentru derularea activităților de analiză și proiectare în cadrul propriei organizații;
b. Descrierea instrumentelor utilizate în vederea colectării și evidența cerințelor, asigurării trasabilității cerințelor, pornind de la specificațiile tehnice, pentru demonstrarea acoperirii integrale a tematicii proiectului, modelării proceselor și activităților în conformitate cu standarde de modelare și reprezentare recunoscute (UML sau echivalent);

Serviciile de analiză și proiectare trebuie să acopere cel puțin următoarele aspecte:

a. Identificarea și documentarea proceselor operaționale care vor fi impactate prin implementarea sistemului în cadrul contractului - succesiunea activităților, participanții și momentul intervenției acestora, locația sau contextul, modalitatea de intervenție, informația procesată și resursele utilizate
b. Arhitectura de sistem – va prezenta cel puțin următoarele niveluri: componente software instalate (sisteme de operare, produse software), arhitectura logică cuprinzând descrierea componentelor de sistem, a celor dezvoltate sau personalizate și caracteristicile funcționale și non-funcționale ale acestora;
c. Scenarii (cazuri) de utilizare – din care să reiasă modul de utilizare a sistemului informatic din perspectiva utilizatorului, modul în care utilizatorii interacționează cu sistemul, în corespondență directă cu activitățile menționate în cadrul proceselor operaționale ale acestor utilizatori. Scenariile de utilizare trebuie să cuprindă și interacțiunile cu sistemele externe, astfel încât să fie evidențiat exact modul în care este fructificată o integrare la nivel de sistem informatic. De asemenea, scenariile de utilizare vor fi însoțite de o listă a actorilor sistemului și maparea acestora cu actorii de business;
d. Modelul de date pentru serviciile solicitate.
e. Modelul de securitate – la nivel logic (organizarea pe roluri, grupuri, drepturi, poziția în structura organizatorică etc.);
f. Integrările la nivel de componentă software – pentru fiecare interacțiune se va specifica sistemul sursă/destinație, modalitatea de implementare, canal de comunicare, setul și structura de date transferate, reguli specifice de validare etc.

Livrabilele rezultate din derularea activităților din cadrul aceste faze sunt:
Livrabil #L3.1 Raport de analiză a SIISPECD (ce include cel puțin următoarele: fluxuri de lucru/procese operaționale specifice serviciilor publice de ocupare, cerințe de integrare).
Livrabil #L3.2 Raport de proiectare a SIISPECD (ce include cel puțin următoarele: arhitectura software și funcțională a sistemului și modul în care se propune configurarea componentelor de sistem astfel încât să se obțină funcționalitățile solicitate în caietul de sarcini și/sau identificate/detaliate, descrierea interfețelor; descrierea modulelor; tipuri/categorii de

formulare/template-uri care vor fi gestionate; model de date; specificații de securitate și de integrare, matricea de trasabilitate a cerințelor).

5.9.4. Implementare

Întrucât SIISPECD va trebui să respecte cerințele funcționale și tehnice specifice Beneficiarului, Contractantul va desfășura activități de configurare, parametrizare, personalizare, dezvoltare software, migrare date și testare.

Implementarea SIISPECD include și activități de asigurare a securității informatice a soluției, și dezvoltarea interfețelor de integrare, pentru schimbul de date cu sisteme externe, în baza specificațiilor detaliate și a raportului de proiectare realizat în faza anterioară.

Contractantul va asigura Beneficiarului o cât mai bună vizibilitate asupra stadiului implementării sistemului, printr-o abordare de implementare flexibilă, iterativă, bazată pe un feedback rapid și o disponibilitate sporită.

În cadrul acestei faze se vor realiza și toate activitățile necesare pentru implementarea extinderii tuturor componentelor infrastructurii IT existente.

Activitățile de configurare, parametrizare, personalizare, dezvoltare software și testarea se vor desfășura pe mediul de testare-dezvoltare.

La sfârșitul fazei de implementare trebuie să fie acoperite toate cerințele și specificațiile solicitate în prezentul document și definite în Faza de analiză a cerințelor și proiectare a sistemului și cele a căror optimizare ar putea fi identificată în timpul dezvoltării.

În cadrul propunerii tehnice se va prezenta:

a. Metodologia detaliată în baza căreia vor fi desfășurate activitățile de implementare;
b. Instrumentele utilizate în desfășurarea activităților de implementare;
c. Metodologia de testare după care se vor realiza activitățile de testare în timpul desfășurării contractului;
d. Instrumentele de testare folosite.

Livrabilele aferente Fazei de implementare sunt:

#L4.1 Plan de testare a SIISPECD (aferent fiecărei etape)

#L4.2 Raport de testare SIISPECD (aferent fiecărei etape)

#L4.3 Documentația de administrare a SIISPECD, care va contine si modelul de date (inclusiv structura bazei de date, explicatii pentru semnificatia, modul de completare, codificare ale tuturor campurilor din bazele de date, relatiile dintre tabele, etc

#L4.4 Documentația de utilizare a SIISPECD

În cadrul fazei de implementare a sistemului, Achizitorul (cu asistența Contractantului) va rula toate scenariile pentru testarea funcțională a sistemului. Testele se vor derula în conformitate cu Planul de Testare Funcțională realizat de Prestator și agreat de Achizitor, plan ce va fi în concordanță cu întregul ciclu de realizare al contractului: etape de testare distribuite pe iterații, seturi de

funcționalități sau alte tipuri de teste.
Planul de testare funcțională va cuprinde toate testele necesare pentru a demonstra acoperirea în întregime a cerințelor funcționale din prezentul document. Astfel, se va avea în vedere faptul că sistemul 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 Achizitorul.
Planul de testare funcțională, însoțit de scenariile de testare, va fi realizat de către Prestator și aprobat de Achizitor înainte de începerea testării propriu-zise.
În cadrul fazei de implementare a sistemului după finalizarea testării funcționale se va realiza testarea de performanță. Prestatorul va preda Autorității Contractante rezultatul raportului de testare performanță.
Obiectivele generale ale testării de performanță sunt:

a. Măsurarea timpilor de răspuns solicitați de Achizitor;
b. Reproducerea cu acuratețe a activităților realizate de utilizatorii reali ai sistemului;
c. Diagnosticarea problemelor de performanță și validarea soluțiilor propuse de către dezvoltatori;

Obiectivele specifice ale testării de performanță sunt:

a. Crearea unor scenarii de testare foarte apropiate de realitate prin care sa se simuleze activitatea normală a utilizatorilor și măsurarea timpilor de răspuns în aceste condiții;
b. Diagnosticarea problemelor de performanță în cazul în care timpii de răspuns nu se încadrează în limitele acceptabile și repetarea iterațiilor de testare pentru a confirma că problemele au fost rezolvate;

În cadrul fazei de implementare a sistemului după finalizarea testării de performanță se va realiza testarea de securitate, care va fi efectuată din perspectiva unui atacator extern prin care vor fi identificate eventualele breșe de securitate, cât și riscurile la care este supus sistemul informatic prin prisma acestora.
Prin testarea securității sistemului informatic va fi asigurată identificarea posibilelor vulnerabilități existente la nivelul sistemelor hardware, bazelor de date și aplicațiilor software, furnizând echipei de implementare recomandări/informații destinate remedierii vulnerabilităților identificate.
Se vor efectua teste de penetrare “pentest” pentru evaluarea securității sistemului informatic prin simularea de atacuri informatice, prin exploatarea vulnerabilităților existente și cunoscute. Procesul va implica o analiză activă a sistemului informatic pentru orice vulnerabilități existente care ar putea rezulta din configurația inadecvată și din breșe cunoscute sau necunoscute, hardware și software.
Testele de penetrare (pentest) vor avea ca rezultat o analiză complexă a securității sistemului informatic, testând eficacitatea măsurilor de securitate implementate prin simulare unor atacuri informatice. Activitățile se vor baza pe practici de “ethical hacking”, pentru o testare de tip Black box – experții nu trebuie să cunoască nici o informație despre sistemele testate, cu excepția numelor aplicațiilor (adresa web) sau a unor adrese IP.

Activitățile de pentest efectuate vor cuprinde:

- Stabilirea și elaborarea planului de testare, precum și a scenariilor de atac
- Evaluarea conectivității între sistemul utilizat pentru test și sistemul testat, descoperirea sistemelor și serviciilor active precum și scanarea sistemelor pentru descoperirea vulnerabilităților
- Construirea de arbori de atac (attack trees) și implementarea de acțiuni definite în aceste structuri
- Analiza următoarelor vulnerabilități ale aplicațiilor web:
- Verificarea input-ului utilizatorului;
- Controlul accesului;
- Cross Site Scripting (XSS) ;
- Buffer overflow;
- Tratarea erorilor;
- Injectare de cod arbitrar;
- Criptarea și stocarea informației în execuția aplicației;
- Erori de configurare a aplicației.

Prestatorul va furniza rapoarte de testare structurate în două părți distincte: partea executivă și partea tehnică. Partea executivă va conține descrierea pe scurt a problemelor și vulnerabilităților identificate și va utiliza metode grafice (cel puțin diagrame, grafice sau hărți). Partea tehnică va detalia din punct de vedere tehnic problemele și vulnerabilitățile identificate.

Recomandările de remediere a problemelor și vulnerabilităților identificate vor cuprinde cele mai bune acțiuni/măsuri/metode ce trebuie întreprinse/luate/folosite pentru eliminarea sau micșorarea riscului generat de problemele și vulnerabilitățile detectate precum și recomandări și propuneri de implementare ale acestora.

5.9.5. Instruire

Pentru a asigura exploatarea în bune condiții a SIISPECD, în cadrul acestei faze, Contractantul va asigura un program de instruire a utilizatorilor, conform cerințelor prezentate în această secțiune a caietului de sarcini.

Planul de desfășurare a programului de instruire va fi supus aprobării Autorității Contractante cu cel puțin 10 zile înainte de începerea fiecărei etape și va conține minim următoarele informații:

a. detalierea modului de organizare și desfășurare,
b. curricula cursurilor de instruire.

Reprezentanții CNCD vor selecta personalul care va participa la programul de instruire în funcție de roluri.

5.9.5.1 Sesiuni de instruire privind soluțiile aplicative implementate

Sesiunile de instruire dedicate utilizatorilor sistemului vor acoperi minim următoarele aspecte:

- Prezentarea sistemului, a modulelor și funcționalităților generale
- conștientizarea utilizatorilor în ceea ce privește măsurile de securitate cibernetică
- Autentificare și profilul utilizatorilor, rolurile și drepturile acestora
- Utilizarea fiecărui modul funcțional
- Modalitatea de utilizare a documentației tehnice și de solicitare a suportului tehnic
- Conștientizarea securității utilizatorilor
- Securitate pentru administratorii sistemului

Astfel, Prestatorul va organiza minim 5 sesiuni a minim 32 ore/ sesiune, pentru grupe de maxim 15 cursanți.

Contractantul va avea obligația de a elabora materialele de instruire și de a le pune la dispoziția participanților la curs, cu cel puțin 10 zile înainte de data începerii cursurilor de instruire.

Pe durata instruirii Prestatorul va întocmi liste de prezență zilnice. La finalul instruirii acesta va livra un Raport de instruire care va avea anexate cel puțin listele de prezență, evaluarea cursurilor și a cursanților, lista de înmânare a diplomelor, diplomele acordate cursanților.

Suportul de curs va fi livrat în format electronic, în limba română. Achizitorul va furniza elementele de identitate vizuală necesare. Participanții la programul de formare vor primi diplome de participare/certificate de absolvire din partea Prestatorulu / furnizorului de formare acreditat, după caz.

Achizitorul va furniza lista persoanelor participante cu minim 5 zile înainte de data planificată pentru începerea fiecărei sesiuni de formare.

Instruirea utilizatorilor se va realiza întro locație din București pusă la dispoziție de contractant, în sistem clasă.

În organizarea sesiunilor de instruire, Contractantul va asigura toată logistica necesară, respectiv: calculatoare/laptop-uri (câte unul pentru fiecare participant la sesiunea de formare), video-proiector, catering pentru participanți (2 pauze de cafea și masa de prânz), suportul de curs și materialele consumabile necesare.

5.9.5.2 Instruire privind conștientizarea securității pentru utilizatori

Furnizorul va asigura servicii de instruire privind conștientizarea securității de către personalul autorității contractante beneficiare, fiind vizată informarea utilizatorilor asupra diverselor riscuri de securitate și a modalităților de adresare și reducere a acestora.

Sesiunile vor fi organizate printr-o platformă modernă de instruire care va fi pusă la dispoziție de furnizor pe perioada implementării și garanției. Această trebuie să îndeplinească următoarele cerințe:

- Platforma trebuie să permită definirea de sesiuni de instruire privind securitatea informatică prin care să fie alocate automat modulele de instruire ce trebuie parcurse de anumite categorii de utilizatori.

- Fiecare modul de instruire se va finaliza cu o testare a utilizatorilor.
- În baza rezultatelor obținute la testări, soluția trebuie să fie capabilă să genereze un „profil de risc al utilizatorului”. Acest profil va fi utilizat pentru a genera acțiuni remediale (ex: instruire suplimentară pentru utilizatorii cu risc ridicat).
- Soluția trebuie să ofere indicatori de performanță (KPI) și rapoarte care să măsoare progresul utilizatorilor în procesul de instruire, oferind echipei de securitate vizibilitatea necesară pentru a furniza intervenții direcționate prin alte sesiuni de conștientizare a securității.
- Platforma trebuie să permită simulări de atacuri de tip phishing pentru a permite instruirea utilizatorilor.
- Platforma trebuie să includă un catalog cu cel puțin 20 de module interactive de tip micro-learning, utilizând tehnici moderne de vizualizare (animație, video sau elemente grafice interactive), disponibile cel puțin în limba română, prin care să fie acoperite cel puțin următoarele teme:
    - Introducere în Securitatea Informației,
    - Securitate e-mail și phishing,
    - Securitate Web,
    - Protecție împotriva programelor malware,
    - Medii de stocare (dispozitive portabile),
    - Cloud Computing,
    - Lucru de la distanță (utilizare Wi-Fi publică),
    - BYOD și securitatea dispozitivelor mobile,
    - Criptare,
    - Parole,
    - Inginerie socială,
    - Rețele sociale,
    - Clasificarea informațiilor,
    - GDPR,
    - Răspuns la încălcare procedurilor (raportarea incidentelor);
- Platforma trebuie să includă o biblioteca ce conține materiale precum videoclipuri scurte, postere, screensavere, imagini de fundal sau buletine informative.
- Următoarele sunt obligatorii și direct aplicabile activității beneficiarului, având prioritate în configurarea și raportarea soluției:
    - GDPR (Regulamentul UE 2016/679): Este obligatoriu, instituția prelucrând volume mari de date cu caracter personal. Soluția trebuie să asigure instruirea specifică și raportarea conformității angajaților cu normele de protecție a datelor.
    - Directiva NIS / NIS 2 (Legea nr. 362/2018): Este obligatorie pentru asigurarea securității rețelelor și sistemelor informatice ale instituției.

- ISO/IEC 27001: Este standardul de referință pentru sistemul de management al securității informației. Soluția trebuie să suporte cerințele de instruire și conștientizare impuse de acest standard.

- Platforma trebuie să aibă capabilitatea de a mapa conținutul de instruire pe aceste standarde
- Soluția trebuie să furnizeze rapoarte detaliate privind nivelul de conștientizare al utilizatorilor referitor la securitate și progresul acestora în procesul de instruire. Aceste rapoarte servesc ca dovadă a instruirii periodice a personalului, cerută de standarde (ex: ISO 27001 A.7.2.2);
- Platforma trebuie să permită auditarea activităților, inclusiv a rezultatelor instruirii.
- Platforma trebuie să permită integrarea cu soluții de managementul identității utilizatorilor pentru a permite să sincronizeze automat grupurile de utilizatori. Totodată platforma trebuie să permită introducerea și actualizarea cursanților prin importarea fișierelor de tip CSV sau introducerea manuală a acestora în interfața de administrare.
- Platforma va licențiată pentru tot personalul autorității contractante, pentru întreaga perioadă de implementare și garanție, și poate fi „în mod Perpetual sau de tip subscripție”.

5.9.5.3 Instruire pentru realizarea resurselor educaționale digitale necesare pentru furnizarea de cursuri de formare privind drepturile omului, efectele discriminării și principiului egalității.

Furnizorul va asigura servicii de instruire de tip hands-on pentru 3 persoane desemnate de beneficiar pentru realizarea resurselor educaționale digitale necesare pentru furnizarea de cursuri de formare privind drepturile omului, efectele discriminării și principiului egalității.
În acest sens, Furnizorul va pune la dispoziție pe perioada implementării și garanției o aplicație software pentru cei 3 creatori de resurse educaționale, fiecare beneficiind de un cont de acces propriu. Aplicația software va fi disponibilă ca serviciu (SAAS – software as a service), full online, pe infrastructura furnizorului, fără necesitatea de a instala aplicații specifice pe dispozitivul pe care este utilizată.
Aplicația software de realizare a resurselor educaționale va fi integrată cu aplicația software de furnizare de cursuri de formare ofertată. Aceasta integrare trebuie sa beneficieze de un sistem de tip Single Sign On – SSO și să beneficieze de un sistem de transfer securizat al datelor (materialelor) între cele două aplicații.
Aplicația software de realizare a resurselor educaționale trebuie să îndeplinească următoarele cerințe:

- Software-ul ofertat este accesibil online prin intermediul browser-elor uzuale (Chrome, Edge, Opera, Mozilla, Safari etc), fără a fi dependent de un anumit sistem de operare.
- Funcționalitățile cerute sunt deja disponibile în software-ul ofertat la data ofertării. Pentru verificarea existenței conformității tehnice se va pune, la cerere, la dispoziția autorității contractante un cont de acces demo la platforma ofertată.

- Aplicația are toate meniurile și informațiile afișate în timpul lucrului minim în limba română.
- Materialele educaționale generate vor avea caracter responsive. Acesta reprezintă capacitatea conținutului de a își adapta elementele ce-l definesc (imagini, texte etc.) în funcție de rezoluția display-ului dispozitivului prin intermediul căruia este accesat.
- Aplicația are un sistem de management al licențelor, printr-un un cont de administrator, care permite alocarea sau re-alocarea licențelor la orice moment, conform necesităților beneficiarului
- Revocarea accesului unui utilizator la o licență, dă dreptul alocării respectivei licențe unui alt utilizator, fără a consuma suplimentar din numărul de licențe disponibile (realocare).
- Editorul permite importul unui proiect anterior exportat cu ajutorul editorului ca pachet .zip (inclusiv pachet .zip exportat cu împachetare SCORM, preluând și metadatele sale)
- Editorul beneficiază de un spațiu personal de lucru și stocare, unde fiecare creator își poate organiza proiectele materialelor și elementele de conținut individual și în dosare (foldere). Asupra acestora se pot aplica acțiuni specifice fișierelor (creare, mutare, duplicare, ștergere, redenumire) atât individual, cât și în grup (pe mai multe materiale o dată).
- Aplicația permite lucrul colaborativ prin acces partajat la sursa fiecărui material digital. Creatorii pot alege cu cine să partajeze materialele având opțiunile de a partaja pe baza de adrese de e-mail, de a partaja către echipa în care au fost alocați la alocarea licențelor, de a partaja pe baza unui link direct către sursa materialului.
- Aplicația permite inserarea în materialul digital interactiv a elementelor de tip text, având minim următoarele funcționalități:
    a. fiecare element de tip text are o zonă de editare a textului specifică, în care se pot alege fontul și mărimea fontului, culoarea fontului, tipul de marcaj (bold, italic, normal, supra-script sau sub-script), culoarea fundalului textului, aliniere (stânga, dreapta, centru, bloc).
    b. elementele de tip text se pot structura sub formă de liste numerice sau cu bule.
    c. este disponibil un sistem AI pentru generarea și reformularea textelor (ChatGPT-4 sau similar) care permite introducerea textului direct în materialul educațional fără a părăsi platforma
    d. în elementele de tip text se pot introduce imagini, tabele, precum și formule matematice.
    e. include un editor de formule matematice, integrat. Acest editor de ecuații și formule științifice oferă suport pentru modul de definire LaTeX, dar asigură și editarea vizuală cu ajutorul unor formule/constructori pre-definiți.
    f. elementelor de tip text li se pot asocia acțiuni de tip hyperlink sau salt întrun punct determinat (pentru realizarea de butoane de navigare internă).
- Aplicația permite inserarea în materialul digital interactiv a elementelor de tip imagine, având minim următoarele funcționalități:
    a. elementele de tip imagine pot fi încărcate de pe dispozitivul propriu în formate diferite, minim .jpg, .png, .svg, .gif, inclusiv gif animat.

b. imaginile pot fi încărcate din baza de date externă, integrată, cu imagini cu drepturi de folosire nerestricționată (CC0) pe baza unui mecanism de tip căutare pe baza de cuvinte cheie.
c. imaginile pot fi generate cu ajutorul instrumentului de tip AI integrat (inteligență artificială)
d. imaginile pot fi editate direct în aplicație, atât în ceea ce privește conținutul (filtre, adăugare de text sau elemente grafice), cât și forma (rotație, redimensionare, tăiere).
e. fiecare imagine poate avea o descriere și o descriere ALT pentru accesibilizare
f. fiecare imagine poate fi descărcată din aplicație în propriul dispozitiv.

- Aplicația permite inserarea în materialul digital interactiv a elementelor de tip carusel de imagini (galerie), având minim următoarele funcționalități:
  a. dă posibilitatea definirii unei ordinii de apariție a unui număr de imagini dorit de creator, fiecare imagine având un număr de ordine, o descriere și o descriere ALT pentru accesibilizare.
  b. au incluse butoane pentru control care la apăsare duc la imagine anterioară sau următoare
  c. elementele de tip imagine pot fi încărcate de pe dispozitivul propriu în formate diferite, minim .jpg, .png, .svg, .gif, inclusiv gif animat.
  d. imaginile pot fi încărcate din baza de date externă integrată (cu imagini cu drepturi de folosire nerestricționată CC0) pe baza unui mecanism de tip căutare pe baza de cuvinte cheie
- Aplicația permite inserarea în materialul digital interactiv a elementelor de tip clip audio, având minim următoarele funcționalități:
  a. dă posibilitatea încărcării din dispozitivul propriu și rulării unui element de tip audio în format mp3.
  b. pentru fiecare element de tip audio se poate defini o imagine de fundal Poster), care va fi vizibilă tot timpul, deasupra barei cu elemente de control.
  c. are de o bară de control al sunetului, care cuprinde un buton de start/pauză, o bara de navigare înainte/înapoi, un element de control de tip sunet pornit/oprit, precum și posibilitatea de stabilirea a vitezei de rulare a sunetului, din mai multe opțiuni predefinite (normal, mai rapid, respectiv mai încet), selector de subtitrare, control de subtitrare oprită/pornită.
  d. Oferă opțiunea de afișare a barei de control a sunetului în formă compactă (implicit în forma responsive), care presupune doar arătarea butonului de start/pauză, fără restul elementelor de control.
  e. pentru fiecare clip audio se pot defini mai multe subtitrări, în oricâte limbi, folosindu-se formatul WebVtt specific pentru fișierele de subtitrare. Subtitrările se pot încărca sub formă de fișiere .vtt și .srt sau se pot edita direct în platformă
  f. clipul audio poate fi înregistrat folosind sistemul de înregistrare integrat în editor
  g. clipul audio poate fi generat folosindu-se sistemul de generare audio integrat în editor. Acest sistem pune la dispoziție minim 3 voci masculine și 3 voci feminine pentru limba română. Audio este generat cu ajutorul unui instrument TTS (text to speech) de tip AI și are opțiunea de a modifica viteza de vorbire și timbrul vocii

folosite. De asemenea se poate genera și pe baza instrucțiunilor SSML.

