PROIECT TEHNIC

Denumire Proiect: REFORMA EVIDENȚEI ȘI MONITORIZĂRII RELAȚIILOR DE 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: 121/DE

Dată contract: 01.02.2023

Proiectant: GO-TECH CONSULTING SRL

BALSEANU ALEXANDRA-DANIELA

Digitally signed by BALSEANU ALEXANDRA-DANIELA
Date: 2023.04.25 17:28:23 +03'00'

Controlul Distribuţiei

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

Istoricul Modificărilor

Versiune	Data	Comentarii
1.0	07.03.2023	Versiune iniţială
2.0	21.03.2023	Versiune actualizată conform observații Inspecția Muncii și Task Force MCID

Cuprins

1 DATE GENERALE

Inspecția Muncii este 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, prin care asigură exercitarea controlului în domeniile relaţiilor de muncă, securităţii şi sănătăţii în muncă şi supravegherii pieţei.

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.

Inspecția Muncii și inspectoratele teritoriale de muncă sunt înființate și funcționează în baza:

- Legii nr. 108/1999 pentru înființarea și organizarea Inspecției Muncii, republicată, cu modificările ulterioare;
- HotărâriiGuvernului 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 Inspectoratele teritoriale de muncă (ITM) în fiecare județ și în Municipiul București..

1.1 Reforma evidenței și monitorizării relațiilor de muncă

În domeniul relațiilor de muncă, Inspecția Muncii are ca atribuție specifică, asigurarea la nivel național a evidenței muncii prestate în baza contractelor individuale de muncă, prin registrul general de evidență a salariaților.

Potrivit dispozițiilor art. 34 alin. 1 din Legea nr. 53/2003, republicată, cu modificările și completările ulterioare, fiecare angajator are obligaţia de a înfiinţa un registru general de evidenţă a salariaţilor.

Temeiul legal al înființării registrului general de evidență online este Legea nr. 144 din 20 mai 2022, pentru modificarea si completarea art. 34 din Legea nr. 53/2003 - Codul muncii.

Potrivit dispozițiilor Legii nr. 144/2022:

-Registrul general de evidenţă a salariaţilor se completează şi se transmite inspectoratului teritorial de muncă în ordinea angajării şi cuprinde elementele de identificare ale tuturor salariaţilor, data angajării, funcţia/ocupaţia conform specificaţiei Clasificării ocupaţiilor din România sau altor acte normative, nivelul şi specialitatea studiilor absolvite, tipul contractului individual de muncă, salariul, sporurile şi cuantumul acestora, perioada şi cauzele de suspendare a contractului individual de muncă, perioada detaşării şi data încetării contractului individual de muncă.

−Registrul general de evidenţă a salariaţilor este accesibil online pentru salariaţi/foşti salariaţi, în privinţa datelor care îi privesc. Dreptul de acces se limitează la vizualizarea, descărcarea şi tipărirea acestor date, precum şi la generarea online şi descărcarea unui extras din registru.

-Vechimea în muncă şi/sau în specialitate poate fi dovedită şi cu extrasul online.

Prin Hotărârea Guvernului nr. 1164/2022 a fost aprobată Procedura de acces online al salariaţilor sau foştilor salariaţi la datele din registrul general de evidenţă a salariaţilor, a modalităţii de generare şi descărcare a extrasului, precum şi a condiţiilor în care prin extras se poate dovedi vechimea în muncă şi/sau specialitate.

Sistemul informatic aferent registrului, denumit în continuare REGES/REVISAL, a fost pus în funcțiune în anul 2006, fiind implementat în baza cerințelor Hotărârii Guvernului nr. 161/2006, conform căreia angajatorii din Romania au avut obligația de a transmite informații despre angajator, salariați și contractele individuale de muncă ale acestora.

În data de 15 august 2011 s-a pus în producție un sistem informatic REGES/REVISAL complet nou, bazat pe prevederile Hotărârii Guvernului nr. 500/2011, care a abrogat Hotărârea Guvernului nr. 161/2006. În data de 19 decembrie 2017 a intrat în vigoare Hotărârea Guvernului nr. 905/2017 privind registrul general de evidență a salariaților, când a fost abrogată Hotărârea Guvernului nr. 500/2011.

Metodologia de înființare a registrului general de evidență a salariaților, de completare și transmitere în registru a elementelor raportului de muncă de către angajatori, pentru acest sistem informatic, este reglementată de Hotărârea Guvernului nr. 905/2017 privind registrul general de evidență a salariaților și de Ordinul Ministerului Muncii, Familiei și Protecției Sociale nr. 1918/2011 pentru aprobarea procedurii si actelor pe care angajatorii sunt obligati sa le prezinte la inspectoratul teritorial de munca pentru obtinerea parolei, precum si a procedurii privind transmiterea registrului general de evidenta a salariatilor in format electronic.

Gestionarea registrului are o importanță majoră în desfășurarea activității de control a Inspecției Muncii și contribuie totodată la elaborarea politicilor publice din domeniul pieței muncii prin informațiile pe care le pune la dispoziția autorităților și instituțiilor publice din domeniu.

Actualul sistem informatic REGES/REVISAL este depășit din punct de vedere tehnologic și al dimensiunii în raport cu datele ce trebuie colectate și stocate, prezintă funcționalități limitate în ceea ce privește gestionarea evidenței angajaților și contribuie la creșterea poverii administrative pentru mediul de afaceri. Creșterea de la an la an a cantității de date transmise, prelucrate și stocate prin intermediul registrului de evidență a salariaților devine astfel un impediment în gestionarea eficientă a relației ITM/angajator/salariat.

În acest context, în vederea implementării Reformei evidenței și monitorizării relațiilor de 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 digital.

Obiectivul general al proiectului îl reprezintă reforma activităților de evidență și monitorizare a relațiilor de muncă și implementarea noului sistem informatic aferent registrului general de evidență a salariaților, care să permită creșterea gradului de digitalizare a instituției și să ofere servicii digitale de înaltă calitate cetățenilor, salariaților și angajatorilor.

Propunerea consultantului, ca urmare a analizei realizate, este de construire a unui sistem informatic nou, complet on-line și centralizat, cu o securitate informatică sporită, bazat pe tehnologii moderne și care să permită interoperabilitatea tehnică și organizațională.

Arhitectura sistemului informatic proiectat va răspunde nevoilor beneficiarilor acestuia, atingând toate obiectivele propuse pentru o bună derulare a activităților prezente și viitoare ale Inspecției Muncii, în ceea ce privește relațiile de muncă.

1.2 Legislație specifică relațiilor de muncă

- ✓ 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
  - Ordinul nr. 2171/2022 pentru aprobarea modelului-cadru al contractului individual de muncă
  - Hătărârea Guvernului nr. 1447/2022 pentru stabilirea salariului de bază minim brut pe țară garantat în plată (act normativ care se modifică periodic)
  - Ordonanța de Urgență a Guvernului nr. 44/2008 privind desfăşurarea activităţilor economice de către persoanele fizice autorizate, întreprinderile individuale şi întreprinderile familiale, cu modificările și completările ulterioare
  - Hotărârea Guvernului nr. 38/2008 privind organizarea timpului de munca al persoanelor care efectueaza activitati mobile de transport rutier, cu modificările și completările ulterioare
  - Ordonanța Guvernului nr. 37/2007 privind stabilirea cadrului de aplicare a regulilor privind perioadele de conducere, pauzele şi perioadele de odihnă ale conducătorilor auto şi utilizarea aparatelor de înregistrare a activităţii acestora, cu modificările şi 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
- ✓ Întocmirea, completarea şi transmiterea registrului general de evidenţă a salariaţilor
  - Hotărârea Guvernului nr. 905/2017 privind registrul general de evidență a salariaților
  - Ordinul Ministerului Muncii, Familiei și Protecției Sociale nr. 1.918/2011 pentru aprobarea procedurii și actelor pe care angajatorii sunt obligați să le prezinte la inspectoratul teritorial de muncă pentru obținerea parolei, precum și a procedurii privind transmiterea registrului general de evidență a salariaților în format electronic
  - Hotărârea Guvernului 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
  - Legii nr. 242/2022 privind schimbul de date între sisteme informatice și crearea Platformei naționale de interoperabilitate
  - Ordonanța de Urgență a Guvernului nr. 89/2022 privind înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizate de autoritățile și instituțiile publice
  - Hotărârea Guvernului nr. 112 / 2023 privind aprobarea Ghidului de guvernanță a platformei de cloud guvernamental
- ✓ Încadrarea în muncă, în România, a cetăţenilor străini

- Ordonața Guvernului 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
- Hotărârea Guvernului 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
- Hotărârea Guvernului 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
- Hotărârea Guvernului 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
- Ordinul comun al Ministerului Muncii, Familiei, Protecției Sociale și Persoanelor Vârstnice și al Ministerului Finanțelor Publice nr. 831/600/2015 pentru aprobarea normelor metodologice de aplicare a Legii nr. 52/2011 privind exercitarea unor activităţi cu caracter ocazional desfăşurate de zilieri
- Ordinul Ministerului Muncii și Protecției Sociale nr. 1140/2020 pentru aprobarea Metodologiei de intocmire si transmitere a Registrului electronic de evidenta a zilierilor, precum si inregistrarile care se efectueaza in acesta

✓ 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
- Hotărârea Guvernului 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
- Ordonanța de Urgență a Guvernului nr. 96/2003 privind protecţia maternităţii la locurile de muncă, cu modificările și completările ulterioare
- Hotărârea Guvernului 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

✓ 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
- Ordonanța Guvernului nr. 2/2001 privind regimul juridic al contravenţiilor, cu modificările şi completările ulterioare

2 INFORMAŢII PRIVIND PROIECTUL

2.1 Situaţia actuală

Din punct de vedere organizatoric, direcțiile, compartimentele și serviciile implicate direct în evidența și monitorizarea relațiilor de muncă sunt :

- La nivelul Inspecției Muncii: Direcția Control Muncă Nedeclarată, Contracte Colective de mMuncă și Monitorizare Relații de Muncă, Direcția Control Relații de Muncă, împreună cu compartimentele și serviciile din subordineși Serviciul Informatică pentru buna funcționare din punct de vedere IT a aplicațiilor și sistemelor implicate
- La nivelul Inspectoratului Teritorial de Muncă București: Serviciul Control Muncă Nedeclarată, Serviciul Monitorizare Relații de Muncă, Contracte Colective de Muncă , Serviciul Control Relații de Muncă și Compartimentul Informatică pentru buna funcționare din punct de vedere IT a aplicațiilor și sistemelor implicate
- La nivelul Inspectoratelor Teritoriale de Muncă: Compartimentele Control Relații de Muncă, Compartimentele Contracte Colective de Muncă și Monitorizare Relații de Muncă, Compartimentele Control Muncă Nedeclarată și Compartimentele Informatică pentru buna funcționare din punct de vedere IT a aplicațiilor și sistemelor implicate

Sistemul informatic aferent registrului, denumit în continuare REGES/REVISAL, a fost pus în funcțiune în anul 2006, fiind implementat în baza cerințelor Hotărârii Guvernului nr. 161/2006, conform căreia angajatorii din Romania au avut obligația de a transmite informații despre angajator, salariați și contractele individuale de muncă ale acestora.

