PROIECT TEHNIC

Denumire Proiect: Reforma activității de control în domeniul relațiilor de muncă și al securității și sănătății în muncă, finanțat prin Planul National de Redresare si Reziliență (PNRR) - Componenta 7. Transformarea digitală, Investiția 6. Digitalizarea în domeniul muncii și protecției sociale

Beneficiar: INSPECȚIA MUNCII

Nr. Contract:

Dată contract:

Proiectant: GO-TECH CONSULTING SRL

Controlul Distribuţiei

Copia Nr.	Distribuţie
1.	INSPECȚIA MUNCII
2.	GO-TECH CONSULTING SRL

Istoricul Modificărilor

Versiune	Data	Comentarii
1.0		Versiune iniţială
2.0		Versiune actualizată conform feedback beneficiar, task force MCID și MMSS
3.0		Versiune actualizată pentru includere funcționalități aplicație evaluare de risc și alocare resurse hardware
3.2		Versiune actualizată pentru includere funcționalități portal extern și intern

Cuprins

1 DATE GENERALE

Inspecția Muncii este un organ de specialitate al administrației publice centrale, cu personalitate juridică, aflat în subordinea Ministerul Muncii și Solidarității Sociale care îndeplinește funcția de autoritate de stat, asigurând exercitarea controlului în domeniile relațiilor de muncă, securității și sănătății în muncă și supravegherii pieței.

Inspecţia Muncii acţionează pentru asigurarea protecţiei sociale a muncii, în baza prevederilor art. 41 din Constituţia României, republicată, şi, respectiv, a prevederilor Convenţiei OIM nr. 81/1947 privind inspecţia muncii în industrie şi comerţ, ratificată prin Decretul Consiliului de Stat nr. 284/1973 şi ale Convenţiei OIM nr. 129/1969 privind inspecţia muncii în agricultură, ratificată prin Decretul Consiliului de Stat nr. 83/1975.

Instituția este înființată și organizată în baza:

- Legii nr. 108/1999 pentru înființarea și organizarea Inspecției Muncii, republicată, cu modificările ulterioare;
- H.G. nr. 488/2017 privind aprobarea Regulamentului de organizare și funcționare a Inspecției Muncii, cu modificările și completările ulterioare.

Inspecţia Muncii îndeplineşte următoarele funcţii generale:

a. de autoritate de stat, prin care se asigură exercitarea controlului aplicării prevederilor legale în domeniile sale de competenţă;

b. de comunicare, prin care se asigură schimbul de informaţii cu autorităţile administraţiei publice centrale şi locale, precum şi cu persoanele fizice şi juridice supuse activităţii de control, informarea acestora şi a cetăţenilor asupra modului cum se respectă şi se aplică prevederile legislaţiei din domeniile de competenţă;

c. de reprezentare, prin care se asigură, în numele statului român şi al Guvernului României, reprezentarea pe plan intern şi extern în domeniile sale de competenţă;

d. de formare, prin care se realizează pregătirea şi perfecţionarea profesională a personalului propriu, în condiţiile legii;

e. de cooperare, prin care se asigură desfăşurarea de acţiuni în comun, pe plan intern şi internaţional, în domeniile de competenţă;

f. de administrare, prin care se asigură gestionarea bunurilor din domeniul public, respectiv privat al statului ori, după caz, al unităţilor administrativ-teritoriale pe care le are în administrare sau în folosinţă, a fondurilor alocate în scopul funcţionării în condiţiile legii, precum şi organizarea şi gestionarea sistemelor informatice necesare activităţilor proprii.

În subordinea Inspecției Muncii sunt organizate și funcționează Inspectorate Teritoriale de Muncă (ITM) în fiecare județ și în Municipiul București.

1.1 Reforma activității de control în domeniul relațiilor de muncă și al securității și sănătății în muncă

În vederea implementării Reformei activității de control în domeniul relațiilor de muncă și al securității și sănătății în muncă, s-a semnat contractul nr. 3993/22.07.2022 între Inspecția Muncii (Beneficiar) și Ministerul Muncii și Solidarității Sociale finanțat prin Planul Național de Redresare și

Reziliență, Investiția 6. Digitalizarea în domeniul muncii și protecției sociale /componenta C7 – Transformare digitală.

Obiectivul general al proiectului îl reprezintă reforma activității de bază a instituției prin modernizarea și eficientizarea activităților de control în domeniul relațiilor de muncă și al securității și sănătății în muncă.

Implementarea proiectului *„Reforma activității de control în domeniul relațiilor de muncă și al securității și sănătății în muncă”* va contribui la creșterea utilizării sistemelor de e-guvernare la nivel național prin implementarea unor servicii centrate pe nevoile cetățenilor, digitalizarea activității desfășurate în beneficiul cetățenilor, prin generarea documentelor interne (adrese, solicitări interne, răspunsuri, etc.), realizarea circuitului acestora, inclusiv, arhivarea, în format electronic și semnarea cu semnătură electronică.

Obiectivele specifice ce vor fi atinse prin implementarea sistemului sunt:

- Eficientizarea activității de control prin utilizarea instrumentelor moderne (de exemplu semnătura electronică în actul de control dar și completarea electronică a documentației aferente controlului și accesarea de pe teren a bazelor de date necesare efectuării verificărilor), prin diminuarea timpului alocat aspectelor procedurale și creșterea timpului alocat verificărilor, utilizarea mai eficientă a resurselor umane și materiale disponibile și facilitarea deplasării la locațiile care trebuie controlate;
- Gestionarea eficienta a evenimentelor ce intra in sfera de competenta a Inspectiei Muncii
- Eficientizarea serviciilor oferite de Inspecția Muncii prin implementarea unui sistem care va contribui la îmbunătățirea serviciilor publice pentru cetățeni și mediul de afaceri precum și către alte autorități și instituții publice printr-o utilizare mai eficientă a resurselor și scurtarea timpilor de răspuns la solicitările primite;
- Creșterea accesului la serviciile electronice moderne prin îmbunătățirea interacțiunii on-line;
- Elaborarea de standarde și practici comune în vederea integrării cu instituțiile publice partenere;
- Îmbunătățirea procesului de comunicare a documentelor de control către entitatea controlată și către organele fiscale;
- Realizarea analizei de risc, planificarea controalelor, si programarea acestora
- Completarea datelor de identificare a unitatilor pentru care se intocmeste pvc, generarea PVCSC si PVSA ca urmare a neconformitatilor inscrise in PVC
- Interacțiunea cu celelalte sisteme informatice existente la nivelul Inspectiei Muncii si cu bazele de date alte instituțiilor partenere
- facilitarea adoptăreii unor decizii eficiente privind identificarea şi combaterea cazurilor de muncă nedeclarată;
- accesarea de pe teren a datelor necesare efectuării controlului, existente în baza de date a Inspecției Muncii precum și a altor instituții (ANF, ONRC, Evidența Populației, etc) precum și prin comunicarea în timp util a tuturor situațiilor deosebite/incidentelor/ dificultăților, întâmpinate în timpul controlului, pentru a primi informațiile, îndrumarea și sprijinul necesare.
- facilitarea verificării plății și, după caz, a executării amenzilor contravenționale de către organele fiscale.

1.2 Legislație specifică

Legislatie in domeniul Securității Și Sănătății în Muncă

- Legea nr.53/2003 - Codul muncii, republicată

- Legea securităţii şi sănătăţii în muncă nr.319/2006, cu modificările şi completările ulterioare
- H.G. nr. 1425/2006 – pentru aprobarea Normelor metodologice de aplicare a prevederilor Legii securităţii şi sănătăţii în muncă nr.319/2006, actualizată
- O.U.G. nr.96/2003 - privind protecţia maternităţii la locurile de muncă, actualizată
- O.U.G. nr.99/2000 - privind măsurile ce pot fi aplicate în perioadele cu temperaturi extreme pentru protecţia persoanelor încadrate în muncă
- Legea nr.126/1995 - privind regimul materiilor explozive, republicată
- O.U.G. nr.4/1995 - privind fabricarea, comercializarea şi utilizarea produselor de uz fitosanitar pentru combaterea bolilor, dăunătorilor şi buruienilor în agricultură şi silvicultură, actualizată
- Legea nr.359/2004 - privind simplificarea formalităţilor la înregistrarea în registrul comerţului a persoanelor fizice, asociaţiilor familiale şi persoanelor juridice, înregistrarea fiscală a acestora, precum şi la autorizarea funcţionării persoanelor juridice, actualizată
- Legea nr.360/2003 - privind regimul substanţelor şi preparatelor chimice periculoase, republicată
- Legea nr. 279/2005 privind ucenicia la locul de muncă, republicată
- Legea nr. 346/2002 privind asigurarea pentru accidente de muncă şi boli profesionale, republicată
- O.U.G. nr. 44/2008 privind desfăşurarea activităţilor economice de către persoanele fizice autorizate, întreprinderile individuale şi întreprinderile familiale, actualizată
- Legea nr. 349/2007 privind reorganizarea cadrului instituţional în domeniul managementului substanţelor chimice, actualizată
- Legea nr. 52/2011 privind exercitarea unor activităţi cu caracter ocazional desfăşurate de zilieri, republicată
- H.G. nr. 33/2018 privind stabilirea contravenţiilor care intră sub incidenţa Legii prevenirii nr. 270/2017, precum şi a modelului planului de remediere
- H.G. nr. 300/2006 - privind cerinţele minime de securitate şi sănătate pentru şantierele temporare sau mobile, actualizată
- H.G. nr. 493/2006 - privind cerinţele minime de securitate şi sănătate referitoare la expunerea lucrătorilor la riscurile generate de zgomot, actualizată
- H.G. nr. 971/2006 - privind cerinţele minime pentru semnalizarea de securitate şi/sau de sănătate la locul de muncă
- H.G.nr.1028/2006 - privind cerinţele minime de securitate şi sănătate în muncă referitoare la utilizarea echipamentelor cu ecran de vizualizare
- H.G. nr.1048/2006 - privind cerinţele minime de securitate şi sănătate pentru utilizarea de către lucrători a echipamentelor individuale de protecţie la locul de muncă
- H.G.nr.1049/2006 - privind cerinţele minime pentru asigurarea securităţii şi sănătăţii lucrătorilor din industria extractivă de suprafaţă sau subteran
- H.G.nr.1050/2006 - privind cerinţele minime pentru asigurarea securităţii şi sănătăţii lucrătorilor din industria extractivă de foraj
- H.G.nr.1051/2006 - privind cerinţele minime de securitate şi sănătate pentru manipularea manuala a maselor care prezintă riscuri pentru lucrători, în special de afecţiuni dorsolombare

- H.G.nr.1058/2006 - privind cerinţele minime pentru îmbunătăţirea securităţii şi protecţia sănătăţii lucrătorilor care pot fi expuşi unui potenţial risc datorat atmosferelor explozive
- H.G.nr.1091/2006 - privind cerinţele minime de securitate şi sănătate pentru locul de muncă
- H.G.nr.1092/2006 - privind protecţia lucrătorilor împotriva riscurilor legate de expunerea la agenţi biologici în muncă
- H.G.nr.1093/2006 - privind stabilirea cerinţelor minime de securitate şi sănătate pentru protecţia lucrătorilor împotriva riscurilor legate de expunerea la agenţi cancerigeni sau mutageni la locul de muncă, modificată
- H.G.nr.1218/2006 - privind stabilirea cerinţelor minime de securitate şi sănătate în muncă pentru asigurarea protecţiei lucrătorilor împotriva riscurilor legate de prezenţa agenţilor chimici, actualizată
- H.G.nr.520/2006 - privind cerinţele minime de securitate şi sănătate referitoare la expunerea lucrătorilor la riscurile generate de câmpuri electromagnetice
- H.G.nr.1876/2005 - privind cerinţele minime de securitate şi sănătate referitoare la expunerea lucrătorilor la riscurile generate de vibraţii, actualizată
- H.G.nr.1875/2005 - privind protecţia sănătăţii şi securităţii lucrătorilor faţă de riscurile datorate expunerii la azbest, actualizată
- H.G.nr.409/2016 - privind stabilirea condiţiilor pentru punerea la dispoziţie pe piaţă a echipamentelor electrice de joasă tensiune
- H.G.nr.1102/2014 - privind cerinţele minime de securitate şi sănătate în muncă referitoare la expunerea lucrătorilor la riscurile generate de radiaţiile optice artificiale
- H.G.nr.612/2010 - privind stabilirea condiţiilor pentru punerea la dispoziţie pe piaţă a articolelor pirotehnice
- H.G.nr.1029/2008 - privind condiţiile introducerii pe piaţă a maşinilor, actualizată
- H.G.nr.600/2007 - privind protecţia tinerilor la locul de muncă
- H.G.nr.355/2007 - privind supravegherea sănătăţii lucrătorilor, actualizată
- H.G. nr. 1007/2006 privind cerinţele minime de securitate şi sănătate referitoare la asistenţa medicală la bordul navelor
- H.G. nr. 1135/2006 privind cerinţele minime de securitate şi sănătate în muncă la bordul navelor de pescuit
- H.G. nr. 1146/2006 privind cerinţele minime de securitate şi sănătate pentru utilizarea în muncă de către lucrători a echipamentelor de muncă
- HG nr. 243/2013 privind cerinţele minime de securitate şi sănătate în muncă pentru prevenirea rănirilor provocate de obiecte ascuţite în activităţile din sectorul spitalicesc şi cel al asistenţei medicale
- H.G. nr. 557/2007 privind completarea măsurilor destinate să promoveze îmbunătăţirea securităţii şi sănătăţii la locul de muncă pentru salariaţii încadraţi în baza unui contract individual de muncă pe durată determinată şi pentru salariaţii temporari încadraţi la agenţi de muncă temporară
- H.G. nr. 867/2009 privind interzicerea muncilor periculoase pentru copii
- H.G. nr. 855/2013 pentru aprobarea Normelor metodologice de aplicare a prevederilor Legii nr. 279/2005 privind ucenicia la locul de muncă

- H.G. nr. 537/2004 pentru aprobarea Normelor metodologice de aplicare a prevederilor Ordonanţei de urgenţă a Guvernului nr. 96/2003 privind protecţia maternităţii la locurile de muncă, cu modificările şi completările ulterioare, actualizată
- H.G. nr. 580/2000 pentru aprobarea Normelor metodologice de aplicare a prevederilor Ordonanţei de urgenţă a Guvernului nr. 99/2000 privind măsurile ce pot fi aplicate în perioadele cu temperaturi extreme pentru protecţia persoanelor încadrate în muncă
- H.G. nr.573/2002 pentru aprobarea procedurilor de autorizare a funcţionării comercianţilor
- H.G. nr. 1156/2002 pentru aprobarea Memorandumului de înţelegere dintre Guvernul României şi Organizaţia Internaţională a Muncii privind eliminarea muncii copilului, semnat la Geneva la 18 iunie 2002
- H.G. nr. 1.256/2011 privind condiţiile de funcţionare, precum şi procedura de autorizare a agentului de muncă temporară
- Ordinul ministrului muncii, familiei şi egalităţii de şanse nr. 1102/2008 privind avizarea spaţiilor destinate depozitării muniţiilor, capselor sau pulberilor pentru muniţie
- Ordinul ministrului muncii, familiei şi protecţiei sociale nr. 455/2010 pentru constituirea comisiilor de abilitare a serviciilor externe de prevenire şi protecţie şi de avizare a documentaţiilor cu caracter tehnic de informare şi instruire în domeniul securităţii şi sănătăţii în muncă din cadrul inspectoratelor teritoriale de muncă
- Ordinul ministrului muncii, solidarităţii sociale şi familiei nr. 3/2007 privind aprobarea Formularului pentru înregistrarea accidentului de muncă — FIAM
  Ordinul ministrului muncii nr. 242/2007 pentru aprobarea Regulamentului privind formarea specifică de coordonator în materie de securitate şi sănătate pe durata elaborării proiectului şi/sau a realizării lucrării pentru şantiere temporare ori mobile
- Ordinul ministrului muncii, solidarităţii sociale şi familiei nr. 450/2006 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 346/2002 privind asigurarea pentru accidente de muncă şi boli profesionale, cu modificările şi completările ulterioare
- Ordinul nr. 875/2002 al ministrului sănătăţii şi familiei privind stabilirea atribuţiilor medicului de medicină generală / medicină de familie cu competenţă în medicina de întreprindere
- Ordinul nr. 1260/2013 pentru aprobarea Normelor metodologice privind examinarea medicală şi psihologică a personalului cu atribuţii în siguranţa transporturilor şi periodicitatea examinării
- Ordinul nr. 803/2001 al ministrului sănătăţii şi familiei privind aprobarea unor indicatori de expunere şi/sau de efect biologic relevanţi pentru stabilirea răspunsului specific al organismului la factori de risc de îmbolnăvire profesională

Legislatie in domeniul relatiilor de munca

Identificarea şi combaterea muncii nedeclarate: încadrarea, executarea, modificarea, suspendarea şi încetarea activităţii persoanelor care desfăşoară orice activitate în temeiul unui contract individual de muncă:

- Legea nr. 53/2003, cu modificările și completările ulterioare – Codul muncii

Întocmirea, completarea şi transmiterea registrului general de evidenţă a salariaţilor:

- H.G. nr. 905/2017 privind registrul general de evidență a salariaților
- H.G. nr. 1164/2022 privind aprobarea Procedurii de acces online al salariatilor sau fostilor salariati la datele din registrul general de evidenta a salariatilor, a modalitatii de generare si

descarcare a extrasului, precum si a conditiilor in care prin extras se poate dovedi vechimea in munca si/sau specialitate.

- Legea nr. 53/2003, republicată, cu modificările și completările ulterioare – Codul muncii

Încadrarea în muncă, în România, a cetăţenilor străini:

- O.U.G. nr. 25/2014 privind încadrarea în muncă şi detaşarea străinilor pe teritoriul României și pentru modificarea și completarea unor acte normative privind munca străinilor în România

Protecţia cetăţenilor români care lucrează în străinătate:

- Legea nr. 156/2000 privind protecţia cetăţenilor români care lucrează în străinătate, republicată
- H.G. nr. 384/2001 pentru aprobarea Normelor metodologice de aplicare a prevederilor Legii nr. 156/2000 privind protecția cetățenilor români care lucrează în străinătate, cu modificările și completările ulterioare

Detaşarea salariaţilor în cadrul prestării de servicii transnaţionale:

- Legea nr. 16/2017 privind detaşarea salariaţilor în cadrul prestării de servicii transnaţionale, cu modificările și completările ulterioare
- H.G. nr. 337/2017 pentru aprobarea Normelor metodologice privind detaşarea salariaţilor în cadrul prestării de servicii transnaţionale pe teritoriul României

Respectarea condiţiilor de funcţionare a agenţilor de muncă temporară:

- H.G. nr. 1.256/2011 privind condițiile de funcționare, precum și procedura de autorizare a agentului de muncă temporară

Prestarea activităţii de către lucrătorii zilieri:

- Legea nr. 52/2011 privind exercitarea unor activităţi cu caracter ocazional desfăşurate de zilieri, republicată, cu modificările și completările ulterioare

Alte competențe:

- Legea nr. 279/2005 privind ucenicia la locul de muncă, republicată
- H.G. nr. 855/06.11.2013 pentru aprobarea Normelor metodologice de aplicare a prevederilor Legii nr. 279/2005 privind ucenicia la locul de muncă
- Legea nr. 367/2022 privind dialogul social
- Legea nr. 335/2013 privind efectuarea stagiului pentru absolvenţii de învăţământ superior, cu modificările și completările ulterioare
- H.G. nr. 473/2014 pentru aprobarea Normelor metodologice de aplicare a prevederilor Legii nr. 335/2013 privind efectuarea stagiului pentru absolvenţii de învăţământ superior, cu modificările și completările ulterioare
- Legea nr. 76/2002 privind sistemul asigurărilor pentru şomaj şi stimularea ocupării forţei de muncă, cu modificările și completările ulterioare
- Legea nr. 202/2002 privind egalitatea de şanse şi de tratament între femei şi bărbaţi, republicată, cu modificările și completările ulterioare
- O.U.G. nr. 96/2003 privind protecţia maternităţii la locurile de muncă, cu modificările și completările ulterioare

- H.G. nr. 537/2004 pentru aprobarea Normelor metodologice de aplicare a prevederilor Ordonanței de urgenta a Guvernului nr. 96/2003 privind protecția maternității la locurile de munca, cu modificările si completările ulterioare
- Legea nr. 67/2006 privind protecţia drepturilor salariaţilor în cazul transferului întreprinderii, al unităţii sau al unor părţi ale acestora, cu modificările și completările ulterioare
- Legea nr. 467/2006 privind stabilirea cadrului general de informare şi consultare a angajaţilor, cu modificările și completările ulterioare
- O.U.G. nr. 44/2008 privind desfăşurarea activităţilor economice de către persoanele fizice autorizate, întreprinderile individuale şi întreprinderile familiale, cu modificările și completările ulterioare
- Ordinul Ministerului Sănătății nr. 870/2004 pentru aprobarea Regulamentului privind timpul de muncă, organizarea şi efectuarea gărzilor în unităţile publice din sectorul sanitar, cu modificările și completările ulterioare.

Alte legi / hotărâri de guvern / ordonanțe de guvern / ordine / regulamente / statute care fac trimitere la existența raporturilor de muncă în baza contractelor individuale de muncă

Controalele se desfăşoară în temeiul şi cu respectarea următoarelor acte normative:

- Legea nr. 108/1999 privind înfiinţarea şi organizarea Inspecţiei Muncii, republicată, cu modificările şi completările ulterioare
- Hotărârea Guvernului nr. 488/2017 privind aprobarea Regulamentului de organizare şi funcţionare a Inspecţiei Muncii
- O.U.G. nr. 2/2001 privind regimul juridic al contravenţiilor, cu modificările şi completările ulterioare.

Reglementări generale:

- Legea 135/2007 privind arhivarea documentelor in forma electronica
- Legea nr. 544/2001, privind liberul acces la informaţiile de interes public, cu modificările și completările ulterioare;
- Hotărârea Guvernului nr. 123/2002 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 544/2001 privind liberul acces la informaţiile de interes public, cu modificările și completările ulterioare;
- Hotărârea Guvernului nr. 478/2016 pentru modificarea și completarea Normelor metodologice de aplicare a Legii nr. 544/2001 privind liberul acces la informaţiile de interes public, cu modificările și completările ulterioare;
- Hotărârea Guvernului nr. 830/2022 pentru modificarea și completarea Normelor metodologice de aplicare a Legii nr. 544/2001 privind liberul acces la informaţiile de interes public, cu modificările și completările ulterioare;
- Ordonanţa Guvernului nr. 27/2002 privind reglementarea activităţii de solutionare a petitiilor, cu modificările și completările ulterioare;
- Legea nr. 233 / 2002 pentru aprobarea Ordonanţei Guvernului nr. 27/2002 privind reglementarea activităţii de soluţionare a petitiilor.

Lista prezentată nu este exhaustivă, proiectarea și dezvoltarea sistemului informatic urmând a fi realizate în baza legilației în vigoare la momentul implementării.

2 INFORMAŢII PRIVIND PROIECTUL

2.1 Situaţia actuală

Sistemul informatic actual SIAMC (Sistemul Informatic pentru Activitati de Monitorizare si Control), denumit intern COLUMBO, este componenta principală a proiectului "Combaterea muncii la negru și sporirea securității muncii în România prin îmbunătățiri de structură și proces în cadrul Inspecției Muncii" COD SMIS 48591, proiect finanțat prin fonduri europene - Programul Operațional Sectorial Creșterea Competitivității Economice, Axa Prioritară III "Tehnologia Informației si Comunicațiilor pentru sectoarele privat și public", Domeniul Major de Intervenție 2 „Dezvoltarea și creșterea eficienței serviciilor publice electronice", Operațiunea 1 „Susținerea implementării de soluții de e-guvernare și asigurarea conexiunii la broadband, acolo unde este necesar", APEL 5, a fost pus în funcțiune în anul 2015, având ca scop creșterea calității inspecțiilor pentru combaterea muncii fără forme legale contribuind în același timp la îndeplinirea obiectivelor Programului Național de Reforme (PNR) care urmărește diminuarea acestui fenomen național.

SIAMC este un pachet de funcționalități integrate pentru coordonarea electronică a proceselor din domeniul specific instituției și are drept scop unificarea și uniformizarea activităților principale desfășurate anterior prin intermediul unor aplicații informatice diferite și centralizarea a datelor la nivelul Inspecției Muncii.

Acesta este format din următoarele **componente**:

- Portalul intern: permite înregistrarea informațiilor rezultate în urma controalelor, administrarea eficientă a formularelor și documentelor, gestionarea diferitelor petiții, gestionarea accidentelor de muncă (comunicare evenimente, procese verbale de cercetare, FIAM) dar și generarea automată de rapoarte pentru fiecare județ în parte;
- Aplicația de tableta Windows mobile: asigură inspectorilor acces la o serie de date atunci când se află pe teren;
- Portalul extern: facilitează înregistrarea on-line a petițiilor depuse de cetățeni, asigurând informarea rapidă a acestora cu privire la cadrul legal, situația achizițiilor publice, dar și date despre angajatori. În acest fel se favorizează interacțiunea dintre instituție și simplii cetățeni, prin posibilitatea transmiterii de documente și a vizualizării răspunsurilor într-un mod electronic.
- Aplicația mobilă Registrul electronic de evidență a zilierilor: având în vedere modificările legislative asupra Legii 52/2011 privind exercitarea unor activități cu caracter ocazional desfășurate de zilieri, prin care instituția a pus la dispoziția beneficiarilor care se încadrează în sfera activităților pentru care se pot utiliza zilieri Registrul electronic de evidență a zilierilor, disponibil atât print-un portal web cât și prin aplicația mobilă.

În prezent, în cadrul Inspecției Muncii și inspectoratelor teritoriale de muncă, nivelul de digitalizare este redus, mare parte dintre activitățile care s-ar putea realiza digital fiind încă realizate pe suport de hârtie. Neimplementarea semnăturii electronice și inexistența unor programe informatice adecvate, au ca efect îngreunarea activității, generarea și circuitul documentelor specifice activității neputându-se realiza exclusiv în format electronic. Întocmirea documentelor de control se realizează pe suport de hârtie, prin completarea documentelor cu regim special (proces verbal de control și proces verbal de constatare și sancționare a contravenților) și a anexelor, care, chiar dacă pot fi întocmite electronic,trebuie printate, neexistând posibilitatea întocmirii, semnării și comunicării electronice, conform prevederilor legale și procedurilor de lucru actuale, fapt care îngreunează activitatea de control și procedura ulterioară de comunicare a acestora către contravenient și către organele fiscale. Totodată, în prezent, angajatorii transmit electronic, către inspectoratele teritoriale de muncă, diferitele notificări/ comunicări, conform

cerințelor legale (ex. detașare transnațională, utilizarea frecventă a muncii de noapte, situația persoanelor plasate la muncă în străinătate, etc) prin e-mail, documente care ulterior sunt printate și își urmează circuitul în instituție în format de hârtie. De asemenea, completarea în format electronic a fișelor de instruire a lucrătorilor în domeniul securității și sănătății în muncă și a fișelor de aptitudine, care se completează, în prezent, pe format de hârtie.

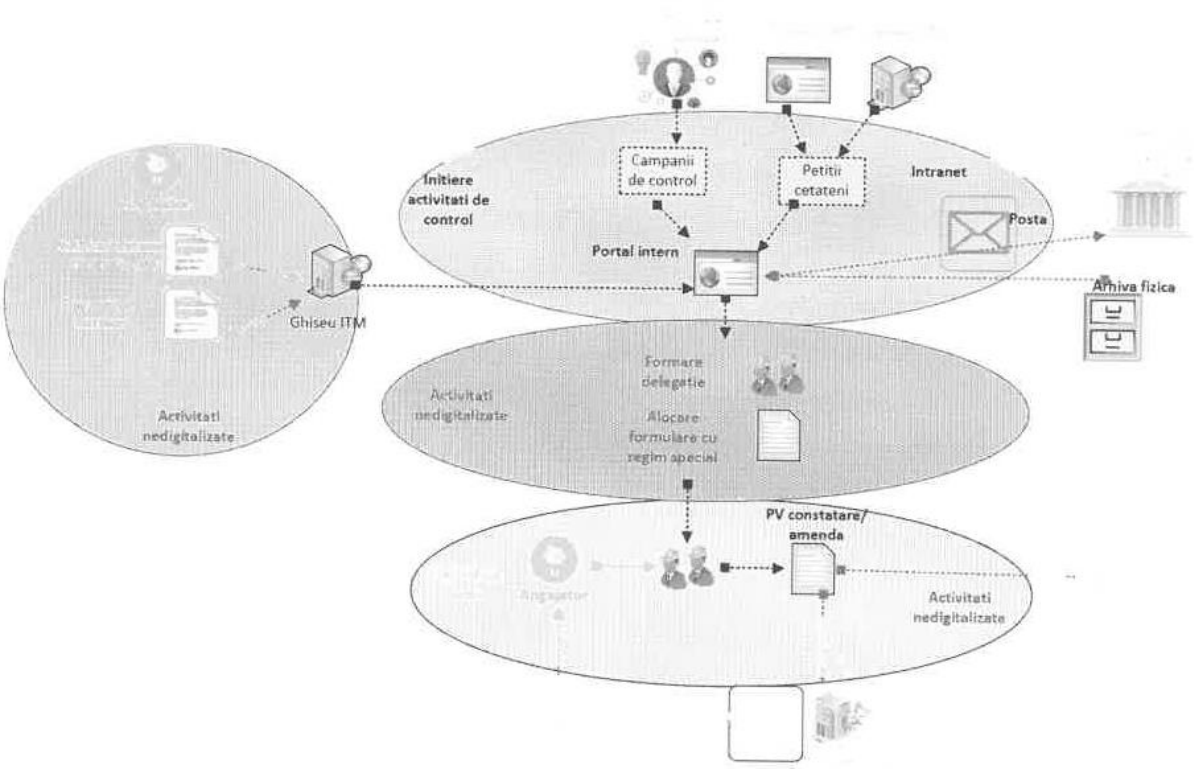


Figura 1 Diagramă activități de control

2.2 Rezultatele analizei

2.2.1 Infrastructura hardware existentă

Un număr considerabil de echipamente (Laptop, PC, All in One) utilizate în mod curent în cadrul inspectoratelor teritoriale de muncă dispun de procesoare foarte vechi ce nu mai fac față complexității programelor folosite și fluxului de lucru din cardul inspectoratelor teritoriale de muncă. Acest lucru, împreună cu memoria RAM foarte scăzută a acestora (mai mult de jumătate din echipamente au 4GB memorie RAM sau mai puțin) duc la o creștere substanțială a timpului necesar pentru realizarea anumitor task-uri. Se recomandă realizarea unui upgrade tehnologic în cel mai scurt timp pentru a fluidiza procesele din cadrul ITM-urilor și pentru a atinge un grad cât mai ridicat de eficiență din punct de vedere IT.

Cele mai multe dintre monitoarele aflate în locații dispun de un display mai mic de 22''. Privind din mai multe perspective, acest lucru este dăunător atât personalului ce îl folosește (un ecran mic folosit pentru un timp îndelungat poate duce la agravarea sănătății celui ce îl folosește) cât și instituției ce nu își folosește la capacitate maximă resursele umane din cadrul acesteia (o persoană dă un randament mai mare în momentul în care poate vizualiza mai multă informație la un moment dat).

Din punctul de vedere al echipamentelor de printare, s-a constatat existența unor lipsuri considerabile întrucât în mai multe locații nu existau suficiente echipamente de printing iar, de multe ori, cele ce existau nu erau funcționale la capacitate maximă sau nu se puteau folosi deloc.

În ceea ce privește vechimea calculatoarelor, aceasta indică o nevoie majoră de schimbare a echipamentelor întrucât mai mult de jumătate dintre echipamentele trecute în chestionarele primite sunt mai vechi de anul 2016 (1167 din 2240).

Mare parte din infrastructură de rețea este uzată și este recomandată înlocuirea echipamentelor de rețea, a serverelor și creșterea lățimii de bandă alocate fiecărui ITM/punct lucru/IM.

În urma analizării sistemelor de operare instalate, s-a constatat preponderența echipamentelor de calcul cu sisteme de operare noi (Windows 10 sau Windows 11). Deși aparent un lucru bun, având în vedere procesoarele prezente pe aceste dispozitive și faptul că sistemele de operare noi sunt din ce în ce mai complexe și necesită o putere de procesare semnificativă, instalarea acestora pe un echipament cu specificații învechite duce la folosirea unui procent mult prea mare din puterea de procesare și din memoria calculatorului numai pentru a putea suporta un astfel de sistem de operare. Acest fapt duce la suprasolicitarea sistemului chiar și în momentul utilizării reduse sau moderate a acestuia.

Deși ponderea mai mare este cea a sistemelor de operare Windows 10 sau 11, există totuși aproximativ 800 de echipamente ce folosesc sisteme de operare mai vechi de Windows 8. Aceste sisteme de operare nu mai dispun de suport din partea Microsoft și nu mai beneficiază de update-uri periodice pentru a putea face față schimbărilor constante și amenințărilor cibernetice ce ar putea apărea pe parcursul timpului. Acest fapt reprezintă o breșă majoră de securitate în cardul ITM-urilor și se recomandă ferm renunțarea la aceste sisteme de operare și înlocuirea acestora cu variantele mai recente. Pentru rezultatul dorit, această înlocuire este necesar să se facă împreună cu înlocuirea echipamentelor cu putere de procesare mult prea mică pentru a suporta complexitatea SO-urilor recente.

Analiza exacta asupra tehnicii de calcul existente este următoarea*:

Locatie	**SCOR ***
DAMBOVITA	128,2761643
SATU MARE	99,71639757
HARGHITA	97,7563072
CALARASI	93,59974575
CONSTANTA	92,17121144
IALOMITA	90,89286763
BOTOSANI	89,80313197

SALAJ	86,54366622
BIHOR	86,30991146
VASLUI	85,52196249
VALCEA	83,44735135
TULCEA	81,43607587
BACAU	81,2076966
TIMIS	78,20287703
ALBA	77,23245773
BRAILA	76,45538148
BUCURESTI	76,31208612
SIBIU	76,14784505
CARAS	75,19881471
BUZAU	73,73017663
IASI	73,42281918
VRANCEA	72,76373875
GIURGIU	72,06557307
TELEORMAN	71,39944011
GORJ	70,92227273
CLUJ	70,40650159

BRASOV	70,29671871
MURES	67,2027539
OLT	65,91231604
ILFOV	63,87800843
HUNEDOARA	62,39770502
BISTRITA	60,28059122
COVASNA	60,07527449
ARAD	58,43916475
DOLJ	55,22052227
SUCEAVA	50,75106663
NEAMT	48,34664849
ARGES	44,44320962
MARAMURES	42,9081431
PRAHOVA	39,63478861
MEHEDINTI	37,36977528
GALATI	34,65714286

*scorul a fost calculat luând în considerare tipul echipamentelor de birou existente, generația acestora, generația și caracteristicile procesoarelor ce le echipează, memoria RAM, capacitatea de stocare.

2.2.2 Digitalizarea activității de control

Pentru a avea o activitate de control eficienta dar și servicii de calitate oferite cetățenilor și mediului de afaceri, este necesara digitalizarea activitatilor de control, activitatilor conexe, de exemplu de completare a fișelor de instruire, și a altor documente din domeniile relațiilor de munca și securității și sănătății in muncă, prin crearea unui sistem informatic nou, actualizat la nivelul de evolutie tehnologica,

cu o securitate informatica sporita și care va aduce mai multe îmbunătățiri activității din prezent a instituției, cele mai importante fiind următoarele:

- Digitalizarea activitatii de control, prin implementarea unui sistem informatic adecvat și a semnaturilor electronice, de Ia întocmirea documentelor specifice pana Ia comunicarea acestora atat entității controlate cat și organelor fiscale, în cazul aplicarii amenzii, are ca efect diminuarea timpului alocat controlului, respectiv, alocat aspectelor procedurale aferente și, implicit, creșterea timpului alocat verificarilor, fapt care conduce Ia îmbunatatirea activitatății de control.
- Simplificarea procedurii de comunicare este atat în beneficiul institutiei cat și în beneficiul destinatarului, respectiv angajatorul controlat și organele fiscale care verifica plata amenzii, sau, dupa caz, procedeaza Ia executarea obligatiei fiscale. Accesarea de pe teren, prin utilizarea unor dispozitive mobile, respectiv, laptopuri și telefoane, a datelor necesare efectuarii controlului, existente în baza de date a Inspecției Muncii precum și a altor institutii (ANAF, ONRC, etc.) conduce Ia efectuarea unor verificări mai complete. De exemplu, se va putea verifica daca salariatul a fost declarat și autoritatilor fiscale, sau daca datele declarate sunt aceleași cu cele din contractul individual de munca.
- Eliminarea procedurii de afișare a documentelor de control catre entitatea controlata, faciliteaza procedura de comunicare a acestora, renuntand Ia o procedura anacronica de "lipire pe ușa contravenientului". în favoarea unei modalitati adaptate secolului XXI, din punctul de vedere al nivelul tehnologic de evolutie în privinta relatiei dintre entitatea controlata și administratie. Acest lucru este atat în beneficiul institutiei, prin scurtarea timpului alocat problemelor procedurale ca o consecinta a eliminarii dificultatilor procedurale implicate, prin deplasarea Ia sediul angajatorului și gasirea unui martor și a entitatii controlate prin eliminarea prejudiciului de imagine pe care îl poate genera faptul ca documentul este vizibil pentru oricine din acea locatie și nu doar pentru acesta. In același timp, comunicarea electronica elimina necesitatea comunicarii documentelor direct contravenientului, care necesita deplasarea acestuia (atunci cand documentele nu sunt lncheiate Ia sediul social), Ia inspectoratul teritorial de munca sau în alta parte, pentru a primi raportul de control.
- lmplementarea unui sistem informatic care sa permita cetatenilor completarea și transmiterea online a petitiilor/altor solicitari direct în sistem electronic, crearea unui modul electronic de raspuns automat Ia întrebarile acestora, crearea pentru angajatori, a posibilitatii de a completa și transmite on-line notificarile/comunicarile etc., necesare pentru a îndeplini obligatiile legale aferente, conduce, de asemenea, Ia îmbunatatirea calitatii serviciilor oferite cetatenilor și mediului de afaceri, prin reducerea birocratiei, facilitarea comunicarii dintre cetateni și administratie, scurtarea timpilor de solutionare a aspectelor semnalate și a solicitarilor acestora. De exemplu, completarea pe un formular disponibil on-line a notificarilor privind detașarea In cadrul prestarii de servicii transnationale, semnarea electronica și transmiterea acestora automata, catre inspectoratul teritorial de munca destinatar, vine atat în sprijinul prestatorilor cat și al lnspectiei Muncii, prin realizarea unei evidente imediate a prestatorilor care detașeaza lucratori pe teritoriul Romaniei și a salariatilor detașati, fapt care va conduce, nu doar Ia o evidenta reala și corecta a acestora, dar și Ia eficientizarea actiunilor de control In acest domeniu prin facilitarea accesului imediat, de catre inspectorii de munca, Ia datele declarate.
- Digitalizarea activității de evidență a instruirii lucrătorilor și a supravegherii medicale.
- Digitalizarea activitatii desfașurate în beneficiul cetatenilor, prin generarea atat a documentelor interne cat și a celor destinate cetatenilor, mediului de afaceri și altor institutii, utilizarea semnaturii electronice, realizarea circuitului acestora, inclusiv arhivarea, în format electronic, conduce Ia îmbunatatirea calitatii serviciilor oferite cetatenilor și mediului de afaceri, prin utilizarea mai eficienta a resurselor și scurtarea timpilor de raspuns Ia solicitarile primite.

2.2.2.1 Sistem informatic integrat

Realizarea proiectului presupune implementarea a minim 3 componente informatice suport, dupa cum urmeaza:

I. Implementarea unui Sistem de Management Electronic al Documentelor (SMED), care sa asigure suport pentru circuitul în format digital al documentelor și al activităților specifice de monitorizare și control, inclusiv în ceea ce privește avizarea/aprobarea documentelor și comunicărilor utilizate in activitatea derulata.

Sistemul implica utilizarea, Ia nivelul institutiei, a fluxurilor electronice, incepand cu crearea de documente proprii/utilizare formulare folosite în activitatea de control/înregistrare a intrării documentelor provenite de Ia entități externe, pana Ia finalizare, prin descărcarea din evidenta (remitere către angajatori/alte instituții publice, arhivare/distrugere electronica, dupa caz).

Resurse/măsuri necesare:

- semnatura electronica, capacitate stocare, conexiune publica și securizata Ia Internet, flux INTRANET (fluxul documentelor interne, inclusiv cele dedicate celorlalte instituții componente ale MMSS);
- creare Spatiu Privat Virtual destinat atât instituțiilor de stat cât și entităților private, gestionat Ia nivelul lnspecției Muncii sau integrat în SPV existent Ia nivel național;
- modificarea prevederilor legale astfel încât sa permită inițierea, derularea și finalizarea unor acțiuni de control exclusiv prin fluxuri electronice de transmitere a datelor și privind obligativitatea inrolarii în SPV și acceptarea acestuia ca suport de comunicare oficială între lnspectia Muncii și entitati de stat/private;
- modificarea si completarea legislatiei, inclusiv cea cu privire Ia comunicarea actelor cu caracter administrativ (ex O.G. 2/2001, etc.).
- elaborarea metodologiilor si procedurilor operationale necesare utilizarii de catre toti angajatii IM/ITM a sistemului informatic si a fluxurilor de lucru.

Prin intermediul echipamentelor mobile de control (laptopuri, telefoane, etc), inspectorul de munca va avea acces la toate datele disponibile în sistem, potrivit drepturilor de acces conferite.

Sistemul presupune

- crearea posibilitatii efectuarii controlului, integral, Ia locul unde se desfașoara activitatea și se face identificarea persoanelor gasite in activitate. De exemplu sistemul informatic ar trebui sa deschida o pagina de control a angajatorului, în care datele de identificare ale inspectorului de muncă sunt preluate automat la logarea acestuia în sistem, iar datele privind unitatea controlată, inclusiv geolocația urmând a fi importate în momentul selectării acesteia pentru control.
- Sistemul informatic va conține câmpuri în care inspectorul de munca, după ce a legitimat lucrătorii găsiți în activitate, să introducă CNP și/sau numele acestora și data nașterii.
- Această pagină electronică de control va genera, automat, și urmatoarele informatii: dacă Ia societatea controlată se află un control deja în desfașurare, inițiat de același inspectorat sau de un alt inspectorat din țară, daca există petiții înregistrate pentru angajatorul supus controlului, sanctiuni aplicate și masuri dispuse în controalele anterioare, informatii privind accidente de munca înregistrate.
- Posibilitatea sistemului informatic de a realiza controlul a identificarea persoanei prin interconectarea cu aplicații ale oricăror altor instituții sau prin platforma națională de interoperatibilitate (vezi Lg 242/2022).

- Va genera o fisa a angajatorului cu elemente din care sa reiasă gradul de prioritate a controlului la acel angajator.
- utilizarea de generatoare de formulare electronice pentru fiecare document operat/ generat in cadrul activitatii de control/ inspectie cu scopul de a se crea posibilitatea extragerii informațiilor necesare întocmirii oricărui tip de raportare din fiecare document emis de inspectorul de muncă (în principal proces-verbal de contraventie și anexa proces-verbal control, proces-verbal de constatare și sanctionare a contraventiilor, proces-verbal de sistare activitate/ oprire din functionare echipament de munca, fisa unitatii, etc). Acest demers presupune utilizarea de câmpuri editabile, acestea urmand a fi stabilite în functie de informatiile necesare pentru generarea automata a raportărilor.
- Generarea procesului-verbal de control/PVCSC, etc - se va putea realiza automat la momentul initierii documentului, cu alocarea automată a numarului si, a datei în momentul finalizarii si salvarii documentului efectuarii controlului. Sistemul va permite generarea automată, dupa caz, a urmatoarelor documente :
    - Proces Verbal de Control – formular tipizat
    - Anexele Ia Procesul Verbal de Control (Fișa unitatii și Anexa constatari și masuri). Sistemul va permite preluarea informatiilor privind îndeplinirea masurilor dispuse în urma controalelor, cat si atentionari privind expirarea termenului de realizare a masurilor. Aceste documente vor purta acelasi numar si data ca procesul verbal de control
    - Procesul Verbal de Constatare și Sanctionare a Contraventiilor - sistemul va permite generarea automata a adreselor de înștiintare catre ANAF - pentru luarea în debit a amenzilor a plicate în urma controlului. Sistemul va permite inregistrarea informatiilor privind plata amenzilor aplicate precum și a contestatiiilor depuse împotriva acestora. Atentionari privind termenul de transmitere la ANAF.
    - Procesul Verbal de sistare activitate/ oprire din functionare echipament de munca.
    - Înștiințare control
- toate documentele generate în format electronic, vor putea fi:
    - printate pe suport hartie (documentele semnate olograf)
    - semnate și transmise în format electronic.
- interconectarea platformei nou-create cu platfomele ANAF, cele ale RECOM, etc. Accesul de la sediu și de pe teren Ia platformele REGES-ONLINE și SIAMC 2.0, precum și Ia baza de date a altor institutii: ANAF- Declaratia 112, iar prin intersectarea înregistrărilor bazelor de date ANAF și REGES-ONLINE să fie semnalate automat, eventuale diferențe; ONRC, Evidența populației, ANOFM, ANPIS, CNPP, IGI – ex: pentru a putea verifica, în timpul efectuării controlului, dacă pentru lucrătorul străin identificat a fost emis un aviz de munca, etc..
- crearea posibilității generării și completării pe teren, în format electronic, pe dispozitive mobile, a proceselor verbale de control, a proceselor verbale de constatare și sancționare a contravențiilor, a proceselor verbale de sistare activitate/oprire din functionare echipament se munca, cat si a instiintarilor, și semnarea acestora de către inspectorul de muncă, în calitate de agent constatator, cu semnatură electronică.
- rapoarte privind rezultatele campaniilor și actiunilor de control.
- rapoarte si extrase privind oricare dintre datele existente în sistem care sa poată fi organizate sub formă de dashboard de catre utilizatorii sistemului informatic.
- calcularea automata a indicatorilor de performanta in baza algoritmilor introduși Ia nivelul Inspecției Muncii.

- prelucrări pe criterii multiple, selectabile de catre utiliztor, pentru analiza și luarea deciziilor în baza informatiilor existente în sistemul informatic.
- comunicarea electronica prin intermediul functionalitatii de tipul spatiului virtual privat, entitatii controlate, a documentelor întocmite cu ocazia controlului, semnate electronic de catre inspectorii de muncă.
- comunicarea electronica, catre organele fiscale, a proceselor verbale de constatare și sanctionare a contraventiilor, în vederea executarii amenzilor aplicate.
- asigurarea unui circuit automat al documentelor, în functie de ordinea semnarii acestora, prin transmiterea automata a documentului catre urmatorul semnatar și prin emiterea unei notificari prin care acesta este lnștiintat ca a primit un document spre semnare/avizare. Crearea posibilității de retur cu observații a documentului supus semnării/avizării în situația în care se consideră că documentul trebuie modificat/completat
- Emiterea, Ia date prestabilite, de rapoarte automate privitoare Ia termenele de valabilitate/ pana Ia care trebuie emis un document. Asigurarea unui motor de cautare a documentelor și a posibilitatii ca acestea sa fie etichetate pentru a putea fi gasite mai ușor în arhiva.
- programul va permite interogari/ analize/ rapoarte care sa extraga date multiple necesare în activitatea de raportare, centralizare și control a activitatii (Ex: verificarea unui angajator sa includa date/ PVC/ PVCSC Ia nivel national și nu doar Ia nivel de judet, extragerea de date (controale/sanctiuni) pentru fiecare inspector, interogarea (pentru fiecare inspector/ ITM) separat pentru fiecare act normativ avut ca obiectiv de control, etc.), interogari pentru analiza accidentelor de munca lnregistrate/generarea de rapoarte dinamice cu posibilitatea utilizarii de criterii multiple de filtrare a datelor existente In sistem.
- Crearea unei posibilități de căutare a punctelor de lucru din diverse județe
- crearea posibilitatii angajatorilor/persoanelor fizice ca, prin utilizarea unei interfete special create, sa emita și sa transmita catre inspectorate orice tip de document. În acest sens, interfata ar trebui sa cuprinda module aferente fiecarui segment de activitate al inspectoratului care presupune interactiunea cu angajatorii/persoanele fizice, module care sa cuprinda generatoare pentru toate documentele care beneficiaza de o reglementare legala. Acestea vor avea un format predefinit, în concordanță cu prevederile legale incidente. Tot prin intermediul acestei interfete trebuie asigurata, pe langa generare și semnare electronica, transmiterea respectivelor documente catre inspectorat. De asemenea, platforma va genera și transmite electronic, în mod automat numarul de înregistrare al documentului respectiv.
- Sistemul va permite crearea de fluxuri de notificare utilizând formulare predefinite .
- Sistemul va permite si încărcarea documentelor în format letric.
- crearea posibilitatii declararii lucratorilor detașati pe teritoriul Romaniei, care sa permita completarea on-line a formularelor predefinite, semnarea electronica și transmiterea prin același sistem, catre inspectoratul teritorial de munca destinatar.
- identificarea lucratorilor sa se poata efectua în functie de situatia din teren și prin completarea unui chestionar electronic pe un dispozitiv electronic portabil.
- crearea unui modul electronic de raspuns automat Ia lntrebarile cetatenilor/ lucratorilor/ angajatorilor.
- crearea posibilitatii înregistrarii on-line a agentilor de plasare a fortei de munca.
- crearea posibilității inregistrarii zilierilor pe teritoriul României, care sa permita completarea on-line a formularelor, semnarea electronica și transmiterea prin același sistem, catre inspectoratul teritorial de munca destinatar.
- evidenta contractelor de stagiu inregistrate de catre agentii economici

- crearea oricăror altor module identificate ca necesare de către autoritatea contractantă, în conformitate cu prevederile legale existente la momentul dezvoltării sistemului informatic.

II. *Crearea și operationalizarea unei aplicatii de Evaluare a Riscului, care sa prelucreze date inclusiv din REGES-ONLINE și care sa sprijine activitatea de planificare a activitatilor de control, prin analiza criteriilor de selectie și evidentiere a entitatilor ce îndeplinesc conditiile de natura a le situa în "zona de interventie imediata", pentru organizarea vizitelor de inspectie, constatarea și compararea rezultatelor obtinute cu cele indicate în aplicatie, precum și dispunerea de masuri de remediere, acolo unde este cazul.*

Resurse/masuri necesare: definirea riscurilor, functie de domeniile de manifestare și stabilirea scorurilor aferente;

- elaborarea Hartii Riscurilor, cu evidentierea zonelor de monitorizare/interventie;
- integrarea datelor introduse în platforma creată, în algoritmul utilizat de aplicatia de Evaluare a Riscului, în vederea generarii automatizate a listei entităților ce urmează a fi incluse în acțiuni de control. Datele utilizate pentru construirea algoritmului de funcționare a aplicatiei, va proveni din riscurile care s-au manifestat și sprijină Inspecția Muncii în îndeplinirea funcției de autoritate de stat prin care se asigură exercitarea controlului în domeniile relațiilor de muncă și securității și sanatății în muncă care au stat Ia baza producerii de evenimente în care au fost implicați lucrători. Aceste informații vor trebui să fie extrase și generate automat din procesele verbale de cercetare întocmite sau avizate de ITM/ IM, procesele verbale de control cu documentele conexe, sesizări, precum și din exploatarea celorlalte baze de date gestionate sau la care are acces Inspecția Muncii (de exemplu, REGES, ONRC, etc.).

III. *Dotarea cu logistica necesara*

- Dotarea cu autoturisme și cu echipament IT (laptop, conexiune Ia internet, firewall, routere, switch layer 3, telefoane inteligente) pentru a putea încheia actele de control pe teren.
- Dezvoltarea unei funcționalități pentru aplicatia mobilă care sa interogheze REGES-ONLINE și sa returneze informatii despre elementele contractului individual de munca, norma de lucru, salariu, etc. sa poata genera rapoarte privind numarul de salariati al angajatorului, etc.
- Sistemul informatic va fi proiectat astfel încât să permită interconectarea ulterioară cu oricare alte sisteme informatice nationale (standard API).

3 DESCRIEREA INVESTIŢIEI

3.1 Scenariul de implementare

Scenariul de implemntare ales presupune crearea unui nou sistem care să includă/ să fie bazat pe un sistem modern de management electronic al documentelor și fluxurilor de lucru, cât și a infrastructurii hardware și software existente necesare rulării sistemului în condiții de înaltă disponibilitate precum și a condițiilor tehnice pentru asigurarea interoperabilității cu alte sisteme IT ale administrației publice / operatorilor economici care utilizează sisteme on-line de management a întreprinderii.

În cazul acestui scenariu investiția va cuprinde:

- Infrastructura hardware pentru procesare, stocare, comunicații, securitatestfel încât să fie asigurate performanțele sistemului atât pentru angajații IM/ITM cât și pentru utilizatorii care doresc să folosească modulul de Petiții on-line, respectiv să înregistreze electronic documente prin registratura automată. În acest scenariu, întreaga infrastructură necesară va fi găzduită în centrul de date al Serviciului de Telecomunicații Speciale.
- Infrastructura software de bază necesară pentru rularea sistemului SIAMC 2.0, această categorie incluzând sisteme de tipul: sisteme de virtualizare, sisteme de operare, baze de date, platforma de salvare și recuperare date în caz de dezastre, sistem de securizare a accesului la date și aplicații.
- Infrastructura de aplicații, aplicatie mobila, sistem de management electronic al documentelor și fluxurilor de lucru, sistem de analiză și raportare prin intermediul cărora va fi realizat sistemul SIAMC 2.0 cu modulele de administrare și de business identificate și descrise în cele ce urmează. 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 printr-o arhitectură cloud ready.
- Serviciile de livrare, instalare, configurare a infrastructurii hardware și software, dezvoltarea, implementarea și testarea sistemului SIAMC 2.0 cu date importate din aplicația curentă SIAMC/COLUMBO, prin migrarea și transfomarea (Data Cleaning) datelor din sistemele existente, la nivelul fiecărui ITM respectiv IM, asigurarea instruirii administratorilor și utilizatorilor, asistență tehnică la intrarea în producție a noului sistem, garanție și mentenanță, precum si asigurarea unei perioade de asistența tehnică la pornire pentru corecție/ modificare a anumitor parametri si aplicațiilor in funcție de feedback-ul primit de la administratorii si utilizatorii sistemului in integralitatea acestuia.
- Organizarea arhivei operaționale a sistemului SIAMC 2.0 utilizând infrastructura de aplicații livrată.

3.2 Cerințe privind soluția tehnică

3.2.1 Cerințe generale

SIAMC 2.0 proiectat va respecta atât politicile şi reglementările interne privind tehnologia informației, cât şi legislația în vigoare privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, precum și orice alte acte normative care se referă la implementarea aplicațiilor sau la domeniul tehnologia informației.

Interfața utilizator a sistemului, în asamblu, precum și a fiecărui subsistem component, va trebui să fie intuitivă (facilă), informativă, fiabilă, atractivă și stabilă. Interfața utilizator, pentru sistemele accesate prin interfață web, trebuie să poată fi accesată utilizând versiuni ale browser-elor (minim Google Chrome/Microsoft Edge/Safari/Firefox) compatibile atât cu dispozitive de tip desktop/laptop, cât și cu dispozitive și telefoane mobile. Interfața utilizator va fi realizată conform ultimelor versiuni ale standardelor HTML, CSS, XML.

Interfața sistemului va trebui să fie disponibilă cel puțin în limba română, dar sistemul în ansamblul său va trebui să asigure suport multilingv în cazul în care se va considera necesară traducerea acesteia.

În cazul modulelor funcționale dezvoltate în cadrul contractului TOATE DREPTURILE PATRIMONIALE DE AUTOR asupra tuturor operelor create de către viitorul Prestator, aferente produsului sau serviciului livrat, SE VOR TRANSFERA CĂTRE BENEFICIAR. împreună cu ultima versiune a codului sursă, comentat și documentat, pentru versiunea sistemului dat initial în producție și la finalul perioadei de garanție și suport, codul obiect și documentația tehnică detaliată și completă a sistemului. Livrarea codului sursă se va realiza împreună cu un instrument dedicat de gestiune și versionare, instrument ce va putea fi utilizat de Achizitor fără limitări după finalizarea periodei de suport și garanție, de tip GIT sau echivalent.

Toate codurile sursă vor include și comentarii scrise în limba română şi în acord cu standardele/convențiile de dezvoltare a codului (în forma susținută de limbajul de programare aferent, de exemplu comentarii în interiorul codului). - Toate codurile sursă vor fi predate în clar, fără a se aplica procedee de ascundere (”obfuscate”). Acceptarea predării codului sursă de către Prestator și preluării acestora de către beneficiar se va realiza doar după validarea acestora de către Beneficiar în infrastructura proprie, la recepția sistemului informatic implementat.

Componentele sistemului propus trebuie să fie protejate împotriva încercărilor deliberate sau accidentale de acces neautorizat la datele pe care acesta le stochează sau prelucrează.

Astfel, sistemul în ansamblul său trebuie să asigure:

- Securitatea datelor printr-un sistem de limitare a accesului la funcționlaitățile aplicației, bazat pe drepturi și defalcat pe mai multe niveluri. Drepturile de acces ale utilizatorilor vor putea fi configurate de administratorii sistemului din interfața sistemului;
- Împiedicarea utilizatorilor de a se conecta la sistem dacă acesta este în incapacitate temporară de a asigura securitatea datelor sau există suspiciuni că mecanismele de protecție au fost compromise;
- Închiderea automată a sesiunilor de lucru ale utilizatorilor, în caz de inactivitate pe o anumită durată predeterminată și configurabilă de timp, nu mai mult de 5 minute după ce se înregistrează ca user-ul devine inactiv, pentru a proteja dezvăluirea accidentală a informațiilor către alte persoane care nu sunt autorizate să le primească;
- Jurnalizarea operațiilor zilnice la nivelul sistemului, individual pentru fiecare utilizator cu drept de acces la modificarea înregistrărilor, cu marcarea orei la care a fost executată fiecare operație, precum și a identității utilizatorului care a iniţiat-o;
- Generarea de rapoarte diverse pentru logurile generate la nivelul aplicațiilor, precum și exportul tuturor logurilor, cel puțin în format csv și/sau alte formate standard;
- Eventualele mecanisme de tip API, interne sau externe, vor fi protejate prin metode de autentificare;
- Confidențialitatea transferului de informații pentru a proteja informațiile împotriva amenințărilor în orice situație, fie când informația este stocată pe servere, fie când aceasta este transportată.

3.2.2 Alinierea la strategii și legislație

Sistemul va fi proiectat astfel încât să implementeze prevederile HG nr. 908/2017 pentru aprobarea Cadrului Național de Interoperabilitate precum și Legea nr. 242 din 20 iulie 2022, privind schimbul de date între sisteme informatice și crearea Platformei naționale 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, sau orice altă legislație ulterioară în vigoare la momentul implementării.

Sistemul va fi proiectat astfel încât să aibă în vedere implementarea principiilor Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal şi privind libera circulație a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), atât în ceea ce privește datele angajaților proprii, cât și a cetățenilor. Se va avea în vedere și realizarea informărilor/notificărilor ce trebuie transmise de Beneficiar persoanelor vizate, ale căror date vor fi stocate sau gestionate prin platformă, în conformitate cu GDPR.

Interfețele de interacțiune cu utilizatorii vor fi proiectate astfel încât să implementeze cerințele din Ordonanța de urgență a Guvernului nr. 112/2018 privind accesibilitatea site-urilor web și a aplicațiilor mobile ale organismelor din sectorul public, pentru a permite ca site-urile web și aplicațiile mobile respective să fie accesibile utilizatorilor, în special persoanelor cu dizabilități, minim îndeplinirea nivelului de conformitate AA.

3.2.3 Arhitectura sistemului

Sistemul va fi proiectat având la bază principiile de funcționare într-un cloud public sau privat, respectiv, dar nelimitat la, rularea sub forma de servicii logice decuplate în instanțe de tip container, bazate pe microservicii, API-uri și micro segmentare a comunicațiilor, beneficiind de resursele de procesare și comunicație flexibile, elastice, distribuite și reziliente ale infrastructurilor de cloud public sau privat.

Arhitectura sistemului va respecta urmatoarele cerințe:

- Unificarea logicii de business și a managementului datelor și eliberarea resurselor de procesare de la nivelul stațiilor de lucru de la care se realizează accesul la aplicațiile software;
- Arhitectura bazată pe servicii astfel încât să permită rularea sesiunilor de acces la date izolat, distribuit și balansat în zone de memorie separate;
- Utilizarea automatizărilor și implementarea conceptului de infrastructură ca un cod (Infrastructure as Code) pentru a permite reconstituirea rapidă și scalarea sistemului într-un timp minim;
- Ușurința de administrare, prin centralizarea resurselor de logică de procesare și a datelor;
- Nu trebuie să fie permise pierderi de date la transferul spre baza de date;
- O arhitectura multi-nivel (denumită și în “N straturi” - nivel date, nivel logică de aplicație, nivel prezentare, nivel utilizator);
- Utilizarea unei arhitecturi modulare care să permită o cuplare slabă (loose-coupled) între componente și în care responsabilitățile fiecărei componente sunt specializate. Structura modulară trebuie să permită adaugarea de noi module cu proprietăți diferite fără modificări în modulele software finalizate;
- Să permită exportul/ publicarea și schimbul de date cu alte sisteme prin utilizarea de standarde deschise, min WebServices, API-uri bazate pe XML, JSON, obiecte serializate, în corelare cu soluția tehnică ofertată.

- În cazul în care se ofertează platforme COTS, acestea vor fi licențiate pentru un număr nelimitat de utilizatori, cu drept de utilizare perpetuu, pentru oricâte instanțe si orice putere de procesare fără niciun cost adițional ulterior pentru Beneficiar.
- Componentele platformei sa permita instalarea într-o topologie de infrastructura care sa aiba o zona DMZ in care sa se instaleze acele componente care sunt expuse catre exteriorul infrastructurii și care sa poată fi protejata prin echipamente de securitate de perimetru. Pentru a avea o securitate de nivel înalt, comunicația între componentele aflate in zona de DMZ si restul componentelor (componentele de tip back-office, componenta de administrare, componenta de tip baze de date) trebuie sa se facă printr-un reverse proxy programatic, adică să nu existe acces direct din extern către componentele din intern.

3.2.3.1 Mediile ce vor fi organízate

Sistemul va include minimum un mediu de producție și un mediu de dezvoltare/testare. Mediul de testare/dezvoltare va fi virtualizat și dimensionat pentru un număr acoperitor de utilizatori ai Beneficiarului, stabilit si comunicat de catre acesta, care vor asigura mentenanța și dezvoltarea sistemului. Acesta va conține toate componentele aplicative precum și modulele funcționale dezvoltate în cadrul acestora și orice alte componente sunt necesare testării noilor funcționalități sau actualizări înainte de trecerea acestora în mediul de producție. Mediul de testare/ dezvoltare va permite testarea patch-urilor sau actualizărilor de tehnologie înainte de instalarea acestora pentru a preveni un impact negativ asupra mediului de producție.

3.2.3.2 Performanțele și disponibilitatea sistemului

Toate componentele sistemului vor trebui să asigure un nivel ridicat de disponibilitate. Sistemul va trebui să fie capabil să funcționeze în regim 24x7 și să asigure o disponibilitate în funcționare de minimum 99.9%. Orice întrerupere accidentală va fi tratată în conformitate cu cerințele de Suport (SLA), iar opririle programate pentru mentenanță necesare vor trebui să fie anunțate în prealabil și să se încadreze în afara intervalului orar 8:00 - 18:00. Operațiunile de realizare a copiilor de siguranță vor fi incluse tot în intervalul de timp neprioritar.

În cazul unui incident care întrerupe funcționarea sistemului/componentelor acestuia în mediul de producție, pentru reluarea funcționării acestuia va trebui să se poată restaura imediat ultima copie de siguranță disponibilă în centrul de salvare date, cu semnalarea perioadei la care s-a făcut restaurarea. Centrul de salvare va fi organizat în cadrul unui centru de date secundar al Serviciului de Telecomunicații Speciale și va avea rol de păstrare a copiilor de siguranță.

Atingerea criteriilor de performanță va fi testată în condiții de încărcare maximă a sistemului pentru fiecare componentă a acestuia, atât în ceea ce privește numărul estimat de utilizatori simultani/sesiuni ce trebuie suportați(e), cât și în ceea ce privește funcționarea în condiții de încărcare de minim 80% a sistemului. În toate aceste situații operațiunile de citire a unor înregistrări simple, nu vor dura mai mult de 0.5 secunde (din momentul accesării unei anumite înregistrări și până în momentul în care aplicația returnează informațiile în forma prestabilită). Operațiunile de scriere a unor înregistrări noi în baza de date nu vor dura mai mult de 1 secundă (măsurat din momentul în care un utilizator lansează salvarea informațiilor dintr-un ecran și până în momentul în care aplicația devine din nou disponibilă pentru operare, utilizatorului respectiv, sau din momentul în care un utilizator accesează o funcție de creare a unei înregistrări noi în baza de date și până în momentul în care aplicația returnează forma în care informațiile pot fi introduse iar utilizatorul poate începe introducerea datelor).

În medie sistemul trebuie să permită accesul **simultan** pentru minim 5.000 de utilizatori externi, cetățeni, angajați, angajatori, prestatori de servicii, și minim 500 deutilizatori ai Inspecției Muncii/ Inspectoratelor teritoriale ce utilizează sau interoghează sistemul.

Sistemul trebuie să ofere mecanisme automate de scalare astfel încât să permită acoperirea unor vârfuri ce ating minim dublul utilizatorilor simultani estimați anterior.

3.2.3.3 Arhitectura Disaster Recovery

La momentul elaborării prezentului proiect tehnic, soluția identificată de Achizitor pentru site-ul secundar este reprezentată de viitorul cloud guvernamental, cu precizarea că găzduirea site-ului principal va fi realizată în cadrul Centrului de Date al Serviciul de Telecomunicații Speciale. Astfel, livrarea și instalarea infrastructurii hardware și software se va realiza în centrul de date STS.

De asemenea intră în răspunderea viitorului prestator să asigure orice pregătiri necesare astfel încât soluția ofertată pentru SIAMC 2.0 să funcționeze potrivit arhitecturii solicitate („cloud-native") și, respectiv, să fie posibilă implementarea unei arhitecturi de tip DR la momentul operaționalizării cloud-ului gubernamental, precum și instalarea sistemului SIAMC 2.0 și a infrastructurii de suport pentru acesta, minim stratul de baze de date, în cloud-ul guvernamental, dacă acesta va fi disponibil pe durata contractului sau a perioadei de Suport și garanție, fără costuri suplimentare pentru Achizitor. Licențierea produselor ofertate va lua în considerare această cerință și va permite transferul produselor licențiate, dacă va fi cazul între cele două locații, fără costuri suplimentare pentru Achizitor, astfel încât să poată fi asigurată funcționarea în arhitectura solicitată.