- Aplicația permite inserarea în materialul digital interactiv a elementelor de tip clip video, având minim următoarele funcționalități:
    a. dau posibilitatea încărcării și rulării unui element de tip video. Pentru fiecare element de tip video se poate defini și o imagine de tip poster, care este vizibilă la începutul clipului video.
    b. beneficiază implicit de o bară de control al clipului, care are buton de start/pauză, o bara de navigare înainte/înapoi, un element de control de tip sunet pornit/oprit, precum și posibilitatea de stabilirea a vitezei de rulare a video, din mai multe opțiuni predefinite (normal, mai rapid, respectiv mai încet), selector de subtitrare (dacă sunt mai multe subtitrări), control de subtitrare oprită/pornită, opțiune de rulare în ecran complet.
    c. are posibilitatea vizualizării barei de control a clipului în formă compactă (implicit pe ecrane cu rezoluție mică), care presupune doar arătarea butonului de start/pauză și a celui de ecran complet, fără restul elementelor de control.
    d. pentru fiecare clip video se pot defini mai multe subtitrări, în oricâte limbi, folosindu-se formatul WebVtt specific pentru fișierele de subtitrare. Subtitrările se pot încărca sub formă de fișiere .vtt și .srt sau se pot edita direct în platformă
    e. include un editor pentru tăierea rapidă a unor secvențe din filmele încărcate de pe calculatorul personal
    f. adăugarea de resurse interactive și de evaluare (chestionare) în interiorul unui video (încărcat sau integrat), care se vor activa la momentele de timp precizate, în interiorul chenarului în care rulează video. După interacțiunea cu respectiva resursă, materialul video va putea fi reluat de unde rămăsese, în interiorul aceluiași chenar
    g. clipurile video pot fi încărcate de pe calculatorul propriu ca fișiere .mp4 si .webm
    h. clipurile video pot fi încărcate dintr-o bibliotecă video, sub formă de animații 2D și 3D stoc (CC0) din surse multiple integrate direct, care pot fi utilizate în multiple rezoluții, pe baza unui mecanism de căutare pe bază de cuvinte cheie
    i. clipurile video pot rula pe bază de link din surse terțe publice (YouTube sau similar) în playerul editorului
    j. este posibilă selectarea mai multor intervale specifice pentru a fi incluse în materialul ce este afișat la rulare, fără a fi nevoie să fie modificată direct sursa video (vor rula doar părțile dorite din materialul video selectat). Această opțiune este disponibilă pentru filme încărcate de pe calculatorul propriu și pentru cele rulate pe bază de link din surse externe.
    k. clipurile video pot fi generate folosindu-se un sistem de generare video de tip AI (inteligență artificială) integrat în editor. Acest sistem facilitează generarea video cu avatar (personaj), împreună cu TTS (text to speech) voce masculină și feminină, în limbi multiple (inclusiv limba română) cu sincronizarea mișcării buzelor avatarurilor disponibile (lipsync) și posibilitatea stabilirii unei imagini de fundal. Sunt disponibili minim 3 avataruri bărbați și minim 3 avataruri femei.
- Aplicația permite inserarea în materialul digital interactiv a elementelor de tip joc de cuvinte (rebus), având minim următoarele funcționalități:

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

a. permite definirea unor indicii (definiții) pentru mai multe cuvinte, fiecare cuvânt formând o linie orizontală. Folosind cate o literă din fiecare cuvânt de pe orizontală se poate forma un cuvânt pe verticală.
b. cuvântul-cheie de pe verticală poate fi afișat inițial sau identificat prin găsirea corectă a cuvintelor de pe orizontală
are opțiunea de a ignora sau nu diacriticele, astfel încât dacă este introdus un cuvânt corect cu sau fără diacritice, acesta să fie tratat în funcție de opțiunea aleasă la crearea jocului.

Aplicația permite inserarea în materialul digital interactiv a elementelor de tip marcaje (etichete), având minim următoarele funcționalități:

a. permite crearea unei aplicații în care utilizatorul poate apăsa pe varii zone marcate ale unei imagini pentru a descoperi informații despre zona respectivă
b. pentru fiecare element de tip etichetă poate defini imaginea de fundal, prin încărcarea unei imagini de pe calculatorul personal (.jpg, .png, .svg, .gif) sau prin alegerea unei imagini reprezentative din baza de date externă integrată (cu poze cu drepturi de folosire nerestricționată CC0).
c. pentru fiecare element de tip etichetă (marcaj) se pot defini zona din imagine aferentă, un titlu și un conținut care este afișat la interacțiunea utilizatorului (click).

- Aplicația permite inserarea în materialul digital interactiv a elementelor de tip atașament, având minim următoarele funcționalități:
  a. permite încărcarea de documente în corpul materialului educațional, astfel încât acestea să poată fi descărcate de către utilizatori când accesează conținutul educațional (ex: teme de lucru, planșe etc), indiferent de platforma pe care rulează conținutul și de tipul fișierului atașat.
  b. prezintă numele documentului, extensia lui, precum și o descriere (opțională)
- Aplicația permite inserarea în materialul digital interactiv a elementelor de tip test (chestionar, quiz), având minim următoarele funcționalități:
  a. conțin întrebări de cel puțin 8 tipuri diferite: cu un singur răspuns, cu răspunsuri multiple, cu plasare de elemente pe poziția corectă, cu reordonare de elemente în ordinea corectă, cu selectare din listă, cu răspuns liber, de tip slider (cursor), cu subliniere răspuns.
  b. fiecare tip de întrebare permite adăugarea de feedback pentru cel ce răspunde, atât pentru răspunsurile corecte, cât și pentru cele incorecte, feedback care va fi afișat imediat după ce respondentul face o selecție.
  c. în textul aferent întrebării sau variantelor de răspuns se pot introduce imagini.
  d. pentru fiecare test există opțiunea de a amesteca automat atât ordinea întrebărilor dintr-un test, cât și ordinea răspunsurilor pentru fiecare întrebare
  e. pentru fiecare test se poate selecta un anumit număr de întrebări ce vor fi arătate din totalul întrebărilor disponibile în acel test, care vor fi prezentate respondentului spre rezolvare (baterie de teste)
  f. pentru fiecare întrebare poate fi stabilit un punctaj distinct, punctajul maxim de 100% fiind raportat la suma punctajelor individuale ale întrebărilor din test
  g. pentru fiecare test se pot stabili mai multe bareme procentuale. Obținerea unei

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

peste un anumit barem va determina apariția unui mesaj definit de creator pentru trecerea peste respectivul barem.

h. pentru fiecare test se poate selecta posibilitatea de utilizare a chestionarelor din trei moduri diferite - învățare, evaluare și sondaj.
i. testele permit stabilirea unui interval de timp pentru parcurgere, cu afișarea timpului disponibil în timpul parcurgerii testului.

- Fiecare material poate fi publicat minim: ca pachet SCORM 2004 revizia 3 și ca pachet HTML5 împachetat .zip ce poate rula independent de platformă.
- Zona de metadate dă posibilitatea definirii pentru materialul produs a: autorului (autorilor), descrierii materialului, cuvintelor cheie, limbii materialului. La publicarea materialelor ca pachete SCORM, toate metadatele sunt împachetate în aceste pachete, pentru a putea fi citite și afișate în platforme LMS compatibile SCORM.
- Pe toata perioada de licențiere a soluției se va asigura mentenanță si update-uri, fiind necesară prezentarea în acest sens a unei declarații asumate de către producătorul aplicației/platformei ofertate, pentru prezentul proiect
- Toate costurile aferente folosirii instrumentelor AI, respectiv aferente folosirii bazelor de date cu multimedia integrate în platformă sunt incluse în prețul de licențiere ofertat, pe toata durata licențierii și fără limitare de folosire.

Folosind editorul ofertat, pe parcursul instruirii se va realiza un șablon (model de structura de modul e-learning) ce va fi utilizat ulterior pentru dezvoltarea cursurilor e-learning de către beneficiar. Șablonul va putea fi modificată de beneficiar în toate aspectele sale. În structura șablonului vor fi integrate minim următoarele elemente:

a. Conținut textual însoțit de elemente grafice relevante pentru subiectul temei (titlu, concepte, obiective etc.).
b. Elemente interactive: audio, video/animație, galerie de imagini, organizator acordeon sau tab, alte elemente interactive disponibile.
c. Întrebări pentru fixarea informațiilor (cu răspuns automat instant) - alegere simplă, alegere multiplă, trage si poziționează, potrivire, completare, răspuns deschis, subliniere răspuns corect.
d. Text cu concluzii însoțit de audio.
e. Asistent virtual cu text și audio, care enunță sarcina/ prezintă informații /enunță instrucțiunile de utilizare, pe măsură ce cursantul parcurge modulul.
f. Un cuprins care să:
    - fie funcțional – la apăsarea pe elementele de cuprins cursantul să fie trimis la respectivele capitole/subcapitole;
    - conțină un indicator al gradului de parcurgere al modului e-learning – procentual, care să se raporteze la toate elementele din cuprins;
    - aibă o funcție de tip căutare, care să caute cuvântul introdus peste tot în modul și să-l evidențieze prin subliniere cu altă culoare acolo unde este găsit;

În structura șablonului vor fi integrate minim următoarele elemente de identitate vizuală ale beneficiarului:

- două zone de grafică – una în care se poate prezenta o imagine reprezentativă pentru modulul de curs și o a doua, in cuprinsul funcțional, unde se va introduce sigla beneficiarului.
- gama de culori a modulelor, care va respecta indicațiile de identitate vizuală ale beneficiarului

5.9.6. Punerea în producție

În cadrul acestei faze:

- Contractantul va realiza migrarea soluțiilor implementate de pe mediul de testare-dezvoltare pe mediul de producție. Soluția implementată va permite transferul configurărilor între mediul de testare-dezvoltare și cel de producție fără a fi necesară dezvoltarea de scripturi suplimentare;
- Achizitorul și Contractantul vor desfășura activitățile necesare pentru punerea în producție a SIISPECD.

Activitățile se vor desfășura în conformitate cu Planul de Trecere în Producție realizat de Contractant și agreat de Achizitor.

Planul de trecere în producție va cuprinde toate activitățile necesare și va ține cont de legăturile logice între subsistemele/componentele sistemului, astfel încât să se asigure o trecere în producție coerentă și cu impact minim asupra activităților zilnice ale angajaților Beneficiarului.

Livrabilele rezultate din derularea activităților din cadrul aceste faze sunt:

Livrabil #L6.1 Plan de punere în producție a SIISPECD

Livrabil #L6.2 Raport de punere în producție a SIISPECD

Livrabil #L6.3 Documentația as-built a SIISPECD

Livrabil #L6.4 Procedura de suport tehnic/mentenanță corectivă/mentenanță evolutivă

5.9.7. Servicii de asigurare a securității cibernetice a rețelei și sistemului informatic

Serviciile de asigurare a securității cibernetice a rețelei și sistemului informatic vor fi asigurate pe o perioadă de minim 60 de luni de la recepție și vor consta în:

a. Serviciile de tip SOC (Security Operations Center) cu componenta de CSIRT (Computer Security Incident Response Team) vor asigura monitorizarea și detectarea tuturor etapelor din lanțul Cyber Kill al atacurilor cibernetice: recunoaștere, armare, livrare, exploatare, instalare, comandă și control (C2) și acțiuni asupra obiectivelor din rețeaua CNCD și sistemul informatic SIISPECD. Pe lângă detecția și triajul incidentelor este foarte importantă și izolarea în timp real, analiza și remedierea efectelor amenințărilor cibernetice. Din acest motiv sunt solicitate servicii SOC disponibile 24/7 pentru întregul an și cu componentă de CSIRT.

b. Servicii de testare a securității de tip pentest – va fi asigurată, anual pe perioada de furnizare a serviciilor, o testare de penetrare de tip black- box. Prima testare se va realiza la inițierea serviciilor.
c. Servicii aferente funcțiunilor/responsabilităților unui CISO (Chief Information Security Officer) - se vor concretiza prin activități de evaluare, analiză, actualizare, elaborare de propuneri transmise spre avizare/aprobare, propunere obiective strategice, stabilire tipurilor de controale și monitorizare continuă a implementării procedurilor și/sau a măsurilor de securitate.

Serviciile de asigurare a securității cibernetice a rețelei și sistemului informatic vor fi asigurate pe baza unei platforme de tip SOC, formată din mai multe componente printre care o soluție SIEM (Security Information and Event Management) și SOAR (Security Orchestration, Automation, and Response), agenți de colectare evenimente, alte soluții de securitate deja existente în structura Autorității Contractuale, etc. Platforma SOC va colecta loguri din rețeaua CNCD și din SISPECD: servere și end-point-uri (Windows, Linux), componente de securitate (firewall, AV, etc.), componente de rețea (routere, switch-uri), fluxuri de rețea - colectarea și analizarea pachetelor de rețea, servicii de rețea (Active Directory), servicii cloud, inclusiv SaaS. Colectarea de jurnale va fi bazată pe colectarea syslog sau alt protocol care nu folosește agenți, dar și pe colectarea bazată pe agenți. Pentru a asigura confidențialitatea și integritatea informațiilor, se va asigura în mod obligatoriu utilizarea de agenți criptați, iar întregul transfer de date (loguri, evenimente, alerte) către și dinspre platforma SOC se va realiza exclusiv în mod criptat.

Platforma SOC va fi capabilă să integreze și să utilizeze informații externe, privind amenințările pentru a îmbunătăți detecția (cel puțin o sursă de Threat Intelligence, lista de IOCs data de DNSC - prin instanța de MISP, etc.). Platforma va fi capabilă să efectueze triajul inițial al alertelor și să ofere un indicator de prioritate pentru alerte/incidente. Platforma trebuie să suporte capacitățile de interogare pentru a permite o analiză și o investigare criminalistică suplimentară a alertelor/incidentelor. Platforma trebuie să includă și o soluție de management a incidentelor.

Vor fi asigurate toate măsurile necesare pentru a nu exista loguri care se pierd în timpul ingestiei, transportului, prelucrării sau stocării acestora**.**

Perioada de inițializare a serviciului se va finaliza cu un raport care va descrie cum s-a făcut implementarea cu succes a platformei, ce tipuri de loguri s-au preluat spre analiză, ce tipuri de loguri nu se pot prelua și care este motivul pentru care nu este vizibilitate pe aceste echipamente/porțiuni de rețea. De asemenea acest raport va conține și rezultate ale testelor de stres, funcționalitate, integrare ale aplicațiilor/platformelor folosite.

Logurile/Evenimentele colectate și incidentele înregistrate vor avea o perioadă de retenție de minim 6 luni. De asemenea se vor păstra și copii de backup a datelor și configurațiilor, respectând recomandările din domeniu, referitor la backup și recovery. Fie că datele sunt în tranzit sau depozitate, Furnizorul are obligația să asigure confidențialitatea, disponibilitatea și integritatea acestora. De asemenea pe toată perioada contractului, furnizorul de servicii de securitate cibernetică va lua toate măsurile necesare pentru a nu introduce nici o vulnerabilitate în rețeaua Autorității

Contractante și pentru a asigura securitatea informației. Datele stocate, după un minim de 6 luni vor fi eliminate în manieră etică și în siguranță, furnizorul aplicând măsuri astfel încât să fie imposibilă recuperarea accidentală a datelor.

Serviciile de asigurare a securității cibernetice a rețelei și sistemului informatic se vor asigura în regim 24/7 pentru următoarele niveluri de suport:

- Nivelul 1: Acest nivel este responsabil pentru monitorizarea și detectarea incidentelor de securitate. Echipa de nivel 1 trebuie să identifice incidentele de securitate, să le analizeze și să le raporteze echipei de nivel 2. De asemenea, această echipă trebuie să asigure o reacție rapidă la incidente și să implementeze măsuri de prevenire a acestora.
- Nivelul 2: Echipa de nivel 2 este responsabilă pentru analiza incidentelor de securitate și pentru a determina impactul acestora asupra organizației. Această echipă trebuie să determine cauzele incidentelor și să dezvolte soluții pentru a preveni incidente similare în viitor. De asemenea, echipa de nivel 2 trebuie să colaboreze cu echipa de nivel 3 pentru a implementa soluțiile dezvoltate.

Tipul de răspuns la incidente trebuie sa fie de natură hibridă: reactivă (monitorizare, triaj, răspuns, analiză, remediere, lecții învățate) pentru toate tipurile de incidentelor de la P1 - prioritate critică până la P4 - prioritate scăzută, dar și de natură proactivă în care se va scana constant infrastructura Beneficiarului după ultimele amenințări identificate prin tehnici de Threat Intelligence, Vulnerability și Patch Management și/sau OSINT.

Abordarea reactivă a incidentelor cibernetice (încălcare a securității cibernetice care poate să afectează confidențialitatea, integritatea și disponibilitatea datelor sau a sistemelor informatice) va urma următorii pași:

- Detectarea incidentului - Incidentul poate fi detectat de către sistemul de securitate sau de către un utilizator.
- Evaluarea incidentului: determinarea tipului de incident și a impactului acestuia asupra organizației.
- Izolare: limitarea răspândirii incidentului și prevenirea unor daune suplimentare.
- Investigarea incidentului: analiza incidentului pentru a determina cauzele și modul în care a avut loc.
- Remedierea incidentului: remedierea efectelor incidentului și eliminarea oricăror vulnerabilități care ar putea fi exploatate în viitor.
- Monitorizarea incidentului: lecții învățate pentru a se asigura că nu se mai întâmplă și pentru a preveni incidente similare în viitor.

CNCD nu dispune de specialiși în securitate cibernetică, astfel că măsurile de remediere necesare vor fi implementate direct de către furnizorul serviciilor de asigurare a securității cibernetice a rețelei și sistemului informatic.

Furnizorul trebuie să urmeze o metodologie de management al schimbării care trebuie agreată de CNCD, pentru orice modificare a modelului de operare al serviciilor de asigurare a securității cibernetice a rețelei și sistemului informatic. Acestea includ modificări ale soluției platformei SOC,

renunțare la anumite surse de log-uri, eliminarea monitorizării pentru anumite dispozitive de rețea, protocoale de comunicații, oricare alte modificări care ar putea afecta serviciile.
Furnizorul trebuie să dețină propriul centru de monitorizare și răspuns la incidente de securitate informatică de tip CSIRT. Componenta de tip SOC (incluzând infrastructura tehnologică aferentă stocării și procesării datelor, precum și centrul operațional / echipa CSIRT) trebuie să fie localizată exclusiv pe teritoriul României. Mai mult, furnizorul are obligația de a respecta în mod expres prevederile Directivei (UE) 2022/2555 (NIS 2) transpusă în legislația națională, în arhitectura, implementarea și operarea întregii componente SOC.
Furnizorul trebuie să asigure, în timpul procesului de inițializare a serviciilor, managementul proiectului, îndrumări, documentație detaliată și să colaboreze cu personalul Autorității Contractante sau cu furnizorii săi pentru a configura procesele necesare care să permită prestarea serviciilor, urmărind cel puțin următoarele:

- identificarea și stabilirea sistemelor de monitorizare a securității Autorității Contractante în scopul de aplicare al proiectului;
- ingerarea evenimentelor și furnizarea accesului pentru sistemele de monitorizare a securității in scopul proiectului;
- Configurarea soluțiilor și proceselor de escaladare evenimente/incidente;
- Stabilirea proceselor de raportare, conținutul, formatul, frecvența și listele de distribuție;
- Furnizorul trebuie să colaboreze cu CNCD pentru a prelua inventarul de active, detalii ale configurațiilor, proprietățile sistemelor și criticitatea activităților.
- Furnizorul va fi răspunzător de toate update-urile și patch-urile necesare funcționării platformei/platformelor în condiții optime și de siguranță.

În vederea asigurării unui nivel ridicat al prestării serviciilor de asigurare a securității cibernetice a rețelei și sistemului informatic furnizorul va pune la dispoziție, pe toata perioada contractului accesul la platforma software SOC pentru colectarea logurilor, corelarea evenimentelor și răspunsul la incidentele de securitate.

5.9.8. Graficul de prestare al serviciilor

Activitățile pentru implementarea SIISPECD se vor desfășura conform unui ”Plan de livrare produse și prestări servicii” care trebuie să respecte următorul graficul de prestare al serviciilor:

Nr. fază	Denumire fază	Luna 1	Luna 2	Luna 3	Luna 4	Luna 5	Luna 6	Luna 7	Luna 8	Luna 9	Luna 10	Luna 11	Luna 12
1	**Livrare, instalare și configurare echipamente**												
	Jalon 1												
2	**Livrare, instalare și**												

Nr. fază	Denumire fază	Luna 1	Luna 2	Luna 3	Luna 4	Luna 5	Luna 6	Luna 7	Luna 8	Luna 9	Luna 10	Luna 11	Luna 12
	configurare software												
	Jalon 2												
3	**Analiză și Proiectare**												
	Jalon 3												
4	**Implementare**												
	Jalon 4												
5	**Instruire**												
6	**Punere în producție**												
	Jalon 5												

Termenii utilizați în calendarul de implementare au următoarele definiții:

- ”Fază” reprezintă un element bine definit și delimitat de acțiune în cadrul contractului ce urmează să fie atribuit, a cărei realizare presupune un timp estimat de realizare rezultat din etapele, respectiv activitățile în care este descompusă;
- ”Etapă” reprezintă un element bine definit și delimitat de acțiune în cadrul unei faze a contractului ce urmează să fie atribuit, a cărei realizare presupune un timp estimat de realizare rezultat din activitățile în care este descompusă;
- ”Jalon” reprezintă un element prin care se marchează finalizarea uneia sau mai multor etape sau faze în cadrul execuției contractului.

Derularea contractului începe după data semnării acestuia de către ambele părți. Perioada de execuție a contractului va fi de maxim 12 luni.

Termenele de implementare și modalitatea de calcul a lunilor proiectului trebuie să fie calculate începând de la data semnării contractului de către părți.

6. Cerințe privind garanția și suportul tehnic

6.1. Garanția echipamentelor

Garanția echipamentelor va fi asigurată de către Prestator pentru o perioadă minimă de 60 luni, atât pentru produse, cât și pentru accesorii, garanția începând din momentul recepției calitative.

În perioada de garanție Prestatorul va garanta că produsele livrate prestate sunt conforme cu specificațiile tehnice din prezentul document și nici o componentă/echipament nu va eșua în a-și îndeplini funcțiunile, în situația în care este corect utilizată.

În perioada de garanție, Prestatorul va trebui să asigure:

a. corectarea gratuită, pentru produsele livrate, a oricăror erori, defecte și neconformități constatate, cu excepția cazurilor în care defectele se datorează în mod exclusiv utilizării inadecvate / necorespunzătoare de către personalul Achizitorului;
b. suport tehnic de specialitate pentru produsele livrate;
c. acces direct la suportul oferit de producător pentru produsele livrate;

d. înștiințarea Achizitorului privind încetarea producției oricăruia din produsele livrate în baza Contractului sau privind încetarea suportului oferit de producător.

În perioada de garanție, Prestatorul are obligația să asigure funcționarea produselor, reparând sau înlocuind prin grija și pe cheltuiala lui orice componentă hardware sau accesoriu.

În cazul în care echipamentele și accesoriile necesită înlocuire în perioada de garanție ca urmare a defectării sau funcționării neconforme cu cerințele specificate în prezentul document, aceasta se va realiza în timpul programului de lucru al Achizitorului, transportul de la și înapoi la Achizitor intrând în sarcina Contractantului.