În data de 15 august 2011 s-a pus în producție un sistem informatic REGES/REVISAL complet nou, bazat pe prevederile Hotărârii Guvernului nr. 500/2011, care a abrogat Hotărârea Guvernului nr. 161/2006. În data de 19 decembrie 2017 a intrat în vigoare Hotărârea Guvernului nr. 905/2017 privind registrul general de evidență a salariaților, când a fost abrogată Hotărârea Guvernului nr. 500/2011.

Metodologia de înființare a registrului general de evidență a salariaților, de completare și transmitere în registru a elementelor raportului de muncă de către angajatori, pentru acest sistem informatic, este reglementată de Hotărârea Guvernului nr. 905/2017 privind registrul general de evidență a salariaților și de Ordinul Ministerului Muncii, Familiei și Protecției Sociale nr. 1918/2011 pentru aprobarea procedurii si actelor pe care angajatorii sunt obligati sa le prezinte la inspectoratul teritorial de munca pentru obtinerea parolei, precum si a procedurii privind transmiterea registrului general de evidenta a salariatilor in format electronic.

Platforma tehnică pusă la dispoziție pentru îndeplinirea acestei obligații este alcătuită din următoarele subsisteme:

- Aplicația Revisal, destinată angajatorilor pentru completarea registrului, actualizarea informațiilor angajatorilor, salariaților și contractelor individuale de muncă aferente. La aceasta se adaugă specificaţiile tehnice de completare a registrului care se adresează angajatorilor care utilizează aplicaţii proprii de gestiune a salariaţilor, altele decât aplicația Revisal.
- Sistemul informatic REGES, destinat Inspecție Muncii și inspectoratelor teritoriale de muncă, care cuprinde sistemul de preluare și raportare la nivel județean - REGES.ITM, și sistemul preluare la nivel central REGES.IM și gestionare a bazei de date aferentă registrului, bază de date aflată în proprietate Inspecție Muncii.

Încă din anul 2006 s-au efectuat o serie de actualizări ale sistemului REGES/REVISAL, iar în data de 15 august 2011 s-a pus în producție un sistem informatic REGES/REVISAL complet nou, bazat pe prevederile HG nr.

500/2011, care a abrogat HG nr. 161/2006. La momentul respectiv, au fost migrate doar contractele de muncă active, iar contractele de muncă încheiate înaintea migrării la sistemul curent au rămas doar în sistemul vechi.

Elementele cuprinse în registru conform Hotărârii Guvernului nr. 905/2017 sunt următoarele:

- datele de identificare ale angajatorului persoană fizică sau juridică de drept privat, respectiv instituţie/autoritate publică/altă entitate juridică care angajează personal în baza unui contract individual de muncă;
- datele de identificare ale salariaților: numele, prenumele, codul numeric personal, cetățenia și țara de proveniență;
- data încheierii contractului individual de muncă şi data începerii activităţii;
- funcţia/ocupaţia conform specificaţiei Clasificării Ocupaţiilor din România (COR) sau altor acte normative;
- tipul contractului individual de muncă;
- durata contractului individual de muncă, respectiv nedeterminată/ determinată;
- durata timpului de muncă și repartizarea acestuia în cazul contractelor individuale de muncă cu timp parţial;
- salariul de bază lunar brut, indemnizaţiile, sporurile, precum şi alte adaosuri așa cum sunt prevăzute în contractual individual de muncă sau, după caz, în contractual colectiv de muncă;
- datele de identificare ale utilizatorului, în cazul contractelor de muncă temporară;
- data transferului astfel cum este prevăzut la art. 90 alin. (9) din Legea nr. 188/1999 privind Statutul funcţionarilor publici, republicată, cu modificările şi completările ulterioare, precum şi datele de identificare ale angajatorului la care se face transferul;
- data preluării prin transfer, astfel cum este prevăzut la art. 90 alin. (9) din Legea nr. 188/1999, republicată, cu modificările şi completările ulterioare, şi art. 32 din Legea-cadru nr. 153/2017 privind salarizarea personalului plătit din fonduri publice, cu modificările şi completările ulterioare, precum şi datele de identificare ale angajatorului de la care se face transferul;
- data la care începe şi data la care încetează detaşarea, precum şi datele de identificare ale angajatorului la care se face detaşarea;
- data la care începe și data la care încetează detașarea transnațională, definită de Legea nr. 16/2017 privind detașarea salariaților în cadrul prestării de servicii transnaționale, statul în care urmeaza să se realizeze detașarea transnațională, denumirea beneficiarului/utilizatorului la care urmează să presteze activitatea salariatul detașat, precum și natura acestei activități;
- data la care începe și data la care încetează detașarea pe teritoriul unui stat care nu este membru al Uniunii Europene sau al Spatiului Economic European, statul în care urmează să se realizeze detașarea, denumirea beneficiarului/utilizatorului la care urmează să presteze activitatea salariatul detașat, precum și natura acestei activități;
- perioada, cauzele de suspendare și data încetarii suspendării contractului individual de muncă, cu excepția cazurilor de suspendare în baza certificatelor medicale;
- data şi temeiul legal al încetării contractului individual de muncă.

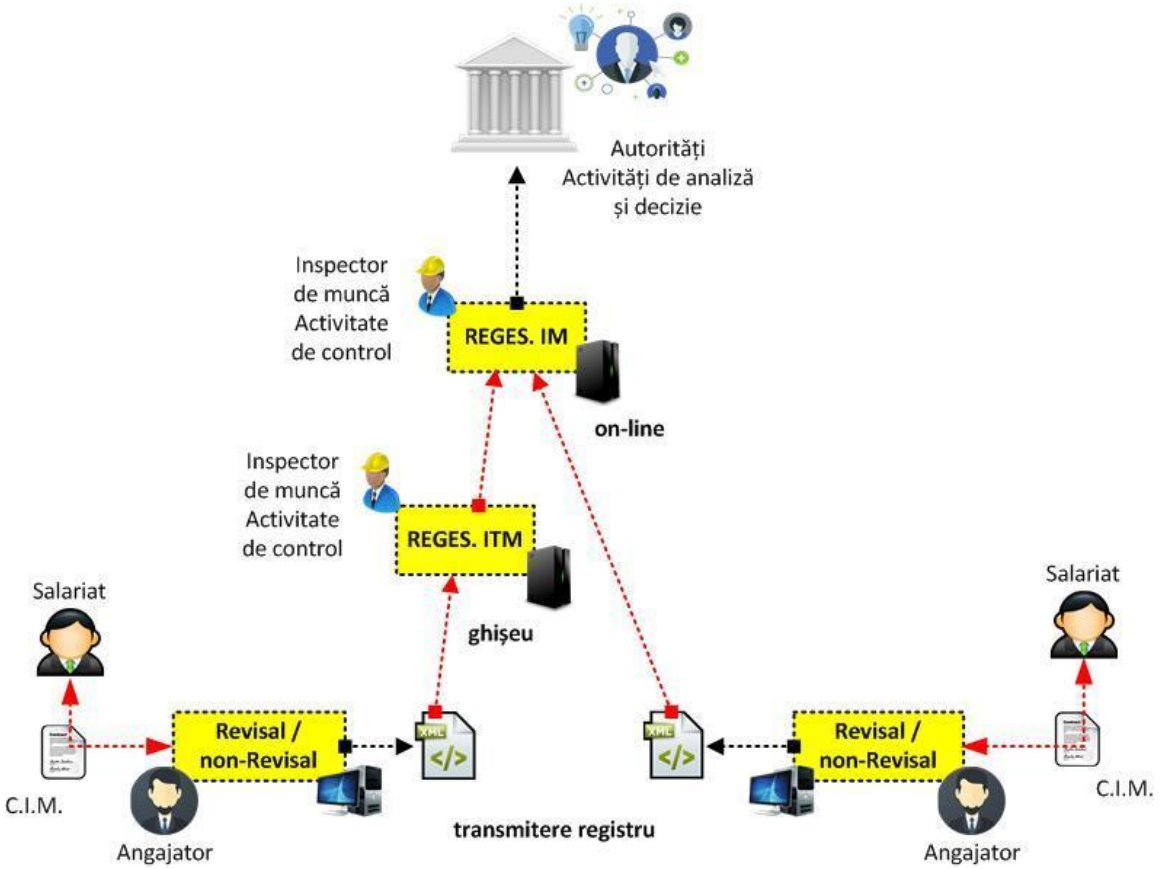


Figura 1 - Diagrama organizării actuale a Inspecției Muncii privind registrul salariaților

Actualul sistem informatic REGES/REVISAL este depășit din punct de vedere tehnologic și al dimensiunii în raport cu datele ce trebuie colectate și stocate, prezintă funcționalități limitate în ceea ce privește gestionarea evidenței angajaților și contribuie la creșterea poverii administrative pentru mediul de afaceri. Creșterea de la an la an a cantității de date transmise, prelucrate și stocate prin intermediul registrului de evidență a salariaților devine astfel un impediment în gestionarea eficientă a relației ITM/angajator/salariat.

Prin intermediul sistemului informatic REGES, Inspecția Muncii asigură evidența la nivel național a contractelor individuale de muncă încheiate și înregistrate de către angajatori. Baza de date REGES trebuie să cuprindă doar datele transmise de către angajatori, referitoare la contractele individuale de muncă încheiate.