3.2.3.4 Alocarea resurselor

Oferta va include resursele hardware și software necesare pentru asigurarea funcționării sistemului în regim de înaltă disponibilitate, cu respectarea cerințelor de performanță și arhitecturale. Dacă soluția propusă necesită resurse suplimentare celor solicitate în continuare, aceste vor fi livrate de Ofertant fără costuri suplimentare pentru Benficiar. Acolo unde sunt specificate anumite cantități (hardware sau software) acestea vor fi considerate minime și obligatorii, ofertantul putând propune doar cantități suplimentare.

Orientativ, alocarea resurselor (cu o rezervă pentru alte componente ce pot fi identificate și propuse de Prestator, inclusiv în ceea ce privește soluția de virtualizare) proiectată de Beneficiar este:

Componentă	**Număr mașini virtuale**	**Număr Core /mașină**	**Număr Core /componentă**
Producție			
Portal Extern	4	16	64
Portal Intern/ componente aplicative SMED, inclusiv componente de automatizare sau accelerare funcționare	6	64	384
Componenta aplicativă zilieri	2	32	32
Baza de date	2	32	64
Componenta consolidare, raportare și analiză date (back-end si publicare date)	2	16	32

Componentă	Număr mașini	Număr Core	Număr Core
Testare/Dezvoltare			
Portal Extern	1	4	4
Portal Intern/ componente aplicative SMED, inclusiv componente de automatizare sau accelerare funcționare	2	16	32
Componenta aplicativă zilieri	2	8	16
Baza de date	2	8	16
Componenta consolidare, raportare și analiză date (back-end si publicare date)	1	4	4
Administrare mediu de productie			
Backup date, sisteme și aplicații	1	16	16
TOTAL			**664**

Oferta va include alocarea resurselor aferentă soluției tehnice propuse, la nivel de mașini virtuale și resurse alocate fiecărei componente software ofertate.

3.2.3.5 Interoperabilitatea sistemului

Pentru a putea comunica atât cu sistemele informatice ale administrației publice din România, ce vor fi migrate în Cloudul Guvernamental cât și cu cele ce nu vor fi migrate 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/)

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)
- furnizare schema logică a fluxurilor de lucru pentru fiecare serviciu disponibil.

Asigurarea interoperabilității organizaționale va fi realizată prin orientarea către servicii, in conformitate cu cadrul național de interoperabilitate pe care se bazează modelul conceptual pentru serviciile publice, și implică definirea în mod clar a relațiilor dintre furnizorii serviciului și clienții serviciului.

Interoperabilitatea organizațională implică găsirea de instrumente pentru formalizarea asistenței reciproce, a acțiunilor comune și pentru interconectarea proceselor operaționale ca parte a furnizării serviciului, de exemplu prin semnarea unor documente de tip MoU (memorandum) și SLA (contract protocol pentru documentarea nivelului de asigurare a serviciilor realizate) între administrațiile publice participante. În ceea ce privește acțiunile transfrontaliere, se vor prefera acordurile multilaterale sau globale europene dacă este cazul.

Din punct de vedere organizațional în timpul fazei de analiză se va realiza clarificarea și formalizarea relațiilor organizaționale în vederea creării și furnizării serviciilor publice europene cu cel puțin următoarele entități: Oficiul Național al Registrului Comerțului (ONRC), Agenția Național de Administrare Fiscală (ANAF), Direcția Generală pentru Evidența Persoanelor (DGEP), Inspectoratul General pentru Imigrări (IGI), Casa Națională de Pensii Publice (CNPP), Agenția Națională pentru Plăți și Inspecție Socială (ANPIS) și Institutul Național de Statistică (INS), ANOFM, etc.

Asigurarea interoperabilității la nivel tehnic a sistemului presupune implementarea unui nivel de integrare (interfețe API) realizat folosind tehnologii moderne, accesibil de către terțe sisteme pentru automatizarea schimbului de date, fără a mai fi nevoie de prelucrări manuale sau exporturi consumatoare de timp și predispuse la erori umane. Modulele ce vor fi dezvoltate (servicii și surse de informații) vor asigura accesibilitatea datelor sau a funcționalității lor folosind abordări orientate spre servicii. Proiectul contribuie la dezvoltarea unei infrastructuri comune de servicii și surse de informații reutilizabile care să permită utilizarea de către administrația publică.

Un alt beneficiu va fi posibilitatea de verificare electronică facilă a înregistrărilor din bazele de date ale instituțiilor partenere.

În cazul registrelor centralizate, o singură entitate organizațională este responsabilă și răspunzătoare pentru calitatea datelor și pentru măsurile necesare pentru a asigura corectitudinea datelor. Astfel de registre se află sub controlul juridic al entităților respective.

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.

Cerințe specifice ale interoperabilității:

- Punerea la dispoziție a informațiilor altor solicitanți, cu condiția implementării unor mecanisme de acces și de control care să garanteze securitatea și confidențialitatea în conformitate cu legislația aplicabilă.
- Dezvoltarea de interfețe cu registre de bază și surse oficiale de informații, publicarea mijloacelor semantice și tehnice și a documentelor necesare altor solicitanți pentru a se conecta și a reutiliza informațiile disponibile.
- Asigurarea unei corespondențe între registru și punerea la dispoziție a metadatelor corespunzătoare către administrația publică în vederea asigurării interoperabilității sistemelor publice pentru furnizarea serviciilor publice electronice, incluzând descrierea conținutului acestuia, forma de asigurare a serviciilor și responsabilitățile legate de acestea, tipul de date primare incluse, condițiile de accesare și licențele relevante, terminologia, un glosar, precum și informații cu privire la datele primare pe care le utilizează din alte registre de bază.
- Ofertantul va furniza documentatia API-urilor a fluxurilor, diagrame de flux, diagram si descrierea campurilor din baza de date, etc, la predarea fiecarui modul in parte precum si la finalizarea proiectului in ansamblu.

3.2.3.6 Securitatea sistemului

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 într-un 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.

3.2.3.6.1 <u>Securitatea accesului la distanță</u>

Accesul utilizatorilor mobili in reteaua privata a institutiei pentru a accesa aplicatiile interne, ce urmeaza a fi implementate in cadrul proiectului, se va realiza printr-o conexiune tip Remote Access VPN, dupa asigurarea in prealabil a unui nivel minim de securitate la nivelul terminalului.

Solutia de Remote Access VPN va consta intr-un client instalat pe fiecare terminal, care va incorpora capabilitati avansate de securitate precum antivirus, HIDS, controlul aplicatiilor instalate, firewall. Conexiunea VPN va fi inchisa la nivelul unui cluster ce concentratoare VPN care vor avea acces atat la Internet cat si in DMZ-ul aplicatiilor interne, autentificarea din clientul VPN se va efectua utilizand credentialele din infrastructura AD a insititutiei si un factor suplimentar de autentificare.

Managementul clientilor tip Remote Access VPN se va realiza dintr-o Consola centrala, parte integrata a solutiei si va permite stabilirea politicilor de securitate pe care un terminal trebuie sa le intruneasca pentru a putea dispune realizarea conexiuniii VPN. De asemenea consola de management va colecta toate datele de telemetrie ale terminalelor instalate si va putea forta realizarea unor scanari antivirus, instalarea unor actualizari de securitate, stabilirea unor politici tip ZTNA si la nevoie revocarea accesului pentru un anumit terminal.

Configuratia VPN-ului pe terminalul mobil se va realiza automat in momentul in care clientul VPN se va conecta la interfata expusa in Internet a Consolei de Management si in mod transparent pentru utilizatorul terminalului mobil, care la conectare va trebui sa introduca doar datele de autentificare. Pentru un nivel suplimentar de securitate, clientul instalat pe terminalul mobil va incerca sa se conecteze automat la reteaua institutiei ori de cate ori va exista o solutie disponibila de tip conexiune la Internet (Ethernet, Wi-Fi, 3G/4G). Aceasta masura va permite securizarea modului de acces la resursele interne ale institutiei si evitarea accesarii unor domenii malitioase din Internet.

Accesul utilizatorilor din cadrul sediilor institutiei la resursele interne se va realiza prin reteaua VPN site-to-site aflata in administrarea STS, reteaua privata a institutiei are la baza o arhitecura tip hub-and-spoke cu tunelare IPSec rutata prin reteaua L3VPN STS dispunand astfel de un nivel ridicat de rezilienta si securitate, echipamentele tip spoke de la nivelul sediilor institutiei vor permite filtrarea, configurarea in mod redundant si criptarea IPSec a traficului la valori de minim 1Gbps, la nivelul echipamentelor de agregare se va asigura o configuratie tip cluster, rutarea in mod redundant si capacitati de criptare IPSec la valori de minim 10Gbps. Traficul de date provenit de la sediile insitutiei va fi filtrat intr-un mod cat mai granular si rutat catre domeniile de interes ale utilizatorilor.

3.2.3.6.2 Securitatea sistemului

In cadrul sistemului se vor respecta următoarele principii:

- abordarea securității prin concepție pentru a asigura securitatea modulelor și a infrastructurii lor complete;
- proiectarea astfel încât serviciile să nu fie 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[1] pentru a asigura integritatea, autenticitatea, confidențialitatea și nerepudierea datelor.

3.2.3.6.3 Autentificare

Sistemul va trebui să fie integrat cu sistemul REGES-ONLINE pentru gestiunea comună a datelor și accesului utilizatorilor, indiferent de tipul acestora, pentru a asigura o interfață unică de acces la toate funcționalitățile și serviciile electronice oferite de IM.

Specificațiile tehnice pentru sistemul de autentificare ce va fi implementat în cadrul REGES-ONLINE sunt disponibile în cadrul documentației de atribuire aferente anunțului de participare CN1061510/ 05.11.2023 ce poate fi consultat în platforma SICAP.

3.2.3.6.4 Confidențialitatea datelor

Sistemul proiectat va respecta urmatoarele principii:

- abordarea **confidențialității prin concepție** pentru a asigura securitatea modulelor și a infrastructurii lor complete;
- utilizarea unor servicii calificate de asigurare a încrederii în conformitate cu regulamentul eIDAS pentru a asigura integritatea, autenticitatea, confidențialitatea și nerepudierea datelor;

[1]Regulamentul (UE) nr. 910/2014.

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

De asemenea, trebuie să asigure respectarea de către operatori a legislației privind protecția datelor, prin:

- **„Planuri de gestionare a riscurilor”** pentru identificarea riscurilor, evaluarea potențialului impact al acestora și planificarea intervențiilor cu măsuri tehnice și organizatorice adecvate. Pe baza ultimelor evoluții tehnologice, aceste măsuri trebuie să asigure un nivel de securitate proporțional cu gradul de risc;
- **„Planuri de continuitate a activității”** și **„planuri de rezervă și de redresare”** pentru a institui procedurile necesare de asigurare a disponibilității funcțiilor în urma unui eveniment dezastruos și readucerea tuturor funcțiilor la situația normală cât mai curând posibil;
- Un **„plan de acces la date și autorizare”** care stabilește persoanele care au acces la date, datele care sunt accesibile și condițiile accesării datelor, pentru a asigura confidențialitatea. Accesul neautorizat și încălcarea normelor de securitate trebuie monitorizat, și măsurile corespunzătoare pentru a preveni orice repetare a încălcărilor trebuie documentate si planificate.

3.2.4 Componentele de infrastructură hardware și securitate

3.2.4.1 Cerințe generale

Toate echipamentele ofertate vor fi compatibile, ofertantul fiind responsabil cu punerea in funcțiune a echipamentelor, efectuarea testelor de acceptanță pentru acestea în centrul de date STS. Ofertantul va include în ofertă toate elementele de conectare a echipamentelor la rețeaua de energie electrică, elementele de conectare între echipamente de tip cablare de rețea și fibră optică, plăcile, adaptoarele, elementele de montaj sau licențele necesare astfel încât sistemul sa funcționeze ca un tot unitar, integrat și interconectat, pe o perioadă de timp nelimitată, fără a avea nevoie de achiziții suplimentare pentru funcționarea în parametrii solicitați. Nu se acceptă licențe și echipamente care vor expira după o anumita perioadă, degradând astfel performanțele sau capacitatea funcțională a sistemului ofertat și acceptat.

Pentru claritate, toate funcționalitățile solicitate pentru toate echipamentele, aplicațiile, software-ul standard și software-ul de infrastructură, etc. vor fi activate și vor funcționa la capacitatea solicitată conform cerințelor, fără a fi necesare elemente suplimentare pentru a funcționa conform prezentelor cerințe.

Din punct de vedere al disponibilității şi scalabilității, sistemul va fi proiectat astfel încât să respecte minim următoarele cerințe:

- Să ofere suport pentru înaltă disponibilitate, atât din punct de vedere hardware cât și software, astfel:
    - Serverele de aplicaţii și baze de date vor fi organizate astfel încât să fie asigurate cerințele de înaltă disponibilitate în mediul de producție dar și a sistemului în ansamblul său;
    - Toate componentele de comunicații vor asigura redundanță;
    - Sursele de alimentare ale serverelor (fizice) vor oferi suport pentru redundanţă;
    - Ventilatoarele serverelor (fizice) vor oferi suport pentru redundanţă;

- Serverele vor fi configurate pentru a oferi suport pentru utilizarea matricilor RAID.

- Să ofere suport pentru scalarea sa, atât din punct de vedere hardware cât și software, astfel:
  - Să permită adăugarea de noi echipamente (fizice) de tip server de aplicaţii, baze de date sau echipamente de stocare;
  - Să permită adăugarea de memorie sau capacitate de stocare (suplimentară) serverelor (fizice).

Sistemul va fi proiectat pentru a oferi suport pentru virtualizare, astfel încât să asigure:

- Separarea nivelului logic al aplicațiilor de infrastructură hardware (de suport a rulării sistemului);
- Posibilitatea creării de instanțe virtuale multiple la nivel de aplicații;
- Integrarea la nivelul infrastructurii software de virtualizare, cu funcționalități specifice de suport al instalării, administrării și monitorizării resurselor de tip container
- Alocarea dinamică a resurselor fizice către instanțele virtuale care au cea mai mare nevoie de procesare;
- Eliminarea eventualelor conflicte la nivel de procesor, memorie sau sistem de operare ce ar putea apărea rulând mai multe aplicaţii în cadrul aceleiași instanţe (non-virtuale) de aplicaţie;
- Proiectarea infrastructurii hardware va fi realizată respectând următoarele cerinţe (generale) de securitate:
  - Comunicația între resursele sistemului va fi limitată doar pe porturile necesare bunei funcţionări a acestuia;
  - Toate serviciile ce nu sunt necesare bunei funcționări a sistemului vor fi oprite implicit şi vor fi configurate să nu pornească în cazul unei reporniri.

Prestatorul desemnat câștigător va fi responsabil cu punerea in funcțiune a echipamentelor, efectuarea testelor de acceptanta pentru acestea.

Echipamentele ofertate şi livrate trebuie să nu fie End of Life sau End of Sales la momentul depunerii ofertei. Oferta va include dovada îndeplinirii cerinței.

Notă 1:

Toate elementele de infrastructură hardware și software ce vor fi incluse în realizarea sistemului vor trebui să respecte principiul DNSH (Do No Significant Harm) așa cum este acesta enunțat în Regulamentul delegat (UE) 2021/2139 al Comisiei din 4 iunie 2021 de completare a Regulamentului (UE) 2020/852 al Parlamentului European și al Consiliului prin stabilirea criteriilor tehnice de examinare pentru a determina condițiile în care o activitate economică se califică drept activitate care contribuie în mod substanțial la atenuarea schimbărilor climatice sau la adaptarea la schimbările climatice și pentru a stabili dacă activitatea economică respectivă aduce prejudicii semnificative vreunuia dintre celelalte obiective de mediu.

Oferta va include o declarație din partea Ofertantului cu privire la respectarea principiului DNSH pentru toate elementele componente a Ofertei, precum și modalitatea concretă în care acestea vor fi asigurate pentru fiecare element de infrastructura de bază și aplicații ofertat, sub sancțiunea declarării ofertei ca neconforme în cazul absenței declarației și descrierii modalității de îndeplinire a cerinței.

Notă 2 :

Luând în considerare faptul că prin intermediul acestei proceduri se vor achiziționa echipamente de comunicații ce vor fi integrate în cadrul unei rețele/infrastructuri private de interes național, echipamentele și soluțiile ofertate vor respecta prevederile art. 3 din Legea nr. 163/2021. Astfel, în oferta tehnică va fi inclus în mod obligatoriu un formular asumat prin semnătură de ofertant, prin care se va prezenta dovada autorizării conform Legii nr. 163/2021 a producătorilor echipamentelor/

soluțiilor ofertate, excepție făcând accesoriile de instalare și de interconectare (module optice, patch-cord-uri, siguranțe electrice, montanți rack, cabluri de alimentare, surse de alimentare, etc.)

3.2.4.2 Cantități

Prestatorul va asigurarea livrarea a minin următoarelor echipamente hardware identificate de Achizitor ca fiind necesare pentru asigurarea îndeplinirii cerințelor de performanță ale SIMAC.

Este responsabilitatea Ofertantului să dimensioneze corect și complet cantitativ și calitativ infrastructura ofertată (servere, storage, comunicații, ups) astfel încât aceasta să corespundă și să asigure îndeplinirea cerințelor generale de infrastructură și nivelul de performanță solicitat pentru soluția ofertată. În cazul în care pe durata implementării se constată că infrastructura ofertată nu asigură nivelul de performanțe solicitat, Prestatorul va fi obligat să completeze/îmbunătățească infrastructura astfel încât aceasta să corespundă nevoilor soluției implementate. Achizitorul nu va fi obligat să facă nici o cheltuială suplimentară în acest sens. Oferta va include în clar asumarea cerinței de către Ofertant.

Produsele ofertate trebuie să fie eficiente din punct de vedere al consumului de energie. Oferta va include detalierea consumului pentru fiecare echipament propus precum și calculul total pentru a fi asigurată îndeplinirea cerinței.

Pentru nici un echipament nu sunt acceptate adaptoare sau soluții improvizate pentru porturile și interfețele acestuia.

Oferta va include toate codurile și fișele de produs pentru toate echipamentele ofertate pentru a se putea face verificarea tehnică a ofertei.

Nr. crt.	Tip de echipament	Cantitate minimă
1.	Echipament de procesare	12
2.	Echipament de stocare date	1
3.	Switch Datacenter	2
4.	Switch Management	1
5.	Router tip 1 – firewall central	4
6.	Router tip 2 – locații județene	88
7.	Router tip 3 – puncte de lucru	32
8.	Soluție acces VPN securizat, licențiere / utilizator	2000

3.2.4.3 Echipamente de procesare – 12 buc

Descriere generală
• Echipament de tip server dual-socket • Răcire Front to Back
Procesor
Serverul va fi echipat cu minim 2 procesoare de tip Intel Xeon sau echivalent de ultimă generație, având următoarele caracteristici: • Frecventa: 2.2 GHz sau superior; • Bus Speed min 16 GT/s • Cache: 60 MB sau superior;

- Număr de core-uri per procesor: minim 32 core-uri cu 64 fire de execuție;
- Număr procesoare instalate: minim 2;
- Număr procesoare suportate: minim 2.

Memorie

- Minim 1024 GB Registered ECC DDR5 memorie instalată, SDDC, suport pentru memory mirroring și hot spare.
- Minim 32 sloturi total (minim 16 libere) pentru memorie RAM cu suport pentru minimum 2 TB RAM.
- Metode suportate de protecție a memoriei: Advanced ECC, Memory sparing

Hard disk drive:

- Minim 2 disk-uri SSD 480GB de tip M.2 care să poată fi configurate într-o matrice de tip RAID 1
- Sistemul trebuie sa suporte extinderea cu minim 10 drive-uri de 2.5”
- Sistemul trebuie livrat cu toate modulele și accesoriile necesare pentru instalarea discurilor în mod hot-swap.

Interfața grafică

- Minim 16MB memorie video

Securitate

- TPM 2.0;
- Suport inclus pentru verificarea semnăturilor criptografice ale driverelor UEFI (încărcate de pe carduri PCIe, dispozitive de stocare), OS boot loader și altor programe executabile ce sunt încărcate înainte ca sistemul de operare să ruleze;
- Suport inclus pentru verificarea și validarea autenticității firmware-ului componentelor critice ale echipamentului (interfețe de rețea, HBA-uri, controller RAID, dispozitive de stocare, dispozitive logice complexe programabile, surse de alimentare);
- Update-urile de firmware trebuie să fie semnate criptografic de către producătorul echipamentului ofertat pentru a fi autentificate la instalare;
- Include suport pentru un mecanism de audit a tuturor operațiunilor de autentificare în sistem sau de modificare a parametrilor de autentificare (conturi utilizator sau certificate). Logurile acestor informații de audit vor fi securizate și vor putea fi accesate doar din componenta de management a soluției propuse;
- Suport inclus pentru resetarea sistemului la starea inițială (setările din fabrică), cu toate datele și configurațiile eliminate din mediile de stocare interne ale echipamentului;
- Firmware rollback;
- UEFI Server Firmware;
- Posibilitatea de a dezactiva “Secure Boot“.

Interfețe de rețea

- Minim 8 x Ethernet 10/25Gbps SFP28 echipate în configurația ofertată (8buc Cablu DAC 25Gbps 3m).
- Interfața de rețea separată pentru administrare la distanță, diferită de cele 8 interfețe de rețea(1 buc patch CAT 6 3m inclusă).
- Soluția ofertata trebuie sa beneficieze de Root of Trust – astfel încât sa permită verificarea actualizărilor de firmware printr-un set de chei criptografice scrise de către producător la nivel de controller hardware, permițând astfel un nivel de securitate suplimentar fata de o verificare standard la nivel de firmware software

Sloturi de expansiune

- Minim 3 sloturi extensie PCIe, din care minim 2 sloturi de tip PCIe Gen5 x16 electric (cu 16 LAN-uri PCI Express conectate).

Conectori interfețe I/O

- Minim: 1 x serial, 1 x VGA, minim 3 x USB din care minim 1 x USB 3.0

Carcasă

- Montabil în rack cu șine glisante. Serverul va fi echipat cu mecanism de închidere pentru a putea securiza accesul la HDD-urile instalate.

Sursa de alimentare

- Minim 2 surse hot plug și redundante instalate cu o putere minimă de 1000W
- Sursele, clasa Platinum sau echivalent, vor fi dimensionate pentru a permite echiparea maximală a serverului (număr maxim de HDD-uri și de module de memorie) fără necesitatea schimbării surselor.

Ventilatoare

- Ventilatoare redundante (N+1), redundante, hot plug

Administrare

Echipamentul trebuie să fie livrat cu capabilități hardware incluse pentru:

- administrarea și monitorizarea serverelor dintr-o interfață centralizată, fără necesitatea de a instala agenți;
- a asigura compatibilitatea, modulul hardware de administrare trebuie să fie furnizat de același producător cu cel al serverelor;
- inventarierea și configurarea subcomponentelor serverelor, incluzând: BIOS, plăci de rețea, plăci HBA, controllere RAID, unități de stocare;
- update-uri de firmware, BIOS și drivere. Update-urile trebuie să fie securizate prin semnătură criptografică, pentru asigurarea autenticității acestora;
- generarea de fișiere de configurare și posibilitatea aplicării lor pe alte servere din infrastructură;
- funcționalitatea de validare a configurației față de o referință;
- monitorizarea stării de funcționare a serverelor și subcomponentelor: alerte, indicatori de performanță și consum de energie electrică;
- instalare și configurare locală și la distanță, inclusiv configurare RAID;
- management operațional cu următoarele funcții: monitorizarea stării sistemului, managementul evenimentelor și alarmelor, inventarul componentelor, inventarul și instalarea update-urilor și patch-urilor, analiza performanței, diagnoza în timp real, repornirea și reconfigurarea automată a serverului;
- LCD display sau panou cu leduri; panoul LCD/LED livrat va permite citirea mesajelor de eroare fără operațiuni suplimentare;
- monitorizare a ventilatoarelor, surselor de alimentare și temperaturii, panou LCD sau cu LED-uri pentru diagnosticarea rapidă a stării de funcționare a componentelor critice: memorii, procesoare, surse de alimentare, ventilatoare, disk-uri, interfețe PCI, placă de bază;
- analize predictive de eroare (fără aplicație externă) pentru: HDD-uri, memorii, procesoare, surse alimentare, ventilatoare cu posibilitatea anunțării administratorului de sistem despre iminenta defectare a uneia dintre componentele enumerate anterior (Predictive Failure Analysis);
- suport instalat și activat cu licențiere perpetuă pentru managementul serverului de la distanță (redirectare interfață grafică, tastatură și mouse, posibilitate de pornire/oprire de la distanță, suport SSL, SNMP, suport pentru remote virtual media).

Sistemul de management trebuie să fie echipat cu următoarele facilități:

- management de la distanță;
- redirectare interfață grafică cu tastatură și mouse;
- posibilitate de pornire/oprire de la distanță;

- suport pentru remote media (virtual CD si floppy);
- suport pentru SSL (Secure Socket Layer);
- monitorizarea consumului de energie și temperatură cu prezentarea de grafice ce pot afișa și date istorice;
- managementul evenimentelor și alarmelor;
- inventarul și monitorizarea componentelor serverului (inclusiv GPU, module optice SFP);
- instalarea update-urilor și patch-urilor pentru componentele serverului;
- analiza performanței și diagnoza în timp real, independent de sistemul de operare instalat;
- repornirea și reconfigurarea automată a serverului;
- integrarea cu Active Directory / LDAP;
- redirectare consolă serială;
- autentificare two-factor;
- integrare cu Microsoft System Center și cu VMware vCenter;
- RESTFul API cu suport Redfish
- Interfețe acces utilizator: HTML5 Web GUI, SSH, telnet, redirecționare pe port serial;
- port dedicat Gigabit Ethernet ce permite accesarea sistemului de management indiferent de stadiul de funcționare a serverului.

Echipamentul trebuie livrat împreună cu aplicație pentru instalarea și configurarea serverului dezvoltată de producătorul serverului capabilă de instalare în mod neasistat.

Aplicație Administrare

- Trebuie să permită administrarea și monitorizarea serverelor dintr-o interfață centralizată, fără necesitatea de a instala agenți;
- Pentru a asigura compatibilitatea, aplicația trebuie să fie furnizată de același producător cu cel al serverelor;
- Trebuie să permită inventarierea și configurarea subcomponentelor serverelor, incluzând: BIOS, plăci de rețea, plăci HBA, controllere RAID, unități de stocare;
- Trebuie să permită update-uri de firmware, BIOS și drivere. Update-urile trebuie să fie securizate prin semnătura criptografică, pentru asigurarea autenticității acestora;
- Trebuie să permită generarea de fișiere de configurare și posibilitatea aplicării lor pe alte servere din infrastructură;
- Trebuie să permită instalarea sistemelor de operare și virtualizare pe serverele aflate în administrare;
- Permite stocarea pe un NAS extern cu funcționalitate de retenție a fișierelor, pentru a asigura protecția la ștergere și modificare a fișierelor de update, template-urilor de configurare și imaginilor de sistem de operare;
- Trebuie să ofere funcționalitatea de validare a configurației față de o referință;
- Monitorizează starea de funcționare a serverelor și subcomponentelor: alerte, indicatori de performanță și consum de energie electrică;
- Permite ștergerea securizată a unităților de stocare de tip SSD si HDD.
- Trebuie să genereze grafice cu nivele de încărcare și utilizare ale serverelor cu un istoric pe o perioada configurabilă de cel puțin 1 an

Compatibilitate cu sisteme de operare

- VMware vSphere 8
- Red Hat Enterprise Linux 9
- Windows Server 2022
- Compatibilitatea cu sistemele de operare va fi probată prin menționarea sistemelor de calcul ofertate pe pagina web a producătorilor sistemelor de operare (HCL).

Conformitate cu standarde europene

Conformitate CE cu următoarele standarde europene în vigoare:

• Siguranța în exploatare: 014/35/EU; • Echipamente de joasă tensiune: 014/35/EU; • Compatibilitate electromagnetica: 2014/30/EU; • Declarație RoHS: 2011/65/EU.
Alimentare cu energie electrică
• Surse de alimentare interne redundante (1+1) AC, 220V, 50 Hz • Cabluri IEC C13 la C14, minim 1,5m
Format
• Rackmountable 19”, maxim 1U (1 rack unit).
Garanție și suport
• Soluția ofertată trebuie să beneficieze de servicii de garanție și suport pentru minim 5 ani de la data recepției, având SLA 24x7 timp de răspuns 4 ore și servicii de mentenanță și suport proactive folosind un canal de comunicare între centrul de date al autorității contractante și centrul de suport al producătorului, care să garanteze diagnosticarea echipamentului sau modulului defect și înlocuirea acestuia în maxim 1 zi lucrătoare, fără alte costuri. • Garanția hardware va fi de minim 60 de luni. • Suportul software va fi de minim 60 de luni, acoperind dreptul de a face update-uri software ori de câte ori este necesar. Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor apărute în funcționare și solicitarea rezolvării acestora în funcție de severitate. Accesul la suportul tehnic al producătorului se va realiza direct, fără să fie nevoie de suportul unui terț. De asemenea, se va asigura dreptul de a face update-uri și upgrade-uri la toate componentele software ofertate (firmware, drivere componente, pachete software de la producător incluse în echipamentul software ofertat). • Pe toată perioada de suport activ al echipamentului ofertat, în cazul in care discurile SSD/flash au fost uzate prin scrieri/rescrieri și au ajuns la limita de utilizare, acestea vor fi înlocuite fără costuri adiționale. • Toate funcționalitățile software solicitate vor include licențiere perpetuă pentru întreaga configurație a echipamentului ofertat, indiferent de upgrade-urile ulterioare ale acestuia. • Echipamentele ofertate trebuie să fie noi și să beneficieze de suport din partea producătorului (nu se acceptă echipamente uzate sau care nu se mai află în linia de fabricație a producătorului). • Mediile de stocare defecte se înlocuiesc fără predarea celor defecte.

3.2.4.4 Echipament de stocare date – 1 buc

Descriere generală	Echipament de stocare dual-controller din clasa Mid-range / Enterprise cu disponibilitate 99.999%.
Controller	Echipamentul trebuie sa aibă două controlere hardware (fizice) prin care se pot scrie și citi datele în mod block (SAN), redundante, hot-swap.
Protocoale suportate pentru accesul la date	Echipamentul ofertat trebuie sa aibă suport inclus pentru protocoale de acces de tip: • block: 16 Gbps Fibre Channel, 1 & 10/25 Gbps iSCSI ;
Porturi instalate (conectivitate)	• 8 porturi 10/25 Gbps SFP (4 porturi per controller) pentru acess de block (iSCSI) complet echipate pentru conectivitate (8buc cablu DAC 3m); • Echipamentul va include porturi de management minim 1Gbps Ethernet pe fiecare controller în parte
Memorie Cache	• Minim 192 GB (96 GB per controller) memorie cache de tip RAM..

Mecanisme de asigurarea a integrității datelor	Echipamentul ofertat trebuie sa ofere mecanisme de protecție a integrității datelor care să asigure integritatea datelor în cazul defectarii simultane a două discuri de același tip care fac parte dintr-un volum de date.
Număr host-uri suportate	• Minim 100 host-uri SAN
Număr maxim LUN-uri	• Cel puțin 100
Dimensiune maximă LUN	• Cel puțin 64 TB
Hard disk-uri instalate	Echipamentul va avea instalate minim: • 24 discuri SSD 7.68TB. În cazul în care echipamentul este prevăzut cu mai mult de 24 de sloturi pentru discuri, toate aceste sloturi vor fi populate cu discuri identice. • Sistemul trebuie să permită definirea de discuri de rezervă care să înlocuiască automat discurile defecte (hot spares)
Suport extensie capacitate de stocare	• Suport pentru minim 144 de discuri interne în sistemul de stocare ofertat, hot-swap; • Suport pentru module de expansiune cu discuri 2,5”; • Modulele de expansiune trebuie să se conecteze la echipamentul de stocare prin magistrale de date redundante, cu lățime de banda de cel puțin 48 Gbps (SAS 12 Gbps 4 canale).
Tipuri de discuri suportate	• SSD: cel putin 1.92TB, 3.84TB, 7.68, 15.36 TB;
Performanță	Echipamentul trebuie sa fie capabil sa susțină o performanță de cel puțin 90.000 IOPS, cu o latenta maxima de 1ms, pentru un mod de acces de tip aleatoriu cu blocuri de 8K într-un model 50/50 Citiri/Scrieri, in condițiile in care operațiunile de compresie si deduplicare sunt active pe întreg sistemul. Parametrii vor fi demonstrați printr-un raport certificat de producător pentru configurația compusă din echipamentul ofertat.
Facilitați de management	Sistem de management si monitorizare integrat în echipament, accesibil de la distanță prin interfața grafică web-based, CLI; să ofere acces securizat SSL/TSL și integrare LDAP; Sistemul de management al echipamentului de stocare trebuie sa asigure integrarea nativa cu platformele de virtualizare (cel puțin VMware) și să asigure cel puțin următoarele funcționalități: • Aplicația de management a echipamentului de stocare trebuie sa permită vizualizarea mașinilor virtuale ce rezidă pe volume alocate către hipervizor; • Integrarea cu aplicația de management a mediului virtual astfel încât să fie posibilă provizionarea de capacitate de stocare direct din aplicația de management a mediului virtual; • Accelerarea hardware a operațiunilor ce au loc intre hipervizor și sistemul de stocare, prin degrevarea unor procese de la nivelul hipervizorului și preluarea lor la nivelul echipamentului de stocare. Această funcționalitate trebuie să permită accelerarea mutării unei mașini virtuale între două volume de date ale hipervizorului și accelerarea efectuării unei copii identice a unei mașini virtuale; • suport inclus pentru VAAI, VASA, VVOLs;

	Sistemul de management trebuie să asigure suport inclus pentru analiza și monitorizare de performantă în timp real, precum și monitorizarea și prioritizarea accesului la date al diferitelor servere; Pentru asigurarea unui nivel optim de disponibilitate operațională, soluția oferită va permite update și upgrade software și hardware al platformei fără întreruperea serviciilor.
Optimizarea capacitații de stocare	Suport inclus pentru alocarea către servere a unei capacitați de stocare mai mare decât cea fizic disponibila (thin provisioning); Pentru îmbunătățirea performanțelor sau a timpilor de răspuns la nivelul aplicațiilor, echipamentul ofertat trebuie sa includă suport (licențiat, dacă este cazul) pentru: • definirea de volume de date organizate în matrici cu nivele de protecție RAID diferite • redistribuirea automată datelor între matricele de discuri atunci când sunt adăugate discuri suplimentare, pentru creșterea capacitații utile.
Protecția si replicarea datelor	• Echipamentul trebuie sa aibă incorporate baterii ce asigură protecția controller-elor și a memoriei cache la cadrările de curent prin salvarea automată a datelor din memoria cache pe discuri flash/SSD, înainte de oprirea echipamentului; • Suport inclus pentru criptarea datelor pe echipamentul de stocare, la nivel de controller, cu management intern respectiv extern al cheilor. • Suport inclus pentru a realiza copii complete ale datelor sau bazate pe imaginea acestora la un anumit moment de timp (snapshot). Snapshot-urile trebuie sa poată fi accesate atât în mod citire, cat si in mod scriere • Suport software inclus pentru replicarea nativă a datelor, sincronă respectiv asincronă, la distanță, între echipamente similare, pentru volume cu acces prin protocol de tip block (FC, iSCSI). • Suport software inclus pentru realizarea de copii de siguranță a datelor, local și la distanță, folosind o tehnologie de jurnalizare a tuturor operațiunilor de scriere care să permită restaurarea datelor la orice moment de timp. Copiile de siguranța trebuie să poată fi grupate pe aplicație, pentru a asigura consistenta recuperării aplicațiilor interdependente. • Pentru utilizarea eficientă a benzii de transmisie dintre centrele de date, soluția de replicare la distanță între diverse echipamente de stocare trebuie să ofere suport pentru replicarea doar a datelor modificate, precum și transmiterea numai a blocurilor de date unice (deduplicare) si comprimate (compresie).
Licențe software	• Toate funcționalitățile software solicitate vor fi activate, licențiate pe echipamentul ofertat, indiferent de capacitatea de stocare prezenta sau viitoare, indiferent de numărul de host-uri ce se vor conecta la echipamentul de stocare.
Sisteme de operare suportate	• Windows Server 2019, Microsoft Hyper-V, VMware ESX, RedHat Enterprise Linux, Novell Suse Enterprise Linux, Citrix Xen Server; • Echipamentul de stocare trebuie să includă licențele necesare accesului sistemelor de operare suportate.
Răcire componente	• Din fața echipamentului către spate (*front to back*).
Format	• Montare în rack standard de 19 inch, maxim 2U

	• Se va furniza kitul de instalare în rack
Garanție și suport	• Se vor asigura servicii de garanție și suport pentru minim 5 ani de la data recepției, având SLA 24x7 timp de răspuns 4 ore și servicii de mentenanță și suport proactive folosind un canal de comunicare între centrul de date al autorității contractante și centrul de suport al producătorului, care să garanteze diagnosticarea echipamentului sau modulului defect și înlocuirea acestuia în maxim 1 zi lucrătoare, fără alte costuri. • Garanția hardware va fi de minim 60 de luni. • Suportul software va fi de minim 60 de luni, acoperind dreptul de a face update-uri software ori de câte ori este necesar. Se va asigura acces 24x7 în centrul de suport al producătorului, cu posibilitatea raportării problemelor apărute în funcționare și solicitarea rezolvării acestora în funcție de severitate. Accesul la suportul tehnic al producătorului se va realiza direct, fără să fie nevoie de suportul unui terț. De asemenea, se va asigura dreptul de a face update-uri și upgrade-uri la toate componentele software ofertate (firmware, drivere componente, pachete software de la producător incluse în echipamentul software ofertat). • Pe toată perioada de suport activ al echipamentului ofertat, în cazul in care discurile SSD/flash au fost uzate prin scrieri/rescrieri și au ajuns la limita de utilizare, acestea vor fi înlocuite fără costuri adiționale. • Toate funcționalitățile software solicitate vor include licențiere perpetuă pentru întreaga configurație a echipamentului ofertat, indiferent de upgrade-urile ulterioare ale acestuia. • Echipamentele ofertate trebuie să fie noi și să beneficieze de suport din partea producătorului (nu se acceptă echipamente uzate sau care nu se mai află în linia de fabricație a producătorului). • Mediile de stocare defecte se înlocuiesc fără predarea celor defecte.

3.2.4.5 Switch datacenter – 2 buc

1.	**Descriere generala**
	• 48 interfețe SFP+ (interfetele SFP+ suportă atât module optice 25 Gigabit Ethernet, 10 Gigabit Ethernet, cât şi module optice 1 Gigabit Ethernet) • 6 interfețe QSFP28 (interfețele QSFP28 suportă atât module optice 40 Gigabit Ethernet cât și module optice 100 Gigabit Ethernet) • 2 surse de alimentare în curent alternativ, redundante • Rackabil 19” 1U • 1 port 10/100/1000 RJ45 pentru management şi consolă • 1 port USB tip A pentru stocare şi boot • Minimum 4 ventilatoare înlocuibile instalate astfel încât răcirea echipamentului să se realizeze din spate spre faţă (Back to Front Airflow), iar un ventilator defect nu va afecta performanțele echipamentului • Defectarea oricărei interfețe fizice de trafic (inclusiv modul optic) nu trebuie sa impacteze disponibilitatea celorlalte interfețe fizice de trafic rămase.
2.	**Performante minimale**
	• 3.6 Tbps switching capacity • 1.2 Bpps switching capacity • Latență maximă 1.5 micro-secundă

	• Minim 4095 VLAN-uri • Minim la 16000 instanțe VRF • Minim 64 căi ECMP • Minim 512 port channel • Minim 32 link-uri într-un port channel • Minim 4 sesiuni SPAN active • Minim 3967 instanțe RPVST • Minim 490 grupuri HSRP • Minim 64 instanțe MST • Minim 1792000 rute LPM • Minim 1792000 intrări IP • Minim 512000 adrese MAC • Maxim 128000 rute multicast • Grupuri IGMP snooping minim 32000 • Numar slice-uri : 1 slice • De la 5000 reguli de filtrare ACL pe intrare și 2000 reguli pe ieșire • IPv4 minim 256K route • IPv6 minim 128K route
3.	**Memorie si procesor**
	• Procesor minimum 6 Cores • Memorie sistem minimum 32 GB • Disc SSD minimum 128 GB • Buffer 40 MB
4.	**Caracteristici minimale incluse**
	• Imagine pentru servicii Layer 3, OSPF, EVPN, BGP și VXLAN • Minim 4 cozi QoS per port • Class of Service (CoS) • Differentiated Services Code Point (DSCP) • Port security • Acces Control Lists pe port şi VLAN • Private VLANs • Traffic Storm Control • Control-plane policing
5.	**Standarde**
	• IEEE 802.1D Bridging and Spanning Tree • IEEE 802.1p QoS/CoS • IEEE 802.1Q VLAN Tagging • IEEE 802.1w Rapid Spanning Tree • IEEE 802.1s Multiple Spanning Tree Protocol • IEEE 802.1AB Link Layer Discovery Protocol • IEEE 802.3ad Link Aggregation with LACP • IEEE 802.3x Flow Control • IEEE 802.3ab 1000BASE-T • IEEE 802.3z Gigabit Ethernet • IEEE 802.3ae 10 Gigabit Ethernet • IEEE 802.3ba 40 Gigabit Ethernet • RMON
6.	**Management**

	Administrare: • ssh CLI , telnet, consolă • Utilizatori/Administratori cu drepturi configurabile • Syslog, SNMP, monitorizare fluxuri de trafic (NetFlow/JFlow sau echivalent), log-uri interne, grafice • Se vor documenta si livra MIB. **Autentificare:** • Bază de date locală • Integrare Radius/TACACS+ • Nu se accepta echipamente al căror management se realizează în cloud-uri publice • Nu se accepta echipamente ce pot fi configurate exclusiv cu software adiacent de management • Toate funcționalitățile sa poată fi configurate exclusiv pe echipamentul ofertat fără necesitatea suplimentara a unui echipament/platforme de management • Sa permita folosirea unei platforme de management pentru echipament prin intermediul careia se pot realiza operatiuni de: automatizarea provizionarii, depanare evenimente, verificare si validare configuratie, monitorizare stare echipamente, monitorizare topologie si alertare si sa fie licentiat in efectuarea tuturor operatiunilor anterior mentionate (platforma de management anterior mentionata trebuie sa fie de la acelasi producator ca si echipamentul)
7.	**Licente**
	• Toate porturile active la viteza maximă • Licențiere inclusă pentru servicii Layer3, OSPF, EVPN, BGP și VXLAN, în cazul în care echipamentul necesită licențiere separată pentru aceste protocoale (sa fie posibila crearea unei topologii folosind protocoalele MP-BGP VXLAN EVPN) • Licentiat pentru utilizarea platformei de management echipament, de la producator (nu compatibil), conform cerintelor din zona de Management (Licentiat perpetuu și cu suport și update pe toată perioada garanției ofertate) • Licentierea trebuie sa asigure functionalitatile mentionate in prezentul CS si dupa expirarea suport-ului si garantiei
8.	**Alimentare cu energie electrica**
	• 2 Sursele de alimentare cu suport pentru standardele româneşti: 220 VAC / 50 Hz internă
9.	**Consum maxim de putere**
	• 600 W
10.	**Temperatura de operare**
	• 0° la 40°C
11.	**Timp de raspuns la solicitare in caz de defectiune**
	• Maximum 4 ore de la solicitare
12.	**Timp de remediere/inlocuire**
	• Inlocuirea echipamentului defect cu unul echivalent, configurat corespunzător, se face în maximum 24 de ore dacă defectul nu este remediat
13.	**Garantie si suport tehnic**
	• Garanție hardware: 5 ani • Update software gratuit: 5 ani

	• Acces direct la suportul tehnic al fabricantului: 5 ani • Discurile sau mediile de stocare defecte vor rămâne în proprietatea autorității contractante (keep your drive sau echivalent) • Suportul va fi de tip 24x7, de la producător, minim 5 ani de la semnarea documentelor de recepție cantitativă și calitativă. • Garanția va include update gratuit la noile versiuni ale sistemului de operare al echipamentului pe toată durata perioadei de garanție ofertată • Contractantul va face dovada activării serviciilor de suport prin prezentarea unui raport ce trebuie să identifice echipamentele pe site-ul producătorului, având ca și client final beneficiarul. • Raportul va trebui să conțină pentru fiecare componentă cel puțin seria și perioada activată de suport. • Echipamentele livrate vor fi noi și neutilizate • Echipamentele ofertate nu trebuie sa fie anunțate/declarate end-of-life/end of sale/end of support la momentul ofertării. În cazul in care in perioada derularii acordului cadru echipamentul ofertat este end-of-life/end of sale/end of support ofertantul il va înlocui cu un echipament echivalent sau superior. • Echipamentul va fi livrat cu ultima versiune a sistemului de operare recomandat de către producător.
14.	**Accesorii**
	• 1 X cablu consolă • 2 X cablu de alimentare energie electrică tip C13-C14 • 1 X kit de instalare 19'' cu toate cablurile de protecţie (împământare), şuruburile, cât şi alte accesorii necesare instalării şi punerii în funcţiune incluse • 10 buc modul optic 25G-LR-S SM conector LC sau compatibil • 10 buc patch FO SM LC-LC, cu lungimi diferite(compatibile tranceiver ofertat) : 10 buc 3m, 10 buc 2m • 10 buc modul optic 25G-SR-S MM conector LC sau compatibil • 10 buc patch FO MM LC-LC, cu lungimi diferite(compatibile tranceiver ofertat) : 10 buc 3m, 10 buc 2m • 6 module optice QSFP28-100GB SMF conector LC exemplu: QSFP-100G-DR-S • 12 buc patch FO SM-LC compatibil transceiver QSFP28 ofertat, cu o lungime de 2m

3.2.4.6 Switch management – 1 buc

1.	**Descriere generală și specificații hardware**
	• 48 interfețe 100M/1G Base-T(sau port-uri SFP cu SFP-T uri instalate in fiecare interfata) , 4 interfețe 1/10/25G SFP28 si 2 interfețe 40/100G QSFP28 (sau port-uri SFP cu SFP uri instalate in fiecare interfata astfel incat sa fie livrata configuratia propusa de port-uri) • minim 2 surse de alimentare în curent alternativ, redundante • Rackabil 19” 1U • minim 1 port 10/100/1000 RJ45 pentru management şi consolă • minim 1 port USB tip A pentru stocare şi boot • Minimum 3 ventilatoare înlocuibile instalate astfel încât răcirea echipamentului să se realizeze din faţă spre spate (Front to Back Airflow), iar un ventilator defect nu va afecta performanțele echipamentului • Procesor minim 4 Core-uri; • Memorie sistem minim 8 GB RAM; • Disc SSD minim 16 GB;

	• Buffer minim 40 MB; • Defectarea oricărei interfețe fizice de trafic (inclusiv modul optic) nu trebuie sa impacteze disponibilitatea celorlalte interfețe fizice de trafic rămase.
2.	**Performanta sistemului**
	• 0.384 Tbps switching capacity (0.696 Tbps switching capacity - bidirectional) • 517 mpps switching capacity • Latență maximă 2 micro-secunde • Minim 4k VLAN-uri • Minim 1000 instanțe VRF • Minim 64 căi ECMP • Minim 256 port channel • Minim 32 link-uri într-un port channel • Minim 4 sesiuni SPAN active • Minim 3967 instanțe RPVST • Minim 490 grupuri HSRP • Minim 64 instanțe MST • Minim16000 rute LPM • Minim 16000 intrări IP • Minim 97000 adrese MAC • Minim 8000 rute multicast • Grupuri IGMP snooping minim 8000 • reguli de filtrare ACL pe intrare(2000/slice) și reguli pe ieșire (1000/slice)
3.	**Standarde și caracteristici minimale incluse**
	Standarde: • IEEE 802.1D Bridging and Spanning Tree • IEEE 802.1p QoS/CoS • IEEE 802.1Q VLAN Tagging • IEEE 802.1w Rapid Spanning Tree • IEEE 802.1s Multiple Spanning Tree Protocol • IEEE 802.1AB Link Layer Discovery Protocol • IEEE 802.3ad Link Aggregation with LACP • IEEE 802.3x Flow Control • IEEE 802.3z Gigabit Ethernet • IEEE 802.3ae 10 Gigabit Ethernet • IEEE 802.3by 25 Gigabit Ethernet • IEEE 802.3ba 40 Gigabit Ethernet • IEEE 802.3ba 100 Gigabit Ethernet • RMON **Caracteristici minimale:** • Imagine pentru servicii Layer 3, OSPF, BGP, VXLAN, EVPN • Minim 4 cozi QoS per port • Class of Service (CoS) • Differentiated Services Code Point (DSCP) • Port security • Acces Control Lists pe port şi VLAN • Private VLANs

	• Traffic Storm Control • Control-plane policing • Rapid Per VLAN Spanning Tree (RPVST+) • VRF • BFD
4.	**Management**
	Administrare: • ssh CLI , telnet, consolă • Utilizatori/Administratori cu drepturi configurabile • Syslog, SNMP, monitorizare fluxuri de trafic (NetFlow/JFlow sau echivalent), log-uri interne, grafice • Se vor documenta si livra MIB. **Autentificare:** • Bază de date locală • Integrare Radius/TACACS+ • Nu se accepta echipamente al căror management se realizează în cloud-uri publice • Nu se accepta echipamente ce pot fi configurate exclusiv cu software adiacent de management • Toate funcționalitățile sa poată fi configurate exclusiv pe echipamentul ofertat fără necesitatea suplimentara a unui echipament/platforme de management • Sa permita folosirea unei platforme de management pentru echipament prin intermediul careia se pot realiza operatiuni de: automatizarea provizionarii, depanare evenimente, verificare si validare configuratie, monitorizare stare echipamente, monitorizare topologie si alertare si sa fie licentiat in efectuarea tuturor operatiunilor anterior mentionate (platforma de management anterior mentionata trebuie sa fie de la acelasi producator ca si echipamentul)
5.	**Licențe**
	• Toate porturile active la viteza maximă • Licențiere inclusă pentru servicii Layer3, OSPF, EVPN, BGP și VXLAN, în cazul în care echipamentul necesită licențiere separată pentru aceste protocoale (sa fie posibila crearea unei topologii folosind protocoalele MP-BGP VXLAN EVPN) • Licentiat pentru utilizarea platformei de management echipament, de la producator (nu compatibil), conform cerintelor din zona de Management (Licentiat perpetuu și cu suport și update pe toată perioada garanției ofertate) • Licentierea trebuie sa asigure functionalitatile mentionate in prezentul CS si dupa expirarea suport-ului si garantiei
6.	**Parametrii functionare**
	Alimentare cu energie electrică: • 2 Sursele de alimentare cu suport pentru standardele româneşti: 220 VAC / 50 Hz internă **Consum maxim de putere:** • 600W

	Temperatura de operare: • De la 0 la 40 grade Celsius
7.	**Garanție și suport tehnic**
	• Garanție hardware: 5 ani • Update software gratuit: 5 ani • Acces direct la suportul tehnic al fabricantului: 5 ani • Discurile sau mediile de stocare defecte vor rămâne în proprietatea autorității contractante (keep your drive sau echivalent) • Suportul va fi de tip 24x7, de la producător, minim 5 ani de la semnarea documentelor de recepție cantitativă și calitativă. • Garanția va include update gratuit la noile versiuni ale sistemului de operare al echipamentului pe toată durata perioadei de garanție ofertată • Timpul de răspuns la solicitare în caz de defecțiune să nu depășească 4 ore de la solicitare • Timpul de remediere/înlocuire a echipamentului defect cu unul echivalent, configurat corespunzător, va fi de cel mult 24 de ore dacă defectul nu poate fi remediat.Garanția va include acces la suportul tehnic al producătorului pe toată durata perioadei de garanție ofertată. • Contractantul va face dovada activării serviciilor de suport prin prezentarea unui raport ce trebuie să identifice echipamentele pe site-ul producătorului, având ca și client final beneficiarul. • Raportul va trebui să conțină pentru fiecare componentă cel puțin seria și perioada activată de suport. • Echipamentele livrate vor fi noi și neutilizate • Echipamentele ofertate nu trebuie sa fie anunțate/declarate end-of-life/end of sale/end of support la momentul ofertării. În cazul in care in perioada derularii acordului cadru echipamentul ofertat este end-of-life/end of sale/end of support ofertantul il va înlocui cu un echipament echivalent sau superior. • Echipamentul va fi livrat cu ultima versiune a sistemului de operare recomandat de către producător.
8.	**Accesorii**
	• 1 X cablu consolă • 2 X cablu de alimentare energie electrică tip C13-C14 • 1 X kit de instalare 19'' cu toate cablurile de protecţie (împământare), şuruburile, cât şi alte accesorii necesare instalării şi punerii în funcţiune incluse • 30 patch-uri RJ45 CAT6 de lungime : 15 buc 2m, 15 buc 3m • 2 module optice QSFP-40GB LR SM LC-LC exemplu: QSFP-40G-LR4S • 4 buc patch FO SM-LC compatibil transceiver QSFP ofertat, cu o lungime de 2m • 2 module optice QSFP28-100GB SMF conector LC exemplu: QSFP-100G-DR-S • 4 buc patch FO SM-LC compatibil transceiver QSFP28 ofertat, cu o lungime de 2m • 2 buc modul optic 25G-LR-S SM conector LC • 4 buc patch FO SM LC-LC, cu lungimi diferite(compatibile tranceiver ofertat) : 4 buc 3m, 4 buc 2m

3.2.4.7 Router tip 1 – 4 buc

Caracteristica	Cerințe specifice minime
Descriere generala	Echipament integrat de protecție in rețea cu capabilități de scanare antivirus, controlul aplicațiilor si prevenirea intruziunilor destinat folosirii ca o soluție de agregare VPN si acces la Internet pentru utilizatorii din rețeaua ITM.
Specificații hardware	• 4 x interfețe 10 GbE SFP+; • 8 x interfețe 1 GbE SFP; • 12 x interfețe 1 GbE RJ45; • 1 x interfață pentru HA; • 1 x interfață pentru Management; • 1 x port USB; • 1 x consola; • Stocare interna 240 GB SSD.
Performanta sistemului	• Firewall Throughput: 25 Gbps; • IPSec VPN Throughput (AES256-SHA256): 13 Gbps; • IPS Throughput: 4.5 Gbps; • Throughput combinat scanari de securitate: 2.5 Gbps; • Tunele IPSec VPN (gateway to gateway) concurente: 2000; • Tunele IPSec VPN (client to gateway) concurente: 16000; • Useri SSL-VPN: 500; • Concurrent session: 3 Milioane; • New Session/Sec: 250000; • Instanțe virtuale: 10; • Configurații redundante posibile: Activ/Activ, Activ/Pasiv.
Parametrii echipament	• Alimentare alternativa 100-240V, 50-60Hz; • 2x surse de alimentare redundante incluse; • Kit de instalare pentru montarea in rack in rack 19”;
Protocoale si standarde	Servicii de Rețea Rutare/Rețea: Suport WAN multiplu; DHCP; Policy routing; Rutare statica; Rutare dinamica RIP, OSPF, BGP; VLAN Tagging (802.1q); Suport Ipv6. Instanțe Virtuale: Instanțe Firewall/Rutare separate; High Availability: Activ/Activ, Activ/Pasiv; Statefull Failover; Link status monitor. Servicii de Securitate Firewall:

	NAT/Transparent; Policy-based NAT; VLAN Tagging(802.1q); SIP/H.323/SCCP NAT Traversal; Profile granulare de protecție per-policy; Suport Ipv6. VPN: IPSec, SSL; Suport criptare: AES-256; Autentificare: SHA-512; Autentificare IKE cu Certificate (v1 si v2) sau preshared key; NAT Traversal. Prevenirea Intruziunilor: Suport Anomalii de protocoale; Suport Semnături definite de utilizator; Suport Ipv6. Antivirus: Suport Antimalware; Blocare Boti; Suport Ipv6. Control Aplicații SSL Scanare SSL pentru IPS si Antivirus.
Management	Administrare: Consola, SSH, HTTPS; Syslog, SNMP, log-uri stocate intern, grafice, notificări email. Autentificare: Baza de date locala; Integrare Active Directory; Integrare LDAP/Radius/TACACS+. Nu se accepta echipamente de tip “cloud-based”. Toate funcționalitățile sa poată fi configurate exclusiv pe echipamentul ofertat, fără necesitatea suplimentara a unui echipament/ unei platforme de management.
Software	• Abonament pentru toate serviciile de protecție activate: 5 ani. • Licență perpetua pentru număr nelimitat de adrese IP. • Licență perpetua 10 instanțe virtuale firewall. • Licență perpetua pentru activarea tuturor interfețelor la viteza maxima. • Licență perpetua pentru activarea echipamentului la capacitate maxima. • Licență perpetua pentru număr nelimitat de stații de administrare. • Echipamentul trebuie sa continue sa funcționeze după expirarea licențelor. • Toate funcționalitățile sa poată fi configurate fără necesitatea unei platforme adiacente de management proprietare.

Garanție si suport tehnic	• Garanție hardware: 5 ani • Update software gratuit: 5 ani • Suportul va fi de tip 24x7, de la producător, minim 5 ani de la semnarea documentelor de recepție cantitativă și calitativă. • Garanția va include update gratuit la noile versiuni ale sistemului de operare al echipamentului pe toată durata perioadei de garanție ofertată • Garanția va include acces la suportul tehnic al producătorului pe toată durata perioadei de garanție ofertată. • Contractantul va face dovada activării serviciilor de suport prin prezentarea unui raport ce trebuie să identifice echipamentele pe site-ul producătorului, având ca și client final beneficiarul. • Echipamentele livrate vor fi noi și neutilizate • Echipamentele ofertate nu trebuie sa fie anunțate/declarate end-of-life/end of sale/end of support la momentul ofertării.

3.2.4.8 Router tip 2 – 88 buc

Caracteristica	**Cerințe specifice minime**
Descriere generala	Echipament integrat de protecție in rețea cu capabilități de scanare antivirus, controlul aplicațiilor si prevenirea intruziunilor destinat folosirii ca o soluție de securitate unificata si comunicații VPN la nivelul inspectoratelor județene.
Specificații hardware	• 7 x interfețe 1GbE RJ45; • 1 x port USB; • 1 x consola; • Stocare interna 128 GB SSD.
Performanta sistemului	• Firewall Throughput: 10 Gbps; • IPSec VPN Throughput (AES256-SHA256): 5 Gbps; • IPS Throughput: 1.3 Gbps; • Throughput combinat scanari de securitate: 650 Mbps; • Tunele IPSec VPN (gateway to gateway) concurente: 200; • Useri SSL-VPN: 200; • Concurrent session: 700000; • New Session/Sec: 35000; • Configurații redundante posibile: Activ/Activ, Activ/Pasiv.
Parametrii echipament	Alimentare alternativa 100-240V, 50-60Hz;
Protocoale si standarde	Servicii de Rețea Rutare/Rețea: Suport WAN multiplu; DHCP; Policy routing; Rutare statica; Rutare dinamica RIP, OSPF, BGP; VLAN Tagging (802.1q);

	Suport Ipv6. Instanțe Virtuale: Instanțe Firewall/Rutare separate; High Availability: Activ/Activ, Activ/Pasiv; Statefull Failover; Link status monitor. Servicii de Securitate Firewall: NAT/Transparent; Policy-based NAT; VLAN Tagging(802.1q); SIP/H.323/SCCP NAT Traversal; Profile granulare de protecție per-policy; Suport Ipv6. VPN: IPSec, SSL; Suport criptare: AES-256; Autentificare: SHA-512; Autentificare IKE cu Certificate (v1 si v2) sau preshared key; NAT Traversal. Prevenirea Intruziunilor: Suport Anomalii de protocoale; Suport Semnături definite de utilizator; Suport Ipv6. Antivirus: Suport Antimalware; Blocare Boti; Suport Ipv6. Control Aplicații SSL Scanare SSL pentru IPS si Antivirus.
Management	Administrare: Consola, SSH, HTTPS; Syslog, SNMP, log-uri stocate intern, grafice, notificări email. Autentificare: Baza de date locala; Integrare Active Directory; Integrare LDAP/Radius/TACACS+. Nu se accepta echipamente de tip “cloud-based”.
Software	• Licență perpetua pentru număr nelimitat de adrese IP. • Licență perpetua pentru activarea tuturor interfețelor la viteza maxima.

	• Licență perpetua pentru activarea echipamentului la capacitate maxima. • Licență perpetua pentru număr nelimitat de stații de administrare. • Nu se solicită licență pentru update-uri ale semnăturilor UTM, dar să fie posibilă această facilitate ulterior. • Echipamentul trebuie sa continue sa funcționeze după expirarea licențelor. • Toate funcționalitățile sa poată fi configurate fără necesitatea unei platforme adiacente de management proprietare.
Service si garanție	• Garanție hardware: 5 ani • Update software gratuit: 5 ani • Acces direct la suportul tehnic al fabricantului: 5 ani • Suportul va fi de tip 24x7, de la producător, minim 5 ani de la semnarea documentelor de recepție cantitativă și calitativă. • Garanția va include update gratuit la noile versiuni ale sistemului de operare al echipamentului pe toată durata perioadei de garanție ofertată; • Echipamentele livrate vor fi noi și neutilizate; • Echipamentele ofertate nu trebuie sa fie anunțate/declarate end-of-life/end of sale/end of support la momentul ofertării.

3.2.4.9 Router tip 3 – 32 buc

Caracteristica	**Cerințe specifice minime**
Descriere generala	Echipament integrat de protecție in rețea cu capabilități de scanare antivirus, controlul aplicațiilor si prevenirea intruziunilor destinat folosirii ca o soluție de securitate unificata.
Specificații hardware	• 4 x interfețe 1 GbE RJ45; • 1 x port USB; • 1 x consola;
Performanta sistemului	• Firewall Throughput: 4 Gbps; • IPSec VPN Throughput (AES256-SHA256): 3.5 Gbps; • IPS Throughput: 950 Mbps; • Throughput combinat scanari de securitate: 550 Mbps; • Tunele IPSec VPN (gateway to gateway) concurente: 200; • Useri SSL-VPN: 200; • Concurrent session: 380000; • New Session/Sec: 35000; • Configurații redundante posibile: Activ/Activ, Activ/Pasiv.
Parametrii echipament	Alimentare alternativa 100-240V, 50-60Hz;
Protocoale si standarde	Servicii de Rețea Rutare/Rețea:

	DHCP; Policy routing; Rutare statica; Rutare dinamica RIP, OSPF, BGP; VLAN Tagging (802.1q); Suport Ipv6. High Availability: Activ/Activ, Activ/Pasiv; Statefull Failover; Link status monitor. Servicii de Securitate Firewall: NAT/Transparent; Policy-based NAT; SIP/H.323/SCCP NAT Traversal; Profile granulare de protecție per-policy; Suport Ipv6. VPN: IPSec, SSL; Suport criptare: AES-256; Autentificare: SHA-512; Autentificare IKE cu Certificate (v1 si v2) sau preshared key; NAT Traversal. Prevenirea Intruziunilor: Suport Anomalii de protocoale; Suport Semnături definite de utilizator; Suport Ipv6. Antivirus: Suport Antimalware; Blocare Boti; Suport Ipv6. Control Aplicații SSL Scanare SSL pentru IPS si Antivirus.
Management	Administrare: Consola, SSH, HTTPS; Syslog, SNMP, log-uri stocate intern, grafice, notificări email. Autentificare: Baza de date locala; Integrare Active Directory; Integrare LDAP/Radius/TACACS+. Nu se accepta echipamente de tip “cloud-based”.

Software	• Licență perpetua pentru număr nelimitat de adrese IP. • Licență perpetua pentru activarea tuturor interfețelor la viteza maxima. • Licență perpetua pentru activarea echipamentului la capacitate maxima. • Licență perpetua pentru număr nelimitat de stații de administrare. • Nu se solicită licență pentru update-uri ale semnăturilor UTM, dar să fie posibilă această facilitate ulterior. • Echipamentul trebuie sa continue sa funcționeze după expirarea licențelor. • Toate funcționalitățile sa poată fi configurate fără necesitatea unei platforme adiacente de management proprietare.
Service si garanție	• Garanție hardware: 5 ani • Update software gratuit: 5 ani • Acces direct la suportul tehnic al fabricantului: 5 ani • Suportul va fi de tip 24x7, de la producător, minim 5 ani de la semnarea documentelor de recepție cantitativă și calitativă. • Garanția va include update gratuit la noile versiuni ale sistemului de operare al echipamentului pe toată durata perioadei de garanție ofertată; • Echipamentele livrate vor fi noi și neutilizate; • Echipamentele ofertate nu trebuie sa fie anunțate/declarate end-of-life/end of sale/end of support la momentul ofertării.

3.2.4.10 Soluție acces VPN securizat – 2000 utilizatori

Caracteristica	**Cerințe specifice minime**
Descriere generala	Soluție de tip platformă de management centralizat al clienților tip Remote Access VPN securizat
Funcționalități generale	• Număr minim de clienți VPN cu capabilități de securitate avansata: 2000. • Permite distribuirea automata a configurațiilor de securitate stabilite de administrator pe toate terminalele înrolate in sistem. • Permite identificarea vulnerabilităților sistemelor de operare si a aplicațiilor instalate pe terminalele înrolate in sistem. • Permite actualizarea centralizată pentru patch-urile sistemului de operare si ale aplicațiilor de interes care nu au instalata ultima versiune de software recomandata • Permite integrarea cu server de AD/LDAP. • Permite accesul securizat la aplicații web • Permite scanarea antivirus a terminalului pe care este instalat • Permite monitorizarea în timp real a incidentelor survenite pe terminalele gestionate. • Permite configurații de tip „split tunneling” pentru conexiunea VPN. • Permite implementarea de soluții tip MFA pentru autentificarea utilizatorilor VPN • Permite instalarea clientului VPN pe terminale cu sisteme de operare

	Windows/Mac
Management	Administrare: a) Acces prin HTTPS a. Utilizatori/Administratori cu drepturi configurabile b) Autentificare: a. Bază de date locală b. Integrare LDAP/Radius/TACACS+ c) Configurarea echipamentului să fie posibilă din GUI pe sisteme multiple de operare (Windows/Mac) d) Nu se accepta soluții al căror management se realizează in cloud-uri publice Nu se accepta soluții ce pot fi configurate exclusiv cu software adiacent de management
Licențe și garanție	• Produsul va fi livrat cu licențele necesare funcționării tuturor capabilităților in conformitate cu specificațiile cerute. • Se oferă suport de la producător cu un SLA de tip 8x5 NBD pentru minim 5 ani. • Furnizorul va face dovada activării serviciilor de suport prin prezentarea unui raport ce trebuie să identifice pe site-ul producătorului soluției, având ca și client final beneficiarul. Raportul va trebui să conțină pentru fiecare componentă cel puțin seria și perioada activată de suport.
Alte caracteristici	• Nu se acceptă produse software a căror funcționare se realizează in cloud-uri publice. • Soluția ofertata va fi de la același producător cu echipamentul de tip Router tip 1 pentru a facilita integrarea in mod nativ. • Soluția va fi livrată la ultima versiune recomandată de producător

3.2.5 Componentele de infrastructură software

Pentru toate produsele software nu se acceptă și nu se vor achiziționa licențe care vor expira după o anumită perioadă, degradând astfel performanțele sau capacitatea funcțională a sistemului ofertat și acceptat în perioada de exploatare a sistemului. Oferta va include menționarea în clar a modalității de licențiere șia perioadei licențiate. Acolo unde nu există un model de licențiere de tip perpetuu, pentru licențele de tip subscripție se va asigura disponibilitatea acestora pentru minim perioada de exploare a sistemului stabilită la 10 ani, conform studiului de fezabilitate aprobat.