După efectuarea reparației/înlocuirii și punerea în funcțiune a echipamentului/componentei defecte, între Contractant (partenerul de service acreditat al Contractantului, după caz) și Achizitor se întocmește un proces-verbal de recepție.

În perioada de garanție, toate costurile legate de înlocuirea sau repararea bunurilor, precum și de remedierea defecțiunilor cad în sarcina Contractantului (diagnosticare, transport, costuri de asigurare, taxe în vamă, manoperă pentru reparare etc.).

6.2. Suportul tehnic pentru produsele software

Furnizorul va asigura suport tehnic pentru produsele software solicitate (actualizări și patch-uri de securitate) pentru o perioadă minimă de 60 luni începând din momentul recepției calitative, fără nici un cost suplimentar pentru Autoritatea contractantă, cu excepția componentelor software pentru care s-a solicitat un alt termen prin prezentul document.

6.3. Servicii de mentenanță a SIISPECD

Contractantul va asigura servicii de mentenanță pe o perioadă de minim 48 luni de la punerea în producție a SIISPECD. Prin serviciile de mentenanță se urmărește asigurarea funcționării optime a aplicațiilor sistemului fără a afecta nivelul de disponibilitate de 99,5% al acestora precum și implementarea noilor cerințe ale aplicațiilor, generate de dinamica și evoluția structurii organizaționale la nivelul instituției, evoluția tehnologica, interoperabilitatea cu sisteme informatice evolutive, cerințe noi privind sistematizarea și organizarea datelor, criterii de căutare, parametrii mediului în care rulează aplicațiile.

Prestarea serviciilor de mentenanță a sistemului conform descrierii din acest capitol au ca obiectiv îndeplinirea indicatorilor beneficiarului și anume:

- adăugarea/modificarea de fluxuri interne ale aplicațiilor;
- Rezolvarea defectelor/disfuncționalităților aplicațiilor/sistemului;
- Respectarea timpilor de rezolvare a incidentelor raportate;
- Disponibilitatea de 99,5% a serviciilor;
- Asigurarea timpului mediu de răspuns pentru o solicitare;
- Lipsa incidentelor cauzate de nerespectarea politicilor de backup și restaurare și a condițiilor de securitate stabilite la nivelul Beneficiarului;
- Lipsa incidentelor cauzate de accesul neautorizat;

- Lipsa incidentelor cauzate de încălcarea politicilor IT.

6.3.1. Descrierea generală a serviciilor de mentenanță solicitate

6.3.1.1 Grupe de servicii

1. Servicii de mentenanță a infrastructurii hardware
2. Servicii de mentenanţă a infrastructurii software
3. Servicii de mentenanță preventivă
4. Servicii de mentenanță evolutivă

6.3.1.2 Condiţii generale pentru prestarea serviciilor

1. Furnizorul va întocmi lunar un raport privind serviciile prestate. Raportul va include:
   - Pentru mentenanța preventivă:
     - Numărul de incidente înregistrat în perioada raportării;
     - Numărul de incidente rezolvate în perioada raportării (inclusiv detalierea respectării Service Level Agreement - SLA);
     - Rezultatele realizate în cursul perioadei de raportare, precum și recomandările sau solicitările aferente pentru perioada următoare.
   - Pentru mentenanța evolutivă:
     - Progresele înregistrate ;
     - Dificultățile întâmpinate în cursul implementării cerințelor și soluțiile propuse pentru a depăși respectivele dificultăți;
     - Rezultatele realizate in cursul perioadei de raportare, precum și recomandările sau solicitările aferente pentru perioada următoare.
2. Furnizorul va pune la dispoziţie un centru de suport unic (Nivel 1) pentru sesizarea şi urmărirea modului de rezolvare a incidentelor.
3. Neîncadrarea în parametrii de disponibilitate şi continuitate a funcţionării serviciilor, depăşirea timpilor de răspuns şi de rezolvare al incidentelor, prestarea cantitativă şi necalitativă a serviciilor in perioadele de timp definite, lipsa de reacţie la producerea de evenimente în sistemul informatic, precum și nesoluţionarea acestora atrage după sine aplicarea de penalizări conform contractului.

6.3.2. Definirea şi prezentarea modelului general de prestare al serviciilor

Modelul general de structurare a serviciilor este următorul:

Nivel 1 – Centrul de suport unic

- Verificări pas cu pas a aplicației în vederea furnizării serviciilor implementate;
- Aplicarea de corecții minore la nivelul aplicațiilor;
- Rezolvarea incidentelor utilizând baza de cunoștințe;

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

- Verificarea și interpretarea informațiilor istorice conform bazei de cunoștințe;
- Menținerea în permanență a legăturii cu beneficiarul;
- Gestionarea trasabilității informațiilor asociate unei sesizări (în aplicația de înregistrare și urmărire a incidentelor).

Nivel 2 – Mentenanță preventivă și analiza performanței sistemului

- Activități de reproducere a incidentului;
- Monitorizarea aplicației prin:
  - Interogarea soluțiilor specifice de monitorizare, unde este cazul;
  - Verificarea și urmărirea sistemului de gestionare a bazelor de date;
  - Verificarea funcționarii aplicațiilor în parametri optimi de funcționare;
- Verificări periodice a funcționalității sistemului:
  - Verificarea istoricului monitorizării acolo unde este cazul;
  - Verificarea jurnalelor de erori ale aplicațiilor, serverelor de aplicații și baze de date;
  - Verificarea jurnalelor la nivelul sistemului de operare;
- Verificări asupra stării echipamentelor tip server în vederea identificării din timp a posibilelor probleme (lipsa spațiu harddisk, memorie insuficientă, capacitate insuficientă procesor);
- Verificarea salvărilor (back-up) bazelor de date și al aplicațiilor;
- Verificarea periodica a funcționalității sistemului;

Nivel 3 – Mentenanță corectivă și evolutivă

- Propuneri de îmbunătățire a aplicațiilor;
- Intervenții în locație daca este cazul;
- Erori ale aplicațiilor;
- Rezolvarea incidentelor la nivelul sistemului de gestionare a bazelor de date;
- Executarea de modificări minore la nivelul aplicațiilor;
- Instalarea versiunilor noi ale aplicațiilor realizate pe baza serviciilor de mentenanță evolutivă.
- Aplicarea modificărilor legislative
- Dezvoltarea de noi funcționalități
- Instalare versiuni noi aplicație

6.3.3. Serviciile de suport Nivel 1 - Centrul de suport unic

6.3.3.1 Cadrul general de desfăşurare al serviciilor

Prestatorul va organiza și dota întro locație proprie, un centru de suport unic (Nivel 1). Acesta va oferi servicii de suport Nivel 1 pentru înregistrarea și urmărirea modului de rezolvare a incidentelor prin intermediul unei aplicații de înregistrare și urmărire a incidentelor.
Serviciile de suport Nivel 1 cuprind:

- Procesarea Incidentelor și Cererilor de Schimbare (în cazul mentenanței evolutive) prin colectarea informațiilor necesare și rutarea cererilor către echipele de suport corespunzătoare
- Primirea și înregistrarea automată a mesajelor de alertare și de eroare transmise via email în mod automat de aplicațiile de monitorizare și diagnosticare din sistemul informatic
- Rezolvarea incidentelor utilizând baza de cunoștințe;
- Verificarea și interpretarea informațiilor istorice conform bazei de cunoștințe;
- Gestionarea trasabilității informațiilor asociate unei sesizări (în aplicația de înregistrare și urmărire a incidentelor).
- Verifică fiecare cerere a beneficiarului conform cu contractul de suport încheiat;
- Se asigura că toate înregistrările sunt tratate în mod eficient și cu promptitudine, în conformitate cu SLA;
- Obține informații necesare tratării cererii de suport, atunci când este cazul;
- Analizează cererea de asistenta sosita;
- Monitorizează toate cererile beneficiarului;
- Menține legătura în permanență cu beneficiarul. Ține beneficiarul la curent cu stadiul fiecărei probleme;

6.3.3.2 Funcţionarea Centrului de Suport Unic

Înregistrarea Incidentelor

Înregistrarea incidentelor, se face de către reprezentanții desemnați ai Beneficiarului folosind aplicația de înregistrare şi urmarire incidente pusă la dispoziție de Prestator.
Reprezentantul desemnat poate verifica online starea în care se afla un incident raportat de el, pe baza numarului de tichet furnizat la înregistrarea incidentului.
Pentru mesajele de alertare și de eroare transmise via email în mod automat de aplicațiile de monitorizare și diagnosticare din sistemul informatic, va fi generat automat un tichet în Aplicația de înregistrare şi urmarire incidente chiar daca mesajul nu conţine suficiente informaţii pentru ca inginerul de suport tehnic să poata identifica problema. Aceste informaţii vor fi adaugate în Aplicația de înregistrare şi urmarire incidente ulterior, pe masura ce vor deveni disponibile responsabilului de incident.

Identificarea problemei

Se verifica dacă problema expusa de Beneficiar este deja introdusă în Aplicația de înregistrare şi urmarire incidente (de catre un alt membru al echipei de suport) şi daca are deja o rezolvare.
Dacă problema nu este introdusa în Aplicația de înregistrare şi urmarire incidente, se trece la

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

identificarea ei.
Se analizează descrierea problemei (mod de manifestare, situaţia anterioara, mesajele de eroare care apar) și dacă este cazul se contactează Beneficiarul pentru informații suplimentare.
Se detecteaza tipul problemei, aplicaţia în care a aparut, versiunea aplicaţiei, modulul aplicaţiei în care a aparut problema. Pentru aceste acţiuni se vor folosi unelte de depanare create pentru fiecare aplicaţie sau echipament.
Daca problema este deja introdusa în Aplicația de înregistrare şi urmarire incidente se încearca rezolvarea ei. Daca problema este deja introdusa în Aplicația de înregistrare şi urmarire incidente şi exista şi o soluţie, aceasta este comunicată Beneficiarului.
Rezolvarea incidentului
Incidentul este rezolvat pe unul din nivelele 1, 2 sau 3 în funcţie de criteriile menţionate la începutul capitolului.
Incidentul va fi escaladat pe nivelul 2 sau 3, dacă este necesar.
Rezolvarea unui incident se face prin completarea tipului de rezolvare şi prin descrierea modalitaţii de rezolvare. Pentru incidentele de tip hardware, Inginerul de Suport Tehnic va încerca sa rezolve incidentul telefonic. Daca problema depaşeşte competenţele sale, cererea de rezolvare va fi redirecţionată catre urmatorul nivel de suport.
Soluţia este testata de catre specialiștii de pe nivelul 2.
Înainte de a-i comunica Beneficiarului modalitatea de rezolvare a incidentului semnalat, membrii echipei de suport (respectiv cel care a raportat problema) trebuie sa testeze validitatea soluţiei incidentului.
Daca testarea se finalizeaza cu succes, inginerul de suport comunica beneficiarului soluţia. Daca testarea soluţiei eşueaza, acesta reasigneaza incidentul.
Comunicarea soluţiei
Inginerul de support tehnic comunica soluţia catre beneficiar. Comunicarea soluţiei se va face pe canalul pe care s-a primit solicitarea.
Validarea soluţiei
În cazul comunicarii scrise, la sfârşitul mesajului, se va solicita confirmarea validitaţii soluţiei transmise. Daca soluţia oferita a fost validata, incidentul respectiv se închide. Daca soluţia nu este corecta/utila incidentul se redeschide şi, daca este cazul, se reasigneaza.

6.3.3.3 Responsabilitățile Prestatorului

a. Asigură serviciile de suport prin utilizarea unui grup de agenți
b. Asigură servicii de helpdesk în limba română printr-un punct unic de contact
c. Pune la dispoziția administratorilor desemnați ai Beneficiarului conturi de utilizator în aplicația de înregistrare și urmărire a incidentelor pentru transmiterea cererilor de suport
d. Primește, validează, înregistrează, clasifică, prioritizează, diagnostichează, rezolvă sau

escaladează cererile de suport primite.

e. Escaladează cererile de suport la echipele de suport corespunzătoare
f. Asigură serviciile de suport în zilele lucrătoare între orele 9-17 prin intermediul Aplicației de înregistrare şi urmarire incidente.
g. Menține evidența administratorilor desemnați ai Beneficiarului care transmit cereri de suport, inclusiv locația acestora și contactele anterioare cu Centrul de Suport Unic. Această evidență poate include și detalii referitoare la investigații, analize, actualizări, modalități de rezolvare și data și ora acestor acțiuni.
h. Dacă un incident sau o cerere de serviciu este escaladată unei echipe de suport, centrul de suport unic va furniza administratorilor desemnați ai Beneficiarului un număr de înregistrare al incidentului/cererii de suport și va informa asupra modalității de rezolvare sau a duratei de rezolvare corespunzătoare tipului și priorității cererii respective. Contactarea administratorului desemnat de Beneficiar și închiderea incidentului sau cererii de suport va fi realizată cu echipele de suport conform procedurii de escaladare.
i. Informează administratorii desemnați ai Beneficiarului asupra modului de rezolvare și închidere a tichetelor.
j. Monitorizează echipele de suport în vederea respectării SLA.
k. Toate comunicările se fac în limba română.

6.3.3.4 Responsabilitățile Beneficiarului

a. Să impună administratorilor desemnați ai Beneficiarului să folosească șablonul stabilit pentru transmiterea incidentelor și a cererilor.
b. Asigură personalului Prestatorului din Centrul de Suport Unic drepturile de acces corespunzătoare la echipamentele, aplicațiile și locațiile aferente sistemului informatic
c. Informează administratorii desemnați ai Beneficiarului asupra întreruperilor planificate în furnizarea serviciilor
d. Sprijină Prestatorul la identificarea, completarea și actualizarea informațiilor din baza de date a Centrului de Suport Unic pentru a fi utilizate de agenții de helpdesk în procesul de rezolvare a cererilor de suport.

6.3.3.5 Cerințe privind Aplicația de înregistrare şi urmarire incidente

Prestatorul va pune la dispoziție o aplicaţie ce va fi utilizată de serviciul Help Desk al acestuia pentru înregistrarea şi urmărirea incidentelor (tichetelor).

6.3.4. Serviciile de suport Nivel 2 – Servicii de mentenanță preventivă și analiză a performanței

6.3.4.1 Cadrul general de desfăşurare al serviciilor

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

Serviciile de mentenanță preventivă au ca scop verificarea și ajustarea periodică a funcționării sistemului în scopul reducerii probabilității apariției incidentelor care pot conduce la afectarea disponibilității sistemului.
Analiza performanței sistemului implica activitati de investigare a neconformităților (identificate fie prin intermediul sistemului de monitorizare sau ca urmare a incidentelor deschise de către administratorii desemnați ai Beneficiarului referitor la performanță) precum și recomandarea de schimbări atât la nivelul componentelor cât și la nivelul arhitecturii întregului sistem integrat pentru îmbunătățirea performanței.
Analiza performanței implică urmărirea și executarea procesului de management al problemelor, bazat pe o analiza a cauzelor acestora, în vederea inițierii de acțiuni corective. Acest serviciu nu include și activitățile de remediere și înlăturare efectiva a cauzei.

6.3.4.2 Descrierea pachetului de servicii

Serviciile de suport de nivel 2 vor asigura:

- Activități de reproducere a incidentului;
- Monitorizarea aplicației prin:
  - interogarea soluțiilor specifice de monitorizare, unde este cazul;
  - Verificarea și urmărirea sistemului de gestionare a bazelor de date;
  - Verificarea funcționarii aplicației în parametri optimi de funcționare;
- Verificări periodice a funcționalității sistemului:
  - Verificarea istoricului monitorizării acolo unde este cazul;
  - Verificarea jurnalelor de erori ale aplicațiilor, serverelor de aplicații și baze de date;
  - Verificarea jurnalelor la nivelul sistemului de operare;
- Verificări asupra stării echipamentelor tip server în vederea identificării din timp a posibilelor probleme (lipsa spațiu harddisk, memorie insuficienta, capacitate insuficienta procesor);
- Verificare loguri si notificari ale aplicațiilor; verificare consistenta date; verificarea functionarii în parametri normali a aplicațiilor;
- Verificarea salvărilor (back-up) bazelor de date și al aplicațiilor
- Analiza log-uri stare funcționare a echipamentelor de stocare
- Analiza log-uri stare funcționare a echipamentelor de securitate
- Analiza log-uri funcționare a serviciilor configurate în aplicațiile de monitorizare
- Analiza log-uri, verificarea încărcării optime a resurselor, verificarea execuției job-urilor de backup, definirea de notificări în sistemul de gestionare a bazelor de date
- Monitorizarea spațiului liber de pe servere pentru a preveni umplerea discurilor cu fișiere temporare, log-uri sau index. În caz de apariție a unui procent prea mic de

spațiu liber (sub 20%) se va proceda la inițierea operațiunilor de disk cleanup la nivel de discuri și empty transaction log la nivelul bazei de date. Consultarea spațiului ocupat de bazele de date și informațiile stocate (Storage Metrics) pentru a preveni cazuri de creștere rapidă a conținutului. Inventarierea listelor importante cu privire la numărul de înregistrări înregistrate în ultima perioadă.

- Colectarea de feedback cu privire la performanțele utilizării aplicațiilor de la utilizatori cheie. Analiza jurnalelor de performanță și timp de răspuns pe pagini și acces la aplicații.
- Verificarea update-urilor la nivel de sistem de operare și aplicații. Documentarea update-urilor și planificarea operațiunii de testare a instalării.
- Verificarea și aplicarea update-urilor pentru sistemul de operare.
- Verificarea update-urilor pentru BIOS și service pack-urilor la nivelul echipamentelor fizice.
- Validarea copiilor de siguranță. Restaurarea copiilor de siguranță în mediul de test pentru testarea copiilor de siguranță.

6.3.4.3 Responsabilitățile Prestatorului

- Asigură efectuarea activităților de monitorizare și analiză a performanței descrise în capitolul anterior, în scopul detectării eventualelor aspecte ce pot duce la apariția de incidente în funcționarea sistemului și trimite cereri de suport la nivelul 3, dacă este cazul;
- Preluarea cererilor de suport sosite de pe nivelul 1 și reproducerea incidentului în scopul diagnosticării acestuia și escaladarea cererilor de suport primite la Nivelul 3, la nevoie
- Asigură serviciile de suport în zilele lucrătoare între orele 09-17, de la distanță sau la nevoie în locația Beneficiarului.

6.3.4.4 Responsabilitățile Beneficiarului

- Asigură personalului Prestatorului de pe nivelul 2 drepturile de acces corespunzătoare la echipamentele, aplicațiile și locațiile aferente sistemului informatic
- Sprijină Prestatorul la identificarea, completarea și actualizarea informațiilor referitoare la incidentele escaladate de pe Nivelul 1

6.3.5. Serviciile de suport Nivel 3 – Servicii de mentenanță corectivă și evolutivă

6.3.5.1 Cadrul general de desfășurare al serviciilor

Serviciile de mentenanță corectivă au ca scop funcționalitatea optima și stabilitatea infrastructurii aplicațiilor sistemului la un nivel de disponibilitate de minim 99,5%. Serviciile de mentenanță evolutivă sunt destinate implementări noilor cerințe ale aplicațiilor, generate de modificări ale

dinamicii și evoluției structurii organizaționale la nivelul instituției, evoluția tehnologica, interoperabilitatea cu sisteme informatice evolutive, cerințe noi privind sistematizarea și organizarea datelor, criterii de căutare, parametrii de mediu în care rulează aplicațiile precum și nomenclatoarele aferente acesteia.

În acest sens, serviciile de suport de nivel 3 vor asigura:

- Propuneri de îmbunătățire a aplicațiilor;
- Probleme de infrastructura (hardware sau software de sistem);
- Intervenții în locație daca este cazul;
- Erori ale aplicațiilor;
- Rezolvarea incidentelor la nivelul sistemului de gestionare a bazelor de date;
- Executarea de modificări minore la nivelul aplicațiilor;
- Instalarea versiunilor noi ale aplicațiilor realizate pe baza serviciilor de mentenanță evolutiva.
- Constatare și înlocuire componente defecte a echipamentelor de stocare
- Constatare și înlocuire componente defecte, update BIOS pentru echipamentele tip server
- Constatare și înlocuire componente defecte, update firmware pentru echipamentele de securitate
- Identificarea și remedierea erorilor de funcționare a serviciilor configurate în aplicațiile de monitorizare

6.3.5.2 Descrierea pachetului de servicii

Serviciile de suport de nivel 3 sunt definite după cum urmează:

Categoria	Serviciul
Managementul Disponibilității	Restaurarea serviciului Mentenanta corectivă Suport operational Imbunatatirea Performantelor Remediere erori și actualizări
Îmbunătățirea Aplicatiilor	Dezvoltare

6.3.5.2.1. Restaurarea serviciului

Activitatile de restaurare a serviciului implica repunerea la dispoziția utilizatorilor a sistemului (infrastructurii hardware, software și a aplicațiilor) în condițiile de performanță agreate ca urmare a unui incident major sau a unei degradari semnificative a performanței. De asemenea sunt incluse activitățile de corectare a sistemului în vederea prevenirii reapariției incidentului din aceleași cauze.

Caracteristici principale:

- Restaurarea serviciilor cât mai curind posibil cu respectarea procesului de management al incidentelor
- Analizarea cauzei producerii incidentului pentru incidentele repetitive cu respectarea procesului de management al problemelor
- Implementarea de masuri corective permanente în vederea prevenirii reapariției incidentului din aceleasi cauze
- Prioritizarea activitatilor pe baza severitatii si impactului incidentelor, precum si conform nivelului de servicii agreat.
- Include și activitatile legate de managementul interacțiunii cu producătorul aplicațiilor software de infrastructură

6.3.5.2.2. Mentenanța corectivă

Serviciile de mentenanța corectivă includ toate activitatile de mentenanță și administrare a infrastructurii hardware, software și a aplicațiilor sistemului care sunt generate ca urmare a unor defecțiuni sau erori, precum și ale unor modificări ale mediului tehnologic (sisteme de operare, baze de date).

6.3.5.2.3. Suport Operational

Suportul operațional constă în executarea de activități planificate și neplanificate, precum și implementarea de schimbări standard care necesită intervenție umană. Aceste activitati includ actualizari ale componentelor aplicatiilor (parametri, fisiere de configurare, tabele) cu valori predefinite necesare în vederea utilizării și operării sistemului. Aceste actualizari nu implica activitati de dezvoltare software sau modificari ale cerintelor functionale.

6.3.5.2.4. Îmbunătățirea performanțelor

Activitatile de imbunatatire a performantei includ implementarea schimbarilor si a modificarilor aprobate, precum si documentarea acestora, în vederea îmbunătățirii modului de operare al sistemului, asa cum au fost ele identificate in cadrul activitatilor de Analiza performantei sistemului. Aceste modificari nu au ca scop modificarea sau adaugarea de functionalitati sistemului.

6.3.5.2.5. Remediere erori și actualizări minore

Activitatile de remediere a erorilor (bug-fixing) și actualizare minora a aplicatiilor implica planificarea (inclusiv analiza de impact), coordonarea, testarea si aplicarea de patch-uri si actualizari tehnologice puse la dispozitie de producătorii aplicatiilor.

6.3.5.2.6. Servicii de dezvoltare

Aceste servicii sunt destinate efectuarii de modificari majore ale aplicatiilor, ceea ce implica activitati de definire, analiza, proiectare, dezvoltare, testare si implementare de schimbari ale aplicatiilor în scopul adăugarii de noi functionalitati sau modificarii functionalitatilor existente.

6.3.6. Nivelul de asigurare a serviciilor (SLA)

6.3.6.1 Utilizatorii Eligibili

Utilizatorii eligibili pentru serviciile furnizate sunt administratorii desemnați ai Beneficiarului.