2.2 Protocoale de colaborare încheiate de Inspecția Muncii cu autoritățile/instituțiile publice prin care se asigură accesul la informațiile din registrul general de evidență a salariaților

În conformitate cu prevederile art. 11 alin. (1) din Hotărârea Guvernului nr. 905/2017 privind registrul general de evidență a salariaților, Inspecția Muncii asigură accesul la informațiile din registru, **pe baza unor aplicații de interogare specifice sau prin punerea la dispoziție a unor informații din registru**, cu respectarea măsurilor de protecție a datelor cu caracter personal, numai dacă în cuprinsul actului normativ de organizare și funcționare a acestora se prevede că acestea au dreptul de a primi aceste informații în vederea realizării atribuțiilor lor. Inspecția Muncii pune la dispoziție, în condițiile legii, datele din registrul general de evidență a salariaților către instanțele de judecată, organele de cercetare penală, autoritățile fiscale, precum și oricăror autorități/instituții publice solicitante față de care transmiterea acestor date este cerută de lege. În baza acestor prevederi legale, Inspecția Muncii a încheiat protocoale de colaborare prin care asigură accesul la informațiile din registrul general de evidență a salariaților următoarelor autorități/instituții publice:

- Autoritatea Naţională pentru Persoanele cu Dizabilităţi;
- Agenția Națională pentru Plăți și Inspecție Socială;
- Agenția Națională de Administrare Fiscală;
- Agenția Națională pentru Ocuparea Forței de Muncă;
- Agenția pentru Finanțarea Investițiilor Rurale;
- Agenția Națională a Funcționarilor Publici;
- Casa Națională de Pensii Publice;
- Curtea de Conturi a României – Autoritatea de Audit;
- Departamentul pentru Lupta Antifraudă;
- Învățământului Superior, a Cercetării, Dezvoltării și Inovării;
- Inspectoratul de Stat pentru Controlul Transportului Rutier – I.S.C.T.R;
- Inspectoratul General al Poliției Române;
- Ministerul Investițiilor și Proiectelor Europene – Direcția Generală
- Ministerul Educației – Unitatea Executivă pentru Finanțarea
- Ministerul Afacerilor Interne – Inspectoratul General pentru Imigrări;
- Ministerul Educației – Direcția OIPOCU;
- Oficiul Naţional al Registrului Comerţului
- Proiecte Europene Competitivitate;
- Institutul Național de Statistică;
- Agenția Națională de Integritate;
- Autoritatea pentru Digitalizarea României etc.

2.3 Rezultatele analizei

Conform situației pe anul 2022 privind activitatea Compartimentelor Contracte Colective de Muncă și Monitorizare Relații de Muncă din cadrul inspectoratelor teritoriale de muncă, centralizate la nivelul Inspecției Muncii:

- Au fost eliberate 9784 de certificate/adeverințe în baza documentelor existente în arhiva inspectoratelor teritoriale de muncă
- Au fost primate 977.320 de solicitări de eliberare certificate/rapoarte cu informații extrase din baza de date gestionată de Inspecția Muncii
- Au fost preluate la sediul ITM 151.240 de registre electronice ale salariaților
- Au fost eliberate 116.680 de parole pentru transmiterea online a registrului electronic al salariaților
- Au fost eliberate 8520 de carnete de muncă

Conform situației controalelor efectuate în vederea identificării și combaterii muncii nedeclarate, în anul 2022:

- Au fost efectuate 65.265 de controale (efectuate de CCRM+CCMN)
- Au fost sancționați 2870 de angajatoripentru muncă nedeclarată

- Au fost depistate 7648 de persoane care prestează activitate pentru munca nedeclarată
- Au fost aplicate amenzi în valoare de 8.412.000

Cerințe de performanță

Pe un eșantion de peste 30 de zile, exceptând perioadele de weekend, se observă o medie zilnică de 30.000 de depuneri totale din care 1.000 la ghișeele ITM iar 22.000 on-line în sistemul informatic actual REGES/REVISAL. Vârfurile de depunere sunt în apropierea sfârșitului de lună sau în prima zi lucrătoare din luna, și atinge in medie peste 31.000 depuneri iar în cazuri excepționale cum este începutul de an sau ca urmare a schimbărilor legislative, poate depăși 90.000 de depuneri zilnic.

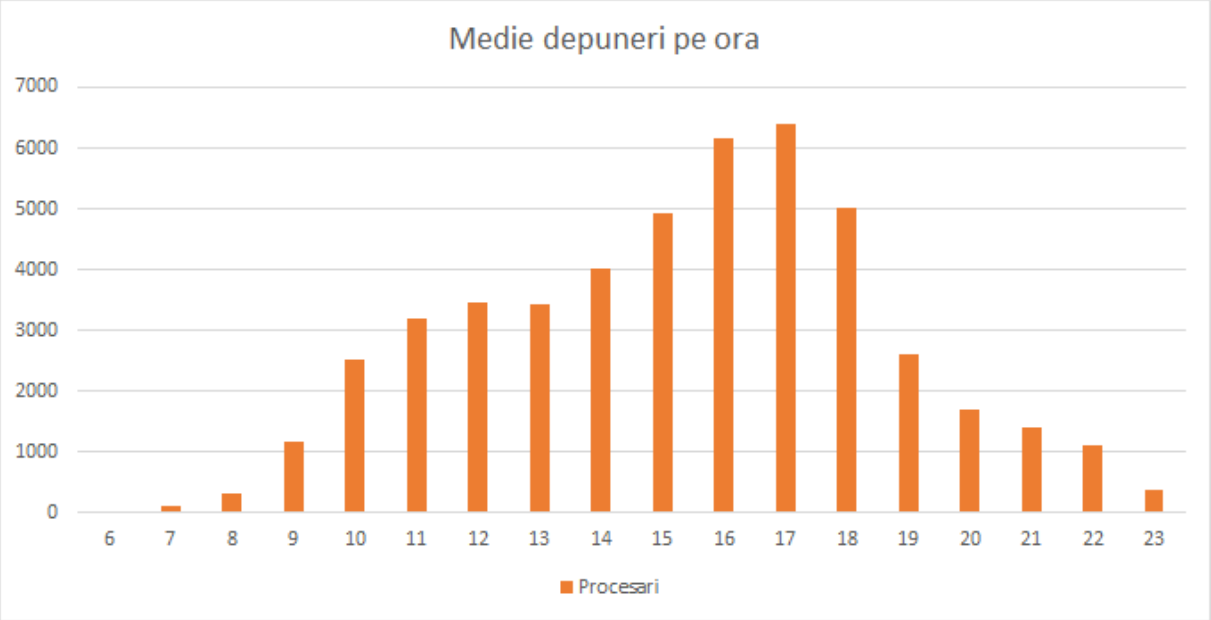


Figura 2 - Media încărcărilor pe ora în sistemul informatic actual REGES/REVISAL

Pentru **dimensionarea performantelor necesare mediului de producție al sistemului** trebuie luate în considerare următoarele valori minimale:

a) Numărul estimat de utilizatori concurenți (la nivel de CUI/CIF/CNP) este de 7.000 în medie iar în momente de vârf poate ajunge la 23.000;

b) Numărul de utilizatori concurenți din IM și ITM-uri este de aproximativ 500.

c) Pentru consultarea datelor de către utilizatorii din alte instituții publice, numărul estimat de utilizatori concurenţi este de 80.

Ca urmare a analizei asupra activităților în domeniul evidenței și monitorizării relațiilor de muncă, s-au constatat următoarele puncte slabe:

- Infrastructură hardware și software depășită tehnologic, fiind schimbată la nivelul anului 2011
- Existența a 2 sisteme informatice, împreună cu infrastructura necesară hardware și aplicativă, din care unul pus în producție în anul 2006
    - Infrastructura hardware și software care susține actualul sistem este găzduită atât la nivel central (la STS), cât și la nivelul fiecărui ITM din țară (server care găzduiește sistemul de

preluare, procesare și raportare la nivel județean – REGES.ITM care funcționează în infrastructura de comunicații asigurată și securizată de STS), fiind necesară mentenanță la nivelul tuturor celor 43 de puncte.

- Numărul de conturi la nivelul celor 43 de entități (Inspecția Muncii plus cele 42 de ITM-uri) este în medie de 1700 de utilizatori pe fiecare din cele 2 sisteme.

- Necesitatea instalării locale a unui clientul offline Revisal în vederea operării registrului de evidență a salariaților la nivelul companiei
- Necesitatea de deplasare la sediul ITM pentru a primi user și parolă în vederea operării online a sistemului
- Necesitatea de deplasare la sediile ITM pentru solicitarea unor informații de bază, respectiv pentru recuperarea registrului propriu la nivel de companie
- Existența unui singur utilizator la nivelul unei companii, care este folosit în practică de mai multe persoane, nepermițandu-se astfel trasabilitatea operațiunilor la nivelul companiei
- În cazul pierderii informațiilor existente în baza de date locală, ITM furnizează registrul în format hârtie pentru companiile cu mai puțin de 50 de angajați, aceste informații trebuind apoi reintroduse manual
- Obținerea de rapoarte în mod manual, prin interogări direct la nivelul bazei de date

Având în vedere cele de mai sus, este necesară reforma evidenței și monitorizării relațiilor de muncă prin implementarea unui Registru General de Evidență a Salariaților **în variantă on-line** (REGES-ONLINE), ca **sursă unică de informație** originală în format electronic, **la nivel național,** care să permită accesul **angajatorilor, salariaților și autorităților** într-un sistem informatic centralizat, contribuind astfel la **îmbunătățirea serviciilor publice pentru cetățeni și mediul de afaceri precum și către terțe autorități și instituții publice.**

Astfel, REGES-ONLINE va permite:

- Întocmirea registrului general de evidență a salariaților;
- Efectuarea înregistrărilor prevăzute de lege;

Temeiul legal al înființării registrului general de evidență online este Legea nr. 144 din 20 mai 2022, pentru modificarea si completarea art. 34 din Legea nr. 53/2003 - Codul muncii.

Potrivit dispozițiilor Legii nr. 144/2022:

Registrul general de evidenţă a salariaţilor se completează şi se transmite inspectoratului teritorial de muncă în ordinea angajării şi cuprinde elementele de identificare ale tuturor salariaţilor, data angajării, funcţia/ocupaţia conform specificaţiei Clasificării ocupaţiilor din România sau altor acte normative, nivelul şi specialitatea studiilor absolvite, tipul contractului individual de muncă, salariul, sporurile şi cuantumul acestora, perioada şi cauzele de suspendare a contractului individual de muncă, perioada detaşării şi data încetării contractului individual de muncă.