3.2.5.1 Componenta de virtualizare

Soluția de virtualizare trebuie să respecte minim următoarele cerințe tehnice și funcționale:

- Soluția trebuie să asigure rate mari de consolidare a mașinilor virtuale pe host-uri prin mecanisme de optimizare și supra alocare a memoriei pentru reducerea costurilor asociate infrastructurii fizice (ex. număr host-uri, număr porturi de rețea / switch-uri) și de licențiere precum și pentru asigurarea continuității în funcționare a aplicațiilor în cazul unor întreruperi parțiale neplanificate.
- Soluția trebuie să permită crearea de grupuri virtuale de resurse (memorie și procesor) pentru controlul și asigurarea performanțelor mașinilor virtuale care folosesc în comun respectivele grupuri de resurse.

- Soluția trebuie să permită adăugarea de noi sisteme de calcul sau de stocare, în grupul de resurse, fără întreruperea serviciilor.
- Soluția trebuie să permită redistribuirea încărcării pe resursele noi adăugate fără întreruperea serviciilor.
- Soluția trebuie să permită balansarea automată a încărcării pe host-urile din cluster prin mutarea mașinilor virtuale în vedere asigurării resurselor optime pentru funcționare.
- Soluția trebuie să ofere disponibilitate continuă, fără pierderi de date sau întreruperi, pentru toate serviciile sau aplicațiile.
- Soluția trebuie sa ofere o arhitectură independentă de un sistem de operare de uz general cu o amprentă pe disc cât mai mică și care permite ca instalarea și boot-area hipervizorului să fie făcută foarte rapid.
- Hipervizorul trebuie să fie compatibil cu diverse tipuri de sisteme de operare pentru mașinile găzduite, cel puțin Linux, Windows sau alte sisteme de operare Unix, bazate pe arhitectura x86.
- Hipervizorul trebuie să ofere flexibilitate în ceea ce privește alocarea resurselor pentru mașinile virtuale: puterea de procesare, memorie, extindere discuri, adăugarea de unități de discuri suplimentare.
- Soluția trebuie să permită creare de profile pentru host-uri (servere fizice) astfel încât instalarea pe mai multe host-uri să se facă foarte rapid, respectând o configurație prestabilită, configurabilă pentru eliminarea erorilor umane de configurare.
- În cazul defecțiunilor hardware sau a altor disfuncționalități apărute, soluția trebuie să genereze, în mod automat, un comportament specific, predefinit.
- Soluția trebuie să poată efectua migrări concurente. Numărul acestora nu trebuie să fie limitat de tipul de licențiere.
- Soluția trebuie să ofere sugestii în ceea ce privește alocarea optimă a resurselor pentru mașinile virtuale.
- Soluția trebuie să permită optimizarea consumului de energie pe serverele din cluster în perioadele cu încărcare mică.
- Soluția trebuie să ofere capabilitatea de a adăuga servere fizice noi (inactive) în cazul creșterii nevoilor de calcul.
- Soluția trebuie să permită alocarea și dealocarea dinamică a resurselor în cazul limitării performanțelor maxime.
- Soluția trebuie să ofere îndrumare cu privire la procesul de consolidare, pe baza unor metodologii de analiză a performanței.
- Soluția trebuie să ofere posibilitatea de a redistribui automat capacitatea de calcul și de a asigura faptul că fiecare mașină virtuală are acces la resursele alocate, în orice moment.
- Soluția trebuie să dispună de capacități de failover astfel încât, în cazul defectării unui host, mașinile virtuale care rulau pe acel host să fie migrate automat pe celelalte host-uri din cluster, iar host-ul degradat să fie trecut automat în mentenanță după evacuarea mașinilor virtuale.
- Soluția trebuie să dispună de capacitate de failover care să detecteze problemele de acces la datastore la nivel de host și să repornească în mod automat mașinile virtuale afectate pe un alt host din cluster.
- Soluția trebuie să dispună de capacități de failover astfel încât, în cazul blocării sistemului de operare instalat într-o mașină virtuală, respectiva mașină virtuală să fie repornită automat pentru deblocarea sistemului de operare, a serviciilor și aplicațiilor.
- Soluția trebuie sa dispună de mecanisme de creștere a resurselor (CPU, RAM) unei masini virtuale pornite, fără a fi necesară repornirea acesteia.

- Platforma de virtualizare va fi licentiata perpetuu astfel incat sa acopere toate procesoarele/core-urile serverelor. Astfel, platforma din centrul de date trebuie sa fie licentiata pentru cel putin 12 servere (minim 24 procesoare). Platforma de virtualizare trebuie sa includa suport pentru o perioada de minim 60 de luni.
- Platforma de virtualizare trebuie sa se integreze cu solutia de virtulizare existenta in centrul de date STS, VMWare vSphere.
  Nu este necesara licentierea solutie de management centralizat, intrucat sistemul va fi intehrat intr-o solutie centralizata de management existenta.

3.2.5.2 Componenta de sisteme de operare de tip server

În funcție de soluția tehnică propusă Ofertanții vor livra sistemele de operare necesare rulării componentelor soluției licențiate conform regulilor producătorilor respectivi.

Toate produsele propuse vor include suport pe o perioadă de minim 60 de luni inclusiv acces la centrul de suport al producătorului pentru soluții tehnice sau actualizări software când este cazul. Este responsabilitatea Prestatorului de a achiziționa acest tip de servicii de la producător sau de la un distribuitor autorizat de acesta, pentru toată perioada de garanție ofertată și de a le transfera Autorității Contractante odată cu livrarea și punerea în funcțiune a soluției software. Detaliile privind contul Achizitorului la producător/distribuitor autorizat vor fi furnizate la livrarea și punerea în funcțiune a soluției software. Instalarea actualizărilor, precum și deschiderea de tichete de suport sau orice alte activități legate de mentenanța și garanția soluției software vor fi asigurate de către prestator pe toată durata perioadei de garanție și suport ofertate.

3.2.5.3 Platforma de salvare date

Descriere generală	Platformă de backup care rulează în mediu virtual și se integrează nativ cu platforma de virtualizare livrată.
Cerințe Generale	Soluția trebuie sa suporte toate sistemele de operare ale mașinilor virtuale, care sunt suportate de VMware, KVM si Hyper-V; Soluția trebuie sa suporte protectia datelor din echipamente de tip NAS, utilizând protocoalele SMB/CIFS si NFS, dar si direct din file servere Linux si Windows;
Cerințe funcționale	Soluția trebuie sa fie agnostica la hardware și să poată utiliza pentru stocare, orice tip de echipament (inclusiv servere obișnuite). Soluția trebuie să stocheze backup-urile în fișiere auto-suficiente, sub forma unor fișiere care pot fi copiate sau mutate. Soluția trebuie să ofere posibilitatea de a crea backup-uri în modul complet (full), sintetic full, și incremental. Soluția trebuie sa ofere mecanisme de compresie și de-duplicare, care să reducă spațiul necesar de stocare a backup-urilor. Funcționalitățile de de-duplicare și compresie nu trebuie să introducă restricții referitor la funcționalitățile solicitate. Soluția trebuie să ofere abstractizarea (virtualizarea) echipamentelor utilizate pentru stocarea backup-urilor, realizând un singur spațiu utilizabil, din alocarea unuia sau mai multor servere sau echipamente de stocare. Această funcționalitate nu trebuie să aibă limitări referitoare la numărul de echipamente ce

	pot fi abstractizate. Soluția trebuie să permită extinderea spațiului de stocare pentru backup, prin integrarea infrastructuri care oferă spațiu de stocare de tip cloud ce utilizează protocol compatibil S3. Utilizarea spațiului de stocare din cloud nu trebuie să fie limitată la cantitatea de date, iar migrarea între spațiul de stocare utilizat și spațiul din cloud să se realizeze transparent, pe baza unor politici ce pot fi controlate de către administratori; Doar blocurile unice vor fi transferate, pentru a minimiza operațiile de transfer; Locația datelor nu va restricționa operațiile de restaurare cerute. Soluția nu va folosi o bază de date centralizată pentru meta-datele de-duplicării. Soluțiile care pot pierde informațiile referitoare la de-duplicare care implică imposibilitatea utilizării/ restaurării datelor, nu sunt acceptate; Soluția trebuie să ofere posibilitatea de a realiza operațiile de restaurare din orice fel de backup (full sau incremental) fie că este vorba de operații de restaurare integrală sau restaurare granulară. Soluția trebuie să ofere posibilitatea de a rula scripturi, înainte sau după execuția unui backup sau a unei replicări; Soluția trebuie să ofere posibilitatea de restaurare de tip self-service, prin care utilizatorii pot restaura fișiere, mașini virtuale, e-mailuri si baze de date (inclusiv restaurare de tip “point-in-time”). Soluția trebuie să ofere posibilitatea de a utiliza REST API pentru operații de administrare. Soluția trebuie să ofere posibilitatea criptării. Criptarea trebuie să poată fi realizată și la nivelul rețelei (transferul datelor să se realizeze criptat), dar și stocarea informațiilor trebuie să se realizeze criptat; Utilizarea criptării nu trebuie să dezactiveze nici o funcționalitate menționata în prezentele cerințe. Soluția trebuie să aibă o arhitectura client/server și să ofere posibilitatea instalării consolei de administrare pentru mai mulți administratori.
Cerințe pentru minimizarea pierderilor de date	Soluția trebuie să ofere mecanisme de limitare a stresului echipamentelor de stocare din producție, în sensul în care sa își poată limita procesele de backup astfel încât să nu afecteze aceste echipamente în perioadele de utilizare intense în care nivelul latenței crește. Această opțiune va fi configurabila la nivelul fiecărui volum/datastore. Soluția va identifica automat *snapshot*-urile orfane pentru mașinile virtuale și va realiza operațiile de consolidare automat, fără intervenția administratorilor, pentru a elimina aceste situații. Soluția va oferi posibilitatea de a realiza backup-uri utilizând capabilitățile de *snapshot* din echipamentele de stocare. De asemenea, integrarea va permite ca operațiile de restaurare să fie realizate din *snapshot*-urile echipamentelor de stocare. Aceste capabilități trebuie să fie disponibile pentru cel puțin trei producători de echipamente de stocare. Soluția trebuie să fie compatibilă cu o soluție *Software Defined Storage* (SDS) ce poate fi integrată în platforma de virtualizare. Soluția trebuie să suporte protocolul NDMP.

	Soluția trebuie să ofere posibilității de a păstra backup-urile realizate, sub scheme de retenție de tip GFS (*Grandfather-father-son*). Soluția trebuie să fie capabilă să realizeze copii ale backup-urilor sau să replice mașinile virtuale într-o locație diferită, utilizând tehnologii pentru accelerare a transferului de date peste rețele WAN. Soluția trebuie să permită, în cazul replicării, păstrării mai multor replici și puncte de restaurare, configurabil, pentru fiecare mașină virtuală. Soluția trebuie să permită utilizarea unei alte mașini virtuale pentru a inițializa relațiile de replicare noi definite ("*seeding*"). Soluția trebuie să ofere procesarea în paralel a mașinilor virtuale, inclusiv a restaurărilor în paralel a discurilor mașinilor.
Cerințe pentru recuperare	Soluția trebuie să ofere mecanisme de restaurare instantanee a mașinilor virtuale, prin care mai multe mașini să poată fi pornite din backup fără a fi necesara copierea datelor. Soluția trebuie să permită prezentarea discurilor mașinilor virtuale direct din backup, către o mașină virtuală pornită; Soluția trebuie să permită următoarele tipuri de restaurare: restaurare integrală (a mașinilor virtuale), fișiere și/sau directoare din mașinile virtuale (restaurare granulară), și discuri ale mașinilor virtuale (disk restore). Soluția trebuie să permită restaurarea fișierelor sau directoarelor către locația originală, către o mașină virtuală ce rulează, și către stațiile de administrare utilizate de administrator; soluția nu va avea limitări referitor la dimensiunea fișierelor sau discurilor ce urmează a fi restaurate. Soluția trebuie să suporte restaurare fișierelor din următoarele sisteme de fișiere: ✓ Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs; ✓ Windows: NTFS, FAT, FAT32, ReFS Soluția trebuie să permită restaurarea fișierelor și directoarelor din sisteme ce utilizează Linux LVM. Soluția trebuie să permită recuperarea rapidă și granulară pentru aplicații ce rulează în mașinile protejate.
Cerințe pentru testarea periodică	Soluția va avea mecanisme de verificare și testare a mașinilor virtuale, iar aceste testări se vor realiza în aceste medii. Astfel, testele și verificările vor fi făcute prin restaurare – nu se accepta soluții care realizează testarea doar prin operații de tip checksum ale backup-urilor, fără realizarea restaurărilor. Testele de restaurare vor include testarea bunei funcționari a mașinilor virtuale, buna funcționare a rețelei și buna funcționare a aplicațiilor. Astfel, va fi permisă atașarea de scripturi care sa poată rula în mașinile recuperate, iar rezultatul va fi păstrat pentru viitoare auditări. Soluția va permite testarea atât pentru backup-urile realizate, dar și pentru replici ale mașinilor virtuale. Soluția trebuie sa aibă integrări cu cel puțin doi producători de

	Securitate, care să permită scanarea cu soluții de tip antivirus, a imaginilor ce urmează a fi restaurate, garantând astfel eliminarea oricăror posibile infecții cu software malițios. Scanarea trebuie să fie realizată la nivelul sistemelor de fișiere din backup-urile mașinilor virtuale, fără a fi necesară extragerea prealabilă a structurilor de date, extragere care ar încetinii procesul de scanare. Pentru compliență cu GDPR, soluția propusă trebuie să permită restaurări automate, în doi pași, prin care în primul pas este permisă aplicarea unor scripturi care să modifice datele, înainte de pasul doi în care se realizează restaurarea propriu zisă. Astfel, se dorește realizarea efectuării operațiilor de ștergere a informațiilor marcate ca uitate/șterse în producție, garantând astfel că în situația restaurării, aceste date nu vor pierde aceasta proprietate.
Monitorizare pentru soluția de protecție	Soluția trebuie să ofere posibilitatea organizarea pe categorii personalizate ale infrastructurii și a obiectelor. Soluția trebuie să ofere posibilitatea de a crea alarme pentru mașini virtuale sau grupuri de mașini virtuale. Soluția trebuie să permită programarea de rapoarte care să poată fi trimise via e-mail. Soluția trebuie să suporte mai multe conexiuni multiple și servere în același timp. Soluția trebuie să includă un set predefinit de alarme, posibilitatea de a defini noi alarme și posibilitatea de a modifica pe cele predefinite. Soluția trebuie să aibă o baza de cunoștințe (knowledge base) care descrie toate alarmele predefinite. Soluția trebuie să aibă dashboard-uri (panouri de comandă) centralizate, pentru a monitoriza elementele de infrastructură. Soluția trebuie să permită monitorizarea serverelor host. Soluția trebuie să permită monitorizarea serverelor de backup, a încărcării acestora sau a diverselor componente. Astfel va fi posibilă monitorizarea taskurilor de backup și replicare, totalul datelor protejate, starea taskurilor, starea mașinilor virtuale și realizarea testării automate. Soluția trebuie să ofere diagnostic inteligent pentru soluția de protecție, monitorizând log-urile acesteia și oferind rezolvări ale potențialelor probleme, oferind rezolvări fără a necesita deschiderea unor cazuri de suport.
Raportare pentru soluția de protecție	Soluția trebuie să permită programarea intervalelor de colecții de date, dar să permită și colecții ad-hoc. Soluția trebuie să permită generarea rapoartelor și trimiterea lor via e-mail. Soluția trebuie să aibă posibilitatea de a urmări schimbările intervenite în configurația mediilor virtuale, cu posibilitatea identificării acestor modificări și a utilizatorilor care au realizat aceste schimbări. Soluția trebuie să permită generarea de rapoarte pentru o

	perioadă de timp aleasă. Intervalul de timp va putea fi ușor modificat. Soluția trebuie să aibă rapoarte predefinite și să permită modificarea acestora. Soluția trebuie să permită analiza obiectelor supradimensionate (mașini virtuale ce au alocate mai multe resurse decât este necesar) și va sugera o metodă de optimizare a resurselor acestora. Soluția trebuie să permită generarea de rapoarte pentru modul de funcționare a soluției de protecție a datelor; Soluția va avea rapoarte referitoare la numărul de mașini protejate și starea acestora, a taskurilor de protecție, ce mașini nu sunt protejate sau care sunt resursele consumate de soluția de protecție, inclusiv spațiul de stocare consumat pentru backup-urile mașinilor virtuale. Soluția trebuie sa aibă rapoarte ce ajuta la planificarea capacităților pentru scenarii de tipul ce se poate întâmpla (scenarii "*what-if*"). Soluția trebuie să ofere vizibilitate granulară a mediului, bazată pe permisiunile utilizatorilor. Soluția trebuie să aibă rapoarte despre starea *snapshot*-urilor mașinilor virtuale, cât spațiu consumă aceste *snapshot*-uri și dacă există potențiale *snapshot*-uri orfane.
Licențe	Soluția trebuie sa fie licențiată pentru minim 50 mașini virtuale și să includă minim 5 ani de suport; Se va livra cu licențele necesare pentru sistemului de operare de tip Server în care va instala platforma de backup.

3.2.5.4 Componenta de gestiune a bazelor de date

Componenta de gestiune a bazei de date trebuie să asigure necesarul de persistență operațională pentru componentele aplicative ale sistemului, prin satisfacerea cerințelor descrise în continuare.

Modalitatea de licențiere va respecta normele de disponibilitate și performanță impuse, la încărcarea generată de utilizatorii menționați în cadrul prezentului proiect tehnic.

Componenta de sistem de gestiune a bazei de date trebuie să îndeplinească minim următoarele cerințe:

- să fie un sistem de gestiune a bazelor de date de tip relațional;
- să ruleze pe arhitecturi cu procesoare pe 64 biti;
- să aibă posibilitatea definirii de indecși pentru accesarea rapidă a datelor;
- să ofere posibilitatea de a face salvare și restaurare automată de date;
- să includă capabilități de căutare complexă la nivel de text, folosind indecși specializați și efectuarea rapidă a cautarilor în acest tip de date;
- să permită în mod nativ stocarea și gestiunea de structuri de date de tip XML;
- să ofere suport pentru proceduri stocate și triggeri;
- să ofere suport pentru tranzacții;

- să permită execuția operațiilor de tip SELECT, INSERT, UPDATE, DELETE;
- să permită definirea de tabele de tip index sau indecși de tip „cluster” pentru acces rapid la anumite tabele;
- să ofere suport pentru replicarea datelor între două instanțe ale bazei de date;
- să permită restricționarea accesului la nivelul obiectelor bazei de date;
- să ofere mecanisme native de restricționare a accesului utilizatorilor;
- să permită restaurarea în regim de lucru online prin intermediul instrumentelor de backup proprii;
- să permită efectuarea de backup automat într-o forma unitară, centralizată și ușor de administrat;
- 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; baza de date va fi configurată în regim de înaltă disponibilitate;
- să ofere securitate tranzacțională în cazul apariției unor erori hardware sau software în clusterul de bază de date;
- să ofere funcționalități native de extragere/preluare a datelor din diferite surse de date (cel putin: a) baze de date - SQL Server, Oracle, DB2 sau echivalent, b) fișiere csv, Excel sau echivalent, c) Web services), realizarea de filtrări, agregări și diferite alte transformări asupra datelor și în final stocarea datelor în tabelele bazei de date.

Oferta va include licențierea a minim 32 de nuclee pentru soluția de baze de date ofertată, în regim de înaltă disponibilitate. Achizitorul nu va achiziționa nici o licență suplimentară pe durata derulării contractului necesare funcționării optime a componentei. Oferta va include asumarea cerinței de către Ofertant.

Soluția ofertată va include suport pe o perioadă de minim 60 de luni inclusiv acces la centrul de suport al producătorului pentru soluții tehnice sau actualizări software când este cazul. Este responsabilitatea Prestatorului de a achiziționa acest tip de servicii de la producător sau de la un distribuitor autorizat de acesta, pentru toată perioada de garanție ofertată și de a le transfera Autorității Contractante odată cu livrarea și punerea în funcțiune a soluției software. Detaliile privind contul Achizitorului la producător/distribuitor autorizat vor fi furnizate la livrarea și punerea în funcțiune a soluției software. Instalarea actualizărilor, precum și deschiderea de tichete de suport sau orice alte activități legate de mentenanța și garanția soluției software vor fi asigurate de către prestator pe toată durata perioadei de garanție și suport ofertate.

3.2.5.5 Componenta de consolidare date data warehouse, analiza raportare

Componenta de consolidare date, analiză și raportare va asigura preluarea și consolidarea datelor din diverse surse de date (interne și externe), generarea de rapoarte complexe și va permite construirea, configurarea și generarea de analize avansate/rapoarte dinamice pe baza datelor preluate și consolidate și respectiv prezentarea în diferite șabloane și formate pentru utilizări viitoare. În afara rapoartelor “standard” (rapoarte predefinite, dezvoltate pe baza unor cerințe clare detaliate pe durata derulării implementării) prin intermediul modulului se vor putea realiza, de către anumiți utilizatori, rapoarte de tipul “ad-hoc” pentru identificarea și analizarea anumitor situații punctuale; rapoartele ad-hoc se vor putea transforma în rapoarte “standard”, printr-o operațiune de “publicare”, fără a fi nevoie de redezvoltarea lor.

Componenta de analiză și raportare de raportare se va dezvolta pe baza unei componente de tipul SGBD **Depozit de Date (Data Warehouse)** care va prelua și va consolida datele din modulele operaționale conform cerintelor componentei de sincronizare – migrare date.

Componenta DW trebuie să ofere urmatoarele functionalități:

- Raportare consolidată și managementul depozitelor de date:
  - Index secundar la nivel de coloane care să comprime și să stocheze datele în memorie pentru access rapid la datele din Data Warehouse;
  - Afișarea rapoartelor într-un mod interactiv, astfel încât utilizatorii sî poată urmări evoluția în timp a anumitor evenimente, să poată efectua filtrări asupra datelor prezentate;
  - Depozit de date relațional și instrumente OLAP: componenta să ofere în mod nativ soluții OLAP și data warehouse;
  - Să permită lucrul în mod partiționat pentru încărcarea rapidă și mentenanță ușoară a tabelelor foarte mari;
  - Baze de date multidimensionale native: stocarea datelor într-un cub cu mai multe dimensiuni, în vederea interogării mai ușoare a datelor și construirii de rapoarte și analize relevante;
  - Functionalități de data mining: functionalități pentru construirea de modele analitice complexe precum și integrarea acestor modele cu operațiile de business;
  - Să permită exportarea datelor minim în format Excel, fișiere CSV, o altă bază de date, fișiere XML;
  - Să permită exportul datelor în documente tip PDF;
  - Să permită exportul datelor într-un feed de date;
  - Să ofere capabilități de colaborare;
  - Să permită utilizatorilor să creeze soluții self-service BI pe seturi de date mari;
  - Să permită generarea de alerte în cazul apariției unor evenimente din baza de date;
- Gestionare facilă a obiectelor bazelor de date:
  - Instrumente de dezvoltare a obiectelor din baza de date, atât relaționale cât și multidimensionale
  - Unelte pentru administrarea bazelor de date și a proceselor uzuale care se execută asupra bazelor de date precum și a rapoartelor
  - Posibilitatea de definire și gestionare a obiectelor bazei de date (tabele, indecsi, proceduri stocate, triggere) direct din instrumentele folosite de dezvoltatori pentru scrierea aplicațiilor
  - Posibilitatea de a oferi compresia datelor
- Perfomanțe ridicate ale sistemului de baze de date:
  - Criptarea transparentă a datelor, a fișierelor de date și a fișierelor jurnal fără să fie necesară modificarea aplicației. Funcționalitatile de criptare sunt necesare pentru îndeplinirea cerințelor și respectarea reglementărilor generale cu privire la confidențialitatea datelor. Criptarea trebuie să ofere inclusiv instrumente de căutare în datele criptate utilizând sisteme de regăsire într-un interval sau căutarea parțială, fără modificarea aplicațiilor existente
  - Auditarea operațiilor: auditarea trebuie să includă informații despre momentul în care au fost citite/accesate datele, în plus față de orice modificare a datelor. Produsul trebuie să ofere caracteristici precum configurarea îmbunătățită și managementul auditurilor în server. Produsul să definească specificațiile de audit în fiecare baza de date, astfel încât configurația auditului să poată fi adaptată pentru diversele baze de date

- Posibilitatea de a filtra evenimentele auditate; posibilitatea de a customiza operația de audit în funcție de evenimentele din baza de date
- Posibilitatea adăugării online a resurselor de memorie mașinilor fizice care găzduiesc bazele de date pentru scalarea acestora la cerere
- Colectarea datelor de performanță: facilități de optimizare și depanare a performanței server-ului de baze de date, pentru a furniza administratorilor o perspectivă interactivă cu privire la performanță.
- Sistem de monitorizare extins al evenimentelor: sistem general de tratare a evenimentelor la nivel de server prin captarea, filtrarea și reglarea evenimentelor generate de procesele de server. Evenimentele trebuie să poată fi captate și exportate în diferite formate de ieșire, inclusiv Event Tracing for Windows (ETW), pentru corelarea cu aplicațiile sistemului de operare și ale bazelor de date, permițând astfel o monitorizare completă a sistemului.
- Posibilitatea comprimării rapide a backup-urilor bazelor de date.
- Posibilitatea definirii limitelor și priorităților resurselor pentru diferite sarcini (workloads), și obținerea unei perfomante crescute în executarea acestora. Modul de alocare a resurselor fizice ale server-ului trebuie să poată fi controlat de către administratorul de sistem.
- Asigurarea continuității activității organizației: duplicarea datelor prin tehnologii de tip data mirorring

- Implementarea structurilor de date complexe:
  - Posibilitatea nativă de modelare a structurilor de date de tip arbore: metode încorporate pentru crearea și operarea pe noduri ierarhice
  - Posibilitatea stocării datelor binare mari, precum documente și imagini, ca parte integrantă a bazei de date, păstrând în același timp consecvența tranzacțională
  - Căutare complexă la nivel de text, folosind indecși specializați; efectuarea rapidă a căutarilor în acest tip de date
  - Managementul performant al coloanelor cu valori rare: modalități eficiente pentru administrarea spațiilor necompletate dintr-o baza de date relațională, astfel încât valorile de tip NULL să nu consume spațiu fizic
  - Posibilitatea crearii de tabele cu mai mult de 1.024 de coloane
  - Utilizarea unei platforme avansate pentru dezvoltarea de aplicații complexe de procesare a evenimentelor
  - Posibilitatea de dezvoltarea de aplicații bazate pe evenimente folosind platforma de procesare a evenimentelor pentru a se permite interogari continue și latenta de milisecunde
  - Posibilitatea de dezvoltare de aplicații prin care să scadă costul de extragere, analiza și corelare a datelor permițând monitorizarea și managementul datelor în timp real
- Componenta trebuie să ofere posibilitatea instalării, fără costuri adiționale, a unui număr nelimitat de baze de date distincte în mașini virtuale alocate serverului licențiat
- Solutia nu trebuie să impună nicio restricție din punct de vedere licențiere aferentă numărului de utilizatori ce se pot conecta la SGBD
- Disponibilitate ridicată și mentenanță:
  - Posibilitatea efectuării backup-ului în multiple fișiere simultan pentru a putea efectua operația pe discuri diferite în paralel;
  - Posibilitatea efectuării backup-ului direct într-o soluție de cloud public, respectand normele de securitate;

- Posibilitatea de a crea, modifica, șterge index-ul concurent cu activitățile utilizatorilor;
- Posibilitatea de a crea un snapshot al bazei de date;
- Modificarea schemei online.

Componenta va permite rularea de rapoarte atât de către utilizatori, cât și în mod neasistat, programat la un anumit moment. În urma obținerii rezultatelor executării rapoartelor neasistate, acestea vor putea fi automat transmise către anumiți utilizatori (specificați pentru fiecare raport în parte).

Componenta de raportare și analiză avansata trebuie să ofere minim următoarele funcționalități:

- Clasificarea rapoartelor și analizelor pe diferite categorii. Sistemul trebuie să poată gestiona accesul grupurilor de utilizatori și sau utilizatorilor individual la anumite categorii de rapoarte.
- Sa permita configurare de tip „point-and-click“.
- Sa ofere funcționalități de navigare ghidată pentru utilizatorii finali, cu posibilități multiple de navigare dintr-un anumit punct, atât pentru rapoarte cât și pentru grafice;
- Sa permita combinarea rezultatelor obținute din surse de date diferite la momentul interogării, astfel încât setul de date rezultat să fie unitar;
- Sa permita organizarea datelor în format tabelar al informațiilor afișate;
- Sa permita crearea de rapoarte utilizand un editor vizual de interogari, dar si scrierea manuala a interogarilor SQL complexe;
- Sa permita salvarea interogarilor SQL ca notite pentru utilizare ulterioara.
- Sa permita definirea de tablouri de bord și includerea rapoartelor/graficelor în acestea, pentru toți utilizatorii finali, în funcție de drepturile fiecăruia;
- Sa permita modificarea tablourilor de bord sau a rapoartelor, posibilitatea de a salva, organiza, administra și partaja rapoartele cu alți utilizatori;
- Sa permita parametrizarea tablourilor de bord si a datelor afisate in functie de diverse criterii relevante;
- Accesul la informație să fie realizat printr-un nivel de metadate care va ascunde utilizatorilor finali complexitatea structurilor fizice de date;
- Sa permita crearea de coloane in cadrul tabelelor virtuale, bazate pe formule de calcul;
- Sa permita crerea de modele virtuale de date pe baza unei interogari; sa permita utilizarea unui model virtual ca sursa de date pentru interogari noi;
- Sa permita includerea dashboard-urilor in alte aplicatii;
- Sa includa un mecanism de caching al datelor utilizate frecvent, pentru accelerarea timpului de livrare al rapoartelor;
- Sa permita configurare cache-ului pentru o anumita interogare, pentru accelerarea livrarii rapoartelor de utilizeaza date care nu se schimba frecvent;
- Sa includa un mecanism de analiza automata a datelor din cadrul unei tabele, cu propunerea automata a celor mai relevante vizualizari pentru datele din tabela respectiva (ex: histograme de valori, harti, linii de trend, agregari etc.)
- Utilizatorii își vor putea crea singuri propriile rapoarte (analize ad-hoc) fără să fie nevoiți să cunoască structurile fizice de date pe care le accesează;

- Se permita restrictionarea accesului la date in functie de utilizator si grup de utilizatori. Restrictionare accesului trebuie sa poata fi facut la nivelul unei surse de date, tabela sau anumite randuri si coloane dintr-o tabela;
- Sa permita restrictionarea accesului la interogari, tablouri de bord si rapoarte, atat la nivel de utilizator, cat la nivel de grup de utilizatori;
- Să ofere o interfață de administrare atât a drepturilor de acces la diferite zone, cât și a drepturilor de acces pe diferite tipuri de acțiuni, inclusiv în ceea ce privește posibilitatea de export a datelor generate într-un raport;
- Sa permita auditarea actiunilor utilizatorilor, inclusiv auditarea accesului la date, precum si vizualizarea informatiilor de audit din cadrul zonei de administrare;
- Sa permita accesarea datelor din cadrul platformelor relaționale, multidimensionale si foi de calcul;
- Interacțiunea utilizatorilor finali cu aplicația trebuie să se poată face într-o interfață de tip web, fără a necesita instalarea de componente software suplimentare pe calculatoarele utilizatorilor;
- Să permită afisarea datelor atat sub tabelara cat si grafica: bar chart, stacked bar chart, histogram, line chart, gauge, donut, waterfall, pivot table, funnel chart, pie chart, scatter plot, map;
- Să permită definirea de borne personalizate cu denumire personalizata si data calendaristica, pentru a marca diverse evenimente importante in timp. Bornele vor fi afisate automat in cadrul vizualizarilor din tabloul de bord ce afiseaza informatii legate de data/timp;
- Să ofere capabilitati de write-back pentru a putea introduce sau modifica anumite date de interes;
- Să ofere capabilități de drill-down (navigare în adâncime) pe diferite nivele de agregate;
- Să permită acces la surse de date multiple, în mod transparent pentru utilizatorul final;
- Să ofere utilizatorilor posibilitatea agregărilor personalizate pe nivel, atât în baza de date, cât și în aplicația de analiză și raportare;
- Să dispună de mecanisme de alertare pentru utilizatorii finali;
- Să ofere utilizatorilor finali posibilitatea subscrierii la alertele definite;
- Să nu necesite replicarea datelor pe un server separat, ci să folosească capabilitățile bazelor de date sursa.
- Mediul de lucru pentru utilizatorii finali sau alți dezvoltatori de rapoarte/analize să fie în mediu web pur, interacțiunea cu sistemul să se realizeze prin operațiuni de tip „point and click” și „drag and drop” (să nu necesite cunoștințe de programare din partea utilizatorilor);
- Sa permita filtrare consecutivă a segmentelor de date analizate („slice & dice”);
- Să permită tuturor utilizatorilor crearea sau modificarea de rapoarte, analize ad-hoc și tablouri de bord, acordarea drepturilor specifice (consultare, creare de obiecte etc.) urmând a fi făcută de către administratori;
- Sa permita definite de sabloane de filtre ce pot fi aplicate de utilizator asupra rezultatelor unei interogari
- Sa permita definirea de sabloane de agregari ce pot fi aplicate de utilizator asupra rezultatelor unei interogari
- Sa suporte unul din standardele SAML, JWT sau OAuth pentru integrarea cu platforme de Single Sign-On.

- Să permită rularea rapoartelor utilizând dispozitive mobile

Componenta trebuie sa includa nativ un motor distribuit pentru procesare analitică de volume mari de date în memorie ale cărui funcționalități să permita:

- Acces la datele din cluster prin interogare de tip standard SQL
- Librarie de Machine Learning care să includă cel puțin:
    - Algoritmi de clasificare, regresie, clustering și collaborative filtering
    - Analiza și caracterizare seturilor de date (featurization): extragerea (feature extraction), transformarea, selecția și reducerea dimensiunilor seturilor de date
    - Posibilitatea de a construi fluxuri de procesare, transformare si machine learning
    - Capabilitati pentru construcția și tuning-ul fluxurilor de machine learning
    - Persistenta: salvare și încărcare algoritmi, modele și fluxuri
    - AutoML
- Procesare date în limbaje multiple, minim Java, Scala, Python si R
- Procesare distribuită de date pe bază de cache în memoria fiecărui nod
- Capabilități de streaming
- Reprezentare date tip graf

Componenta trebuie sa includa nativ un motor distribuit de interogare federata a datelor, pentru analiza simultana a datelor din mai multe surse de date, care sa permita cel putin:

- conectarea mai multor surse de date, cel putin baze de date, fisiere, cozi de mesaje
- utilizarea nativa a bazei de date structurate si a bazei de date nestructurate din cadrul platformei Big Data
- suport complet pentru standardul SQL
- posibilitatea de a efectua operatii de tip join pe tabele apartinand unor surse diferite
- drivere (ex. JDBC, ODBC) pentru conectarea sistemelor externe
- rularea in mod distribuit, pentru a putea efectua operatii pe seturi mari de date
- conectivitate cu o gama variata de sisteme de baze de date relationale, columnare, NoSQL, BigData, CSV, cozi de mesaje si multe altele
- capabilitati de analiza avansata a datelor federate, cel putin utilizand functii pentru: sumarizare, machine learning, date spatiale, JSON
- creara de view-uri simple si view-uri materializate
- vizualizarea planului de executie pentru o interogare SQL
- utilizarea unui instrument vizual de monitorizare a interogarilor efectuate, cu afisarea planului de executie si a timpului consumat

Componenta trebuie sa includa nativ un instrument colaborativ pentru elaborarea proceselor de analiza avansata si rularea experimentelor de tip data science, care sa permita:

- realizarea de analize specifice asupra datelor existente, cu posibilitati de vizualizare sub diferite forme grafice: bar chart, line chart, distributie de valori, matrice de corelare a variabilelor, scatter plot, box plot, heatmap, histograme de valori, pie chart, 3D, grafice animate pentru afisarea progresului in timp

- publicarea rezultatelor obtinute ca aplicatii web.

Va fi considerată dezvoltarea a minim 20 rapoarte/ indicatori de control în componenta de analiză ofertată (7 rapoarte de complexitate mică, dezvoltate pe baza unei singure tabele, 10 rapoarte de complexitate medie, devoltate pe baza a 2-3 tabele și 3 rapoarte de complexitate mare dezvoltate pe baza a mai multe tabele și/sau multiple criterii de selecție/filtrare) suplimentare față de cele prevăzute în componenta de raportare specifică SIAMC 2.0, respectiv a **Programului cadru anual de acțiuni al Inspecției Muncii** la nivel national, **Programului propriu anual de acțiuni al inspectoratului** și a **Planului Anual de Control** la nivel de ITM, precum și funcționalităților aferente **Evaluării de risc**, care vor fi definite pe parcursul fazei de analiză/colectare a cerințelor.

La nivelul Componentei de realizare a rapoartelor si dashboardurilor vor fi disponibile toate datele/tabelele existente la nivelul Componentei Depozit de Date, chiar dăcă acestea nu vor fi utilizate la dezvoltarea rapoartelor mentionate in prezentul proiect tehnic.

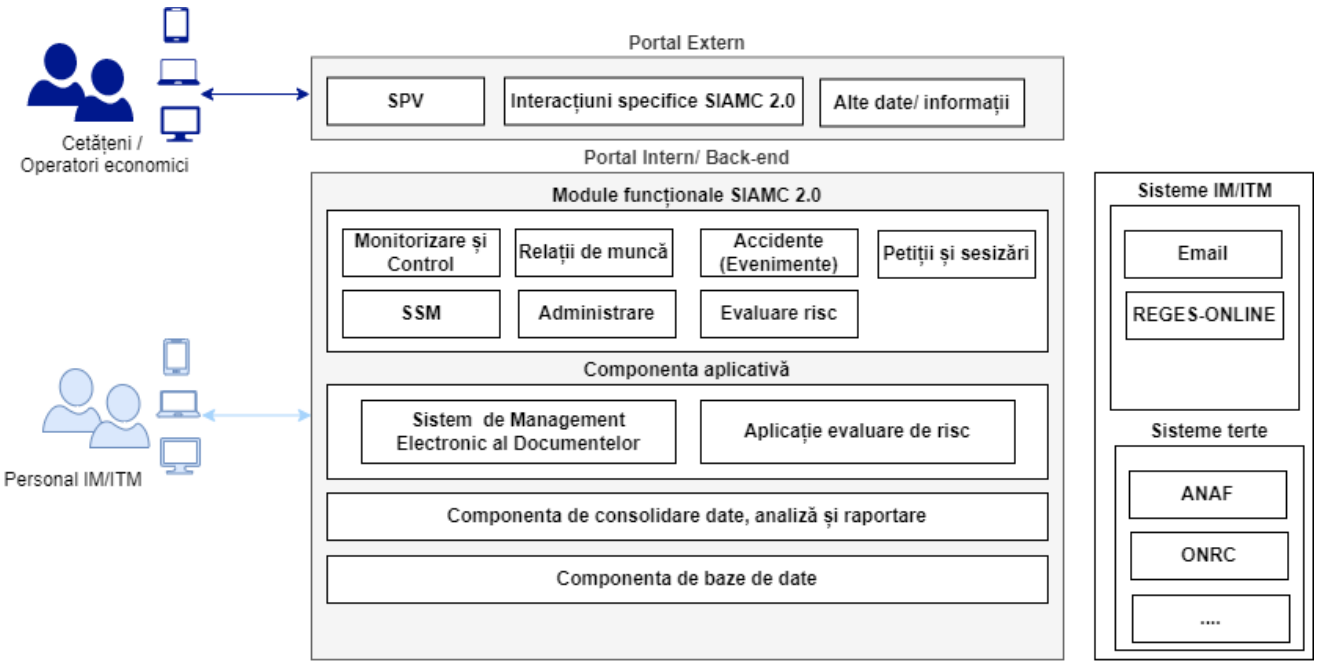
Oferta va include licențierea a minim 32 de nuclee pentru soluția de consolidare date, analiză și raportare, în regim de înaltă disponibilitate, fără a limita numărul de utilizatori ce pot define sau accesa rapoarte/ indicatori sau planurile de acțiuni. Achizitorul nu va achiziționa nici o licență suplimentară pe durata derulării contractului necesare funcționării optime a componentei. Oferta va include asumarea cerinței de către Ofertant.

Soluția ofertată va include suport pe o perioadă de minim 60 de luni inclusiv acces la centrul de suport al producătorului pentru soluții tehnice sau actualizări software când este cazul. Este responsabilitatea Prestatorului de a achiziționa acest tip de servicii de la producător sau de la un distribuitor autorizat de acesta, pentru toată perioada de garanție ofertată și de a le transfera Autorității Contractante odată cu livrarea și punerea în funcțiune a soluției software. Detaliile privind contul Achizitorului la producător/distribuitor autorizat vor fi furnizate la livrarea și punerea în funcțiune a soluției software. Instalarea actualizărilor, precum și deschiderea de tichete de suport sau orice alte activități legate de mentenanța și garanția soluției software vor fi asigurate de către prestator pe toată durata perioadei de garanție și suport ofertate.

3.2.5.6 Componenta aplicativă

Componenta aplicativă va fi realizată de o manieră intergrată, atât la nivelul fluxurilor de date cât și a accesului la date și funcționlaități, trecerea între modulele componente ale sistemului trebuind să fie transparentă pentru utilizator.

Componenta aplicativă va include cel puțin un subsitem de management electronic al documentelor și un subsitem de evaluare risc cu funcționaități specifie de colectare date, procesare, alertare.



Arhitectura generală SIAMC 2.0

3.2.5.6.1 Sistemul de Management Electronic al Documentelor (SMED)

3.2.5.6.1.1 Considerente generale

Sistemul SMED va oferi doua tipuri de functionalitati:

- Functionalitati specifice SIAMC 2.0 (fluxurile de lucru si functionalitatile specifice precum Monitorizare si control, RM, SSM, Accidente/Evenimente)
- Functionalitati generice pentru gestiunea oricaror documente si fluxuri de lucru din cadrul IM/ITM

SMED va permite organizarea accesului și funcționalităților astfel încât să asigure cerințele arhitecturale pentru o zona DMZ și una de back-end sub forma:

- Portal Extern pentru operatori economici si mediul de afaceri
- Portal Intern pentru personalul IM/ITM

Livrarea SMED (Sistemului de management electronic al documentelor) va include și servicii de implementare a unor module suport, minim:

- Registratură electronica pentru toate activitățile IM, și toate canalele de intrare/ ieșire documente, inclusiv gestionarea 68numerelor de înregistrare generate din activitățile de Monitorizare, control, etc. ce se vor derula în viitorul sistem informatic
- Implementarea de registre dedicate gestiunii formularelor cu regim special
- Implementarea nomenclatoarelor arhivistice identice la nivelul IM și a tuturor ispectoratelor teritoriale de muncă, cu termene de păstrare identice
- Definirea de fluxuri de lucru pentru procese standard, cum ar fi cele referitoare la managementul ceririlor de concedii sau la managementul achizițiilor
- Definirea structurii organizatorice a IM și ITM-uri precum și implementarea acesteia în cadrul sistemului de managent electronic al documentelor
- Implementarea conceptului de Spațiu Privat Virtual a fiecărui utilizator extern, persoană fizică sau juridică, spațiu în care IM/ITM pot transmite comunicări oficiale, semnate electronic, cărora

le vor fi associate minim informații legate de tip, data emiterii, emitent, data arhivării (ulterior terecerii în arhiva operațională a sistemului va face indisponibilă comunicarea nu va mai putea fi accesată de PF/PJ vizată). Persoanele fizice sau juridice, în contul propriu, vor putea consulta comunicările, le vor putea descărca, vor putea filtra lista proprie după diverse criterii și acolo unde va fi cazul vor putea iniția fluxuri de răspuns/ contestare a comunicărilor respective direct din SPV.

De asemenea SMED va trebui să permită definirea de fluxuri ad-hoc și să ofere o interfață grafică de modelare și configurare a acestor fluxuri, tip BPM.

Din punct de vedere logic SMED va include cel putin urmatoarele module nativ/puternic integrate:

- Fluxuri de lucru și documente;
- Registratură electronică;
- Arhivare electronică;
- Captură documente;
- Management arhivă fizică de documente.

Prin componenta aplicativă SMED se va genera întregul flux aferent fiecărei activități desfășurate în cadrul ITM si IM, cum ar fi de exemplu: fluxurile aferente controlului, evenimentelor, petițiilor, autorizărilor, respectiv cele de înregistrare, analiză, evaluare, planificare, repartizare, inițiere, efectuare activitati, astfel cum vor fi acestea detaliate în faza de proiectare și dezvoltare a sistemului. Sistemul va genera inclusiv o fisa a unității (dashboard) care va cuprinde toate informațiile, notificările și alertele cu privire la angajator si la activitatile desfasurate de acesta.

SMED va rula în regim de înaltă disponibilitate, fără a limita numărul de utilizatori ce pot administra sau utiliza sistemul sau oricare din modulele acestuia, atât interni cât și externi. Achizitorul nu va achiziționa nici o licență suplimentară pe durata derulării contractului necesare funcționării optime a componentei. Oferta va include asumarea cerinței de către Ofertant.

Soluția ofertată va include suport pe o perioadă de minim 60 de luni inclusiv acces la centrul de suport al producătorului pentru soluții tehnice sau actualizări software când este cazul. Este responsabilitatea Prestatorului de a achiziționa acest tip de servicii de la producător sau de la un distribuitor autorizat de acesta, pentru toată perioada de garanție ofertată și de a le transfera Autorității Contractante odată cu livrarea și punerea în funcțiune a soluției software. Detaliile privind contul Achizitorului la producător/distribuitor autorizat vor fi furnizate la livrarea și punerea în funcțiune a soluției software. Instalarea actualizărilor, precum și deschiderea de tichete de suport sau orice alte activități legate de mentenanța și garanția soluției software vor fi asigurate de către prestator pe toată durata perioadei de garanție și suport ofertate.

3.2.5.6.1.2 Portal extern

Portalul web extern dedicat operatorilor economici si cetățenilor va fi structurat pe două zone cu acces diferențiat:

- Zona publică, accesibilă oricărui utilizator, fără autentificare;
- Zona privată, accesibilă utilizatorilor care s-au înregistrat și înrolat în platformă (au un cont de acces) structurată sub forma unui spațiu virtual privat care va conține, dar fără a avea caracter exhaustiv, următoarele:
    - Datele contului cu următoarele secțiuni: informații despre utilizator, inclusiv poza, Adresa de corespondenta, Adresa de domiciliu, Informații act de identitate, Activitatea mea (care va oferi un sumar al tuturor solicitărilor depuse si al documentelor utilizatorului). Fiecare secțiune va avea link-uri către detaliile corespunzătoare.

- Datele Utilizatorului cu următoarele secțiuni: Informații personale, Act de identitate, Adresa domiciliu, Adresa de corespondenta. In aceasta secțiune utilizatorul va avea posibilitatea editării tuturor informațiilor
- Solicitările mele cu următoarele secțiuni: zona de filtrare in care utilizatorul va putea filtra informațiile după tipul solicitării, Stare solicitare, Data (interval de la – pana la). Lista de solicitări va prezenta informații sumare despre fiecare solicitare precum: Data, Nr înregistrare, Stare, documente asociate (cu posibilitatea de descărcare), link către solicitare
- Documentele mele. Documentele vor fi structurare in funcție de tipul lor, astfel: documente generale, asociate profilului utilizatorului si care vor putea fi folosite in cadrul accesării serviciilor (Carte de identitate, Certificat de înregistrare etc) si documente specifice fiecărui tip de serviciu accesat. Aceasta secțiune va fi editabila permițând utilizatorului sa gestioneze lista cu Documentele sale.
- Companiile mele. Permite utilizatorului sa creeze si sa administreze persoanele juridice (companiile) pe care le reprezintă: adăugare\modificare companie si împuterniciți, asociere\dezasociere utilizatori din platforma care au dreptul sa inițieze solicitări pentru compania respectiva, gestiune puncte de lucru si documente Persoana juridica. Mecanismul de aprobare va fi implementat astfel încât persoana care introduce compania in baza de date va avea drepturi depline (pe baza împuternicirii încărcate) si va putea asocia/dezasocia alți utilizatori suplimentari care pot administra solicitările si documentele companiei.
- Notificările mele este o secțiune in care se vor centraliza toate notificările primite de utilizator cu posibilitate filtrării acestora după categorie (mail, sms, aplicație) si status (citite/necitite)

- Zona de servicii disponibile operatorului economic sau cetățeanului, dedicata accesării serviciilor de către un operator economic sau cetățean va oferi cel puțin următoarele funcționalități:
  - Va permite configurarea modului de prezentare fluxurilor de lucru si serviciilor furnizate de către IM/ITM într-o manieră structurată atât pe categorii de problematici, cât şi pe tipuri de servicii furnizate de către diferite compartimente din cadrul instituției, astfel încât utilizatorul să poată regăsi ușor problematica dorită sau formularul necesar.
  - Pentru fiecare flux de lucru si serviciu furnizat de IM/ITM se va prezenta o secțiune ce va include o descriere a acestuia, documentele necesare pentru prestare, compartimentul din IM/ITM care prestează serviciul respectiv, programul de prestare a serviciului, costuri și durata serviciului, cât și o secțiune pentru solicitarea serviciului în formă electronică, pentru cele disponibile. Definirea serviciilor în platformă se va putea realiza de către funcționarii din IM/ITM printr-o interfață intuitivă și concepută specific pentru acest scop.
  - Pentru fluxurile si serviciile ce vor fi furnizate în variantă electronică, Portalul va asigura preluarea solicitărilor și direcționarea automată către componenta din back-end în vederea înregistrării și procesării cererilor.
  - Realizarea unui flux de lucru sau serviciu în formă electronică va presupune parcurgerea de către utilizator a unei succesiuni de activități asistate de Portal. Serviciile electronice vor fi centrate pe activități digitale şi pe finalitatea acestora și cat mai puțin posibil pe formulare care să replice formularele off-line existente în cazul interacțiunii fizice.
  - Fiecare flux de lucru sau serviciu electronic disponibil în Portal va consta într-o succesiune de activități particularizate, configurate în etapa de implementare a sistemului conform reglementărilor şi modului de organizare al instituției.

- Pentru serviciile electronice fără autentificare, transmiterea oricărui formular web completat de utilizator va fi precedată de verificarea prin cod Captcha.
- Activitățile care compun un serviciu electronic reprezintă o succesiune de pași care pot include:
  - secțiuni de informare
  - secțiuni care conțin formulare web care trebuie completate, eventual cu atașarea de fișiere (fotografii, documente scanate)
  - ecrane de vizualizare a unor documente generate automat de către Portal in baza informațiilor furnizate pana la acel moment
- Formularele aferente serviciilor electronice vor fi realizate in tehnologie web si vor putea fi completate de utilizator direct din browser, fără a fi necesara instalarea de componente software suplimentare.
- Formularele web care compun serviciile electronice vor include controale de culegere a informației de tip text simplu, text mult linie, lista de selecție valori dintr-un nomenclator, bifa (checkbox).
- Formularele web vor putea realiza validări ale datelor introduse de utilizator, pentru verificarea respectării unor constrângeri referitoare la lungimea minima sau maxima a textului, la limite ale valorilor numerice sau ale datelor calendaristice.
- Formularele vor putea ascunde sau afișa condiționat texte informative sau câmpuri de editare in funcție de valorile introduse de utilizator in câmpuri anterioare ale aceluiași formular web sau ale unuia anterior.
- Formularele web completate de utilizator vor fi interpretate in timp real de sistem, care va indica utilizatorului următoarea activitate necesara in vederea finalizării demersului dorit activitate care poate include:
  - completarea altui formular;
  - atașarea de documente;
  - efectuarea unei plăti electronice.

Sistemul va permite configurarea in cadrul unui serviciu electronic a unor reguli referitoare la obligativitatea atașării anumitor tipuri de documente (de exemplu documentul de identitate al titularului etc.). Regulile vor fi dependente de tipul de demers (serviciu electronic) si de opțiunile selectate de către operatorul economic sau cetățean in cadrul formularului web (se vor putea solicita documente diferite in funcție de situația concreta a solicitantului, rezultata din informațiile introduse/selectate in cadrul formularului web). Cel puțin următoarele validări vor fi disponibile:

- Document cu semnătura electronica
- Dimensiune Document

Pentru utilizatorii autentificați, sistemul va permite extragerea automata din formularele web completate de catre operatorul economic sau cetățean a unor informații structurate (de exemplu Nume, CNP, adresa, reprezentant legal) si va oferi opțiunea salvării acestora atașat profilului utilizatorului respectiv. In procesul de completare a formularelor web, sistemul va inițializa formularul (sau câmpuri ale acestuia) cu unele dintre informațiile structurate salvate in cadrul profilului utilizatorului. In mod similar, sistemul va permite încărcarea documentelor atașate într-o ,,biblioteca" de documente personale ale utilizatorului, de unde acesta le va putea ulterior selecta si atașa unor formulare web, aferent unor solicitări de servicii specifice.

Utilizatorii autentificați vor avea acces si vor putea vizualiza in mod organizat istoricul solicitărilor trimise către instituție, din secțiunea „Solicitările mele” din cadrul Profilului utilizatorului. In cadrul unei

solicitări se vor putea vizualiza, cronologic, toate etapele comunicării intre utilizator si instituție si se va putea vizualiza stadiul rezolvării fiecărei solicitări in parte.

Pentru fiecare cerere va exista posibilitatea configurării următoarelor secțiuni:

- Secțiune sumar cerere care prezinta cronologic stările prin care a trecut cererea cu evidențierea stării curente si a stărilor viitoare
- Detalii solicitant; in momentul depunerii unei cereri noi, aceasta secțiune va apărea expandata si va prelua toate informațiile existente in profilul utilizatorului. Daca cererea este intr-un alt stadiu decât cel de depunere aceasta secțiune va apărea colapsata (cu posibilitatea expandării) si va afișa doar detaliile principale ale solicitantului (nume si CNP/CUI)
- Detalii cerere care va cuprinde formularul cererii si orice alte informații necesare
- Documente depuse de cetățean. In aceasta secțiune se vor gestiona documentele depuse de cetățean. Daca sunt cerute clarificări pe parcursul fluxului de rezolvare, fiecare transa de documente depuse va fi evidențiată separat, cu afișoarea numărului de înregistrare.
- Documente finale: documentele emise de instituție
- Orice alta informație cu privire la interacțiunea operatorului economic sau a cetățeanului cu IM/ITM

In cazurile in care nu este posibila automatizarea completa a serviciului electronic (adică furnizarea serviciului electronic strict in baza informațiilor completate de către solicitant, fără a fi necesara intervenția unui operator uman), fluxul de execuție a serviciului solicitat va putea include si activități care vor fi efectuate off-line (manual) de către un operator uman (funcționar) - de exemplu: verificarea preliminara a completitudinii solicitării, determinarea cuantumului unei taxe pentru care sistemul nu dispune de reguli automate de calcul.

La finalizarea procesului aferent unei cereri de solicitare a unui serviciu, Portalul va genera un document electronic (pdf) care va cuprinde toate informațiile completate de către solicitant in formularele web aferente pașilor de proces deja urmați, document care va putea fi semnat electronic de către solicitant (daca instituția impune aceasta condiție) si transmis prin Portal. Generarea documentelor electronice in baza informațiilor structurate completate de către solicitant in formularele web trebuie sa fie bazata pe șabloane configurabile, in care vor putea fi incluse atât informații structurate culese din formularele aferente serviciului electronic cat si paragrafe formatate de text predefinit si informații referitoare la plățile efectuate in contextul respectivului demers, daca este cazul

Portalul pentru acces extern cetățean va permite funcționarea si ca aplicație pentru telefoane mobile inteligente (Android si iOS), tablete etc.

Pentru toate funcționalitățile platformei, disponibile pentru cetățeni, se vor defini, in timpul etapei de analiza si proiectare, comportamentul particularizat in funcție de specificul IM/ITM, pe dispozitivele telefon inteligent, tableta etc.

3.2.5.6.1.2.1 Portal intern

Portalul intern va asigura gestiunea integrata a activităților si documentelor realizate de către funcționarii IM/ITM, va fi disponibil tuturor angajaților și va oferi funcționalități privind gestiunea informațiilor si datelor, digitalizarea tuturor proceselor de administrare a documentelor, îmbunătățirea colaborării dintre angajații IM/ITM si ai instituțiilor din subordine în vederea rezolvării activitatilor specifice ale SIAMC 2.0, precum si automatizarea si digitalizarea fluxurilor de lucru.

Portalul intern va fi structurat astfel încât sa le permită angajaților IM/ITM accesul diferențiat, facil si intuitiv la toate funcționalitățile disponibile, ținând cont de structura organigramei.

Următoarele tipuri de funcționalități vor fi disponibile:

- Tablou de bord personalizat pentru fiecare utilizator, cu următoarele zone:
    - Zona operațională care va permite inițierea unui flux sau unei activitati noi, vizualizarea tuturor activitatilor, căutare si accesare a acestora cu acces limitat in funcție de organigrama.
    - Zona cu funcționalități dedicate fiecărui modul functional specific (Monitorizare si control, RM, SSM, Accidente, etc.)
    - Vedere Cetățean/Operator economic va prezenta o vedere integrata cu toate datele aferente unui cetățean sau unui operator economic (controale, RM, SSM, etc), date rezultate din interacțiunea acestuia cu IM/ITM sau preluate din alte sisteme/module
    - Notificări
    - Raportare
    - Administrativ, secțiune in care se vor organiza toate funcționalitățile de administrare a parametrilor de funcționare ai platformei
    - Cereri si solicitări pe care trebuie sa le rezolve fiecare angajat cu evidențiere coloristica a termenelor de soluționare
    - Link-uri rapide către diverse aplicații uzitate in mod regulat
    - Cereri externe in procesare/aprobare la mine: lista cu solicitările la care angajatul respectiv trebuie sa realizeze o activitate. Pe fiecare cerere va exista un buton care sa permită accesarea lucrării
    - Petiții si fluxuri ad-hoc in procesare/aprobare la mine
    - Activități interne in procesare/aprobare la mine
    - Arhiva activităților procesare/aprobare la mine

In cadrul portalului intern pentru IM/ITM se vor organiza meniurile astfel încât fiecare tip de serviciu sa aibă o secțiune dedicata cu toate informațiile necesare.

Meniurile si paginile vor fi personalizare specific pentru fiecare tip de utilizator in funcție de drepturile de acces acordate acestuia precum si de rolul din fiecare flux de lucru.

3.2.5.6.1.2.2 Fluxuri de lucru

În cadrul portalului intern vor fi disponibile următoarele tipuri de fluxuri:

- Fluxuri externe sau aferente interactiunii dintre IM/ITM si operatorii economici sau cetateni
- Fluxuri de lucru interne care țin de organizarea si funcționarea interna a IM/ITM
- Alte fluxuri administrative.

Sistemul va permite evidențierea vizuală a fiecărei categorii de fluxuri.

Sistemul va permite configurarea în cadrul unui flux electronic a unor reguli referitoare la obligativitatea atașării anumitor tipuri de documente sau introducerea unor anumite informatii la un anumit pas din flux, reguli ce vor fi definite într-o interfață vizuala si ușor de folosit de către un administrator de sistem.

Pentru a crea o experiență ușoara si ergonomica utilizatorilor aplicației, structura interfetelor in care se vor gestiona interactiunile dintre IM/ITM si operatorii economici (controale, transmitere documente cu privire la RM sau SSM, eliberare autorizatii de functionare, etc) vor avea, pe langa elementele specifice fiecarei tip de activitate, urmatoarele elemente generale (lista completă va fi stabilită în etapa de analiză cu Prestatorul):

- Detalii operator economic implicat in activitatea respectiva. Platforma va permite: fie selectarea acestuia dintr-o lista predefinita, in cazul in care acesta este deja in baza de date fie preluarea automata din ONRC, fie introducerea informațiilor acestuia.

- Detalii alte entitati implicate (angajati, lucratori, etc). Platforma va permite fie selectarea acestora dintr-o lista predefinita, in cazul in care acestia exista deja in baza de date fie introducerea informațiilor
- Detaliile dosarului activitatii sau fluxului electronic din platforma, unde inspectorul va putea consulta formularele web completate, documentele atasate sau generate, alte informatii.
- In cazul in care se solicita clarificări, documentele furnizate de operatorul economic vor fi afișate separat, evidențiind ca este un răspuns la solicitare
- Secțiune documente interne. Documentele generate in timpul rezolvării unei activitati sau flux electronic, care sunt interne si nu trebuie sa ajungă la operatorii economici vor fi gestionate într-o zona distincta din cadrul dosarului activitatii. Inspectorul IM/ITM va avea posibilitatea sa încarce, semneze si\sau sa înregistreze aceste documente. Platforma va pune la dispoziție instrumente de configurare si administrare prin care sa se poată configura comportamentul acesteia in funcție de fiacare situație (de exemplu sa nu permită la trecerea unui pas decât in momentul in care se încarcă un anumit tip de document sau decât in momentul in care documentul a fost semnat electronic de un anumit număr de persoane).
- Acolo unde va fi posibil documentele vor fi generate automat de sistem pe baza unui template configurabil de către utilizator.
- Secțiune documente adresate operatorului economic care va conține documentele furnizate acestuia ca răspuns la o solicitare sau ca rezultat al unui control, etc
- Zona de aprobare si navigare in flux: toate activitatile vor avea o zona in care se vor afișa toți pașii de elaborare, aprobare sau informare precum si utilizatorii responsabili pentru fiecare. Sistemul va permite definirea de fluxuri de lucru care presupun interactiunea atat intre angajatii IM/ITM cat si intre angajatii IM/ITM si operatorii economici.
- Sistemul va permite generarea unui raport de audit care prezinta toți pașii si informațiile aferente fiecărui pas (responsabil, acțiune, descriere)
- Sistemul va permite definirea de sarcini specifice pe fiecare pas al fluxului, sarcini care vor fi disponibile anumitor angajati ai IM/ITM sau operatorilor economici. Utilizatorul care este responsabil de pasul respectiv va putea introduce la fiecare sarcina data de rezolvare si persoana responsabila. De asemenea, sistemul va permite prezentarea unui set restrans de informatii anumitor utilizatori, pe un pas al fluxului de lucru.
- Sistemul va permite configurarea pentru fiecare flux de lucru sau activitate, dintr-o interfață grafica, a cel puțin următoarelor elemente:
    - Detaliile si descrierea activitatii.
    - Lista de documente de intrare necesare cu marcarea acestora ca obligatoriu/opțional, necesita semnătura electronica
    - Pașii fluxului si acțiunile necesare: încărcare document, semnare document, generare document, înregistrare document, introducere de informatii, validare de informatii, aprobare, etc.
- La finalizarea unei activitati sau a unui flux, sistemul va genera un document electronic (pdf) care va cuprinde toate informațiile completate în formularele web aferente pașilor de proces deja urmați, document care va putea fi fie semnat electronic de către inspector direct in sistem și transmis fie prin Portal, fie transmis prin e-mail, fie imprimat în cazul în care se dorește depunerea sa la ghișeu, fie salvat în spațiul privat virtual personal al utilizatorului (în cazul utilizatorilor autentificați). Generarea documentelor electronice în baza informațiilor structurate completate de către utilizatori în formularele web trebuie să fie bazată pe șabloane configurabile, în care vor putea fi incluse atât informații structurate culese din formularele aferente fluxului electronic cât și paragrafe formatate de text predefinit.

- Sistemul va permite configurarea unor termene maxime de soluționare pentru fiecare etapă a procesului precum si pentru un anumit pas. Sistemul va permite configurarea de notificări privind stadiul realizării unei etape din flux (soluționare, depășire, blocare, etc)
- Ulterior modificarii starii unei activitati, persoanele interesate vor fi notificate automat prin email despre stadiul procesării dosarului și vor putea vizualiza online stadiul acestuia.
- Sistemul va permite configurarea de noi activitati sau fluxuri electronice, fără a necesita operațiuni de recompilare a întregii platforme.
- Sistemul va furniza rapoarte statistice în timp real cu privire la timpul petrecut într-o anumită stare a fluxului sau a unei solicitări\activități, rata de conversie (numărul de activități finalizate), durata unei activități etc.

Fluxurile prezentate nu sunt limitative, acestea putând fi completate/modificate în funcție de cerințelele legislației în domeniul de competenta al inspectiei muncii, in vigoare la momentul dezvoltarii sistemului.

3.2.5.6.1.2.3 Automatizare procese

Portalul intern va oferi cel puțin următoarele instrumente de automatizare a activității inspectorilor IM/ITM:

- Generare automata de documente (de ex. generarea procesului verbal de control la finalizarea unui flux sau activitati de control)
- Înregistrare automata a documentelor in registre de intrare/ieșire (de ex. cand se genereaza procesul verbal aferent activitatii de control acesta sa poata fi inregistrat automat in registrul corespunzator)
- Adăugare dinamica a unor documente necesare daca acestea sunt deja emise de instituție pentru dosarul respectiv (de exemplu informatii sau documente care se preiau automat de la ANAF, la un anumit pas al fluxului, in functie de regulile si logica configurata)
- Generare automata de notificări cu posibilitatea configurări acestora in funcție de anumite reguli (de exemplu la incarcarea unui document sau la alocarea unei sarcini catre un angajat)
- Semnalizarea prin folosirea unor coduri de culori specifice a termenelor de finalizare/soluționare configurate pe fiecare activitate sau pas al fluxului
- Generare de borderouri si confirmări de primire pentru corespondenta fizica
- Pași de aprobare pe baza unor algoritmi predefiniți (de exemplu aprobarea contului unui operator economic pe baza răspunsului obținut in urma consultării un sistem terț)
- Integrare cu o căsuța de email pentru preluarea automata a mesajelor si inițierea unor activitati. Sistemul va permite selectarea fișierelor atașate mesajului electronic si preluarea acestora automat in cadrul solicitării deschise.

3.2.5.6.1.2.4 Instrumente contextuale

Portalul intern va beneficia de instrumente specifice care se vor putea activa din modulul de configurare conform fiecărui context:

- Semnătura electronica a documentelor. Orice utilizator al portalului intern va avea posibilitatea sa semneze documente direct in portalul intern, fără a fi nevoie sa le descarce. Portalul intern va oferi posibilitatea ca orice utilizator sa-si poată utiliza cel puțin certificatele de semnătură digital gestionate de STS. De asemenea aplicația trebuie sa permită semnarea automata cu un certificat de tip Sigiliu electronic, pentru documentele generate automat, fără intervenția umana
- Scanare documente: in momentul in care trebuie parcursa o activitate din flux care presupune încărcarea unui document (fie la ghișeu, fie in cadrul IM/ITM, pentru un flux intern, va exista posibilitatea sa se activeze integrarea cu un scaner. Aceasta funcționalitate va permite utilizatorului sa preia direct in aplicație documentul scanat.