6.3.6.2 Tipuri de evenimente

Tipurile de evenimente care fac obiectul serviciilor de suport sunt:

Tip eveniment	Descriere
Incident	Fenomen datorat unei erori interne a sistemului care împiedica întro măsură mai mare sau mai mica desfășurarea activității în mod normal a beneficiarilor sistemului.
Eroare	Problema de funcționalitate a sistemului, de orice natura, care conduce la apariția unui incident ce are ca efect oprirea temporara sau totala a activității sistemului informatic
Informare	Cerere de informare fără impact operațional

6.3.6.3 Niveluri de prioritate (severitate) a incidentelor

Prioritate	Descriere
Prioritate 4	Nu exista impact operațional, este o solicitare sub forma de cerere de informare sau sugestie.
Prioritate 3	Exista un impact operațional care poate afecta o parte din activitățile utilizatorilor aplicațiilor, dar care nu afectează decât o parte nesemnificativa a utilizatorilor aplicațiilor. Activitatea se poate desfășura aproape normal.
Prioritate 2	Exista un impact operațional minor, din cauza căruia este posibil ca anumite funcții să nu mai fie disponibile. O parte din funcționalitățile principale nu pot fi folosite sau o parte din utilizatorii aplicațiilor sunt afectați. Este posibil ca activitatea să continue.
Prioritate 1	Exista un impact operațional major sau blocant, în care este posibil ca funcții critice să nu mai fie disponibile. Funcționalități importante nu pot fi folosite sau o mare parte din utilizatorii aplicațiilor sunt afectați. Activitatea beneficiarului este perturbata în mod semnificativ.

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

6.3.6.4 Indicatorii nivelului de asigurare a serviciului și orar de funcționare

În funcție de prioritatea și tipul de eveniment pe perioada de derulare a contractului se cer următorii timpi de răspuns (Service Level Agreement - SLA):

Tip eveniment și prioritate	Timp răspuns	Timp furnizare soluție intermediară	Timp de rezolvare	Orar funcționare
Incident				
Prioritate 1	2 ore	4 ore	8 ore	24x7
Prioritate 2	2 ore	12 ore	1zi	24x7
Prioritate 3	2 ore	1zi	2 zile	8x5
Eroare				
Prioritate 1	2 ore	4 ore	8 ore	24x7
Prioritate 2	2 ore	12 ore	1zi	24x7
Prioritate 3	2 ore	1zi	2 zile	8x5
Cerere informare				
Prioritate 4	2 ore	-	10 zile	8x5

6.3.6.5 Excluderi

Următoarele evenimente sunt excluse din calculul metricelor ce stau la baza analizei performanței serviciilor:

- Întreruperile planificate și agreate, precum și cele cauzate de echipamente/sisteme ce nu intră în scopul proiectului.
- Orice act sau omisiune din partea Beneficiarului, a contractorilor și Prestatorilor săi sau a oricarei alte entitati asupra căreia Beneficiarul exercita control, inclusiv incapacitatea Beneficiarului de a-și îndeplini responsabilitățile.
- Evenimentele cauzate de aplicatii, echipamente, utilitati ale Beneficiarului, altele decât cele descrise în scopul proiectului.
- Întreruperi ale serviciilor neraportate sau pentru care nu a fost deschis incident la centrul unic de suport.

6.3.6.6 Indicatori de evaluare a serviciilor de suport

În vederea definirii cantitative a serviciilor de suport, se vor utiliza pentru măsurare următorii indicatori:

1. Numărul de fluxuri interne ale aplicațiilor adăugate/modificate in perioada de mentenanță a sistemului;
2. Numărul de defecte/funcționalități ale aplicațiilor/sistemului rezolvate în perioada de mentenanță;
3. Timpul mediu de rezolvare a evenimentelor;
4. Disponibilitatea sistemului;
5. Timpul mediu de răspuns pentru evenimente
6. Numărul incidentelor cauzate de nerespectarea politicilor de backup și restaurare și a condițiilor de securitate stabilite la nivelul Beneficiarului și integrate în sistemul informatic ;
7. Numărul de incidente cauzate de accesul neautorizat;
8. Numărul de incidente cauzate de încălcarea politicilor IT.

6.3.6.7 Volumul serviciilor

6.3.4.7.1. Volumul estimat pentru serviciile de mentenanță preventivă

Tipul serviciilor	UM	Efort anual
Servicii de mentenanță preventivă infrastructura hardware (servere, infrastructura de stocare, infrastructura de rețea, infrastructura de securitate)	**Zile- om**	**36**
Servicii mentenanță preventivă infrastructura software (sisteme de operare, sistem de virtualizare, soluții de management și monitorizare)	**Zile- om**	**24**
Servicii mentenanță preventivă aplicații	**Zile- om**	**72**

Volumul prezentat mai sus include serviciile de suport Nivel 1 și 2, precum și serviciile aferente mentenanței corective de pe Nivelul 3 de suport. Aceste servicii vor fi disponibile neîntrerupt pentru perioada de 60 de luni (incluzând în acest termen și perioada suprapusa cu garanția echipamentelor și suportul tehnic pentru produsele software).

6.3.4.7.2. Volumul maxim pentru serviciile de mentenanță evolutivă

Servicii mentenanță evolutiva	UM	Efort anual
Servicii de mentenanță evolutivă infrastructura hardware (servere, infrastructura de stocare, infrastructura de rețea, infrastructura de securitate)	**Zile- om**	**36**

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

Servicii mentenanță evolutiva	UM	Efort anual
Servicii mentenanță preventivă infrastructura software (sisteme de operare, sistem de virtualizare, soluții de management și monitorizare)	**Zile- om**	**60**
Servicii mentenanță evolutivă aplicații	**Zile- om**	**216**

Serviciile de mentenanță evolutivă vor fi livrate la cererea Beneficiarului și intră în categoria modificărilor guvernate de procedura de management al modificărilor descrise la capitolul 6.3.7.

6.3.7. Abordarea serviciilor de mentenanță evolutivă

Fiecare solicitare de adăugare de funcționalități noi sau modificări în aplicațiile sistemului va fi guvernată de procedura de management al schimbărilor și tratată ca un proiect distinct, ce va fi implementat etapizat.

Schimbările pot aparea datorita modificărilor de mediu, modificărilor cerintelor sau a logicii generale a sistemului.

Cererile de schimbare se pot lansa doar de Beneficiar, chiar dacă pot fi recomandate de Prestator.

Beneficiarul si Prestatorul vor discuta schimbarile propuse și aceste discuții vor avea ca rezultat una din cele trei variante:

- acordul de a nu efectua schimbarea
- cerere de schimbare scrisa din partea beneficiarului
- recomandare pentru schimbare din partea prestatorului

Documentele care vor fi utilizate in cadrul acestei proceduri sunt prezentate in continuare.

6.3.7.1 Documentul de cerere de schimbare

Beneficiarul emite cererea de schimbare prin completarea unui document de cerere de schimbare. După completarea și semnarea de către partea emitenta, documentul cu cererea de modificare va fi transmis Prestatorului.

Toata documentatia referitoare la cerere (scrisori, Procese verbale, documentatie de asistenta) va fi atasata documentului de cerere de schimbare.

6.3.7.2 Evaluarea cererii de schimbare

Cererile de schimbare sunt evaluate de ambele parti si aprobate sau respinse pe baza justificarii si a consecintelor prezentate.

Daca se considera necesar, se poate convoca o sedinta pentru a se discuta cererile. Discutiile trebuie

documentate si adaugate la dosarul cererii de schimbare.

6.3.7.3 Calculul costurilor schimbării

Prestatorul va efectua o analiza initiala a schimbării solicitate. Acest lucru va fi realizat intr-un cadru de timp agreat cu Beneficiarul. Rezultatele analizei vor cuprinde:

- identificarea cerințelor care vor fi afectate de schimbare
- detalii asupra costului, pe baza de timp si resurse;
- timpul necesar pentru implementarea schimbarii, data la care Furnizorul poate incepe sa lucreze si impactul asupra reperelor de timp ale Proiectului.

6.3.7.4 Aprobarea cererii de schimbare

Dupa aprobarea unei cereri de schimbare de către Beneficiar, detaliile aprobarii (inclusiv semnaturile) se vor introduce in documentul cererii de schimbare. O copie va fi trimisa tuturor partilor implicate. Cand este necesar se va trimite si documentatia suport. Apoi documentul cererii de schimbare poate fi inchis.

6.3.7.5 Respingerea cererii de schimbare

Dacă Beneficiarul respinge o cerere de schimbare, detaliile respingerii (inclusiv semnaturile) se vor introduce in documentul cererii de schimbare. O copie va fi trimisa tuturor partilor implicate. Cand este necesar se va trimite si documentatia suport. Apoi documentul cererii de schimbare poate fi inchis.

6.3.7.6 Implementarea schimbării

Implementarea schimbărilor aprobate, va avea loc dupa primirea cererii de schimbare aprobate.

6.3.8. Raportare

Prestatorul va pune la dispozitia Beneficiarului lunar, pe parcursul execuției contractului, un Raport intermediar în care se vor detalia:
mentenanța preventivă:

- Un sumar al incidentelor deschise
- Disponibilitatea sistemului
- Descrierea activitatilor de mentenanta preventive intreprinse
- Raport cu privire la numărul de incidente înregistrat in perioada raportării;
- Raport cu privire la numărul de incidente rezolvate in perioada raportării (inclusiv detalierea respectării Service Level Agreement – SLA, timp de răspuns, timp de rezolvare);

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

- Analiza incidentelor si a indisponibilitatii serviciilor– escalation/downtime / outage
- Un sumar al schimbarilor în arhitectura sistemului integrat (schimbari de configurații, schimbări de organizare, aplicarea de patch-uri, etc)
- Rezultatele realizate în cursul perioadei de raportare, resursele utilizate, precum și recomandările sau solicitările aferente și planificarea activităților contractului pentru perioada următoare.

mentenanța evolutivă:

- Progresele înregistrate;
- Dificultățile întâmpinate în cursul implementării cerințelor și soluțiile propuse pentru a depăși respectivele dificultăți;
- Rezultatele realizate in cursul perioadei de raportare, resursele utilizate, precum și recomandările sau solicitările aferente, și planificarea activităților de mentenanță evolutiva pentru perioada următoare.

Toate rapoartele intermediare vor fi transmise Autorității Contractante în cea de-a treia zi lucrătoare a lunii următoare celei în care s-au prestat serviciile.

6.4. Predare sistem

La finalul perioadei de mentenanță Prestatorul va asigura servicii de transfer a sistemului către echipa desemnată de Achizitor pentru întreținerea ulterioară a acesteia, fie echipa internă, fie un contractor extern.

Serviciile de transfer vor include minim:

- Actualizarea documentației de administrare și utilizare a sistemului, conform ultimei versiuni instalate în mediul de producție;
- Codul sursă (dacă este cazul), arhitectura și structura datelor comentate și actualizate, conform ultimei versiuni instalate în mediul de producție, livrat utilizând un instrument de gestiune și versionare, inclusiv instrumentul de gestiune utilizat cu posibilitate de utilizare fără limitări;
- Transferul bazei de date de cunoștințe cu privire la activitatea de suport și mentenanță acumulată în perioada de suport și garanție;
- O sesiune de minim 5 zile, de instruire a echipei desemnate cu întreținerea sistemului cu privire la arhitectura acestuia, componente, activitățile uzuale de întreținere, salvare și restaurare a sistemului, cu aplicabilitate practică pe mediul de test existent;
- Servicii de role shadowing prin care Prestatorul va sprijini, on the job - în realizarea de operații de zi cu zi, pentru minim 1 lună, personalul Achizitorului sau a contractorului extern, în administrarea, întreținerea și dezvoltarea sistemului, folosind documentația și baza de date de cunoștințe pregătită de Prestator.

Activitățile de transfer vor fi planificate și derulate cu minim 6 luni înainte de finalizarea perioadei de garanție și suport tehnic acordate prin contract.

6.5. Cerințele generale predare coduri sursă

În conformitate cu prevederile art. 12 din Ordonanță de urgență nr. 41 din 28 iunie 2016 privind stabilirea unor măsuri de simplificare la nivelul administrației publice centrale și pentru modificarea și completarea unor acte normative, toate drepturile patrimoniale de autor asupra tuturor operelor create de către Furnizor aferente produsului sau serviciului livrat, se vor transfera către Autoritatea Contractantă. Pentru modulele/componentele software dezvoltate, cu excepția produselor standard, este obligatoriu ca Furnizorul să pună la dispoziția beneficiarului codul sursă al aplicației/aplicațiilor sau configurărilor/customizărilor efectuate împreună cu toată documentația aferentă astfel:

a. Toate codurile sursă vor fi predate de către Furnizor beneficiarului CNCD cu toate versionarile;
b. CNCD impreună cu Furnizorul va verifica daca codul sursă predat CNCD coincide cu codul sursă utilizat în producție. Furnizorul va compila codul sursă împreună cu beneficiarul. Furnizorul va verifica descrierea și comentariile din codul sursă împreună cu beneficiarul.
c. Toate codurile sursă vor include și comentarii scrise în limba română şi în acord cu standardele/convenţiile de dezvoltare a codului (în forma susținută de limbajul de programare aferent, de exemplu comentarii în interiorul codului).
d. Toate codurile sursă vor fi predate în clar, fără a se aplica procedee de ascundere (”obfuscate”);
e. Acceptarea predării codului sursă de către Furnizor și preluării acestora de către beneficiar se va realiza doar după validarea acestora de către Autoritatea contractantă în infrastructură, la recepția sistemului informatic implementat.

Codurile sursă furnizate vor deveni proprietatea CNCD cu drepturi depline (acces, modificare, transfer, etc.).

7. Locul și durata desfășurării activităților

7.1. Locul desfășurării activităților

Echipamentele vor fi livrate și instalate la locațiile indicate.

Pentru activitățile ce vor fi realizate la sediul Autorității contractante, Contractantul trebuie să transmită datele de identificare a persoanelor care își vor desfășura activitatea la sediul și are obligația de a asigura instruirea lucrătorilor proprii cu privire la riscurile specifice activității pe care o vor desfășura la alt sediu decât cel propriu.

Întâlnirea de demarare a activităților din contract (kick-off meeting) între echipa propusă de Contractant și reprezentanții Beneficiarului se realizează la sediul Beneficiarului sau sediul Contractantului (stabilire de comun acord).

Întâlnirile de lucru, de monitorizare a progresului activităților și a rezultatelor intermediare, corespunzătoare fiecărei etape din contract sau ori de câte ori sunt necesare se realizează la sediul Beneficiarului (pentru fiecare întâlnire, se stabilește de comun acord). În funcție de subiectele abordate, părțile pot agrea ca aceste întâlniri de lucru să se desfășoare și online.

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

7.2. Durata contractului

Durata contractului va fi de 12 de luni, de la semnarea contractului.

8. Resurse umane necesare/expertiza necesară pentru realizarea activităților contractului și obținerea rezultatelor

8.1. Experți cheie solicitați pe categorie de expertiză

Contractantul va pune la dispoziția Autorității Contractante lista completă a personalului său (inclusiv cel care aparține asociaților şi subcontractanţilor) care va fi implicat în derularea contractului şi prestarea serviciilor şi care vor necesita acces în locațiile de instalare şi acces la informații despre acestea. Datorită caracterului confidențial al informațiilor la care persoanele nominalizate vor avea acces, Autoritatea Contractanta îşi rezervă dreptul de a verifica personalul respectiv, conform normelor sale interne privind accesul la date şi informații cu caracter confidențial şi de a interzice accesul în amplasamente sau la informații legate de contract acelor persoane care nu îndeplinesc condițiile impuse de Autoritatea Contractantă.

Contractantul se obligă să păstreze, atât el cât și resursele umane propuse, confidențialitatea asupra informațiilor primite de la Beneficiar pe parcursul derulării contractului și asupra rezultatelor obținute în executarea contractului.

Echipa ce va fi prezentată de ofertant va trebui sa aibă o vastă experiența în implementarea de sisteme informatice integrate. În acest sens, ofertantul trebuie să asigure pe întreaga perioada de derulare a contractului personalul necesar în funcție de obiectivele, rezultatele şi activitățile/ livrabilele solicitate în prezentul document, garantând cel puţin personalul având calificarea și experiența profesională descrisă mai jos.

Ofertantul va prezenta componența echipei, instrumentele/ metodele de coordonare a activității acesteia şi va detalia rolurile, atribuțiile și responsabilitățile experților și modalitatea concretă în care echipa prezentată interacţionează cu personalul de suport/ back- stopping pentru îndeplinirea contractului.

În vederea implementării cu succes a proiectului, Contractantul va organiza și va pune la dispoziția autorității contractante o echipă de experți care, prin atribuțiile și pregătirea lor, vor realiza implementarea SIISPECD.

Personalul minim solicitat de către beneficiar și care va fi alocat de Prestator ce va realiza efectiv activitățile care fac obiectul contractului ce urmează a fi atribuit este prezentat în cele ce urmează:

Nr. crt.	Categorie expert	Număr de experți
1.	Manager de proiect	1
2.	Arhitect de sistem	1
3.	Analist Coordonator	1
4.	Expert îmbunătățire procese de business	1
5.	Expert coordonator dezvoltare aplicații web	1
6.	Expert coordonator implementare sistem de	1

Nr. crt.	Categorie expert	Număr de experți
	management documente	
7.	Expert coordonator testare	1
8.	Coordonator instruire pentru utilizare și administrare	1
9.	Expert stocare și protecție copii de siguranță	1

Profilul experților cheie este prezentat în continuare.

8.1.1. Expert cheie nr. 1: Manager de proiect

Managerul de proiect va fi implicat în activitățile contractului privind:

a. Gestionarea și supravegherea modului de execuție a contractului, din punct de vedere administrativ/logistic, comunicațional și operațional în vederea atingerii obiectivelor stabilite
b. supervizarea procedurilor de lucru, asigurarea organizării, coordonării, controlului activităților echipei de proiect;
c. verificarea conformității tuturor livrabilelor de contract din punctul de vedere al prevederilor documentelor contractuale și al dispozițiilor legale aplicabile privind conținutul documentelor realizate de către prestator;
d. participarea la toate activitățile contractului de achiziție;
e. coordonarea echipei tehnice de implementare a sistemului informatic pentru realizarea activităților;
f. funcționarea corectă a sistemului din punct de vedere al respectării cerințelor, consistenței datelor, al constrângerilor de timp, al validărilor de date și al gestiunii erorilor;
g. reprezintă prestatorul în relația cu toate părțile implicate în contract.
h. Este responsabil cu monitorizarea/verificarea permanentă și evaluarea punctuală a atingerii rezultatelor echipei de experți, pentru implementarea sistemului informatic în condițiile stabilite prin documentele contractuale și la termenele prevăzute în graficul Gantt al contractului.

Managerul de proiect va îndeplini următoarele cerințe:

a. Studii de specializare în managementul proiectelor dovedite prin prezentarea unei diplome/ a unui certificat de absolvire în domeniul managementului de proiect, eliberat(ă) de un organism de formare, pentru ocupația manager de proiect (COR 242101/241919) sau echivalent, sau prin prezentarea de diplome de studii superioare care au inclus în curriculumul educațional cursuri de management de proiect;
b. Experiență specifică constând în implicarea în cel puțin un proiect/contract similar (prin proiect/contract similar se înțelege implementarea unui sistem informatic) în care să fi

îndeplinit același tip de activități sau similare ca cele pe care urmează să le îndeplinească în viitorul contract, probată prin scrisori de recomandare din partea beneficiarilor proiectelor sau copie după contractul respectivului proiect/contract, lista de personal a proiectului sau orice alte documente similare din cadrul cărora să reiasă experiența expertului propus etc. De asemenea, din documentele suport trebuie să reiasă clar activitățile similare celor specifice rolului din prezentul Contract, pe care le-a avut expertul în proiectul/proiectele respectiv/respective;

c. Declarație de disponibilitate pentru perioada aferentă activităților pe care și le asumă din prezentul contract.

8.1.2. Expert cheie nr. 2: Arhitect de sistem

Arhitectul de sistem va fi implicat în activitățile contractului privind:

a. Proiectarea arhitecturii la nivel hardware, software și funcțională a sistemului
b. Elaborarea documentației de proiectare
c. Asistă managerul de proiect pentru planificarea implementării soluției proiectate în funcție de constrângerile impuse de arhitectura proiectată
d. Coordonarea echipei tehnice și transpunerea în elemente și componente funcționale a cerințelor din caietul de sarcini și necesităților identificate în etapele de analiză
e. Colaborarea cu responsabilii tehnici ai fiecărei componente a sistemului și cu ceilalți experți pentru implementarea sistemului în conformitate cu cerințele Beneficiarului și documentația de proiectare.
f. Urmărirea respectării caracteristicilor proiectate pe parcursul implementării sistemului
g. Avizarea documentelor de natură tehnică elaborate de către echipa prestatorului pe durata derulării proiectului.

Arhitectul de sistem va îndeplini următoarele cerințe:

a. Studii superioare absolvite/finalizate cu diplomă de licență sau echivalent;
b. Deținerea de competențe în dezvoltarea arhitecturilor prin utilizarea unei metodologii cadru de realizare a acestora, dovedite prin certificare recunoscută la nivel național sau internațional;
c. experiență specifică constând în implicarea în cel puțin un proiect/contract similar (prin proiect/contract similar se înțelege implementarea unui sistem informatic) în care să fi îndeplinit același tip de activități sau similare cu cele pe care urmează să le îndeplinească în viitorul contract, probată prin scrisori de recomandare din partea beneficiarilor proiectelor sau copie după contractul respectivului proiect/contract, lista de personal a proiectului sau orice alte documente similare din cadrul cărora să reiasă experiența expertului propus etc. De asemenea, din documentele suport trebuie să reiasă clar activitățile similare celor specifice rolului din prezentul Contract, pe care le-a avut expertul în proiectul/proiectele respectiv/respective.

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

d. Declarație de disponibilitate pentru perioada aferentă activităților pe care și le asumă din prezentul contract.

8.1.3. Expert cheie nr. 3: Analist Coordonator

Analistul coordonator va fi implicat în activitățile contractului, având următoarele responsabilități:

a. Coordonarea echipei de analiști pentru desfășurarea și documentarea etapei de analiză detaliată a cerințelor de business, descrierea fluxurilor/ proceselor de business/ cazurilor de utilizare, descrierea/ detalierea cerințelor din perspectiva soluției ce urmează a fi implementată și de elaborarea specificațiilor funcționale ale acesteia;
b. Acesta va colabora cu ceilalți membri ai echipei de implementare cu scopul de a asigura implementarea corectă a cerințelor Beneficiarului cu privire la funcționalitățile de business ale soluției, asistență și suport tehnic;
c. Realizarea documentelor de specificații funcționale și implementarea acestora la nivelul soluției informatice, așa cum au fost evidențiate și agreate în documentația de analiză;
d. Pregătire manuale de utilizare și de administrare;
e. Expertul analist coordonator va asigura o privire de ansamblu asupra tuturor ariilor funcționale ale soluției informatice și va fi responsabil de întocmirea documentației de analiză.

Analistul Coordonator va îndeplini următoarele cerințe:

a. Studii superioare absolvite/finalizate cu diplomă de licență sau echivalent;
b. Experiență specifică constând în implicarea în cel puțin un proiect/contract similar (prin proiect/contract similar se înțelege implementarea unui sistem informatic care să fi inclus digitalizarea serviciilor publice; notă: prin serviciu public se înțelege un serviciu furnizat de o autoritate a administrației publice) în care să fi îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract, probată prin scrisori de recomandare din partea beneficiarilor proiectelor sau copie după contractul respectivului proiect/contract, lista de personal a proiectului sau orice alte documente similare din cadrul cărora să reiasă experiența expertului propus etc. De asemenea, din documentele suport trebuie să reiasă clar activitățile similare celor specifice rolului din prezentul Contract, pe care le-a avut expertul în proiectul/proiectele respectiv/respective;
c. Declarație de disponibilitate pentru perioada aferentă activităților pe care și le asumă din prezentul contract.