În sistemul actual de registru, astfel cum a fost prezentat, angajatorii au obligația să completeze următoarele date:-datele de identificare ale angajatorului persoană fizică sau juridică de drept privat, respectiv instituţie/autoritate publică/altă entitate juridică care angajează personal în baza unui contract individual de muncă, cum ar fi: denumire, cod unic de identificare - CUI, codul de identificare fiscală - CIF, sediul social şi numele şi prenumele reprezentantului legal - pentru persoanele juridice, respectiv: numele, prenumele, codul numeric personal - CNP, domiciliul - pentru persoanele fizice;

-datele de identificare ale salariaţilor, cum ar fi: numele, prenumele, codul numeric personal - CNP, cetăţenia şi ţara de proveniență - Uniunea Europeană - UE, non-UE, Spaţiul Economic European - SEE;
-data încheierii contractului individual de muncă şi data începerii activităţii;

-funcţia/ocupaţia conform specificaţiei Clasificării Ocupaţiilor din România (COR) sau altor acte normative;
-tipul contractului individual de muncă;
-durata contractului individual de muncă, respectiv nedeterminată/determinată;
-durata timpului de muncă şi repartizarea acestuia, în cazul contractelor individuale de muncă cu timp parţial;
salariul de bază lunar brut, indemnizaţiile, sporurile, precum şi alte adaosuri, astfel cum sunt prevăzute în contractul individual de muncă sau, după caz, în contractul colectiv de muncă;
- datele de identificare ale utilizatorului, în cazul contractelor de muncă temporară;
- data transferului astfel cum este prevăzut la art. 90 alin. (9) din Legea nr. 188/1999 privind Statutul funcţionarilor publici, republicată, cu modificările şi completările ulterioare, precum şi datele de identificare ale angajatorului la care se face transferul;
-data preluării prin transfer, astfel cum este prevăzut la art. 90 alin. (9) din Legea nr. 188/1999, republicată, cu modificările şi completările ulterioare, şi art. 32 din Legea-cadru nr. 153/2017 privind salarizarea personalului plătit din fonduri publice, cu modificările şi completările ulterioare, precum şi datele de identificare ale angajatorului de la care se face transferul;
-data la care începe şi data la care încetează detaşarea, precum şi datele de identificare ale angajatorului la care se face detaşarea;
-data la care începe şi data la care încetează detaşarea transnaţională, definită de Legea nr. 16/2017 privind detaşarea salariaţilor în cadrul prestării de servicii transnaţionale, statul în care urmează să se realizeze detaşarea transnaţională, denumirea beneficiarului/utilizatorului la care urmează să presteze activitatea salariatul detaşat, precum şi natura acestei activităţi;
-data la care începe şi data la care încetează detaşarea pe teritoriul unui stat care nu este membru al Uniunii Europene sau al Spaţiului Economic European, statul în care urmează să se realizeze detaşarea, denumirea beneficiarului/utilizatorului la care urmează să presteze activitatea salariatul detaşat, precum şi natura acestei activităţi;
-perioada, cauzele de suspendare şi data încetării suspendării contractului individual de muncă, cu excepţia cazurilor de suspendare în baza certificatelor medicale;
data şi temeiul legal al încetării contractului individual de muncă.

- Accesul persoanelor fizice, salariaților sau al foștilor salariațila datele din REGES ONLINE, cu asigurarea măsurilor de protecție a datelor cu caracter personal;
- Creșterea accesului la serviciile electronice moderne prin îmbunătățirea interacțiunii on-line cu administrația publică;
- Asigurarea accesului autorităților, instituțiilor publice și a salariaților la datele din REGES-ONLINE, pe baza unor aplicații de interogare specifice, cu asigurarea măsurilor de protecție a datelor cu caracter personal;
- Creșterea securității sistemului informatic REGES și a accesului la datele conținute;
- Integrarea cu instituțiile partenere și care au competență în domeniul politicilor salariale din România a datelor relevante aparținând tuturor categoriilor de salariați;
- Generarea automată de rapoarte necesare activității de control.

Cu respectarea legislației, noul sistem REGES-ONLINE va permite simplicarea, debirocratizarea și digitalizarea, precum și folosirea eficientă a resurselor.

Un avantaj major al implementării complet on-line este **îmbunătățirea timpului de actualizare** a modificărilor sistemului, deoarece toți utilizatorii vor beneficia întotdeauna de ultima versiune a aplicației într-un mod unitar și mult mai rapid. Utilizatorii vor putea accesa sistemul REGES din orice locație prin intermediul unor mecanisme web sau mobile fără a mai fi necesară instalarea unei aplicații (Revisal). Totodată inspectorii de muncă și autoritățile vor avea acces imediat, în timp real, la datele introduse de angajatori.

Asigurarea securității informatice este un subiect din ce în ce mai important și având în vedere sensibilitatea datelor gestionate în registru, este nevoie de o sporire a securității sistemului astfel încât să se asigure un grad ridicat de protecție și încredere.
Îmbunătățirea **securității** sistemului informatic se va face în mai multe direcții:

- Se vor folosi metode moderne de control de securitate la nivel software și de arhitectură, se vor achiziționa echipamente specializate de asigurare a securității aplicațiilor web și bazelor de date și totodată se vor implementa controale avansate de securitate.
- Pentru angajatori se va introduce autentificarea cu 2 factori, folosind numele și parola actuale dar și certificate digitale calificate, mai ales în contextul în care că majoritatea angajatorilor din România utilizează deja certificate digitale calificate ca urmare a obligativității depunerii declarației 112 la ANAF.
- Pentru utilizatorii Inspecției Muncii și inspectoratelor teritoriale de muncă se va introduce autentificarea folosind certificate digitale calificate astfel încât toți utilizatorii să acceseze sistemul în mod securizat corespunzător.
- Pentru angajații care vor accesa informații despre contractele individuale de muncă se va implementa autentificarea folosind doi factori de autentificare și/sau identitatea digitală.

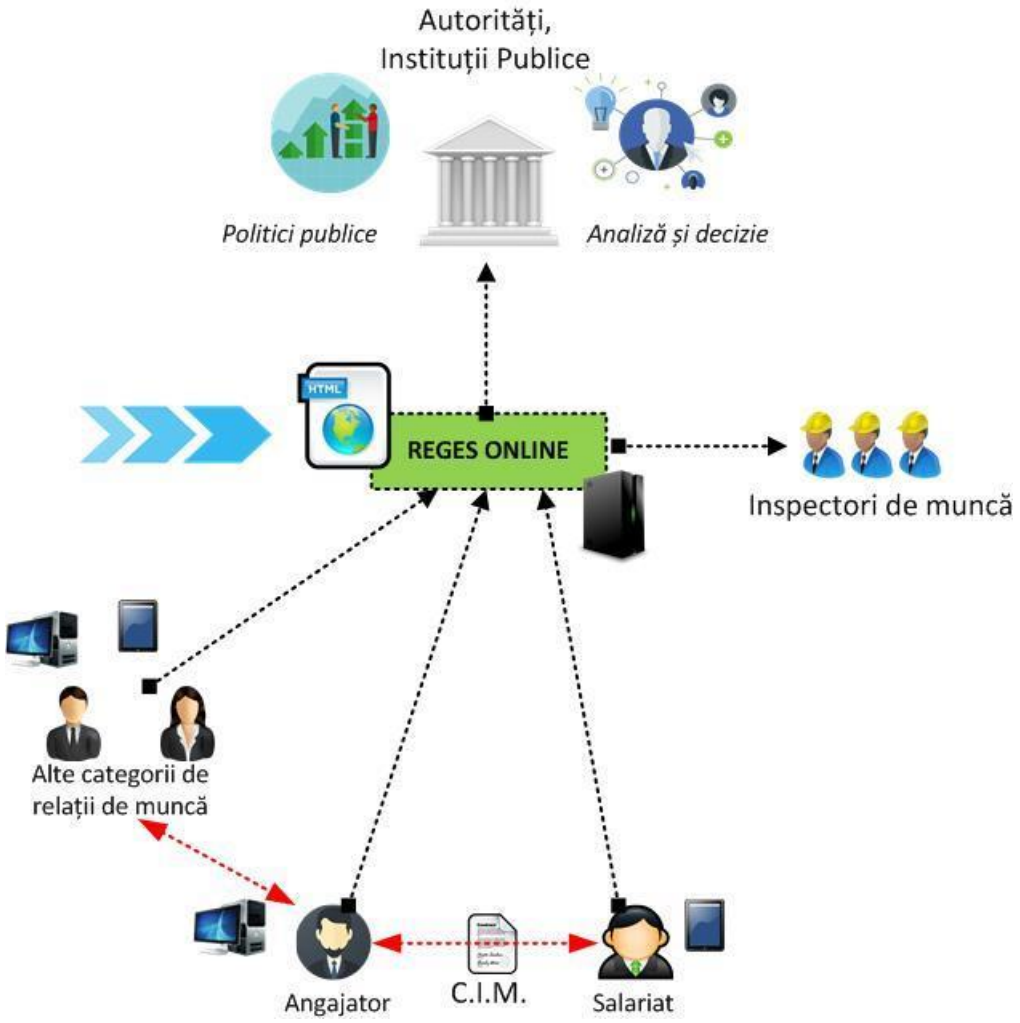


Figura 3 - Diagrama REGES-ONLINE

Asigurarea interoperabilității sistemului este foarte importantă și presupune implementarea unui nivel de integrare 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.

Prin integrarea cu alte autorități și instituții publice, precum ONRC, Direcția Generală Pentru Evidența Persoanelor, Ministerul Educației, ANAF, IGI, CNPP, ANOFM, INS, etc. se va obține imaginea completă în ceea ce privește persoanele care obțin venituri salariale, dar și îmbunătățirea calitativă a politicilor salariale din România elaborate de către Ministerul Muncii și Solidarității Sociale.

Astfel, este necesară pe de-o parte **interoperabilitatea tehnică** care va permite accesul autorităților și instituțiilor publice la datele din registru la nivel de interfață de programare a aplicațiilor (API - Application Programming Interface) și pe de altă parte **interoperabilitatea organizațională** prin alinierea proceselor operaționale existente sau definirea și aplicarea unor procese operaționale noi. 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.