- Captarea documentelor va fi adaptata la contextul de utilizare astfel: in portalul web documentele se vor putea incarca prin navigarea si selectarea unui document aflat pe calculator sau prin preluare automata de la un scaner, in aplicatia care ruleaza pe telefonul mobil va permite incarcarea de imagini din telefon, etc
- Integrare cu dispozitive de citire si recunoastere autoamata a cartilor de identitate
- Căutare avansata: sistemul va permite căutarea avansata după mai multe criterii: detalii angajator/angajat, detalii solicitare, adresa, date de contact, etc.
- Posibilitate configurare generare cod de bare sau cod QR pe orice document încărcat sau generat de aplicație.
- Posibilitate extragere date cetățean pe baza imaginii cărții de identitate prin procesare de tip OCR.

Portalul intern va avea integrata o harta de tip GIS care va permite:

- Vizualizarea informațiilor geografice (simbol specific) și a atributelor asociate (tooltip) pentru entitatile carora li se pot introduce elementele de geolocatie (de exemplu locul in care se desfasoara un control);
- Navigarea în hartă prin acțiuni de zoom in/out și navigare, utilizând butoane dedicate sau mouse;
- Inițierea de acțiuni direct de pe harta (cu preluarea automata a coordonatelor)
-

3.2.5.6.1.3 Modulul de arhivare electronica

Modulul de arhivare electronica a documentelor va îndeplini minim următarele cerințe:

- trebuie sa ofere un model de date in care continutul unui document si metadatele asociate formeaza un obiect de un anumit tip;
- trebuie sa ofere mecanisme de securitate bazate pe grupuri, roluri, useri, functii din organigrama. nu trebuie sa existe limitare privind numarul de grupuri ce poate fi definit la nivelul depozitului de documente. drepturile de securitate si permisiunile trebuie sa fie special proiectate astfel incat sa permita controlarea accesului utilizatorilor la documente si tipul drepturilor de acces;
- trebuie sa permita sincronizarea automata intre grupurile functionale din arhiva electronica si grupurile de utilizatori definite in sistemul de Active Directory;
- interfata de utilizare a sistemului trebuie sa permita utilizarea ei in mai multe limbi, cel putin: romana, engleza, franceza, germana, rusa. Fiecare utilizator sa isi poata selecta limba preferata in momentul autentificării în sistem (in fereastra de autentificare). dupa autentificare toate mesajele si elementele interfetei de utilizare vor fi prezentate in limba selectata de utilizator;
- trebuie sa poata oferi acces catre mai multe arhive individuale pentru acelasi utilizator, trebuie sa ofere posibilitatea desemnarii relatiei pe care o are fiecare utilizator in raport cu celelalte arhive gestionate, inclusiv rolul general pe care acel utilizator il are pentru fiecare astfel de arhiva (este administrator sau este utilizator normal);
- trebuie sa ofere de asemenea posibilitatea organizarii utilizatorilor in grupuri. un utilizator poate face parte din unul sau mai multe grupuri. permisiunile de securitate trebuie sa se asocieze cu grupurile de utilizatori (aplicandu-se tuturor utilizatorilor membri ai acelui grup la momentul de timp al controlului accesului);

- permisiunile de securitate sa se desemneze prin “clase de permisiuni”. o clasa de permisiuni sa dispuna de un nume si sa poata fi asociata unui set de grupuri, roluri, tipuri de documente gestionate, meniuri de acces la aplicatie, acces la registre de documente
- trebuie sa permita stabilirea nivelului de autorizare pe care utilizatorul il are alocat in cadrul arhivei, cel putin: citire, scriere, complet, vizualizare doar fisa document fara posibilitate de vizualizare continut, cu recursivitate sau nu.
- clasa de permisiuni trebuie sa poata oferi unui grup de utilizatori unul din niveluri principale de acces catre un document:
    - acces la vizualizarea fisei de documente dar fara acces la continutul efectiv al documentului,
    - acces la vizualizarea atat a fisei de document cat si la continutul electronic al documentului,
    - acces la vizualizarea atat a fisei de document cat si la continutul electronic al documentului cu posibilitatea de modificarea datelor din fisa de date a documentului,
    - acces la vizualizarea atat a fisei de document cat si la continutul electronic al documentului cu posibilitatea de modificarea datelor din fisa de date a documentului sau stergere document
- utilizatorii trebuie sa poata avea acces la documentele din arhivele electronice in conformitate cu rolul asociat acestora si cu drepturile de acces inregistrate de catre administratorul arhivei. functiile utilizate de catre utilizatorii sistemului trebuie sa fie minimal:
    - administrare: pentru monitorizarea proceselor si informatiilor legate de administrarea arhivei,
    - cautarea si vizualizarea: pentru cautarea documentelor in arhiva electronica;
- trebuie sa permita definirea de colectii de documente ce contin documente grupate din arhiva grupate dupa diverse criterii, cu scopul de a oferi acces temporar unui set de utilizatori alesi ad-hoc
- trebuie sa permita arhivarea oricaror tipuri de documente indiferent de tipul de fisier in care este stocat
- utilizatorii trebuie sa fie definiti de catre operatorii autorizati ai administratorului de arhiva, operatori ce au la randul lor rolul de utilizator administrator tehnic al arhivei
- pentru fiecare utilizator al subsistemului se vor inregistra cel putin informatiile urmatoare:
    - Numele de utilizator,
    - Numele si prenumele persoanei respective,
    - Adresa de email a utilizatorului;
    - IP de acces
    - Username de Active Directory corespondent
    - Grupuri de Active Directoy corespondente
    - Data intrare in organizatie
    - Numar de logari esuate permise
    - Acces read-write sau read-only general in sistem
    - Departamentul din care face parte
    - Functia de incadrare in organigrama

- facilitate de anonimizare si pseudonimizare asupra datelor personale aferente utilizatorilor persone fizice dar si a personalor juridice referite in cadrul aplicatiei, in conformitate cu recomandarile standardului GDPR
- nu trebuie sa se impuna limitari asupra numarului de documente si metadate stocate sau asupra capacitatii de stocare pe care o poate gestiona;
- trebuie sa ofere interfete de cautare in arhiva si administrare arhiva accesibile din browser: cel putin Internet Explorer/Edge, Google Chrome si Mozilla firefox;
- trebuie sa ofere posibilitatea de salvare si reutilizare a seturilor de criterii de cautare avansata in arhiva;
- trebuiesa permita operatiuni de download bulkpe baza seturilor de cautare salvate
- Să pună la dispoziţia utilizatorilor toate funcţiile platformei prin intermediul unui client web de tip ”out-of-the box”.
- Sistemul trebuie sa permita procesare si afisarea in aceasi structura de documente atat a documentelor electronice clasice (in format scanat) cat si a fisierelor de tip Electronic Data Interchange (EDI)
- Să permită adăugarea de documente electronice printr-un mecanism de tip ”drag-and-drop” in clientul web.
- Să permită organizarea documentelor într-o structura ierarhică intuitivă. Această organizare ierarhică va fi prezentată într-o structură arborescentă, similară sistemelor de fişiere comune/obişnuite. Documentele trebuie să poată fi organizate în structuri care să simuleze modalitatea reală de organizare în dosare şi fişete.
- Sistemul trebuie sa permita importul automat in arhiva electronica a fisierelor existente de pe suport de stocare electronic, organizat in foldere si subfoldere impreuna cu fisiere excel asociate care sa contina tipul documentelor si valorile metadatelor pentru fiecare fisier
- Sistemul trebuie sa permita importul automat in arhiva electronica a fisierelor de tip EDI (Electronic Data Interchange) cel putin din formatele: XML, iDOC, CSV, XML/EDIFACT conform ISO TS 20625, cu setarea de layouturi configurabile pentru fiecare tip de document EDI
- Să ofere posibilitatea de organizare a documentelor pe dosare (foldere)
- permite definirea de criterii de indexare suplimentare a documentelor, chiar dacă fizic sunt stocate în foldere diferite.
- permite definirea de “liste filtrate” de documente, vizibile pentru utilizator ca niște foldere, prin specificarea parametrilor utilizați la filtrare (exemplu: documente de un anumit tip, cu o anumita valoare într-un câmp de indexare sau create de un anumit utilizator) și a modului de afișare a rezultatelor (grupate după un an, sau după orice alt câmp, de exemplu);
- “Listele filtrate” pot fi generale, accesibile pentru toți utilizatorii sau specifice numai unui anumit utilizator/ grup de utilizatori și pot fi numite sugestiv (ex. „documente control X”;
- Să ofere posibilitatea stocării documentelor într-un spaţiu centralizat şi organizat şi posibilitatea de a asocia metadate pentru fiecare document în parte
- permite administratorilor definirea de volume de stocare a documentelor (locații fizice în care vor fi salvate documentele în sistem, pe medii diferite), precum și posibilitatea de a se conecta la unul sau mai multe „Depozite de stocare”, în funcție de drepturile pe care aceștia le au.
- permite adminstratorului configurarea atributelor (câmpuri de date) fiecărui tip de document prin utilizarea unei interfeţe prietenoase de tip web, fără a fi nevoie de intervenţia în codul aplicaţiei.

- Sa permita adminstratorului să definească un set general de atribute la nivelul organizaţiei din care se vor alege ce atribute să apară pe fiecare tip de document
- Să permită operaţii multiple executate asupra documentelor:
    - versionarea automată a documentelor, permițând păstrarea tuturor versiunilor prin care trece un document/ înregistrare;
    - check-out/ check-in, pentru asigurarea modificării coerenta a documentelor (în lucrul colaborativ); un document aflat in statusul de “check-out” (în editare), va rămâne în continuare vizibil pentru ceilalți utilizatori, doar în mod vizualizare (read-only);
    - etichetarea fiecărei versiuni, pentru a permite utilizatorilor identifice facil versiunea căutată;
    - “Roll back”, adică de revenire la o versiune anterioara;
    - posibilitatea de anexare la documentul inițial şi a altor documente;
    - indexarea automata a documentelor;
- În ceea ce privește prelucrarea documentelor pe tipuri de documente şi metadate specifice acestor tipuri trebuie să permită:
    - arhivarea documentelor în funcţie de termenele de păstrare şi tipurile de documente
    - definirea tipurilor de documente permise pentru fiecare flux de lucru;
    - să se poată predefini fluxuri de lucru pentru fiecare tip de document;
    - stocarea şi indexarea automată a documentelor în foldere/dosare predefinite în funcţie de tipul documentelor;
    - indexarea automată a documentelor în funcţie de departament şi tipul documentului;
- Să ofere suport pentru ciclul de viaţă al unui document (crearea, modificarea, validarea, aprobarea, publicarea, arhivarea). În funcţie de starea unui document sunt disponibile spre utilizare diferite acţiuni asupra documentelor.
- sa permita implementarea nomenclatorului arhivistic conform legislaţiei.
- sa permita mutarea documentelor care nu mai sunt active într-un depozit special de arhivă, atunci când utilizatorii definesc acele documente ca fiind bune de arhivat;
- sa permita definirea de termene de păstrare la salvarea documentelor în concordanţă cu cerinţele legislative;
- sa permita arhivarea documentelor în funcţie de termenele de păstrare şi tipurile de documente;
- Să poată stoca metadatele în cel puţin sistemul de baze de date relaţionale ofertat
- Sa permita urmărirea şi trasabilitatea modificărilor efectuate pe un document.
- Modificările asupra documentelor să poată fi realizate numai atunci când un document este scos (checked out). Un utilizator care a făcut check out pe document va lucra cu acesta, iar după terminarea acestei activităţi, prin acţiunea de check in, documentului i se va incrementa numărul versiunii în mod automat, operaţia de check in putând fi completată de comentarii asupra versiunii.
- Să permită nativ versionarea documentelor prin funcţionalităţi de tip „Check In – Check Out”. Formatul de stocare al documentelor electronice trebuie să fie cel nativ, astfel se exclude păstrarea documentelor în formatul propriu sistemului, pentru a asigura recuperarea facilă a datelor în caz de defecţiune.

- trebuie sa poata asigura salvarea criptata a continutului documentelor, folosind algoritmul de criptare aes.
- trebuie sa permita integrarea cu orice server de directory care implementeaza protocolul ldap, pentru sincronizarea utilizatorilor si autentificarea acestora in sistem;
- trebuie sa permita dezactivarea utilizatorilor si reactivarea ulterioara daca este cazul;
- utilizatorii definiti in sistemul de gestiune utilizatori al sistemului, trebuie sa fie obligati sa isi schimbe parola la prima logare si trebuie sa isi poata schimba parola ulterior ori de cate ori doresc;
- utilizatorii sa fie deconectati automat din sistem dupa o perioada in care acesta nu mai e utilizat;
- trebuie sa permita utilizatorilor introducerea in arhiva a documentelor in regim bulk (mai multe documente deodata) impreuna cu metadatele de caracterizare aferente;
- trebuie sa aloce un numar unic de inregistrare pentru fiecare nou document intrat in arhiva;
- trebuie sa poata aplica automat un set de reguli de securitate, la incarcarea documentelor in arhiva si ulterior, in functie de metadatele documentului;
- utilizatorii sa poata naviga in cadrul arhivei si in functie de perspective care sa ghideze utilizatorii dupa diverse criterii legate de informatiile de arhivare: data, metadate specifice documentului. perspectivele sa poata fi definite ad hoc de catre utilizatorul arhivei fara a dispune de cunostinte de programare. trebuie sa nu existe limitari in ceea ce priveste numarul de perspective si numarul de niveluri de structurare a datelor in cadrul perspectivelor;
- trebuie sa pemita definirea de mai multearhive operationale;
- in cadrul arhivei operationale trebuie sa se permita utilizatorilor adaugarea si stergerea documentelor electronice;
- trebuie sa se permita utilizatorilor modificarea metadatelor documentelor electronice din arhiva operationala direct din interfata de utilizare;
- trebuie sa se permita popularea arhivei operationale utilizand modulul de captura documente;
- trebuie sa ofere auditarea operatiilor efectuate, operatiile de configurare/administrare a auditului si de consultare a acestuia sa se realizeze de catre administratori. informatiile referitoare la audit nu pot fi alterate nici macar de administratori fara a se marca cine a facut acea operatie. trebuie sa ofere mecanisme proprii de protectie a informatiilor de audit;
- utilizatorii sa poata vizualiza, pentru fiecare document in parte, istoricul modificarilor, cu evidentierea modificarilor in fiecare nou context;
- trebuie sa permita afisarea unui link de acces pentru fisa fiecarui document, link ce poate fi transmis pe email sau prin alte mijloace de comunicare electronica;
- trebuie sa permita transmiterea pe email a documentului direct din interfata de acces a arhivei;
- trebuie sa permita selectarea anumitor documente cu care se lucreaza frecvent si gruparea lor intr-o zona de documente de tip favorite;
- trebuie sa dispuna de interfata de vizualizare a detaliilor si descarcare a continutului fisierelor zip (pentru fiecare din fisierele arhivate intr-o arhiva format zip);
- trebuie sa permita afisarea direct in browser a documentelor de tip imagine, fara a fi nevoie de achizitionarea de licente pentru programe software auxiliare care sa fie instalate pe statia de lucru.
- trebuie sa suporte cel putin urmatoarele formate de fisiere utilizate de catre achizitor; pdf, tiff, jpeg, bmp, gif, doc, docx, rtf, txt, html, ppt, pptx.

- trebuie sa permita vizualizarea documentelor pe diferite niveluri de zoom, de la ansamblu pana la cele mai mici detalii
- trebuie sa dispuna de posibilitatea de a utiliza clienti de acces, pentru echipamente mobile (telefoane/tablete), la arhivele gestionate;
- modulul de arhivare electronica va gestiona si permite accesul utilizatorilor la documentele ce vor fi arhivate de catre achizitor folosind modulul de captura documente pus la dispozitie de catre prestator
- trebuie sa ofere posibilitatea de arhivare si expunere a continutului arhivat, catre orice alt sistem, prin folosirea standardului cmis (content management interoperability services);
- modulul arhivare electronica va dispune de funcționalități de gestiune nomenclatoare arhivistice.
- În ceea ce privește căutarea platforma trebuie sa asigure:
    - căutarea automată a documentelor inclusiv după textul conţinut cel puţin pentru: documentele scanate utilizând OCR, fişiere office (Word, Excel), fişiere PDF şi emailuri;
    - salvarea căutărilor pentru utilizare ulterioară;
    - rafinarea rezultatelor unei căutări prin filtrări şi ordonări suplimentare operate doar asupra rezultatelor căutărilor;
    - căutarea rapidă după valorile din oricare câmp de indexare (metadata), după titlul documentului și după conținutul acestuia (full text)
    - căutări utilizând operatori logici booleni (”and” şi ”or”) și de comparație ”egal”, ”conţine”, ”mai mic”, ”mai mare”, căutări de proximitate (de exemplu sunt căutați doi termeni, condiția fiind ca între aceștia să nu existe mai mult de 3 cuvinte), etc;
    - căutări doar în ultima versiune a documentelor sau în toate versiunile acestora;
    - să realizeze un “scoring” al rezultatelor obținute în urma operației de căutare și să afișeze rezultatele ordonate conform acestui scoring; scoring-ul va tine cont de relevanța termenilor de căutare dar și de data de creare și accesare a documentelor;
    - un mecanism de subliniere a termenilor după care a fost efectuata căutarea, atât în metadate cât și în interiorul documentului;
    - exportarea listei de obiecte rezultată în urma operației de căutare, în formate standard, cum ar fi csv sau excel;
    - definirea de câmpuri care să fie văzute in lista de rezultate precum și ordinea acestora, va permite ordonarea rapidă a rezultatelor după orice câmp precum și gruparea rezultatelor “on-the-fly”;
    - definirea de “liste filtrate” de documente, vizibile pentru utilizator ca niște foldere, prin specificarea parametrilor utilizați la filtrare (exemplu: documente de un anumit tip, cu o anumita valoare într-un câmp de indexare sau create de un anumit utilizator) și a modului de afișare a rezultatelor (grupate după un an, sau după orice alt câmp, de exemplu);
    - să permită exportul conținutului listelor filtrate în xls sau csv;
- Sa ofere un cadrul integrat de colaborare pe documente prin scrierea de mesaje de colaborare pe document adresate anumitor utilizatori şi păstrarea istoricului.
- Să permită integrarea cu alte sisteme informatice, astfel încât să schimbe informaţii cu acestea sub formă de documente. Aceasta funcţionalitate priveşte (şi) interogarea (la nevoie a) arhivelor de către organizaţii externe.

- Să dispună de integrare nativă cu aplicaţii Microsoft Office (in vederea asigurării compatibilizării cu sistemele utilizate în prezent de Achizitor), astfel încât să permită:
    - editarea şi/sau salvarea documentelor direct pe server, diun repository.
    - pre-vizualizare (preview) a documentelor direct în interfață, fără să fie nevoie să se deschidă documentele în aplicațiile native asociate, pentru toate tipurile uzuale (PDF, imagine, Word, Excel, Powerpoint, etc)
    - din aplicațiile Word si Excel sunt posibile următoarele operații:
        - accesarea depozitului/ depozitelor de documente la care utilizatorii au acces;
        - deschiderea documentelor din depozitele de documente și salvarea documentelor în depozitele de documente;
        - vizualizarea metadatelor documentelor;
        - executarea operațiunilor de check-in/ check-out;
        - compararea versiunilor aceluiași document, prin utilizarea funcționalității "compare" din Microsoft Word
        - sa permita definirea șabloanelor direct in aplicația Microsoft Word sau Excel. Astfel, orice document existent în format Word sau Excel va putea fi transformat în șablon, prin definirea zonelor în care vor fi precompletate valorile din metadate.
        - înregistrarea directă a documentelor și inserarea automată a numerelor de înregistrare şi a datei de înregistrare în conţinutul documentelor WORD şi EXCEL.
    - Din aplicatia Microsoft Outlook/ Mozille Thunderbird sau alti clienti de email sa se poate realiza salvarea automată a fișierelor e-mail și a atașamentelor în depozitele de stocare a documentelor, cu preluarea automată a câmpurilor de indexare specifice e-mail-urilor: expeditor, recipient, subiect și conținut e-mail.
- Să permită transmiterea prin email a documentelor sau a unui link către documentele stocate in depozitul de documente al soluţiei ("repository"). Pentru fiecare link transmis, utilizatorul trebuie să aibă posibilitatea să seteze durata de valabilitate a link-ului și numărul de descărcări premise prin intermediul link-ului respectiv;
- Să includă nativ un modul de captură a documentelor, prezentându-se în acest sens documente oficiale de la producător.
- Să includă un modul de management de fluxuri de lucru cu documentele, prezentându-se în acest sens documente oficiale de la producător.
- Asigură o securitate ridicată în ceea ce privește accesul la documente, astfel:
    - accesul la documentele gestionate este posibil exclusiv prin intermediul aplicației client și nu prin file-sharing;
    - Dispune de mecanisme de definire a permisiunilor la nivel de depozit de documente, de entitate sau de atribut al entității;
    - permisiunile care se pot defini sunt: vizualizare date, editare date, ștergere și de modificare a permisiunilor;
    - permisiunile de acces la documente sunt calculate dinamic, în funcție de valorile metadatelor asociate documentelor
    - drepturile de acces se pot gestiona la nivel de container de documente și fișier, precum și pe tipuri de documente sau pe fiecare atribut de pe tipurile de documente, utilizând utilizatori şi grupuri de utilizatori.

- Să ofere o consolă administrativă, punând la dispoziţia administratorilor de sistem o interfaţă prietenoasă pentru administrare.
- Să ofere posibilitatea creării structurii de date, utilizând o interfaţă grafică, astfel:
- definirea de mai multe volume de stocare a documentelor (mai multe locații fizice în care vor fi salvate documentele în sistem, pe medii diferite);
    - configurarea facilă, direct în aplicaţie, la nivel de atribut pentru cel puțin următoarele caracteristici: eticheta afişată utilizatorilor, tipul de date permis (text, număr, data calendaristică, logic = adevărat sau fals), lungimea permisă, valoare implicită (exemplu: utilizator curent, data curentă), lista de valori, formula de calcul funcţie de alte metadate;
    - definirea de către administrator de noi ecrane ale aplicaţiei mapate pe tipuri de documente, în care să gestioneze diferite formulare, liste, entităţi organizatorice, date, relaţii părinte-copil, relaţii cu subpagini mapate pe alte tipuri de documente, pe care să le poată publica direct în meniul aplicaţiei pentru utilizatori;
    - administrarea şabloanelor folosind categorii de documente, compartimente de utilizat, dosare, categorii predefinite, metadate și valori pre-completate pentru metadate;
- Să permită aflarea numărului de documente gestionat de platforma precum si a dimensiunii acestora prin punerea la dispoziție a unui set de rapoarte predefinite dintre care:
    - situaţie ocupare storage atât per unitate cât şi per utilizator,
    - documente create sau modificate de către utilizatori într-o anumită perioadă;
- Să ofere posibilitatea de a monitoriza și notifica evenimentele astfel:
    - monitorizarea fluxurilor de lucru active;
    - generarea de alerte şi notificări din fluxuri de lucru;
    - monitorizarea şi generarea de alerte pentru fluxurile de lucru care nu sunt executate în numărul de zile stabilit;
    - notificare a utilizatorilor privind modificările ce apar în sistem: a fost creat un nou document, documentul a ajuns într-un nou stadiu, etc.
    - notificarea pe e-mail despre o sarcină de efectuat sau neefectuată;
- Să permită auditarea operaţiunilor de login, logout, acces pe foldere, acces pe fişiere. Informaţiile de audit vor conține inclusiv IP-ul de acces, data, ora, utilizatorul şi acţiunea efectuată;
- Să permită păstrarea istoricului activității prin intermediul configurărilor aferente proceselor precum introducerea documentelor, aprobări, printări, etc.
- Să permită administratorului restaurarea documentelor şterse de către utilizatori.
- Să permită criptarea documentelor direct în sistemul de fişiere, astfel încât, dacă un utilizator va putea accesa locația de stocare să nu poată accesa conținutul documentelor.
- Să fie de tip enterprise si sa poată fi instalată pe o gama variata de sisteme de operare incluzând Linux, Windows şi Unix.

3.2.5.6.1.3.1 Gestiune nomenclatoare arhivistice

- modulul de gestiune nomenclatoare arhivistice trebuie sa fie accesibil prin interfata de tip web;
- modulul de gestiune nomenclatoare arhivistice trebuie sa permita crearea, publicarea si gestionarea de nomenclatoare arhivistice;
- modulul de gestiune nomenclatoare arhivistice trebuie sa permita modificarea si versionarea nomenclatoarelor existente;

- modulul de gestiune nomenclatoare arhivistice trebuie sa permita publicarea nomenclatoarelor arhivistice;
- modulul de gestiune nomenclatoare arhivistice trebuie sa permita exportul de nomenclatoare;
- modulul de gestiune nomenclatoare arhivistice trebuie sa permita introducerea de perioade de pastrare pentru documente, inclusiv perioada de pastrare permanenta;
- modulul de gestiune nomenclatoare arhivistice trebuie sa permita modificari ale elementelor componente (ex. entitati, tipuri de documente, perioade de pastrare), pentru versiunile publicate ale nomenclatorului, doar prin crearea unor versiuni noi.

3.2.5.6.1.4 Modul de captură

Componenta de captură a documentelor trebuie să dispună de următoarele caracteristici minime:

- Să permită scanarea documentelor pe hârtie și încărcarea acestora în sistem, utilizând scanarea locală sau la distanţă.
- Integrare nativă cu modulul de registratură permițând înregistrarea şi direcţionarea fişierelor în timpul procesului de scanare, către compartimentul de destinaţie.
- sa permita scanarea documentelor format hârtie şi obţinerea de imagini scanate.
- sa permita scanarea asincronă şi realizează legătura fişierului scanat la informaţiile de înregistrare în funcţie de codul de bare aplicat pe document.
- Aplicația dispune de capabilitatea de a imprima coduri de bare şi numere de înregistrare cu imprimante de coduri de bare speciale și aplicarea pe documente;
- În timpul operaţiei de clasificare, imaginile scanate pot fi combinate într-un document, iar la sfârşit exportate în format .pdf, încărcându-se apoi în sistemul de management al documentelor.
- Indexarea documentelor electronice va fi realizată atunci când imaginile scanate sunt convertite în documente .pdf în care se pot efectua căutări
- Sa permita folosirea de metadescriptori (câmpuri) pentru paginile scanate şi nu impune limitări cu privire la numărul acestora.
- realizează operaţiuni automate de OCR pentru toate fişierele de tip imagine şi PDF. În plus, sa permita indexarea şi căutarea automată a documentelor inclusiv după textul conţinut cel puţin pentru: documentele scanate utilizând OCR, fişiere office (Word, Excel), fişiere PDF şi emailuri;
- Validarea metadescriptorilor asociaţi la nivel de imagine scanată se va realiza automatizat, pe baza unor reguli de validare, sau manual. În cadrul procesului de validare pot fi incluse referinţe către sisteme externe.
- sa permita înregistrarea și rutarea automata a documentelor pe flux în timpul procesului de scanare către compartimentul de destinație.
- Fluxuri de scanare multiple şi rutarea documentelor pe fluxuri pot fi definite şi întreţinute vizual, direct în aplicaţie, fără necesitatea de a scrie cod.
- sa permita trimiterea documentelor pe fluxuri de lucru de la ecranul de control/ecranul tactil al scanerului.
- sa permita pre-vizualizarea (preview) documentelor direct în interfață, fără să fie nevoie să se deschidă documentele în aplicațiile native asociate, pentru toate tipurile uzuale (PDF, imagine, Word, Excel, Powerpoint, etc);
- sa permita definirea mai multor algoritmi de extracție text, câte unul pentru fiecare furnizor, cu un număr mare de apariții ale documentelor în fiecare lună

- sa permita Eliminare manuală a datelor de intrare de până la 90% din documentele tipărite
- sa permita Clasificări de documente și identificare pe baza formulelor REGEX
- sa permita Validare text extras din tabelele bazei de date relaționale;
- sa permita Validare manuală pentru documentele care nu au trecut de extragerea automată a textului și validare acestuia
- sa permita extragerea datelor utilizând OCR full text sau OCR pe zone speciale ale documentelor / zone de document
- sa permita extragerea directă a datelor folosind PDF API
- sa permita extragerea mixtă a datelor combinată din extragerea de date cu PDF API și expresia REGEX
- sa permita Indexarea documentelor pentru căutare rapidă și recuperare prin metadate extrase în mod automat

3.2.5.6.1.5 Modulul de registratură electronică

Modulul de registratura a documentelor trebuie să îndeplinească minim următoarele cerințe:

- trebuie sa permita inregistrarea si distributia de documente curente in format electronic in cadrul organizatiei;
- trebuie sa permita definirea structurii organizationale in forma arborescenta;
- trebuie sa permita definirea de noi tipuri de entitati la nivelul structurii organizationale (divizie, departament, birou, etc);
- trebuie sa permita definirea de registre si registraturi;
- trebuie sa se poata defini utilizatori cu rol de “registrator” din punctele de intrare / iesire a documentelor din organizatie in vederea inregistrarii de documente, cu scopul de a le distribui in interiorul sau in afara organizatie;
- inregistrarea documentului va genera actiunea de a acorda unui document un numar unic de identificare la nivelul organizatiei, putand fi astfel urmarit in cadrul organizatiei si in relatia cu tertii;
- trebuie sa permita ca numarul de inregistrare sa fie acordat automat in momentul crearii unui document in sistem, numai daca utilizatorul foloseste aceasta optiune, aplicatia oferind in acest fel posibilitatea de a stoca si documente fara numar de inregistrare;
- trebuie sa permita gestionarea centralizata si unicitatea numerelor de inregistrare, numarul unic de inregistrare se va acorda pe baza unui sistem de numerotare centralizat la nivelul intregii organizatii, care se va reseta la inceputul fiecarui an calendaristic si odata alocat un numar de inregistrare documentului, acesta sa nu mai poate fi modificat de catre nici un utilizator;
- va permite crearea si gestionarea de registre de numere, definite de catre administratorul solutiei, care pot fi de mai multe tipuri si vor detine serii de numere secventiale care se vor asocia cu tipuri de documente;
- va permite ca un registru sa poata fi asociat la mai multe tipuri de documente, iar in acelasi timp un tip de documente sa poata fi asociat la mai multe registre;
- va gestiona documente de intrare, de iesire sau informative, oricare dintre acestea putand fi trimise catre unul sau mai multi destinatari;
- trebuie sa permita fiecarui destinatar, pentru documentele ce necesita rezolvare, crearea de raspunsuri la documentul primit si transmiterea acestora catre alte unitati organizationale;

- trebuie sa se poata afisa harta de proces a documentului, care va indica utilizatorii si data la care au primit documentul pentru a furniza rezolutii, precum si statusul la fiecare utilizator;
- trebuie sa permita gestionarea de nomenclatoare pentru emitentii si destinatarii externi;
- un document va fi trecut in starea „finalizat" numai dupa ce toti utilizatorii implicati in fluxul de distributie a acelui document vor finaliza documentul;
- utilizatorii trebuie sa poata regasi documente in cadrul modulului software registratura dupa datele asociate. numarul de inregistrare, emitent, destinatar, data emitere;
- trebuie sa permita definirea drepturilor de acces la documente astfel incat utilizatorii asociati unei registraturi vor avea acces numai la documentele pe care le-au initiat sau le-au fost trimise.
- Aplicatia va permite inregistrarea automata a emailurilor primite si a documentelor atasate direct in cadrul aplicatiei prin configurarea adreselor de email si a setarilor de server;
- trebuie să ofere o imagine de ansamblu a procesului de activitate, de tip tablou de bord;
- Soluția pentru registratură electronică trebuie să permită generarea automată a numerelor de înregistrare pe documentele supuse înregistrării, conform regulilor de generare a numerelor (ex: cu prefix, sufix);
- trebuie să permită ca, după aplicarea filtrelor de căutare, raportul registrului obținut să poată fi exportat în format electronic (de exemplu: PDF, XLS, CSV) și să poată fi descărcat local pe calculatorul utilizatorului;
- trebuie să permită ca numerele de înregistrare să fie resetate la începutul fiecărui an calendaristic;
- trebuie să permită clonarea inregistrarii intr-un registru, pentru optimizarea procesului de inregistrare;
- trebuie să permită vizualizarea direct din interfata a cotinutului documentelor atasate la o inregistrare;
- trebuie să permită marcarea predarii fizice a documentelor catre destinatari din cadrul organizatiei, cu posibilitatea de captare de pe o tableta grafica atasata statiei de lucru a semnaturii persoanei;
- trebuie să permită generarea borderourilor de documente predate;
- trebuie să permită scanarea asincrona a documentelor pentru introducerea acestora in sistem (prin utilizarea codurilor de bare imprimate pe etichete de coduri de bare si lipite pe documentele in format fizic / hard-copy);
- Aplicatia va oferi posibilitatea de a inregistra automat si a remite expeditorului o recipisa de confirmare a receptiei cel putin cu urmatoarele elemente: numarul de inregistrare, data inregistrarii, continutul pe scurt, pagina de inregistrare in format PDF care sa contina prima pagina a documentelor anexate transmise spre inregistrare pe email pe care s-a aplicat in partea de sus a paginii bonul de inregistrare in format electronic;
- Sistemul va permite definirea oricator registre configurabile facil de administratorul aplicatiei;
- Sistemul va permite configurarea coloanelor care sa apara in fiecare registru in functie de nevoile spcifice ale beneficiarului, ca de exemplu dar fara a ne limita la: in registrul de contracte se pot defini coloane gen termen de expirare, zile alerta, tip contract , centru de cost, departament baza. Elementele configurabile minimale: denumire coloana, pozitie, obligatoriu sau nu, Eticheta afisare, Selectie din lista de valori, Valori disponibile pentru selectie, tip de date;
- Pentru operativitate sistemul va permite copierea automata a valorilor metadatelor documentelor inregistrate in coloanele din registrul in care sunt inregistrate documentele;

- Aplicatia va permite configurarea coloanelor care sa apara in fiecare registru cel putin pentru urmatoarele elemente: eticheta multilimba, tip de data, dimensiune, obligativitate, lista de valori asociata, formula de calcul, valori implicite;
- Aplicatia va pemite configurarea taburilor in care sa fie organizate informatiile in fiercare registru, cel putin a urmatoarelor elemente: eticheta multilimba, pozitie, vizibil sau nu;
- Pentru usurinta administrarii aplicatia va permite imporul si exportul configurarilor unui regisru in format XML;
- Pentru usurinta administrarii aplicatia va pemite clonarea configurarilor unui registru;
- În cazul documentelor externe, se vor înregistra, cel puțin, următoarele informații (câmpuri):
    - Număr de înregistrare dat de către o altă instituție;
    - CNP sau CUI, după caz;
    - Proveniența documentului;
    - Adresa provenienței (județ, localitate, stradă, număr, bloc, scară, apartament)
    - Tipul documentului;
    - Termenul de rezolvare (în număr de zile) sau data până la care trebuie rezolvat documentul;
    - Descrierea documentului;
    - Observații.
- În cazul documentelor provenite din exteriorul instituției sistemul trebuie să permită introducerea modului de intrare în sistem. Utilizatorul trebuie să aiba la dispoziție un nomenclator de moduri de intrare, nomenclator ce trebuie să poată fi gestionat de către administratorii sistemului. Exemplu de valori din nomenclatorul reprezentand modurile de intrare: registratură, email, curier, online,etc;
- Pentru tipurile de acte care au definite fluxuri de lucru automate, după înregistrarea actelor, soluția trebuie să trimită automat actele la serviciile definite in cadrul fluxurilor automate de lucru. Soluția va permite marcarea câmpurilor obligatorii ale unui formular electronic și validarea completării acestora;
- Modulul registratură va utiliza nomenclatoare pentru: proveniență (alte instituții, companii, ministere), adresă (județe, orașe), tipul documentului. Nomenclatoarele utilizate vor putea fi actualizate;
- Termenul de rezolvare a tipului de document selectat de către utilizator se va completa automat, dar va putea fi modificat de utilizator, după caz;
- Utilizatorul să poată lista un bon (raport) după înregistrarea documentului, care să conțină, pe lângă datele specificate la înregistrare și numărul și data înregistrării; bonul va fi înmânat solicitantului;
- Modulul de registratură va pune la dispoziție un serviciu web (sau funcție API), care să fie apelat de către orice aplicație din instituție, pentru a putea genera număr unic din registrul general;
- Se vor putea aloca numere speciale pentru documentele la care legislația prevede acest lucru. Acest număr trebuie sa fie generat automat de sistem, astfel se vor genera registre speciale suplimentare registrului unic al instituției;
- Conexarea cu alte documente (toate documentele adiționale referitoare la un anumit document trebuie să se poată conexa cu prima înregistrare a documentului);

- Utilizatorii trebuie să poată înregistra observații in momentul operării (trimiterea sau rezolvarea) documentelor. Mai mulți utilizatori pot înregistra observații la aceeași document, iar aceste observații apar centralizat în istoricul documentului;
- În momentul repartizării unui document utilizatorul trebuie să aibă posibilitatea sa completeze o rezoluție generală cu privire a motivul repartizării;
- Modulul trebuie să permită posibilitatea de validare la introducerea datelor.

3.2.5.6.1.6 Modulul de fluxuri de lucru

SMED trebuie să includă un motor de fluxuri de lucru care asigură capabilitatea de gestiune a proceselor cu documente ce să permită circulaţia documentelor pe trasee ierarhice sau definite de autorul documentului, cu posibilitatea aprobării sau respingerii acestora, standardizarea, distribuirea şi circulaţia informaţiilor şi a documentelor interne în cadrul structurii, precum şi a celor generate în relaţia cu autorităţi externe.

Soluția trebuie să includă atât instrumentele pentru dezvoltare cât şi mediul de rulare pentru proiectarea, execuţia și monitorizarea fluxurilor de documente.

Modulul de fluxuri de lucru cu documente trebuie să asigure minim următoarele funcționalități:

- sa permita autorilor de procese definirea şi întreţinerea vizuală, direct în aplicaţie, a fluxurilor de lucru aplicabile documentelor înregistrate;
- sa permita autorilor de procese proiectarea fluxurilor de lucru bazate pe organigrama entității;
- sa permita autorilor de procese să definească termene limită pentru fiecare etapă a fluxului de lucru;
- sa permita autorilor de procese să proiecteze fluxuri de lucru cu sarcini singulare sau sarcini paralele;
- sa permita autorilor de procese să definească condiţiile de terminare pentru o activitate paralelă;
- sa permita autorilor de procese să definească comenzi condiţionale în cadrul fluxurilor de lucru (de ex. în cazul în care facturile care depăşesc o anumită sumă, trebuie să fie aprobate de către o altă persoană);
- sa permita autorilor de procese definirea variabilelor pentru fluxurile de lucru;
- sa permita autorilor de procese modificarea cu uşurinţă a fluxurilor de procese, regulilor şi logicii de rutare fără intervenţia utilizatorilor IT şi fără activităţi de tip IT ca instalarea de noi pachete ale aplicaţiei sau modificări in schema bazei de date.
- sa permita autorilor de procese să aloce drepturi de executare pentru fiecare flux de lucru;
- sa permita autorilor de procese să definească tipuri de documente permise pentru fiecare flux de lucru;
- sa permita autorilor de procese să definească fluxuri de lucru pentru fiecare tip de document;
- sa permita autorilor de procese să programeze declanșarea schimbului de date cu sistemele externe prin API (Application Programming Interface) înainte şi după iniţierea unui flux de lucru şi de asemenea, pentru orice pas al fluxului de lucru;
- sa permita autorilor de procese să programeze un timp expirare pentru flux de lucru;
- sa permita autorilor de procese blocarea editării documentelor după anumite etape a fluxului de lucru - de exemplu: nesă permitărea editării unui contract după aprobare;

- sa permita autorilor de procese să utilizeze grupuri şi roluri pentru definirea fluxurilor de lucru;
- sa permita autorilor de procese punerea în aplicare a oricărui tip de acţiune înainte sau după orice etapă a fluxului de lucru;
- sa permita autorilor de procese definirea şi validarea metadatelor ca obligatorii într-o etapa din fluxul de lucru;
- sa permita autorilor de procese să programeze escaladarea automată a paşilor dacă nu există un răspuns într-un anumit număr de zile;
- sa permita autorilor de procese exportul definiției fluxurilor de lucru în format de tip imagine, pentru a-l putea prezenta spre avizare;
- sa permita autorilor de procese exportul și importul definiției fluxurilor de lucru într-un format standardizat, cum ar fi XML
- redirecţionarea automată a sarcinilor în cazul în care utilizatorul şi-a delegat sarcinile;
- informarea utilizatorilor prin e-mail despre o nouă sarcină primită pe un flux de lucru;
- notificarea utilizatorilor pe e-mail despre o sarcină de efectuat sau neefectuată;
- deschiderea sarcinilor de către utilizatori din notificări primite pe e-mail;
- sa permita utilizatorilor se scrie un comentariu la terminarea unei sarcini a unui flux de lucru
- sa permita administratorului să genereze un tabel cu toate fluxurile de lucru şi toate informațiile necesare;
- sa permita utilizatorilor să creeze filtre de căutare care să se aplice fluxurilor de lucru;
- sa permita administratorilor să oprească un flux de lucru;
- administrarea de delegaţii pentru utilizatorii în concediu medical sau de odihnă;
- trimiterea documentelor pe fluxuri de lucru în mod automat în timpul procesului de scanare.
- trimiterea documentelor pe fluxuri de lucru de la ecranul de control/ecranul tactil al scanerului.
- notificarea utilizatorilor prin mesaje implicite pentru iniţializarea fluxului de lucru şi pentru acţiunile oricărui pas;
- sa permita editarea documentelor de către utilizatorii din fluxul de lucru;
- mutarea automată a fişierului într-un dosar pre-selectat, după o etapă a fluxului de lucru;
- sa permita utilizatorilor selectarea etapei fluxului de lucru în cazul în care documentul este returnat prin respingere şi întoarcerea la etapa anterioară sau în altă etapă a fluxului de lucru
- sa permita utilizatorilor selectarea persoanei din grupul de lucru, pentru ca documentele să nu fie trimise întregului grup;
- sa permita generarea unui istoric al fluxurilor de lucru pentru utilizatori individuali şi întreaga organizaţie;
- monitorizarea fluxurilor de lucru active;
- generarea de alerte şi notificări din fluxuri de lucru;
- monitorizarea şi generarea de alerte pentru fluxurile de lucru care nu sunt executate în numărul de zile stabilit;
- sa permita definirea si planificarea livrarii rapoartelor de tip alerta pe documente in cadrul sistemului, ca de exemplu dar fara a ne limita la: numar de documente nou create in ultima luna pe fiecare tip, documente ce urmeaza sa expire in urmatoarele x zile, numar de documente modificate de fiecare utilizator din departament in ultima saptamana.

- Rapoartele se vor putea livra automat pe email: zilnic, saptamanal, lunar specificand si ora la care se doreste livrarea acestora impreuna cu grupurile de utilizatori sau casutete de mail de livrare
- Rapoartele se vor putea livra in format: HTML, Excel, PDF atat in format tabelar cat si in format grafic cu layout configurabil / usor de definit de catre administrator

- Să permită initierea automată de fluxuri de lucru diferentiate pentru emailurile trimise la diferite adrese de email in functie de: adresa de email, expeditor, titlu sau cuvinte cheie continute in titlu, continut email sau cuvinte cheie
- Să permita nivele de aprobare diferentiate in functie de valorile stabilite la pasul respectiv de flux
- Să permita termene limita de executie atat la nivel de flux cat si la nivel de pas de flux de lucru
- Să permita definirea de mesaje implicite la initierea unui flux de lucru si la actiuni pe fiecare pas de lucru
- Să permită configurarea mutarii automate sau nu a documentelor in anumite foldere la transmiterea pe un anumit flux sau dupa anumiti pasi pe flux
- Să permit afișarea unui status vizual de progres pentru documentele aflate pe fluxul de lucru
- Să permită evidentierea vizuală a documentelor respinse de la aprobare
- Să permită definirea de pasi de tip DECIZIE pe flux
- Să permită definirea de pasi secventiali si paraleli de executie a fluxului
- Să permită trimiterea de informari pe mail, notificari automate in aplicatia mobile și în contul SPV a utilizatorilor pentru pașii unui flux
- Să permită mutarea automata in foldere speciale a documenelor respinse
- Să permită semnarea electronica a documentelor la aprobarea pe flux de fiecare utilizator
- Să permită aplicarea de semnaturi si stampile scanate pe documente word si pdf la aprobarea pe flux de fiecare utilizator
- Să permită ilustrarea grafica diferentiata a fisierelor care se afla pe un flux dar sunt inca necitite de catre destinatarii de pe flux, pe modelul Inbox Email Google sau similar.
- Să permită apelarea de servicii web, cereri http, sau alte functii de tip API dupa anumiti pasi de pe flux pentru integrarea cu alte sisteme existente in organizatia beneficiarului
- Sistemul trebuie sa permita definirea si planificarea livrarii a rapoartelor de tip alerta pe documente in cadrul sistemului, ca de exemplu dar fara a ne limita la: numar de documente nou create in ultima luna pe fiecare tip, documente ce urmeaza sa expire in urmatoarele 7 zile, numar de documente modificate de fiecare utilizator din departament in ultima saptamana.
- Rapoartele se vor putea livra automat pe email: zilnic, saptamanal, lunar speicifcand si ora la care se doreste livrarea acestora impreuna cu grupurile de utilizatori sau casutetele de mail de livrare
- Rapoartele se vor putea livra in format: HTML, Excel, PDF atat in format tabelar cat si in format grafic cu layout configurabil / usor de definit de caatre administrator
- Sistemul trebuie sa configurare initierii automate de fluxuri de lucru diferentiate pentru emailurile trimise la o diferite adrese de email in functie de: adresa de email, expeditor, titlu sau cuvinte cheie continute in titlu, continut email sau cuvinte cheie
- Sistemul trebuie sa permita termene limita de executie atat la nivel de flux cat si la nivel de pas de flux de lucru

- Sistemul trebuie sa permita Definirea de mesaje implicite la initierea unui flux de lucru si la actiuni pe fiecare pas de lucru
- Sistemul trebuie sa permita editarea documentelor care circula pe un flux de lucru
- Sistemul trebuie sa permita Configurarea mutarii automate sau nu a documentelor in anumite foldere la transmiterea pe un anumit flux sau dupa anumiti pasi pe flux
- Sistemul trebuie sa permita Marcarea fisierelor cu litere si culori diferite care sa reflecte progresul acestora pe fiecare pas de flux
- Sistemul trebuie sa permita Marcarea cu rosu a documentelor respinse de la aprobare
- Sistemul trebuie sa permita Mutarea automata in foldere speciale a documenelor respinse
- Sistemul trebuie sa permita Semnarea electronica a documentelor la aprobarea pe flux de fiecare utilizator
- Sistemul trebuie sa permita Aplicarea de semnaturi si stampile scanate pe documente word si pdf la aprobarea pe flux de fiecare utilizator
- Sistemul trebuie sa permita Ilustrarea grafica diferentiata a fisierelor care se afla pe un flux dar sunt inca necitite de catre destinatarii de pe flux
- Sistemul trebuie sa permita Apelarea de servicii web, cereri http, sau alte functii de tip API dupa anumiti pasi de pe flux pentru integrarea cu alte sisteme existente in organizatia beneficiarului
- In functie de procesele si procedurile Achizitorului, fluxurile de aprobare vor include minim următoarele automatizari:
    - Functia Superior – aplicatia trimite automat notificarea de tip informare doar catre Superiorul direct al Arhivatorului initiator, in baza relatiei predefinite de tip Superior
    - Functia Escalare pas de informare – daca un utilizator informat pe un pas de flux nu confirma informarea intr-un interval predefinit aplicatia finalizeaza automat pasul si notifica aprobatorii de pe pasul urmator;
    - Mutare document in folder dedicat dupa aprobare – pe pasul de trecere a documentului in stare Aprobat, acesta este mutat automat in zona de documente aprobate corespunzator tipului de document
    - Informare initiator aprobare document – initiatorul primeste notificare automata privitor la aprobarea documentului. Notificarea se trimite de pe pasul pe care s-a facut aprobarea finala
    - Notificare tert neparticipant la flux – finalizarea unui flux poate fi notificata unui tert care nu a participat la flux, dar este necesar sa afle ca documentul s-a aprobat sau generat
    - Pasul de respingere se poate selecta prin configurare – la respingere, documentul este restituit initiatorului sau unei persoane de pe un pas anterior
    - Blocarea posibilitatii de modificare a unui document dupa trimiterea pe flux.

3.2.5.6.1.7 Modulul de management arhivă fizică de documente

Modulul de management arhivă fizică de documente trebuie să asigure minim următoarele funcționalități:

- sa permita crearea și gestionarea pentru mai multe fonduri de arhivă
- sa permita definirea mai multor diagrame de organizare, unul pentru fiecare fond
- să permit gestionarea istoricului organigramelor

- Sa permita definirea si clasificarea multiplă a documentelor / „Nomenclatoare arhivistice” în conformitate cu legislaţia
- Sa respecte legislația şi regulamentul privind „Arhivele Naţionale”
- Sa se poata gestiona recepţii de documente de la clienţi
- Sa permita inregistrare de noi „Unități Arhivistice”
- Sa se poata defini registru Intrări-Ieşiri
- Sa permita scanarea de documente
- Acces securizat online pentru clienţi la fondul de documente
- Sa se poata genera rapoarte de monitorizare și management al fondului de documente
- Sa existe o fişa de Evidenţă a fondului arhivistic
- Sa permita administrarea depozitului: cladiri, corpuri, rânduri, rafturi, poliţe, alveole, cutii
- Sa permita gestionarea (crearea, actualizarea, stergerea) documentelor reglementate pentru managementul arhivei fizice.

3.2.5.6.2 Aplicație de evaluare risc

Sistemul SIAMC 2.0 va include/ integra și funcționalități de analiză predictiva care analizează datele din orice sursă și poate detecta anomalii si activitati ilicite in diverse domenii de activitate

Acest modul/ această subcomponentă va utiliza inteligența artificială pentru a îmbogăți datele cu metadate relevante pentru inspecția muncii, minimizând nevoia de conservare și catalogare manuală a datelor. Aceste metadate imbogatite trebuie să facă apoi posibilă optimizarea locației datelor, îmbunătățirea accesului la date, dezvoltarea rapidă a fluxurilor și accelerarea unei analize de risc eficiente.

Modulul trebuie să asigure minim următoarele funcționalități:

- automatizarea colectării, analizei și rezolvarea punctelor de date semnificative care dezvăluie întreaga amploare a incidentelor trecute și va ajuta la prezicerea riscurilor viitoare;
- Să dețină capabilitati avansate de ML/AI pentru a lucra cu diferite tipuri de fisiere – video, audio, documente, postări pe rețelele sociale/site-uri dedicate recrutării forței de muncă, imagini din orice sursa și alte baze de date;
- Colectarea și analiza datelor pentru a răspunde la întrebări de genul „cine, ce, când, unde și de ce”;
- Găsirea în mod continuu de perspective și semnificații în datele analizate, cu capabilități de de anticipare și căutare in permanenta a schimbărilor semnificative, modele emergente sau comportamente care ar putea indica un risc sau evenimente importante, sa modeleze evenimentele trecute pentru a descoperi ceea ce ar putea urma cu privire la comportamentul unui angajator;
- Să identifice în mod proactiv riscurile la legislația muncii potențiale pentru a permite inspectorilor sa reactioneze înaintea producerii încălcării;
- Posibilitatea de analiză a datelor procurate, centrată pe entitate care să potrivească diferite versiuni ale aceleiași entități găsite în cadrul ei, pentru a produce o versiune unitară a fiecărei entități (în mod principal angajatori persoane juridice sau fizice)

3.2.5.6.2.1 Detectarea alertelor

Modulul va trebui să permită detectarea sistematică a activității suspecte prin utilizarea unui motor de scoring de neconformare, care să permită combinații de tehnici analitice pentru a determina probabilitatea neconformității. Componentele pentru detectare și alertă trebuie să permită minim:

- Acordarea unui punctaj pentru mutații în activitatea angajatorilor, minim: număr angajați, număr contracte de muncă pe perioadă determinată/part-time, cifră de afaceri, comportament fiscal, grad de conformare la măsuri corective anterioare etc și alte activități utilizând o combinație de reguli de business, de detectare a anomaliilor și tehnici analitice avansate
- Folosirea de date istorice pentru a dobândi o cunoaștere profundă a comportamentului și pentru a determina dacă anumite activități este probabil să aibă loc, luând în considerare acțiunile anterioare, istorice
- Realizarea de modele comportamentale pentru entitate și realizarea de peer group analysis pentru entități similare
- Generarea de alerte pentru comportamente și activități dubioase
- Configurarea regulilor și a altor parametri prin care este realizată detectarea de către utilizatorii sistemului.

3.2.5.6.2.2 Generarea alertelor

Modulul trebuie să includă o componentă de generarea a alertelor, care vizualizează alerte, le asociază entităților și le asigură inspectorilor/factorilor decizionali o perspectivă mai completă asupra riscului unei entități sau tranzacții. Modulul trebuie să asigure minim:

- Calcularea scorului de risc - Fiecărei alerte i se va aloca un scor de risc în funcție de caracteristicile specifice ale activității, cu coduri de motiv transparente și explicații privind motivul generării alertei.
- Prioritizarea alertei - Alertele ar trebui să fie prioritizate prin scor și severitate, și direcționate spre utilizatori de sistem/grupuri potriviți(te).
- Alocarea alertei - fluxul trebuie să poată să aloce automatizat alertele către grupuri prestabilite de inspectori sau analiști, în funcție de regulile și cerințele decise de către utilizatori.

Modulul trebuie să pemrită analiza datelor, cuprinzand minim următoarele funcționalități:

- Să permită realizarea de analize de risc specifice (grup de angajatori, domenii de activitate, zone geografice, etc.) prin procesarea datelor aflate la dispoziția IM (surse interne și externe);
- Să furnizeze analize avansate pentru a selecta din mai multe surse de date informații despre factorii de risc asociați cu normele din legislația muncii , tendințele și modelele comportamentului angajatorilor legate de conformare la legislația muncii , plăți, nivel de declarare etc.
- Să permită dezvoltarea și introducerea de reguli și atenționări personalizate în sistem pentru a evidenția ariile de risc pentru a sorta datele în funcție de risc și alte atribute;
- Să ofere o interfață grafică și un tablou de bord interactiv, modalitate flexibilă de vizualizare a datelor, query builder cu funcții de drag and drop, sample, drill, pivot și filtrare directă a datelor de analizat;
- Să ofere utilizatorului machete, sa permita utilizarea informațiilor din registrul riscurilor, a indicatorilor de risc, precum și posibilitatea stabilirii unor parametri pentru aplicarea indicatorilor de risc

- Să creeze și să mențină profiluri de risc, să stocheze valorile indicatorilor de risc utilizati la determinarea profilurilor de risc, regulile si rezultatele evaluării riscului în baza de date privind indicatorii de risc, utilizând o combinație de tehnici de potrivire precum meta-caractere, dicționar, calcule și formule.
- Solutia trebuie să fie integrata cu alte funcții ale IM care utilizează analiza de risc
- Să ofere utilizatorului capabilități de analiză de risc predictivă.
- Să ofere posibilitatea de analiza de risc individuala in care sa fie extrase toate informatiile pentru un angajator (CUI) centralizate intr-un document (de exemplu, "Fisa de risc la legislația muncii") cu preluarea inclusiv a informatiei referitoare la clasa de risc in care este incadrat angajatorul. Documentul va cuprinde tabele, rapoarte, butoane de comanda pentru generare date, link-uri, pop-up-uri, ferestre de dialog, situatii extrase, in functie de volumul datelor continute de fiecare informatie cat si de necesitatea analizei de risc.
- Să existe posibilitatea efectuării unei analize de risc individuale, pentru interpretarea datelor centralizate in cadrul unui raport ce va cuprinde pentru fiecare subcapitol campuri editabile de "Observatii" ce vor fi completate de catre personalul specializat din cadul structurilor de analiza de risc, in functie de analiza efectuata asupra datelor/informatiilor.
- Să efectueze analize de risc multi-CUI, pentru o lista de angajatori identificati dupa un anumit criteriu predefinit de catre utilizator si care sa emita rapoarte, interogari, analize asupra carora se pot formula conditii, functii matematice, statistice, logice, etc necesare efectuarii unei analize de risc asupra angajatorilor supusi interogarii. Acest modul va permite analiza angajatorilor pe domenii de activitate, pe specific legislativ, precum si pentru anumite tipuri de date conexe legislației. Modulul va cuprinde functii predefinite (logice, statistice, matematice), iar variabilele vor fi selectate sub sub forma unor butoane pop-up din cadrul datelor regasite in aplicatiile conexate.
- Să realizeze analiza de risc pentru stabilirea riscului de neconformare la normele legislației muncii, etapă preliminară a activității de verificare a conformării la legislația muncii a angajatorului.
- Să permită extragerea și integrarea informațiilor din fișa de feedback analiza de risc vs verificare verificare documentară;

3.2.5.6.2.3 Web crawler

Această subcomponentă va asigura colectarea de date specifice platformelor de recrutare/instruire SSM online, date ce vor fi utilizate și integrate în analizele de risc realizate de IM.

Subcomponenta nu va genera costuri recurente pentru Beneficiar, va fi dezvoltată și configurată astfel încât să asigure minim:

- Scanarea și stocarea metadatelor provenite din mediul on-line pentru a crea un set de date vizat;
- O interfață ușor de utilizat pentru personalul fără abilități tehnice de programare (non-coders utilizatorul final);
- Posibilitatea utilizatorului de a-si crea propriile mecanisme pentru a colecta datele dorite de pe orice site web, inclusiv de pe site-uri complexe;
- Structurarea datelor colectate în formate standard, minim Excel, HTML și CSV precum și posibilitatea injectării acestora în baza de date prin mecanisme de tip API;
- Extragerea de date dinamice in timp real despre angajatori, clasamente, comentarii, postări sociale etc;

- Capacitatea de a utiliza o colecție de adrese IP în solicitările de colectare a datelor;
- Înglobeze tehnologii de învățare automată care sa poată citi, analiza și apoi transforma documentele web în date relevante;
- Sa beneficieze de o configurație care să permită curățarea automată a datelor;
- Sa includa un proxy rotator inteligent pentru a permite accesarea, ocoli ReCaptcha și blocarea bypass-ului de catre serverele web si maximizarea vitezei;
- Sa permita utilizatorilor să programeze task-urile (agenti automati) pentru a rula la o anumită oră sau repeta secvența în fiecare minut, zi, săptămână, lună, an, etc;
- Integrarea datelor colectate în modulul de evaluare risc
- Sa permita selectia numărului de conexiuni de deschis simultan si sa ofere posibilitatea anularii sau reluarea descărcărilor întrerupte.

3.2.6 Descriere procese și cerințe funcționale SIAMC 2.0

Implementarea SIAMC 2.0 se va realiza utilizând componentele aplicative solicitate la capitolul 3.2.5 sau prin dezvoltări suplimentare, cu respectarea cerințelor generale, de aliniere la strategii și legislație, precum și arhitecturale ale caietului de sarcini.

În etapele de proiectare și dezvoltare a tuturor modulelor sistemului informatic vor fi luat în considerare prevederile legale, procedurile de organizare internă/a activităților de control, formularele standard și/sau orice alte prevederi ce reglementează activitatea IM/ITM în vigoare la momentul implementării, chiar dacă acestea nu au fost specific inventariate și menționate în documentele de analiză a nevoilor sau proiectare de nivel înalt a sistemului.

3.2.6.1 Monitorizare și Control

3.2.6.1.1 Preambul

Acest capitol prezintă succint modalitatea actuală de realizare a activităților de monitorizare și control din cadrul Inspecției Muncii și Inspectoratelor Teritoriale de Muncă, în scopul asigurării respectării și prevenirii încălcărilor dispozițiilor legale referitoare la relațiile de muncă, securitatea si sanatatea in munca și/sau alte obligații ale agenților economici, stabilite prin acte normative cu caracter special. Efectuarea activităților de control este reglementată la nivel de instituție prin intermediul procedurilor operaționale, care prezintă în mod formalizat, toți pașii care trebuie urmați, a metodelor de lucru stabilite și a regulilor de aplicat în vederea realizării activităților de control.

Se consideră următoarele categorii de activități de control:

- **Controlul de fond/sistem** – Acest gen de control are ca obiectiv verificarea modului în care angajatorii aplica ~~aplică~~ prevederile legislației muncii și a clauzelor din contractele colective de muncă, precum și realizarea unei analize de ansamblu a activității în domeniul relațiilor de munca si/sau al securitatii si sanatatii in munca, în vederea eliminării deficientelor constatate și conștientizării angajatorului pentru respectarea legislației muncii. Este un control care tinde să acopere prin obiectivele sale întreaga problematică a raporturilor de muncă dintr-o unitate și care, de regulă, este un control planificat la unități cu un număr semnificativ de salariați sau cu deficiențe majore în activitate, rezultate din controalele precedente. Acest gen de control poate fi efectuat în domeniul relațiilor de muncă, in domeniul securitatii si sanatatii in munca, sau în echipa complexă vizând atât problematica relațiilor de muncă (RM) cât și cea a securității și sănătății în munca (SSM), caz în care cooperarea între serviciul control RM și serviciul SSM se impune cu necesitate și începe prin planificarea lunară a acțiunilor de control și stabilirea

echipelor complexe de control având în componenta specialiști din ambele domenii de activitate.

- **Controlul tematic** – Este un control care acoperă un număr limitat de domenii (tematici) din cele reglementate de legislația muncii și se desfășoară într-o scurta perioadă de timp. Aceste tipuri de controale oferă o imagine parțială a modului de organizare și desfășurare a activității angajatorului, concludentă însă asupra problemei care constituie tema controlului.
- **Controlul inopinat -** are ca obiectiv verificarea punctuală a unei stări, situaţii sau a unor consecinţe determinate de încălcarea directă de către entitatea controlată, ori de către personalul său, a unei reglementări care lezează grav un interes legitim, public sau privat.
- **Controlul tip campanie –** controlul efectuat in cadrul campaniilor organizate la nivel nationl sau local, targhetate pe criterii stabilite in metodologia aferenta campaniei.

În cele ce urmează este prezentată în mod succint modalitatea actuală de planificare și realizare a unui control. În vederea îndeplinirii obiectivelor proiectului, în timpul etapei de analiză și proiectare a noului SIAMC 2.0, se vor stabili procedurile de lucru care vor fi implementate, formularele și documentele care vor fi utilizate, precum și întregul circuit a documentelor aferent acestor procese. Se va avea în vedere faptul că activitățile de control se desfășoară preponderent pe teren, inspectorii de muncă urmând a beneficia de o soluție informatică accesibilă de pe dispozitive mobile capabilă să ofere toate funcționalitățile necesare. De asemenea, după finalizarea implementării proiectului, majoritatea activităților care la momentul actual se desfășoară pe teren sau la ghișeu, se vor efectua prin intermediul SIAMC 2.0, eficientizând astfel interacțiunea intre IM/ITM și agenti economici/cetățeni.

Planificarea acțiunilor de control

În mod general, următoarele documente stau la baza planificării acțiunilor de control:

- **Programul cadru anual de acțiuni al Inspecției Muncii** – documentul întocmit la sfârșitul anului pentru anul următor în care sunt stabilite: acțiunile directoare privind activitatea Inspecției Muncii, responsabilitatea realizării, termenul, coordonarea și monitorizarea acestora. Programul cadru de acțiuni al Inspecției Muncii stă la baza întocmirii programelor proprii anuale de acțiuni ale inspectoratelor teritoriale de muncă;
- **Programul propriu anual de acțiuni al inspectoratului** – documentul întocmit in baza Programului cadru anual de acțiuni al Inspecției Muncii la sfârșitul anului pentru anul următor, aprobat de către inspectorul general de stat, care stă la baza organizării și desfășurării activității de control, în domeniul relațiilor de muncă si al securitatii si sanatatii in munca a inspectoratului.
- **Plan anual de control** – documentul care se elaborează după aprobarea Programului cadru anual de acțiuni pentru ITM.
- **Acțiuni/Campanii organizate la nivel national sau local** – acțiuni de control în domeniul relațiilor de muncă si al securitatii si sanatatii in munca organizate la nivel local în urma analizei de risc efectuată întru-un anumit sector de activitate specific zonei.
- **Sesizări** – cererea, reclamația, sesizarea sau propunerea formulată în scris ori prin poșta electronică, pe care un cetățean sau o organizație legal constituită o poate adresa autorităților și instituțiilor publice centrale și locale.
- **Protocol de colaborare/plan comun de acțiuni** – acorduri încheiate la nivelul Inspecției Muncii sau a inspectoratelor teritoriale de muncă prin care sunt stabiliți termenii și condițiile efectuării de inspecții comune interinstituționale.
- **Solicitări de cooptare la acțiuni de control** – participarea la acțiunile de control inițiate de alte autorități sau instituții publice centrale și locale la care sunt solicitați să participe și inspectorii de muncă.

Pregătirea acțiunilor de control

La momentul actual, premergător deplasării la sediul social/punct de lucru al angajatorului/agentului economic controlat, inspectorul de muncă efectuează următoarele verificări**:**

- Petiții și sesizări, informații, evenimente/accidente, adrese sau memorii primite de la persoane fizice și juridice, solicitări primite de la alte instituții publice.
- Obiectul de activitate al angajatorului/agentului economic vizat pentru acțiunea de control;
- Consultarea Sistemului informatic integrat de gestionare a datelor COLUMBO/SIAMC în vederea verificării istoricului de controale efectuate la angajatorul/agentul economic vizat pentru control și a măsurilor dispuse în controalele anterioare;
- Consultarea Registrului general de evidenta a salariatilor
- Consultarea bazei de date a Oficiului National al Registrului Comerțului - portal ONRC online privind statutul agentului, respectiv datele de identificare și adresa sediului social/puncte de lucru declarate;
- Consultarea altor baze publice de date specifice, la care inspectorii de muncă au acces, respectiv alte resurse disponibile online (pagina de internet a unității vizate, alte informații publice);
- Informații, registre/documente deținute de alte servicii și compartimente din cadrul ITM, sau alte instituții publice, după caz. În situația organizării unor acțiuni de control, efectuate în cooperare cu alte instituții, se realizează o documentare prealabilă (schimb de informații), avându-se în vedere metodologiile de control sau protocoalele încheiate cu instituțiile colaboratoare. În funcție de specificul acțiunii de control, conducerea inspectoratului desemnează o persoană de contact, din cadrul inspectoratului, care să furnizeze informații inspectorilor de muncă aflați pe teren.

Anterior plecării în deplasare inspectorii de muncă, precum și alte categorii de personal, întocmesc **Ordinul de Deplasare** consemnând denumirea entității care urmează a fi controlată, sau, când aceasta nu se cunoaște se menționează strada/zonă comercială/codul CAEN și/sau o zonă bine delimitată, îl prezintă spre aprobare conducătorului instituției și se înregistrează în **Registrul de delegații**. Completarea **Registrului de Delegații** pentru înregistrarea ordinelor de deplasare se va face astfel încât să se regăsească obligatoriu denumirea angajatorului/angajatorilor la care urmează a se efectua controlul, sau, când aceasta nu se cunoaște se menționează strada/zonă comercială/codul CAEN și/sau o zonă bine delimitată, data, numele inspectorilor de muncă din echipa de control, sau orice alte date necesare în funcție de specificul activității. În condițiile în care acțiunea de control urmează să fie definitivată ulterior, după data inițierii și implică o nouă deplasare, se va completa un nou ordin de delegare/deplasare cu mențiunea scopului si a duratei deplasării.