8.1.4. Expert cheie nr. 4: Expert îmbunătățire procese de business

Expertul îmbunătățire procese de business va fi implicat în activitățile contractului, având următoarele responsabilități:

a. identificarea legislației și a procedurilor operaționale care reglementează serviciile publice în scopul proiectului

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

b. maparea grafică a proceselor existente și viitoare
c. elaborarea proiectelor de implementare a noului model de livrare a serviciilor publice de ocupare
d. colaborarea cu ceilalți membri ai echipei de implementare cu scopul de a asigura implementarea corectă a noului model de livrare al serviciilor publice.
e. Participă la elaborarea livrabilelor aferente serviciilor de analiză și proiectare

Expertul îmbunătățire procese de business va îndeplini următoarele cerințe:

a. Studii superioare absolvite/finalizate cu diplomă de licență sau echivalent;
b. Deținerea de competențe în domeniul managementului proceselor de business și a managementului cerințelor, dovedite prin certificare recunoscută la nivel național sau internațional;
c. Experiență specifică constând în implicarea în cel puțin un proiect/contract similar (prin proiect/contract similar se înțelege un proiect/contract în cadrul căruia au fost prestate servicii de analiză și îmbunătățire a proceselor de business), în care să fi îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract, probată prin scrisori de recomandare din partea beneficiarilor proiectelor sau copie după contractul respectivului proiect/contract, lista de personal a proiectului sau orice alte documente similare din cadrul cărora să reiasă experiența expertului propus etc. De asemenea, din documentele suport trebuie să reiasă clar activitățile similare celor specifice rolului din prezentul Contract, pe care le-a avut expertul în proiectul/proiectele respectiv/respective;
d. Declarație de disponibilitate pentru perioada aferentă activităților pe care și le asumă din prezentul contract.

8.1.5. Expert cheie nr. 5: Expert coordonator dezvoltare aplicații web

Expertul coordonator dezvoltare aplicații web va fi implicat în activitățile contractului privind:

a. transpunerea în funcționalități a cerințelor documentate în etapele de analiză și proiectare
b. participarea la activitățile de instalare, dezvoltare/configurare pe platforma de dezvoltare și administrare aplicații web propusă, pentru implementarea în bune condiții a Portalului de servicii electronice publice.
c. Testarea funcționării soluției instalate și configurate, la nivelul sistemului, cu setul de date de test agreat cu Beneficiarul astfel încât să fie acoperite cerințele specifice de sistem.
d. asigurarea expertizei în domeniul tehnic cu privire la aplicațiile web dezvoltate pe platforma de dezvoltare și administrare aplicații web, precum și participarea la activitățile de testare.
e. colaborarea cu ceilalți membrii ai echipei cu scopul de a asigura implementarea corectă

a cerințelor Beneficiarului.

f. documentarea configurărilor efectuate și transfer de cunoștințe către echipa de administrare IT din partea Beneficiarului.
g. Stabilirea și elaborarea curriculei pentru instruirea utilizatorilor standard privind funcționalitățile sistemului implementate.
h. Participarea la elaborarea documentației de instruire atât pentru utilizatorii standard cât și pentru administratorii sistemului.
i. Participarea la elaborarea documentațiilor de utilizare și administrare pentru soluția implementată.

Expertul coordonator dezvoltare aplicații web va îndeplini următoarele cerințe:

a. Studii superioare absolvite/finalizate cu diplomă de licență sau echivalent;
b. Certificare profesională eliberată sau atestată /recunoscută național/ internațional care să demonstreze specializarea în platforma de dezvoltare și administrare aplicații web propusă.
c. experiență specifică constând în implicarea în cel puțin un proiect/contract similar (prin proiect/contract similar se înțelege un proiect/contract de implementare a unei aplicații web platforma de dezvoltare și administrare aplicații web propusă) în care să fi îndeplinit același tip de activități sau similare cu cele pe care urmează să le îndeplinească în viitorul contract, probată prin scrisori de recomandare din partea beneficiarilor proiectelor sau copie după contractul respectivului proiect/contract, lista de personal a proiectului sau orice alte documente similare din cadrul cărora să reiasă experiența expertului propus etc. De asemenea, din documentele suport trebuie să reiasă clar activitățile similare celor specifice rolului din prezentul Contract, pe care le-a avut expertul în proiectul/proiectele respectiv/respective;
d. Declarație de disponibilitate pentru perioada aferentă activităților pe care și le asumă din prezentul contract.

8.1.6. Expert cheie nr. 6: Expert coordonator implementare sistem de management documente

Expertul coordonator implementare sistem de management documente va fi implicat în activitățile contractului pentru:

a. transpunerea în funcționalități a cerințelor documentate în etapele de analiză și proiectare
b. participarea la activitățile de instalare, dezvoltare/configurare a platformei de management documente oferite, pentru implementarea în bune condiții a componentelor/modulelor specifice ariilor funcționale identificate în etapa de analiză.
c. Testarea funcționării soluției instalate și configurate, la nivelul sistemului, cu setul de date de test agreat cu Beneficiarul astfel încât să fie acoperite cerințele specifice de sistem.

d. asigurarea expertizei în domeniul tehnic cu privire la platforma de management documente propusă, precum și participarea la coordonarea activităților de testare internă a prestatorului pentru sistem, înainte de testarea acesteia de către Beneficiar.
e. colaborarea cu ceilalți membrii din echipă pentru a asigura implementarea corectă a cerințelor Beneficiarului.
f. documentarea configurărilor efectuate și transfer de cunoștințe către echipa de administrare IT din partea Beneficiarului.
g. Stabilirea și elaborarea curriculei pentru instruirea utilizatorilor finali privind funcționalitățile sistemului implementate.
h. Participarea la elaborarea documentației de instruire atât pentru utilizatorii finali cât și pentru administratorii sistemului.
i. Participarea la elaborarea documentațiilor de utilizare și administrare pentru soluția implementată.

Expertul coordonator implementare sistem de management documente va îndeplini următoarele cerințe:

a. Certificare profesională atestată /recunoscută național/ internațional care să demonstreze specializarea în platforma de management documente propusă.
b. experiență specifică constând în implicarea în cel puțin un proiect/contract similar (prin proiect/contract similar se înțelege implementarea unui sistem informatic care să fi inclus o soluție software de management documente pe platforma propusă) în care să fi îndeplinit același tip de activități sau similare cu cele pe care urmează să le îndeplinească în viitorul contract, probată prin scrisori de recomandare din partea beneficiarilor finali ai proiectelor sau copie după contractul respectivului proiect/contract, lista de personal a proiectului sau orice alte documente similare din cadrul cărora să reiasă experiența expertului propus etc. De asemenea, din documentele suport trebuie să reiasă clar activitățile similare celor specifice rolului din prezentul Contract, pe care le-a avut expertul în proiectul/proiectele respectiv/respective;
c. Declarație de disponibilitate pentru perioada aferentă activităților pe care și le asumă din prezentul contract.

8.1.7. Expert cheie nr. 7: Expert coordonator testare

Expertul coordonator testare va fi implicat în activitățile contractului, având următoarele responsabilități:

a. coordonarea tuturor activităților de testare și a echipei de testare:
b. Testarea aplicațiilor software din punct de vedere tehnic, funcțional, performanță și identificarea posibilelor erori;
c. Testarea tuturor cerințelor din caietul de sarcini, și a celor identificate/detaliate în urma

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

desfășurării etapei de analiză și proiectare;

d. Analiza problemelor și recomandarea de soluții;
e. Identificarea, specificarea și implementarea îmbunătățirilor în ceea ce privește funcționarea soluțiilor software;
f. Crearea de scenarii de utilizare și scripturi de testare dacă e cazul;
g. Va conlucra îndeaproape cu ceilalți experți și cu echipa de implementare, fiind responsabil de testarea tehnică, funcțională și de performanță a întregii platforme;
h. Acesta va fi responsabil de elaborarea documentației de testare. De asemenea, are ca responsabilitate finală întocmirea Raportului de Testare a soluției.
i. Avizează documentațiile de proiectare și testare elaborate de către echipa Prestatorului pe durata derulării proiectului

Expertul coordonator testare va îndeplini următoarele cerințe:

a. Studii superioare absolvite/finalizate cu diplomă de licență sau echivalent;
b. Deținerea de competente avansate privind stabilirea activităților optime de testare pe baza efectuării analizei sistemelor informatice și realizarea testelor în funcție de metodologia specifica de dezvoltare a software-ului suspus respectivelor teste (dovedite prin participarea la cel puțin un program de perfecționare în acest domeniu și prezentarea diplomei / certificării aferente recunoscuta la nivel național / internațional, cum ar fi cele echivalente cu ISTQB);
c. Experiență specifică constând în implicarea în cel puțin un proiect/contract similar (prin proiect/contracte similar se înțelege implementarea unui sistem informatic), în care să fi îndeplinit același tip de activități sau similare cu cele pe care urmează să le îndeplinească în viitorul contract, probată prin scrisoare/scrisori de recomandare de la Beneficiarul/Beneficiarii, documentații tehnice aferente implementării sau orice alte documente similare care să ateste activitățile desfășurate în cadrul unui astfel de proiect, precum și informații relevante referitoare la metodele/tehnologiile utilizate în activitatea de testare.
d. declarație de disponibilitate pentru perioada aferentă activităților pe care și le asumă din prezentul contract.

8.1.8. Expert cheie nr. 8: Coordonator instruire pentru utilizare și administrare

Expertul coordonator instruire pentru utilizare și administrare va fi implicat în activitățile contractului privind:

a. Coordonarea întocmirii materialelor de curs.
b. Colaborarea cu ceilalți experți din echipă cu scopul de a asigura documentația de instruire si programele de formare a utilizatorilor și administratorilor.
c. planificarea și desfășurarea ședințelor de instruire
d. analizarea modului de organizare și desfășurare a cursurilor

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

e. monitorizarea/verificarea permanentă și evaluarea punctuală a atingerii rezultatelor echipei de experți formatori, pentru îndeplinirea contractului și obiectivelor stabilite la termenele prevăzute în graficul Gantt al contractului.

Expertul Coordonator instruire pentru utilizare și administrare va îndeplini următoarele cerințe:

a. Studii superioare absolvite/finalizate cu diplomă de licență sau echivalent;
b. pregătire de specialitate în domeniul formării profesionale a adulților, probată prin certificat de absolvire a cursului de specializare ”Formator” Cod COR – 242401 sau ”Formator de formatori ”, Cod COR – 242402 sau echivalent;
c. experiență specifică constând în implicarea în cel puțin un proiect/contract similar (prin proiect/contract similar se înțelege implementarea unui sistem informatic) în care să fi îndeplinit același tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract, probată prin scrisori de recomandare din partea beneficiarilor finali ai proiectelor sau copie după contractul respectivului proiect/contract, lista de personal a proiectului sau orice alte documente similare din cadrul cărora să reiasă experiența expertului propus etc. De asemenea, din documentele suport trebuie să reiasă clar activitățile similare celor specifice rolului din prezentul Contract, pe care le-a avut expertul în proiectul/proiectele respectiv/respective;
d. Declarație de disponibilitate pentru perioada aferentă activităților pe care și le asumă din prezentul contract.

8.1.9. Expert cheie nr. 9: Expert stocare și protecție copii de siguranță

Expertul în stocare și protecție copii de siguranță va fi implicat în activitățile contractului privind:

a. Analiza infrastructurii existente și stabilirea cerințelor de implementare pentru noul sistem;
b. Proiectarea configurării soluției de stocare și protecție copii de siguranță;
c. Efectuarea configurărilor necesare pentru implementarea soluției;
d. Documentarea configurărilor/dezvoltărilor efectuate;
e. Participarea la instruirea administratorilor și întocmirea documentațiilor de administrare a soluției de stocare și protecție copii de siguranță;
f. Colaborarea cu responsabilii tehnici ai fiecărei componente a sistemului și cu ceilalți experți pentru implementarea sistemului în conformitate cu cerințele Beneficiarului și documentația de proiectare.

Expertul în stocare și protecție copii de siguranță va îndeplini următoarele cerințe:

a. Certificare profesională eliberată sau atestată /recunoscută național/ internațional de un producător de tehnologie care să demonstreze specializarea în soluția de realizare a copiilor de siguranță propusă.
b. Experiență specifică constând în implicarea în cel puțin un proiect/contract similar (prin proiect/contract similar se înțelege implementarea unui sistem informatic care să fi inclus soluția de realizare a copiilor de siguranță propusă), probată prin scrisoare/scrisori

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

de recomandare de la Beneficiarul/Beneficiarii, documentații tehnice aferente implementării sau orice alte documente similare care să ateste rolul, activitatea desfășurată în cadrul unui astfel de proiect, precum și informații relevante referitoare la soluție (produs software implementat, descriere soluție).

c. Declarație de disponibilitate pentru perioada aferentă activităților pe care și le asumă din prezentul contract.

8.2. Alte condiții referitoare la calificarea experților

Ofertanții trebuie să prezinte în oferta tehnică, pentru fiecare expert cheie solicitat, următoarele informații/ documente:

- CV – în format Europass;
- Copii ale documentelor relevante care să demonstreze îndeplinirea cerințelor referitoare la studii, expertiză și experiență specifică relevantă solicitată și prezentată în CV, cum ar fi:
  - Diplome, certificate de absolvire, certificări, atestate sau orice alte documente similare prin care să se demonstreze pregătirea/calificarea solicitată; pentru experții nerezidenți vor fi acceptate documentele menționate anterior emise în țara de rezidență, însoțite de traducere autorizată.
  - Referințe/ recomandări emise beneficiarul proiectului/contractului, semnate, sau alte documente edificatoare din care sa reiasa activitatile desfasurate, care să probeze experiența în domeniile cerute și care să evidențieze experiența profesională specifică similară, astfel cum au fost detaliate în cadrul capitolului 8.1
- Declarație de disponibilitate semnată de persoana propusă

Autoritatea contractantă își rezervă dreptul de a:

- verifica exactitatea informațiilor și a dovezilor furnizate de ofertanți și de a solicita și alte documente/ informații care să clarifice experiența echipei de proiect propusa;
- contacta beneficiarii proiectelor/ contractelor prezentate la experienta profesionala, în vedere confirmarii celor prezentate de către ofertanți.

Notă: Achizitorul va lua în considerare experiența dobândită în proiectele similare aflate în desfășurare, dacă serviciile similare prestate au fost confirmate și recepționate de Beneficiar.

Prin similitudine, se includ în cadrul experienței specifice a experților dezvoltările parțiale, până la Milestone-uri specifice din cadrul unor Contracte în derulare, cu condiția ca prestarea serviciilor de dezvoltare și implementare de sisteme/aplicații informatice să fi fost confirmată de Beneficiar în cadrul unor recepții parțiale.

În accepțiunea Achizitorului, pentru evaluarea experienței similare a experților, noțiunea de proiect se referă la existența unui cadru reglementat juridic prin care un expert a derulat în mod coerent (având o finalitate bine precizată și atinsă) tipul de activități care sunt de interes pentru evaluare.

Pentru a demonstra că îndeplinesc cerințele minime obligatorii, experții propuși vor depune copii după documente.
Certificatele emise în altă limbă decât româna, vor fi însoțite de traduceri autorizate ale acestora.
O persoană desemnată să facă parte din echipa de experți-cheie ai Contractului poate îndeplini un singur rol în cadrul echipei de experți-cheie.
Este în sarcina operatorului economic să se asigure că diplomele / certificările / atestările / acreditările sau alte documente similare, în domeniu, sunt eliberate de către o organizație / organism de drept public sau privat care respecta standardele naționale sau internaționale de certificare.
Furnizorul trebuie să se asigure că niciunul dintre experți nu se află în conflict de interese în ceea ce privește participarea lor la activitățile din cadrul contractului. Toate persoanele propuse vor depune declarații pe proprie răspunde în acest sens.
Experții sunt obligați să respecte confidențialitatea informațiilor pe parcursul implementării proiectului.

8.2.1. Personalul administrativ și personalul suport/backstopping pentru activitatea experților cheie în cadrul Contractului

Ofertantul va furniza întreg personalul suport/auxiliar (personal administrativ sau, după caz, alți experți) necesar îndeplinirii corespunzătoare a obligațiilor ce îi revin pe întreaga perioadă de derulare a contractului. Ofertantul este responsabil în exclusivitate și integral pentru stabilirea componenței echipei de proiect, pentru organizarea tuturor experților propuși, precum și pentru depunerea efortului necesar desfășurării în bune condiții a tuturor activităților solicitate prin prezentul document.

8.2.2. Alte cerințe legate de personalul direct implicat în prestarea serviciilor

Contractantul nu va face schimbări de personal fără aprobarea Achizitorului.
Înlocuirea oricărui expert cheie se realizează ca urmare a notificării Contractantului în acest sens și aprobării subsecvente de către Achizitor. Este recomandat ca înlocuirea acestora să se facă numai în cazuri excepționale (de ex: demisie sau ineficiență în implementare, caz de boală, accident, etc.), cu îndeplinirea tuturor cerințelor privind criteriile de selecție pentru experiența profesională a experților/ formatorilor, calificările și experiența profesională a experților cheie din cadrul echipei de implementare pe baza cărora s-a selectat candidatul.
Pentru înlocuirea unui expert, Contractantul va avea în vedere prevederile art. 162 alin. (1), lit. b) din HG nr. 395/2016, respectiv va transmite, în maxim 5 zile lucrătoare de la luarea la cunoștință a situațiilor invocate mai sus, , însoțite de adresă de înaintare, documentele pentru noul expert propus solicitate prin documentația de atribuire, fie în vederea demonstrării îndeplinirii criteriilor de calificare/selecție stabilite, fie în vederea calculării punctajului aferent factorilor de evaluare.
În termen de 5 zile lucrătoare de la primirea documentelor, Achiziorul va analiza documentele primite și corespondența acestora cu cerințele minime din documentația de atribuire pentru experții care nu au constituit factor de evaluare, respectiv cu cerințele minime și punctajul obținut în etapa

de evaluare de către expertul care urmează a fi înlocuit, pentru experții care au constituit factor de evaluare. Pentru această a doua categorie de experți, noul expert propus trebuie să obțină un punctaj cel puțin egal cu cel al expertului pe care îl înlocuiește.
În cazul în care documentele prezentate corespund cerințelor, așa cum este descris mai sus, Achizitorul comunică formal Contractantului, în termenul precizat anterior aprobarea noului expert.
În cazul în care documentele prezentate necesită completări, Contractantul are obligația ca în 3 zile lucrătoare la primirea solicitării de completare din partea Achizitor să transmită elementele lipsă. În cazul în care acestea nu pot fi furnizate, în același termen de 3 zile Contractantul este obligat să prezinte o nouă propunere de înlocuire care va parcurge procesul descris anterior. Dacă nici de această dată expertul propus nu corespunde cerințelor minime, respectiv nu îndeplinește punctajul minim, contractul va fi reziliat.
În cazul în care membrul echipei cu rol de personal-cheie nu este înlocuit imediat și responsabilitățile acestuia urmează să fie preluate după un anumit interval de timp de către noul personal cheie, Autoritatea Contractantă poate solicita Contractantului să desemneze o persoană care să îndeplinească rolul de personal-cheie temporar, până la sosirea noului personal-cheie, sau să ia alte măsuri pentru a compensa absența temporară a personalului-cheie care nu poate fi înlocuit (absent). Indiferent de situație, Autoritatea Contractantă nu va efectua nici o plată pentru perioada absenței personalului-cheie sau a absenței înlocuitorului acestuia.
Toate costurile generate de înlocuirea personalului sunt exclusiv în sarcina Contractorului.

8.2.3. 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.
Pentru îndeplinirea cu succes a activităților descrise, Contractantul va pune la dispoziția echipei de proiect proprii toate resursele materiale necesare. În mod minimal, fiecare expert va avea la dispoziție un echipament de calcul portabil, pe care va exista instalat software tip office (editor de text, program de calcul tabelar, instrument de realizare prezentări grafice etc.).
De asemenea, Contractantul va pune la dispoziție următoarele:

- Hardware necesar pentru prestarea serviciilor;
- Instrumente software pentru prestarea serviciilor.

Contractantul are obligația ca toate instrumentele software utilizate pentru îndeplinirea contractului (producerea livrabilelor necesare) să fie licențiate conform prevederilor legale în vigoare și în funcție de tipul de instrument folosit, modul de licențiere recomandat de producător, număr de utilizatori etc.

8.2.4. Infrastructura și resursele disponibile la nivel de Autoritate Contractantă pentru îndeplinirea Contractului

În situația în care va fi necesar, pentru derularea proiectului în bune condiții, CNCD va pune la dispoziție Contractantului următoarele:

- Spațiu în sediul propriu;
- Dotările permanente ale CNCD – mobilier, linii de comunicații, etc.;
- De asemenea, cheltuielile administrative (energie electrică, termică, comunicații, etc.) vor fi suportate de către CNCD.

9. Cadrul legal care guvernează relația dintre Autoritatea Contractantă și Contractant (inclusiv în domeniile mediului, social și al relațiilor de muncă)

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.

În acest sens, Ofertantul va prezenta o declarație din care să rezulte faptul că la elaborarea ofertei a ținut cont de obligațiile relevante din domeniile mediului, social și al relațiilor de muncă. Instituțiile competente de la care operatorii economici pot obține informațiile detaliate privind obligațiile relevante din domeniile mediului, social și al relațiilor de muncă sunt Ministerul Mediului și Ministerul Muncii, Familiei, Protecției Sociale și Persoanelor Varsnice și de la Inspectoratele Teritoriale de Munca, respectiv și - site-ul: http://www.anpm.ro/web/guest/legislatie;

http://www.inspectmun.ro/legislatie/ legislatie.html.

10. Managementul/Gestionarea Contractului și activități de raportare în cadrul Contractului

10.1. Plan de livrare produse și prestări servicii

Activitățile în cadrul Contractului se vor desfășura conform unui ”Plan de livrare produse și prestări servicii” propus de către Ofertant în cadrul ofertei și care trebuie să respecte calendarul de implementare din capitolul 5.9.8 al prezentului Caiet de sarcini.

Derularea contractului începe după data semnării acestuia de către ambele părți. Perioada de execuție a contractului va fi de maxim 12 de luni.

Ofertanții vor prezenta ”Planul de livrare produse și prestări servicii” avut în vedere pentru toată durata contractului, în format Gantt, incluzând cel puțin următoarele:

a. Toate fazele/etapele descompuse în activitățile necesare pentru implementarea cu succes a contractului, inclusiv dependențele dintre acestea, respectiv rezultatele acestora;
b. Activitățile trebuie prezentate sub formă etapizată și să se înscrie în constrângerile de timp ale contractului. Activitățile se vor planifica cu o granularitate de cel mult 1 lună pe întreaga perioadă de derulare a proiectului, astfel încât să fie posibilă urmărirea eficientă a evoluției implementării.
c. Evidențierea jaloanelor;
d. Distribuția resurselor umane (experți) pe activități care trebuie să conveargă la obiectivele contractului.