În cadrul sistemului nou implementat se vor defini schemele de mesaje care vor fi schimbate cu alte instituții, la fel cum s-a identificat și publicat schema de mesaje pentru angajatorii care raportează date în sistemul actual. Aceste mesaje vor sta la baza comunicării digitale inter-instituționale, vor reține autorul și destinatarul, datele solicitate și datele transmise, data și ora la care au fost cerute si soluționate precum si protocolul prin care cele două instituții coopereaza și schimba aceste date.

Un alt beneficiu va fi posibilitatea de verificare electronică facilă a înregistrărilor din bazele de date ale instituțiilor partenere. Acest lucru va fi realizat prin implementarea nivelului de integrare modern, cu posibilitatea de integrare într-un sistem centralizat la nivelul Ministerului Muncii și Solidarității Sociale a tuturor datelor provenite din sistemele informatice ale instituțiilor aflate în coordonare. Implementarea nivelului de interoperabilitate al REGES-ONLINE este un pas necesar pentru realizarea acestui deziderat.

3 DESCRIEREA INVESTIȚIEI

3.1 Scenariul de implementare

Scenariul de implemntare ales presupune crearea unui nou sistem atât din punct de vedere al arhitecturii prin transformarea acestuia într-un sistem disponibil on-line (REGES-ONLINE) 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 electronice de management a resurselor umane.

Investiția va cuprinde:

- Infrastructura harware pentru procesare, stocare, balansare, comunicații, securitate și salvare date, astfel încât să fie asigurate performanțele sistemului inclusiv în cazul accesului anagajaților în regim self-service la dosarul propriu. În acest scenariu, sistemul va fi unul centralizat fără a necesita echipamente de procesare/stocare în cadrul inspectoratelor teritoriale de muncă, întreaga infrastructura necesară urmând a fi găzduită în centrul de date al Serviciului de Telecomunicații Speciale, utilizând spațiile deja ocupate de rack-urile Inspecției Muncii existente in centrul de date STS și respectând cerințele de putere consumată și climatizare actuale ce pot fi asigurate in centru. Tehnologic, infrastructura trebuie să fie compatibilă cu cea care va fi implementată în cadrul proiectului de Cloud guvernamental, astfel încât, dacă este cazul, aceasta să poată fi integrată în respectiva infrastructură.
- Infrastructura de virtualizare și orchestrare, compatibilă cu cea care va fi implementată în cadrul proiectului de Cloud guvernamental, astfel încât, dacă este cazul, aceasta să poată fi integrată în respectiva infrastructură.
- Infrastructura software de bază necesară pentru rularea sistemului REGES-ONLINE, această categorie incluzând sisteme COTS de tipul: sisteme de baze de date, platforma de salvare și recuperare date în caz de dezastre, platforma de monitorizare a infrastructurii hardware, software și de aplicații, platforma de management a identității utilizatorilor și, după caz de management a accesului administratorilor la date, platforma de integrare cu capabilități de extragere, transformare și încărcare date, platforma de generare/anonimizare date de test, platforma de gestiune servicii web, platforma de gestiune configurații echipamente de comunicații, după caz, și/sau alte platforme ce pot fi indentificate în cadrul etapei de proiectare tehnică
- Infrastructura de aplicații, sistemul REGES-ONLINE cu modulele de administrare și de business identificate, a căror detaliere se va realiza în etapa de realizare a proiectului tehnic. 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: sistem complet on-line cu acces self service pentru angajați, realizat utilizând standarde deschise și în linie cu cadrul național de interoperabilitate, scalabil și înalt disponibil printr-o arhitectură cloud native.
- Serviciile de livrare, instalare, configurare a infrastructurii hardware și software, dezvoltarea, implementarea și testarea sistemului REGES-ONLINE, migrarea datelor din sistemele existente, asigurarea instruirii administratorilor și utilizatorilor, asistență tehnică la intrarea în producție a noului sistem, garanție și mentenanță. În cazul în care, pe durata implementării proiectului, sau pe durata prestării serviciilor de garanție și suport va fi necesară migrarea REGES-ONLINE în cloud-ul guvernamental, acest serviciu de migrare a infrastructurii de bază și aplicații va fi asigurată de prestator fără costuri suplimentare. Această cerință va fi asumată în clar în oferta depusă.

- Servicii de informare și publicitate pentru angajatori și angajați în vederea asigurării unei tranziții facile de la sistemul actual către REGES-ONLINE

3.2 Cerințe privind soluția tehnică

3.2.1 Cerințe generale

Sistemul REGES-ONLINE 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 cel puțin ultimele 3 versiuni ale browser-elor web Google Chrome, Microsoft Edge, Safari. Interfețele REGES-ONLINE trebuie să fie compatibile atât cu dispozitive de tip desktop/laptop, cât și cu dispozitive și telefoane mobile – moble ready. Interfața utilizator va fi realizată conform ultimelor versiuni ale standardelor HTML, CSS, XML.

Interfața sistemului REGES-ONLINE 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.

Sistemul va fi proiectat astfel încât să poată fi utilizat inclusiv de către utilizatori cu dizabilități, conform normelor legale în vigoare și standardelor industriei.

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 data 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.

3.2.2 Alinierea la strategii și legislație

Sistemul va fi proiectat astfel încât să implementeze prevederile Hotărârii Guvernului nr. 908/2017 pentru aprobarea Cadrului Național de Interoperabilitate, prevederile Legii nr. 242/2022, privind schimbul de date între sisteme informatice și crearea Platformei naționale de interoperabilitate, dispozițiilor Ordonanței de Urgență a Guvernului nr. 89/2022 privind înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizate de autoritățile și instituțiile publice, Hotărârii Guvernului nr. 112/2023 privind aprobarea Ghidului de guvernanță a platformei de cloud guvernamental, și/sau orice altă legislație aplicabilă 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 fi de tip web dezvoltată pe multi-nivel, respectând 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;
- Implementarea unui model de securitate centralizat, prin mecanisme de tip “single sign-on". Practic, utilizatorii se autentifică o singura data la accesarea sistemului informatic, accesul ulterior la modulele de aplicații și funcționalități realizandu-se fără a mai fi necesară o autentificare suplimentară. Rolurile de acces vor fi gestionate centralizat;
- Arhitectura bazată pe servicii astfel încât să permită rularea sesiunilor de acces la date izolat, distribuit și balansat în zone de memorie separate;
- 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;
- Trebuie 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.

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 care vor asigura mentenanța și dezvoltarea sistemului ulterior finalizării serviciilor de suport și garanție ofertate. Acesta va conține toate componentele aplicative precum și modulele funcționale dezvoltate în cadrul acestora și orice alte componente care 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 rapid ultima copie de siguranță disponibilă în centrul de salvare date, cu semnalarea perioadei la care s-a făcut restaurarea.

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 minimum 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 1.000 de vizitatori, precum și pentru minim 10.000 de utilizatori de tip angajat în sistem self service, 7.000 de utilizatori de tip angajator/ reprezentat al angajatorului și minim 1.000 de utilizatori ai Inspecției Muncii / Inspectoratelor teritoriale de muncă ce utilizează sau interoghează sistemul.

Sistemul trebuie să ofere mecanisme automate de scalare astfel încât să permită acoperirea unor vârfuri ce ating minim 23.000 de utilizatori de tip angajator / reprezentanți ai angajatorilor.

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 REGES-ONLINE 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 REGES-ONLINE și a infrastructurii de suport pentru acesta, minim stratul de base 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 proiectată de Beneficiar este:

Componentă	Număr mașini virtuale	Număr Core /mașină	Număr Core /componentă
Producție			
Portal Extern	**4**	**16**	**64**
Server aplicație REGES-ONLINE	**8**	**16**	**128**
Baza de date	**2**	**32**	**64**
Aplicatie consolidare, raportare și analiză date	**2**	**16**	**32**
Componenta de integrare date	**2**	**24**	**48**
Testare/Dezvoltare			**0**
Portal Extern	**2**	**4**	**8**
Server aplicație REGES-ONLINE	**2**	**8**	**16**
Baza de date	**1**	**8**	**8**
Aplicatie consolidare, raportare și analiză date	**1**	**4**	**4**
Componenta de integrare date	**1**	**4**	**4**
Administrare mediu de productie			**0**
Monitorizare date, aplicatii si sisteme	**1**	**32**	**32**
LDAP	**4**	**8**	**32**
Componenta de securizare a accesului	**2**	**12**	**24**
Componenta de securizare date	**2**	**12**	**24**
Backup date, sisteme și aplicații	**1**	**12**	**12**
Compoenta mascare date (GDPR)	**1**	**4**	**4**
Suport virtualizare - cf soluie tehnica			
TOTAL			**504**

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, Ordonanța de Urgență a Guvernului nr. 89/2022 privind înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizate de autoritățile și instituțiile publice, Hotărârea Guvernului nr. 112/2023 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: Direcția Generală Pentru Evidența Persoanelor, ONRC, IGI, ANAF, CNPP, ANOFM, INS, Ministerul Educației, angajatori care utilizează sisteme IT proprii pentru managementul datelor angajaților și doresc ca actualizarea datelor în sistemul REGES-ONLINE să fie realizată automat.

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. Acest lucru va fi realizat prin implementarea nivelului de integrare modern, cu posibilitatea de integrare într-un sistem centralizat la nivelul Ministerului Muncii și Solidarității Sociale a tuturor datelor provenite din sistemele informatice ale instituțiilor aflate în coordonare. Implementarea nivelului de interoperabilitate al REGES-ONLINE este un pas necesar pentru realizarea acestui deziderat.

Sistemul va avea o contribuție importantă în domeniul politicilor salariale din România și colectării veniturilor și taxelor datorită faptului că va putea pune la dispoziția instituțiilor care au competență în domeniile respective a informațiilor referitoare la veniturile înregistrate. Totodată se vor putea îmbunătăți controalele

anti-fraudă la nivel național, aducând beneficii majore privind transparența fluxurilor de bani și pentru identificarea evaziunii fiscale.

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 administrațiilor publice.