În tematica de control se evidențiază obiectivele controlului, cu indicarea actului normativ și dispozițiilor acestuia care fac obiectul verificărilor. În cazul în care, urmare unei situații de fapt, sunt indicii de încălcare a altor prevederi legale decât cele stabilite inițial, inspectorii de muncă pot extinde verificările și perioada controlată prin solicitarea și a altor documente, cu consemnarea acestui fapt în actul de control.

Efectuarea controlului

La momentul actual, inspectorii de muncă au obligația de a se deplasa la unitatea/ locația menționată în ordinul de deplasare, la sediul social si/sau la orice punct de lucru al unității, sau orice alt loc de muncă organizat de persoane fizice sau juridice, aflat pe teritoriul de competenta. Aceștia se prezintă, se legitimează și comunică obiectivul controlului. După legitimare și prezentarea tematicii de control, inspectorul de muncă solicită **Registrul Unic de Control** (acolo unde este posibil) și înscrie toate elementele prevăzute de acesta și solicită documentele de înființare a entității și a altor informații legate de aceasta (verificarea denumirii exacte, a adresei, a codului unic de înregistrare și a numărului de înmatriculare la Registrul Comerțului, forma de capital, activitatea principală și codul CAEN, numele și prenumele conducătorului unității/reprezentantul legal al acesteia, etc.).

În situația în care la locația stabilită pentru control nu este identificată entitatea înscrisă în ordinul de deplasare (ex. locație închisă, în locația respectivă desfășoară activitate o altă entitate, etc.), inspectorul de muncă întocmește în ziua lucrătoare următoare o **Notă de Deplasare** care se înregistrează în **Registrul General al Inspectoratului**, în care se menționează detaliat situația de fapt, notă care se înaintează spre informare șefului ierarhic, urmând a se realiza procedura de comunicare a înștiințării. Nota de deplasare se arhivează de către inspectorul de muncă la dosarul cu actele de control aferente.

Inspectorul de muncă procedează la înștiințarea, în scris, a entității ce urmează a face obiectul controlului cu privire la data, locația și ora prezentării cu documentele necesare efectuării inspecției. După caz, înștiințarea se înmânează sub semnătură/ comunică angajatorului/ reprezentantului legal al acestuia/ persoanei aflata la locul de muncă controlat sau prin poștă. În cazul în care la locul de muncă verificat nu se află nici o persoană din cadrul entității controlate căreia să i se înmâneze înștiințarea, sau, deși este prezentă, refuză să o primească, comunicarea acesteia se realizează prin poștă (curierat), cu confirmare de primire, la sediul angajatorului sau la domiciliul angajatorului persoană fizică. În cazul în care comunicarea prin poștă nu este realizată în termen de 20 de zile calendaristice de la trimitere, se procedează la **afișarea înștiințării** la sediul / domiciliul angajatorului / reprezentantului legal al acestuia. Comunicarea se consemnează într-un **Proces-Verbal de Afișare**, care se semnează de către inspectorii de muncă ce efectuează afișarea, in prezenta unui martor, care vor proceda și la fotografierea locului afișării; procesul verbal de afisare va fi semnat si de martorul prezent la afisare. Fotografiile vor fi anexate la procesul – verbal de afișare. Termenul stabilit prin înștiințarea afișată pentru prezentarea documentelor solicitate este de maxim 5 zile lucrătoare. În mod excepțional, în cazul în care, din motive obiective, reprezentanții legali ai entității vizată pentru control nu se pot prezenta cu actele necesare definitivării controlului, la data stabilită prin înștiințare sau alte motive obiective care țin de activitatea inspectorului de muncă, acesta stabilește o dată cât mai apropiată la care va avea loc verificarea și implicit încheierea procesului verbal de control.

Efectuarea verificărilor și aplicarea sancțiunilor

Prin verificarea documentelor originale, ale entității controlate, verificările vizuale ale echipamentelor de munca/condițiilor de munca, existente la fata locului, inspectorul de muncă constată modul în care sunt respectate toate prevederile actului normativ, aflate în sarcina entității controlate, parcurgând fiecare prevedere în parte. Constatările se menționează în **anexa procesului verbal de control**, pe baza analizării documentelor supuse controlului și vor fi structurate corespunzător punctelor din tematica de control, orice constatare consemnată în actul de control fiind însoțită de justificarea rezultată din documentele verificate. Constatările vor fi complete și clare, susținute de exemple punctuale cu referirile la actul normativ, incluzând articolul și aliniatul invocat.

În cazul în care s-au reținut abateri de natura infracțională, inspectorul de muncă care a întocmit **procesul verbal de control** sesizează organul de urmărire penală competent, atașând o copie a procesului-verbal de control întocmit, și va informa despre acest lucru pe inspectorul șef. Dovada sesizării organului de urmărire penală se păstrează împreună cu documentul cu regim special.

În cazul în care documentele întocmite de inspectorii de muncă au fost contestate în instanță, compartimentul juridic al ITM va putea solicita și obține documente, copii ale acestora, precum și, după caz, orice informații necesare formulării apărării.

Prin sondaj documentele rezultate în urma controlului, întocmite de către inspectorii de munca vor fi analizate, după caz, de către inspectorul șef adjunct/șeful de serviciu, conform atribuțiilor din fișa postului și a prevederilor Regulamentului de Organizare și Funcționare al ITM.

Inspectorul de muncă în gestiunea căruia se află procesul-verbal de constatare și sancționare a contravențiilor va avea responsabilitatea comunicării acestuia, potrivit prevederilor legale, organelor de specialitate ale unităților subordonate Ministerului Finanțelor Publice – Agenția Națională de Administrare Fiscala (ANAF).

Documente specifice acțiunilor de control

La nivelul ITM există o serie de documente, cu sau fără regim special necesare desfășurării acțiunilor de control:

- **Legitimația de control și insigna** – reprezintă însemnele prin care inspectorul de muncă face dovada, în fața entității controlate, cu privire la identitatea să și cu privire la instituția la care este încadrat ca funcționar public și îi conferă acestuia drepturile prevăzute de lege;
- **Ordinul de deplasare** – reprezintă formularul tipizat, fără regim special care justifică deplasarea în interes de serviciu;
- **Tematica de control** – documentul în care se stabilesc obiectivele controlului derivate din obligațiile pe care le stabilește actul normativ special în sarcina agentului economic controlat;
- **Înștiințarea** – formularul cu regim special prin care reprezentantul angajatorului/agentului economic controlat este convocat să prezinte documentele la sediul acestuia sau la sediul inspectoratului teritorial de muncă, cu precizarea datei, orei și a documentelor solicitate.
- **Proces verbal de control** – formularul cu regim special care se utilizează în activitatea de control de către inspectorii de muncă și în care se consemnează: date referitoare la inspectorul de muncă (nume și prenume, instituția din care face parte inspectorul de muncă, nr. legitimației de control), denumirea angajatorului/agentului economic controlat și datele de identificare ale acestuia, adresa locului de muncă/punctului de lucru, reprezentantul legal al unității, persoana delegată, alți participanți, perioada controlului, obiectivele controlului, termenul de comunicare a modului în care au fost remediate deficiențele constatate, condițiile în care documentul poate fi contestat, numărul de exemplare în care s-a întocmit, precum și nr. și data înregistrării în registrul unic de control;
- **Anexa la procesul verbal de control, de constatare și de măsuri dispuse în domeniul securitatii si sanatatii in munca** si in domeniul relatiilor de munca - formularul tipizat în care se consemnează de către inspectorii de muncă aspectele verificate, neconformitățile constatate, cu precizarea dispozițiilor legale încălcate și a măsurilor dispuse, precum și a termenului de remediere a deficiențelor. Anexa va avea seria și numărul procesului-verbal de control pe fiecare pagină și va fi semnată de inspectorii de muncă și, atunci când este prezent, și de către reprezentantul angajatorului/agentului economic controlat;
- **Procesul verbal de sistare a activitatii / de oprire din functiune a echipamentelor de munca -** formularul cu regim special prin care se dispune sistarea activitatii sau oprirea din functiune a echipamentelor de munca;
- **Proces verbal de constatare și sancționare a contravențiilor** – formularul cu regim special, care se completează de către inspectorii de muncă, potrivit dispozițiilor Ordonanței Guvernului nr.2/2001 privind regimul juridic al contravențiilor, cu modificările și completările ulterioare;
- **Anexa la procesul verbal de constatare și sancționare a contravențiilor** – formularul care se întocmește de către inspectorii de muncă în completarea spațiului existent pe formularul cu regim special destinat descrierii faptei și care constituie parte integrantă a procesului-verbal de constatare și sancționare a contravențiilor. Anexa va avea seria și numărul procesului-verbal de constatare și sancționare a contravențiilor pe fiecare pagină și va conține semnăturile conform OG nr.2/2001, cu modificările și completările ulterioare;
- **Procesul verbal de ridicare documente** – formularul tipizat în care sunt menționate documentele care se ridică în original de la locația supusă controlului, document care este semnat de către inspectorii de muncă și de către persoana care le-a pus la dispoziție;
- **Notă de deplasare privind acțiunea inițiată/desfășurată, dar nefinalizată prin încheierea unui proces verbal de control** – un document unilateral încheiat de inspectorii de muncă, în care se

consemnează detaliat situația de fapt întâlnită pe teren și care a condus la imposibilitatea identificării unui sediu social sau lucrativ.

- **Înscrisurile care se atașează la procesul verbal de control** – xerocopii ale documentelor emise de angajatorul/agentul economic verificat și care stau la baza constatărilor și a măsurilor dispuse;
- **Proces-verbal de afișare** – înscrisul prin care inspectorii de muncă fac dovada comunicării prin afișare a unui document/act administrativ (înștiințare, proces verbal de control, proces - verbal de constatare și sancționare a contravenților).

- **Imputernicire**-formular tipizat prin care angajatorul/reprezentantul legal desemneaza persoana care il reprezinta in relatia cu ITM-ul, semnatura acestuia fiindu-i opozabila.

- **Fisa cu date de identificare** –formular tipizat care se completeaza la angajator la data efectuarii controlului in care sunt inscrise elemente de identificare ale unitatii controlate (ex. date de contact, adresa sediu social, adrese puncte de lucru, activitati desfasurate, organizarea activitatii de ssm, categorii de personal autorizat, accidente înregistrate de angajator, s.a)

- **Fișa de identificare** - formularul tipizat, utilizat de inspectorul de muncă în vederea identificării persoanelor care desfăşoară activitate la locul de muncă verificat, care se atașează la procesul verbal de control, fără a fi anexă la acesta.

- **Proces-verbal de identificare** - înscrisul în care echipa de control consemnează datele persoanelor care desfăşoară activitate la momentul verificării locului de muncă, pentru care nu a fost posibilă identificarea prin fişa de identificare. Acesta va cuprinde cel puțin următoarele elemente: data și ora la care se încheie, adresa locului de muncă supus verificării, numele și prenumele persoanelor identificate, denumirea angajatorului pentru care desfășoară activitate persoanele identificate conform celor declarate de acestea alte date de identificare obținute din documentele la care au acces, activitatea prestată de aceste persoane, elementele declarate verbal de acestea (ex: data de când lucrează, salariul, etc.), descrierea succintă a împrejurării care a determinat utilizarea acestei metode de identificare (ex: nu știe să scrie, nu vorbește limba română, etc.), numele, prenumele/funcția și instituția din care fac parte reprezentanții organelor de control care realizează identificarea.

În ceea ce privește formularele cu regim special, se vor avea în vedere procedurile operaționale specifice privind utilizarea acestora în derularea activităților de control. Sistemul va permite definirea unor fluxuri de lucru care vor transpune aceste proceduri operaționale, inclusiv în ceea ce privește înregistrarea în registre gestionate distinct a fiecărui tip de formular cu regim special.

3.2.6.1.2 <u>Cerințe funcționale</u>

Scopul acestui modul este de a eficientiza activitatea de control a Inspecției Muncii și Inspectoratelor Teritoriale de Muncă, în ceea ce privește planificarea, pregătirea și realizarea activității de control, inclusiv înregistrarea și comunicarea tuturor documentelor rezultate către entitatea controlată în mod securizat, prin folosirea semnăturii electronice. Se va avea în vedere faptul că activitatea de control se desfășoară pe teren, fiind necesar accesul în mod securizat de pe dispozitive mobile la toate informațiile specifice controlului.

Prestatorul va asigura implementarea procedurilor, documentelor, șabloanelor, notificărilor și constrângerilor existente la momentul derulării proiectului.

Acest modul va dispune de o zonă publică (front-office), accesibilă prin intermediul portalului web, dedicată operatorilor economici (angajatorilor) și cetățenilor, precum și de o zonă privată (back-office)

dedicată personalului din cadrul IM/ITM. Accesul va fi posibil numai după autentificare, iar informațiile afișate vor depinde de rolului utilizatorului conectat în sistem.

Sistemul va permite:

- Accesul utilizatorilor externi (operatori economici / angajatori, cetățeni) pe baza contului de utilizator folosit pentru conectarea la REGES-ONLINE. Utilizatorii externi vor urma procedura de înrolare stabilită la nivel de ITM în vederea obținerii detaliilor de acces.
- Accesul utilizatorilor interni (personal IM/ITM) pe baza contului de utilizator folosit la nivel de instituție.
- Configurarea setului de permisiuni la nivel de modul, cu definirea tipurilor de rolului și a grupurilor de acces, atât pentru utilizatorii interni (de exemplu: drepturi de validare documente doar pentru inspectorii de muncă din compartimentul SSM, drepturi de vizualizare pentru toți inspectorii) cât și pentru utilizatorii externi
- Definirea tuturor tipurilor de documente și formulare specifice acțiunilor de control, a metadatelor minime necesare a fi completate în cadrul sistemului, precum și a fluxului de procesare. Lista tipurilor de documente ce vor fi disponibile în cadrul sistemului și toate informațiile asociate vor fi definitivate în cadrul etapei de analiză a proiectului.
- Separarea din punct de vedere logic a diferitelor tipuri de control, pentru a respecta structurile interne ale instituțiilor (de exemplu: un inspector de muncă din zona RM, va vedea cu precădere informațiile specifice acestui tip de controale).
- Gestiunea formularelor tipizate și celor cu regim special, având în vedere procedurile interne privind regimul și circuitul documentelor în domeniul relațiilor de muncă, al securitatii si sanatatii in munca si al supravegherii pietei produselor.
- Completarea documentelor direct în cadrul unor formulare web, fără a fi nevoie descărcarea formularului tipizat. Semnarea documentelor în format electronic, sau încărcarea unor documente scanate care prezintă semnături olograf. Se vor avea în vedere cel puțin documentele menționate în capitolele anterioare.
- Încărcarea documentelor completate în afara sistemului, inclusiv documente suport, acolo unde este cazul. Modulul trebuie să permită încărcarea documentelor inclusiv de pe dispozitive mobile. În cazul formularelor tipizate scanate și încărcate în cadrul sistemului, se vor putea extrage în mod automat anumite metadate pentru a permite indexarea și regăsirea lor ulterioară.
- Vizualizarea tuturor documentelor încărcate anterior. Va permite modificarea sau ștergerea documentelor și a anexelor, cu respectarea ciclului de viață al fiecărui tip document.
- Validarea completării tuturor informațiilor necesare cu integrarea sistemelor ITM și a altor sisteme terțe cu care este necesară integrarea. În cazul în care nu este posibilă realizarea unei validări automate (de exemplu: eroare de conexiune cu un sistem terț sau informații indisponibile), acest lucru va fi marcat vizual, dar nu va împiedica transmiterea documentelor pe flux. Pentru fiecare din sistemele terțe cu care este necesară integrarea, Beneficiarul va realiza demersurile administrative necesare obținerii acordului proprietarului sistemului pentru realizarea interoperabilității. Prestatorul trebuie să asigure suportul tehnic.
- Atenționarea utilizatorului în mod vizual și prin mesaje de eroare clare asupra erorilor de completare a documentelor (informații sau anexe lipsă, câmpuri necompletate sau completate necorespunzător)
- Urmărirea statusului documentelor transmise spre procesare în mod vizual. Fiecare etapă de validare va fi definită ca un pas într-un proces fiind posibilă astfel vizualizarea întregului flux al documentului atât pentru etapele automate, cât și pentru acelea unde este necesară procesarea de către un operator.

- Transmiterea notificărilor în mod automat conform fluxului definit de procesare a fiecărui tip de document. Notificările vor putea fi transmise direct in sistem si prin email. Notificările vor putea fi transmise către un utilizator sau către un grup de utilizatori, în funcție de fluxul definit la momentul implementării.
- Planificarea acțiunilor de control
    - Utilizarea de mecanisme de analiză și propunere pentru sprijinirea construirii planurilor anuale pornind de la Planul cadru (liniile directoare stabilite de către IM
    - Utilizarea unui mecanism de identificare a angajatorilor care îndeplinesc criteriile de control, de exemplu prin stabilirea unui indice de prioritate pentru control
        - Acest indice va putea fi stabilit pe categorii (RM, SSM) – astfel încât să rezulte prioritatea instituțiile pentru activitatea de control
        - Exemple de criterii pentru stabilirea indicatorului:
            - Numărul angajaților – "firma are mai mult de X angajați"
            - Cât de periculoasă este pentru lucrători Activitatea desfasurata
            - existența, in cadrul angajatorului respectiv, de Grupuri sensibile la riscuri(tineri, femei, gravide, persoane vârstnice, cu dizabilități s.a.
            - Sesizari, reclamatii
            - Societati care au fost identificate ca folosesc munca nedeclarata sau subdeclarata
            - Societati nou infiintate
            - Societati din categoriile de activitati prevazute in anexa 5 din HG 1425/2006 - activități industriale
            - Frecvența controalelor efectuate – "Firma nu a mai fost controlată de x ani/luni"
            - Gradul de realizare a măsurilor dispuse în urma activităților de control
            - Nr-ul/frecvența accidentelor pe o perioadă de timp
            - Deținerea autorizațiilor specifice (SSM)
            - Situația depunerii declarațiilor 112
            - Cifra de afaceri
            - Arie geografica
        - Selectarea criteriilor și generarea indicelui de control se va realiza la nivelul ITM
        - Posibilitatea sprijinirii distribuirii firmelor către inspectori astfel încât:
            - propunerea de distribuirea a firmelor să se facă automat pe baza criteriilor respective (de exemplu cod CAEN) – dar inspectorul să poată edita și confirma varianta finală – care va merge spre aprobarea ierarhică
        - Indicele de prioritare control nu va afecta componenta de planificare a ordinii și datei controalelor - inspectorul va putea să selecteze/programeze instituțiile controlate)
    - Posibilitatea determinării fondului de timp existent la nivelul unui inspectorat teritorial de muncă, în funcție de numărul total de inspectori în cadrul fiecărui ITM pentru

control, instruiri, cercetari evenimente, participari la determinari de noxe, CO, CM, alte concedii, programe de perfectionare, lucratri birou, etc.

- Vizualizarea sub formă de calendar a acțiunilor de control planificate, atât la nivel individual (inspector de muncă), cât și la nivel de departament sau inspectorat. Sistemul va permite filtrarea informațiilor afișate după diferite criterii, cum ar fi tematică de control, angajator, status (control în desfășurare, control încheiat etc.).

- Pregătirea acțiunilor de control
  - Inspectorii de muncă vor putea vizualiza toate informațiile necesare pregătirii controlului direct în cadrul sistemului, fără a fi necesară accesarea unor sisteme informatice diferite. Astfel, va fi posibilă vizualizarea în mod centralizat a tuturor informațiilor necesare privind angajatorul / operatorul economic care va fi supus controlului, inclusiv istoricul controalelor efectuate, documentele din sfera RM și SSM asociate angajatorului, eventualele petiții (reclamații, solicitări) care îl menționează. Va fi posibilă adăugarea unor documente și/sau informații suplimentare asociate angajatorului, disponibile pentru consultare ulterioară. Sistemul va permite limitarea posibilității de vizualizare a informațiilor, prin intermediul sistemului de drepturi și permisiuni, cu scopul asigurării confidențialității.
  - Pentru fiecare acțiune de control, va fi început un flux de lucru specific care va include toți pașii necesari de la momentul pregătirii controlului până la finalizarea acestuia. Acest flux de lucru va include diferitele validări privind tipurile de documente care trebuie completate / generate la o anumită etapă și termenele prevăzute de lege. Fluxul de control va fi definit în cadrul etapei de analiză a proiectului, în conformitate cu procedurile operaționale în vigoare în momentul implementării contractului. Se vor avea în vedere cel puțin informațiile prezentate în capitolul anterior.
  - Inspectorii de muncă vor putea declanșa fluxul de control direct în cadrul platformei, cu posibilitatea solicitării de transmitere a documentelor controlate direct în cadrul platformei. Angajatorul va putea va fi notificat cu privire la necesitatea transmiterii documentelor de controlat și va avea posibilitatea de a încărca și transmite toate aceste documente prin platformă (de exemplu: ulterior primirii unei sesizări, inspectorul de muncă va putea solicita angajatorului prezentarea unor documentelor SSM. Angajatorul va fi notificat și va avea putea a încărca și transmite toate documentele solicitate direct în cadrul platformei, fără a fi necesară deplasarea la ghișeu).
  - Toate documentele interne și fluxurile de validare ale acestora (de exemplu: ordin de deplasare, registru de delegații) vor fi realizate în sistem informatic, cu pre-completarea automată a tuturor detaliilor necesare (de exemplu: în cazul unui ordin de deplasare, vor fi pre-completate informațiile privind inspectorul de muncă care inițiază documentul pe flux, nr. legitimație).

- Efectuarea controlului
  - Inspectorii de muncă vor putea accesa toate funcționalitățile sistemului necesare efectuării controlului folosind în principal dispozitive mobile. Aceleași funcționalități vor fi disponibile și prin intermediul dispozitivelor de tip desktop. Între cele doua versiuni ale sistemului nu vor exista diferențe semnificative privind aspectul („look and feel”), prin păstrarea unui design unitar al soluției propuse.
  - Posibilitatea consultării profilului/fișei angajatorului de pe telefon și de listare a fisei angajatorului (ex. pentru situațiile cu conexiune slabă)
  - Autentificarea în versiunea mobilă se va face în mod securizat, folosind aceleași metode și detalii de conectare ca în cea desktop, inclusiv autentificarea cu doi factori.

- Inspectorii de muncă vor avea la dispoziție toate documentele necesare a fi completate în cadrul acțiunii de control. Va fi posibilă completarea documentelor direct în cadrul soluției, prin intermediul unor formulare web, precum și încărcarea oricărui tip de document direct de pe dispozitivul mobil (minim fișiere de tip .jpg/.jpeg).
- Soluția va permite validarea în timp real a informațiilor incluse în formularele specifice acțiunii de control (de exemplu în fișele de identificare este necesară posibilitatea realizării unor validări în timp real privind identitatea persoanei și a statutului de angajat, zilier, ucenic sau stagiar al acesteia, precum orice alte informații considerate relevante disponibile în sistemele informatice ale beneficiarului).
- Soluția va permite notificarea/ înștiințarea angajatorului direct în cadrul sistemului, într-o zonă de notificări, precum și prin intermediul metodei de notificare aleasă de angajator. Va fi posibilă și generarea tuturor documentelor pentru transmiterea prin poștă (curierat), fără a fi necesară reintroducerea informațiilor. Toate aceste evenimente vor fi înregistrate în cadrul sistemului pentru consultarea ulterioară.
- Soluția va permite partajarea informațiilor unui control între două inspectorate teritoriale de muncă în cazul în care angajatorul/agentul economic controlat are sediul social în alt județ decât cel în care există punctul de lucru la care s-a efectuat acțiunea de control, cat si pentru situatia in care controlul se efectueaza in judetul unde are sediul social dar activitatea se desfasoare pe teritoriul altor judete. Inspectorii de muncă din ambele ITM-uri vor avea acces la toate detaliile necesare privind angajatorul, fără a fi necesară duplicarea informațiilor.
- Platforma va permite semnarea electronică a tuturor documentelor generate în cadrul acțiunilor de control și transmiterea în mod securizat angajatorului supus controlului, cu confirmare de primire. Pentru semnarea electronică a documentelor nu va necesară descărcarea și reîncărcarea documentelor în sistem.
- Platforma va permite semnarea olografă a documentelor în timpul acțiunii de control sau, dupa caz, semnarea cu semnatura electronica
- Încărcarea oricărui tip de document privitor unui control primit în mod fizic la ghișeu de către operatorul ITM. Sistemul va permite completarea tuturor informațiilor necesare privind angajatorul pentru care se înregistrează documentul prin selecția acestuia din cadrul unui nomenclator preexistent, precum și asocierea documentului prezentat în format fizic fluxului de lucru de control dacă este cazul.

- Efectuarea verificărilor și aplicarea amenzilor
  - Sistemul va genera automat formularul cu regim special PVC/PVCSC cu serie si numar, cu campurile aferente
  - Sistemul va genera automat formularul cu regim special sistare activitate/oprire din functionare echipamente de munca cu serie si numar, cu campurile aferente
  - Implementarea unui mecanism de completarea a informației privind contul de trezorerie unde se va stinge obligația creată de către amendă – fie automat pe baza unor criterii prestabilite in functie de apartenenta teritoriala (sau completarea de către agentul constatator cu informatiile primite de la angajator cu datele de trezorerie in care se incaseaza alte venituri din amenzi pentru amenzile aplicate persoanelor fizice)
  - Angajatorii vor putea vizualiza în spațiul privat istoricul informațiilor și documentelor asociate acțiunilor de control cărora au fost supuși. Fluxurile de lucru care vor fi implementate vor fi definite în așa fel încât să permită afișarea documentelor necesare doar atunci când este cazul.

- Integrarea cu sistemul informatic al ANAF în vederea transmiterii informațiilor privind amenzile aplicate, precum și înregistrarea efectuării plății, fără a fi nevoie prezentarea dovezii de plată la ghișeu.
- Angajatorii vor putea vizualiza în spațiul privat istoricul informațiile și documentele asociate acțiunilor de control cărora au fost supuși. Fluxurile de lucru care vor fi implementate vor fi definite în așa fel încât să permită afișarea documentelor necesare doar atunci când este cazul.
- Integrarea cu SPV al ANAF pentru comunicarea automata în SPV ANAF a amenzilor/sancțiunilor aplicate, spre informarea atât a operatorului economic cât și a ANAF cu privire la sumele de colectat când este cazul
- Angajatorii vor putea completa sau încărca și transmite către ITM toate tipurile de documente solicitate în timpul unei acțiuni de control. În cazul în care un document a fost deja transmis anterior, în cadrul altei acțiuni de control, se va putea refolosi documentul inițial în cazul în care acesta nu a suferit modificări (de exemplu: actele constitutive ale societății, fisa unitatii, contractul cu serviciul extern de prestari in domeniul ssm), sau încărca un document nou.
- Gestionarea măsurilor dispuse/planului de acțiuni ce trebuie realizat de către angajator în termenele stabilite.
  - Afișarea termenelor și notificarea angajatorului cu un număr definit de zile înainte, cu posibilitatea definirii numărui de zile prin configurarea sistemului
  - Posibilitatea angajatorului de a transmite catre inspectoratul teritorial de munca care a efectuat controlul raspunsul privind modul de îndeplinirea măsurilor prin completarea anumitor date și încărcarea de documente dacă este cazul
  - Fiecare măsură să poată fi asociată logic de PV-ul prin care s-a dispus măsura
- În cazul in care un utilizator (de ex. inspector ITM) a fost inactivat (prin incetarea raporturilor de serviciu, detasare etc.) sa existe un mecanism de modificare a utilizatorului care gestionează dosarul/ monitorizeaza activitatea dpdv al ssm sau rm pentrut angajatorii care au fost controlați de inspectorul inactivat, astfel incat istoricul acestor controale sa poata fi accesate. Conform drepturilor acordate de administrator, inspectorilor si functionarilor cu atributii in acest sens si sa se mentina in toate rapoartele realizate la nivelul institutiei..

- Înregistrarea automată a tuturor documentelor transmise către ITM sau de către ITM în registratura electronică și generarea automată a numărului de înregistrare.
- Generarea și transmiterea automată a formularelor avizate de către ITM către angajator, acolo unde este cazul, în format needitabil, semnat electronic cu semnătură electronică (certificat de sistem).
- Arhivarea electronică a tuturor documentelor procesate în cadrul sistemului, cu posibilitatea consultării ulterioare, conform schemei de roluri și permisiuni, cu posibilitarea generarii de rapoarte in care datele solicitate pot fi extrase din datele arhivate.

Prin sistemul informatic se va genera întregul flux aferent activității de control, de la analiza, evaluare, planificare, programare, inițiere, efectuare verificare și finalizare control prin încheierea documentelor aferente, astfel cum vor fi detaliate în faza de proiectare și dezvoltare a sistemului.

Fluxul de control va include și o fisa de unitate care va cuprinde toate notificările și alertele cu privire la angajatorul supus controlului, precum și istoricul angajatorului respectiv in ambele domenii de activitate rm+ssm (petitii, controale anterioare, constatari, masuri dispuse, sanctiuni, etc).

3.2.6.2 Relații de Muncă (RM)

3.2.6.2.1 <u>Preambul</u>

Inspecția Muncii are următoarele atribuții specifice în domeniul relațiilor de muncă (RM):

- controlează aplicarea reglementărilor legale, generale și speciale, cu privire la încheierea, executarea, modificarea, suspendarea și încetarea contractelor individuale de muncă;
- controlează stabilirea și acordarea drepturilor cuvenite salariaților ce decurg din lege, din contractul colectiv de muncă aplicabil și din contractele individuale de muncă;
- controlează aplicarea măsurilor de respectare a egalității de șanse și de tratament între femei și bărbați;
- asigură la nivel național evidenta muncii prestate în baza contractelor individuale de muncă, prin registrul general de evidentă al salariaților, precum și evidenta zilierilor și a beneficiarilor prestațiilor acestora;
- controlează folosirea forței de muncă, în scopul identificării cazurilor de muncă nedeclarată;
- primește și transmite în sistem informatic, prin inspectoratele teritoriale de muncă, datele depuse de angajatori și beneficiari referitoare la salariați (REGES ONLINE) și la zilieri (Aplicație Zilieri);
- asigură înregistrarea contractelor colective de muncă la nivel de unități și verifică prevederile acestora, potrivit procedurii aprobate de inspectorul general de stat, și conciliază conflictele de muncă declanșate la nivelul unităților;

În vederea demonstrării îndeplinirii obligațiilor legale, angajatorul trebuie să întocmească și să transmită Inspectoratului Teritorial de Muncă de care aparține, în conformitate cu prevederile legale în vigoare o serie de documente, registre, evidențe:

- Evidență Zilieri
    - Registrul Electronic de Evidență a Zilierilor în conformitate cu Legea nr. 52/2011 privind exercitarea unor activitati cu caracter ocazional desfasurate de zilieri, republicată, cu modificările și completările ulterioare și cu prevederile Metodologiei de întocmire si transmitere a Registrului electronic de evidență a zilierilor, precum și înregistrările care se efectuează în acesta, aprobată prin Ordinul ministrului muncii și protecției sociale nr. 1140/2020.
- Contracte de stagiu
    - Evidența contractelor de stagiu
    - Adeverințe privind perioada de stagiu
- Contracte de ucenicie
    - Evidența contractelor de ucenicie
- Contracte de muncă
    - Notificare privind munca de noapte (în conformitate cu Legea 53/2003, art. 125(6))
    - Notificare privind intenția efectuării concedierii colective conform prevederilor art. 69 din Legea nr. 53/2003
    - Notificare privind decizia de aplicare a măsurii de concediere colectivă conform disp. art. 72 din Legea nr. 53/2003
    - Notificări mediere angajări cetățeni români în străinătate

- Notificări privind plasarea forței de muncă conform art. 12 alin. 4 și 5 din Legea nr. 156/2000 (r3)
- Notificări detașare salariați UE/non UE în Romania în baza Legiinr. 16/2017 privind detașarea salariaților în cadrul prestării de servicii transnaționale
- Notificări detașare salariați străini în România potrivit art. 26 din OG 25/2014
- Solicitare evidență avize autorizare repaus săptămânal cumulat

- Notificare privind incheierea Datele aferente contractului de prestări servicii de completare a registrului general de evidență a salariaților și salariați, inclusiv datele de identificare ale prestatorului.
- Înregistrare agenți de plasare a forței de muncă în străinătate și a furnizorilor de servicii de plasare a forţei de muncă
- Notificări sedii secundare ale agenților de plasare a forței de muncă în străinătate
- Depunerea dosarului în vederea înregistrării contractelor colective muncă respective, a acordurilor colective
- Depunerea dosarului în vederea înregistrării actului adițional la CCM sau Acord
- Înregistrarea contractelor colective de muncă
- Înregistrarea acordurilor colective de muncă
- Înregistrarea conflictelor colective de muncă
- Înregistrarea grevelor
  - notificare privind declanşarea şi încetarea grevei se comunică de către organizatorii grevei inspectoratului teritorial de muncă în raza căruia îşi are sediul unitatea în care se declanşează greva
  - adresa cu privire la hotărârea de a declara greva
  - inregistrarea notificarea privind renunţarea la grevă
  - inregistrarea fisei grevei
- Înregistrarea hotărârilor arbitrale
- Înregistrarea copiei dosarului electronic depus de sindicat sau federație, în vederea obținerii reprezentativității
- Emiterea dovezii referitoare la înregistrarea copiei dosarului electronic depus de sindicat sau federație
- Înregistrarea situaţiei cumulative, semnate de reprezentantul legal al confederaţiei patronale, cuprinzând lista federaţiilor patronale afiliate, cu specificarea organizaţiilor patronale şi a unităţilor membre ale acestora, precum şi a numărului total de angajaţi/lucrători al fiecăreia, în vederea certificării de către inspectoratele teritoriale de muncă;
- Înregistrarea solicitării pentru eliberarea certificatului eliberat de Inspecţia Muncii, privind numărul de angajaţi/lucrători ai unităţilor cuprinse în situaţia cumulativă, semnată de reprezentantul legal al federaţiei patronale, cuprinzând lista unităţilor membre pe baza informaţiilor extrase din baza de date organizată la nivelul Inspecţiei Muncii cu registrele generale de evidenţă a salariaţilor depuse de angajatori.

Evidență zilieri

Odată cu intrarea în vigoare a Ordinului ministrului muncii și protecției sociale nr. 1.140/2020, începând cu data de 25 iulie 2020, operatorii economici au obligația să țină evidența zilierilor în Registrul electronic de evidență a zilierilor, prin intermediul aplicației web disponibile în portalul Inspecției Muncii

(https://www.inspectiamuncii.ro:4443/) sau prin intermediul aplicației mobile gratuite Inspecția Muncii (aplicația poate fi descărcată gratuit din Google Play sau AppStore).

Aplicația „Inspecția Muncii/Zilieri" este destinată angajatorilor / operatorilor economici în scopul ținerii evidenței și transmiterii facile către Inspecția Muncii a registrelor de zilieri în vederea monitorizării activităților cu caracter ocazional desfășurate de zilieri. Aceasta permite înregistrarea zilierilor, completarea și transmiterea Registrului electronic de evidență a zilierilor în conformitate cu Legea nr. 52/2011 cu modificările și completările ulterioare. Manualele de utilizare ale celor două versiuni ale aplicației sunt disponibile la https://www.inspectiamuncii.ro/registrul-electronic-de-evidenta-a-zilierilor

Beneficiarul va pune la dispoziția Prestatorului codul sursă al acestei aplicații. Decizia de a îmbunătăți aplicația existentă sau de a dezvolta un nou modul funcțional este la latitudinea Prestatorului.

Beneficiarul va pune la dispoziția Prestatorului codul sursă al aplicațiilor, in vederea dezvoltarii unui nou modul functional în noul sistem informatic.

Contracte de stagiu

Actele normative care stabilesc executarea stagiului de către absolvenții de învățământ superior sunt Legea 335/2013 privind efectuarea stagiului pentru absolvenții de învățământ superior și Hotărârea 473/2014 pentru aprobarea Normelor metodologice de aplicare a prevederilor Legii nr. 335/2013 privind efectuarea stagiului pentru absolvenții de învățământ superior.

Astfel, se reglementează, pentru absolvenții de învățământ superior, perioada de 6 luni de debut în profesie, în conformitate cu prevederile Codului Muncii, cu excepția profesiilor pentru care există reglementări speciale. Legea cuprinde dispoziții privind: organizarea perioadei de stagiu, procedura de evaluare a stagiarului, contractul de stagiu, drepturile și obligațiile părților, finanțarea stagiului, regimul sancționator.

Stagiarul, pe perioada stagiului, prestează muncă în baza unui **contract individual de muncă** și **a contractului de stagiu**. Contractul de stagiu se încheie odată cu încheierea contractului individual de muncă, având o durată de 6 luni, cu excepția situațiilor în care prin legi speciale este prevăzută o altă perioadă de stagiu. Contractul de stagiu se încheie obligatoriu în formă scrisă, în limba română. Obligația de încheiere a contractului de stagiu în formă scrisă revine angajatorului. Modelul-cadru al contractului de stagiu se stabilește prin normele metodologice pentru aplicarea prevederilor Legii nr.335/2013.

La finalul stagiului, angajatorul eliberează **un certificat/o adeverință de finalizare a stagiului** care se vizează de inspectoratul teritorial de muncă în a cărui rază teritorială își are sediul angajatorul.

Fluxul actual de lucru este:

- angajatorul depune contractul de stagiu la ITM-ul de care aparține și primește număr de înregistrează - se eliberează doar o dovada a depunerii
- Ulterior revine cu un întreg dosar care conține informațiile specifice desfășurării stagiului - de exemplu conducătorul de stagiu, documente doveditoare privind îndeplinirea stagiului. Scopul dosarului este avizarea adeverinței emise de angajator pentru cel care execută stagiul. Dosarul este transmis la departamentul RM - șef serviciu – lucrător.
- Lucrătorul introduce datele relevante în sistem – datele colectate din dosar conțin informații în plus față de datele din REGES online
- ITM-ul vizează dosarul

În scop pentru soluție sunt:

- posibilitatea de a adaugă elementele contractului in sistem (pornind din selecția contractului de la REGES) – pentru notificarea inițială
- posibilitatea generării adeverinței eliberate de angajatori si supuse avizării de către ITM din sistem pe baza unui tipizat

- posibilitatea transmiterii si avizării electronice a dosarului cu posibilitatea de solicitare și răspuns la clarificări
- notificarea parților interesate la transmiterea/primirea documentelor/clarificări
- posibilitatea identificarii domeniilor de activitate in care se incheie contractele de stagiu, in vederea elaborarii de politici publice in domeniul muncii in acord cu dinamica pietei muncii.

Contracte de ucenicie

Ucenicia la locul de muncă reprezintă formarea profesională realizată în baza unui contract de ucenicie la locul de muncă. Ucenicia la locul de munca se organizează pentru calificările stabilite prin legislația în vigoare și pentru ocupațiile cuprinse în Clasificarea Ocupațiilor din Romania (COR), pentru care exista standarde de pregătire profesională, respectiv standarde ocupaționale. Formarea profesionala realizata la locul de munca in baza unui contract de ucenicie, se organizează la inițiativa angajatorilor, de furnizori de formare profesionala autorizați în condițiile legii.

Persoana încadrată în muncă în baza contractului de ucenicie are statut de ucenic. Contractul de ucenicie este un contract individual de munca de tip particular, încheiat pe durata determinată, in temeiul căruia o persoana fizică, denumită ucenic, se obligă să se pregătească profesional și să muncească pentru și sub autoritatea unei persoane juridice sau fizice denumite angajator, care se obliga sa ii asigure plata salariului si toate condițiile necesare formarii profesionale. Încheierea, executarea, modificarea, suspendarea si încetarea contractului de ucenicie se fac în condițiile respectării reglementarilor Legii nr. 53/2003 - Codul muncii, republicata, cu modificările si completările ulterioare, referitoare la ucenicie si la contractul individual de munca.

Contractul de ucenicie se încheie obligatoriu in forma scrisa, in limba romana, si se înregistrează in termen de 20 de zile la inspectoratul teritorial de munca județean, respectiv al municipiului București. Obligația de încheiere a contractului de ucenicie, in forma scrisa, revine angajatorului. Anterior începerii activității, contractul de ucenicie se înregistrează si in registrul general de evidenta a salariaților, care se transmite inspectoratului teritorial de munca.

În sistemul actual se tine o evidenta a contractelor de ucenicie si se completează de către ITM câmpurile specifice privind furnizorul de formare, ucenicul ș.a.m.d.

În scopul soluției viitoare sunt:

- Colectarea datelor privind contractul uceniciei de la angajator - în momentul adăugării contractului de ucenicie in REGES
- Crearea unui câmp separat pentru inserarea atât a furnizorului de formare, cât și a angajatorului
- implementarea unei modalități automate de aplicare a dovezii înregistrării la ITM pentru ca apoi dosarul să poată continua parcursul către AJOFM
    - de exemplu eliberarea unui pdf automat cu nr de înregistrare, pentru a-i servi depunătorului
- posibilitatea identificarii functiilor/meseriilor cuprinse in COR pentru care angajatorii asigura formarea profesionala, a domeniilor de activitate in care se incheie contractele de ucenicie, in vederea elaborarii de politici publice in domeniul muncii in acord cu dinamica pietei muncii.
- Evidenta tuturor angajatorilor care incheie contracte de ucenicie.

Contracte de muncă

Toate notificările specifice ce țin de contracte de muncă sunt depuse de către angajatori la ITM-uri, primesc număr de înregistrare și apoi datele documentelor depuse se introduc în actualul sistem de către inspectorii ITM.

Se dorește ca angajatorul să introducă aceste date în momentul producerii lor.

În conformitate cu prevederile legale, angajatorii sunt obligați să transmită către IM/ITM o serie de notificări asociate contractelor de muncă înregistrate în cadrul sistemului REGES Online și anume:

- Notificare privind munca de noapte - Scopul notificării este informarea faptului că în punctul de lucru respectiv se desfășoară muncă de noapte. Angajatorul depune la registratura ITM se programul, locația, dar nu și angajații nominali. Elaborarea unui model tipizat al notificarii care sa cuprinda si mentiunea faptului ca salariatii care vor desfasura munca de noapte au fost supusi unui examen medical gratuit.
- Notificare privind intenția de concediere colectivă
- Notificare privind decizia de aplicare a concedierii colective – Se declară de către angajator prin depunerea la registratura ITM, cu precizarea numărului de salariați, categorii salariați, motiv dar fără precizarea nominală a căror angajați. Crearea posibilitatii sindicatelor sau reprezentantilor salariatilor de a transmite eventuale puncte de vedere asupra masurii de concediere colectiva, inspectoratului teritorial de munca, iar acestea sa se poata conexa deciziei de concediere colectiva.
- Crearea posibilitatii notificare automate a sindicatului în situația prevăzută la art. 72 alin. 5 și 6 din Codul muncii, sau, după caz, în situația prevăzută de art. 73 alin. 3 din Codul muncii
- Mediere angajări cetățeni români în străinătate – Se declară de către angajator prin depunerea la registratura ITM. Se precizează date din punct de vedere statistic pe o perioadă (de exemplu trimestru)
- Detașare salariați UE/non UE în Romania în baza Legii nr. 16/2017și Detașare salariați străini în România potrivit art. 26 din OG 25/2014 – Detașările se referă de obicei la activități pe perioade limitate desfășurate de către salariați străini pe teritoriul României. Reprezentantul legal al angajatorului străin depune la registratura ITM informațiile privind fiecare angajator român beneficiar, cu precizarea numărului de salariați și care sunt aceștia. În scopul soluției sunt:
    - crearea de câmpuri ce trebuie completate în mod obligatoriu pentru a putea transmite notificarea astfel incat sa cuprinda toate campurile stabilite de legislatia nationala
- Evidență avize repaus săptămânal – În cazul unor anumitor tipuri de activități, datorită specificului acestora, repausul săptămânal să fie cumulat (de exemplu în loc de repausul săptămânal de 48 de ore consecutive, în situatii de excepție zilele de repaus săptămânal pot fi acordate cumulat, după o perioadă de activitate continuă ce nu poate depăși 14 zile calendaristice). Angajatorul declară / depune la registratura o solicitare și documentele care atestă natura și programul activităților pentru a primi autorizarea unui astfel de regim de repaus. ITM verifică documentația depusă și emite fie o autorizare, fie o respingere, fie o admitere parțială. Se dorește implementarea unui flux de procesare a solicitărilor cu:
    - depunere online prin completarea datelor și generarea unei solicitări pe baza unui șablon și cu posibilitatea de a adăuga documente justificative
    - posibilitatea solicitării și trimitere a răspunsului la clarificări
    - generarea autorizării electronice cu posibilitatea completării detaliilor de avizare/respingere/admitere parțială de către lucrătorul ITM și semnarea și transmiterea electronică a acestuia
- Contracte de prestarii servicii de completare REGES-ONLINE – Această evidență a angajatorilor care întreprind astfel de activități se va regăsi în REGES Online. În scopul SIAMC este ca lucrătorii RM să poată vedea dacă angajatorul are prestator de servicii, respectiv perioada contractului respectarea obligatiei de a notifica inspectortul teritorial de munca despre incheierea contractelor de prestari servicii in termenul de 3 zile de la data incheierii – fără a sări dintr-un sistem în altul.

- Contracte colective de muncă – Presupune depunerea de către angajator la ITM a contractelor colective de muncă și a actelor adiționale la acestea ori de câte ori se emit în scopul înregistrării de către ITM.
    - Fluxul actual de lucru este:
        - Documentele privind CMM sunt depuse la registratură și în sistemul actual se adaugă documentul de intrare
        - Lucrarea este direcționată către departamentul de RM - șef serviciu / lucrător
        - Inspectorul formalizează decizia (admitere/respingere)
    - În scopul soluției sunt:
        - depunerea electronică de către oricare dintre părțile semnatare cu completarea detaliilor necesare și atașarea documentelor semnate electronic
        - posibilitatea angajatorului de a declara părțile implicate in CCM (reprezentant sindicat sau reprezentantul salariaților)
        - posibilitatea lucrătorului ITM de a:
            - solicita clarificări / completări la dosar
            - genera din sistem pe baza unor tipizate deciziile de înregistrare admitere/respingere
- Dosare pentru obținerea reprezentativității de către Sindicate și de către Patronat. Fluxul actual de lucru presupune:
    - depunerea către reprezentanții Sindicatelor sau ai Patronatelor a documentelor specifice la registratura ITM
        - depunerea documentelor include și o listă a angajatorilor
    - trecerea lucrării prin fluxul de registratura - RM - șef de serviciu - lucrător
    - Lucrătorii ITM introduc datele în sistem și eliberează o dovadă / adeverință Se dorește ca:
        - Sindicatele/patronatele să depună cererea online cu completarea datelor în sistem
            - la selectarea angajatorilor ai căror angajați sunt membrii în sindicat utilizatorul să introducă CIF-ul/CUI-ul angajatorului iar aplicația să preia datele acestuia
        - Configurarea unui flux de procesare eliberarea electronice cu posibilitatea de a solicita calificări si completări
        - Adeverința va fi un tipizat generat de sistem cu posibilitatea de generare / semnare electronica.

3.2.6.2.2 <u>Cerințe funcționale</u>

Scopul acestui modul este de a permite completarea, înregistrarea și gestiunea întregului flux de validare a diferitelor tipurilor de documente (notificări), în vederea îndeplinirii obligațiilor specifice angajatorilor în ceea ce privește Relațiile de Muncă (RM), în conformitate cu cadrul legal în vigoare la momentul implementării sistemului, și pe toată durata perioadei de suport tehnic și garanție ofertată.

Pentru a evita blocajele din perioada de tranziție de la actualul mod de lucru care implică depunerea la ghișeu a documentelor și viitorul mod de lucru informatizat, sistemul va permite angajaților beneficiarului efectuarea tuturor operațiunilor specifice pentru înregistrare corespunzătoare a

documentelor, în conformitate cu procedurile, documentele, șabloanele, notificările și constrângerile în vigoare la momentul derulării proiectului.

Acest modul va dispune de o zonă publică (front-office), accesibilă prin intermediul portalului web, dedicată operatorilor economici (angajatorilor) și cetățenilor, precum și de o zonă privată (back-office) dedicată personalului din cadrul IM/ITM. Accesul va fi posibil numai după autentificare, iar informațiile afișate vor depinde de rolul utilizatorului conectat în sistem.

Sistemul va permite:

- Accesul utilizatorilor externi (operatori economici / angajatori, cetățeni) pe baza contului de utilizator folosit pentru conectarea la REGES Online. Utilizatorii externi vor urma procedura de înrolare stabilită la nivel de ITM în vederea obținerii detaliilor de acces.
- Accesul utilizatorilor interni (personal IM/ITM) se va face pe baza contului de utilizator folosit la nivel de instituție, avându-se în vedere prevederile de securitate la nivel instituțional.
- Configurarea setului de permisiuni la nivel de modul, cu definirea tipurilor de rolulri și a grupurilor de acces, atât pentru utilizatorii interni (de exemplu: drepturi de validare documente doar pentru inspectorii de muncă din compartimentul RM, drepturi de vizualizare pentru toți inspectorii), cât și pentru utilizatorii externi (de exemplu: vizualizare doar a documentelor asociate entității economice gestionate).
- Definirea tuturor tipurilor de documente aflate în aria de acoperire a RM, a metadatelor minime necesare a fi completate în cadrul sistemului, precum și a fluxului de procesare. Lista tipurilor de documente ce vor fi disponibilă în cadrul sistemului și toate informațiile asociate vor fi definitivate în cadrul etapei de analiză a proiectului.
- Vizualizarea de către angajatori tipurilor de documente care trebuie completate și posibilitatea descărcării formularelor tipizate aferente acestor tipuri de documente.
- Încărcarea și gestionarea prin sistem a contractelor colective de muncă si a actelor aditionale ale acestora depuse la ITM
- Completarea documentelor direct în cadrul unor formulare web, fără a fi nevoie descărcarea formularului tipizat. Semnarea documentelor în format electronic, și încărcarea unor documente scanate care prezintă semnături olograf, în funcție de decizia de implementare.
- În cazul documentelor de tip registru (de exemplu, Registrul de evidență zilieri, Evidența contractelor de stagiu / ucenicie), vor fi posibile următoarele acțiuni:
    - Vizualizarea registrelor transmise anterior (Istoric). Va fi posibilă refolosirea unui anumit registru, prin preluarea tuturor informațiilor deja introduse și crearea unei noi versiuni a registrului. Registrul inițial deja transmis nu va fi modificat.
    - Refolosirea detaliilor (de exemplu, informațiilor pentru fiecare zilier) introduse anterior, cu scopul minimizării timpului necesar completării unui astfel de registru. Toate detaliile referitoare la persoane vor fi păstrare centralizat la nivel de angajator / operator economic.
    - Posibilitatea definirii unor valori predefinite fie la nivel de sistem, fie la nivel de angajator cu scopul folosirii acestora pentru completarea facilă a informațiilor (de exemplu: ora începerii activității, ocupație, număr ore lucrate).
- Încărcarea documentelor completate în afara sistemului, inclusiv documente suport, acolo unde este cazul. Modulul trebuie să permită încărcarea documentelor inclusiv de pe dispozitive mobile. În cazul formularelor tipizate scanate și încărcate în cadrul sistemului, se vor putea extrage în mod automat anumite metadate pentru a permite indexarea și regăsirea lor ulterioară.

- Vizualizarea tuturor documentelor încărcate anterior. Va permite modificarea sau ștergerea documentelor și a anexelor, cu respectarea ciclului de viață al fiecărui tip document. Va fi posibilă refolosirea unui document, prin crearea unei noi versiuni, fără a modifica versiunea anterioară dacă aceasta a fost deja transmisă spre validare.
- Transmiterea spre înregistrare și validare către ITM a tuturor tipurilor de documente. Pentru fiecare document în parte care poate fi transmis în cadrul sistemului vor fi definite un set de metadate minim obligatorii pentru a asigura procesarea lor optimă. Metadatele vor fi completate în mod automat în toate cazurile unde este posibil acest lucru (de exemplu: detaliile de identificare ale angajatorului).
- Validarea completării tuturor informațiilor necesare cu integrarea sistemelor ITM și a altor sisteme terțe cu care este necesară integrarea. În cazul în care nu este posibilă realizarea unei validări automate (de exemplu: eroare de conexiune cu un sistem terț sau informații indisponibile), acest lucru va fi marcat vizual, dar nu va împiedica transmiterea documentelor pe flux. Pentru fiecare din sistemele terțe cu care este necesară integrarea, Beneficiarul va realiza demersurile administrative necesare obținerii acordului proprietarului sistemului pentru realizarea interoperabilității. Prestatorul trebuie să asigure suportul tehnic.
- Atenționarea utilizatorului în mod vizual și prin mesaje de eroare clare asupra erorilor de completare a documentelor (informații sau anexe lipsă, câmpuri necompletate sau completate necorespunzător)
- Urmărirea statusului documentelor transmise spre procesare în mod vizual. Fiecare etapă de validare va fi definită ca un pas într-un proces fiind posibilă astfel vizualizarea întregului flux al documentului atât pentru etapele automate, cât și pentru acelea unde este necesară procesarea de către un operator.
- Urmărirea solicitărilor de completare a documentelor/dosarelor transmise. Angajatorii vor avea posibilitatea de a răspunde acestor solicitări, cu respectarea termenelor legale, prin transmiterea documentelor sau informațiilor solicitate direct în sistem.
- Transmiterea notificărilor prin e-mail, în mod automat conform fluxului definit de procesare a fiecărui tip de document. Notificările vor putea fi transmise către un utilizator sau către un grup de utilizatori, în funcție de fluxul definit la momentul implementării.
- Înregistrarea automată a tuturor documentelor transmise către ITM în registratura electronică și generarea automată a numărului de înregistrare. Repartizarea catre serivciul, compartimentul, biroul, abilitate sa gestioneze si/sau sa solutioneze, aceste documente, pana la desemnarea angajatului ITM/IM responsabil, operatiuni efectuate tot in mod electronic.
- Generarea și transmiterea automată a formularelor avizate de către ITM către angajator, acolo unde este cazul, în format needitabil, semnat electronic cu semnătură electronică (certificat de sistem).
- Arhivarea electronică a tuturor documentelor procesate în cadrul sistemului, cu posibilitatea consultării ulterioare.
- Încărcarea și înregistrarea oricărui tip de document privitor la RM primit în mod fizic la ghișeu de către operatorul ITM. Sistemul va permite completarea tuturor informațiilor necesare privind angajatorul pentru care se înregistrează documentul prin selecția acestuia din cadrul unui nomenclator preexistent.
- Definirea unor timpi standard de procesare pentru fiecare tip de document în parte, atât la nivel de proces, cât și la nivel de etapă în cadrul procesului, ținând cont de eventualele zile nelucrătoare sau sărbători legale, conform procedurilor operaționale ale ITM.
- Alocarea automată a documentelor spre procesare către o anumită persoană, un anumit rol sau un anumit grup de persoane (de exemplu un compartiment). De asemenea, în caz de nevoie, se

va putea efectua modificarea operatorului alocat, în conformitate cu procedurile interne în vigoare.

- Vizualizarea tuturor documentelor asociate aceluiași dosar în cadrul fluxului de lucru. Operatorul alocat va putea modica statusul procesului dacă este necesar, va putea adăuga observații sub formă de text sau alte documente suport și va putea solicita clarificări. În cazul în care pentru un anumit dosar sunt transmise documente adiționale, sistemul va permite înregistrarea acestor documente cu număr de înregistrare în Registratura electronică. Sistemul va lega logic cele două procese, permițând astfel vizualizarea centralizată a tuturor documentelor.
- Modificarea facilă a diferitor fluxuri de lucru aferente documentelor, direct din interfață, prin configurarea pașilor din proces, a persoanelor sau a grupurilor (compartimentelor) implicate sau a tipurilor de validări necesare.
- Adăugarea direct din interfață a unor noi tipuri de documente, modificarea celor existente și definirea metadatelor aferente acestora, respectiv a fluxurilor de procesare.

Toate informațiile/datele preluate sub orice forma de catre sistem se vor regasi in campurile aferente din fisa unitatii.

Crearea, atat a unor rapoarte predefinite, care sa contina informatiile stabilte conform procedurilor de lucru, cat si posibilitate de a creea, de catre utilizator, a unor noi tipuri de rapoarte, in functie de solicitarile survenite.

3.2.6.3 Sănătate și Securitate în Muncă (SSM)

3.2.6.3.1 <u>Preambul</u>

Securitatea și sănătatea în muncă constituie un ansamblu de activități instituționalizate având ca scop asigurarea celor mai bune condiții în desfășurarea procesului de muncă, apărarea vieții, integrității fizice și psihice, sănătății lucrătorilor și a altor persoane participante la procesul de munca.

Inspecția Muncii are următoarele atribuții în domeniul Sănătate și Securitate în Muncă (SSM):

- verifică aplicarea prevederilor legislative privind securitatea și sănătatea în muncă, condițiile de muncă în sectoarele public, mixt și privat, notificând prin înscrisuri neconformitățile;
- controlează aplicarea prevederilor legale referitoare la politicile de prevenire bazate pe evaluarea riscurilor;
- controlează pe parcursul execuției și la punerea în funcțiune a unor obiective, instalații și utilaje aplicarea și asigurarea măsurilor de securitate și sănătate în muncă;
- verifică modul de organizare și funcționare a Comitetelor de Securitate și Sănătate în Muncă;
- controlează modul în care sunt îndeplinite obligațiile unităților referitoare la instruirea personalului privind securitatea muncii;
- controlează aplicarea prevederilor legale referitoare la certificarea echipamentelor tehnice, a echipamentelor individuale de protecție la producători, importatori și utilizatori;
- controlează modul în care conducerile agenților economici instruiesc angajații privind cunoașterea riscurilor de îmbolnăvire profesionala și a masurilor preventive ce se impun;
- constată și sancționează în baza actelor normative, neconformitățile constatate în timpul controalelor, a verificării și cercetării accidentelor de muncă;
- controlează dotarea locurilor de muncă cu truse de prim ajutor și modul în care personalul din unități este pregătit să acorde primul ajutor în caz de accident sau intoxicație acută profesională;

- controlează modul de aplicare a masurilor privind supravegherea și asigurarea stării de sănătate a salariaților;
- controlează respectarea prevederilor legale privind îmbunătățirea condițiilor de muncă;
- controlează respectarea prevederilor de ergonomie a muncii și impune luarea de masuri tehnice și organizatorice de îmbunătățire progresiva a condițiilor de munca și de reducere a efortului fizic și psihic;
- controlează respectarea prevederilor legale referitoare la organizarea timpului de munca, ritmul muncii, pauze de odihnă;
- controlează respectarea legislației în vigoare privind angajarea și repartizarea lucrătorilor în raport cu starea de sănătate, aptitudinile fizice și psihice ale acestora;
- controlează dacă schimbarea locurilor de munca se face în concordanta cu avizele și propunerile medicale;
- controlează respectarea prevederilor legale privind refacerea capacității de termoreglare a organismului și dotarea locurilor de munca cu utilități tehnic sanitare;
- controlează respectarea prevederilor legale privind munca femeilor;
- controlează dacă persoanele juridice sau fizice autorizate să presteze servicii în domeniul securității muncii respectă condițiile de acreditare;
- verifică modul în care au fost duse la îndeplinire masurile dispuse cu ocazia controalelor sau a cercetării evenimentelor.

Angajatorul are obligația de a asigura securitatea și sănătatea lucrătorilor în toate aspectele legate de muncă. În cadrul responsabilităților sale, angajatorul are obligația să ia măsurile necesare pentru:

- asigurarea securității și protecția sănătății lucrătorilor;
- prevenirea riscurilor profesionale;
- informarea și instruirea lucrătorilor;
- asigurarea cadrului organizatoric și a mijloacelor necesare securității și sănătății în muncă.

Urmare a îndeplinirii obligatiilor legale, angajatorul va întocmi și prezenta inspectorilor de muncă, cu ocazia controalelor sau a cercetării de evenimente, în conformitate cu prevederile legale în vigoare cel putin urmatoarele documente:

- Autorizația de funcționare din punct de vedere al securității și sănătății în muncă
- Decizii interne pentru:
    - personalul cu atribuții în domeniul SSM și certificatele de pregătire profesională;
    - componenta serviciului intern de prevenire si protectie
    - decizie pentru conducatorul serviciului extern de prevenire si protectie
    - contractul de prestări cu serviciul extern SSM și medicina muncii
    - conducătorii locurilor de muncă;
    - personalul care aplica masurile de prim ajutor
- Documentele Comitetului de Securitate și Sănătate în Muncă (CSSM):
    - decizia de înființare a comitetului/comitetelor de securitate si sanatate in munca si componenta acestora;
    - regulamentul propriu de funcționare
    - convocatoare CSSM

- raport trimestrial activitate CSSM
- raportul anual al conducătorului unității în CSSM cu privire la situația securității și sănătății în muncă;
- raportul medicului care asigura supravegherea stării de sănătate a salariaților;
- planul anual de masuri în domeniul SSM și fondul de cheltuieli necesar;
- programul de activitate al serviciului intern de prevenire si protectie
- Evidență procese verbale privind întrunirile Comitetului SSM în conformitate cu HG 1425/2006 art.66(8) si dovada transmiterii acestora catre ITM ul teritorial

- Evaluarea riscurilor de accidentare și îmbolnăvire profesionala la locurile de munca
- Starea de sanatate a lucratorilor:
  - Dosarul medical individual, respectiv ultima fisa de aptitudine si evidenta fiselor de aptitudine la acelasi angajator
  - Fisele de identificare a factorilor de risc profesional cf.HG 355/2007
  - Fisa de aptitudini medicale
  - Înscrierea în fișa individuala de instruire a aptitudinilor/inaptitudinilor medicale - ex: "Apt pentru lucru la înălțime"
  - Aviz psihologic personal care concura la siguranta circulatiei
- Programe de instruire, testare pe meserii sau activități
  - Tematici de instruire, instrucțiuni proprii ssm pt activitățile desfășurate, pentru E.M. utilizate, instr. proprii privind durata instruirilor in cele 3 faze și suplimentară
  - Teste utilizate pentru evaluarea cunoștințelor în procesul de instruire
  - Fişele individuale de instruire în domeniul securității și sănătății în muncă
- Măsuri tehnico-organizatorice de prevenire alarmare, intervenție, evacuare și prim-ajutor
- Diploma de absolvire a cursurilor în domeniul securității și sănatatii în muncă
- lista internă de dotare cu echipamentele individuale de protecție (EIP), corespunzător riscurilor existente la locurile de muncă (Certificate de conformitate pentru EIP, Fişe de magazie individuale pentru dotarea cu EIP)
- Documentele care să ateste ca echipamentele de muncă utilizate în cadrul unității sunt certificate de organismele competente, potrivit legii
- Registre de supraveghere a parametrilor tehnologici ai instalatiilor, AMC urilor aflate în funcțiune
- Contractul colectiv de muncă întocmit la nivelul unității (clauzele referitoare la securitatea și sănătatea în muncă, la timpul de muncă, regimul pauzelor, munca în schimburi și intensitatea acesteia)
- Regulamentul de Organizare și Funcționare și Regulamentul Intern
- Măsuri tehnice și/sau organizatorice luate pentru protecția împotriva electrocutării prin atingere directă și indirectă, buletine de verificare PRAM
- Determinările de noxe, în cazul unităților cu tehnologii care degaja noxe chimice, buletine de măsurare
- Determinarea limitelor de zgomot la locurile de muncă (dacă sunt sub cele maxim admise pentru protecția neuropsihică și psihosenzorială a executanților), buletine de măsurare

- Instructiuni proprii pentru completarea și/ sau aplicarea reglementărilor de securitate şi sănă tate în muncă, ţinand seama de particularităţile activităților și ale locurilor de muncă aflate în responsabilitatea lor
- Documente privind autorizarea exercitării meseriilor și a profesiilor prevăzute în legislația specifică, ca de ex. electrician, lucru la inalțime, fochist, sudor ISCIR, stivuitorist, macaragiu etc.
- Evidenţa locurilor de muncă cu condiții deosebite: vătămătoare, grele și periculoase
- Implementare noilor prescripții minime pentru semnalizarea de securitate și/sau sănătate în munca
- Documentul privind protecția la explozie și evaluarea riscurilor de explozie
- Evidența angajaților artificieri și pirotehnicieni autorizați în conformitate cu HG 536/2002 art.122(3)
- Evidența substanțelor și preparatelor chimice periculoase în conformitate cu Legea 360/2003 art. 24 alin. 2
- Evidența angajaților artificieri și pirotehnicieni autorizați în regim transnațional sau transfrontalier în conformitate cu HG 536/2002 art.125 indice 2
- Evidența informărilor cu privire la perioada de desfășurare a cursurilor de calificare în meseria de artificier și pirotehnician în conformitate cu HG 536/2002 art.118
- Evidența dosarelor de cursanți în meseria de artificier și pirotehnician care își încetează activitatea în conformitate cu HG 536/2002 art.117(4)
- Evidență procese verbale privind întrunirile Comitetului SSM în conformitate cu HG 1425/2006 art.66(8)
- Informări privind neconcordanțele între stocul faptic și cel scriptic de materii explozive din depozit în conformitate cu HG 536/2002 art.73(3)
- Informări ale angajatorilor privind constatarea de lipsuri la materiile explozive sosite în depozitele autorizate în conformitate cu HG 536/2002 art.70(5)
- Listă notificări în prealabil privind utilizarea agenților biologici în conformitate cu HG 1092/2006 art.23(1)-(3)
- Evidenta informărilor de la persoanele juridice autorizate care execută lucrări cu caracter temporar, de prospecțiune și explorări geologice sau în cadrul intervențiilor cu mijloace antigrindină referitoare
- Notificări privind începerea activităților cu lucrători expuși la azbest în conformitate cu HG 1875/2005 art.12,15
- Evidența înștiințărilor deciziilor emise de angajator privind încetarea raporturilor de muncă ale salariatelor conform în conformitate cu OUG 96/2003 art.24
- Evidența înștiințărilor și rapoartelor de evaluare privind salariatele gravide, care au născut recent sau care alăptează în conformitate cu OUG 96/2003
- Listă declarații prealabile pentru șantierele temporare sau mobile în conformitate cu HG 300/2006 art.47-48
- Orice alte documente relevant.

În cele ce urmează sunt prezentate succint câteva din fluxurile specifice de lucru la nivelul ITM în domeniul SSM. În vederea îndeplinirii obiectivelor proiectului, în timpul etapei de analiză și proiectare a noului SIAMC, se vor stabili procedurile de lucru care vor fi implementate, formularele și documentele care vor fi utilizate, precum și întregul circuit a documentelor aferente acestor procese. Se va avea în vedere faptul că este necesară implementarea unor zone dedicate atât pentru operatorii economici

(angajatori), cât și pentru cetățeni (de exemplu solicitanți autorizații), cu scopul eficientizării interacțiunii dintre IM/ITM, agenti economici și cetățeni.

Autorizare de funcționare din punct de vedere SSM

În vederea asigurării condițiilor de securitate și sănătate în munca și pentru prevenirea accidentelor și a bolilor profesionale, angajatorii au obligația să obțină autorizația de funcționare din punct de vedere al securității și sănătății în munca, înainte de începerea oricărei activități, în conformitate cu art.3 din Norma Metodologica de aplicare a Legii SSM nr. 319/2006 (HG 1425/2006 actualizata inclusiv cu HG 955/2010 și HG 1242/2011) - numai pentru angajatorii care nu se înregistrează la Registrul Comerțului.