Graficul Gantt va fi realizat cu un instrument software de planificare a activităților care să permită stabilirea duratelor și a dependențelor și calcularea și evidențierea căii critice a proiectului, precum și replanificarea automată a activităților în cazul decalării unor termene (fără a fi necesară replanificarea manuală a tuturor activităților care depind de activitatea care a suferit decalaje). Nu este permisă utilizarea în cadrul graficului Gantt a unor constrângeri de start sau de finalizare având la bază momente de timp arbitrar alese. Toate activitățile, cu excepția primei activități a proiectului, care nu va avea predecesor, vor avea dependențe de clar identificate de alte activități. Singura activitate fără succesor va fi ultima activitate a proiectului.

Planul de livrare produse și prestări servicii va fi însoțit de o secțiune descriptivă în cadrul căreia vor fi detaliate toate elementele indicate în cadrul acestuia, respectiv va cuprinde descrierea detaliată și explicită a metodologiei/programului (planul) de lucru conceput pentru execuția contractului pentru toate activitățile precizate în plan (detaliere grafic de execuție).

Ofertantul va trata inclusiv modul de luare și ierarhizare a deciziilor, cu indicarea deciziilor care se iau de Furnizor cu deplină autoritate și a deciziilor care se iau de către Achizitor, pe baza propunerilor făcute de Furnizor.

Ofertantul va prezenta o descriere detaliată care va conține, după caz, și planul de lucru cu asociații/subcontractanții în raport cu eventualele activități care urmează să fie derulate de către fiecare asociat/subcontractant în parte (conținând toate datele de identificare a entităților care vor fi

incluse în contract).

10.2. Abordare și metodologie în cadrul Contractului

Ofertantul va trebui să prezinte în cadrul ofertei modul de organizare a activității sale pentru a finaliza fazele de execuție. De asemenea, va descrie detaliat metodele folosite în cadrul contractului, principalele activități legate de organizarea contractului, experții cheie, programul și livrabilele. Descrierea trebuie sa fie suficient de clară și concretă astfel încât să se poată identifica rezultatele pentru fiecare activitate.

Propunerea tehnică va conține cel puțin următoarele:

a. Viziunea proprie asupra realizării contractului, din care sa reiasă modul în care a înțeles contextul și scopul acestuia;
b. Identificarea aspectelor principale legate de îndeplinirea obiectivelor contractului și a rezultatelor așteptate și o scurtă descriere a acestora;
c. Ofertantul va prezenta detaliat metodologia de management de proiect utilizată.

10.2.1. Organizarea

Ofertantul va prezenta organizarea și responsabilitățile fiecărei părți implicate în contract, inclusiv propunerile pentru organizarea Achizitorului.

Ofertantul va descrie facilitățile suport pe care experții implicați le vor avea din partea ofertantului pe timpul execuției contractului.

10.2.2. Monitorizare și control

Ofertantul va detalia modul în care va realiza monitorizarea și raportarea astfel încât să asigure derularea cu succes a contractului.

10.2.3. Registrul riscurilor

Ofertantul va identifica potențialele riscuri, pe baza experienței proprii din proiecte similare. Se vor identifica riscuri din categorii diferite, care necesită abordări diferite și va detalia impactul riscurilor identificate și se va prezenta posibile măsuri de remediere în vederea micșorării acestui impact.

10.3. Atribuțiile și responsabilitățile părților

Contractantul va avea obligația ca pentru produsele software livrate, să obțină din timp în numele Achizitorului, sau să transfere acestuia, prin documente cu caracter juridic, licențele necesare pentru utilizarea acestora conform contractului. Aceasta prevedere se aplică tuturor componentelor/resurselor licențiate și/sau sub licențiate, componentelor software comercializate de Contractant, componentelor software ale unor terți, componentelor pre-existente, uneltelor software necesare livrării, monitorizării și mentenanței ș.a.m.d.

Contractantul va prezenta documente care dovedesc faptul că software-ul în ansamblul său este supus sau nu unor politici de licențiere (inclusiv se vor avea în vedere utilitarele și uneltele furnizate integrat ca parte a soluției/software-ului precum și pentru orice adaptare, îmbunătățire, adăugare sau modificare a software-ului unor terți care este inclus în soluția furnizată). Documentele

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

justificative trebuie să fie clare, să permită identificarea tipului de licențiere, metodele de calcul (fie virtual, fizic, grad de încărcare, număr de utilizatori etc.), condițiile de utilizare, perioada de timp precum și orice altă informație valabilă la momentul contractării). Orice diferend juridic ulterior cu un terț pe subiectul drepturilor de proprietate intelectuală va cădea în sarcina și responsabilitatea Contractantului.

Ofertantul va include în oferta sa licențe (drepturi de utilizare pentru Autoritatea Contractantă) pentru toate componentele software livrate. Licențierea poate fi perpetuă sau de tip abonament. În cazul licențierii perpetue, se vor include și costurile suportului tehnic în condițiile stipulate în prezentul caiet de sarcini în capitolul.

În cazul licențierii de tip abonament, dacă nu s-a prevăzut altfel în curpinsul prezentului caiet de sarcini, Autoritatea Contractantă va dobândi un drept de utilizare pentru o perioadă de 5 ani de la recepție, incluzând și costurile suportului tehnic în condițiile stipulate în prezentul caiet de sarcini în capitolul.

Contractantul va avea obligația ca transferul drepturilor de folosință, și al oricăror drepturi conexe către Achizitor va avea loc de la data plății Achizitorului.

Contractantul va avea obligația să despăgubească Achizitorul împotriva oricăror: a) reclamații și acțiuni în justiție, ce rezultă din încălcarea unor drepturi de proprietate intelectuală (brevete, nume, mărci înregistrate etc.) și b) daune-interese, costuri, taxe și cheltuieli de orice natură, aferente, cu excepția situației în care o astfel de încălcare rezultă din respectarea caietului de sarcini întocmit de către Achizitor.

Toate documentele și informațiile primite de la Ofertant precum și rezultatele tuturor activităților Contractantului din contract (cum ar fi: documente de analiză, arhitecturi de sisteme, adrese, etc., fără a se limita la acestea) reprezintă informații confidențiale, iar Ofertantul câștigător va asigura respectarea confidențialității lor.

Contractantul și personalul său au obligația de a respecta confidențialitatea documentelor și informațiilor menționate mai sus, pe toată perioada executării contractului, pe perioada oricărei prelungiri a acestuia și după încetarea contractului.

Toate documentele, rapoartele și datele, inclusiv diagrame, scheme tehnice, specificații tehnice, planuri și orice alte materiale realizate de către Contractant în cadrul contractului, trec în proprietatea /proprietatea intelectuală a Achizitorului, aceasta având dreptul să le utilizeze, modifice, transfere fără acceptul Contractantului sau al unei terțe părți. Contractantul le va furniza Achizitorului, la finalizarea contractului, fără a le utiliza în alte scopuri care nu au legătura cu contractul.

Contractantul nu va publica articole sau informații legate de serviciile prestate, nu va face referire la acestea în cazul prestării altor servicii către terți și nu va divulga informațiile obținute de la Achizitor, fără acordul scris al acesteia.

Orice rezultate sau drepturi legate de acestea, inclusiv drepturi de proprietate intelectuală sau industrială, obținute în cadrul contractului, sunt proprietatea Achizitorului, care poate dispune de ele după cum consideră.

Achizitorul va asigura accesul reprezentanților Contractantului în locațiile în care se vor efectua activitățile de livrare, instalare, punere în funcțiune și testare a produselor, precum și condițiile necesare efectuării acestora, astfel cum vor fi stabilite prin Contract.

10.4. Gestionarea relației dintre Contractant și Achizitor

Fiecare parte contractantă are obligația coordonării propriilor resurse și a activităților pentru derularea contractului, în conformitate cu atribuțiile precizate în prezentul caiet de sarcini.

Achizitorul și Contractantul identifică acțiunile corective pentru abordarea abaterilor constatate față de prevederile contractului.

Pe parcursul derulării contractului, Achizitorul verifică dacă toate activitățile planificate au fost realizate conform clauzelor contractuale. Achizitorul se asigură pe toată perioada derulării contractului și nu doar la finalizarea/terminarea acestuia că activitățile planificate au fost realizate, cerințele stabilite au fost îndeplinite, serviciile au fost prestate, soluția informatică implementată a fost admisă la recepție și instruirea personalului a fost finalizată.

Contractantul este responsabil în totalitate de asigurarea managementului contractului din punct de vedere administrativ și financiar, sens în care va fi orientat spre obținerea rezultatelor stabilite pentru îndeplinirea obiectivelor. Acesta trebuie să respecte condițiile formulate în contract.

10.5. Raportarea în cadrul contractului

La demararea contractului, va avea loc o reuniune între echipa propusă de Contractant și reprezentanții Achizitorului pentru a se stabili:

a. principiile de comunicare reciprocă finalizate printr-un plan de comunicare întocmit de Contractant și validat de Achizitor;
b. graficul de desfășurare a activităților;
c. detaliile privind colaborarea;
d. frecvența reuniunilor;
e. modelele de procese-verbale;
f. planurile de acțiune în cazul apariției unor probleme;
g. alte detalii logistice și organizaționale.

La finalul reuniunii se va întocmi o minută, ce va cuprinde toate aspectele stabilite în această întâlnire.

Contractantul va elabora rapoarte trimestriale prin care să prezinte evoluția activităților și întârzierile, dacă acestea sunt semnificative. Rapoartele trimestriale vor detalia:

a. Progresele înregistrate;
b. Activități aflate în derulare cu data estimativă a finalizării acestora și cu rezultatele anticipate;
c. Dificultățile întâmpinate în cursul implementării proiectului și soluțiile propuse pentru a depăși respectivele dificultăți;
d. Rezultatele realizate în cursul perioadei de raportare, resursele utilizate, precum și recomandările sau solicitările aferente, și planificarea activităților pentru perioada

următoare.

Contractantul trebuie să consulte Achizitorul cu privire la oricare aspect/problemă care apare în procesul de implementare. Contractantului i se poate cere să participe la întâlniri periodice, pentru a comunica problemele identificate și pentru a găsi soluții optime. De asemenea, acesta va lua toate măsurile pentru a comunica în timp util, toate problemele identificate, în vederea evitării riscurilor rezultate din activitatea prestată.

Achizitorul (prin echipa de management a proiectului condusă de Managerul de Proiect) va fi responsabil de monitorizarea activităților desfășurate de Contractant, de punerea în aplicare a rezultatelor acestui contract și de monitorizarea activităților derulate.

Contractantul va avea nevoie de aprobarea prealabilă a Achizitorului pentru livrabile, precum și pentru materialele elaborate în cadrul contractului.

Toate comunicatele/raportările și documentele vor fi transmise către Achizitor, care analizează activitatea Contractantului și formulează eventuale recomandări în legătură cu implementarea contractului în vederea avizării/aprobării documentelor respective.

10.6. Evaluarea performanței Contractantului

Performanța Contractantului va fi evaluată pe baza livrabilelor contractului, luându-se în considerare caracterul corect și complet al livrabilelor aferente prestării serviciilor din cadrul contractului, astfel:

- Foarte bine – Livrabilele au putut fi folosit cu succes pentru realizarea activităților din implementare. Nu au fost necesare modificări majore ale livrabilelor transmise de către Contractant ca urmare a observațiilor formulate de Autoritatea Contractantă.
- Bine – Livrabilele au putut fi folosit cu succes pentru realizarea activităților din implementare. Au fost necesare ajustări nemateriale ca urmare a observațiilor formulate de Autoritatea Contractantă pentru livrabilele transmise de către Contractant. S-a răspuns în timp util și adecvat la toate observațiile adresate de Autoritatea Contractantă. Nu au existat solicitări majore ale Contractantului pentru prelungirea termenelor din cauza lipsei de claritate sau a existentei neconcordantelor sau erorilor în livrabile.
- Acceptabil – Livrabilele au putut fi folosite pentru realizarea activităților din implementare. Au fost necesare câteva ajustări/corecturi ca urmare a observațiilor formulate de Autoritatea Contractantă. Cu toate acestea observațiile au fost abordate adecvat. Nu au existat solicitări ale Contractantului pentru prelungiri semnificative ale termenelor din cauza lipsei de claritate sau a existentei neconcordantelor sau erorilor în livrabile.
- Nesatisfăcător – Livrabilele au putut fi folosite pentru realizarea activităților din implementare doar după ce conținutul acestora a fost semnificativ modificat și corectat de Contractant ca urmare a observațiilor adresate de Autoritatea Contractantă ceea ce a condus la întârzieri ale activităților din calendarului general al proiectului (ex. proiectul nu a putut fi finalizat la timp). Implementarea a fost finalizata cu întârzieri majore din cauza lipsei de claritate sau a existentei neconcordantelor în livrabile.

Contractantul va ține evidența valorilor asociate indicatorilor de performanță și va include informații referitoare la nivelul de performanță înregistrat în toate rapoartele și documentele întocmite pentru realizarea întâlnirilor de pe durata derulării contractului, așa cum sunt acestea descrise în Caietul de sarcini.

11. Recepția produselor și serviciilor

Recepția produselor și serviciilor se va realiza conform „Planului de livrare produse și prestări servicii” întocmit de Contractant conform prevederilor capitolului 5.9.8. din prezentul document.

11.1. Recepția produselor

Dreptul Achizitorului de a inspecta, testa și, dacă este necesar, de a respinge produsele, nu va fi limitat sau amânat din cauza faptului că produsele au fost inspectate și testate de Contractant, anterior furnizării acestora la locația de livrare/instalare.

Transferul drepturilor de proprietate și/ sau folosința, și al oricăror drepturi conexe către Achizitor va avea loc de la data recepției calitative.

Recepția produselor se va efectua pe baza de proces verbal semnat de Contractant și Achizitor și va consta în recepție cantitativă, recepție calitativă respectiv proces verbal de punere in functiune după cum urmează:

A. Recepția cantitativă a produselor se va realiza după livrarea produselor în cantitatea solicitată la locația indicată de Achizitor și va consta în efectuarea următoarelor operațiuni:
   - numărare bucată cu bucată a echipamentelor, componentelor și a accesoriilor acestora;
   - verificarea aspectului exterior, a integrității fizice și a caracteristicilor constructive;
   - verificarea existenței tuturor componentelor și accesoriilor;
   - verificarea existenței documentelor de însoțire a mărfii (aviz de însoțire a mărfii/ aviz de expediție etc.);
   - verificarea existenței documentației tehnice aferente fiecărui tip de echipament;
   - verificarea existenței certificatelor de garanție
   - verificarea existenței documentelor de licențiere pentru software-ul livrat;
   - verificarea suporților optici/USB (sau alte tipuri de suporți care permit Autorității contractante arhivarea și păstrarea produselor achiziționate) pe care sunt inscripționate produsele software;
   - întocmirea unui Proces verbal de recepție cantitativă (PVRcant.) între reprezentanții părților, în care se va consemna îndeplinirea tuturor operațiunilor descrise mai sus;
   - Achizitorul își rezervă un termen de maxim 5 zile lucrătoare pentru realizarea recepției cantitative.

B. Recepția calitativă se va realiza după finalizarea activităților aferente prezentate în secțiunile 5.9.1 și 5.9.2 din prezentul document și va consta în efectuarea următoarelor operațiuni:

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

- verificarea semnării procesului verbal de recepție cantitativă;
- verificarea instalării și electroalimentării echipamentelor livrate;
- verificarea aplicării pe echipamente a etichetelor autocolante cu respectarea regulilor de vizibilitate conform Ghidului de identitate vizuală „Vizibilitate, transparență și comunicare în perioada de programare 2021—2027” publicat la https://mfe.gov.ro/pocidif/identitate-vizuala-program-pocidif/;
- verificarea configurării hardware-software a echipamentelor livrate;
- verificare conexiuni fizice în rack: etichetare, documentare și cosmetizare;
- verificarea funcționalităților de disponibilitate prin realizare teste de redundanță (alimentare, conectivitate, calcul/stocare, HA failover, replicare/restaurare date);
- verificarea conformității produselor livrate cu specificațiile tehnice din Caietul de sarcini și din Propunerea tehnică, prin efectuarea de inspecții și teste funcționale. Inspecțiile și testele funcționale din cadrul recepției vizează respectarea cerințelor Caietului de sarcini și a specificațiilor Producătorului (caracteristici tehnice, constructive, electrice, cerințele funcționale etc.);
- testările funcționale din cadrul recepției se vor efectua pe baza unui set de teste, teste care vor fi propuse de către contractant și agreate de Autoritatea contractantă;
- verificarea versiunii codurilor software instalate, a licențelor corespunzătoare acestora, astfel încât la finalizarea recepției calitative Autoritatea contractantă să se asigure că va deține toate documentele juridice privind licențele proprii sau cele din partea terților;
- verificarea Raportului de instalare.
- întocmirea unui Proces Verbal de Recepție Calitativă (PVRcal.) între reprezentanții părților, în care se va consemna îndeplinirea tuturor operațiunilor descrise mai sus;
- Achizitorul își rezervă un termen de maxim 5 zile lucrătoare pentru realizarea recepției calitative a produselor.

Procesul verbal de recepție calitativă va include unul din următoarele rezultate:

- acceptat;
- refuzat.

În cazul procesului verbal de recepție calitativă refuzat, Contractantul va analiza observațiile primite și va efectua modificările solicitate în termen maxim de 5 zile lucrătoare, după care se va relua procedura de recepție a acestora.

11.2. Recepția serviciilor

Recepția serviciilor solicitate se va realiza conform fazelor definite în „Planul de livrare produse și prestări servicii”. Fiecare fază sau etapă, după caz, se va finaliza cu întocmirea unui Proces verbal de recepție cantitativă și calitativă fază sau etapă, după caz, se va verifica existența, conformitatea și completitudinea livrabilelor aferente prestării serviciilor cu specificațiile contractuale și specificațiile tehnice minimale ale caietului de sarcini și ale ofertei câștigătoare.

Achizitorul va stabili dacă documentele/livrabilele sunt complete și respectă cerințele minime din

documentele contractuale și condițiile/cerințele detaliate rezultate ca urmare a evaluărilor/analizelor efectuate de Achizitor. Totodată, se va verifică că livrabilele documentare respectă regulile de vizibilitate conform Ghidului de identitate vizuală pentru Programul Regional Sud-Muntenia 2021-2027 publicat la https://mfe.gov.ro/pocidif/identitate-vizuala-program-pocidif/

Achizitorul are dreptul de a verifica modul de prestare a serviciilor pentru a stabili conformitatea cu prevederile documentelor contractuale și din cele rezultate ca urmare a evaluării, în termen de 5 (cinci) zile lucrătoare de la primirea livrabilelor.

Recepția livrabilelor se va realiza de către o comisie formată din reprezentanți ai Achizitorului.

În situația în care comisia de recepție constată că sunt îndeplinite cerințele solicitate prin documentele contractuale și din cele rezultate ca urmare a evaluărilor, se va întocmi proces-verbal de recepție cantitativă și calitativă, care va fi semnat de către membrii din comisia de recepție și de către reprezentanții Contractantului.

Contractantul are obligația de a depune livrabilele, în vederea recepției, înainte de termenul limită de prestare a fiecărei faze sau etape, după caz, astfel încât să includă perioada de verificare de către Achizitor (5 zile lucrătoare), precum și cea necesară remedierii eventualelor deficiențe (3 zile lucrătoare).

După semnarea de către membrii din comisia de recepție și de către reprezentanții Contractantului a proceselor-verbale de recepție cantitativă și calitativă, aferente tuturor fazelor definite în „Planul de livrare produse și prestări servicii”, în termen de cel mult 5 zile lucrătoare de la semnarea ultimului proces verbal de recepție cantitativă și calitativă, se va întocmi un Proces verbal de recepție finală (PVRfin.) între reprezentanții părților, în care se va consemna obținerea tuturor rezultatelor contractului.

12. Modalități și condiții de plată

Plata se va efectua, în tranșe corespunzătoare jaloanelor definite în „Planul de livrare produse și prestări servicii” realizat pe baza calendarului de implementare prezentat în capitolul 10.1 al prezentului caiet de sarcini.

Contractantul va emite facturi pentru produsele livrate și serviciile prestate, conform tranșelor de plată. Facturile vor avea menționat numărul Contractului, datele de emitere și de scadența. Facturile vor detalia cantitativ / valoric produsele furnizate și serviciile prestate și vor prezenta prețul unitar al acestora. Facturile vor fi transmise către achizitor prin portalul eFactura.

Facturile vor fi emise după semnarea de către Achizitor a proceselor verbale de recepție calitativă, respectiv recepție cantitativă și calitativă, acceptate, pentru fiecare fază/etapă corespunzătoare jaloanelor definite în „Planul de livrare produse și prestări servicii”.

Plățile se vor efectua în conformitate cu prevederile art. 6 alin. (1) lit. c) din Legea nr. 72/2013 privind măsurile pentru combaterea întârzierii în executarea obligațiilor de plată a unor sume de bani rezultând din contracte încheiate între profesioniști și între aceștia și Achizitori.

Plățile se vor efectua în lei, în contul Contractantului, în baza facturilor fiscale însoțite de procesele-

verbale de recepție calitativă, semnate de reprezentanții ambelor părți.

13. Metodologia de evaluare a Ofertelor prezentate

13.1. Modul de prezentare al ofertelor tehnice

Toate specificațiile tehnice din prezentul Caiet de sarcini sunt obligatorii și minimale pentru toți ofertanții.

Propunerea tehnică, inclusiv documentele anexă (cu excepția documentațiilor tehnice ale producătorilor care sunt în limba engleză), în cazul în care sunt emise în altă limbă decât română, vor fi transmise în limba de origine, însoțite de o traducere autorizată a acestora în limba română. În cazul în care certificatele/diplomele/documentele care confirmă experiența profesională indicată sunt emise în altă limbă decât româna, acestea vor fi transmise în limba de origine, însoțite de o traducere autorizată a acestora în limba română.

Prin propunerea tehnică depusă, ofertantul are obligația de a face dovada conformității serviciilor și produselor care urmează a fi prestate și livrate cu cerințele prevăzute în caietul de sarcini.

Propunerea tehnică va fi prezentată întro formă narativă, în care ofertanții vor include în ordine următoarele capitole:

1. Descrierea arhitecturii soluției propuse suficient de detaliată astfel încât să se poată verifica îndeplinirea tuturor cerințelor privind arhitectura din caietul de sarcini

2. Lista produselor hardware (echipamentelor) ofertate specificând în clar identificatorul unic producător (part-number) asociat fiecărui echipament, numărul de echipamente ofertate pentru fiecare tip de echipament, configurația acestora, precum și corelarea acestora cu cerințele caietului de sarcini. Toate echipamentele ofertate vor trebui să fie regăsite în oferta financiară. Se va completa în oferta tehnică un tabel ce cuprinde următoarele informații:

Nr. Crt.	Denumire echipament (*)	Producător	Echipament propus (**)	Cod echipament (***)	Cantitate

Note:

(*) Denumirea echipamentului conform Caietului de Sarcini.

(**) Denumirea completă dată de producător. Se va insera câte un singur produs pe un rând.

(***) Va conține codul echipamentului provenit de la producător care permite identificarea unică a echipamentului.

3. Lista produselor software ofertate, specificând în clar numele licenței de la producător, ediția, producătorul, cantitatea și unitățile de licențiere specifice producătorului precum „User” sau „Processor Core” precum și corelarea acestora cu cerințele caietului de sarcini. Lista licențelor trebuie să cuprindă toate licențele propuse de ofertant. Toate produsele software ofertate vor trebui să fie regăsite în oferta financiară și prezentate în oferta tehnică sub formă de tabel după cum urmează:

Nr. Crt.	Denumire produs (*)	Producător	Nume produs propus (**)	Cantitate	Unitate de	Modul de licențiere

					măsură	(***)

(*) Denumirea produslui conform Caietului de Sarcini.