Administratorul informațiilor din REGES-ONLINE este Inspecția Muncii responsabilă și răspunzătoare pentru colectarea, utilizarea, actualizarea, păstrarea și ștergerea (conform legii) informațiilor. Printre responsabilitățile sale se numără și definirea utilizării permise a informațiilor, respectarea reglementărilor privind confidențialitatea datelor și a politicilor de securitate, asigurarea caracterului actual al informațiilor și a posibilității de accesare a datelor de către utilizatorii autorizați.

Prin proiectul REGES-ONLINE se va permite elaborarea și implementarea unui plan de asigurare a calității datelor pentru a garanta calitatea datelor cuprinse în acestea. Salariații și angajatorii ar trebui să poată fi în măsură să verifice exactitatea, corectitudinea și caracterul complet al datelor proprii incluse în registrele de bază.

Prin sistemul REGES-ONLINE se va pune la dispoziție un ghid privind terminologia utilizată și un glosar al termenilor relevanți utilizați în scopul informării persoanelor.

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.

3.2.3.6 Securitatea sistemului

În cadrul proiectului 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 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 fizic, accesul în sala serverelor la sisteme se va face prin implementarea diferitelor politici de securitate, acces în funcție de drepturi, rolul fiecărui operator și activitatea ce trebuie desfășurată;
- 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 utilizatori, prin păstrarea lor într-un director comun, împreună cu rolul și modalitatea de acces;
- La nivel de aplicație, prin logarea tuturor activităților efectuate asupra datelor.

3.2.3.6.1 Securitatea sistemului

Securitatea reprezintă o preocupare de bază atunci când este furnizat un serviciu public.

In cadrul proiectului se vor respecta urmatoarele principii:

- că urmează abordarea securității prin concepție pentru a asigura securitatea modulelor și a infrastructurii lor complete;
- că serviciile nu sunt vulnerabile la atacurile care ar putea să le întrerupă funcționarea și ar putea provoca furtul sau deteriorarea datelor;
- utilizarea unor servicii calificate de asigurare a încrederii în conformitate cu regulamentul eIDAS1 pentru a asigura integritatea, autenticitatea, confidențialitatea și nerepudierea datelor.

3.2.3.6.2 Autentificare

Pentru orice beneficiar sistemul va permite, conform regulamentului eIDAS 910/2014, atributele specificate de regulamentul menționat.

Pentru acces REGES-ONLINE trebuie să poată opera cu următorul set minim de date pentru o persoană fizică, care conține toate atributele obligatorii de mai jos:

a) numele de familie actual(e);

b) prenumele actual(e);

c) data nașterii;

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

d) un identificator unic, care este alcătuit de către statul membru expeditor în conformitate cu specificațiile tehnice privind identificarea transfrontalieră și care are o durată de viață cât mai mare.

Setul minim de date pentru o persoană fizică poate conține unul sau mai multe din atributele suplimentare de mai jos:

a) prenumele și numele de familie la naștere;

b) locul nașterii;

c) adresa actuală;

d) sexul.

Pentru acces REGES-ONLINE trebuie să poată opera cu următorul set minim de date pentru o persoană juridică, care conține toate atributele obligatorii de mai jos:

a) denumirea oficială actuală;

b) un identificator unic, care este alcătuit de către statul membru expeditor în conformitate cu specificațiile tehnice privind identificarea transfrontalieră și care are o durată de viață cât mai mare.

Setul minim de date pentru o persoană juridică poate conține unul sau mai multe din atributele suplimentare de mai jos:

e) adresa actuală;

f) codul de înregistrare în scopuri de TVA;

g) codul de identificare fiscală;

3.2.3.6.3 Specificații și proceduri tehnice minime pentru nivelurile de asigurare a încrederii ale mijloacelor de identificare

În conformitate cu REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2015/1502 AL COMISIEI din 8 septembrie 2015 se aplică următoarele definiții:

1. „sursă sigură” înseamnă orice sursă, indiferent de formă, în privința căreia se poate avea încredere că furnizează date, informații și/sau dovezi exacte care pot fi utilizate pentru dovedirea identității;
2. „factor de autentificare” înseamnă un factor în privința căruia s-a confirmat că are legătură cu o persoană și care se încadrează în una dintre următoarele categorii:
   (a) „factor de autentificare bazat pe posesie” înseamnă un factor de autentificare în cazul căruia subiectul trebuie să demonstreze că se află în posesia acestuia;
   (b) „factor de autentificare bazat pe cunoștințe” înseamnă un factor de autentificare în cazul căruia subiectul trebuie să demonstreze cunoașterea informației în cauză;
   (c) „factor de autentificare inerent” înseamnă un factor de autentificare care se bazează pe o caracteristică fizică a unei persoane fizice și în cazul căruia subiectul trebuie să demonstreze că prezintă respectiva caracteristică fizică;
3. „autentificare dinamică” înseamnă un proces electronic care utilizează criptografia sau alte tehnici pentru a oferi un mijloc de a crea, la cerere, o dovadă electronică a faptului că subiectul controlează datele de identificare sau se află în posesia acestora, dovadă care se modifică la fiecare autentificare a subiectului în sistemul care verifică identitatea subiectului;
4. „sistem de management al securității informațiilor” înseamnă un set de procese și proceduri menite să gestioneze la niveluri acceptabile riscurile legate de securitatea informațiilor.

În cadrul serviciilor de eGuvernare oferite în prezent de diferite instituții publice există implementate mai multe modalități și soluții de asigurare a accesului la serviciile electronice care sunt strâns legate de sistemele

informatice ce oferă aceste servicii. De regulă un sistem este configurat sa permit utilizarea unui singur tip de credențial, iar credențialele cele mai des utilizate sunt cele de tipul nume utilizator/parolă.

Prin intermediul proiectului „Platforma Software Centralizata pentru Identificare Digitala" PSCID – cu care REGES-ONLINE se va integra - se vor asigura pe langă autentificarea bazată pe credentiale de tipul ID-uri de utilizatori/parole și suportul pentru credențiale de tip certificate digitale stocate pe toke-nuri/smartcard-uri hardware și o soluție de autentificare securizată care să permită:

- utilizarea de credentiale de tipul dispozitive de autentificare virtuale (token/software de tip onetime password, etc);
- instrumente de protejare împotriva anti-malware și anti-phishing prin care utilizatorul certifica ca serviciul utilizat este autentic, prin personalizarea paginii de autentificare de pe server, asigurându-se astfel securitatea autentificării împotriva atacurilor de tip furt de identitate;

Asigurarea managementului utilizatorilor asigura în principal:

- identificarea în mod unic în sistem, a fiecarui utilizator, prin crearea unei identități electronice unice în cadrul sistemului și definirea de conturi unice și personalizate de acces;
- accesul utilizatorilor se va realiza doar prin autentificarea utilizatorilor. Vor exista informații de interes public publicate în portal care nu vor necesita autentificare; utilizarea însă a oricărui serviciu oferit prin intermediul portalului va fi asigurată doar după selectarea modalității de autentificare și prezentarea credențialelor de acces;
- gestionarea centralizată și unitară în sistem a accesului utilizatorilor prin asigurarea autorizării utilizatorilor și componentele și modulele funcționale ale acesteia conform cu drepturilor de acces definite.

Pentru personele fizice, angajați, foști angajați care vor accesa informații despre contractele de muncă se va implementa autentificarea folosind doi factori de autentificare, respectiv nume și parolă și o modalitate suplimentară de tip one-time-password, prin SMS sau folosind o aplicație mobile/ un cod transmis prin e-mail. În procesul de obținere a datelor de acces se va asigura că utilizatorii sunt înscriși atât cu numele și parola dar și cu numărul de telefon mobil / adresa de e-mail.

Sistemul va folosi următorele nivele de încredere:

- Nivelul minim pentru Angajatori: **substanțial conform regulamentului 910/2014**

Pentru angajatori se va introduce autentificarea cu 2 factori, folosind numele și parola actuale dar și certificate digitale calificate. Precizăm că majoritatea angajatorilor din România utilizează deja certificate digitale calificate ca urmare a obligativității depunerii declarației 112 la ANAF.

- Nivelul minim pentru utilizatorii Inspecției Muncii și inspectoratelor teritoriale: **ridicat conform regulamentului 910/2014** și a regulamentului de punere în aplicare (UE) 2015/1502 al comisiei din 8 septembrie 2015
- Nivel minim pentru angajați: **substanțial conform regulamentului 910/2014** și a regulamentului de punere în aplicare (UE) 2015/1502 al comisiei din 8 septembrie 2015

Pentru angajații care vor accesa informații despre contractele de muncă se va implementa autentificarea folosind doi factori de autentificare, respectiv nume și parolă și o modalitate suplimentară de tip one-time-password, prin SMS sau folosind o aplicație mobile/ un cod transmis prin e-mail. În procesul de obținere a datelor de acces se va asigura că utilizatorii sunt înscriși atât cu numele și parola dar și cu numărul de telefon mobil / adresa de e-mail.

3.2.3.6.4 Confidențialitatea datelor

Confidențialitatea este o activitate de bază pentru furnizarea serviciilor publice.

In cadrul proiectului se vor respecta urmatoarele principii:

- că urmează abordarea **confidențialității prin concepție** pentru a asigura securitatea modulelor și a infrastructurii lor complete;
- că respectă cerințele și obligațiile 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;

Utilizarea unor servicii calificate de asigurare a încrederii în conformitate cu regulamentul eIDAS[2] pentru a asigura integritatea, autenticitatea, confidențialitatea și nerepudierea datelor.

3.2.4 Componentele de infrastructură hardware

3.2.4.1 Cerințe generale

Echipamentele ofertate vor fi compatibile unele cu celelalte, ofertantul fiind responsabil cu punerea in funcțiune a echipamentelor, efectuarea testelor de acceptanță pentru acestea. 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:
    - Servere-le 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;

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

- 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;
- 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:
  - Intercomunicația 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.

Toate echipamentele vor beneficia de garanție hardware de minimum 60 de luni. Garanția hardware va fi solicitată cu un SLA (Service Level Agreement) de la producător de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, cel mai târziu a doua zi lucrătoare – Next Business Day), fără alte costuri.

Nota :

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.