În vederea autorizării din punct de vedere al securității și sănătății în muncă, angajatorul are obligația să depună la inspectoratul teritorial de munca pe raza căruia își desfășoară activitatea o cerere, completata în doua exemplare semnate în original de către angajator, conform modelului prevăzut în lege. Cererea va fi însoțita de următoarele acte:

- copii de pe actele de înființare;
- declarația pe propria răspundere din care rezulta ca pentru activitățile declarate sunt îndeplinite condițiile de funcționare prevăzute de legislația specifica în domeniul securității și sănătății în munca.

În vederea autorizării din punct de vedere al securității și sănătății în muncă, inspectoratele teritoriale de munca procedează după cum urmează:

- înregistrează cererile de autorizare a funcționarii din punct de vedere al SSM;
- verifica actele depuse în susținerea acestora, precum și declarația pe propria răspundere prevăzută in HG 1425/2006;
- completează și emit certificatul constatator;
- asigura evidenta certificatelor constatatoare eliberate;
- asigura arhivarea documentației în baza căreia s-au emis certificatele constatatoare.

Evidență servicii externe de prevenire și protecție

Presupune fluxul de lucru privind abilitarea firmelor care solicită să presteze servicii externe de prevenire și protecție. Acesta presupune:

- organizarea periodică a unor intalniri ale comisiei de abilitare cu publicarea datei întâlnirii comisiei
- depunerea de către solicitanți, la registratura ITM a dosarelor cu cel putin 10 ~~X~~ zile înainte de data întrunirii comisiei
- repartizarea solicitărilor la secretariatul comisiei de abilitare din cadrul ITM-ului
- analizarea propunerilor de către comisie și acordarea sau nu a certificatul de abilitare pentru servicii externe de prevenire și protecție

Pe portalurile ITM sunt publicate liste cu toate informațile privind serviciile externe de prevenire și protecție.

Monitorizare materii explozive, substanțe și preparate chimice periculoase

Substanțe și preparate chimice periculoase

Conform art. 24, alin. 2 din Legea nr. 360/2003 privind regimul substanțelor si preparatelor chimice periculoase, angajatorii care lucrează cu astfel de substanțe sunt obligați sa furnizeze inspectoratului teritorial de munca lista cu substanțele si preparatele chimice periculoase pe care le vor deține.

Materii explozive

Activitățile de preparare, producere, procesare, experimentare, deținere, tranzitare pe teritoriul țării, transmitere sub orice formă, transfer, transport, introducere pe piață, depozitare, încărcare, încătușare, delaborare, distrugere, mânuire, comercializare și folosire a materiilor explozive trebuie supuse

autorizării de către ITM (art. 1, alin. (1) și art. 8, alin. (1), (2), și (3) din Legea nr. 126/1995 privind regimul materiilor explozive, republicată).

Funcționarea depozitelor de materii explozive se supune autorizării de către ITM (art. 1 alin. 1 și art. 9 din Legea nr. 126/1995 privind regimul materiilor explozive, republicată).

Obligația de a obține în prealabil autorizația din partea ITM revine:

- Persoanelor juridice care, prin actul constitutiv al societății, au ca obiect de activitate operațiuni dintre cele enumerate mai sus;
- Persoanelor juridice și fizice care dețin, folosesc sau comercializează materii explozive, cu excepția unităților și formațiunilor Ministerului Apărării Naționale, Ministerului Afacerilor Interne, Serviciului de Protecție și Pază și Serviciului Român de Informații;
- Persoanelor care produc, dețin, transferă sau comercializează articole pirotehnice, precum și persoanelor care folosesc obiecte pirotehnice în scopuri tehnice;

Autorizarea se obține numai la solicitarea celui interesat și pe o durata determinată, cu posibilitatea de prelungire, cu observația că este interzisă îndeplinirea activităților prevăzute în autorizație prin intermediari neautorizați (art. 8, alin (4) și (5) din Legea 126/1995 privind regimul materiilor explozive, republicată).

Obiectivele activității de autorizare sunt:

- Obținerea de către solicitanți a autorizațiilor pentru a efectua operațiuni cu materii explozive.
- Crearea unei baze de date care să asigure evidența angajatorilor care au obținut autorizarea pentru a efectua operațiuni cu materii explozive
- Respectarea legislației în vigoare care prevede că introducerea pe piață a explozivilor de uz civil și a articolelor pirotehnice este admisă numai în condițiile în care acestea respectă cerințele esențiale aplicabile lor, urmărind să se asigure un înalt nivel de protecție a sănătății umane și siguranței publice, protecția și siguranța consumatorilor, precum și protecția mediului.

La momentul actual, procesul se desfășoară în opt etape principale:

- **Depunerea dosarului în vederea autorizării.** Persoanele fizice și juridice autorizate potrivit legii trebuie să depună (personal, prin poștă sau prin PCU electronic) la registratura ITM, sau prin autentificare în contul dedicat angajatorului, a unui dosar care va conține elementele legal prevăzute. După ce a fost înregistrat, dosarul este repartizat compartimentului SPIAASSM. Totodată, Inspectorul Șef nominalizează inspectorul de muncă din cadrul serviciului CSSM, care va efectua evaluarea solicitantului, atât din punct de vedere al documentației, cât și pe teren. Concluziile evaluării vor fi incluse într-un referat, în cuprinsul căruia inspectorii de muncă din cadrul serviciului CSSM sau al CSPIAASSM vor propune, după caz, eliberarea sau neeliberarea autorizației.

CSSM sau SPIAASSM cf atributiilor stabilite in cadrul fiecarui inspectorat realizează

- **Verificarea documentelor depuse și procesarea cererii**. Personalul din cadrul compartimentului SPIAASSM, trebuie:
    - să verifice dacă documentația depusă este completă și conține:
        - Cererea pentru autorizare;
        - Copie de pe certificatul de înregistrare și statutul operatorului economic;
        - Certificatul constatator de la Oficiul Registrului Comerțului
        - Cazierul judiciar pentru asociați și administratori;
        - Planul locației unde se desfășoară activitatea;

        - Schema electrică monofilară de alimentare cu energie electrică a locației unde se desfășoară activitatea;
        - Schema privind modul de asigurare a iluminatului;
        - Planul cuprinzând dotarea și amplasarea mijloacelor tehnice pentru combaterea și prevenirea incendiilor;
        - Schema instalației de protecție contra tensiunilor accidentale, inclusiv contra supratensiunilor atmosferice cu precizarea rezultatelor măsurării rezistenței prizelor efectuate la termenul scadent;
        - Descrierea modului de asigurare a pazei și a gardurilor împrejmuitoare, acolo unde este cazul;
        - Descrierea modului de asigurare a depozitării materiilor prime și a producției finite;
        - Descrierea modului de asigurare a supravegherii, alarmării și evacuării personalului în caz de pericol;
        - Lista mijloacelor de transport în interiorul depozitului;
        - Lista cu personalul calificat și autorizat să efectueze operațiuni cu materii explozive;
    - Să verifice dacă cererea pentru autorizare conține, cel puțin: denumirea, sediul și obiectul activității, adresa, numărul de telefon/fax, persoana de contact, precum și tipul materiilor explozive cu care se efectuează operațiuni.
    - Să verifice dacă certificatul constatator de la Oficiul Registrului Comerțului este eliberat cu cel mult 30 zile anterior datei de solicitare a autorizării.
    - Să verifice dacă solicitanții care dețin depozite de materiale explozive, în vederea autorizării acestora, au depus suplimentar la dosar și:
        - Date privind capacitatea maximă de stocare în echivalent TNT, numărul camerelor de stocare și capacitatea acestora, tipul depozitului, pentru depozitele de explozivi de uz civil;
        - Date privind capacitatea maximă de stocare, conform masei nete de amestec pirotehnic, numărul camerelor și capacitatea acestora, tipul depozitului, pentru depozite de articole pirotehnice;
    - Să proceseze cererea solicitantului în cel mai scurt termen, dar nu mai mult de 30 zile calendaristice de la data depunerii documentației complete;
    - Să notifice solicitanților, înainte de expirarea termenului legal și cu motivare corespunzătoare, prelungirea termenului de procesare a cererii precum și durata acestei prelungiri; (termenul poate fi prelungit o singură dată, pentru o perioadă de maxim 15 zile calendaristice, iar valabilitatea documentelor depuse inițial nu este afectată de această prelungire);
    - Să informeze solicitantul în cel mai scurt termen, dar nu mai mult de 5 zile lucrătoare de la primirea cererii, cu privire la necesitatea transmiterii de documente suplimentare, în cazul unei documentații incomplete;
    - Să informeze solicitantul în cel mai scurt termen, dar nu mai mult de 5 zile lucrătoare de la data depunerii cererii, în cazul în care cererea a fost respinsă pentru motive de natură procedurală.
    - Să transmită solicitantului, atunci când este cazul, decizia de a nu aviza dosarul și să motiveze clar această decizie;
- **Activități de corespondență cu IPJ.** Personalul din cadrul compartimentului SPIAASSM, trebuie:

- să întocmească adresa către IPJ în care va fi precizată propunerea ITM de a elibera, sau nu, autorizația.
- să transmită, prin serviciul de corespondență, dosarul complet către IPJ, în termen de 10 zile lucrătoare de la data depunerii. IPJ are obligația de a analiza dosarul, conform domeniului de competență și de a-l retransmite către ITM, însoțit, după caz, de avizul sau refuzul avizării, în termen de 10 zile lucrătoare de la data primirii.
- Să primească, prin serviciul de corespondență, dosarul de la IPJ, însoțit, după caz, de avizul sau refuzul avizării acestuia.

- **Emiterea și eliberarea autorizației.** Personalul din cadrul compartimentului SPIAASSM, trebuie:
  - să completeze formularul de autorizație prevăzut în Anexa nr. 1 sau Anexa nr. 2 din H.G. nr. 536/2002 pentru aprobarea Normelor tehnice privind deținerea, prepararea, experimentarea, distrugerea, transportul, depozitarea, mânuirea și folosirea materiilor explozive utilizate în orice alte operațiuni specifice în activitățile deținătorilor, precum și autorizarea artificierilor și a pirotehnicienilor, actualizată.
  - să prezinte Inspectorului Șef autorizația spre a fi semnată.
  - să înregistreze și să ștampileze autorizația.
  - să facă o copie autorizației care va fi inclusă în dosar.
  - să elibereze solicitantului autorizația în original.
- **Arhivarea documentelor.** Personalul din cadrul compartimentului SPIAASSM, trebuie:
  - Să arhiveze dosarele care au obținut autorizarea, așezându-le în ordinea cronologică a solicitărilor;
  - Să asigure evidența electronică a cererilor de solicitare, autorizațiilor eliberate și a răspunsurilor formulate prin introducerea tuturor datelor în aplicațiile specifice (COLUMBO/SIAMC, bazele de date proprii ale ITM);
- **Acordarea vizei anuale.** Autorizația obținută în urma parcurgerii etapelor descrise mai sus, se vizează anual de către ITM și IPJ, în termen de 15 zile de la data expirării acesteia; neprezentarea autorizației pentru viză duce la pierderea dreptului titularului de a efectua operațiuni cu materii explozive. Pentru obținerea vizelor anuale, persoana autorizată care solicită viza trebuie să depună la registratura ITM, un dosar care va conține elementele prevăzute de art. 12, alin. (5) din H.G. nr. 536/2002 pentru aprobarea Normelor tehnice privind deținerea, prepararea, experimentarea, distrugerea, transportul, depozitarea, mânuirea și folosirea materiilor explozive utilizate în orice alte operațiuni specifice în activitățile deținătorilor, precum și autorizarea artificierilor și a pirotehnicienilor, actualizată. Personalul din cadrul compartimentului SPIAASSM, trebuie:
  - Să ridice de la secretariatul ITM dosarele depuse pentru vizarea anuală, prin intermediul serviciului de corespondență sau prin PCU electronic;
  - Să verifice dacă acestea sunt complete și conțin:
    - Solicitare pentru acordarea vizei anuale;
    - Autorizația inițială;
    - Certificatul constatator de la Oficiul Registrului Comerțului prin care se certifică menținerea aceluiași obiect de activitate;
    - Declarația pe propria răspundere prin care să se menționeze că nu s-au schimbat condițiile inițiale de autorizare;
  - Să verifice dacă solicitarea se încadrează în termenul legal de 15 zile de la data expirării autorizației;

- Să aducă din arhiva instituției dosarul inițial (pentru obținerea autorizației) și să-l completeze cu documentele depuse pentru obținerea vizei;
- Să verifice ca dosarul nou întocmit să parcurgă etapele descrise anterior (între lit. B alin. 5 și lit. D alin 1 inclusiv);
- Să prezinte Inspectorului Șef autorizația pentru înscrierea vizei în caseta corespunzătoare;
- Să facă o copie autorizației vizate și să o includă în dosar;
- Să elibereze autorizația vizată solicitantului;
- Să arhiveze documentele în ordinea cronologică a solicitărilor;
- Să asigure evidența electronică a documentației, prin introducerea datelor în aplicațiile specifice;

- **Predarea autorizației.** La încetarea activității, este obligatorie predarea autorizației, instituției care a emis-o.(art. 11 alin. 3 din Legea nr. 126/1995 privind regimul materiilor explozive, republicată). Personalul din cadrul compartimentului SPIAASSM, trebuie să arhiveze în dosare și electronic autorizațiile depuse.
- **Eliberarea unei noi autorizații.** Persoanele fizice sau juridice care au obținut autorizația pentru a efectua operațiuni cu materii explozive, pot solicita o nouă autorizație în următoarele situații:
  - Schimbarea denumirii sau a sediului;
  - Deteriorarea, sustragerea sau pierderea autorizației;
  - Completa epuizare a spațiilor rezervate vizei anuale;

  Personalul din cadrul compartimentului SPIAASSM, trebuie:
  - Să ridice de la registratura ITM, cererile pentru eliberarea unor noi autorizații;
  - Să verifice corectitudinea documentelor depuse
  - Să completeze și să solicite Inspectorului Șef semnătura pe noul formular;
  - Să elibereze autorizațiile solicitanților, cu confirmarea primirii din partea acestora;

Noul SIAMC va asigura funcționalități specifice celor prezentate anterior. În cadrul etapei de analiză a proiectului se va definitiva procesul care va fi implementat, lista și conținutul fiecărui document în parte, în conformitate cu prevederile legale aflate în vigoare la momentul implementării contractului.

Artificieri și pirotehniști

Efectuarea operațiunilor cu explozivi, respectiv lucrări de împușcare, preparare de amestecuri explozive simple și emulsii explozive, transport, manipulare, depozitare, gestionare, distrugere, precum și alte operațiuni specifice acestui domeniu, inclusiv prestarea unor servicii similare, se efectuează numai de către artificieri autorizați. Utilizarea articolelor pirotehnice de divertisment din categoriile 2, 3 și 4, a articolelor pirotehnice din categoria P2, T2 H.G. 1102/2014 art. 18 lit. b), precum și a articolelor pirotehnice de scenă se încredințează numai persoanelor care sunt autorizate ca pirotehnicieni. Activitățile de artificier sau de pirotehnician pot fi desfășurate numai după obținerea calificării profesionale corespunzătoare, dovedită prin carnetul de artificier, respectiv de pirotehnician.

Obiectivele activității de autorizare sunt:

- Obținerea de către solicitanți a carnetelor de artificier, respectiv de pirotehnician, care condiționează desfășurarea activităților specifice.
- Existența unei baze de date care să asigure atât evidența nominală a tuturor artificierilor și pirotehnicienilor autorizați cât și a operatorilor economici care au angajați artificieri sau pirotehnicieni.
- Respectarea legislației în vigoare care prevede ca introducerea pe piață a explozivilor de uz civil și a articolelor pirotehnice să fie admisă numai în condițiile în care acestea respectă cerințele

esențiale aplicabile lor, urmărind să se asigure un înalt nivel de protecție a sănătății umane și siguranței publice, protecția și siguranța consumatorilor, precum și protecția mediului.

La momentul actual, procesul de autorizare se desfășoară în 5 etape principale:

- **Depunerea dosarului în vederea examinării** - Autorizarea artificierilor și a pirotehnicienilor se face în baza unui examen susținut în prezenta unei comisii formate din reprezentanți ai ITM-ului pe raza căruia solicitantul își are domiciliul, reședința sau rezidența. Participarea și susținerea de către candidați a examenului în vederea autorizării este condiționată de transmiterea (personal sau prin poștă) către comisie, a unui dosar care va conține elementele prevăzute de art. 119, alin. (2) din HG 536/2002, actualizată. După ce a fost depus la registratura ITM și înregistrat, dosarul este repartizat compartimentului SPIAASSM. Personalul din cadrul compartimentului SPIAASSM preia de la secretariat, prin serviciul de corespondență, dosarele repartizate.
- **Verificarea documentelor depuse și activități de corespondență** – Personalul ITM trebuie să verifice dacă documentația depusă este completă și conține următoarele documente:
    - Cererea pentru autorizare;
    - Copia actului de identitate;
    - Copie de pe certificatul de calificare în meseria de artificier, respectiv de pirotehnician,
    - Certificatul de cazier judiciar;
    - Certificat medical din care să rezulte faptul că solicitantul este clinic sănătos;
    - Aviz psihologic din care să rezulte că solicitantul este apt pentru meseria de artificier sau pirotehnician;
    - Două fotografii 3x4 cm.

  Personalul ITM trebuie să verifice dacă cererea pentru autorizare conține datele personale și lucrările pentru care se solicită autorizarea. Solicitantul va fi notificat pentru următoarele evenimente:
    - **Programare examen** – în termen de 10 zile lucrătoare de la data înregistrării cererii cu privire la data programării examenului de autorizare. Această dată trebuie să se afle în termenul legal de 30 de zile calendaristice de la data înregistrării cererii.
    - **Amânare examen** – în cazul amânării examenului pentru motive corespunzătoare, solicitantul va fi notificat înainte de expirarea termenului inițial. Amânarea se poate face o singură dată pentru o perioadă de maxim 15 zile lucrătoare, fără a afecta valabilitatea documentelor din cadrul dosarului.
    - **Respingere solicitare** – în cazul în care, solicitatului îi este refuzată participarea la examen, acest lucru trebuie comunicat, cu motivație argumentată, conform prevederilor legale.
    - **Solicitare de completare dosar** – în care cererea formulată de acesta nu este însoțită de actele doveditoare corespunzătoare
- **Examinarea candidaților** – Examinarea candidaților în vederea autorizării se va face de către membrii comisiei de examinare, numiți prin decizia Inspectorului Șef, în funcție de tipul de lucrări pe care solicitantul intenționează să le execute. Personalul desemnat din cadrul compartimentelor SPIAASSM sau CSSM, trebuie:
    - Să consemneze rezultatele examenului de autorizare într-un proces verbal care va fi semnat de către toți membrii comisiei;
    - Pentru candidații declarați „respinși”, să emită decizii de nepromovare a examenului, care vor fi motivate în mod clar, prezentându-se cauzele și care vor putea fi contestate la Inspecția Muncii și, după caz, la instanța judecătorească competentă, potrivit legii.

Solicitantul poate relua procedura de autorizare numai după o perioadă de 30 zile de la data restituirii dosarului.

- **Emiterea și eliberarea carnetului de artificier sau de pirotehnician** - Solicitanții care au promovat examenul de autorizare, trebuie să efectueze o practică timp de două luni, sub supravegherea unui artificier autorizat, respectiv a unui pirotehnician autorizat și cu experiență. Pentru fiecare solicitant declarat admis, personalul desemnat din cadrul compartimentului SPIAASSM, trebuie:
    - Să completeze adeverințe din care să rezulte promovarea examenului pentru autorizarea ca artificier, respectiv pirotehnician, cu specificarea tipului activității (sau activităților) autorizate, care vor fi necesare pentru efectuarea practicii.
    - Să prezinte Inspectorului Șef adeverințele spre a fi semnate, să le înregistreze la secretariatul ITM și să le facă câte o copie.
    - Să elibereze solicitanților adeverințele în vederea parcurgerii perioadei de practică, cu confirmarea primirii din partea acestora.
    - Să ridice de la registratura instituției documentele depuse de solicitanții care au efectuat perioada de practică și care atestă parcurgerea acestei perioade.
    - Să completeze, să înregistreze și să vizeze la Inspectorul Șef carnetul de artificier, respectiv de pirotehnician, conform modelelor prevăzute în anexa nr. 10 a) și 10 b) din H.G. nr. 536/2002, actualizată.
    - Să facă o copie a carnetului astfel întocmit, apoi să elibereze originalul titularului, cu confirmare de primire din partea acestuia (pe copia care va rămâne în dosarul inițial);
- **Arhivarea documentelor și a datelor**:
    - Să înregistreze și să arhiveze dosarele persoanelor cărora le-a fost eliberat carnetul de artificier, respectiv de pirotehnician;
    - Să asigure evidența electronică a cererilor de solicitare, a carnetelor eliberate și a notificărilor transmise, introducând datele în aplicațiile specifice;
    - Să restituie, pe bază de semnătură, dosarele persoanelor care nu au promovat examenul de autorizare;
    - Să asigure evidența nominală a tuturor artificierilor și pirotehnicienilor autorizați, atât pentru cei salariați la diverși operatori economici, cât și pentru cei care practică această activitate în mod independent; să se asigure că evidența respectivă conține numele persoanei autorizate, domiciliul, reședința sau rezidența acestuia, tipul de lucrări pentru care este autorizat, data eliberării autorizației, alte informații;
    - Să asigure evidența operatorilor economici care au angajați artificieri și pirotehnicieni, actualizând în termen de 5 zile lucrătoare baza de date cu orice modificare intervenită;
    - Să asigure arhivarea dosarelor provenite de la furnizorii de formare profesională autorizați care au organizat cursuri de calificare în meseria de artificier, respectiv de pirotehnician, în situația în care aceștia își încetează activitatea și au obligația de a preda dosarele ITM – ului pe raza căruia și-au desfășurat activitatea;
    - Să asigure evidența cursurilor de calificare în meseria de artificier, respectiv de pirotehnician organizate de către furnizorii de formare profesională, cât și perioadele de desfășurare ale acestora;

Suplimentar etapelor prezentate anterior, în cadrul ITM se desfășoară și următoarele activități:

- **Suspendarea carnetului de artificier sau de pirotehnician** – Carnetul de artificier, respectiv de pirotehnician poate fi suspendat de către ITM:

- la propunerea inspectorilor de muncă cu atribuții în domeniu, pe o perioadă de trei luni, în situația în care se constată abateri ale titularului de la prevederile legale privind securitatea și sănătatea în muncă;
- la propunerea organelor de poliție, pe o perioadă de trei luni, când se constată abateri de la prevederile legale privind siguranța publică;
- în situația neefectuării examenului psihologic anual (cu 30 de zile înainte de data expirării valabilității ultimei examinări psihologice), până la momentul efectuării examinării;

Personalul din cadrul compartimentului SPIAASSM, trebuie:

- Să ridice de la secretariatul ITM carnetele depuse ca urmare a suspendării acestora;
- Să asigure evidența acestora și a perioadelor de suspendare;
- Să înapoieze carnetele titularilor după expirarea perioadei de suspendare;

- **Anularea carnetului de artificier sau de pirotehnician** - Carnetul de artificier, respectiv de pirotehnician poate fi anulat de către ITM:
  - ca urmare a încălcărilor grave sau repetate ale prevederilor legale privind regimul explozivilor sau articolelor pirotehnice;
  - la întreruperea activității pe o perioadă de mai mult de 4 ani;
  - neefectuarea examenului psihologic în următoarele trei luni de la data expirării ultimei examinări psihologice;
  - în cazul în care, în urma efectuării examenului psihologic, rezultă că persoana examinată nu este aptă să își exercite meseria;

  În cazul anulării, este obligatorie predarea carnetului de artificier, respectiv de pirotehnician instituției care l-a emis. Personalul din cadrul compartimentului SPIAASSM, trebuie:
  - Să ridice de la secretariatul ITM carnetele depuse ca urmare a anulării acestora;
  - Să asigure evidența și arhivarea lor;
  - Să se asigure ca obținerea unui nou carnet are loc numai după trecerea a cel puțin 2 ani de la data anulării, pe baza unui nou examen de autorizare.

Noul SIAMC va asigura funcționalități specifice celor prezentate anterior. În cadrul etapei de analiză a proiectului se va definitiva procesul care va fi implementat, lista și conținutul fiecărui document în parte, în conformitate cu prevederile legale aflate în vigoare la momentul implementării contractului.

AVIZAREA DE CĂTRE ITM A SPAŢIILOR DE DEPOZITARE A MUNIŢIILOR, CAPSELOR SAU PULBERILOR PENTRU MUNIŢIE

Procesul de avizare se desfăşoară în următoarele etape principale:

- A. Depunerea dosarului în vederea obţinerii avizului
- B. Verificarea documentelor depuse şi procesarea cererii
- C. Emiterea avizului
- D. Aprobarea şi semnarea avizului de către Inspectorul Şef
- E. Eliberarea avizului
- F. Arhivarea documentelor
- G. Reînnoirea avizului

A. Depunerea dosarului în vederea autorizării

Deţinătorul spaţiului de depozitare:

- Depune şi înregistrează la registratura inspectoratului dosarul în vederea obţinerii avizului

Inspectorul Şef:

- Nominalizează inspectorul de muncă din cadrul compartimentului SPIAASSM sau Serviciului CSSM, conform organizării fiecărui ITM, căruia ii este repartizat dosarul şi care va efectua evaluarea solicitantului, atât din punct de vedere al documentaţiei, cât şi pe teren.

Personalul din cadrul compartimentelor SPIAASSM sau CSSM (conform organizarii ITM teritorial):

1. Îşi ridică de la secretariat prin serviciul de corespondenţă dosarele repartizate.

B. Verificarea documentelor depuse şi procesarea cererii

Personalul din cadrul compartimentelor SPIAASSM sau CSSM:

1. Verifică dacă documentaţia depusă este completă şi conţine:

a) cerere de solicitare;

b) actul constitutiv al persoanei juridice, din care să rezulte faptul că, potrivit atribuţiilor specifice, urmează să deţină sau, după caz, să folosească arme şi muniţii, pentru persoanele juridice prevăzute la art. 67 alin. (2) din lege;

c) certificatul de înmatriculare emis de oficiul registrului comerţului şi certificatul constatator pentru activitatea desfăşurată, emis în conformitate cu prevederile legale, pentru armurieri, intermediari şi persoanele juridice prevăzute la art. 67 alin. (3) şi (4) din lege;

d) un memoriu tehnic care conţine descrierea spaţiului de depozitare, a modului de depozitare, a cantităţilor de muniţie, capse sau pulberi pentru muniţie, pentru care se solicită avizarea şi amplasarea lor;

e) schiţa locului de amplasare a spaţiului de depozitare, cu indicarea distanţelor faţă de diverse obiective învecinate;

f) schiţa de detaliu a spaţiului de depozitare;

g) planul de prevenire şi protecţie, elaborat în baza evaluării riscurilor, în conformitate cu prevederile Legii securităţii şi sănătăţii în muncă nr. 319/2006, cu modificările ulterioare;

h) instrucţiunile proprii, elaborate în conformitate cu specificul activităţii desfăşurate, conform prevederilor Legii nr. 319/2006, cu modificările ulterioare.

2. Procesează cererea solicitantului în cel mai scurt termen.

3. Se deplasează la spaţiul de depozitare pentru care se solicită avizul şi verifică dacă sunt îndeplinite condiţiile prevăzute la cap. II din Ordin pentru fiecare spaţiu de depozitare.

4. Elaborează referatul care cuprinde concluziile evaluării, în cuprinsul căruia propun, după caz, eliberarea sau neeliberarea avizului.

5. Acordă avizul sau, după caz, refuzul motivat privind neavizarea spaţiului de depozitare în termen de cel mult 15 zile de la data depunerii dosarului.

C. Emiterea avizului

Personalul din cadrul compartimentului SPIAASSM:

1. Completează formularul de Aviz spaţiu de depozitare a muniţiilor/capselor/pulberilor pentru muniţie prevăzut în Anexa nr. 1, având în vedere

- Completarea temeiului legal corespunzător, respectiv:

- art. 104 din Legea nr. 295/2004 privind regimul armelor şi al muniţiilor, republicată, cu modificările şi completările ulterioare;

- Bararea (tăierea) cu o linie orizontală a elementelor care nu fac obiectul autorizării, după caz.

D. Aprobarea şi semnarea avizului de către Inspectorul Şef

Personalul din cadrul compartimentului SPIAASSM:

1. Înaintează Inspectorului Şef avizul spre a fi semnat;

2. Înregistrează şi ştampilează avizul prin intermediul Registraturii;

3. Face o copie avizului care va fi inclusă în dosar;

E. Eliberarea avizului

Personalul din cadrul compartimentului SPIAASSM:

1. Înştiinţează solicitantul să se prezinte la sediul ITM în vederea ridicării formularului original al avizului spaţiului de depozitare

2. Eliberează solicitantului formularul original al avizului însoţit de adresa de înaintare întocmită în două exemplare, unul rămânând la ITM

3. Aduce la cunoştinţa solicitantului următoarele aspecte deosebit de importante:

• În cazul în care spaţiul de depozitare avizat este modificat (numai în baza unui proiect de execuţie elaborat de către un proiectant autorizat), trebuie să se obţină un nou aviz al inspectoratului teritorial de muncă

• Inspectoratul teritorial de muncă poate suspenda până la remedierea deficienţelor constatate sau poate revoca, după caz, avizul atunci când se constată că deţinătorii nu au respectat condiţiile în baza cărora a fost eliberat avizul.

• În situaţia în care operatorul economic îşi desfăşoară activitatea de depozitare pentru muniţii, capse sau pulberi pentru muniţii şi pe teritoriul altor judeţe, acesta este obligat să obţină avizul de la fiecare inspectorat teritorial de muncă pe raza căruia îşi desfăşoară activitatea de depozitare.

F. Arhivarea documentelor

Personalul din cadrul compartimentului SPIAASSM:

1. Arhivează dosarele care au obţinut avizul, aşezându-le în ordinea cronologică a solicitărilor;

2. Asigură evidenţa electronică a cererilor de solicitare şi avizelor eliberate prin introducerea tuturor datelor în aplicaţiile specifice (COLUMBO/SIAMC, bazele de date proprii ale ITM);

G. Reînnoirea avizului

Personalul din cadrul compartimentelor SPIAASSM şi CSSM:

1. Soluţionează solicitările privind reînnoirea avizului pe baza constatărilor efectuate asupra îndeplinirii condiţiilor iniţiale pentru care a fost acordat avizul.

2. Reînnoiesc avizul prin aplicarea vizelor anuale, pe fila verso a avizului, termenul de soluţionare fiind acelaşi, respectiv de cel mult 15 zile de la data depunerii dosarului.

3.2.6.3.2 <u>Cerințe funcționale</u>

Scopul acestui modul este de a permite completarea, înregistrarea și gestiunea întregului flux de validare a diferitelor tipuri de documente (notificări), în vederea îndeplinirii obligațiilor specifice angajatorilor în ceea ce privește Sănătatea și Securitatea în Muncă (SSM), în conformitate cu cadrul legal în vigoare la momentul implementării sistemului, și pe toată durata perioadei de suport tehnic și garanție ofertată.

Acest modul va dispune de o zonă publică (front-office), accesibilă prin intermediul portalului web, dedicată operatorilor economici (angajatorilor) și cetățenilor, precum și de o zonă privată (back-office) dedicată personalului din cadrul IM/ITM. Accesul va fi posibil numai după autentificare, iar informațiile afișate vor depinde de rolul utilizatorului conectat în sistem.

Pentru a evita blocajele din perioada de tranziție de la actualul mod de lucru care implică depunerea la ghișeu a documentelor și viitorul mod de lucru informatizat, sistemul va permite angajaților beneficiarului efectuarea tuturor operațiunilor specifice pentru înregistrare corespunzătoare a documentelor.

Sistemul va permite:

- Accesul utilizatorilor externi (operatori economici / angajatori, cetățeni) pe baza contului de utilizator folosit pentru conectarea la REGES-ONLINE. Utilizatorii externi vor urma procedura de înrolare stabilită la nivel de ITM în vederea obținerii detaliilor de acces.
- Accesul utilizatorilor interni (personal IM/ITM) pe baza contului de utilizator folosit la nivel de instituție.
- Accesul prin sistem la contractele colective de muncă depuse la ITM
- Configurarea setului de permisiuni la nivel de modul, cu definirea tipurilor de roluri și a grupurilor de acces, atât pentru utilizatorii interni (de exemplu: drepturi de validare documente doar pentru inspectorii de muncă din compartimentul SSM, drepturi de vizualizare pentru toți inspectorii)
- Definirea tuturor tipurilor de documente tipizate si formulare cu regim special utilizate aflate în aria de acoperire a SSM, a metadatelor minime necesare a fi completate în cadrul sistemului, precum și a fluxului de procesare. Lista tipurilor de documente ce vor fi disponibile în cadrul sistemului și toate informațiile asociate vor fi definitivate în cadrul etapei de analiză a proiectului. Se vor avea în vedere documentele prezentate în capitolele anterioare.
- Vizualizarea de către angajatori și cetățeni a tuturor tipurilor de documente care trebuie completate și posibilitatea descărcării formularelor tipizate aferente acestor tipuri de documente.
- Completarea documentelor direct în cadrul unor formulare web, fără a fi nevoie descărcarea formularului tipizat. Semnarea documentelor în format electronic, sau încărcarea unor documente scanate care prezintă semnături ograf.
- Încărcarea documentelor completate în afara sistemului, inclusiv documente suport, acolo unde este cazul. Modulul trebuie să permită încărcarea documentelor inclusiv de pe dispozitive mobile. În cazul formularelor tipizate scanate și încărcate în cadrul sistemului, se vor putea extrage în mod automat anumite metadate pentru a permite indexarea și regăsirea lor ulterioară.
- Încărcarea documentelor generate și semnate electronic în afara sistemului, cu posibilitatea verificării semnăturii electronice.
- Vizualizarea tuturor documentelor încărcate anterior. Va permite modificarea sau ștergerea documentelor și a anexelor, cu respectarea ciclului de viață al fiecărui tip de document.
- Transmiterea spre înregistrare și validare către ITM a tuturor tipurilor de documente, conform procedurilor în vigoare. Pentru fiecare document în parte care poate fi transmis în cadrul sistemului vor fi definite un set de metadate minim obligatorii pentru a asigura procesarea lor optimă. Metadatele vor fi completate în mod automat în toate cazurile unde este posibil acest lucru (de exemplu: detaliile de identificare ale angajatorului).
- Validarea completării tuturor informațiilor necesare cu integrarea sistemelor ITM și a altor sisteme terțe cu care este necesară integrarea. În cazul în care nu este posibilă realizarea unei validări automate (de exemplu: eroare de conexiune cu un sistem terț sau informații indisponibile), acest lucru va fi marcat vizual, dar nu va împiedica transmiterea documentelor pe flux. Pentru fiecare din sistemele terțe cu care este necesară integrarea, Beneficiarul va realiza

demersurile administrative necesare obținerii acordului proprietarului sistemului pentru realizarea interoperabilității. Prestatorul trebuie să asigure suportul tehnic.

- Atenționarea utilizatorului în mod vizual și prin mesaje de eroare clare asupra erorilor de completare a documentelor (informații sau anexe lipsă, câmpuri necompletate sau completate necorespunzător)
- Urmărirea statusului documentelor transmise spre procesare în mod vizual. Fiecare etapă de validare va fi definită ca un pas într-un proces fiind posibilă astfel vizualizarea întregului flux al documentului atât pentru etapele automate, cât și pentru acelea unde este necesară procesarea de către un operator.
- Urmărirea solicitărilor de completare a documentelor/dosarelor transmise. Angajatorii vor avea posibilitatea de a răspunde acestor solicitări.
- Transmiterea notificărilor în mod automat conform fluxului definit de procesare a fiecărui tip de document. Notificările vor putea fi transmise prin email. Notificările vor putea fi transmise către un utilizator sau către un grup de utilizatori, în funcție de fluxul definit la momentul implementării.
- Înregistrarea automată a tuturor documentelor transmise către ITM în registratura electronică și generarea automată a numărului de înregistrare.
- Generarea și transmiterea automată a formularelor avizate de către ITM către angajator, acolo unde este cazul, în format needitabil, semnat electronic cu semnătură electronică (certificat de sistem).
- Arhivarea electronică a tuturor documentelor procesate în cadrul sistemului, cu posibilitatea consultării ulterioare.
- Încărcarea oricărui tip de document privitor la SSM primit în mod fizic la ghișeu de către operatorul ITM. Sistemul va permite completarea tuturor informațiilor necesare privind angajatorul pentru care se înregistrează documentul prin selecția acestuia din cadrul unui nomenclator preexistent.
- Definirea unor timpi standard de procesare pentru fiecare tip de document în parte, atât la nivel de proces, cât și la nivel de etapă în cadrul procesului, ținând cont de eventualele zile nelucrătoare sau sărbători legale, conform procedurilor operaționale ale ITM.
- Alocarea automată a documentelor spre procesare către o anumită persoană, un anumit rol sau un anumit grup de persoane (de exemplu un compartiment). De asemenea, în caz de nevoie, se va putea efectual modificarea operatorului alocat, în conformitate cu procedurile interne în vigoare.
- Vizualizarea tuturor documentelor asociate aceluiași dosar în cadrul fluxului de lucru. Operatorul alocat va putea modifica statusul procesului dacă este necesar, va putea adăuga observații sub formă de text sau alte documente suport și va putea solicita clarificări. În cazul în care pentru un anumit dosar sunt transmise documente adiționale, sistemul va permite înregistrarea acestor documente cu număr de înregistrare în Registratura electronică. Sistemul va lega logic cele două procese, permițând astfel vizualizarea centralizată a tuturor documentelor.
- Modificarea facilă a diferitor fluxuri de lucru aferente documentelor, direct din interfață, prin configurarea pașilor din proces, a persoanelor sau a grupurilor (compartimentelor) implicate sau a tipurilor de validări necesare.
- Adăugarea direct din interfață a unor noi tipuri de documente, modificarea celor existente și definirea metadatelor aferente acestora, respectiv a fluxurilor de procesare.

- Implementarea unei modalități de adăugare și urmărire în sistemul informatic a instruirilor și fiselor de instruire privind normele SSM pentru angajați.
- Sunt în scop pentru implementare minim următoarele fluxuri specifice activităților SSM:
    - Emitere autorizare de funcționare din punct de vedere SSM, precum și accesarea autorizărilor emise de către Registrul Comerțului (ONRC)
    - Gestiune evidență servicii externe de prevenire și protecție
    - Autorizare Monitorizare preparare, detinere, transport, depozitare, manuire materii explozive, muniții, substanțe, preparate chimice periculoase, agenti biologici, substante toxice.
    - Autorizare depozitare materii explosive
    - autorizare depozitare spatii muniții
    - Notificari substanțe, preparate chimice periculoase,
    - Notificari agenti biologici,
    - Evidenta autorizari substante toxice
    - Gestiune evidența artificierilor și pirotehnicienilor autorizați, autorizare cat si incetare activitate.
    - Declaratii prealabile santiere temporare și mobile
    - Notificări graviditate, modificari
    - Evidență organizare activitate de prevenire și protecție
    - Evidență convocatoare si rapoarte trimestriale CSSM
    - Evidență raportului anual in CSSM a conducatorului unitatii
    - Comunicarea evenimentelor
    - Completarea on-line a formularului de Proces Verbal de Cercetare și generarea versiunii imprimabile, inlcusiv de către angajator
    - Încărcarea dosarului de cercetare a evenimentului, inclusiv Procesul Verbal de Cercetare semnat/ asumat, inclusiv de către angajator
    - FIAM
    - Anexa FIAM împreună cu documentele justificate privind încheieirea perioadei de incapacite temporară de muncă
    - Îndeplinirea măsurilor dispuse cu ocazia controalelor cât și cu ocazia cercetării evenimentelor
    - Registre evidenta evenimente/ accidentați
    - Registru unic de evidenta al zilierilor accidentati in munca
    - Procesul de avizare al documentaţiilor cu caracter tehnic de informare și instruire în domeniul SSM
    - Notificare privind începerea activităţilor cu expunere la pulberea degajată de azbest
    - Evidenta anexa 29 – Informare privind producerea in afara granitelor tarii a unui eveniment considerat accident de munca
    - Constatarea de lipsuri la materiile explozive sosite în depozitele autorizate HG 536/2002
    - Neconcordanțe între stocul faptic și cel scriptic de materii explozive din depozit HG 536/2002
    - Evidenta angajatorilor care au locuri de munca in conditii speciale si/sau deosebite
    - Evidenta locurilor de munca incadrate in conditii speciale si/sau deosebite
    - Declarare si raportare boli profesionale

Emitere autorizare de funcționare din punct de vedere SSM.

Pentru SIAMC 2.0 sunt în scop cel puțin următoarele:

- introducerea posibilității de solicitare și eliberare online a autorizației (certificatului constatator)
- posibilitatea evidențierii eliberării autorizațiilor rezultate din solicitările depuse la ghișeu
- pentru autorizarile efectuate prin Registrul Comertului – sa existe posibilitatea vizualizarii si printarii certificatelor constatatoare din sistem

Flux de solicitare și eliberare integral online

Posibilitatea lansării și procesării solicitărilor de către angajator din sistem:

- solicitarea presupune completarea unui formular web, generarea documentului specific solicitării pe baza unui tipizat, semnarea electronica și transmiterea acestuia împreună cu toate documentele justificative
- Înregistrarea solicitării în momentul depunerii documentației
- Existența un mecanism automat de transmitere/direcționare automată a cererilor către departamentul specializat pentru eliberarea autorizației SSM al ITM-ului din județul unde angajatorul are sediul social
- Preluarea solicitărilor de către un grup de utilizatori cu drepturi elevate (șef serviciu) care alocă solicitarea responsabililor de prelucrare a cererilor
- Existența unui mecanism de afișare și avertizare pentru lucrătorii ITM din departamentul specializat privind prelucrarea solicitării în termenul legal (30 de zile)
    - De exemplu notificări cu x zile înainte de expirarea termenului
- Posibilitatea solicitării de completări/clarificări în urma analizei dosarului din cadrul SIAMC
    - Solicitarea de clarificări să permită completarea detaliilor, generarea adresei de informare a angajatorului cu posibilitatea de semnare electronică de către ITM și transmiterea/notificarea angajatorului
- Eliberarea autorizației prin generarea documentului, semnarea electronică de către ITM și informarea angajatorului asupra eliberării documentului cu posibilitatea de listare a documentului si transmiterea autorizației angajatorului.
- Flux de solicitare și eliberare hibrid (depunere la ghișeu dar cu formalizarea rezoluției în sistem)
- Pentru situațiile când cererile se depun fizic - procesarea cererii se va realiza offline, in sistem se va încărca documentul final (certificatul constatator de autorizare a funcționării)
- Notificarea prin email a angajatorului
- Utilizarea datelor introduse pentru inspectori în activitatea de control (accesarea informațiilor fie direct în profilele angajatorilor, fie din Registrul Comertului, fie prin rapoarte specifice)
- Posibilitatea evidențierii modalității de eliberare și transmitere a documentului către angajator:
    - Autorizație semnată electronic -transmitere electronică în cadrul sistemului
    - Autorizație semnată olograf cu transmitere prin poștă
- Inspecția Muncii va analiza oportunitatea actualizării procedurilor interne privind modalitatea de eliberare a autorizației:
    - fie se va realiza fie olograf fie electronic în funcție de solicitarea angajatorului sau
    - autorizațiile se vor elibera integral în format electronic indiferent de sursa solicitării.

Gestiune evidență servicii externe de prevenire și protecție

Presupune procesarea electronică a procesului privind abilitarea firmelor care solicită să presteze servicii externe de prevenire și protecție.

Transmiterea unei atentionari inspectorilor de munca in situatia in care serviciul extern nu mai functioneaza sau i s-a retras abilitarea sau daca exista modificari in structura acestuia.

Flux de solicitare și eliberare integral online

- Publicarea pe portalurile ITM-urilor a datelor privind întrunirea comisiilor
- Posibilitatea depunerii cererilor de către angajatorii autentificați
    - trebuie sa existe și un flux de înregistrare a angajatorilor străini care pot solicita și deveni furnizori de servicii externe de prevenire și protecție
- Direcționarea cererilor către departamentul specializat din ITM-ul județului corespondent sediului social al angajatorului si apoi catre secretariatul comisiei de abilitare.
- Posibilitatea de a solicita completări/clarificări în cadrul sistemului
- Încărcarea rezoluției finale (decizia comisiei și a documentului eliberat) în sistem, cu notificarea solicitantului.
- în momentul abilitării – transmiterea unei notificări privind drepturile elevate pe care le primește utilizatorul astfel încât să poată realiza raportarea semestrială

Evidențierea în sistem a abilitării firmelor care au solicitat acest lucru la ghișeu

- Pentru cererile depuse fizic la ghișeu, se vor încărca rezoluțiile de către lucrătorii ITM astfel încât sistemul să conțină evidența tuturor celor autorizați să presteze servicii externe de prevenire și protecție

Constituirea și actualizarea structurii serviciului extern

- Posibilitatea afișării în sistem a structurii serviciului extern prin preluarea persoanelor și a funcțiilor (șef și lucrători) din cererea de abilitare precum și posibilitatea de actualizare/modificare a structurii serviciului extern în momentul depunerii documentelor de modificare
- Modificarea se va realiza printr-un flux similar cu obținerea abilitării, comisia întrunită analizând atât cererile noi de abilitare cât și modificările.
- Existența unui mecanism de verificare automată a datelor persoanelor introduse în formular astfel încât solicitantul și lucrătorii ITM să fie avertizați în cazul în care persoana nominalizată pentru poziția de conducător al serviciul extern în cadrul unei cereri de abilitare sau actualizare a structurii să nu aibă deja aceeași calitate in cadrul altui serviciu extern
- E xistența unui mecanism de verificare si avertizare automată a lucratorilor ITM in situatia incetarii/suspendarii CIM a persoanei nominalizate pentru poziția de conducător al serviciul extern

Flux de raportare semestrială

- Posibilitatea realizării automate a unei raportări semestriale în baza datelor existente în sistem, care va putea fi semnat electronic sau olograf de către angajator.
- Configurarea de notificări de atenționare a angajatorului privind apropierea termenului de raportare semestrială. Raportul trebuie să fie transmis automat, la sfarșitul semestrului, cu informarea comisiei că a fost transmis. Totodata comisia trebuie să poată vizualiza acest raport, iar in cazul unor greșeli, să îl poată corecta.

- Notificarea ITM in situatia in care nu s-au transmis doua rapoarte semestriale consecutive. Notificari si catre comisia de abilitare a serviciilor externe

Retragerea autorizației

Măsura de retragere a autorizației se impune în situațiile în care furnizorul de servicii nu depune 2 rapoarte consecutive sau dacă se modifică componența structurii serviciului și ITM-ul nu a fost notificat.

Toate informațiile/datele preluate sub orice forma de catre sistem se vor regasi in campurile aferente din fisa unitatii.

Din punct de vedere al cerințelor funcționale, se dorește:

- Configurarea de notificări pentru informarea inspectorilor:
  - În ziua expirării termenului de depunere a raportării semestriale
  - În ziua îndepliniri condițiilor cumulative pentru retragerea autorizației
  - La momentul încetării contractului individual de muncă al conducătorului serviciului extern pe baza datelor transmise în ReGES
- Posibilitatea formalizării retragerii autorizației. Lucrătorii ITM responsabili vor putea genera documentul de retrage a autorizației în baza unui formular standardizat, precompletat cu datele existente în sistem și încărca ulterior documentul aprobat, acțiune care va retrage accesul de raportare a angajatorului, acesta rămânând cu dreptul de a vizualiza raportările efectuate până în acel punct

Publicarea pe portal a datelor de contact a firmelor abilitate să furnizeze servicii externe de prevenire și protecție

- se va genera si publica într-o zona a portalului public - lista firmelor abilitate. Lista se va actualiza automat in urma operării în sistem privind autorizarea/retragerea abilitării - cu posibilitatea de căutare si filtrare (ex pe județe).

Monitorizare materii explozive

Materii explozive

Flux de obținere a autorizației pentru depozit

- Posibilitatea de a solicita online sau de formalizare a rezoluției solicitărilor primite la ghișeu cu următoarele aspecte:
  - Completarea unui formular specific, generarea documentelor pe baza unui șablon și depunerea solicitării
  - Depunere documente on line in vederea obtinerii autorizatiei pentru depozit
  - Posibilitatea de a solicita și primi clarificări/completări în cadrul sistemului
  - In cazul depunerii documentatiei la ghiseu, sa existe posibilitatea incarcarii documentelor in sistem.
  - Eliberarea sau respingerea solicitării de eliberarea a autorizației

Flux de obținere a autorizației de deținere, transport, manipulare

- Posibilitatea de a solicita online sau de formalizare a rezoluției solicitărilor primite la ghișeu
  - Completarea unui formular specific, generarea documentelor pe baza unui șablon și depunerea solicitării
  - Depunere documente on line in vederea obtinerii autorizatiei pentru detinere, transport, manipulare
  - Posibilitatea de a solicita și primi clarificări/completări în cadrul sistemului
  - Eliberarea sau respingerea solicitării de eliberarea a autorizației

- In cazul depunerii documentatiei la ghiseu, sa existe posibilitatea incarcarii documentelor in sistem

Flux de obținere a avizului de începere

- Posibilitatea de a solicita online sau de formalizare a rezoluției solicitărilor primite la ghișeu
  - Completarea unui formular specific, generarea documentelor pe baza unui șablon și depunerea solicitării
  - Depunere documente on line in vederea obtinerii avizului de incapere
  - Posibilitatea de a solicita și primi clarificări/completări în cadrul sistemului
  - Eliberarea sau respingerea solicitării de eliberarea a avizului

Posibilitatea retragerii autorizațiilor și avizelor

- Să existe un mecanism de retragere a autorizației in sistem coroborat cu activitatea de control astfel încât să se poată realiza maparea/asocierea retragerii cu activitatea de control din modulul de Monitorizare și Control.

Monitorizarea situației existente

- Notificarea angajatorului și a lucrătorilor ITM cu x zile înaintea expirării autorizării
- Din punct de vedere al raportării/activității de control – inspectorii trebuie să poată vedea ca la căutarea după un CUI toate punctele de lucru care sunt autorizate/avizate pentru astfel de activități astfel încât să nu fie necesară navigarea pagină cu pagină în toate punctele de lucru al unei firme care are mai multe autorizații/avize.
- Sistemul trebuie să evidențieze termenii depășiți privind reînnoirea autorizațiilor

Monitorizare muniții

Flux de obținere a autorizației

- Posibilitatea de a solicita online sau de formalizare a rezoluției solicitărilor primite la ghișeu cu următoarele aspecte:
  - Completarea unui formular specific, generarea documentelor pe baza unui șablon și depunerea solicitării
  - Depunere documente on line in vederea obtinerii autorizatiei
  - Posibilitatea de a solicita și primi clarificări/completări în cadrul sistemului
  - Eliberarea sau respingerea solicitării de eliberarea a autorizației
  - In cazul depunerii documentatiei la ghiseu, sa existe posibilitatea incarcarii documentelor in sistem.

Monitorizare substanțe și preparate chimice periculoase

Posibilitatea de notificare a ITM-ului de către angajator asupra substanțelor chimice perioculoase pe care le utilizează în punctul de lucru din județul respectiv

- Are scop declarativ/informativ – nu se obține autorizație sau aviz
- Adăugarea datelor privind substanțele să se facă în mod facil pentru a ușura ulterior activitatea de control (de exemplu posibilitatea de utilizare a unui nomenclator pentru substanțe sau pe categorii de substanțe – având în vedere numărul mare al acestora)

Monitorizare agenti biologici

Posibilitatea de notificare a ITM-ului de către angajator asupra agentilor biologici pe care ii utilizează în punctul de lucru din județul respectiv

- Are scop declarativ/informativ – nu se obține autorizație sau aviz

- Adăugarea datelor privind agentii biologici să se facă în mod facil pentru a ușura ulterior activitatea de control (de exemplu posibilitatea de utilizare a unui nomenclator pentru agenti biologici sau pe categorii de agenti biologici – având în vedere numărul mare al acestora)

Monitorizare substante toxice

Posibilitatea de notificare a ITM-ului de către angajator asupra substantelor toxice pe care le utilizează în punctul de lucru din județul respectiv

- Are scop declarativ/informativ – nu se obține autorizație sau aviz
- Adăugarea datelor privind substantele toxice să se facă în mod facil pentru a ușura ulterior activitatea de control (de exemplu posibilitatea de utilizare a unui nomenclator pentru substanțe sau pe categorii de substanțe – având în vedere numărul mare al acestora)

AUTORIZARE ARTIFICIERI, PIROTEHNISTI

Gestiune evidența artificierilor și pirotehnicienilor autorizați.

Activitatea presupune gestionarea obținerii calității de artificier sau pirotehnician autorizat și se obține de către persoane fizice.

Desfășurarea concursurilor și a rezultatelor nu sunt în scop

- Depunerea online a documentelor de solicitare de către persoana care dorește să obțină carnetul de artificier/pirotehnist
- Procesarea cererii prin mecanismul de direcționare către șefii de serviciu al ITM-ului responsabil și delegarea lucrării lucrătorului din cadrul departamentului specializat
- Incarcarea in sistem a testelor de verificare a artificierilor/pirotehnistilor
- Incarcarea in sistem a procesului verbal intocmit de catre comisia de examinare artificieri/pirotehnistilor, chiar redactarea acestuia
- Încărcarea rezoluției în sistem (chiar dacă carnetul se va elibera în continuare fizic)
- Posibilitatea formalizării rezoluției și celor care depun cererile la ghișeu
- Posibilitatea informării ITM-urilor privind modificarea reședinței astfel încât în lista pirotehnicienilor/artificierilor să se vadă ITM-ul de care aparține precum și istoricul mobilității acestuia
    - Se dorește existența unui mecanism de informare/atenționare/notificare a persoanei autorizate și a angajatorului asupra obligației notificării ITM pentru transfer
- Posibilitatea încărcării în sistem a dovezii susținerii testului psihologic anual pentru păstrarea carnetului
- Pentru angajatori trebuie să existe:
    - un mecanism de asociere a persoanelor fizice autorizate cu verificarea în sistem a faptului că au calitatea de artificier/pirotehnist
    - posibilitatea actualizării listei (evidențierea intrării și plecării angajaților calificați în aceste domenii)
- Pentru inspectorii de muncă în urma datelor colectate în aplicație trebuie să existe minim posibilitatea de a vedea atât sub forma unui raport cât și la căutarea după CNP a datelor privind persoanele autorizate:

- tipul autorizațiilor deținute (artificier, pirotehnist, ambele)
- data obținerii
- istoricul angajatorilor
- istoricul suspendărilor, anulărilor, retragerilor – dacă există

ȘANTIERE TEMPORARE ȘI MOBILE

- posibilitatea încărcării informațiilor (eventual cu posibilitatea de a genera declarația și a o semna electronic) de către firmă sau de către operatorul ITM dacă angajatorul depune declarația la ghișeu
- afișarea unei liste a șantierelor declarate cu posibilitatea de căutare a datelor completate în formulare precum și filtrarea/selectarea pe perioade pentru identificarea șantierelor active
    - pentru activitatea de control să existe posibilitatea extragerii unui raport cu toate locațiileunde se fac lucrări pe baza acestor declarații
    - evidenta informarilor

NOTIFICĂRI GRAVIDITATE

Aceste înregistrări au scop informativ astfel încât inspectorii sa poată vedea dacă angajatorii au declarat acest lucru.

- Posibilitatea angajatorului de a adăuga un sistem/depune o notificare de informare pentru angajata care este gravidă.
- posibilitatea încărcării informațiilor din notificare (cu posibilitatea de a genera notificarea și a o semna electronic) de către firmă sau de către operatorul ITM dacă angajatorul depune declarația la ghișeu
- evidenta informarilor

SERVICII INTERNE DE SSM

Evidență organizare activitate de prevenire și protecție

- Posibilitatea angajatorului să își declare modalitatea de organizarea activitate de prevenire și protecție (serviciu extern sau declararea lucrătorului desemnat) – nivelul de detaliere va fi stabilit în etapa de analiză.

Comitete de Securitate si Sanatate in Munca

Evidenta convocatoare si rapoarte trimestriale CSSM

Activitatea presupune gestionarea activitatii CSSM

Aceste înregistrări au scop informativ pentru inspectorii de munca din cadrul ITM.

Posibilitatea încărcării informațiilor (cu posibilitatea de a genera convocatorul și al semna electronic) de către firmă sau de către operatorul ITM dacă angajatorul depune declarația la ghișeu

Evidenta raportului anual in CSSM a conducatorului unitatii

Activitatea presupune gestionarea activitatii CSSM

Aceste înregistrări au scop informativ pentru inspectorii de munca din cadrul ITM.

Posibilitatea încărcării informațiilor (cu posibilitatea de a genera raportul anual și al semna electronic) de către firmă sau de către operatorul ITM dacă angajatorul depune declarația la ghișeu

Instruirea din punct de vedere al securitatii si sanatatii in munca

Implementarea unei modalități de adăugare și urmărire în sistemul informatic a instruirilor și fiselor de instruire in domeniul SSM pentru angajați.

Activitatea presupune gestionarea activitatii de instruire la nivelul angajatorilor

Posibilitatea incarcarii in sistem cel putin a informatiilor referitoare la unitate, conducator unitate, conducator loc de munca, tipul de instruire, persoana instruita, data instruirii, durata instruirii, materialul prelucrat, semnaturile electronice/olografe ale tuturor factorilor implicati in procesul de instruire, rezultatele examinarilor medicale, traseul de deplasare de la domiciliu si invers, durata acestei deplasari, etc.

ACCIDENTE

Fișa de Comunicare a evenimentelor

Activitatea presupune gestionarea evenimentelor in cadrul ITM

Aceste înregistrări au scop informativ pentru inspectorii de munca din cadrul ITM.

Posibilitatea încărcării informațiilor (cu posibilitatea de a genera comunicarea și a o semna electronic) de către firmă sau de către operatorul ITM dacă angajatorul depune declarația la ghișeu

Posibilitatea transmiterii comunicarii evenimentelor care intra in competenta de cercetare a ITM catre Inspectia Muncii

Dosar de Cercetare

Pentru cercetarea efectuata de catre angajator - victima/victime lucratori

Activitatea presupune intocmirea, gestionarea, evidenta si arhivarea dosarelor de cercetare intocmite de catre angajatori

Activitatea presupune întocmirea și transmiterea dosarului de cercetare intocmit de catre angajator, potrivit competentelor de cercetare, la ITM în vederea avizării

Emiterea avizului/respingerea dosarului de catre ITM

Aceste înregistrări au scop informativ pentru inspectorii de munca din cadrul ITM.

Pentru cercetarea efectuata de catre inspectoratele teritoriale de munca - victima/victime lucratori

Activitatea presupune intocmirea, gestionarea, evidenta si arhivarea dosarelor de cercetare intocmite de catre inspectoratele teritoriale de munca si inaintarea acestora la Inspectia Muncii in vederea avizarii

Activitatea presupune întocmirea și transmiterea dosarului de cercetare intocmit de catre angajator, potrivit competentelor de cercetare, la IM în vederea avizării

Emiterea avizului de catre IM

Pentru cercetarea efectuata de catre ITM - victima/victime zilieri

Activitatea presupune întocmirea și transmiterea dosarului de cercetare intocmit de catre angajator, potrivit competentelor de cercetare, la IM în vederea avizării

Emiterea avizului/respingerea dosarului de catre IM

Aceste înregistrări au scop informativ pentru inspectorii de munca din cadrul ITM

Fluxurile de mai sus nu sunt limitative, acestea putând fi completate/modificate în funcție de cerințelele legislației în domeniul SSM.

FIAM

Activitatea presupune gestionarea evenimentelor in cadrul ITM

Aceste înregistrări au scop informativ pentru inspectorii de munca din cadrul ITM.

Posibilitatea încărcării informațiilor (cu posibilitatea de a genera FIAM și al semna electronic) de către firmă sau de către operatorul ITM dacă angajatorul depune declarația la ghișeu.

Posibilitatea de a genera rapoarte functie de campurile cuprinse in acest formular.

Anexa FIAM împreună cu documentele doveditoare

Activitatea presupune gestionarea evenimentelor in cadrul ITM

Aceste înregistrări au scop informativ pentru inspectorii de munca din cadrul ITM.

Posibilitatea încărcării informațiilor (cu posibilitatea de a genera Anexa FIAM și al semna electronic) de către firmă sau de către operatorul ITM dacă angajatorul depune declarația la ghișeu.

Posibilitatea de a genera rapoarte functie de campurile cuprinse in acest formular.

Registre evidenta accidente - (accidentați in muncă - 3 zile ITM, incidente periculoase, accidente ușoare, accidentați cu mai mult de 3 zile de incapacitate temporară de muncă)

Activitatea presupune gestionarea evenimentelor in cadrul ITM

Aceste înregistrări au scop informativ pentru inspectorii de munca din cadrul ITM.

Înregistrarea automata a evenimentelor in registrele de evidenta existente la nivelul inspectoratelor

Înregistrarea automata a Anexei FIAM in registrele de evidenta existente la nivelul inspectoratului

Calcularea indicatorilor specifici - frecventa, gravitate, indice de durata medie

Registru unic de evidenta al zilierilor accidentati in munca

Activitatea presupune gestionarea evenimentelor in cadrul ITM

Aceste înregistrări au scop informativ pentru inspectorii de munca din cadrul ITM.

Înregistrarea automata a evenimentelor în care sunt implicați zilieri în registrele de evidență existente la nivelul inspectoratelor.

Evidenta anexa 29 – Informare privind producerea in afara granitelor tarii a unui eveniment considerat accident de munca

Activitatea presupune gestionarea evenimentelor in cadrul ITM

Aceste înregistrări au scop informativ pentru inspectorii de munca din cadrul ITM.

Posibilitatea încărcării informațiilor (cu posibilitatea de a genera Anexa 29 și a o semna electronic) de către CNPAS/CJPAS

DOCUMENTATII CU CARACTER TEHNIC DE INFORMARE SI INSTRUIRE

Avizarea documentaţiilor cu caracter tehnic de informare și instruire în domeniul SSM

Activitatea presupune gestionarea documentaţiilor cu caracter tehnic de informare și instruire în domeniul SSM avizate de Comisia de abilitare din cadrul ITM

Aceste înregistrări au scop informativ pentru inspectorii de munca din cadrul ITM.

Posibilitatea încărcării informațiilor (cu posibilitatea de a incarca documentatia și a o semna electronic) de către firmă sau de către operatorul ITM dacă angajatorul depune documentația la ghișeu

AZBEST

Notificare privind începerea activităţilor cu expunere la pulberea degajată de azbest

Activitatea presupune gestionarea activităţilor cu expunere la pulberea degajată de azbest in cadrul ITM

Aceste înregistrări au scop informativ pentru inspectorii de munca din cadrul ITM.

MATERII EXPLOZIVE

Constatarea de lipsuri la materiile explozive sosite în depozitele autorizate HG 536/2002

Activitatea presupune gestionarea neconformitatilor privind materiile explozive

Aceste înregistrări au scop informativ pentru inspectorii de munca din cadrul ITM.

Neconcordanțe între stocul faptic și cel scriptic de materii explozive din depozit HG 536/2002

Activitatea presupune gestionarea neconformitatilor privind materiile explozive

Aceste înregistrări au scop informativ pentru inspectorii de munca din cadrul ITM.

CONDITII DEOSEBITE /SPECIALE

Evidenta angajatorilor care au locuri de munca in conditii speciale si/sau deosebite

Activitatea presupune gestionarea angajatorilor care au locuri de munca in conditii speciale si/sau deosebite

Activitatea presupune gestionarea masurilor stabilite la nivelul angajatorilor care au locuri de munca in conditii speciale si/sau deosebite

Aceste înregistrări au scop informativ pentru inspectorii de munca din cadrul ITM.

Evidența locurilor de munca încadrate în condiții speciale și/sau deosebite

Activitatea presupune gestionarea evidentei locurilor de munca incadrate in conditii speciale si/sau deosebite

Activitatea presupune gestionarea masurilor stabilite la nivelul angajatorilor care au locuri de munca in conditii speciale si/sau deosebite.

Aceste înregistrări au scop informativ pentru inspectorii de munca din cadrul ITM.

3.2.6.4 Accidente (Evenimente)

3.2.6.4.1 Preambul

Definiții și clasificare

Prin eveniment se înțelege accidentul care a antrenat decesul sau vătămări ale organismului, produs în timpul procesului de muncă ori în îndeplinirea îndatoririlor de serviciu, situaţia de persoană dată dispărută sau accidentul de traseu ori de circulaţie, în condiţiile în care au fost implicate persoane angajate, incidentul periculos, precum şi cazul susceptibil de boală profesională sau legată de profesiune.

Prin accident de muncă se înțelege vătămarea violentă a organismului, precum și intoxicația acută profesională, care au loc în timpul procesului de muncă sau în îndeplinirea îndatoririlor de serviciu și care provoacă incapacitate temporară de muncă de cel puțin 3 zile calendaristice, invaliditate ori deces.

Conform Legii 319/2006, este, de asemenea, accident de muncă:

- accidentul suferit de persoane aflate în vizită în întreprindere, cu permisiunea angajatorului;
- accidentul suferit de persoanele care îndeplinesc sarcini de stat sau de interes public, inclusiv în cadrul unor activități culturale, sportive, în țară sau în afara granițelor țării, în timpul și din cauza îndeplinirii acestor sarcini;

- accidentul survenit în cadrul activităților cultural sportive organizate, în timpul și din cauza îndeplinirii acestor activități;
- accidentul suferit de orice persoană ca urmare a unei acțiuni întreprinse din propria inițiativă pentru salvarea de vieți omenești, precum și accidentul suferit în timpul intervenției de urgență sau al pregătirii în vederea participării la aceasta, pe durata efectuării serviciului de voluntariat organizat conform prevederilor legale;
- accidentul suferit de orice persoană, ca urmare a unei acțiuni întreprinse din proprie inițiativă pentru prevenirea ori înlăturarea unui pericol care amenință avutul public și privat;
- accidentul cauzat de activități care nu au legătură cu procesul muncii, dacă se produce la sediul persoanei juridice sau la adresa persoanei fizice, în calitate de angajator, ori în alt loc de muncă organizat de aceștia, în timpul programului de muncă, și nu se datorează culpei exclusive a accidentatului;
- accidentul de traseu, dacă deplasarea s-a făcut în timpul și pe traseul normal de la domiciliul lucrătorului la locul de muncă organizat de angajator și invers;
- accidentul suferit în timpul deplasării de la sediul persoanei juridice sau de la adresa persoanei fizice la locul de muncă sau de la un loc de muncă la altul, pentru îndeplinirea unei sarcini de muncă;
- accidentul suferit în timpul deplasării de la sediul persoanei juridice sau de la adresa persoanei fizice la care este încadrată victima, ori de la orice alt loc de muncă organizat de acestea, la o altă persoană juridică sau fizică, pentru îndeplinirea sarcinilor de muncă, pe durata normală de deplasare;
- accidentul suferit înainte sau după încetarea lucrului, dacă victima prelua sau preda uneltele de lucru, locul de muncă, utilajul ori materialele, dacă schimba îmbrăcămintea personală, echipamentul individual de protecție sau orice alt echipament pus la dispoziție de angajator, dacă se afla în baie ori în spălător sau dacă se deplasa de la locul de muncă la ieșirea din întreprindere sau unitate și invers;
- accidentul suferit în timpul pauzelor regulamentare, dacă acesta a avut loc în locuri organizate de angajator, precum și în timpul și pe traseul normal spre și de la aceste locuri;
- accidentul suferit de lucrători ai angajatorilor români sau de persoane fizice române, delegați pentru îndeplinirea îndatoririlor de serviciu în afara granițelor țării, pe durata și traseul prevăzute în documentul de deplasare;
- accidentul suferit de personalul român care efectuează lucrări și servicii pe teritoriul altor țări, în baza unor contracte, convenții sau în alte condiții prevăzute de lege, încheiate de persoane juridice române cu parteneri străini, în timpul și din cauza îndeplinirii îndatoririlor de serviciu;
- accidentul suferit de cei care urmează cursuri de calificare, recalificare sau perfecționare a pregătirii profesionale, în timpul și din cauza efectuării activităților aferente stagiului de practică;
- accidentul determinat de fenomene sau calamități naturale, cum ar fi furtună, viscol, cutremur, inundație, alunecări de teren, trăsnet (electrocutare), dacă victima se afla în timpul procesului de muncă sau în îndeplinirea îndatoririlor de serviciu;
- dispariția unei persoane, în condițiile unui accident de muncă și în împrejurări care îndreptățesc presupunerea decesului acesteia;
- accidentul suferit de o persoană aflată în îndeplinirea atribuțiilor de serviciu, ca urmare a unei agresiuni.