(**) Denumirea completă dată de producător, inclusiv ediția (exemplu „Standard”, „Enterprise”, dacă este cazul). Se va insera câte un singur produs pe un rând.

(***) Va conține detalierea modului de licențiere al producătorului cu explicații privind modalitatea de îndeplinire a cerințelor caietului de sarcini.

Configurațiile echipamentelor conținând part-numberele sub-ansamblelor, denumirile și cantitățile vor fi prezentate în tabele separate pentru fiecare echipament ofertat

4. Lista mașinilor virtuale/containerelor necesare pentru soluția propusă, având în vedere cerințele de înaltă disponibilitate și performanță a soluției solicitate, indicând pentru fiecare mașină virtuală/container: rolul acesteia, sistemul de operare necesar, software-ul instalat, numărul de nuclee de procesare necesar a fi alocat, memoria RAM necesar a fi alocată, storage necesar a fi alocat.

5. Descrierea soluției tehnice propuse pentru îndeplinirea obiectivelor stabilite prin caietul de sarcini. Pentru sistemele/ subsistemele/ componentele solicitate, ofertantul va include/descrie în mod obligatoriu în oferta tehnică și modalitatea de implementare a funcționalităților solicitate;

6. Metodologia de prestare a serviciilor, ce va include:

a. obiectivele contractului și sarcinile stabilite prin caietul de sarcini;
b. identificarea și explicitarea aspectelor-cheie privind îndeplinirea obiectivelor contractului și atingerea rezultatelor așteptate;
c. modul de abordare ce va fi urmat în prestarea serviciilor, inclusiv descrierea conceptului utilizat pentru atingerea obiectivelor contractului;
d. metodologia de realizare a activităților ce corespund rezultatului final al contractului și a rezultatelor intermediare aferente, în raport cu serviciile și responsabilitățile stabilite prin caietul de sarcini;
e. modul de abordare a activității de identificare a riscurilor ce pot apărea pe parcursul derulării contractului și măsuri de diminuare a riscurilor în raport cu prevederile caietului de sarcini;

7. Planul de derulare a activităților contractului în conformitate cu abordarea și metodologia propusă, demonstrând astfel înțelegerea prevederilor din caietul de sarcini, abilitatea de a transpune prevederile întrun plan de lucru fezabil, descompunerea fazelor în etape, activități și sub-activități și încadrarea acestora în timp de așa manieră încât să se asigure alocarea corespunzătoare a resurselor pentru finalizarea acestora în termenele limită specificate în caietul de sarcini. Planul de lucru va fi realizat prin utilizarea unui software de management de proiect și va prezenta următoarele:

a. denumirea și durata fazelor, etapelor, activităților și sub-activităților din cadrul contractului
b. succesiunea și inter relaționarea fazelor, etapelor, activităților și sub-activităților
c. punctele-cheie de control – ”jaloanele”
d. resursele umane implicate în realizarea activităților și încărcarea acestora

e. data estimată de început și finalizare a fiecărei activități/sub activități

8. Personalul ce va realiza efectiv activitățile care fac obiectul contractului prezentând, pentru experții cheie următoarele documente:

a. Curriculum Vitae, semnat personalizat pentru pozitia din proiect;
b. Diplome, certificate de absolvire, certificări, atestate sau orice alte documente similare prin care să se demonstreze pregătirea/calificarea solicitată
c. Scrisoare/scrisori de recomandare de la Beneficiarul/Beneficiarii serviciilor prestate, fișă de post, contract de muncă sau orice alte documente similare care să ateste activitatea desfășurată, din care să rezulte durata angajamentului și funcția îndeplinită.
d. Declarație de disponibilitate pentru perioada aferentă activităților pe care și le asumă din prezentul contract.

Pentru fiecare expert-cheie propus se va completa/adapta o matrice similară cu cea prezentată cu titlu indicativ mai jos din care va reieși în mod clar atât îndeplinirea tuturor cerințelor minime stabilite la nivelul caietului, cât și îndeplinirea cerințelor pentru obținerea de punctaje suplimentare, dacă este cazul.

1	**NUME Prenume – Expert cheie nr. 1: Manager de proiect**					
Cerințe minime:*						
Studii				**Document suport:** Diplomă nr.xxxx, eliberată în urma absolvirii licenței în anul xxxxx.		
Competențe.....				**Document suport: Diplomă nr./ data / Certificat nr./ data**		
Experiență specifică**	**Număr /dată contract *sau* Denumire proiect (cod proiect, dacă este cazul)**	**Beneficiar contract/ proiect și Perioada contract / proiect**	**Obiect principal /obiective / activități principale contract / proiect**	**Activitățile prestate în contract / proiect de către persoana propusă**	**Rolul deținut în contract/proiectul de către persoana propusă**	**Documente suport**
1.	**Xxx/xx.xx.xxxx**	**Denumire beneficiar Xx.xx.xxxx - Xx.xx.xxxx**	**Precizați**	**Precizați**	**Precizați**	**Copie contract Copie PV recepție nr/data Document constatator nr./data Etc**
2.						
3.						

Nota*: Cerințele minime se vor prelua din caietul de sarcini pentru fiecare expert-cheie.

Notă**: Precizați toate informațiile solicitate pentru fiecare contract/proiect pe care solicitați ca autoritatea contractantă să-l considere experiență similară a expertului cheie propus. Pentru fiecare proiect se vor prezenta documentele suport conform cerințelor din caietul de sarcini.

Propunerea tehnică narativă reprezintă documentul central al propunerii tehnice, toate documentele suport prezentate pentru demonstrarea îndeplinirii tuturor cerințelor trebuie să fie menționate în aceasta, atașate ca anexe.

În mod obligatoriu, Ofertanții vor numerota fiecare pagină a Propunerii tehnice narative.
În Anexa 1 a Propunerii tehnice, ofertanții vor prezenta o matrice de conformitate în format .doc sau docx., având următoarea structură tabelară*:

Cerința minimă din Caietul de sarcini	**Detalii privind modul de îndeplinire a cerinței**	**Referință la documentația tehnică**

În coloana ” Cerința minimă din Caietul de sarcini” se vor înscrie cerințele numerotate din caietul de sarcini, câte o cerință pe fiecare rând.
În coloana ” Detalii privind modul de îndeplinire a cerinței” se va descrie modul în care oferta propusă îndeplinește fiecare cerință. Ofertele care se vor limita la a confirma faptul că cerința este îndeplinită, fără să prezinte concret modul în care vor realiza acest lucru, vor fi considerate neconforme. Nu se acceptă descrierea detaliată a modului în care este îndeplinită cerința prin copierea conținutului cerinței. Ofertele care în conținutul lor vor avea elemente de conținut copiat fără detalieri relevante din care să rezulte clar modul în care oferta respectivă îndeplinește acea cerință vor fi respinse ca neconforme în baza art. 137 alin (3) litera a din HG 395/2016. În această coloană nu se vor include poze, capturi de ecran sau referințe de tip URL. Ofertantul va prezenta răspunsuri detaliate la toate cerințele Caietului de Sarcini prin care să arate modul concret în care cerințele sunt îndeplinite.
În coloana ” Referință la documentația tehnică” se vor înscrie informații care asigură posibilitatea verificării facile a corespondenței cu cerințele, cum ar fi: trimiteri la capturi de ecran din documentațiile de produs atașate, la documente cu capturi de ecran, referințe URL sub formă de hyperlink la capturi de ecran din documentații publicate pe website-uri ale producătorilor.
În cazul trimiterilor la capturi de ecran din documentațiile de produs atașate se vor preciza numele documentului/fișierului și pagina/paginile unde se regăsește captura/capturile de ecran.
În cazul capturilor de ecran, aceasta vor fi incluse întrun document separat și numerotate, astfel încât trimiterile la ele să indice numele documentului/fișierului și numărul figurii/figurilor. Este interzisă includerea de capturi de ecran în tabelul cu matricea de conformitate.
Documentația tehnică și documentele suport necesare pentru identificarea soluției ofertate se prezintă ca anexe la propunerea tehnică, structurat, pe tipuri de componente, respectând ordinea de prezentare a acestora din caietul de sarcini
În mod obligatoriu, Ofertanții vor numerota fiecare pagină a Anexei 1 Matricea de conformitate.
Lipsa din ofertă a oricăror informații dintre cele solicitate în acest capitol sau prezentarea unor descrieri nerelevante sau care nu demonstrează îndeplinirea fiecărei cerințe, poate conduce la declararea ofertei ca fiind neconformă și, implicit, la descalificarea Ofertantului.
În cazul constatării unor neconcordanțe, specificațiile oficiale ale Producătorului produsului

(valabile la data limită de depunere a ofertelor) vor fi considerate ca referință, conținutul acestora primând asupra specificațiilor tehnice prezentate de ofertant.
În conformitate cu prevederile art.123 alin.(1) din HG nr. 395/2016, fiecare ofertant va indica, motivat, în propunerea tehnică depusă informațiile care sunt confidențiale, clasificate sau sunt protejate de un drept de proprietate intelectuală, în baza legislației aplicabile
Având în vedere complexitatea proiectului și importanța respectării termenului de implementare menționat în prezentul caiet de sarcini, asumat și prin contractul de finanțare, Autoritatea Contractantă solicită ofertanților prezentarea unei sesiuni demonstrative online prin care să se demonstreze că produsele software ofertate îndeplinesc nativ (out-of-the-box, respectiv prin funcționalități deja existente în cadrul acesteia, fără a necesita servicii suplimentare de dezvoltare software) și că ofertantul are capacitatea tehnică necesară desfășurării în bune condiţii a contractului, conform soluţiei tehnice propuse.
Sesiunea demonstrativă are scopul de a verifica funcţionalităţi aferente Platformei de dezvoltare și administrare aplicații web (LCAP) și a Platformei software de management al documentelor.
Cu minim 2 zile lucrătoare înainte de data planificată pentru sesiunea demonstrativă, la solicitarea Autorității Contractante, în etapa de evaluare tehnică, Ofertantul are obligația să transmită Autorităţii Contractante lista participanţilor la sesiunea demonstrativă în care se menţionează rolul în timpul sesiunii şi relaţia pe care aceştia o au cu Ofertantul - participanţii vor fi dintre experţii propuşi în oferta tehnică. Autoritatea Contractantă nu va accepta în sesiunea demonstrativă decât persoanele nominalizate de ofertant în lista participanţilor şi care figurează în lista de experţi menţionaţi în oferta depusă.
Ofertantul va pune la dispoziţia experţilor săi echipamentele (de ex. laptop-uri) şi software-ul necesar pentru derularea în bune condiţii a sesiunii demonstrative.
Echipamentele ofertantului vor fi utilizate de acesta ca suport pentru susținerea sesiunii demonstrative şi nu vor fi conectate la reţeaua Autoritatii Contractante.
În cadrul sesiunii demonstrative vor fi prezentate cerinte minime obligatorii (care sunt prevăzute în capitolele caietului de sarcini) ale Platformei de dezvoltare și administrare aplicații web (LCAP) și a Platformei software de management al documentelor..
Implementarea Platformei Integrate de Servicii Electronice este un process de lungă durată. Din acest motiv, Furnizorul trebuie să demonstreze că are capacitatea de implementare a soluției ofertate prin demonstrarea următoarelor funcționalități:

- Platforma de dezvoltare și administrare aplicații web (LCAP)
  1. Adăugarea rolurilor și configurarea acestora pentru a restricționa sau permite accesul la anumite pagini, componente, acțiuni, fluxuri de lucru sau entități;
  2. Configurarea permisiunilor la nivel de pagină, modul, entitate, acțiuni și butoane, astfel încât anumite funcționalități să fie disponibile doar pentru rolurile autorizate.
  3. Configurarea execuției automate a următoarelor joburi sau acțiuni la momente specifice sau la intervale recurente (declanșatoare de timp, declanșatoare de interval):

a. Rulare interogări SQL pentru actualizarea sau extragerea datelor.

b. Rulare executabile sau scripturi pentru automatizarea sarcinilor complexe.

4. Crearea unui flux de lucru prin utilizarea elementelor standard BPMN (Business Process Model and Notation) precum: Eveniment de start și eveniment de stop, activități care reprezintă sarcini sau operațiuni ce trebuie executate și Porți de decizie (XOR) pentru a direcționa fluxul de lucru în funcție de condiții specifice. Adăugarea de activități în fluxul de lucru folosind funcții predefinite cu variabile de intrare și ieșire, facilitând personalizarea proceselor.
5. Crearea unui obiect JSON nou
6. Crearea unui portal nou
7. Adăugarea, ștergerea și vizualizarea surselor de date, precum și executarea de interogări SQL.
8. Generare PDF din șablon HTML, conversia datelor HTML în Microsoft Word, generare coduri de bare.
9. Creare interfață REST API pentru a permite comunicarea cu diferite sisteme și aplicații. Implementarea de mecanisme de securizare a API-urilor prin utilizarea de chei API și token-uri web JSON (JWT.
10. Interfață vizuală de tip drag-and-drop pentru a permite crearea și personalizarea ușoară a formularelor.
11. Definirea de formulare cu Dropdown-uri, casete de verificare, butoane radio pentru selectarea unor opțiuni din liste predefinite sau generate dinamic.
12. Crearea de liste de opțiuni pentru câmpurile de tip dropdown sau opțiuni multiple, generate din:

    a. Liste statice definite în formă cheie/valoare.

    b. Interogări ale bazei de date pentru extragerea datelor relevante.

    c. API-uri care returnează date în format JSON.
13. Posibilitatea de a adăuga câmpuri dinamice, care să fie afișate sau ascunse automat pe baza interacțiunii utilizatorului (ex.: câmpuri condiționale).
14. Design responsiv pentru a asigura o experiență de utilizare optimizată pe dispozitive mobile, inclusiv adaptarea automată a formularelor la dimensiunea ecranului.
15. Suport pentru salvarea automată a progresului utilizatorului și pentru repornirea interacțiunii de la același punct, dacă formularul este închis sau întrerupt.
16. Crearea unei entități care să aibă ca rezultat:

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

a. Generarea automată a tabelelor corespunzătoare în baza de date, cu chei index bazate pe relațiile definite cu alte entități.

b. Generarea paginii asociate entității, care poate fi afișată sau ascunsă în meniul principal, și poate fi definită ca pagină de nivel superior sau subordonată altei pagini.

c. Crearea automată a unui formular pentru introducerea datelor, cu câmpuri bazate pe proprietățile entității.

d. Definirea de surse de date specifice pentru entitate.

e. Posibilitate generării de butoane și acțiuni în interfață pentru operațiuni CRUD (Creare, Citire, Actualizare, Ștergere).

f. Posibilitatea definirii și utilizării de API-uri pentru operațiuni asupra entităților.

g. Posibilitatea generării de tablouri de bord vizuale (dashboard-uri) pentru monitorizarea KPI-urilor bazate pe datele entității.

17. Definirea de relații între entități (unul-la-unu, unul-la-mulți, mulți-la-mulți), cu impact direct asupra structurii bazei de date și a operațiunilor disponibile.

18. Crearea de liste de date afișate sub formă tabelară, extrase din solicitări JSON de la API-uri externe.

19. Utilizarea funcțiilor de tip drag-and-drop pentru a organiza meniurile și paginile

20. Setarea paginilor pentru a fi publicate sau scoase din publicare la date și ore specifice, automatizând gestionarea conținutului.

- Platforma software de management a documentelor

1. Se va prezenta interfata de administrare a soluției ofertate demonstrându-se că permite gestiunea utilizatorilor, a grupurilor de utilizatori și are posibilitatea definirii și gestionarii unitatilor organizatorice. Se va demonstra o modalitate simpla de configurare și personalizare a platformei și a fișierelor de configurare ale sistemului. Se va demonstra că interfata de administrare permite gestiunea locatiilor de stocare a documentelor, a tipurilor de obiecte, permite definirea și gestiunea de catre administratorul sistemului a profilurilor de backup ale sistemului.
2. Funcționalitățile motorului de recunoaștere optică a caracterelor prin care: administratorul să poată configura extragerea automată a textului din toate documentele electronice la momentul încărcării în depozite (inclusiv pentru fișiere de tip imagine), pentru a facilita căutarea avansată de tip full-text în toate documentele din depozite (pentru care exista drepturile de acces relevante) utilizând operatori logici, funcții de autocompletare în baza caracterelor deja introduse, auto corecție a termenilor în cazul în care aceștia au fost introduși greșit, opțiunea de evidențiere a termenilor căutați, posibilitatea de excludere a unor termeni de căutare, etc.;

3. Versionarea automată a documentelor salvate de către utilizatori prin mecanismul de Check-in/Check-out.
4. Funcționalitatea „roll back” (posibilitatea de a reveni la o versiune anterioara), precum și posibilitatea de comparare a versiunilor.
5. Designer dedicat pentru definirea formularelor web pentru unele tipuri de documente gestionate. Designerul de formulare web va asigura cel puțin:
   a. crearea de formulare dinamice de tip responsiv și interactive;
   b. crearea de formulare cu tab-uri și metadate dinamice cu afișare de metadate în funcție de condiționalități;
   c. completarea automată a anumitor câmpuri;
   d. includerea pe câmpuri a unor formule de calcul;
   e. Posibilitatea definirii a câmpurilor de tip: dată, text, casetă de verificare, semnături, imagine, link, de tip buton pentru adăugarea sau ștergerea liniilor;
   f. introducerea de reguli și validări pe câmpurile formularului;
   g. preluarea de date din surse externe de informație, cum sunt alte sisteme software sau baze de date externe;
6. Modificarea fluxurilor de lucru predefinite prin intermediul designerului grafic, prin operații de drag and drop și asignare de relații. Modificarea nu trebuie să presupună scriere de cod.
7. Flux ad-hoc de documente, prin stabilirea activităților asociate (avizare, aprobare, semnare, etc.), definirea a minim 5 participanți și a tranzițiilor dintre activități. La definirea unui astfel de flux se va putea stabili: tipul distribuției (secvențial sau paralel), prioritatea, participanții implicați (la nivel de utilizator sau grup), definirea de escaladări (termenul de declanșare, utilizatorul către care se escaladează). Utilizatorul va putea să salveze fluxul astfel definit (ca șablon) pentru utilizarea ulterioară.
8. Aplicarea semnăturii electronice calificate asupra documentelor încărcate în depozit, asigurând îndeplinirea următoarelor cerințe:
   a. posibilitatea marcării poziției de aplicare a semnăturii pentru toți semnatarii;
   b. Nu va condiționa semnarea documentelor cu semnătură electronică calificată prin mecanisme de check-out/check-in. Cu alte cuvinte, platforma va permite semnarea „on the fly” (fără descărcare/încărcare pe/de pe stația de lucru a utilizatorului) a documentelor transmise pe fluxurile de lucru electronice sau stocate în depozit.
9. Configurarea de către administrator a funcțiilor, serviciilor și meniurilor aplicației în conformitate cu rolul, apartenența la grupuri și drepturile utilizatorului. Parametrizările se vor realiza fără a fi necesară dezvoltarea de cod.
10. Se vor prezenta interfetele de căutare în depozit direct din interfața grafică a soluției. Se vor prezenta cel putin urmatoarele capabilitati:
    - demonstrarea posibilitatii de căutare full-text
    - căutare avansata în toate documentele utilizând:
    - operatori logici
    - funcții de autocompletare în baza caracterelor deja introduse
    - evidențierea termenilor căutați
    - lista cu cele mai recente căutari
    - opțiunea de căutari preferate
    - optiunea de salvare a rezultatelor cautarii cu posibilitatea accesarii ulterioare

– vizualizare serii de imagine în forma miniaturi (Thumbnail) cu previzualizare

Rezultatul căutărilor va putea fi afișat în formă tabelară, grid sau arborescent, cu posibilitati suplimentare de grupare, ordonare și filtrare.

Prezentarea în cadrul sesiunii demonstrative a funcționalităților prezentate mai sus se va baza pe prezentarea practică a produselor software ofertate (de exemplu: a interfețelor expuse de acestea, a fișierelor de configurare ale acestora, etc.) în cadrul unor medii demonstrative.

Neprezentarea de către Ofertant în cadrul sesiunii demonstrative a tuturor funcționalităților prezentate mai sus va conduce la declararea ofertei ca neconformă.

Menționăm că solicitările referitoare la sesiunile demonstrative nu presupun implementarea de părți din contract. Ofertanții pot utiliza versiuni de tip demo/trial/temporar ale produselor ofertate.

13.2. Aplicarea criteriului de atribuire

Contractul va fi atribuit pe baza criteriului “cel mai bun raport calitate-preț”, în condițiile în care oferta îndeplinește cerințele caietului de sarcini. Comisia de evaluare va evalua și compara ofertele depuse pentru toate obiectivele, rezultatele și activitățile/livrabilele solicitate.

Nr. crt.	Factori de evaluare	Pondere (%)	Punctaj maxim acordat
1.	Valoarea propunerii financiare, fără TVA	40%	40 puncte
2.	Experiența personalului desemnat pentru executarea contractului	20%	20 puncte
3.	Demonstrarea unei abordări, înțelegeri și metodologii adecvate pentru implementarea contractului, precum și o planificare adecvată a resurselor umane și a activităților	20%	20 puncte
4.	Specificații tehnice extinse pentru echipamente	10%	10 puncte
5.	Criterii ecologice privind echipamentele care au impact asupra mediului pe durata întregului ciclu de viaţă	10%	10 puncte
Total		**100%**	**100 puncte**

Punctajul total maxim, care poate fi obținut de o oferta este de 100 puncte, respectiv:

Pf (punctaj total pentru ofertă financiară) + Pe (punctaj total pentru experiența experților propuși) + Pd (punctaj total pentru - Demonstrarea unei abordări, înțelegeri și metodologii adecvate pentru implementarea contractului, precum și o planificare adecvată a resurselor umane și a activităților) + Ps(punctaj total pentru - Specificații tehnice extinse pentru echipamente) + Pc (punctaj total pentru - Criterii ecologice privind echipamentele care au impact asupra mediului pe durata

întregului ciclu de viaţă) = 40 puncte + 20 puncte + 20 puncte + 10 puncte+10 puncte = 100 puncte
În conformitate cu art. 32, alin. 9 din HG 395/2016, ponderile stabilite pentru factorii de evaluare sunt stabilite astfel încât să nu conducă la distorsionarea rezultatului aplicării procedurii pentru atribuirea contractului.

În conformitate cu prevederile art. 139 din HG 395 / 2016 pentru aprobarea Normelor metodologice de aplicare a prevederilor referitoare la atribuirea contractului de achiziţie publică / acordului-cadru din Legea nr. 98/2016 privind achiziţiile publice, cu modificările și completările ulterioare, **în cazul în care două sau mai multe oferte sunt clasate pe primul loc, cu punctaje egale, departajarea se va face având în vedere punctajul obţinut la factorii de evaluare, în ordinea descrescătoare a ponderilor acestora**. În situaţia în care egalitatea se menţine, autoritatea contractantă are dreptul să solicite noi propuneri financiare, și de a desemna, ca ofertă oferta câștigătoare, oferta care va înregistra propunerea financiară cea mai mică.