3.2.4.2 Cantități

Nr. crt.	Tip de echipament	Cantitate minimă
1.	Server de aplicații și baze de date	10
2.	Sistem de stocare	1
3.	Echipamente de comunicații switch LEAF	3

4.	Echipamente de comunicatii pt administrare	1
5.	Echipamente de balansare a încărcării	2
6.	Rack	2
7.	Soluție backup, set	1
8.	Terminal interactiv	42
9.	Echipament de interconectare	2

3.2.4.3 Servere

SERVER DE APLICAȚII și BAZE DE DATE – 10 buc.
Descriere generală
• Echipamente de tip server dual-socket pentru sisteme informatice de aplicații • Răcire Front to Back
Procesor
Serverul va fi echipat cu minim 2 procesoare în arhitectura x86_64 totalizând minim 48 de nuclee. Procesoarele propuse vor fi de ultimă generație, la data depunerii ofertei, și vor avea performanțe echivalente unui scor cpubenchmark de minim 57.000
Memorie
• Minim instalata 2048GB Registered ECC DDR4-3200 memorie instalată, SDDC, suport pentru memory mirroring și hot spare. • Metode suportate de protecție a memoriei: *Advanced ECC*, *Memory sparing*
Hard disk drive
• Minim 2 x 480GB SSD hot plug de 2.5" instalate. • Serverul va fi echipat cu un număr minim de 8 bay-uri pentru HDD-uri. • Sistemul trebuie livrat cu toate modulele și accesoriile necesare pentru instalarea discurilor în mod hot-swap.
Controller raid intern
• Raid Controller hardware cu suport pentru RAID 0,1,5,10,50,6,60 și pentru HDD-uri SAS și SATA sau echivalent • Memorie cache: minim 4 GB DDR4 • Viteza memorie cache: minim 2133MHz
Interfața grafică
Minim 16MB memorie video
Securitate
• TPM 2.0; • Suport inclus pentru verificarea semnăturilor criptografice ale driver-ilor UEFI (încărcate de pe carduri PCIe, dispozitive de stocare), OS boot loader și altor programe excecutabile 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);
- 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;
- Protecție pe perioada transportului la intervenție asupra hardware.
- UEFI Server Firmware;
- posibilitatea de a dezactiva “Secure Boot“.

Interfața de rețea

- Minimum 2 porturi 32 Gbps FC SFP+ fiecare populat cu transceiver și 2 cabluri optice de minimum 5m. Porturile trebuie să fie dispuse în placi de FC separate, pentru asigurarea redundanței.
- Minim 2 porturi Ethernet 10/25 Gb SFP+ fiecare, toate porturile vor fi populate cu trancivere de 10Gb
- Interfața de rețea separată pentru administrare la distanță, diferită de cele 8 interfețe de rețea (1 buc patch CAT6).
- Solutia ofertata trebuie sa beneficieze de Root of Trust – astfel incat sa permita verificarea actualizarilor de firmware printr-un set de chei criptografice scrise de catre producator la nivel de controller hardware, permitand astfel un nivel de securitate suplimentar fata de o verificare standard la nivel de firmware software
- Adaptoarele de rețea și FC vor fi adaptate la arhitectura ofertată, astfel încât sistemul să funcționeze conform specificațiilor.

Sloturi de expansiune

Minim 3 sloturi extensie PCIe din care minim 1 de tip PCIe x16 electric (cu 16 canale PCI Express conectate)

Conectori interfețe I/O

Minim: 1 x serial, 1 x VGA, minim 3 x USB din care minim 2 x USB 3.0

Carcasa

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

Sursa de alimentare

- Minim 2 surse hot plug și redundante instalate.
- Sursele 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:
  - administrare și monitorizarea serverelor dintr-o interfață centralizată, fără necesitatea de a instala agenți;
  - a asigura compatibilitatea, sistemul 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;
  - monitorizare starea 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;
  - memorii, procesoare, surse de alimentare, ventilatoare, disk-uri, interfețe PCI, placă de bază;
  - analize predictive de eroare pentru: HDD-uri și memorii 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 facilitați:
  - 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;
  - 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;
  - integrare cu Microsoft System Center și cu VMware vCenter;

- RESTFul API cu suport Redfish
- Interfafețe access utilizator: HTML5 Web GUI, SSH, redirecționare pe port serial;
- port dedicat Gigabit Ethernet ce permite accesarea sistemului de management indiferent de stadiul de funcționare al serverului.

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

Securitate

- Suport inclus pentru blocarea configurației și a firmware-ului serverului pentru asigurarea securității împotriva modificărilor neautorizate sau rău intenționate;
- Suport inclus pentru verificarea semnăturilor criptografice ale driver-ilor UEFI (încărcate de pe carduri PCIe, dispozitive de stocare), OS boot loader și altor programe excecutabile ce sunt încărcate înainte ca sistemul de operare să ruleze;
- Suport hardware inclus pentru pentru verificarea și validarea autenticității firmware-ului componentelor critice al echipamentului (interfețe de rețea, HBA-uri, controller RAID, dispozitive de stocare);
- Update-urile de firmware trebuie să fie semnate criptografic de către producătorul echipamentului ofertat pentru a fi autentificate la instalare.

Aplicație Administrare

- Trebuie să permită administrare 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 server-elor;
- 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 semnatură 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;
- 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
- Red Hat Enterprise Linux
- Windows Server 2019

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.
Format
Rackmountable 19”.

Livrare și instalare:

- toate cablurile și kit-urile de instalare necesare montării și punerii în funcțiune vor fi incluse în oferta tehnică și financiară, conform specificațiilor producătorului.
- prestatorul trebuie să doteze rack-urile ofertate cu unul sau mai multe switch-uri KVM de minim 8 porturi fiecare, care să includă tastatură, touchpad și display LCD de minimum 17 inch și cu prelungitoare și cabluri necesare pentru conectarea tuturor echipamentelor ofertate, socnform soluției tehnice propuse, la rețeaua electrică existentă în centrul de date.
- orice alte accesorii necesare instalării și punerii în funcțiune a serverelor recomandate de către producătorul echipamentului ofertat:
    - se vor livra și instala cabluri, conectori și oricare alte accesorii de montaj conforme cu specificațiile producătorului necesare punerii în funcțiune a echipamentelor;
    - echipamentele se vor livra în locația indicată de Beneficiar cu toate componentele (procesor, memorii, ssd-uri s.a.m.d.) instalate (Factory Integrated);
    - Pachet de servicii de reparații în garanție și suport, minim 60 de luni *;
    - Garanția hardware va fi asigurată cu un SLA (Service Level Agreement) de la producător de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, cel mai târziu a doua zi lucrătoare – Next Business Day), care să garanteze diagnosticarea echipamentului sau modulului defect și înlocuirea acestuia fără alte costuri; Suportul și accesul la update-uri de la producătorul echipamentelor. Responsabilitatea furnizorului este de a achiziționa acest tip de servicii de la producător, beneficiarul serviciilor fiind Autoritatea contractantă;
    - Toate componentele și accesoriile trebuie să fie furnizate de la același producător/compatibile;
    - Nu sunt acceptate adaptoare sau soluții improvizate pentru porturile și interfețele echipamentului;
    - Perioada de garanție se va extinde cu numărul de zile în care echipamentul a fost nefuncțional.

Ofertantul va prezenta codurile și fișele de produs pentru echipamentele ofertate pentru a se putea face verificarea tehnică a ofertei. Licențele se vor oferta pentru preț de tip guvernamental sau OEM.

* Notă:

Pe toată durata garanției furnizorul va trebui să asigure Achizitorului următoarele:

- Accesul pe site-ul producătorului/producătorilor pentru descărcarea de actualizări firmware sau alte componente software ale echipamentelor și tehnologiilor livrate;

- Acces pe site-ul producătorului/producătorilor, în secțiunea de suport, pentru deschiderea de tichete, în vederea remedierii defecțiunilor pentru toate componentele hardware și tehnologiilor livrate;
- Înainte de semnarea procesului verbal de recepție calitativă, Furnizorul va trebui să facă dovada existenței suportului corespunzător echipamentelor și tehnologiilor livrate în contul Achizitorului într-un cont special creat la producători, pe toată perioada de garanție, fapt ce va atesta dreptul de descărcare și utilizare a componentelor software ale echipamentelor hardware și tehnologiilor livrate.

Detaliile privind contul Achizitorului la producător/producători vor fi furnizate la livrarea echipamentelor. Instalarea actualizărilor firmware, precum și deschiderea de tichete de suport sau orice alte activități legate de mentenanța și garanția echipamentelor vor fi asigurate de către prestator pe toată durata perioadei de garanție și suport ofertate.

3.2.4.4 Sistem de stocare

Echipament de stocare date – 1 bucată	
Cerințe generale	Soluția ofertata trebuie permită montarea într-un rack standard de centru de date de 19”, kit de montare în rack inclus, cu sistem de prindere pentru cabluri. Soluția ofertată trebuie să fie formată dintr-un singur echipament de stocare date, nu se acceptă soluții în cluster sau perechi de echipamente. Se acceptă ca echipamentul să dispună de mai multe noduri.
Sistem de operare & suport pentru clustering	Sistemul de operare trebuie să suporte platforme ale sistemelor de operare, minim: Windows, Hyper-V, VMware, Citrix, Solaris, HP-UX, IBM-AIX si Linux
Disponibilitate	Soluția ofertată trebuie să fie proiectată cu o disponibilitate minimă de 99,9999%.
Capacitate & Scalabilitate	Sistemul va fi ofertat cu o echipare de minim 280TB spatiu util folosind discuri flash NVMe de aceeasi capacitate (de maxim 7.68TB) organizate intr-o matrice RAID cu cel putin 2 blocuri de paritate pentru fiecare set de date scris, inainte de aplicarea politicilor de deduplicare / compresie. Toate discurile ofertate în cadrul soluției vor avea capabilități de criptare built-in; se vor include toate licențele necesare și se vor respecta cerințele de securitate impuse de standardul FIPS 140-2. Nu se va accepta criptarea la nivel de controller sau criptare software. Discurile flash vor fi ofertate cu minim 5 ani garantie. Garantia va trebui sa acopere un numar nelimitat de operatiuni de scriere pe discurile ofertate, adica va trebui sa acopere inclusiv situatia in care apare fenomenul de wear-out pe durata celor 5 ani de garantie.
	Solutia ofertata trebuie sa includa un numar minim de 4 controllere redundante, capabile sa functioneze in modul activ-activ, in care toate volumele sunt accesibile in mod simetric, de pe oricare din controllerele instalate.
	În configurația ofertată, cu toate volumele provizionate cu deduplicarea și compresia active, sistemul trebuie să fie capabil să susțină o performanță, astfel: - de cel putin 1.750.000 IOPS la o latenta maxima de 0.3ms, pentru un mod de acces de tip aleatoriu cu blocuri de 16K; - de cel putin 770.000 IOPS cu o latenta maxima de 0.5ms, intr-un model de