Accidentele de muncă se clasifică, în raport cu urmările produse și cu numărul persoanelor accidentate, în:

- accidente care produc incapacitate temporară de muncă de cel puțin 3 zile calendaristice;
- accidente care produc invaliditate (prin invaliditate se înțelege pierdere parțială sau totală a capacității de muncă, confirmată prin decizie de încadrare într-un grad de invaliditate, emisă de organele medicale în drept);
- accidente mortale;
- accidente colective, când sunt accidentate cel puțin 3 persoane în același timp și din aceeași cauză.

Procedura de comunicare, cercetare și înregistrare

Conform legii, angajatorul are obligația să comunice evenimentele, de îndată, după cum urmează:

- inspectoratelor teritoriale de muncă;
- asigurătorului, potrivit Legii nr. 346/2002 privind asigurarea pentru accidente de muncă și boli profesionale, evenimentele urmate de incapacitate temporară de muncă, invaliditate sau deces, la confirmarea acestora;
- organelor de urmărire penală, după caz.

Angajatorii au obligația să declare toate evenimentele și nu doar pe acelea care reprezintă accident de munca. Prin eveniment, se înțelege accidentul care a antrenat decesul sau vătămări ale organismului, produs în timpul procesului de muncă ori în îndeplinirea îndatoririlor de serviciu, situația de persoană dată dispărută sau accidentul de traseu ori de circulație, în condițiile în care au fost implicate persoane angajate, incidentul periculos, precum și cazul susceptibil de boală profesională sau legată de profesiune.

Important de menționat este și faptul că, dacă printre victimele evenimentului se află și lucrători ai altor angajatori, evenimentul va fi comunicat și angajatorilor acestora de către angajatorul la care s-a produs evenimentul.

De asemenea, în cazul evenimentelor produse în afara granițelor țării, în care sunt implicați lucrători ai unor angajatori români, angajatorul are obligația de a comunica evenimentul și misiunii diplomatice sau oficiului consular român din țara respectivă.

Comunicarea evenimentelor se va face conform modelului prevăzut în anexa nr. 13 din Normele metodologice de aplicare a prevederilor Legii 319/2006.

Angajatorii au obligația legală, de a lua măsurile necesare pentru a nu se modifica starea de fapt rezultată din producerea evenimentului, până la primirea acordului din partea organelor care efectuează cercetarea, cu excepția cazurilor în care menținerea acestei stări ar genera producerea altor evenimente, ar agrava starea accidentaților sau ar pune în pericol viața lucrătorilor și a celorlalți participanți la procesul muncii.

Cercetarea evenimentelor are ca scop stabilirea împrejurărilor și a cauzelor care au condus la producerea acestora, a reglementărilor legale încălcate, a răspunderilor și a măsurilor ce se impun a fi luate pentru prevenirea producerii altor cazuri similare și, respectiv, pentru determinarea caracterului accidentului.

Cercetarea evenimentelor este obligatorie și se efectuează după cum urmează:

- de către angajator, în cazul evenimentelor care au produs incapacitate temporară de muncă;
- de către ITM, în cazul evenimentelor care au produs invaliditate evidentă sau confirmată, deces, accidente colective, incidente periculoase, în cazul evenimentelor care au produs incapacitate temporară de muncă lucrătorilor la angajatorii persoane fizice, precum și în situațiile cu persoane date dispărute. Invaliditate confirmată reprezintă o pierdere parțială sau totală a capacității de muncă, confirmată prin decizie de încadrare într-un grad de invaliditate, emisă de organele medicale în drept, pe când prin noțiunea de invaliditate evidentă se are în vedere pierderea capacității de muncă datorată unor vătămări evidente, cum ar fi un braț smuls din

umăr, produse în urma unui eveniment, până la emiterea deciziei de încadrare într-un grad de invaliditate de către organele medicale în drept.

- de către Inspecția Muncii, în cazul accidentelor colective, generate de unele evenimente deosebite, precum avariile sau exploziile;
- de către autoritățile de sănătate publică teritoriale, respectiv a municipiului București, în cazul suspiciunilor de boală profesională și a bolilor legate de profesiune.

Cercetarea se face imediat după comunicare. Dacă cercetarea se face, potrivit legii, de către angajator, acesta are obligația să numească de îndată, prin decizie scrisă, comisia de cercetare a evenimentului, care va fi compusă din cel puțin 3 persoane, dintre care o persoană trebuie să fie, după caz lucrător desemnat, reprezentant al serviciului intern de prevenire și protecție sau reprezentant al serviciului extern de prevenire și protecție, cu pregătire corespunzătoare conform legii.

Cercetarea presupune întocmirea unor note de constatare la fața locului, prelevare de probe de la locul accidentului, întocmirea unor schițe, efectuarea unor fotografii, audierea accidentaților, audierea persoanelor prezenta, corespondența cu alte instituții/unități în vederea obținerii actelor solicitate etc. De asemenea, pentru cercetarea evenimentelor se pot solicita experți sau specialiști, aceștia având obligația să răspundă solicitării.

Cu anumite excepții, când se poate solicita prelungirea termenului, termenele de cercetare sunt stabilite astfel:

- cel mult 10 zile lucrătoare de la data producerii – în cazul evenimentului urmat de incapacitate temporară de muncă
- cel mult 15 zile lucrătoare de la data producerii acestora – în cazul evenimentelor care au avut ca urmare deces, invaliditate evidentă, invaliditate confirmată ulterior, a accidentelor colective sau a situațiilor de persoane date dispărute, precum și cercetarea incidentelor periculoase
- Cercetarea se va finaliza cu întocmirea unui dosar care va cuprinde, pe lângă alte documente imperativ prevăzute de lege, procesul verbal de cercetare, document în cuprinsul căruia se vor consemna toate detaliile evenimentului, inclusiv cauza și urmările acestuia, descrierea echipamentelor de muncă și protecție, modul de efectuare a cercetării, reglementările legale încălcate și persoanele responsabile de încălcarea acestora și alte elemente prevăzute de lege.

Dosarul de cercetare, întocmit de comisia numită de către angajator, se înaintează pentru verificare și avizare la ITM-ul pe raza căruia s-a produs evenimentul, în termen de 5 zile lucrătoare de la finalizarea cercetării, urmând ca ITM-ul să analizeze, avizeze și restituie dosarul în cel mult 7 zile lucrătoare de la data primirii. Dosarul de cercetare original, întocmit de ITM va fi înaintat în vederea avizării la Inspecția Muncii, în cel mult 5 zile lucrătoare de la finalizarea cercetării.

În baza procesului-verbal de cercetare întocmit de persoanele împuternicite, conform legii, angajatorul are obligația să înregistreze accidentul de munca în registrele de evidență prevăzute de lege și să completeze FIAM (Formular pentru Înregistrarea Accidentului de Muncă), care va trebui la rândul lui avizat de ITM. La finalizarea perioadei de incapacitate temporară de muncă a accidentatului în muncă se intocmește, de catre angajator, anexa la FIAM care se inaintează ITM teritorial spre informare.

Declarare si raportare boli profesionale

Procesul-verbal de cercetare a cazului de boala profesionala se intocmeste de catre medicul de medicina muncii din cadrul directiei de sanatate publica judetene si a municipiului Bucuresti, din care un exemplar se transmite catre inspectoratul teritorial de munca

Fisa de declarare a cazului de boala profesionala BP2 se comunica la inspectoratul teritorial de munca

3.2.6.4.2 Cerințe funcționale

Scopul acestui modul este de a permite completarea, înregistrarea și gestiunea întregului flux de validare a diferitelor tipurilor de documente (notificări), în vederea îndeplinirii obligațiilor specifice angajatorilor în ceea ce privește evenimentele, în conformitate cu cadrul legal în vigoare la momentul implementării sistemului, și pe toată durata perioadei de suport tehnic și garanție ofertată.

Acest modul va dispune de o zonă publică (front-office), accesibilă prin intermediul portalului web, dedicată operatorilor economici (angajatorilor) și cetățenilor, precum și de o zonă privată (back-office) dedicată personalului din cadrul IM/ITM. Accesul va fi posibil numai după autentificare, iar informațiile afișate vor depinde de rolului utilizatorului conectat în sistem.

Vor fi implementate minim următoarele fluxuri specifice activităților SSM / Evenimente - Accidente de muncă, în conformitate cu prevederile legale în vigoare:

- Comunicare eveniment de către angajator
- Cercetare eveniment:
    - de către angajator
    - de către Inspectoratele Teritoriale de Munca
    - de către Inspectia Muncii
- Cercetare evenimente în care au fost implicați zilieri și întocmirea procesului verbal conform modelului stabilit prin prevederile legale in vigoare
- Raportare statistica inregistrare accident de munca (FIAM si Anexa la FIAM)
- Inregistrare in baza de date/registre
- Arhivare pv cercetare/dosar/FIAM/Anexa FIAM
- Declarare si raportare boli profesionale

Sistemul va permite:

- Accesul utilizatorilor externi (operatori economici / angajatori, cetățeni) pe baza contului de utilizator folosit pentru conectarea la REGES-ONLINE. Utilizatorii externi vor urma procedura de înrolare stabilită la nivel de ITM în vederea obținerii detaliilor de acces.
- Accesul utilizatorilor interni (personal IM/ITM) pe baza contului de utilizator folosit la nivel de instituție.
- Configurarea setului de permisiuni la nivel de modul, cu definirea tipurilor de roluri și a grupurilor de acces, atât pentru utilizatorii interni cât și externi
- Definirea tuturor tipurilor de documente aflate în aria de acoperire a SSM/ Evenimente/ Accidente de muncă, a metadatelor minime necesare a fi completate în cadrul sistemului pentru fiecare document în parte, precum și a fluxurilor de procesare a acestora. Lista tipurilor de documente ce vor fi disponibile în cadrul sistemului, toate informațiile asociate, precum și fluxurile operaționale vor fi definitivate în cadrul etapei de analiză a proiectului.
- Vizualizarea tipurilor de documente care trebuie completate și posibilitatea descărcării formularelor tipizate aferente acestor tipuri de documente.
- Lansarea sesizărilor privind evenimentele/ accidentelor de muncă direct din sistem:
    - Completarea documentelor direct în cadrul unor formulare web de către angajator, fără a fi nevoie descărcarea formularului tipizat. Semnarea documentelor în format electronic, sau încărcarea unor documente scanate care prezintă semnături olograf.
    - De asemenea sa existe posibilitatea ca un angajator sa raporteze victima altui angajator cu evitare duplicatului - notificare celuilalt angajator - pentru a evita introducerea de duplicate.

    - Pentru sesizarea evenimentelor – să existe și un mecanism de comunicare sau formalizare a comunicării pentru sesizările din partea altor instituții (presa, politie, spital) si/sau persoane fizice – de exemplu prin modulul de sesizări.
- Acestea vor trece prin registratură și vor fi redirecționate la departamentul din cadrul ITM care se ocupa de accidente astfel încât să se poată realiza evidența și asocierea acestor sesizări cu accidenteleÎncărcarea documentelor completate în afara sistemului, inclusiv documente suport, acolo unde este cazul. Modulul trebuie să permită încărcarea documentelor inclusiv de pe dispozitive mobile. În cazul formularelor tipizate scanate și încărcate în cadrul sistemului, se vor putea extrage în mod automat anumite metadate pentru a permite indexarea și regăsirea lor ulterioară.
- Încărcarea documentelor generate și semnate electronic în afara sistemului, cu posibilitatea verificării semnăturii electronice.
- Vizualizarea tuturor documentelor încărcate anterior. Va permite modificarea sau ștergerea documentelor și a anexelor, cu respectarea ciclului de viață al fiecărui tip document. Va fi posibilă refolosirea unui document, prin crearea unei noi versiuni, fără a modifica versiunea anterioară dacă aceasta a fost deja transmisă spre validare.
- Selectarea detaliilor angajaților implicați în accidente de muncă din cadrul listei persoanelor cu care operatorul economic are relații de muncă (angajați, zilieri, ucenici, stagiari). În cazul în care în eveniment a fost implicat un angajat al altui operator economic, va fi posibilă completarea manuală a detaliilor acestuia, cu validarea corectitudinii informațiilor prin reguli de validare specifice (de exemplu: CNP valid, angajator existent), inclusiv semnalarea automata dacă angajatul nu are CIM sau daca are CIM suspendat
- Transmiterea spre înregistrare și validare către ITM a tuturor tipurilor de documente necesare comunicării, cercetării și înregistrării evenimentelor/ accidentelor de muncă (de exemplu: Comunicare eveniment, Proces Verbal de Cercetare, Formular pentru Înregistrarea Accidentului de Muncă, etc.). Pentru fiecare document în parte care poate fi transmis în cadrul sistemului vor fi definite un set de metadate minim obligatorii pentru a asigura procesarea lor optimă. Metadatele vor fi completate în mod automat în toate cazurile unde este posibil acest lucru (de exemplu: detaliile de identificare ale angajatorului).
- Posibilitatea de a anunța de către angajator și transfera cercetarea către ITM în cazul schimbării situației victimei (invaliditate, deces)
- Posibilitatea preluarii tuturor documentelor rezultate in urma cercetarii efectuate de catre comisia desemnata de catre angajator in vederea revizuirii si completarii de catre ITM in situatia preluarii cercetarii de catre inspectorat (pentru cazurile in care un eveniment urmat de incapacitate de munca a devenit cu invaliditate sau deces)
- Posibilitatea ca documentele elaborate de catre angajator, ITM, IM, sa se realizeze direct in program (adrese (inaintare, solicitare documente - spital, medicina legala), efectuare expertize, solicitari documente politie, serviciul criminalistic, etc), avize, respingeri dosare, procese verbale de cercetare, opis documente din dosarul de cercetare, FIAM, Anexa FIAM, etc. De asemeni sa se ofere posibilitatea crearii unei arhive electronice in care sa se regaseasca documentele din dosarele de cercetare, scanate, etc. Aceasta arhiva se asigure si sa conexeze toate documentele ce au fost create in cadrul evenimentului cercetat.
- Validarea completării tuturor informațiilor necesare cu integrarea sistemelor ITM și a altor sisteme terțe cu care este necesară integrarea.
    - În cazul în care nu este posibilă realizarea unei validări automate (de exemplu: eroare de conexiune cu un sistem terț sau informații indisponibile), acest lucru va fi marcat vizual,

dar nu va împiedica transmiterea documentelor pe flux. Pentru fiecare din sistemele terțe cu care este necesară integrarea, Beneficiarul va realiza demersurile administrative necesare obținerii acordului proprietarului sistemului pentru realizarea interoperabilității. Prestatorul trebuie să asigure suportul tehnic.

- Atenționarea utilizatorului în mod vizual și prin mesaje de eroare clare asupra erorilor de completare a documentelor (informații sau anexe lipsă, câmpuri necompletate sau completate necorespunzător)
- Urmărirea statusului documentelor transmise spre procesare în mod vizual. Fiecare etapă de validare va fi definită ca un pas într-un proces fiind posibilă astfel vizualizarea întregului flux al documentului atât pentru etapele automate, cât și pentru acelea unde este necesară procesarea de către un operator.
- Urmărirea solicitărilor de completare a documentelor/dosarelor transmise. Angajatorii vor avea posibilitatea de a răspunde acestor solicitări.
- Transmiterea notificărilor în mod automat conform fluxului definit de procesare a fiecărui tip de document. Notificările vor putea fi transmise prin email. Notificările vor putea fi transmise către un utilizator sau către un grup de utilizatori, în funcție de fluxul definit la momentul implementării.
- Înregistrarea automată a tuturor documentelor transmise către și de către ITM în registratura electronică și generarea automată a numărului de înregistrare.
- Generarea și transmiterea automată a formularelor avizate de către ITM către angajator, acolo unde este cazul, în format needitabil, semnat electronic cu semnătură electronică (certificat de sistem).
- Arhivarea electronică a tuturor documentelor procesate în cadrul sistemului, cu posibilitatea consultării ulterioare.
- Încărcarea oricărui tip de document privitor Accidentele de muncă primit în mod fizic la ghișeu de către operatorul ITM. Sistemul va permite completarea tuturor informațiilor necesare privind angajatorul pentru care se înregistrează documentul prin selecția acestuia din cadrul unui nomenclator preexistent.
- Definirea unor timpi standard de procesare pentru fiecare tip de document în parte, atât la nivel de proces, cât și la nivel de etapă în cadrul procesului, ținând cont de eventualele zile nelucrătoare sau sărbători legale, conform procedurilor operaționale ale ITM.
- Alocarea automată a documentelor spre procesare către o anumită persoană, un anumit rol sau un anumit grup de persoane (de exemplu un compartiment). De asemenea, în caz de nevoie, se va putea efectua modificarea operatorului alocat, în conformitate cu procedurile interne în vigoare.
- Vizualizarea tuturor documentelor asociate aceluiași dosar în cadrul fluxului de lucru. Operatorul alocat va putea modifica statusul procesului dacă este necesar, va putea adăuga observații sub formă de text sau alte documente suport și va putea solicita clarificări. În cazul în care pentru un anumit dosar sunt transmise documente adiționale, sistemul va permite înregistrarea acestor documente cu număr de înregistrare în Registratura electronică. Sistemul va lega logic cele două procese, permițând astfel vizualizarea centralizată a tuturor documentelor.
- Modificarea facilă a diferitor fluxuri de lucru aferente documentelor, direct din interfață, prin configurarea pașilor din proces, a persoanelor sau a grupurilor (compartimentelor) implicate sau a tipurilor de validări necesare.

- Adăugarea direct din interfață a unor noi tipuri de documente, modificarea celor existente și definirea metadatelor aferente acestora, respectiv a fluxurilor de procesare.
- Posibilitatea de a relua cercetarea in momentul in care anexa 2 la FIAM modifica rezoluția situației angajatului (de exemplu invaliditate in loc de reluarea muncii)
- Posibilitatea de a vizualiza istoricul/parcursul acțiunilor în dosar (ex operațiuni de transfer al cercetării nu doar rezultatul cercetării final)
- Referitor la comunicarea rezoluției către terți (victime, asigurator, poliție) – să existe un mecanism de confirmare a angajatorului că și-a îndeplinit această obligație (ex, checkbox de confirmare pe propria răspundere)
- Posibilitatea ca unitatea (angajatorul), angajatul, familia victimei sa conteste PV-ul. Angajatorul să poată contesta în sistem. Pentru celelalte cazuri, se va utiliza modulul de sesizări dar trebuie să existe posibilitatea asocierii sesizărilor respective la cazul de accident pentru a evidenția contestarea PV-ului și a contestatorului precum și operarea în sistem a soluției dispuse ulterior.
    - În cazul în care este realizată o contestație, lucrătorul cazului ITM/IM să fie notificat de către sistem
- Posibilitatea de admite sau respinge contestația cu închiderea lucrării și informarea tuturor părților interesate.
    - Acest lucru să se realizeze prin alegerea modalității de închidere si adăugarea documentelor specifice acolo unde este cazul (PV-ul actualizat)
- Posibilitatea CNPP de a trimite anexa specifica pentru lucrători ai angajatorilor romani care lucrează in străinătate - si au fost accidentați acolo ANEXA 29
- Posibilitatea incarcarii in sistem a documentelor dintr-un dosar de cercetare in baza unui opis prestabilit
- Restrictii de vizualizare a dosarului. Sa poate fi vizualizat doar de cei implicati in cercetare si avizare. Pentru ceilalti inspectori, doar date statistice.
- Evidenta proceselor verbale de cercetare a cazurilor de boala profesionala si a fisa de declarare a cazurilor de boala profesionala BP2
- Implementarea unui flux integrat comunicare, cercetare avizare, inregistrare, evidenta evenimente
- Implementarea de fluxuri separate de cercetare a evenimentelor, functie de competentele de cercetare
- Posibilitatea transmiterii de atentionari in situatiile in care nu se indeplinesc obligatiile legale(ex: in cazul depasitii termenelor de cercetare/inaintare dosar, netransmitere fiam, netransmitere anexa FIAM
- Posibilitatea transmiterii PVCSCc urmare cercetarii evenimentului (daca este cazul) direct la angajator.

3.2.6.5 Petiții și sesizări

3.2.6.5.1 <u>Preambul</u>

Prin petiție se înțelege cererea, reclamația, sesizarea sau propunerea formulată în scris ori prin poștă electronică, pe care un cetățean sau o organizație legal constituită o poate adresa autorităților și instituțiilor publice (art. 2 din Ordonanța Guvernului nr. 27/2002 privind reglementarea activității de soluționare a petițiilor cu modificările ulterioare)

Persoanele fizice sau juridice pot depune petiții sau sesizări privind nerespectarea prevederilor legale în ceea ce privește relațiile de muncă. La momentul actual, petițiile pot fi depuse prin următoarele căi de

comunicare: sistem informatic (https://www.inspectiamuncii.ro/petitii-si-sesizari), fax, email, poșta sau la ghișeul IM/ITM. Toate petițiile și sesizările sunt înregistrate manual în mod obligatoriu în Registrul unic de evidență, care se ține în format electronic securizat în actualul SIAMC.

În momentul înregistrării petiției se vor completa informațiile de identificare privind expeditorul, în funcție de tipul acestuia (persoană fizică, persoană juridică, angajat IM/ITM, instanță judecătorească, instituție). În acest moment este posibilă depunerea unei petiții în mod anonim. Indiferent de forma în care este recepționată o sesizare scrisă din partea cetățenilor (posta, curier, fax, e-mail, site, depunere la sediul IM/ITM), transmiterea unui răspuns scris este în responsabilitatea IM/ITM, prin departamentul desemnat.

In vederea soluționării, corespunzătoare și în termenul legal a petițiilor care ii sunt adresate, IM/ITM are obligația sa răspundă la fiecare petiție primită de la petenți într-un limbaj simplu și ușor de înțeles, in termen de maximum (n/30) de zile de la data înregistrării acesteia, indiferent de rezoluție:

- Clasare – dacă petiția este clasată (se vor înregistra în mod obligatoriu informații privind "Motiv clasare" si "Articol clasare")
- Conexare – dacă înainte de trimiterea răspunsului la o petiție se înregistrează o petiție a aceluiași petiționar, care vizează aceeași problemăInformare – dacă în urma rezolvării acestei petiții este necesara trimiterea unei informări către alta instituție sau persoana privind soluționarea.
- Răspuns – corespunde răspunsului ce urmează sa fie trimis petentului.
- Redirecționare – dacă petiția nu intra in competenta ITM si este identificata instituția care poate rezolva solicitarea sau daca anumite aspecte sesizate de petent sunt de competenta altei/altor institutii.
- Sesizare – daca in urma rezolvării petiției a fost identificata o situație care intra in competenta altei instituții (de exemplu: sesizare către Organul de Cercetare Penala).

In situația in care aspectele sesizate prin petiție necesita o cercetare mai amănunțită (de exemplu declanșarea unui control), IM/ITM trebuie să informeze petentul cu privire la cauzele întârzierii și să precizeze termenul în care va fi soluționata petiția. In termen de (n) zile lucrătoare de la primirea unei petiții, IM/ITM va trimite petentului in cauza o informare cu privire la recepționarea, înregistrarea si declanșarea investigațiilor cu privire la soluționarea petiției primite.

3.2.6.5.2 <u>Cerințe funcționale</u>

Scopul acestui modul este de a permite completarea, înregistrarea și gestiunea întregului flux de gestiune a petițiilor și sesizărilor provenite de la persoane fizice și/sau juridice, în conformitate cu cadrul legal în vigoare la momentul implementării sistemului, și pe toată durata perioadei de suport tehnic și garanție ofertată.

Acest modul va dispune de o zonă publică (front-office), accesibilă prin intermediul portalului web, dedicată operatorilor economici (angajatorilor) și cetățenilor, precum și de o zonă privată (back-office) dedicată personalului din cadrul IM/ITM. Accesul va fi posibil numai după autentificare, iar informațiile afișate vor depinde de rolul~~ui~~ utilizatorului conectat în sistem. În cazul petițiilor anonime, nu va fi necesară autentificarea în cadrul sistemului, dar se vor implementa mecanisme de tip CAPTCHA care să evite transmiterea automată de către operatori non-umani.

Sistemul va permite:

- Accesul utilizatorilor externi (operatori economici / angajatori, cetățeni) pe baza contului de utilizator folosit pentru conectarea la REGES-ONLINE. Utilizatorii externi vor urma procedura de înrolare stabilită la nivel de ITM în vederea obținerii detaliilor de acces.
- Accesul utilizatorilor interni (personal IM/ITM) se va face pe baza contului de utilizator folosit la nivel de instituție, avându-se în vedere prevederile de securitate la nivel instituțional.

- Configurarea setului de permisiuni la nivel de modul, cu definirea tipurilor de roluri și a grupurilor de acces, atât pentru utilizatorii interni (de exemplu: drepturi de validare documente doar pentru inspectorii de muncă, drepturi de vizualizare pentru toți inspectorii), cât și pentru utilizatorii externi (de exemplu: vizualizare doar a petițiilor depuse).
- Completarea și transmiterea petițiilor direct în cadrul unui formular web disponibil în cadrul sistemului. Conținutul acestui formular, inclusiv câmpurile obligatorii și opționale vor fi definite în cadrul etapei de analiză a proiectului.
- Posibilitatea selectării dintr-un nomenclator a informațiilor privind angajator / operator economic pentru care se face reclamația, dacă acestea sunt disponibile în cadrul sistemelor ITM. În cazul în care nu este posibilă realizarea unei validări automate (de exemplu: eroare de conexiune cu un sistem terț sau informații indisponibile), acest lucru va fi marcat vizual, dar nu va împiedica transmiterea petiției.
- Posibilitatea selectării modalității de primire a răspunsului la petiție (de exemplu: folosind setările existente în contul de utilizator sau selectarea unei alte metode disponibile, care va fi aplicabilă doar în cazul acestei petiții). Sa poata opta pentru raspunsul in scris, comunicat prin posta sau in format electronic.
- Posibilitatea definirii mai multor tipuri de petiții, în funcție de obiectul acestora. Selecția va fi simplă și intuitivă pentru utilizatorul final. În funcție de tipul petiției, câmpurile necesare a fi completate vor putea fi diferite (de exemplu atunci când un angajat vrea să raporteze un angajator vor fi necesare atât CNP-ul angajatului cât și CUI/CIF-ul angajatorului raportat). sa existe posibilitatea sa se transmita o petitie si fara CUI/CIF dar cu descrierea locului de munca (pot fi angajatori persoane fizice)
- Posibilitatea încărcării unor documente suport. Posibilitatea de definire a tipurilor de documente acceptate (de exemplu .doc/docx, .pdf, .jpg/jpeg) și a dimensiunii maxime a acestora.
- Atenționarea utilizatorului în mod vizual și prin mesaje de eroare clare asupra erorilor de completare a formularului (informații sau anexe lipsă, câmpuri necompletate sau completate necorespunzător)
- Înregistrarea automată a tuturor petițiilor transmise către ITM în registratura electronică și generarea automată a numărului de înregistrare si transmiterea automata a acestuia catre petent. Petițiile se înregistrează cronologic, în ordinea primirii, indiferent de modalitatea de primire a acestora: prin registratura, prin posta electronica, prin sistemul on-line.
- Alocarea automată a petițiilor spre procesare către o anumită persoană, un anumit rol sau un anumit grup de persoane (de exemplu un compartiment). De asemenea, în caz de nevoie, se va putea efectual modificarea operatorului alocat, în conformitate cu procedurile interne în vigoare.
- În cazul în care petiția include informații privind un operator economic, dar acesta nu a fost selectat din cadrul nomenclatorului, inspectorul ITM responsabil va putea completa această informație, astfel încât să permită regăsirea ulterioară din cadrul dosarului operatorului economic.
- Definirea unor timpi standard de procesare atât la nivel de proces, cât și la nivel de etapă în cadrul procesului, ținând cont de eventualele zile nelucrătoare sau sărbători legale, conform procedurilor operaționale ale ITM.
- Transmiterea notificărilor în mod automat conform fluxului definit de procesare al petițiilor. Notificările vor putea fi transmise prin email. Notificările vor putea fi transmise către un utilizator sau către un grup de utilizatori, în funcție de fluxul definit la momentul implementării.

- Crearea unei arhive organizate privind petitiile inregistrate cu posibilitatea extragerii unor rapoarte specifice, functie de anumite criterii si de datele stocate in sistem,
- Asigurarea confidentialitatii petitie/petentului si a raspunsului la petitiei.

3.2.6.6 Solicitări de informații de interes public

- Gestionarea fluxului de solicitare informații de interes public
    - Pentru a trimite o solicitare de informatii de interes public, solicitantul trebuie sa se autentifice in portalul extern (siteul instituției), in zona privata dedicata acestuia.
    - Accesarea meniului de informații de interes public, unde va avea la dispozitie un formular de completare a informatiilor. În urma completării câmpurilor obligatorii cu posibilitatea de a transmite solicitarea către un ITM-ul selectat sau către IM. Utilizatorul va avea posibilitatea atașării de documente în format electronic
    - Dupa ce se completează campurile obligatorii, la transmiterea formularului sistemul trebuie să afișeze numărul de inregistrare alocat solicitării din registratura electronică, cu ajutorul caruia acesta va putea verifica statusul solicitarii.
    - Accesul utilizatorilor interni (personal IM/ITM) se va face pe baza contului de utilizator folosit la nivel de instituție, avându-se în vedere prevederile de securitate la nivel instituțional. Sistemul va asigura configurarea setului de permisiuni la nivel de modul, cu definirea tipurilor de roluri și a grupurilor de acces, atât pentru utilizatorii interni.
    - Dupa inregistrarea la Registratura si transmiterea pe flux, utilizatorul cu rol de CRP va inregistra printr-un clik solicitarea de informatii de interes public si in Registrul electronic specific din sistem:
        - Utilizatorul va accesa solicitarea, verifica toate informatiile din cadrul acesteia si face completari, poate redistribui solicitarea catre un alt compartiment pentru adaugarea raspunsului, raspunsul va fi transmis de departamentul de comunicare si relatii cu publicul.
    - Crearea unei arhive organizate privind solicitările de informatii de interes public inregistrate cu posibilitatea extragerii unor rapoarte specifice, functie de anumite criterii si de datele stocate in sistem.

3.2.6.7 Operatori economici

3.2.6.7.1 <u>Preambul</u>

Acest modul va permite gestionarea în mod centralizat a informațiilor privind persoanele juridice, române sau străine care își desfășoară activitatea pe teritoriul României. Prin intermediul acestui modul, inspectorii de muncă vor putea vizualiza în mod centralizat toate informațiile privind angajatorii și anume:

- Profil angajator: detalii de identificare (denumirea (firma), numărul de înregistrare în registrul comerțului, codul unic de înregistrare, identificator unic la nivel european, starea firmei, forma juridică, sediu social, durată de funcționare, stare firmă); detalii privind activitatea principală, secundară și alte activități autorizate (cod CAEN), reprezentant legal – CNP, adresa, telefon, e-mail, etc; detalii privind sucursale, subunități, sedii secundare și puncte de lucru; detalii privind reprezentanți legali. Aceste informații vor fi preluate din sistemul informatic al Oficiului Național al Registrului Comerțului (ONRC), în timp real pentru a minimiza situațiile în care inspectorii nu

regăsesc un angajator în baza de date proprie, cu posibilitatea de alertare a situatiei de firma aflata in insolventa/lichidare

- Detalii de ordin fiscal prezente în declarația 112 preluate din sistemul informatic al Agenția Național de Administrare Fiscală (ANAF).
- Detalii privind angajații, contractele de muncă preluate din sistemul REGES Online sau din alte surse.
    - Femei
    - Barbati
    - Sub 18 ani
    - sub 16 ani
    - Alaptare
    - Gravide
    - Persoane cu handicap
    - cetateni straini
- Detalii privind istoricul de controale efectuate (sanctiuni primite), la angajatorul/agentul economic și a măsurilor dispuse în controalele anterioare si modul de indeplinire a acestora
- Sistemul va conexa toate documentele inregistrate si generate pentru angajatorul respectiv (de exemplu existenta unui contract colectiv de munca, notificari privind munca de noapte)
- Organizarea activitatii de prevenire si protectie
- Lucrator desemnat
- Serviciul extern
- Detalii privind documentele, informările și notificările transmise de angajator în domeniul Relații de Muncă (Relații de Muncă) și Sănătate și Securitate în Muncă (SSM), inclusiv Accidente, boli profesionale, incadrarea locurilor de muncă în conditii deosebite/speciale.
- Petiții, informații, adrese sau memorii primite de la persoane fizice, juridice, alte instituții publice și înregistrate în cadrul ITM pentru respectivul angajator.
- Echipamentele de munca ca necesita autorizare: ISCIR INSEMEX, etc
- Meseriile si profesiile autorizate
- Lista cu substantele si preparatele chimice periculoase
- Materii explozive
- Produse fitosanitare.

3.2.6.7.2 <u>Cerințe funcționale</u>

Platforma va permite:

- Precompletarea datelor referitoare la operatorul economic utilizând datele la zi din REGES-ONLINE corelate cu datele de la ONRC cu posibilitatea actualizării acestor date de către inspectorul care realizează controlul
- Datele aferente angajatorului vor cuprinde inclusive situatiile de insolventa, lichidare, etc precum si datele lichidatorului judiciar care reprezinta angajatorul.
- Vizualizarea angajatorilor existenți în sistem sub formă de listă cu posibilitatea de filtrare după următoarele criterii: starea firmei, forma juridică, locație sediu social, durată de funcționare, detalii privind activitatea principală, secundară și alte activități autorizate (cod CAEN); detalii privind sucursale, subunități, sedii secundare și puncte de lucru (locație). Alte criterii vor putea fi definite în cadrul etapei de analiză a proiectului, în funcție de necesitățile beneficiarului la momentul implementării.

- Căutarea unui angajator după detaliile de identificare (denumirea (firma)/o parte din denumirea firmei, numărul de înregistrare în registrul comerțului, codul unic de înregistrare, identificator unic la nivel european, nume administrator si/sau asociat).
- Adăugarea manuală a unui angajator în cazul în care acesta nu se regăsește în listă. Se vor putea introduce aceleași categorii de informații ca cele colectate de la sistemele terțe. Se va implementa o modalitate prin care se va evita crearea duplicatelor cu ajutorul unor reguli stricte de validare. De asemenea, se va implementa un mecanism care permite rezolvarea potențialelor conflictele generate în urma sincronizării.
- Modificarea detaliilor unui angajator se va putea realiza numai de către utilizatorii cu roluri dedicate, cu respectarea strictă a regulilor de validare existente.
- Vizualizarea în mod centralizat a informațiilor gestionate de alte module din cadrul SIAMC, fără a presupune replicarea acestor informații (de exemplu lista documentelor transmise de operatorul economic prin intermediul platformei sau lista controalelor desfășurate anterior și a măsurilor dispuse de către inspectorii de muncă).
- Generarea unei „fișe a operatorului economic" care servește ca o carte de identitate a acestuia și care va include toate informațiile existente în cadrul sistemului despre angajator într-un format structurat, actualizate cu ocazia fiecarui control efectuat. Această fișă va putea fi salvată în cadrul sistemului și imprimată dacă este cazul, pentru a putea păstra istoric situația unui operator economic la un anumit moment de timp. Formatul și informațiile incluse în această fișă vor fi definite în etapa de analiză a proiectului.
- Comunicarea bidirecțională cu restul de module din cadrul SIAMC. Va fi posibilă de exemplu asocierea unei activități de control la nivelul unui punct de lucru al unui angajator / operator economic prin selecția angajatorului și punctului de lucru dorit direct din modulul Monitorizare și Control.

La momentul logării inspectorului de muncă la sistem, va exista un modul de atenționări/alerte, referitoare la depasirea termenelor de implementare a masurilor, alte neconformitati. Ex: depasirea termenului de cercetare eveniment /netransmiterea semestriala a raportului de activitate de catre serviciul extern SSM care se ocupa de angajatorul respectiv/ raportul CSSM.

- Gestiunea unui registru prestatorilor de servicii
    - În vederea organizării unei evidențe centralizate, se va crea și se va menține un registru al prestatorilor cu care angajatorii au încheiat contracte de prestări servicii pentru diverse activități: SSM, RM, etc..
    - Angajatorii pot contracta un astefel de prestator de servicii, autorizat, prin selectarea acestuia din registru și pot delega către acest prestator una sau mai multe activități.
    - Pentru angajatorii și prestatorii care sunt în sistem, la operațiunea de asociere a unui utilizator prestator de servicii cu entitatea juridică contractată în care va avea roluri de adaugare/editare date este necesar ca administratorul de profil angajator să poată specifica că utilizatorul respectiv face parte, sau nu, dintr-o societate prestatoare de servicii și să indice exact societatea respectivă.

3.2.6.8 Administrare platformă

Scopul modulului de administrare dezvoltat în cadrul soluției va fi de a permite gestionarea utilizatorilor, a accesului și a seturilor de date de către Serviciul Informatic al Inspecției Muncii si a Inspectoratelor Teritoriale de Munca..

Operațiunile aferente modulului de administrare trebuie să poată fi realizate direct din interfața aplicației, în funcție de drepturile de acces acordate rolului respectiv. Platforma va permite definirea unei structuri ierarhice de roluri pentru a permite managementul simplificat al drepturilor de acces (de exemplu: un utilizator cu rol de administrator de la nivelul unui ITM va putea gestiona utilizatorii din cadrul ITM-ului propriu, dar nu și pe cei dintr-un alt ITM, în timp ce un utilizator de la nivelul IM va putea gestiona toți utilizatorii). Modalitatea concretă de implementare a acestei cerințe va fi definită în cadrul etapei de analiză a proiectului.

Accesul în zona de administrare, precum și pentru accesul la anumite module, funcționalități sau seturi de date ce se vor defini în etapa de analiză (de exemplu documentele specifice zonei de monitorizare și control) se va realiza în mod securizat doar prin rețeaua internă a IM/ITM. Accesul din afara instituției se va fi posibil doar prin intermediul unui VPN.

Sistemul va trebui să permită închiderea automată a sesiunilor de lucru ale utilizatorilor în caz de inactivitate pe o anumita durată, configurabilă, de timp - din zona de administrare.

3.2.6.8.1 <u>Cerințe generale</u>

Platforma trebuie asigure următoarele funcționalități:

- Adăugarea, modificarea, suspendarea/activarea utilizatorilor din aria de acoperire a unui utilizator cu rol de administrator (de exemplu din cadrul ITM-ului propriu).
- Generarea automată a parolelor inițiale aferente unui cont de utilizator, conform regulilor specifice privind numărul minim/maxim de caractere, tipul acestora. Funcționalitățile de resetare a parolei unui cont de utilizator nu vor necesita intervenția administratorilor, decât în cazuri specifice, așa cum vor fi definite în cadrul etapei de analiză (de exemplu: cont blocat datorită unei suspiciuni de fraudă).
- Configurarea caracteristicilor parolelor privind numărul și tipul de caractere, perioada de valabilitate, posibilitatea de refolosire a parolelor anterioare, precum și gestiunea autentificării multi-factor.
- Configurarea obligației de schimbare a parolei expirate la următoarea încercare de acces în cadrul sistemului, cu notificarea prealabilă a utilizatorului privind necesitatea schimbării parolei într-un anumit termen.
- Vizualizarea listelor de utilizatori și a detaliilor acestora (de exemplu: nume, prenume, funcție, departament, rol/roluri, legitimatie, status) cu posibilitatea de filtrare / căutare în listă (de exemplu: rol, grup utilizatori, nume și prenume, email/nume utilizator și status).
- Exportul listei de utilizatori într-un format tabelar (.csv, .xls/.xlsx) de către utilizatorii cu drepturi specifice.
- Posibilitatea de import a mai multor utilizatori pe baza unui șablon prestabilit, direct din interfața de administrare a aplicației, acolo unde este cazul.
- Suspendarea unui utilizator fără a șterge informațiile asociate acestuia, în conformitate cu prevederile specifice privind protecția datelor cu caracter personal. În cazul utilizatorilor interni instituției, se va avea în vedere faptul că toate documentele asociate acestora, precum și istoricul acțiunilor efectuate în sistem (de exemplu în cazul controlului) va trebui păstrat, în conformitate cu prevederile legale. Accesul la funcționalitate de suspendare a unui utilizator trebuie să poată fi realizată și de către alți utilizatori pe baza grupurilor de securitate definite,

astfel încât fiecare ITM să își poată gestiona independent modificările de personal (plecări, concedii medicale, alte situații neprevăzute)

- Transferul documentelor și/sau al informațiilor asociate unui cont prin funcționalități de tip delegare (temporară sau permanentă), cu păstrarea istoricului acțiunilor efectuate în cadrul sistemului.
- Ca metodă complementară de management a utilizatorilor interni IM/ITM trebuie să existe și posibilitatea de integrare cu soluția Active Directory configurata la nivelul Achizitorului. Gradul de integrare va fi stabilit în etapa de analiză pentru proiectarea sistemului.

3.2.6.8.2 Gestionarea accesului

Accesul în cadrul sistemului va fi posibil doar utilizatorilor care dispun de un cont de utilizator activ, cu excepția informațiilor publice disponibile în cadrul portalului web. Se vor avea în vedere următoarele categorii de utilizatori:

- utilizatori interni ai IM și ITM, în funcție de nivelele de acces și rolurile definite în platformă;
- utilizator externi reprezentanți ai altor instituții ale statului, cu acces limitat pe baza unui protocol încheiat în temeiul legii, pe seturile de date specificate în respectivele protocoale sau solicitări de acces;
- utilizatori externi, persoane fizice sau juridice, cu acces limitat la informațiile și funcționalitățile platformei (de exemplu: un utilizator asociat unui angajator va putea vizualiza doar informațiile aferente operatorului economic, doar atunci când aceste devin disponibile. In cazul unui control, informațiile vor fi disponibile doar atunci când inspectorul de muncă decide acest lucru, în conformitate cu procedurile în vigoare).

Pentru gestionarea accesului la funcționalitățile aplicației sistemul trebuie să facă uz de un mecanism complet de roluri, grupuri și permisiuni astfel încât accesul la seturile de date să poată fi configurat de către utilizatorii desemnați de către Beneficiar.

Astfel sistemul trebuie să permită:

- Adăugarea de noi roluri, sau modificarea rolurilorexistente;
- Asocierea drepturilor de acces rolurilor sau grupurilor astfel configurate. Drepturile de acces vor putea fi configurate atât la nivel de funcționalitate (de exemplu: posibilitate de adăugare document), cât și la nivel de date (de exemplu: posibilitate de vizualizare doar a detaliilor angajatorilor din aria de acoperire).
- Gestiunea grupurilor de utilizatori, inclusiv crearea de legături părinte-copil între grupuri. Mecanismul de grupuri va reprezenta o modalitate de a grupa un set de utilizatori atât din punct de vedere administrativ (ex. un ITM, un compartiment/serviciu al unui ITM, utilizatori externi care au primit acces pe baza unui protocol încheiat în temeiul legii cu IM) cât și din punct de vedere al gestionării accesului la anumite seturi de date. Un utilizator trebuie să poată face parte dintr-un număr nelimitat de grupuri de securitate cumulând astfel corespunzător drepturile de acces.
- Posibilitatea de a vedea în profilul unui utilizator grupul/rile din care face parte.

3.2.6.8.3 Rapoarte referitoare la utilizatori

Soluția dezvoltată trebuie să asigure păstrarea și posibilitatea de consultarea:

- încercărilor de conectare și dacă utilizatorii au reușit (da/nu) - cu posibilitatea de căutare, filtrare și export a listei (user, rol, grup, IP și momentul încercării de conectare -zi, data, ora, minut, secunda)

- operațiunile realizate de către utilizatori asupra rapoartelor prin păstrarea a cel puțin - raport accesat, motiv generare raport, criteriu de căutare (CNP, CUI), utilizatorul care a accesat și IP-ul și momentul în timp (zi, data, ora, minut, secunda)

Informațiile astfel colectate trebuie să se poată vizualiza într-un raport specific în zona de administrare cu posibilitatea de căutare, sortare și filtrare după diferite criterii, precum și export în format tabelar (.xlsx, .csv).

3.2.6.8.4 Administrare nomenclatoare și formulare colectare date

Sistemul trebuie să ofere funcționalități de administrare a formularelor și nomenclatoarelor utilizate în colectarea datelor de la utilizatori (ex. datele introduse de angajatori).

Beneficiarul urmărește ca modificările/actualizările simple asupra formularelor de colectare date (adăugarea unui nou câmp de un tip predefinit, actualizarea sau adăugarea unui nomenclator) să se poată realiza direct din interfața de administrare.

Astfel sistemul dezvoltat trebuie să asigure:

- posibilitatea de a adăuga noi nomenclatoare de către personalul desemnati IM/ ITM
- posibilitatea de a putea adăuga/modifica lista de valori ai unui nomenclator de către personalul desemnati IM/ ITM
- posibilitatea de a crea legături de tip copil-părinte între nomenclatoare acolo unde este cazul (ex. structura ierarhică a codurilor COR/ CAEN).
- posibilitatea de a adăuga câmpuri noi în formularele de colectare date (angajator, CIM, salariat etc.). Exemple de tipuri de câmpuri: text, număr, checkbox, radio, dată, adresă web, listă derulantă, încărcare fișier.

3.2.6.9 Platforma de analiză și raportare. Indicatori de control

Platforma de analiză și raportare va asigura preluarea și consolidarea datelor din diverse surse de date (interne și externe), generarea de rapoarte complexe și va permite construirea, configurarea și generarea de analize avansate/rapoarte dinamice pe baza datelor preluate și consolidate și respectiv prezentarea în diferite șabloane și formate pentru utilizări viitoare. Prin implementarea acestei platforme se va asigura o separare a resurselor alocate serviciilor on-line puse la dispoziție prin SIAMC (operațiuni tranzacționale de tip OLTP) de cele destinate activităților de raportare și analiză. De asemenea, prin implementarea acestei componente, Beneficiarul va dispune de instrumente ce vor permite efectuarea unor analize avansate și investigații utilizând datele din întreaga organizație, atât cele structurate, cât și cele nestructurate.

Platforma de analiză și raportare va fi compusă din:

- **Componenta depozit de date / data warehouse (baze de date pentru realizarea interogărilor)** – datele din bazele de date de producție (tranzacționale) ale aplicațiilor existente (actualul SIAMC, REGES Online) vor fi replicate într-o bază de date care va deservi operațiuni de tip interogare. Odată cu replicarea datelor, se va proceda și la transformarea acestora pentru a răspunde mai bine cerințelor impuse de activitatea de raportare. În această componentă se vor putea constitui depozite de date (Data Warehouse) care vor facilita rularea de rapoarte complexe peste datele structurate. Replicarea datelor va fi unidirecțională, dinspre bazele de date existente (de producție) către noua baza de date de raportare.
- **Componenta Raportare** va permite crearea și rularea de rapoarte peste informațiile stocate în Componenta depozit de date. În afara rapoartelor „standard” (rapoarte predefinite, dezvoltate pe baza unor cerințe clare detaliate pe durata derulării implementării) prin intermediul platformei se vor putea realiza, de utilizatori cu rol dedicat, rapoarte „ad-hoc” pentru identificarea și analizarea anumitor situații punctuale. Rapoartele ad-hoc se vor putea

transforma în rapoarte „standard”, printr-o simplă operațiune de „publicare”, fără a fi nevoie de redezvoltarea lor.

Cerințele funcționale și rapoartele vor fi realizate utilizând Componenta de consolidare date data warehouse, analiza raportare ofertată.

3.2.6.9.1 Analiză, Raportare și Indicatori de Control

Scopul acestui modul va fi de a permite realizarea analizelor care vor sprijini elaborarea **Programul cadru anual de acțiuni al Inspecției Muncii** la nivel național și a **Programului propriu anual de acțiuni al inspectoratului** și a **Planului Anual de Control** la nivel de ITM prin analiza criteriilor de selecție și de evidențiere a entităților care îndeplinesc condițiile de natură de a le situa în „zona de intervenție imediată”, pentru organizarea vizitelor de inspecție, constatarea și compararea rezultatelor obținute cu cele indicate în aplicație, precum și dispunerea de măsuri de remediere, acolo unde este cazul.

Acest modul trebuie să permită definirea și urmărirea principalilor indicatori de performanță la nivel de IM/ITM. Definirea și urmărirea indicatorilor trebuie să fie posibilă atât la nivel national/IM cât și la nivelul fiecărui județ/ITM.

Pentru implementarea acestui modul se vor avea în vedere funcționalitățile standard descrise în capitolul Platformă de analiză și raportare. Prin intermediul acestui modul vor putea fi realizate analize și rapoarte folosind seturile de date disponibile în cadrul SIAMC, fără a fi necesară intervenție programatică.

Acest modul va permite realizarea unor analize și rapoarte care includ minim următoarele date și tipuri de indicatori:

- Dispersie teritorială operatori economici, cel puțin: distribuție geografică, distribuție geografică după obiectul de activitate principal / secundar și alte activități autorizate (cod CAEN); evidențiere sedii principale, secundare și a datelor asociate (de exemplu: vizualizare de tip hartă, cu posibilitate de filtrare la nivel de regiune și evidențierea agenților economici din regiunea respectivă, precum și vizualizarea contextuală a detaliilor unui agent economic);
- Detalii agregate privind numărul de angajați, zilieri, ucenici la nivel de agent economic în funcție de o anumită perioadă de timp – vizualizare agregată de tip tabelar (de exemplu lista agenților economici și a numărului de angajați în luna ianuarie) și vizualizări de tip serie de timp (de exemplu evoluția în timp a numărului de angajați);
- Detalii agregate la nivel de operator economic privind situația controalelor și a măsurilor dispuse, sancțiunilor și sesizărilor, atât însumat, cât și cu o dimensiune temporală; vizualizarea informațiilor atât prin agregare la nivel de operator economic, cât și prin agregare la nivel de județ, regiune, inspector de muncă, tip control.
- Detalii agregate la nivel de operator economic privind cel puțin următoarele informații:
    - Nivelul potențialului de risc de accidentare și/sau îmbolnăvire profesională la locurile de muncă inspectate (de exemplu: societăți comerciale care operează cu substanțe/produse/bunuri capabile să genereze atmosfere explozive/toxice, sau prezintă caracteristici detonante/deflagrante; societăți comerciale care operează cu substanțe chimice periculoase; societăți comerciale noi cu activități din anexa 5 la NM;)
    - Situația accidentelor de muncă și a îmbolnăvirilor profesionale, inclusiv clasificarea acestora.
- Detalii agregate la nivel de IM/ITM privind numărul de inspectori de muncă, număr zile de control efectuate (zile de control propriu-zis; zile de control în care s-a verificat modul de realizare a măsurilor dispuse; zile de control la sesizări), număr zile alocate cercetării accidentelor de muncă, atât în format tabelar, cât și ca serii de timp și histograme.

De asemenea se vor dezvolta Rapoarte și indicatori care să permită urmărirea eficienței actelor de control, raportat la numărul de contestații în justiției a acetelor de control, precum și a verdictelor finale pricind aceste acte contestate, la nivel de IM/ ITM/ Inspector de muncă.

Suplimentar rapoartelor prezentate anterior, utilizatori din cadrul organizației beneficiarului, IM/ITM, vor putea construi și alte rapoarte și analize folosind informațiile/datele disponibile în cadrul SIAMC 2.0, fără a fi necesară intervenție programatică. În acest sens, în cadrul etapei de analiză a proiectului vor fi definite toate structurile de date necesare pentru a permite crearea diferitelor analize și rapoarte. Aceste structuri de date vor fi adaptate în așa fel încât să fie clare și intuitive pentru utilizatorii finali,.

3.2.6.10 Evaluare de risc

Sistemul informatic va conține un subsistem care, pe baza criteriilor de risc stabilite de către Beneficiar, din datele existente în sistemul informatic precum și pe baza parametrilor monitorizați și stabiliți de către Beneficiar va genera automat angajatorii care se află în zona de intervenție.

Subsistemul va asigura integrarea datelor introduse în platforma creată, în algoritmul utilizat de aplicatia de Evaluare a Riscului, în vederea generarii automatizate a listei entităților ce urmează a fi incluse în acțiuni de control. Datele utilizate pentru construirea algoritmului de funcționare a aplicatiei, vor proveni din riscurile care s-au manifestat și sprijină Inspecția Muncii în îndeplinirea funcției de autoritate de stat prin care se asigură exercitarea controlului în domeniile relațiilor de muncă și securității și sanatății în muncă care au stat Ia baza producerii de evenimente în care au fost implicați lucrători. Aceste informații vor trebui să fie extrase și generate automat din procesele verbale de cercetare întocmite sau avizate de ITM/ IM, procesele verbale de control cu documentele conexe, sesizări, precum și din exploatarea celorlalte baze de date gestionate sau la care are acces Inspecția Muncii.

Subsistemul va permite realizarea de analize de tip: Descriptiv (ce s-a întâmplat), Diagnostic (de ce s-a întâmplat), Predictive (ce se va întâmpla), Prescriptive (ce ar trebui făcut).

3.2.6.10.1.1 Fluxul de detectare a neconformarii la legislația muncii

Scopul implementarii unui flux de detectare a neconformarii la legislația muncii este să asiste utilizatorii la crearea unei vizualizari holistice a angajatorilor și să seteze entități care vor reprezenta diversele atribute ale profilului angajatorului. Scopul strategic ar fi acela de a determina nivelul de risc pentru angajator sau altă entitate, de a produce alerte în ceea ce privește profilurile cu risc crescut, și de a demara verificări/inspecții pentru acele cazuri ce prezintă risc crescut.

Aceasta va include integrarea alertelor de eveniment sau monitorizarea in timp real în componentele de analiză a datelor ale soluției pentru a crea un punctaj unificat al angajatorilor, ce va asigură baza justificativă pentru monitorizarea și detectarea comportamentelor neconforme.

3.2.6.10.1.2 Entități de soluționare

O analiză a datelor procurate, centrată pe entitate care să potrivească diferite versiuni ale aceleiași entități găsite în cadrul ei, pentru a produce o versiune unitară a fiecărei entități (în mod principal angajatori persoane juridice sau fizice). Pentru ca această funcție să fie mai eficientă, se vor utiliza date analitice avansate pentru a realiza soluționarea, ca de exemplu Fuzzy Matching, pentru soluționarea variațiilor din câmpurile de texte.

3.2.6.10.1.3 Registrul electronic al riscurilor (RER)

Constituirea (realizarea) Registrului electronic al riscurilor la legislația muncii care va reprezenta un instrument informatic structurat pentru documentarea riscurilor, descrierea și inventarierea acestora. Riscurile de neconformare sunt identificate și înregistrate în registru, împreună cu indicatorii de risc aferenti (RER) si va cuprinde:

a) toate riscurile identificate, fiind principalul instrument utilizat în cadrul procesului de management al riscurilor la legislația muncii , clasificate în cele 4 mari categorii (declararea elementelor

muncii din domeniul de competență (CIM/SSM), nivelul de declarare, conformarea la măsurile corective, plata impozitelor datorate), precum și subcriterii de risc aferente;

b) dezvoltarea indicatorilor de risc aferenți fiecărui subcriteriu de risc (indicatori de tip valoric sau binari), având în vedere cel puțin următoarele:

- descrierea regulii incalcate si consecințele la legislația muncii potențiale;
- descrierea surselor de date utilizate pentru aplicarea indicatorului de risc, precum si explicatiile privind modul de calcul al indicatorului, etc,

c) calculul scorului de neconformare, atunci cand a fost aplicat un indicator de risc valoric și stabilirea scorului de neconformare, atunci cand a fost aplicat un indicator de risc de tip binar;

d) sa permita ajustarea unor parametri pentru modificarea/ajustarea

indicatorilor de risc;

e) instrumentul informatic trebuie să permită actualizarea RER ori de cate ori este nevoie (adăugare/excludere indicatori, modificare formule calcul, păstrare istoric etc.)

3.2.6.10.1.4 Registrul de Risc al Angajatorului (RRA)

Constituirea (realizarea) Registrul de Risc al Angajatorului (RRA), care va efectua, în mod automat, încadrarea angajatorilor în clase şi subclase de risc în scopul organizării de către I.M. a activităților de corectare și impunere a conformării la legislația muncii pe baza analizei de risc conform prevederilor legislației în vigoare.

Informațiile conţinute de registru vor fi actualizate automat, periodic, pe măsura colectării și prelucrării unor informaţii relevante privind un angajator sau un grup de angajatori. Data de referință a informațiilor este data la care a fost inițiată procedura de actualizare. Totodată, RRA va putea fi completat, actualizat ori de câte ori este necesar, cu noi informații introduse de personalul desemnat din cadrul inspecției muncii (de exemplu, “fişe de alertă a riscului”/“fişe de feedback”/ “raport de impact”).

Analiza se va efectua pentru o perioada de cel putin 3 ani pentru care exista situații si declaratii informative depuse.

Cerințe funcționale ale RRA:

RRA va permite calcularea unui scor de risc pentru fiecare angajator utilizând indicatorii de risc dezvoltați în Registrul electronic al riscurilor (RER), prin ajustarea scorului de încălcare a legislației muncii cu scorul general de neconformare.

Ca urmare a scorului de risc determinat, RRA va permite segmentarea si ierarhizarea angajatorilor in clase și subclase de risc, pe baza pragurilor de semnificatie stabilite;

RRA trebuie să poată oferi recomandări automate de tratamente la legislația muncii inscrise intr-o listă și posibilitatea selecției manuale a tratamentelor pentru angajatori sau un grup de angajatori;

Prin configurarea componentelor aplicative, de analiză și raportare ofertate trebuie să poată fi obţinute minm următoarele tipuri de rapoarte:

a) raport care să prezinte informaţii privind datele şi/sau sursele de date referitoare la un angajator sau la grupul de angajatori pentru care s-a făcut interogarea, date pe baza cărora a fost efectuată evaluarea nivelului de risc şi încadrarea angajatorului într-o anumită clasă/subclasă de risc;

b) raport privind indicatorii de risc de încălcare utilizaţi pentru calculul nivelului de risc al angajatorului sau al unui grup de angajatori, precum şi valoarea obţinută în urma evaluării acestor indicatori;

c) raport privind modul de calcul al scoring-ului, încadrarea angajatorului sau a unui grup de angajatori în clasa şi subclasa de risc la momentul solicitării, precum şi istoricul încadrărilor în clase şi subclase de risc pentru un angajator sau un grup de angajatori;

d) raport privind tratamentele asociate clasei şi subclasei de risc în care este încadrat un angajator sau un grup de angajatori, precum şi istoricul tipurilor de tratament aplicate angajatorului sau grupului de angajatori şi rezultatele tratamentelor aplicate ce au fost înregistrate în fişele de feedback/rapoartele de impact;

e) raport privind evoluţia încadrarilor în clase/subclase de risc pentru un grup de angajatori selectaţi pe baza unui atribut comun (cod CAEN, mărime angajator, cifra de afaceri, număr angajaţi, stare angajator, etc.), precum şi eficienţa tratamentelor aplicate acestora.

3.2.6.11 Integrarea cu alte sisteme

SIAMC va fi construit în așa fel încât să permită comunicarea cu sisteme electronice externe în scopul accesării unor servicii electronice expuse de către terțe instituții. SIAMC va fi configurabil și suficient de flexibil astfel încât să permită extinderea viitoare prin configurarea accesului la alte servicii electronice. SIAMC va fi capabil să transmită cereri către sisteme externe și să primească răspunsuri, atât sincron cât și asincron, păstrând referința la tranzacția inițială. Integrarea cu sisteme terțe se va putea face de la nivel de flux de lucru, atât în timp real, în cadrul unor formulare web, cât și ca etapă distinctă în cadrul unui flux complex de procesare a unor documente.

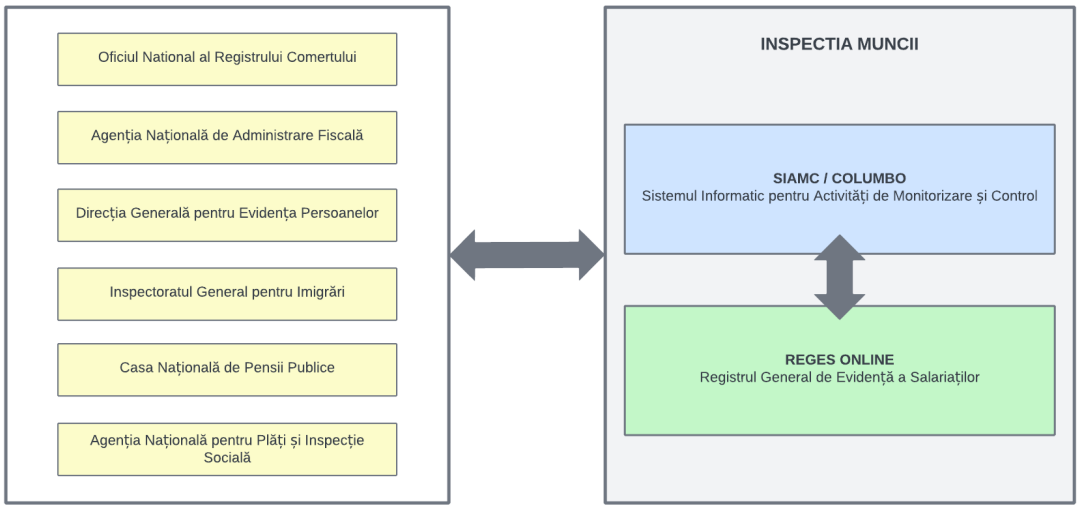


Figura 3 – Integrare cu alte sisteme

SIAMC se va integra cel puțin cu următoarele platforme informatice ale altor autorități sau instituții publice:

- **Oficiul Național al Registrului Comerțului (ONRC)** în vederea preluării informațiilor privind angajatorii, persoane fizice sau juridice, care desfășoară activități pe teritoriul României. Se vor avea în vedere cel puțin următoarele categorii de informații: detalii de identificare (denumirea (firma), numărul de înregistrare în registrul comerțului, codul unic de înregistrare, identificator unic la nivel european, starea firmei, forma juridică, sediu social, durată de funcționare, stare firmă); detalii privind activitatea principală, secundară și alte activități autorizate (cod CAEN); detalii privind sucursale, subunități, sedii secundare și puncte de lucru; detalii privind reprezentanți legali.

- **Agenția Națională de Administrare Fiscală (ANAF)** în vederea preluării informațiilor de ordin fiscal prezente în declarația 112, respectiv pentru transmiterea proceselor verbale de constatare și sancționare a contravenienților, în vederea executării amenzilor aplicate.
- Agenția Națională pentru Ocuparea Forței de Muncă
- Inspectoratul General pentru Imigrări, în vederea preluării informațiilor privind existența avizului de angajare sau încadrarea străinului intr-una din situațiile exceptate
- Inspectoratul General al Poliției Române, în vederea preluării informațiilor privind cazierul judiciar.

Se va avea în vedere și integrarea cu platformele existente sau nou-create ale Direcției Generale pentru Evidența Persoanelor (DGEP), Inspectorul General al Poliției Române, Jandarmeria Română, Inspectoratului General pentru Imigrări (IGI), Casei Naționale de Pensii Publice (CNPP), Agenției Naționale pentru Plăți și Inspecție Socială (ANPIS) și Institutul Național de Statistică (INS), precum și cu PCUe și cu Ghișeul Unic. Aceste integrări sunt necesare pentru efectuarea diferitelor verificări și validări conform legislației în vigoare, respectiv în vederea simplificării proceselor operaționale la nivelul instituției.

Pentru fiecare din sistemele terțe cu care este necesară integrarea, Beneficiarul va realiza demersurile administrative necesare obținerii acordului proprietarului sistemului pentru realizarea interoperabilității. Va fi în sarcina Prestatorului să asigure suportul necesar demersurilor tehnice în vederea stabilirii modalității concrete de realizare a integrării și de asemenea de realizare a dezvoltărilor sau configurărilor necesare în soluția ofertată.

3.2.6.11.1 Integrare cu alte sisteme

Accesul autorităților și instituțiilor publice la datele din REGES-ONLINE se va realiza la nivel de interfață de programare a aplicațiilor (API - Application Programming Interface). Interoperabilitatea tehnică include specificații privind interfața, serviciile de interconectare, serviciile de integrare a datelor, prezentarea și schimbul de date și protocoale securizate de comunicare.

Din punct de vedere al integrării cu alte sisteme, sistemul REGES-ONLINE va permite integrări prin export/import de date către terți în format tabelar, integrări ce vor viza: sistema interne ale Inspecției Muncii, sisteme IT utilizate de angajatori pentru actualizarea automată a datelor angajaților și contractelor de muncă, sistema publice terțe ce dețin informații necesare în procesele de validare și verificare a datelor despre angajatori și angajați.

În plus se va introduce conceptul de „event-based interoperability” prin care se vor transmite evenimente de tip „publish/subscribe” către alte sisteme.

Orice actualizare în REGES-ONLINE a contractelor va produce evenimente, pe baza unor filtre stabilite, care vor fi publicate în brokerul de mesaje ofertat. La acest broker vor fi abonate sistemele altor instituții/autorități care vor consuma mesajele respective. Brokerul de mesaje va putea primi mesaje din exterior totodată și va declanșa fluxuri în sistem.

3.2.6.12 Performanțe sistem

Proiectarea sistemului și a bazei de date va fi realizată astfel încât să fie asigurate performanțele solicitate pe toată durata implementării proiectului și a perioadei de suport tehnic și garanție. În cazul în care în acest Interval se vor înregistra scăderi ale performanței sistemului datorate încărcării bazei de date, Prestatorul va fi responsabil pentru optimizarea sistemului astfel încât acesta să fie readus în parametrii inițial solicitați fără costuri suplimentare pentru Achizitor. Oferta va include asumarea cerinței de către Ofertant.