13.2.1. Factor de evaluare 1 - Valoarea propunerii financiare, fără TVA

Prețurile care se compară sunt prețurile fără TVA menționate în Formularul de ofertă, formular ce va fi completat conform modelului Formular Ofertă Financiară;
Punctajul se acorda conform următorului algoritm de calcul:
a) Pentru cel mai scăzut dintre prețuri se acordă punctajul maxim alocat;
b) Pentru celelalte prețuri ofertate punctajul P(n) se calculează proporțional, astfel:
P(n) = (Preț minim ofertat / Preț n) x punctaj maxim alocat.
Notă:
Având în vedere prevederile Legii nr. 98/2016 și ale HG nr. 395/2016 cu privire la achizițiile publice, în situația în care comisia de evaluare va constata că elemente de preț ale unei oferte sunt aparent neobișnuit de scăzute, prin raportare la prețurile pieței, va solicita ofertantului care a depus oferta în cauză, explicații cu privire la posibilitatea îndeplinirii contractului în condițiile de calitate impuse prin documentația de atribuire.
Explicațiile aduse de ofertant vor fi însoțite de dovezi concludente privind modul de organizare și metodele utilizate în cadrul procesului de lucru, nivelul de salarizare al personalului ofertantului, performanțele și costurile implicate de anumite echipamente etc.
În cazul în care ofertantul nu prezintă comisiei de evaluare informațiile și/sau documentele solicitate sau acestea nu justifică în mod corespunzător nivelul scăzut al prețului sau al costurilor propuse, oferta va fi considerată inacceptabilă.

13.2.2. Factor de evaluare 2 - Experiența personalului desemnat pentru executarea contractului

Experiența experților cheie, concretizată în numărul de proiecte/contracte similare în care respectivii experți au îndeplinit aceleași tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract. – punctaj maxim 100 de puncte.

La punctajul obținut de oferte se va aplica pondere de 20% pentru acest criteriu rezultând punctajul pentru ofertă, care nu poate depăși punctajul maxim al criteriului de 20 de puncte.
Pentru factorul de evaluare " Experiența personalului desemnat pentru executarea contractului " a fost stabilit un număr de 5 (cinci) subfactori care vor fi utilizaţi de comisia de evaluare ca puncte de reper în aprecierea factorului.

Experiența similară a experților cheie propuși

Denumire factor de evaluare	**Denumire sub-factor de evaluare**	**Punctaj maxim acordat**
Experiența similară a experților cheie propuși	Arhitect de sistem	4 puncte
	Analist Coordonator	4 puncte
	Expert îmbunătățire procese	4 puncte
	Expert coordonator dezvoltare aplicații web	4 puncte
	Expert coordonator implementare sistem de management documente	4 puncte

Punctajul aferent experienței experților-cheie se va acorda pentru fiecare în parte, astfel:

Denumire sub-factor de evaluare	**Algoritm de calcul**
1. Arhitect de sistem	Pentru ca oferta să fie conformă, expertul trebuie să dețină experiența similară dovedită prin participarea la minim 1 proiect/contract de implementare a unui sistem informatic, în care a desfășurat activități similare prin raportare la rolul, atribuțiile și responsabilitățile pe care expertul le va avea în cadrul prezentului contract. Experiența similară în proiecte de implementare a unui sistem informatic în care a îndeplinit același tip de activități cu cele ce urmează să le îndeplinească în viitorul contract va fi punctată, cu maxim 4 puncte, astfel: - Implicarea expertului în 1 proiecte/contracte conform descrierii criteriului – 0 puncte; - Implicarea expertului în 2-4 proiecte/contracte conform descrierii criteriului – 2 punct; - Implicarea expertului în 5-7 proiecte/contracte conform descrierii criteriului – 3 puncte; - Implicarea expertului în 8 sau mai multe proiecte/contracte conform descrierii criteriului – 4 puncte.

Denumire sub-factor de evaluare	Algoritm de calcul
2. Analist coordonator	Pentru ca oferta să fie conformă, expertul trebuie să dețină experiența similară dovedită prin participarea la minim 1 proiecte/contracte de implementare unui sistem informatic care să fi inclus digitalizarea serviciilor, în care a desfășurat activități similare prin raportare la rolul, atribuțiile și responsabilitățile pe care expertul le va avea în cadrul prezentului contract. Experiența similară în proiecte de implementare a unui sistem informatic care să fi inclus digitalizarea serviciilor, în care a îndeplinit același tip de activități cu cele ce urmează să le îndeplinească în viitorul contract va fi punctată, cu maxim 4 puncte, astfel: - Implicarea expertului în 1 proiecte/contracte conform descrierii criteriului – 0 puncte; - Implicarea expertului în 2-4 proiecte/contracte conform descrierii criteriului – 2 puncte; - Implicarea expertului în 5-7 proiecte/contracte conform descrierii criteriului – 3 puncte; - Implicarea expertului în 8 sau mai multe proiecte/contracte conform descrierii criteriului – 4 puncte.
3. Expert îmbunătățire procese de business	Pentru ca oferta să fie conformă, expertul trebuie să dețină experiența similară dovedită prin participarea la minim 1 proiect/contract în cadrul căruia au fost prestate servicii de analiză și îmbunătățire a proceselor de business, în care a desfășurat activități similare prin raportare la rolul, atribuțiile și responsabilitățile pe care expertul le va avea în cadrul prezentului contract. Experiența similară în proiecte în cadrul cărora au fost prestate servicii de analiză și îmbunătățire a proceselor de business, în care a îndeplinit același tip de activități cu cele ce urmează să le îndeplinească în viitorul contract va fi punctată, cu maxim 4 puncte, astfel: - Implicarea expertului în 1 proiecte/contracte conform descrierii criteriului – 0 puncte; - Implicarea expertului în 2-4 proiecte/contracte conform descrierii criteriului – 2 puncte; - Implicarea expertului în 5-7 proiecte/contracte conform descrierii criteriului – 3 puncte; - Implicarea expertului în 8 sau mai multe proiecte/contracte conform descrierii criteriului – 4 puncte.

Denumire sub-factor de evaluare	**Algoritm de calcul**
4. Expert coordonator dezvoltare aplicații web	Pentru ca oferta să fie conformă, expertul trebuie să dețină experiența similară dovedită prin participarea la minim 1 proiecte/contracte de implementare a unei aplicații web pe platforma de dezvoltare și administrare aplicații web propusă, în care a desfășurat activități similare prin raportare la rolul, atribuțiile și responsabilitățile pe care expertul le va avea în cadrul prezentului contract. Experiența similară în proiecte de implementare a unei aplicații web pe platforma de dezvoltare și administrare aplicații web propusă în care a îndeplinit același tip de activități cu cele ce urmează să le îndeplinească în viitorul contract va fi punctată, cu maxim 4 puncte, astfel: - Implicarea expertului în 1 proiecte/contracte conform descrierii criteriului – 0 puncte; - Implicarea expertului în 2-4 proiecte/contracte conform descrierii criteriului – 2 puncte; - Implicarea expertului în 5-7 proiecte/contracte conform descrierii criteriului – 3 puncte; - Implicarea expertului în 8 sau mai multe proiecte/contracte conform descrierii criteriului – 4 puncte.
5. Expert coordonator implementare sistem de management documente	Pentru ca oferta să fie conformă, expertul trebuie să dețină experiența similară dovedită prin participarea la minim 1 proiecte/contracte de implementare a unui sistem informatic care să fi inclus o soluție software de management documente pe platforma propusă, în care să fi desfășurat activități similare prin raportare la rolul, atribuțiile și responsabilitățile pe care expertul le va avea în cadrul prezentului contract. Experiența similară în proiecte/contracte de implementare a unui sistem informatic care să fi inclus o soluție software de management documente pe platforma propusă, în care a îndeplinit același tip de activități cu cele ce urmează să le îndeplinească în viitorul contract va fi punctată, cu maxim 4 puncte, astfel: - Implicarea expertului în 1 proiecte/contracte conform descrierii criteriului – 0 puncte; - Implicarea expertului în 2-4 proiecte/contracte conform descrierii criteriului – 2 puncte; - Implicarea expertului în 5-7 proiecte/contracte conform descrierii criteriului – 3 puncte;

Denumire sub-factor de evaluare	Algoritm de calcul
	- Implicarea expertului în 8 sau mai multe proiecte/contracte conform descrierii criteriului – 4 puncte.

13.2.3. Factor de evaluare 3 - Demonstrarea unei abordări, înțelegeri și metodologii adecvate pentru implementarea contractului, precum și o planificare adecvată a resurselor umane și a activităților

Denumire factor de evaluare	Denumire sub-factor de evaluare	Punctaj maxim acordat
Demonstrarea unei abordări, înțelegeri și metodologii adecvate pentru implementarea contractului, precum și o planificare adecvată a resurselor umane și a activităților	1. Metodologia și abordarea propusă pentru implementarea contractului	10 puncte
	2. Încadrarea în timp, succesiunea și durata activităților propuse	10 puncte
		20 puncte

Pentru factorul de evaluare " Demonstrarea unei abordări, înțelegeri și metodologii adecvate pentru implementarea contractului, precum și o planificare adecvată a resurselor umane și a activităților " a fost stabilit un număr de 2 (doi) sub-factori care vor fi utilizați de comisia de evaluare ca puncte de reper în aprecierea factorului.

Fiecare sub-factor va fi apreciat în funcție de calificativul "foarte bine, bine, satisfăcător/acceptabil". Comisia de evaluare va acorda calificativul luând în considerare liniile directoare prezentate în tabelul de mai jos.

Fiecărui calificativ îi corespunde o notă.

Punctajul total al acestui factor de evaluare se calculează prin însumarea punctajelor 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.

Punctajul maxim acordat acestui factor de evaluare este de **20 puncte**.

Demonstrarea unei abordări, înțelegeri și metodologii adecvate pentru implementarea contractului, precum și o planificare adecvată a resurselor umane și a activităților

1. Metodologia și abordarea propusă pentru implementarea contractului		
Factorul de evaluare urmărește aprecierea tuturor aspectelor metodologice propuse de ofertant pentru îndeplinirea cerințelor Caietului de sarcini. Se vor urmări (descrierea nu este exhaustivă) intrările, procesele și ieșirile pentru fiecare activitate și livrabil solicitate, atribuțiile și responsabilitățile experților pentru ducerea la îndeplinire în cele mai bune condiții a activităților și obținerea rezultatelor așteptate. În cazul în care contractul este atribuit unui grup de operatori economici, se urmărește aprecierea modului în care se vor distribui sarcinile fiecărui membru al grupului, precum și a responsabilităților fiecăruia în derularea contractului, inclusiv pentru activitățile comune. Se vor indica și standardele aplicabile și instrumentele utilizate.	**Calificative**	**Punctaj**
A. Nivelul metodologiei prezentate este satisfăcător/acceptabil întrucât: - abordarea propusă și metodologia prezentată nu are la bază/nu include metodologii, metode, tehnici și/sau instrumente testate, recunoscute în domeniu; - abordarea propusă și metodologia prezentată arată un nivel limitat de înțelegere a contextului, respectiv a particularității sarcinilor și specificului activităților stabilite în Caietul de sarcini; - abordarea propusă și metodologia prezentată nu includ detalii privind modul în care Ofertantul își propune să realizeze activitățile solicitate prin Caietul de sarcini și să ajungă la îndeplinirea rezultatelor proiectului.	SATISFĂCĂTOR/ ACCEPTABIL	0 puncte
B. Nivelul metodologiei prezentate este bun întrucât: - abordarea propusă și metodologia prezentată se bazează partial pe metodologii, metode, tehnici și/sau instrumente testate, recunoscute; - abordarea propusă și metodologia prezentată arată un nivel corespunzător de înțelegere a contextului, respectiv a particularității sarcinilor și a specificului activităților stabilite în Caietul de sarcini, în corelație cu aspectele-cheie, precum și cu riscurile și ipotezele identificate. Resursele utilizate sunt documentate.	BINE	5 puncte

C. Nivelul metodologiei prezentate este foarte bun întrucât: - abordarea propusă și metodologia prezentată se bazează în mare măsură pe o serie de metodologii, metode și/sau instrumente testate*1), tehnici/standarde recunoscute*2); - abordarea propusă și metodologia prezentată demonstrează o foarte bună înțelegere a contextului, respectiv a particularității sarcinilor stabilite în caietul de sarcini, în corelație cu aspectele-cheie, precum și cu riscurile și ipotezele identificate; - abordarea propusă și metodologia prezentată sunt adaptate la specificul Contractului în vederea obținerii tuturor livrabilelor solicitate și atingerii obiectivelor contractului, printr-o alocare justificată a resurselor; - aspectele importante sunt abordate întrun mod practic, inovator și eficient, prezentând modalități de îmbunătățire a rezultatelor și creștere a nivelului calitativ de realizare a activităților, prin utilizarea de cunoștințe/informații de dată recentă în domeniu. *1) Metodologiile, metodele și/sau instrumentele au fost utilizate în alte proiecte; *2) Metodologiile, metodele și/sau instrumentele sunt descrise în literatura de specialitate.	FOARTE BINE	10 puncte
2. Încadrarea în timp, succesiunea și durata activităților propuse		
Factorul de evaluare urmărește întocmirea și prezentarea unui plan de implementare care să cuprindă: planificarea timpului, succesiunea și durata etapelor și activităților, luându-se în considerare și timpul necesar pentru mobilizare (grafic Gantt) cu evidențierea momentelor semnificative (jaloane) ale proiectului și descrierea modului de utilizare a resurselor pentru fiecare fază, în raport cu necesitatea atingerii rezultatelor și respectarea termenelor indicate. Factorul de evaluare urmărește aprecierea planului de implementare propus (faze, activități, durată etc.), a modalității de determinare a drumului critic și alocarea resurselor pentru fiecare fază/activitate (experți implicați, alte resurse necesare de exemplu, dar nelimitativ: tehnice, logistice, administrative etc.) pentru îndeplinirea cerințelor caietului de sarcini.	**Calificative**	**Punctaj**
A. Raționament utilizat în evaluarea conținutului propunerilor tehnice: 1. durata activităților este în mică măsură potrivită complexității	SATISFĂCĂTOR/ ACCEPTABIL	0 puncte

acestora sau succesiunea dintre acestea, inclusiv perioada de desfășurare, este stabilită întrun mod foarte puțin adecvat în raport cu logica relației dintre acestea sau durata prevăzută pentru fiecare fază este corelată în mică măsură cu activitățile prevăzute a fi realizate în lunile respective și resursele estimate pentru desfășurarea acestora; 2. punctele de reper (jaloanele) sunt identificate, dar nu sunt semnificative/relevante sau nu sunt încadrate corect în timp sau nu sunt corelate corespunzător cu raportările, în special cele prevăzute în Caietul de sarcini; 3. fazele principale sunt incluse în calendarul activităților, dar acestea nu sunt detaliate în activități, planul de implementare neputând fi utilizat așa cum este prezentat ca dată de intrare în cadrul întâlnirilor de monitorizare a progresului în cadrul Contractului.		
B. Raționament utilizat în evaluarea conținutului propunerilor tehnice: 1. durata activităților corespunde parțial complexității acestora, iar succesiunea dintre acestea, inclusiv perioada de desfășurare este corelată doar partial cu logica relației dintre acestea; 2. durata prevăzută pentru fiecare fază este corelată partial cu activitățile prevăzute a fi realizate în lunile respective și resursele estimate pentru desfășurarea acestora; 3. punctele de reper (jaloanele) identificate sunt în mică măsură semnificative pentru execuția contractului, dar sunt încadrate corect în timp și corelate corespunzător cu raportările, în special cele prevăzute în caietul de sarcini; 4. există un grad de detaliere corespunzător, care facilitează înțelegerea planului de limplementare propus și utilizarea să în monitorizarea activității în cadrul Contractului.	BINE	5 puncte
C. Raționament utilizat în evaluarea conținutului propunerilor tehnice: 1. durata activităților corespunde deplin complexității acestora, iar succesiunea dintre acestea, inclusiv perioada de desfășurare, este stabilită în funcție de logica relației dintre acestea; 2. durata prevăzută pentru fiecare fază este corelată cu activitățile prevăzute a fi realizate în lunile respective și resursele identificate pentru desfășurarea acestora; 3. punctele de reper (jaloanele) identificate sunt semnificative	FOARTE BINE	10 puncte

"Conținutul acestui material nu reprezintă în mod obligatoriu poziția oficială a Uniunii Europene sau a Guvernului României."

pentru execuția contractului, sunt încadrate corect în timp și corelate corespunzător cu raportările, în special cele prevăzute în caietul de sarcini; 4. fazele principale sunt incluse în calendarul activităților, sunt detaliate în activități, planul de implementare poate fi utilizat așa cum este prezentat ca dată de intrare în cadrul întâlnirilor de monitorizare.		

13.2.4. Factor de evaluare 4 – Specificații tehnice extinse pentru echipamente

Pentru factorul de evaluare "Specificații tehnice extinse pentru echipamente" a fost stabilit un număr de 2 (doi) subfactori care vor fi utilizaţi de comisia de evaluare ca puncte de reper în aprecierea factorului:

Nr crt.	Sub-Factori de evaluare	Punctaj sub-factor de evaluare	Pondere (%)
1.	Specificații tehnice extinse pentru echipamentele tip Computere de birou	8 puncte	8%
4.	Specificații tehnice extinse pentru echipamentele tip Computere portabile	2 puncte	2%
	TOTAL	**10 puncte**	**10 %**

13.2.4.1 Factor de evaluare 4.1 - Specificații tehnice extinse pentru echipamentele tip Computer de birou

Punctajul maxim la acest factor de evaluare este 8 puncte.
Algoritm de calcul:
Se acordă 8 puncte ofertantului care oferă echipamente tip Computer de birou care îndeplinesc integral toate Specificațiile tehnice extinse din caietul de sarcini cap. 5.7.6
Ofertantul trebuie să prezinte o documentație tehnică care să ateste că soluția ofertată îndeplinește cerințele solicitate, fiind aplicabile prevederile din cap. 14 Modul de prezentare al ofertelor tehnice din caietul de sarcini.
Justificare: Scopul acestui criteriu este de a asigura autorității contractante posibilitatea obținerii unei tehnologii superioare, asigurând astfel o sustenabilitate sporită pe termen lung.

13.2.4.2 Factor de evaluare 4.2 - Specificații tehnice extinse pentru echipamentele tip Computer portabil

Punctajul maxim la acest factor de evaluare este 2 puncte.
Algoritm de calcul:
Se acordă 2 puncte ofertantului care oferă echipamente tip Computer Portabil care îndeplinesc integral toate Specificațiile tehnice extinse din caietul de sarcini cap. 5.7.7
Ofertantul trebuie să prezinte o documentație tehnică care să ateste că soluția ofertată îndeplinește cerințele solicitate, fiind aplicabile prevederile din cap. 14 Modul de prezentare al ofertelor tehnice din caietul de sarcini.
Justificare: Scopul acestui criteriu este de a asigura autorității contractante posibilitatea obținerii unei tehnologii superioare, asigurând astfel o sustenabilitate sporită pe termen lung.

13.2.5. Factor de evaluare 5 – Criterii ecologice privind echipamentele care au impact asupra mediului pe durata întregului ciclu de viaţă

Criteriile ecologice privind echipamentele care au impact asupra mediului pe durata întregului ciclu de viaţă – punctaj maxim 10 de puncte.

La punctajul obținut de oferte se va aplica pondere de 10% pentru acest criteriu rezultând punctajul pentru ofertă, care nu poate depăși punctajul maxim al criteriului de 10 de puncte.

Denumire factor de evaluare	**Denumire sub-factor de evaluare**	**Punctaj maxim acordat**
Criterii ecologice privind echipamentele care au impact asupra mediului pe durata întregului ciclu de viaţă	Factor de evaluare 5.1: Consumul de energie al stației de lucru în modul Activ (Pornit)	7 puncte
	Factor de evaluare 5.2: Consumul de energie al laptopului în modul Activ (Pornit)	3 puncte

Punctajul aferent Criteriilor ecologice privind echipamentele care au impact asupra mediului pe durata întregului ciclu de viaţă se va acorda pentru fiecare sub-factor de evaluare în parte, astfel:

13.2.5.1 Factor de evaluare 5.1 – Consumul de energie al stației de lucru în modul Activ (Pornit)

Punctajul maxim la acest factor de evaluare este **7 puncte**.

Punctajul la acest factor de evaluare se acorda astfel:

- Pentru stația de lucru cu cel mai scăzut consum de energie în modul Activ (Pornit) dintre cele ofertate se acordă punctajul maxim alocat;
- Pentru celelalte stații de lucru ofertate P(n) se calculează proporțional, astfel: P (n) = (Consumul de energie în modul Activ (Pornit) minim ofertat / Consumul de energie în modul Activ (Pornit) ofertat x punctajul maxim alocat,

unde:

P(n) – punctajul pentru computerul ofertat n

Consumul de energie în modul Activ (Pornit) minim ofertat – cel mai mic consum de de energie în modul Activ (Pornit) dintre stațiile de lucru ofertate care îndeplinesc cerințele minimale din Caietul de sarcini

Consumul de energie în modul Activ (Pornit) ofertat – Consumul de energie în modul Activ (Pornit) pentru stația de lucru ofertată

Precizări:

Se acordă puncte pentru stații de lucru cu consum de energie în modul Activ (Pornit) mai mic decât specificațiile minime din Caietul de Sarcini (ETEC calculată conform cerințelor Programului Energy Star pentru Computere versiunea 8.0).

Ofertanții trebuie să furnizeze documente emise de producător (fișă de produs sau rapoarte de testare efectuate conform metodelor de testare) din care să rezulte consumul produsului ofertat..

Justificare: *Scopul acestui criteriu este de a se asigura că echipamentele vor avea un consum de energie semnificativ redus în modul de lucru Activ (Pornit).*

13.2.5.2 Factor de evaluare 5.2 – Consumul de energie al laptopului în modul Activ (Pornit)

Punctajul maxim la acest factor de evaluare este **3 puncte**.

Punctajul la acest factor de evaluare se acorda astfel:

a. Pentru computerul cu cel mai scăzut consum de energie în modul Activ (Pornit) dintre cele ofertate se acordă punctajul maxim alocat;

b. Pentru celelalte computere ofertate P(n) se calculează proporțional, astfel: P (n) = (Consumul de energie în modul Activ (Pornit) minim ofertat / Consumul de energie în modul Activ (Pornit) ofertat

x punctajul maxim alocat,

unde:

P(n) – punctajul pentru computerul ofertat n

Consumul de energie în modul Activ (Pornit) minim ofertat – cel mai mic consum de de energie în modul Activ (Pornit) dintre computerele ofertate care îndeplinesc cerințele minimale din Caietul de sarcini.

Consumul de energie în modul Activ (Pornit) ofertat – Consumul de energie în modul Activ (Pornit) pentru computerul ofertat

Precizări:

Se acordă puncte pentru computere cu consum de energie în modul Activ (Pornit) mai mic decât specificațiile minime din Caietul de Sarcini (ETEC calculată conform cerințelor Programului Energy Star pentru Computere versiunea 8.0).

Ofertanții trebuie să furnizeze documente emise de producător (fișă de produs sau rapoarte de testare efectuate conform metodelor de testare) din care să rezulte consumul produsului ofertat..

Justificare: *Scopul acestui criteriu este de a se asigura că echipamentele vor avea un consum de energie semnificativ redus în modul de lucru Activ (Pornit).*

Avizat:

Manager de Proiect

Cristina Maria VLAD

Vlad Cristina-Maria

Digitally signed by Vlad Cristina-Maria
Date: 2026.03.10 12:45:57 +02'00'

Verificat:

Responsabil Achiziții

Adriana Maria MUCALĂU

Semnatar: Mucalau Adriana-Maria
Data si ora semnarii: 10-03-2026 12:39:37

Întocmit,

Consultant coordonator:

Laurențiu-George Nica

LAURENTIU-GEORGE NICA

Digitally signed by LAURENTIU-GEORGE NICA
Date: 2026.03.06 11:49:38 +02'00'

Coordonator procese soluționare petiții și sesizări

Cristiana GRIMBERG

Cristiana Grimberg

Semnat digital de Cristiana Grimberg
Data: 2026.03.10 12:21:33 +02'00'