3.2.6.13 Suport pentru utilizatori

Sistemul va trebui sa ofere mecanisme moderne de asigurare a suportului tehnic către utilizatorii de tip angajator/ angajat, astfel încât aceștia să poată folosi eficient sistemul, fără a aglomera personalul IM cu acest proces. Astfel sistemul va pune la dispoziția utilizatorilor o bază de date de cunoștințe și un robot on-line pentru a răspunde solicitărilor de suport din partea utilizatorilor.

4 ABORDARE ȘI METODOLOGIE

Prestatorul trebuie să aibă o abordare metodologică asupra întregului proces de implementare şi va descrie în cadrul ofertei sale modul în care intenționează să deruleze fiecare etapă a proiectului.
Achizitorul solicită ca în cadrul proiectului să fie parcurse cel puţin următoarele etape obligatorii, care vor fi finalizate cu livrabile ce vor fi acceptate de către achizitor:

- Analiza situației existente la momentul implementării sistemului, conform cerințelor Caietului de sarcini;
- Proiectarea soluției care să respecte cerințele Caietului de Sarcini și cerințele actualizate, identificate în etapa de analiză, cu prezentarea către Achizitor a minim 2 iterații/propuneri intermediar a scenariilor de utilizare realizate în proiectarea sistemului înainte de livrarea versiunii inițiale supuse recepției de către Achizitor;
- Instalarea, configurarea și testarea infrastructurii hardware și software propuse de Prestator;
- Dezvoltarea sistemului informatic și integrarea acestuia conform cerințelor caietului de sarcini, analizei și proiectării aprobate de Achizitor, cu prezentarea către Achizitor a minin 2 iterații/prototipuri intermediare înainte de livrarea versiunii inițiale supuse testării funcționale de către Achizitor
- Instalarea și configurarea sistemului informatic pe infrastructura hardware și software ofertată, conform cerințelor identificate în caietul de sarcini, analiză și proiectare;
- Migrarea datelor existente în sistemele anterioare în noul sistem
- Testarea sistemului informatic, atât din punct de vedere funcțional cât și pentru îndeplinirea cerințelor de securitate și performanță;
- Pilotarea sistemului informatic și asistență pentru intrarea în producție a fiecărei componente a acestuia;
- Instruirea utilizatorilor și administratorilor sistemului atât pentru operarea acestuia cât și pentru administrarea, întreținerea și extinderea acestuia;
- Organizarea unui centru de suport tehnic și asigurarea serviciilor specifice de suport tehnic, mentenanță și garanție a sistemului integrat ofertat;
- Asigurarea serviciilor de promovare și publicitate a noului sistem.

Notă:

Acceptanța sistemului informatic sau a fiecărei componente a acestuia va presupune parcurgerea cu succes a tuturor testelor funcționale, de performanță și securitate, și îndeplinirea **integrală a tuturor cerințelor** caietului de sarcini, analizei și proiectării.

4.1 Etapa de analiză

Rolul principal al fazei de analiză este acela de a înțelege în mod corect nevoile tuturor categoriilor de utilizatori ai viitorului sistem informatic, ca o permisă absolut necesară pentru calibrarea în mod corespunzător a tutuor fluxurilor de date și a proceselor de business ce vor fi implementate astfel încât, pornind de la cerințele funcționale enunțate în cadrul prezentului proiect tehnic, SIAMC 2.0 să poată asigura atingerea nivelului de performanță și de funcționalitate solicitat de către Inspecția Muncii.

În vederea implementării sistemului, Prestatorul va trebui să execute activități de analiză 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, pentru aria de acoperire a proiectului;

c. Cerințele clientului colectate și evaluate în timpul acestei faze.

Activitățile desfășurate în această etapă se vor concentra inițial pe completarea informațiilor prezentate în caietul de sarcini astfel încât Prestatorul să poată avea o imagine corectă și completă a domeniului de interes.

Analiza va avea în vedere, dar nu se va limita numai la:

- întâlniri de lucru între Prestator şi Beneficiar, iar acolo unde este cazul şi alți reprezentanți ai instituțiilor subordonate Beneficiarului;
- existența și conținutul altor aplicații informatice similare, existente la Beneficiar;
- toate documentele puse la dispoziția Prestatorului cu privire la indicatorii de performanță ce trebuie implementați în cadrul sistemului;
- necesitățile specifice Beneficiarului şi, daca este cazul, cele impuse de regulamentele comunitare sau de legislația în vigoare din România;

Aceasta activitate se va concretiza într-unul sau mai multe documente detaliate de analiza, care vor include definirea proceselor de lucru (situația existentă și viitoare), specificațiile funcționale necesare etapelor de dezvoltare şi implementare, incluzând, fără a se limita la acestea: scheme logice de funcționare, structuri de date, specificațiile tehnice şi funcționale detaliate pentru aplicație şi pentru indicatorii de performanță dezvoltați.
Prestatorul va derula activități de colectare date necesare pentru definirea în detaliu a cerințelor aferente noului sistem. Vor fi colectate informațiile necesare în vederea:

a. Identificării legislației și a procedurilor operaționale care reglementează procesele din scopul proiectului;

b. Mapării grafice a proceselor (se va utiliza un instrument software de modelare BPMN). Furnizorul va pune la dispoziția Beneficiarului instrumentele software necesare pentru vizualizarea diagramelor de proces.

Documentele rezultate în urma acestei activități vor fi redactate în limba româna şi vor fi aprobate de Beneficiar.

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

Propunerea tehnică trebuie să cuprindă următoarele:

a. Metodologia detaliată pentru derularea activităților de analiză

b. Descrierea instrumentelor utilizate în vederea colectării și evidența cerințelor, asigurării trasabilității cerințelor pornind de la obiectivele proiectului pana 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);

c. Prezentarea detaliată a livrabilelor aferente prestării activităților de analiză, care să includă:
    - Formularul/formularele aferente fiecărui livrabil;
    - Descrierea informațiilor conținute de către fiecare livrabil;
    - Modul de interpretare al conținutului fiecărui livrabil.

Analiza se va efectua la sediul Beneficiarului și va avea ca finalitate un pachet de specificații funcționale agreat de comun acord cu acesta. Cu acordul Beneficiarului, anumite activități din cadrul fazei de analiză se vor putea desfășura prin mijloace de comunicare la distanță.

Serviciile de analiză vor acoperi cel puțin următoarele aspecte:

a. Analiza contextului existent;

b. Înțelegerea structurii organizatorice a Beneficiarului;

c. Analiza situației din momentul de față din cadrul instituției Beneficiarului și a organizațiilor partenere prin ședințe de analiză, chestionare etc. Se vor identifica și documenta procesele care vor fi impactate prin implementarea soluției în cadrul contractului;

d. Definirea cerințelor informaționale pentru noul sistem. Se va contura astfel, imaginea viitorului sistem prin stabilirea proceselor operaționale care să precizeze succesiunea activităților, participanții și momentul intervenției acestora, locația sau contextul, modalitatea de intervenție, informația procesată și resursele utilizate. Pentru prezentarea proceselor se vor utiliza instrumente de modelare a proceselor și activităților în conformitate cu standarde de modelare și reprezentare recunoscute (BPMN sau echivalent);

e. Stabilirea tipurilor de roluri de utilizatori care vor interacționa în viitorul sistem;

f. Se vor evidenția activitățile care urmează a fi automatizate, astfel încât să se identifice clar funcțiile viitorului sistem informatic.

g. Maparea structurilor de date disponibile sub aspectul necesității de asigurare a compatibilității/interoperabilității SIAMC 2.0 cu respectivele sisteme. În acest scop, componenta de ETL va trebui să dețină capabilități de conversie/transformare și procesare a datelor de intrare (“input”) în diferite alte formate de date structurate („output”) necesare în cadrul fluxurilor de lucru ce generează date pentru necesitățile sistemului SIAMC 2.0.

Prestatorul va notifica beneficiarul asupra momentului estimat de acesta pentru finalizarea activităților de analiză în vederea organizării unei sesiuni de prezentare a livrabilelor astfel rezultate, această etapă urmând să fie considerată finalizată după predarea de către prestator a livrabilelor antemenționate și, respectiv, ulterior analizării, verificării și aprobării acestora de către beneficiar.

Livrabil: Raport de analiză (ce include cel puțin următoarele: fluxuri de lucru/procese specifice, cazuri de utilizare, matricea de trasabilitate, surse și categorii de date, nomenclatoare, cerințe de configurare, integrare etc.). Livrabilele vor avea anexate toate documentele ce reies din etapa de Analiza a cerințelor conform solicitărilor

4.2 Etapa de proiectare

Etapa de proiectare va avea la bază livrabilele aprobate de beneficiar în urma definitivării etapei de analiză și cerințele caietului de sarcini și va avea drept finalitate detalierea la nivel tehnic a cerințelor și specificațiilor rezultate din activitatea de analiză pentru toate nivelurile și componentele/modulele și/sau funcționalitățile SIAMC, scop în care vor fi suprinse cel puțin următoarele aspecte:

- Arhitectura de sistem: se va prezenta cel puțin pe următoarele niveluri i) hardware, ii) comunicații, iii) componente software instalate, iv) arhitectura logică cuprinzând descrierea componentelor de sistem, precum și a celor dezvoltate sau personalizate, inclusiv specificațiile funcționale și non-funcționale ale acestora;
- Modelul de securitate implementat la nivel: i) logic (organizarea pe roluri, grupuri, drepturi, etc.) și ii) fizic (servere, comunicații, aplicații etc.);
- Integrările la nivel de componentă software: pentru fiecare interacțiune se va specifica sistemul sursă/destinație, modalitatea de implementare, canalul de comunicare, setul și structura de date transferate, reguli specifice de validare etc;

- Modelul de date propus: se vor prezenta, la nivel logic, structurilor de date de la nivelul fiecărei componente/fiecărui modul a soluției;
- Scenarii 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 fructificata 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. Pentru prezentarea cazurilor de utilizare se vor folosi instrumente în conformitate cu standarde de modelare și reprezentare recunoscute (UML sau echivalent). Prestatorul va prezenta scenariile de utilizare detaliate pentru întreg sistemul în minim 2 iterații înainte de livrarea versiunii supuse recepției de către Achizitor și va prezenta, la fiecare iterație, opțiunile de proiectare avute în vedere, respectiv va implementa în vederea recepției feedback-ul Achizitorului în proiectarea sistemului.
- Scenariile (cazuri) de testare și planurile de testare propuse: se va prezenta detaliat modalitatea de testare pentru verificarea/validarea implementării corecte a tuturor cerințelor prezentului proiect tehnic, prin raportare la elementele de detaliu/specificații/cerințe rezultate în urma etapei de analiză, inclusiv din perspectiva testelor de penetrare și managementul continuității;
- Planul de instruire a utilizatorilor;
- Proiectarea/design-ul următoarelor elemente:
    - Structura bazei de date nominale la nivel central;
    - Fluxurile de date (interne și de interconectare cu sistemele/aplicațiile externe) la nivel logic;
    - Structura de date de la nivelul depozitului de date (DW);
    - Interfețele utilizatorilor, pentru fiecare componentă/modul în parte, inclusiv interfețele de raportare și analiză și cele de migrare de date;
    - Conectorii cu sistemele informatice/aplicațiile software terțe existente la nivelul instituțiilor partenere în vederea asigurării schimbului automat de date dintre acestea, respectiv a accesului programatic la respectivele date (achiziția și expunerea de date) via servicii web. Se vor descriere serviciile de integrare, inclusiv din perspectiva dezvoltărilor/configurărilor/personalizărilor necesare pentru asigurarea schimbului de date/interconectarea/interoperabilitatea SIAMC cu terțe sisteme informatice și, respectiv, privind achiziția de date, precum și a specificațiilor funcționale și non-funcționale ale acestora (interfețele de comunicare dintre diferitele componente, modelul de date și standardele utilizate);
    - Procese de back-up și restaurare;

Propunerea tehnică trebuie să cuprindă următoarele:

a. Metodologia detaliată pentru derularea activităților de proiectare
b. Descrierea instrumentelor utilizate în acest proces
c. Prezentarea detaliată a livrabilelor aferente prestării activităților de proiectare, care să includă:
    - Formularul/formularele aferente fiecărui livrabil;
    - Descrierea informațiilor conținute de către fiecare livrabil;
    - Modul de interpretare al conținutului fiecărui livrabil.

Livrabil: Raport de proiectare a sistemului (ce include cel puțin următoarele: arhitectura de sistem și modul în care se propune configurarea componentelor de sistem astfel încât să se obțină

funcționalitățile solicitate în proiectul tehnic și/sau identificate/detaliate în etapa de analiză – arhitectura hardware de rețea și securitate, software și funcțională; interfețe; module; funcționalități; specificații tehnice fluxuri; tipuri/categorii de formulare/template-uri care vor fi gestionate; model de date; specificații de securitate și de integrare). Livrabilele vor avea anexate toate documentele ce reies din etapa de proiectare a sistemului conform solicitărilor din acest subcapitol.

4.3 Etapa de dezvoltare

Etapa de dezvoltare va avea la bază livrabile aprobate de beneficar în urma definitivării etapei de analiză și proiectare, în cadrul acesteia urmând a fi derulate activități de configurare, personalizare/dezvoltare a componentelor sistemului informatic (definire fluxuri, dezvoltare module/componente, dezvoltare interfețe, dezvoltare proceduri/procese /back-up/restaurare soluție și date etc), astfel încât la finalul fazei de dezvoltare va rezulta o soluție informatică completă, dezvoltată în conformitate cu cerințele prezentului proiect tehnic.

În cadrul fazei de dezvoltare, Prestatorul va realiza inclusiv testarea internă a dezvoltărilor software realizate (înainte de a proceda la predarea unei anumite dezvoltări software/unei noi versiuni/patch către beneficiar în vederea realizării propriilor sale teste).

Prestatorul va prezenta prototipuri vizuale ale sistemului în minim 2 iterații înainte de livrarea versiunii supuse recepției de către Achizitor și va prezenta, la fiecare iterație, opțiunile de dezvoltare avute în vedere, respectiv va implementa în vederea recepției feedback-ul Achizitorului în dezvoltarea sistemului. Dezvoltarea prototipurilor la nivel de modul/secțiune se va realiza pe echipamentele Prestatorului. În baza prototipurilor aprobate de beneficiar se va realiza dezvoltarea ulterioară, inclusiv cu realizarea transferului/importului de date din alte aplicații, în măsura în care se identifică necesitatea în urma analizei. In cazuri justificate, Beneficiarul poate solicita ajustarea/corectarea specificațiilor funcționale ca urmare a prezentării prototipurilor, Prestatorul asigurând analiza, dezvoltarea, testarea şi implementarea acestor modificări, la fiecare iterație.

Prestatorul va asigura o comunicare eficienta și permanentă cu Beneficiarul şi, daca este necesar, la solicitarea Beneficiarului, cu reprezentanții desemnați în acest sens de către alţi contractori ai acestuia.

Testarea tuturor funcționalităților aplicației, inclusiv a indicatorilor de performanta, va fi realizata de către Beneficiar. Prestatorul va elabora în acest sens documentația necesara şi va asigura întreaga logistica aferenta derulării acesteia în bune condiții. Prestatorul va asigura echipamentele necesare dezvoltării şi testării.

Împreună cu codul sursă aferent personalizărilor/dezvoltărilor realizate (predat în format electronic și însoțit de comentarii, pentru toate soluțiile și aplicațiile dezvoltate în vederea implementării prezentului proiect, precum și de procedura de compilare a codului sursă), în cadrul livrabilelor aferente acestei etape prestatorul va pune la dispoziția beneficiarului:

- Documentația tehnică emisă de producător (manuale de utilizare, acolo unde este cazul), precum și manuale de utilizare actualizate în vederea utilizării și administrării componentelor/modulelor SIAMC. Manualele de utilizare vor conține prezentarea detaliată a modului de utilizare a fiecărei componente/modul al SIAMC, vor fi elaborate în limba română și vor fi destinate atât administratorilor (în vederea operării și administrării sistemului) și utilizatorilor (interni și externi) cât și, după caz, clienților terți.
- Scripturile pentru crearea bazelor de date și a componentelor funcționale, interfețele utilizatori, configurările utilizatorilor și drepturile de acces, proceduri de back-up și restaurare, proceduri de roll-back;
- După caz, versionările componentelor/modulelor SIAMC dezvoltate de Prestator (inclusiv eventualele Release notes);

- Interfețele pentru migrarea datelor
- Conectorii cu sistemele informatice/aplicațiile software terțe existente la nivelul instituțiilor partenere în vederea asigurării schimbului automat de date dintre acestea;
- Planurile de testare actualizate (inclusiv scenariile/cazurile de testare) în urma parcurgerii etapei de dezvoltare;
- Rezultatele testelor interne realizate;
- Tabelul de corespondență actualizat (matricea de trasabilitate) în urma parcurgerii etapei de dezvoltare.

În cadrul propunerii tehnice ofertantul trebuie să prezinte:

a. Metodologia detaliată în baza căreia vor fi desfășurate activitățile de dezvoltare și testare internă, demonstrând integrarea acestor proceduri cu procedurile de analiză și proiectare;

b. Instrumentele utilizate în desfășurarea activităților de dezvoltare și testare internă;

c. Detalierea livrabilelor aferente prestării activităților de dezvoltare și testare internă.

Livrabile:

Raport faza dezvoltare care să conțină minim matricea de trasabilitate actualizată, rezultatele testărilor interne, scripturile pentru crearea bazelor de date și a componentelor funcționale, interfețele utilizatori, configurările utilizatorilor și drepturile de acces, proceduri de back-up și restaurare, proceduri de roll-back, conectorii cu sistemele informatice/aplicațiile software terțe existente la nivelul instituțiilor partenere în vederea asigurării schimbului automat de date dintre acestea

Cod sursă

Documentație tehnică

Documentație de utilizare

Release notes/sistemul de management al configurațiilor

4.4 Etapa de implementare

Prestatorul trebuie să includă în cadrul răspunsului tehnic o listă detaliată a tuturor serviciilor de implementare necesare pentru instalarea si punerea in functiune a soluției propuse şi o listă a tuturor operațiunilor și facilităților ce trebuie oferite de Achizitor, pe care Prestatorul le consideră necesare pentru funcționarea optimă a sistemului ofertat. Prestatorul trebuie să se asigure că la nivelul sistemului de operare, pentru fiecare componentă a soluției propuse se vor dezactiva toate serviciile ce nu sunt folosite.

4.4.1 Livrare, instalare, punere în funcțiune a infrastructurii hardware și de comunicații

Prestatorul este responsabil în totalitate de livrarea produselor, respectiv activități legate de furnizarea produselor, cum ar fi: transportul, asigurarea, instalarea, punerea în funcțiune, asistență tehnică în perioada de garanție și orice alte asemenea obligații care revin acestuia prin contract.

Toate cheltuielile legate de activitățile echipelor de instalare vor fi suportate integral de Ofertant.

Pentru livrarea și implementarea infrastructurii hardware solicitate vor trebui asigurate următoarele activități:

a. Livrarea echipamentelor necesare funcționării soluției informatice;

b. Servicii de livrare, etichetare, instalare și punere în funcțiune echipamente;

c. Derularea activităților corespunzătoare recepției cantitative a echipamentelor;

d. Derularea activităților corespunzătoare recepției calitative a echipamentelor;

e. Livrarea documentației tehnice a echipamentelor recepționate.

Documentația asociată livrării va conține obligatoriu informații privind:

a. Tipul și codul echipamentelor ce vor fi instalate în site, conform cu propunerea tehnică detaliată anterior;

b. Diagrama conexiunilor fizice între echipamente și poziția acestora în rack-ul/urile existent/e la beneficiar;

c. Tabele cu informații privind conexiunile dintre echipamente (va conține tipul de cablu folosit, etichetarea, ce echipamente conectează, etc.) ;

d. Conexiunile acestora la prizele de electroalimentare în rack-ul/urile ofertat/e sau existent/e la beneficiar.

Ofertantul va pune la dispoziția Autorității Contractante lista completă a personalului său (inclusiv cel care aparține asociaților și subcontractanților) care va fi implicat în derularea contractului și prestarea serviciilor de instalare, configurare și punere în funcțiune și care vor necesita acces în locațiile de instalare și acces la informații despre acestea.

Procedurile de etichetare care vor fi elaborate de comun acord cu Beneficiarul și vor conține obligatoriu informații privind:

a. Procedura de etichetare fizică a echipamentelor hardware, a cablurilor de interconectare și a cablurilor de electroalimentare;

b. Proceduri de etichetare electronică la conectarea remote pe echipamente pentru administrare (prompt echipamente, banere de login, descriere interfețe, etc), daca este cazul.

Se vor efectua următoarele operații în vederea punerii în funcțiune a infrastructurii hardware și de comunicații:

a. Transportul echipamentelor de către Prestator la sediul Beneficiarului în vederea instalării și punerii în funcțiune, respectând normele de transport impuse de către producător și de ambalare (în cazul în care echipamentele livrate nu sunt ambalate în ambalajul original);

b. Instalarea fizică a fiecărui echipament în rack;

c. Interconectarea echipamentelor (folosind cabluri UTP cat.5/6, Fibră optică etc.) furnizate de către ofertant;

d. Conectarea echipamentelor la sursele de electroalimentare;

e. Interconectarea noilor echipamente cu sistemul de comunicații existent, daca este cazul;

f. Inițializarea echipamentelor;

g. Teste de interconectare pentru fiecare legătură;

h. Refacerea conexiunilor eronate, în cazul în care unele teste de interconectare dau erori de comunicație;

i. Marcarea cu etichete a fiecărui echipament și conexiune conform cu procedura de etichetare agreată. Modul concret de realizare, inscripționare și fixare a etichetelor pe echipamente și cabluri se va propune de către Prestator și se va accepta de către Autoritatea Contractanta după intrarea în vigoare a contractului, dar înainte de începerea instalării acestora.

Echipamentele hardware livrate trebuie să fie noi și să beneficieze de garanție și suport conform cerințelor generale de garanție hardware (nu se accepta echipamente uzate fizic sau moral, de tip refurbished sau care sunt EOL sau EOS sau sunt anunțate EOL sau EOS).

Activitățile de instalare a produselor hardware se vor realiza de către reprezentanții Ofertantului sub supravegherea personalului Autorității Contractante/ reprezentanților STS.

Toate echipamentele vor fi configurate de către Prestator conform soluției tehnice agreate cu Beneficiarul/ reprezentanții STS în urma ședințelor comune.

Planul de adresare IP pentru configurarea echipamentelor instalate va fi pus la dispoziția Prestatorului de către Beneficiar, iar acesta din urmă va configura adresele IP de producție pe echipamentele respective, după efectuarea tuturor testelor de verificare.

Echipamentele trebuie livrate împreună cu toate accesoriile necesare punerii în funcţiune, chiar daca acestea nu au fost solicitate în mod explicit în capitolul 3 al prezentei documentații, dar sunt necesare pentru operaționalizarea și integrarea echipamentelor în infrastructura existentă la Achizitor / STS.

Livrabile:

Avize de însoțire a mărfii

Certificate de garanție și conformitate

Raport de instalare și punere în funcțiune echipamente, ce va conține obligatoriu informații privind:

a. ***Tipul și codul echipamentelor ce au fost instalate în fiecare site, conform propunerii tehnice anexă la contract;***
b. ***Diagrama conexiunilor fizice între echipamente și poziția acestora în rack/rack-uri;***
c. ***Tabele cu informații privind conexiunile dintre echipamente (va conține tipul de cablu folosit, etichetarea, ce echipamente conectează, etc.);***
d. ***Tabel cu informații referitoare la conexiunile electrice ale tuturor echipamentele instalate;***
e. ***Descrierea modului de configurare a fiecărui echipament, precum și a softului de bază aferent (inclusiv cu capturi de ecran din consola de administrare);***
f. ***Consumul energetic al echipamentelor și distribuția acestuia conform schemei de cablare electrica și balansării surselor de alimentare ale echipamentelor redundante;***
g. ***Descrierea modului de verificare și testare a infrastructurii – Plan de recepție***
h. ***Descrierea modalității de acces la suport tehnic (conturi, chei de acces, etc)***
i. ***Dovada accesului beneficiarului la serviciile solicitate (de tip SLA)***

4.4.2 Livrare, instalare și configurare infrastructură software de bază și de aplicații

Prestatorul este responsabil de livrarea, instalarea și configurarea infrastructurii software de bază și aplicații ofertate.

Activitățile de instalare și configurare a infrastructurii software de bază și aplicații se vor realiza de către reprezentanții Ofertantului sub supravegherea personalului Autorității Contractante.

Livrabile:

Kituri de instalare și chei de acces unde este cazul

Certificate de garanție și conformitate (unde se aplică)

Documentație tehnică

Raport de instalare și configurare a componentelor software, ce va conține obligatoriu:

a. ***Tabel cu produsele software livrate și instalate***
b. ***Tabel cu mașinile virtuale configurate***
c. ***Descrierea modului de instalare a fiecărei componente software***
d. ***Lista de verificare a instalării și configurării preliminare a componentelor software***
e. ***Modalitatea de acces a suportului tehnic (conturi portal suport, chei de acces, etc)***
f. ***Dovada accesului beneficiarului la serviciile de garanție solicitate***

4.4.3 Instalarea și configurarea sistemului informatic

Prestatorul este responsabil de instalarea și configurarea sistemului SIAMC 2.0 pe infrastructura hardware și software ofertată și instalată de acesta (mediul de test și mediul de producție)

Activitățile de instalare și configurare a sistemului se vor realiza de către reprezentanții Ofertantului sub supravegherea personalului Autorității Contractante/ reprezentanții STS.

Ofertantul trebuie să descrie în detaliu metodologia după care va derula activităţile de implementare (deployment) în mediul de producţie.

Ofertantul trebuie să prezinte împreună cu oferta procedurile de implementare și livrabilele care vor rezulta în urma prestării serviciilor corespunzătoare etapei de implementare a sistemului informatic, precum și formularele asociate (modele) ale acestor livrabile

Livrabile:

Raport de instalare și configurare sistem SIAMC 2.0

Documentații tehnice complete

Cod sursă și cod obiect, commentate și descrise, livrate împreună cu un instrument de gestionare și versionare a codului sursă

4.4.4 Instalare și configurare a aplicatiilor pe dipozitivele mobile(telefon/laptop)

Prestatorul este responsabil de instalarea și configurarea clientului de VPN si a aplicațiilor pe pe dipozitivele mobile (telefon/laptop) ce vor fi achiziționate de Beneficiar și puse la dispoziția acestuia ulterior.

Furnizarea unei proceduri de instalare și configurare a aplicațiilor pe dispozitivele mobile ce vor fi puse la dispoziție de Beneficiar.

Livrabile:

Raport de instalare și configurare aplicații pe dispozitive mobile și laptop-uri

4.5 Etapa de testare

În cadrul propunerii tehnice Ofertantul trebuie să prezinte:

- Modalitatea în care va realiza testarea infrastructurii hardware și software de bază
- Modalitatea în care se va realiza testarea sistemului informatic și testele de acceptanță specifice
- Metodologia de testare după care se vor realiza activitățile de testare în timpul desfășurării contractului, inclusiv cea pentru testarea funcțională, testarea de performanță, înaltă disponibilitate și securitate;

- Modalitatea de testare a interfețelor de migrare a datelor și metodologia de verificare a consistenței și corectitudinii acestora
- Metodologiile și tehnicile utilizate în evaluarea vulnerabilităților
- Instrumentele de testare folosite
- Livrabilul/livrabilele rezultate și formularul/formularele care vor fi utilizate;

Testele de acceptanță se vor derula pe mediul de testare, în conformitate cu Planul de Teste realizat de Prestator și agreat de Beneficiar, 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.

Un set relevant dintre aceste teste (respectiv pentru toate componentele/modulele și/sau procesele/funcționalitățile care pot avea un impact semnificativ asupra bunei funcționări a sistemului), vor fi rulate pe mediul de producție înainte de momentul GoLive al SIAMC.

Beneficiarul (cu asistența Prestatorului) va rula toate scenariile pentru testele de acceptanță ale întregului sistem (infrastructură hardware, software de bază, sistem informatic) sau componentă livrată (module dacă este cazul).

Ofertantul va include în planul de testare metodologia de testare a corectitudinii și consistenței datelor migrate, iar pe parcursul derulării testelor de acceptanță va derula procedurile de migrare a informațiilor istorice din sistemul existent.

În cadrul testării de acceptanță se vor efectua teste de performanță cel puțin pentru a demonstra capabilitățile sistemului de a susține numărul de utilizatori concurenți/total solicitat în Caietul de sarcini și performanțele de accesare/răspuns a sistemului definite în analiză și proiectare.

Planul de testare pentru acceptanță va cuprinde toate testele necesare pentru a demonstra acoperirea în întregime a cerințelor din prezentul proiect tehnic. Astfel, se va avea în vedere faptul că infrastructura hardware și sofware, precum și sistemul informatic funcționează corect din punct de vedere al respectării cerințelor, consistenței datelor, al constrângerilor de timp, al validărilor de date și al gestiunii erorilor, inclusiv pentru funcționalitățile existente care au fost extinse sau modificate. Criteriul de succes – sistemul trece toate testele definite în planul de testare agreat împreună cu Beneficiarul.

Testarea de acceptanță se va desfășura pe infrastructura livrată și date introduse/migrate din sistemele anterioare și se va finaliza cu un Proces verbal de acceptanță funcțională. Procesul verbal de acceptanță finală a sistemului va fi acordat după etapa de asistență la intrarea în producție și implementarea tuturor observațiilor Beneficiarului.

Ofertantul va realiza evaluarea securității sistemului integrat care va adresa sistemul informatic, infrastructura software și echipamentele pe care se bazează acesta precum și interfețele cu alte sisteme informatice și aplicații specifice. În cadrul evaluărilor vor fi realizate inclusiv teste de penetrare din interiorul și exteriorul rețelei.

Ofertantul va realiza minim următoarele analize, documentate prin intermediul unui livrabil ***Analiză și raport securitate***:

- Conformitatea soluției cu cerințele de securitate din cadrul proiectului;
- Evaluarea securității din perspectiva modului de implementare și configurare a sistemului informatic. Vor fi analizate din punct de vedere al securității informației toate componentele sistemului informatic: aplicații, baze de date și infrastructura IT
- Verificarea și validarea modului de implementare a controalelor de securitate
- Teste de securitate de tip "ethical hacking" asupra întregului sistemului
- Analiza de risc a sistemului în urma vulnerabilităților identificate

În urma executării activității de testare a securității se va livra un raport ce va conține informații detaliate privind vulnerabilitățile identificate, măsurile și sugestiile de remediere a acestora. După remedierea vulnerabilităților identificate se va reface testarea de securitate și se va prezenta raportul rezultat.

Livrabile:

Plan și documentație de testare

Rapoarte de testare

Analiză și raport securitate

4.6 Etapa de lansare și punerea în producție (GoLive), inclusiv migrarea și integrarea datelor

Etapa de lansare și punere în producție a sistemului se va realiza în baza unui plan de trecere în producție, care trebuie să țină cont de sistemele/integrările existente, astfel încât să se asigure o trecere în producție coerentă și cu impact minim asupra activității Beneficiarului și a utilizatorilor externi (angajatori, etc). La momentul GO LIVE, sistemul informatic integrat va fi livrat beneficiarului complet, respectiv "la cheie", având implementate toate componentele/modulele solicitate potrivit prevederilor prezentului proiect tehnic astfel încât acesta să poată fi utilizate în mod normal.

În vederea realizării acestui deziderat, prestatorul va avea în responsabilitate realizarea pe parcursul acestei etape a oricăror ajustări/optimizări considerate necesare de beneficiar în raport cu procesele/fluxurile de lucru implementate și/sau a corectării eventualelor erori de funcționare/bug-uri care nu au putut fi identificate în mod rezonabil în cadrul etapei de testare a calității.

Tot în cadrul acestei etape, înainte de GO LIVE se va finaliza migrarea datelor istorice și integrarea cu sistemele terțe, urmată de reluarea în mod punctual a etapei de testare a calității în vederea verificării și validării de către beneficiar a serviciilor de migrare și integrare astfel realizate.

Ofertantul va include în oferta tehnică etapele pe care le consideră necesare a se derula în cadrul acestei etape, împreună cu instrumentele utilizate (software), descrierea livrabilelor și a formularelor model pentru acestea.

Ofertantul va asista on-site sau on-line, zilnic, pe o durată de 3 luni de la intrarea în producție, personalul Achizitorului pentru operarea infrastructurii livrate și a sistemului SIAMC – realizarea operațiilor în sistem împreuna cu personalul Achizitorului. Observațiile colectate, îmbunătățirile sau problemele semnalate vor fi discutate săptămânal cu Achizitorul și apoi implementate în sistem.

La finalul perioadei de asistență, Ofertantul va livra un Raport de asistență la intrarea în producție sumarizator a problemelor și îmbunătățirilor rezolvate și a modalității efective de implementare.

Procesul verbal de acceptanță finală a sistemului va fi acordat după implementarea problemelor și îmbunătățirilor semnalate de Achizitor în această etapă.

Livrabile

Raport privind lansarea și punerea în producție a sistemului SIAMC

Certificat de garanție sistem informatic

Pachet documente actualizate (dacă e cazul) în cadrul acestei etape

Raport de asistență la intrarea în producție

4.7 Etapa de instruire

Oferta trebuie să cuprindă sesiuni de instruire pentru personalul Achizitorului: personalul IM și ITM-urilor, conform cerințelor detaliate mai jos.

Ofertanții vor propune în cadrul ofertelor metodologia după care se va desfășura programul de formare precum și un plan (calendar) de sesiuni de instruire astfel încât să fie acoperite toate cerințele cantitative și calitative solicitate.

Pe durata instruirii, Prestatorul va întocmi rapoarte de prezență zilnice. La finalul instruirii, Prestatorul va livra câte un Raport de instruire pentru fiecare sesiune de instruire care să aibă anexate cel puțin Listele de prezență, Evaluarea cursului și a cursanților, Lista de înmânare a certificatelor de participare, Certificate de participare cursanți.

4.7.1 Instruirea utilizatorilor

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

- Prezentarea sistemului, a modulelor și funcționalităților generale
- Autentificare și profilul utilizatorilor, rolurile și drepturile acestora
- Utilizarea fiecărui modul funcțional
- Modalitatea de utilizare a documentației tehnice și de solicitare a suportului tehnic

Structura grupului de utilizatori ce vor participa la programul de formare:

- 2100 de utilizatori din partea IM și ITM-urilor

Prestatorul va organiza minim 100 sesiuni a minim 32 ore/ sesiune în fiecare oraș reședință de județ (40 de orașe reședință, în afară de București și Ilfov), pentru grupe de maxim 30 de cursanți.

Instruirea se va realiza în limba română. Sesiunile de instruire se vor desfășura în locații asigurate de Prestator, din fiecare reședință de județ. Locațiile vor fi alese astfel încât să fie respectate toate cerințele legale impuse de starea de alertă/urgență dacă va fi cazul la momentul derulării programului de formare. Prestatorul va asigura toate condițiile necesare în acest sens, coform cerințelor legale.

Prestatorul va asigura și logistica necesară desfășurării programului de formare: calculatoare/laptop-uri (câte unul pentru fiecare participant la sesiunea de formare), video-proiector, flipchart, catering pentru participanți (2 pauze de cafea și masa de prânz), suportul de curs și materialele consumabile necesare. Suportul de curs va fi disponibil în format electronic și va respecta prevederile de identitate vizuala aferente proiectelor finanțate prin PNRR. Achizitorul va furniza elementele de identitate vizuală necesare. Participanții la programul de formare vor primi diplome de participare/absolvire din partea Prestatorului. Șablonul diplomelor va fi propus de Prestator și aprobat de Achizitor.

Instruirea se va realiza pe mediul de instruire asigurat de Prestator care va reproduce mediul de producție și va fi încărcat cu date de test semnificative pentru înțelegerea conceptelor și modului de funcționare a platformei integrate.

Oferta va include programa și planul de formare propus pentru atingerea obiectivului serviciului.

4.7.2 Instruirea administratorilor

Instruirea administratorilor platformei, va trebui să acopere minim următoarele aspecte:

1. Administrare infrastructură hardware și de securitate ofertată
2. Administrare infrastructură software de bază ofertată

3. Administrare și configurare sistem SIAMC, a componentei de Sistem de Management electronic al Documentelor și de Analiză și Raportare
4. Modalități de asigurare a suportului tehnic

Instruirea va fi realizată de personal calificat al Prestatorului sau producătorilor soluțiilor ofertate, în limba română. Durata sesiunii de formare trebuie să fie de minim 5 zile a 6 ore/zi și se va finaliza cu o diplomă de participare. Prin parcurgerea programului de formare participanții trebuie să dobândească competențe de administrare și utilizare a infrastructurii si sistemului SIAMC, dar și de acordare de suport colegilor utilizatori din IM și ITM-uri.

Prestatorul va asigura și logistica necesară desfășurării programului de formare: calculatoare/laptop-uri (câte unul pentru fiecare participant la sesiunea de formare), video-proiector, flipchart, catering pentru participanți (2 pauze de cafea și masa de prânz), suportul de curs și materialele consumabile necesare. Suportul de curs va fi livrat în format electronic, cu respectarea prevederilor de identitate vizuala aferente proiectelor finanțate PNRR. Achizitorul va furniza elementele de identitate vizuală necesare. Participanții la programul de formare vor primi diplome de participare/absolvire din partea Prestatorului. Șablonul diplomelor va fi propus de Prestator și aprobat de Achizitor.

Instruirea se va realiza pe mediul de instruire asigurat de Prestator care va reproduce mediul de producție și va fi încărcat cu date de test semnificative pentru înțelegerea conceptelor și modului de funcționare a platformei integrate.

Pentru componentele de infrastructură hardware și de securitate se va asigura pregătirea personalului pentru a executa toate activitățile de administrare și utilizare a echipamentelor și a soluțiilor livrate în cadrul fiecărui lot, fără suportul Prestatorului. Instruirea va include ședințe practice privind instalarea, configurarea, administrarea și operarea echipamentelor și a soluțiilor livrate, mentenanță preventivă a acestora și realizarea procedurilor de back-up și disaster recovery. Instruirea va fi realizată de instructori autorizați de producătorii produselor livrate. Participanților la instruire le vor fi furnizate documentații tehnice și materiale de instruire pe suport electronic sau imprimat. Se vor furniza obligatoriu pe suport electronic toate pachetele/kiturile software instalate (inclusiv sistemele de operare), fișierele și codurile de licență, fișierele de configurare, împreună cu toate procedurile scrise aferente. Activitatea de instruire va avea o durată de minim 3 zile pentru minim 3 persoane, pentru fiecare soluție hardware și de securitate ofertată.

Oferta va include programa de formare propusă astfel încât să fie atins obiectivul serviciului.

4.8 Etapa de suport tehnic, mentenanță și garanție

Sistemul informatic în ansamblul său trebuie să beneficieze de garanție și mentenanță din partea Prestatorului de minimum 60 de luni (5 ani) de la data lansării și punerii în producție a SIAMC (realizarea acceptanței finale).

Garanția reprezintă perioada de timp în cadrul căreia contractantul are obligația asigurării și controlului calității funcționării SIAMC, respectiv remedierea defectelor/deficiențelor constatate/incidentelor semnalate ce pot surveni în raport cu buna funcționare a sistemului informatic, precum și a produselor/echipamentelor/componentelor/modulelor/subansamblurilor/accesoriilor aferente, pe propria să cheltuială (fără costuri suplimentare în sarcina autorității contractante).

Pe perioada de garanție ofertată, pentru **operațiuni de modificare a parametrilor și configurărilor SIAMC, ajustări în funcție de diverse modificări apărute la nivelul organizației Achizitorului sau legislative**, cerința minimă și obligatorie, este de a se asigura în costul contractului, un număr de 400 de zile-om dedicate exclusiv activităților de dezvoltare sau configurare a sistemului pentru modificările identificate, la nivelul contractului sau pentru integrări cu alte sisteme dezvoltate și implementate în perioada de valabilitate a contractului, conform comenzilor Autorității contractante.

Pe parcursul întregii perioade de garanție ofertate, Contractantul este responsabil de efectuarea tuturor operațiunilor necesare, după cum urmează:

- Efectuarea diagnozelor (on-line), precum și a intervențiilor (de la distanță/remote maintenance sau on-site în cazul defectelor fizice);
- Livrarea pieselor de schimb/componentelor înlocuitoare în regim NBD de la constatarea defectului (inclusiv transport de la și la beneficiar), inclusiv eventuale materiale mărunte, piesele de schimb/subansambluri, elemente de conectică care pot fi necesare pentru efectuarea reparației, precum și instalarea și, după caz, configurarea on-site a acestora
- În situația în care remedierea unui anumit defect hardware nu poate fi realizată în regimul solicitat (on-site, NBD), fiind necesară demontarea componentei/componentelor și transportul acestora către reprezentantul producătorului/unitatea de service autorizată de acesta, asemenea servicii se vor considera incluse în prețul ofertat (nu se vor percepe costuri suplimentare pentru beneficiar) și, în mod corelativ, ofertantul va proceda la înlocuirea întregului produs (pentru întreaga durată necesară remedierii) cu un alt produs similar din punctul de vedere al specificațiilor tehnice, de natură să asigure continuitatea nivelului de funcționalitate și performanțe solicitat cel puțin la un nivel rezonabil, în termen de cel mult 24 de ore de la apariția unei asemenea situații;
- Toate produsele/ echipamentele/ componentele/ subansamblele/ modulele/ accesoriile sistemului care vor fi înlocuite în perioada de garanție, vor beneficia de o nouă perioadă de garanție (egală cu cea inițial solicitată) și care va curge de la data instalării și punerii în funcțiune a componentelor noi;
- Mediile de stocare uzate/defecte se înlocuiesc fără predarea mediilor de stocare ce trebuie înlocuite
- Fiecare intervenție în perioada de garanție va fi documentată cu ajutorul unei fișe de intervenție

Prestatorul va asigura prestarea în favoarea Beneficiarului a următoarelor servicii de suport tehnic, mentenanță și asistență de specialitate pentru soluția ofertată, pe întreaga perioadă de garanție ofertată, în raport cu:

- Infrastructura hardware, însumând echipamentele/componentele aferente sistemului informatic, astfel încât acestea să beneficieze de toate funcționalitățile necesare pentru a asigura nivelul de performanță solicitat de către Autoritatea contractantă;
- Infrastructura software de bază, însumând activele necorporale/pachetele software livrate pentru asigurarea bunei funcționări a sistemului informatic, indiferent de tipul și de modul de licențiere a acestora; precum și în raport cu
- Dezvoltările și/sau configurările personalizate realizate de Prestator în vederea îndeplinirii cerințelor funcționale stabilite prin prezentul proiect tehnic.

Serviciile solicitate vor include cel puțin următoarele:

- În cazul licențelor (active necorporale de tip COTS/Open source): servicii de suport aferente soluțiilor ofertate, precum și, în cazul activelor necorporale de tip COTS, servicii de mentenanță prin intermediul cărora se asigură upgrade-ul la cele mai noi versiuni ale programelor/suitelor de aplicații ofertate, incluzând actualizări, versiuni de întreținere, patch-uri (cum ar fi cele de securitate) și documentația tehnică aferentă;
- În cazul celorlalte tipuri de active necorporale (cum ar fi acele aplicații software aferente unor funcționalități ale infrastructurii hardware ofertate și/sau managementului acesteia): furnizarea oricăror subscripții necesare, incluzând eventualele actualizări ale acestora, astfel încât infrastructura ofertată (hardware și software) să poată funcționa în mod corespunzător, la nivelul de performanță necesar pentru rularea sistemului în condiții optime și având activate toate opțiunile necesare în acest sens;

- În cazul echipamentelor hardware: servicii de asigurare a accesului la upgrade-urile la ultima versiune a componentele software aferente (incluzând microcodul/ ”firmware-ul”, drivere componente, pachete software, sisteme de operare incluse în echipamentele ofertate etc.), precum și servicii de mentenanță și suport proactive, folosind un canal de comunicare direct între centrul de date al beneficiarului și centrul de suport al producătorului, care să garanteze diagnosticarea echipamentului sau modulului defect în vederea remedierii defectelor/înlocuirea acestuia, prin personal calificat (fără costuri suplimentare în sarcina autorității contractante)

Totodată, accesul la serviciile de suport tehnic asigurate de producătorul echipamentelor hardware va putea fi realizat nemijlocit (înțelegând prin aceasta independent de serviciile de suport tehnic asigurate de ofertant sau de către un alt terț), având SLA 24x7 și timp de răspuns de cel mult 4 ore (prin excepție de la timpii de răspuns specificați pentru nivelurile de prioritate).

Toate funcționalitățile software solicitate vor include licențiere perpetuă pentru întreaga configurație a echipamentului ofertat, indiferent de upgrade-urile ulterioare ale acestuia.

- În cazul dezvoltărilor și/sau configurărilor personalizate realizate de prestator: servicii de suport tehnic, mentenanță corectivă și evolutivă, precum și asistență de specialitate din partea ofertantului pentru remedierea defectelor/deficiențelor constatate sau a incidentelor survenite în raport cu SIAMC. Aceste tipuri de servicii includ expertiza necesară pentru soluționarea problemelor care:
- Sunt datorate bug-urilor/erorilor de funcționare care conduc la nefuncționarea sau funcționarea defectuoasă a sistemului și care degradează performanțele sistemului, a căror remediere poate necesita instalarea de modificări, upgrade-uri sau orice alte modificări prin efectul unor procese de gestionare a acestora, cum ar fi controlul versiunilor, modificări ale mediului de testare/producție și/sau retro-fitting la versiunea existentă de software;
- Impun realizarea unor operații curente de întreținere în vederea optimizării modului de funcționare a acesteia și/sau remedierea, dacă este cazul, a datelor pierdute sau modificate ca urmare a unor componente defecte ale sistemului;
- Implică modificări minore ale unor parametri de funcționare sau a unor funcționalități pentru a căror implementare nu este necesară modificarea soluției ofertate prin scriere de cod/compilări/recompilări de cod și/sau alterarea/modificare logicii de business/fluxurilor de lucru deja implementate.

Suportul tehnic în funcționarea sistemului va include și activitățile de mentenanță evolutivă ce constau în:

- Preluarea de solicitări de îmbunătățire a aplicațiilor software implementate și puse în producție;
- Aplicarea modificărilor legislative aplicațiilor software implementate și puse în producție;
- Dezvoltarea de noi funcționalități în aplicațiile software implementate și puse în producție.

Mentenanța evolutivă intra în categoria modificărilor guvernate de procedurile de management al schimbării fiind stabilită de comun acord prin ordinul de începere prestare servicii mentenanță evolutivă transmis de Achizitor. Acesta va specifica și cantitatea de efort necesar implementării modificărilor, calculat în zile/om.

Orice modificare legislativă sau modificare descoperită după faza de analiză detaliată va fi implementată de către contractor in perioada contractuală.

Serviciile se vor presta prin intermediul unui Centru de suport dedicat organizat și operat de către Prestator, pe întreaga perioadă de garanție ofertată (5 ani de la obținerea acceptanței finale). În acest sens, Prestatorul va pune la dispoziție o linie telefonică și o adresă de email dedicate, disponibile 24/7 pentru IM/ITM, cu respectarea următorului SLA:

Niveluri de prioritate

Pe parcursul execuției contractului, încadrarea nivelului de prioritate poate fi modificată fie cu acordul părților (în funcție de evoluția anumitor incidente) sau de către Prestator, dar numai cu anunțarea în avans a Achizitorului asupra acestui aspect și furnizarea justificărilor tehnice aferente în susținerea deciziei de reîncadrare.

În înțelesul celor de mai sus, prin sintagma "nivel de prioritate" se înțelege:

Nivel Prioritate	**Descriere** *(pentru încadrarea în nivelul de prioritate aferent se aplică cel puțin una din condițiile de mai jos)*	**Timp de răspuns**	**Timp maxim de rezolvare**
Critic	**Sistemul nu funcționează**, respectiv: - Incidentul/defectul/deficiența împiedică desfășurarea activității **tuturor utilizatorilor**; - Serviciile/procesele de business sunt **indisponibile**; - Utilizatorii **nu se pot conecta** și nu pot utiliza sistemul.	2 ore	***4 ore*** pentru implementarea măsurilor intermediare necesare în vederea obținerii unui nivel de funcționare ***limitat*** *(similar cu cel descris la nivelul Major)*.
Major	**Sistemul funcționează limitat**, respectiv: - Incidentul/defectul/deficiența împiedică desfășurarea activității **majorității utilizatorilor** în condiții normale; - Serviciile/procesele de business sunt disponibile **în mod restrâns** (există pierderi însemnate asupra nivelului de funcționalitate) **și/sau performanța** acestora este **semnificativ degradată/redusă**; - Utilizatorii **se pot conecta** și pot utiliza sistemul, însă **experimentează probleme/erori** care nu permit continuarea activității în integralitate.	4 ore	***8 ore pentru atingerea nivelului normal de funcționare***
Mediu	**Sistemul funcționează în cea mai mare parte normal**, dar: - Incidentul/defectul/deficiența împiedică desfășurarea activității **unui număr restrâns de utilizatori** în condiții normale; - Majoritatea serviciilor/proceselor de business sunt disponibile și/sau **performanța** acestora **nu este degradată/redusă în mod semnificativ**; - Utilizatorii **se pot conecta** și pot utiliza sistemul, însă **experimentează anumite probleme/erori** *(recuperabile)* de funcționare a acestora, fiind totuși posibilă continuarea activității.	12 ore	***48 ore pentru atingerea nivelului normal de funcționare***
Minor	**Sistemul funcționează aproape de parametrii normali**, dar:	24 ore	***5 zile pentru atingerea nivelului normal de***

	- Sunt semnalate incidente/ defecte/deficiențe cu un **impact minimal asupra sistemului/ utilizatorilor**; - Serviciile/procesele de business sunt disponibile, dar performanța unora dintre acestea este afectată în mod nesemnificativ; - Utilizatorii se pot conecta și pot utiliza sistemul, însă experimentează unele erori minore de funcționare a acestora care nu împiedică desfășurarea activității curente.		***funcționare***

În scopul prezentului proiect tehnic:

- Prin sintagmele "semnificativ", "majoritate", "cea mai mare parte" se înțelege un nivel de peste 50% prin raportare la capacitatea totală (respectiv număr de utilizatori, nivelul de performanță acceptat de achizitor la momentul intrării în producție a sistemului sau, după caz, totalitatea serviciilor/proceselor/funcționalităților sistemului);
- Prin sintagmele "restrâns" și "nesemnificativ" se înțelege un nivel de sub 50% prin raportare la capacitatea totală (respectiv număr de utilizatori, nivelul de performanță acceptat de achizitor la momentul intrării în producție a sistemului sau, după caz, totalitatea serviciilor/proceselor/ funcționalităților sistemului);
- Sintagmele "nivel normal de funcționare" sau "parametrii normali de funcționare" semnifica nivelul de performanță acceptat de achizitor la momentul intrării în producție a sistemului pentru totalitatea serviciilor, proceselor, funcționalităților acestuia.
- Pentru întârzierile care se datorează neîndeplinirii sau a îndeplinirii în mod necorespunzător a obligațiilor solicitate și asumate de Prestator se aplică penalitățile contractuale stabilite. Acestea se aplică per tip de incident/defect/deficiență unic(ă), indiferent de numărul de solicitări subsecvente care pot fi transmise Prestatorului până la recepția finală a respectivei solicitări. Depășirile timpilor maximi de rezolvare asumați pentru perioada de garanție și suport tehnic dau dreptul beneficiarului de a calcula și aplica penalizări de 0,0001 % din valoarea contractului pentru fiecare oră de depășire a acestora. Valoarea penalităților astfel calculate va fi reținuta din garanția de bună execuție constituită de Prestator.

Nivelul de performanță a serviciilor solicitate (SLA)

Prestatorul trebuie să asigure următoarelor niveluri de performanță al SLA, pe toată durata perioadei de garanție ofertate:

SLA recepție și răspuns:

- Recepționarea solicitărilor, analiza preliminară a acestora și formularea unui răspuns preliminar de către prestator trebuie să se încadreze în timpii de răspuns stabiliți conform priorității asociate, pentru cel puțin 95% din totalul solicitărilor transmise lunar;

SLA rezolvare:

- Soluționarea problemelor, incluzând instalarea corecții *(patches)* sau upgrade-uri, realizarea ajustărilor/implementarea îmbunătățirilor necesare trebuie să se încadreze în timpii de maximi de rezolvare stabiliți conform priorității asociate, pentru cel puțin 95% din totalul solicitărilor transmise lunar.

Condiții de aplicare SLA:

Timpii de răspuns și de rezolvare:

- Încep să curgă de la momentul transmiterii unei solicitări de către Achizitor către Prestator, se contorizează prin raportare la orele normale de program ale Achizitorului *(respectiv de luni până vineri, între 8.00 și 17.00)*, cu excepția cazurilor în care incidentul este încadrat în nivelul de prioritate Critic sau Major, caz în care Prestatorul va asigura suport pentru remedierea problemei 24/24, 7/7, astfel încât să fie asigurate cerințele de disponibilitate a sistemului (vezi cap 6.4). Prin ore / zile se înțelege ore lucrătoare / zile lucrătoare.
- În situația în care soluționarea problemelor implică un *down-time* al sistemului/oprirea anumitor componente din cadrul acestuia, Prestatorul va solicita acceptul Achizitorului pentru stabilirea *(de comun acord cu acesta)* a momentului planificat pentru desfășurarea intervenției. În asemenea situații, Prestatorul va proceda la planificarea operațiilor necesare astfel încât, ori de câte ori va fi posibil, down-time-ul:
  - Să nu se producă în timpul orelor normale de program;
  - Să nu depășească 24 de ore; sau
  - În situația în care este necesar un down-time mai mare, operațiile necesare să fie desfășurate în week-end;
- Acești timpi sunt calculați de la momentul recepționarii solicitării și până la trimiterea către prestator a notificării privind rezolvarea incidentului pe mediul de producție.

Recepția solicitărilor:

- În cazul în care Achizitorul nu confirmă prestatorului rezolvarea incidentului/ defectului/ deficienței în termen de 10 zile de la data punerii în producție, recepția se consideră acceptată/ aprobată fără rezerve de către achizitor (fără a mai fi necesară vreo formalitate prealabilă).
- În situația în care, în termenul anterior specificat, Achizitorul revine și reclamă același incident/ defect/ deficiență, solicitarea nu se va considera soluționată, iar timpii de rezolvare stabiliți conform priorității asociate vor curge în continuare până la închiderea definitivă a solicitării.
- Dacă Achizitorul, indiferent de motive, amână punerea în producție, respectarea timpilor maximi de rezolvare stabiliți conform priorității asociate se raportează la recepția efectuată pe mediul de test/ staging, cu respectarea termenelor mai sus menționate.

Excluderi:

- În situația în care sistemul nu este disponibil din motive ce țin exclusiv de infrastructura hardware asigurată de Achizitor, timpul necesar remedierii problemei de către Prestator nu estesunt contorizat
- Durata de timp disponibilă Achizitorului pentru confirmarea rezolvării incidentului/defectului/ deficienței potrivit celor mai sus menționate (atât în ceea ce privește recepția pe mediul de test cât și în ceea ce privește cea pe mediul de producție) nu se contorizează în cadrul timpilor maximi de rezolvare stabiliți conform priorității asociate.
- În situația în care, soluționarea unui incident/defect/deficiențe impune obținerea unor informații suplimentare din partea Achizitorului, timpii în care respectivele informații sunt puse la dispoziția prestatorului vor fi excluși din calculul SLA.

DoA – DeadOnArival – reprezintă defectele de fabricație și sau transport neimputabile direct ofertantului. În cazul în care este identificat un astfel de defect/o astfel de situație, va fi întocmit un Proces Verbal specific în care va fi stablită clar modalitatea de remediere în concordanță cu politicile fabricanților. Timpul necesar remedierii problemei de tip DoA decătre Prestator nu va fi contorizat.

Evidența/gestionarea solicitărilor adresate Prestatorului se va realiza prin intermediul unei persoane/echipe desemnate de achizitor, în ale cărei responsabilități va intra interacțiunea cu acesta în vederea remedierii defectelor/deficiențelor constatate. Solicitările vor fi semnalate prestatorului, în mod obligatoriu, în scris, prin intermediul unei aplicații dedicate de raportare incidente ce va fi pusă la dispoziție de Prestator, pentru minim toți utilizatorii sistemului, pe durata perioadei de garanție ofertate, utilizându-se un formular standardizat pus la dispoziție de acesta.

În raport cu solicitările primite potrivit celor arătate mai sus, prestatorul va proceda la:

- Analiza preliminară a problemelor ridicate de reprezentații Achizitorului și formularea către aceștia a unui răspuns preliminar;
- Prioritizarea problemelor (fie după nivelul de prioritate alocat de Achizitor, sau, după caz, potrivit reîncadrării realizate de Prestator în urma analizei și răspunsului preliminar de mai sus);
- După caz, comunicarea solicitărilor către centrul de suport tehnic al producătorului spre competentă soluționare;
- Înregistrarea, actualizarea și monitorizarea/verificarea evoluției stării cererilor până la închiderea acestora;
- Comunicarea cu reprezentanții Achizitorului în vederea analizării stadiului incidentelor deschise sau, după caz, obținerii de informații suplimentare referitoare la produsele afectate și soluțiile de asistență/suport tehnic aplicabile;
- Furnizarea descrierii soluției de remediere a defectelor/deficiențelor/incidentelor semnalate.
- Soluționarea problemelor, incluzând instalarea de corecții (patches) sau upgrade-uri, realizarea ajustărilor/implementarea îmbunătățiri necesare, monitorizarea operării corespunzătoare a sistemului ulterior realizării acestor demersuri și, după caz, actualizarea/revizuirea documentației tehnice predate achizitorului și instruirea utilizatorilor.

Acolo unde este posibil serviciile de asistență tehnică vor putea fi asigurate "remote", dacă soluționarea unei probleme nu necesită prezența on-site a personalului calificat al Prestatorului

În vederea asigurării Autorității contractante cu privire la îndeplinirea la termen şi la parametrii de calitate solicitaţi a obligaţiilor contractuale ce revin Prestatorului pe parcursul perioadei de garanţie, conform celor specificate în caietul de sarcini, Prestatorul are obligaţia de a constitui garanția de bună execuție conform prevederilor legale în vigoare.

Ofertanții trebuie să descrie în detaliu metodologia și procedurile după care vor derula activitățile de garanție, mentenanță și suport, inclusiv organizarea echipei de suport, definirea responsabilităților asociate pe nivele, fluxul de derulare al procesului, instrumentele utilizate pentru gestionarea incidentelor raportate.

4.9 Managementul proiectului

Îndeplinirea obiectivelor proiectului înseamnă atingerea standardelor de calitate propuse, în limitele de timp şi de buget stabilite.

Metodologia de management de proiect va pune la dispoziție o serie de componente şi procese care să ajute în procesul de planificare, monitorizare şi control şi care să asigure că proiectul va fi realizat la timp, cu bugetul alocat, la nivelul de calitate programat şi cu atingerea tuturor obiectivelor propuse.

Ofertantul va trebui să descrie în cadrul ofertei, detaliat, metodele folosite în cadrul contractului, principalele activități legate de organizarea contractului, experții cheie, programul și livrabilele. Descrierea trebuie să fie suficient de clară și concretă astfel încât să se poată identifica rezultatele pentru fiecare activitate.

Propunerea tehnică va conține cel puțin următoarele:

- Viziunea proprie asupra realizării contractului, din care să reiasă modul în care a înțeles contextul și scopul acestuia;
- Identificarea aspectelor principale legate de îndeplinirea obiectivelor contractului și a rezultatelor așteptate și o scurtă descriere a acestora;
- Metodologia de management de proiect utilizată de Ofertant. Este obligatorie folosirea unei metodologii recunoscute pe plan internațional. Ofertantul va descrie detaliat propria

metodologie de proiect pe care intenționează să o utilizeze pe parcursul implementării contractului, adaptată proiectului actual.

- Planul de proiect în format Gantt Chart și detalierea acestuia. Descrierea trebuie să evidențieze etapele, activitățile specifice fiecărei etape, resursele umane și materiale necesare îndeplinirii fiecărei etape, livrabilele așteptate de la fiecare etapă, modul în care acestea concură la atingerea obiectivelor.

Pentru realizarea cu succes a activității de management de proiect, Ofertantul trebuie să dețină și să utilizeze un instrument colaborativ de gestionare a activităților contractului, instrument care să permită Achizitorului o imagine la zi asupra activităților planificate, derulate, responsabililor de aceste activități, materialelor livrabile realizate sau aflate în curs de realizare. Accesul Achizitorului la instrument se va realiza web, prin Internet. Oferta va preciza instrumentul propus precum și capabilitățile acestuia raportat la nevoile evidențiate în caietul de sarcini.

Ofertantul va prezenta planul de management al contractului, împreună cu toate procedurile și formularele aferente acestora, prin intermediul căruia se va detalia modul de gestionare al întregului proiect. În acest sens, se va prezenta cel puțin: planificarea activităților contractului, cu indicarea tuturor fazelor/etapelor determinante de realizare a activităților (în ordinea și succesiunea logică, împreună cu modul de interacționare/alocare al resurselor în vederea prestării serviciilor ofertate și cu specificarea standardelor/regulamentelor relevante aplicate în scopul realizării diferitelor activități), inclusiv modalitatea de raportare lunara a progresului pentru activitățile din cadrul contractului (intervalele de raportare, conținutul informațional al raportării precum și circuitul de aprobare al rapoartelor de progres), modalitatea de comunicare între participanții la contract (echipa de proiect și reprezentanții Achizitorului).

Se va prezenta planul de proiect (format Gantt Chart) avut în vedere pentru prestarea serviciilor pe toată durata contractului. Planul de proiect prezentat trebuie să includă cel puțin:

- Toate activitățile necesare pentru implementarea cu succes a contractului, inclusiv dependențele dintre acestea, respectiv rezultatele acestora;
- Activitățile trebuie prezentate sub formă etapizată și să se înscrie în constrângerile de timp ale contractului;
- Fazele/subfazele de bază de realizare a activităților, evidențiindu-se reperele de referință (milestones);
- Distribuția resurselor pe activități care trebuie să conveargă la obiectivele contractului.

Ofertantul va trata modul de luare și ierarhizare a deciziilor 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).

Ofertantul va prezenta în cadrul propunerii tehnice modul în care se va gestiona rezolvarea problemelor care pot să apară pe parcursul contractului. Se va descrie procesul de management al problemelor şi formularele care vor fi utilizate pentru managementul problemelor, escaladarea şi rezolvarea acestora.

Ofertantul trebuie să prezinte în cadrul proiectului modalitatea (metodologia) prin care se va realiza comunicarea între participanţii la contract.

Ofertantul va prezenta în cadrul propunerii tehnice planul de acceptanţă care va fi utilizat în cadrul proiectului pentru recepţiile/acceptanţele parţiale şi recepţia/acceptanţa finală. Se va prezenta planul împărţit pe etape precum şi formularele aferente recepţiilor/acceptanţelor parţiale şi recepţiei/acceptanţei finale.

Ofertantul va prezenta în cadrul propunerii tehnice şi modalitatea de tratare a schimbărilor în cadrul contractului. Se va prezenta procedura de management al schimbărilor precum şi formularele care vor fi utilizate în cadrul acestui proces pe durata contractului.

Ofertantul va prezenta modalitatea de tratare a riscurilor în cadrul contractului. Se vor prezenta procedura de management a riscurilor, registrul inițial al riscurilor care conține cele mai importante riscuri identificate de acesta și măsurile propuse de remediere, precum și formularele care vor fi utilizate în cadrul acestui proces pe durata contractului. Se vor identifica riscuri din categorii diferite, care necesită abordări diferite, inclusiv pe baza experienței proprii din proiecte similare.

Ofertantul trebuie să prezinte în cadrul propunerii tehnice o descriere a procedurilor de asigurare și control al calității aplicabile proceselor pe care le derulează în activitatea curentă.

Ofertantul trebuie să descrie cum va realiza monitorizarea evoluției contractului și să descrie criteriile de calitate urmărite pe perioada desfășurării contractului.

Ofertantul trebuie să includă în propunerea tehnică și varianta preliminară a planului de calitate pentru derularea proiectului, care va conține cel puțin următoarele informații:

- Descrierea indicatorilor și criteriilor de calitate și a modalităților de măsurare prevăzute
- Descrierea fazelor, etapelor și activităților din cadrul proiectului(inclusiv metodologii, standarde, proceduri, formulare și instrumente utilizate);
- Organizarea proiectului și echipele implicate
- Descrierea pachetelor de lucru și a livrabilelor rezultate în urma prestării serviciilor;
- Descrierea criteriilor de acceptanta pentru livrabile, pachete de lucru, faze, etape etc..

4.10 Resurse umane

Implementarea adecvată și eficientă a activităților presupuse de ducerea la îndeplinire a obiectului contractului potrivit prevederilor prezentului proiect tehnic depinde în mod decisiv de implicarea din partea prestatorului pe parcursul perioadei de execuție a unei echipe corespunzătoare.

Listă experți necesari:

- Manager proiect - 1
- Analist de business -1
- Arhitect de sistem - 1
- Expert infrastructură hardware (1 sau mai mulți)
- Expert infrastructură software(1 sau mai mulți)
- Expert baze de date - 1
- Expert analiză și raportare- 1
- Expert SMED - 1
- Coordonator tehnic -1
- Expert testare - 1
- Expert securitate -1
- Coordonator suport tehnic -1
- Coordonator instruire -1

5 GRAFIC DE IMPLEMENTARE

Durata estimată de implementare a investiției este de maxim 24 luni de la intrarea in vigoare a contractului, care este estimată pentru **ianuarie 2024**.

Implementarea proiectului va include minim următoarele componente:

- Livrare, instalare și configurare infrastructura hardware și software necesară realizării sistemului și asigurării unui nivel înalt de performanță și disponibilitate
- Servicii de analiză, dezvoltare, implementare, testare a sistemului SIAMC, asigurare a interoperabilității cu alte sisteme și de migrare a datelor istorice din sistemele software aflate în producție la Beneficiar
- Serviciile de testare trebuie să includă și teste de performanță pentru a demonstra capabilitățile sistemului de susține numărul de utilizatori (concurenți / totali), teste de securitate a sistemului și de asigurare a înaltei disponibilități și interoperabilității cu aplicațiile terțe identificate.
- Servicii de asistență tehnică la pornire de minim 6 luni incluse în durata de implementare a proiectului
- Servicii de instruire în vederea utilizării și administrării sistemului, cu recomandarea ca acestea să aibă loc înainte de testarea de acceptanță a sistemului

5.1.1.1 Grafic estimat de implementare

Activitate	**Constrângeri de implementare/ Termen finalizare activitate**
Analiză și proiectare sistem informatic	Luna 6 a contractului de prestări servicii
Dezvoltare sistem informatic	Luna 14 a contractului de prestări servicii
Livrare, instalare și configurare infrastructură hardware, de comunicații și software de bază	Luna 6 a contractului de prestări servicii
Testare sistem informatic	Luna 16 a contractului de prestări servicii
Punere în producție sistem informatic	Luna 16 a contractului de prestări servicii
Instruire utilizatori și administratori	Luna 18 a contractului de prestări servicii
Asistență la pornire	Luna 24 a contractului de prestări servicii (Lunile 18-24 ale contractului de prestări servicii)