Echipament de stocare date – 1 bucată	
	access de tip aleatoriu, bazat pe blocuri de 16K si cu un raport Citire / Scriere - 60/40
Cache	Sistemul ofertat va include un minimum de 3TB memorie cache DDR4 instalată. Memoria cache va fi complet dinamică pentru operațiuni de scriere și citire. Nu se vor accepta carduri, module de memorie sau discuri adiționale.
Deduplicare	Sistemul ofertat va suporta și va include licențe pentru compresia și deduplicarea online, indiferent de capacitatea instalată pe sistem.
	Sistemul trebuie să suporte activarea simultană a proceselor de compresie și deduplicare pe același volum.
	Sistemul ofertat va suporta atât volume deduplicate cât și ne-deduplicate în același timp în sistem, pentru a putea adresa și situația în care sunt stocate date nededuplicabile (sau deja deduplicate).
No Single point of Failure	Sistemul ofertat va fi de tip No Single Point of Failure la nivel de card de controller, memorie cache, ventilatoare, surse de alimentare.
Management	Solutia de stocare propusa va include suport pentru sistemul integrat de management la distanta al solutiei, pentru provizionarea spatiului de stocare folosind profilele de provizionare de server, in vederea automatizarii / provizionarii integrate a infrastructurii propuse. Suplimentar, soluția propusă va include în configurația propusă o interfață grafică locală și una de tip command-line, din care va fi posibilă efectuarea taskurilor de provizionare și administrare a resurselor instalate. Sistemul de management trebuie să permită configurarea de alerte prin e-mail.
Suport Raid & Virtualizare	Sistemul ofertat trebuie să fie capabil să protejeze datele împotriva pierderii simultane a cel puțin două discuri în cadrul unui grup de RAID (RAID 6). Suplimentar prin provizionarea din start a unui spațiu de tip spare solicitat, soluția ofertată va trebui să demareze în mod automat procesul de RAID Rebuild, în orice situație în care se defectează un disk.
	În vederea utilizări cât mai eficiente a discurilor instalate, soluția ofertată va include suport în configurația propusă, pentru tehnologiile wide-stripe și global spare.
Protecția datelor	Sistemul ofertat va avea implementată o tehnologie care să îi permită, ca în situația în care alimentarea cu tensiune este întreruptă, să facă o copie a datelor din memoria cache pe un support nevolatil.
	Soluția de stocare ofertată va avea inclusă o soluție licențiată pentru toată capacitatea utilă ofertată, care să permită: - crearea de imagini ale volumelor de stocare create (snapshot-uri); - crearea unei clone virtuale pornind de la o imagine a unui volum.
Protocoale suportate	Sistemul ofertat va include suport în configurația propusă pentru următoarele protocoale: - Fibre Channel; - iSCSI; - NVMe over FC.

Echipament de stocare date – 1 bucată	
Porturi	Soluția ofertată va fi echipată cu: - minimum 4 porturi 32Gb FC, porturile vor fi prevăzute cu SFP-uri de 32Gb; - minimum 1 port 1Gb RJ-45 pentru management; - minimum 1 port 10Gb RJ45 pe fiecare controller ce vor putea fi folosite pentru replicare.
Mentenanță	Storage-ul ofertat va suporta upgrade de firmware atât pentru controllere cât și pentru discuri, fără a fi necesară oprirea sistemului sau indisponibilizarea volumelor provisionate (upgrade online).
Snapshot / Point in time copy/Clone/Integrare	Sistemul de stocare ofertat trebuie să se integreze cu soluția de virtualizare ofertată.
	Sistemul de stocare ofertat va avea suport (integrare) pentru platforme de tip container.
	Soluția trebuie să asigure mecanisme de deduplicare, domeniul de deduplicare să poată fi configurabil pentru a permite pornirea sau oprirea deduplicarii volumelor în funcție de politica setată de administrator.
Replicare Remote	Sistemul de stocare ofertat trebuie să suporte în mod nativ, atât replicare sincronă, cât și replicare asincronă cu un echipamentul de stocare SAN similar, provizionat într-un alt centru de date, pe o conexiune cu caracteristici care permit acest lucru.
Licențe	Sistemul de stocare va fi ofertat cu următoarele licențe, de la momentul instalării și operaționalizării, pe toata capacitatea suportata a sistemului: Thin provisioning, Snapshot, Clone, Monitorizarea Performanței, conversia online a volumelor (thin catre thin compressed, thin catre thin de-dup etc.), Quality of services, Replicare la distanta. Vor fi livrate toate licențele necesare în vederea asigurării funcțiilor avansate suportate de echipament, dacă acestea nu sunt incluse în caracteristicile de bază.

Echipamentul se va livra cu toate accesoriile și cablurile necesare montării în rack și punerii în stare de funcțiune a sistemului ca un tot unitar, cu prelungitoare și cabluri necesare pentru conectarea echipamentelor la rețeaua electrică existentă în centrul de date, cât și pentru conectarea sistemului rezultat în rețeaua internă a Autorității Contractante (elemente fizice de montaj; șuruburi, piulițe, șine, cât și software-ul aferent).

Oferta va include 2 switch-uri fiber channel, pentru conectarea redundantă a serverelor la echipamentul de stocare de date, compatibil cu acestea. Switchurile vor avea minimum 24 porturi fiecare și toate vor fi active și licențiate, cu viteză de 32Gb FC, montabile în rack standard de 19”. Toate porturile vor fi prevăzute cu SFP-uri de 32Gb. Se vor include și 24 patch cord-uri de fibră optică cu o lungime de minimum 5 m pentru fiecare switch. Switch-urile vor include toate licențele necesare pentru monitorizarea performanței, alertare și diagnoză rețea de stocare, inclusiv licența pentru ISL Trunking. Kitul de montare în rack va fi inclus în ofertă.

Echipamentele se vor instala și configura conform indicațiilor beneficiarului, în urma propunerilor ofertantului.

Discurile SSD vor fi ofertate cu minimum 60 luni garanție. Garanția va trebui să acopere un număr nelimitat de operațiuni de scriere pe discurile ofertate, adică va trebui sa acopere inclusiv situația în care apare fenomenul de wear-out pe durata celor 60 luni de garanție.

Garanția hardware a componentelor din compunerea echipamentului de stocare va fi de minimum 60 de luni. Garanția hardware va fi asigurată cu un SLA (Service Level Agreement) de la producător de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, cel mai târziu a doua zi lucrătoare – Next Business Day), care să garanteze diagnosticarea echipamentului sau modulului defect și înlocuirea acestuia, fără alte costuri.

Suportul software va fi de minimum 60 de luni. 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 va fi făcut direct de către personalul achizitorului în portalul producătorului, 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 (sistem de operare, firmware).

Responsabilitatea furnizorului este de a achiziționa acest tip de servicii de la producător, beneficiarul serviciilor fiind Autoritatea contractantă.

Responsabilitatea acordării garanției și suportului software va fi a Producătorului în conformitate cu serviciul de tip SLA (Service Level Agreement) achiziționat de furnizor pentru Autoritatea contractantă.

Pe toata durata garanției furnizorul va trebui să asigure Achizitorului următoarele:

- Accesul pe site-ul producătorului/producătorilor pentru descărcarea de actualizări firmware sau alte componente software ale echipamentelor și tehnologiilor livrate;
- Acces pe site-ul producătorului/producătorilor, în secțiunea de suport, pentru deschiderea de tichete, în vederea remedierii defecțiunilor pentru toate componentele hardware și tehnologiilor livrate;
- Înainte de semnarea procesului verbal de recepție calitativă, Furnizorul va trebui să facă dovada existenței suportului corespunzător echipamentelor și tehnologiilor livrate în contul Achizitorului într-un cont special creat la producători, pe toată perioada de garanție, fapt ce va atesta dreptul de descărcare și utilizare a componentelor software ale echipamentelor hardware și tehnologiilor livrate.

Detaliile privind contul Achizitorului la producător/producători vor fi furnizate la livrarea echipamentelor. Instalarea actualizărilor firmware, precum și deschiderea de tichete de suport sau orice alte activități legate de mentenanța și garanția echipamentelor vor fi asigurate de către prestator pe toată durata perioadei de garanție și suport ofertate.

Echipamnetele de stocare de date și echipamnetele de procesare de tip server trebuie să fie compatibile. Oferta va include demonstrarea modalității de îndeplinire a cerinței.

Accesorii și periferice: în ofertă vor fi incluse toate accesoriile necesare interconectării echipamentelor de tip server cu echipamentul de stocare, conform recomandărilor producătorului/ producătorilor.

Nu sunt acceptate adaptoare sau soluții improvizate pentru porturile și interfețele echipamentului.

Perioada de garanție se va extinde cu numărul de zile în care echipamentul a fost nefuncțional.

3.2.4.5 Echipamente de interconectare

Caracteristică	**Cerințe tehnice minimale**
Descriere generală	Echipament de interconectare tip LEAF.
Procesor	Min. 6 core
Memorie	Min. 32 GB memorie de tip RAM

Caracteristică	Cerințe tehnice minimale
Stocare internă	- Min. 128 GB disc SSD; - Min. 40 MB buffer.
Interfețe de rețea/porturi și conectori interfețe I/O	- 48 interfețe SFP+ (interfețele SFP+ trebuie să suporte atât module optice min. 25 Gigabit Ethernet și 10 Gigabit Ethernet, cât şi module optice 1 Gigabit Ethernet), complet echipate pentru a asigura conectarea echipamentelor ofertate la cea mai mare viteză posibilă - 6 interfețe QSFP28 (interfețele QSFP28 trebuie să suporte atât module optice 40 Gigabit Ethernet cât și module optice 100 Gigabit Ethernet); - 1 port 10/100/1000 RJ45 pentru management şi consolă; - 1 port USB tip A pentru stocare şi boot.
Performanțe/ funcționalități	- Min. 3 Tbps switching capacity; - Min. 1.2 Bpps switching capacity; - Latență maximă: 1.5 micro-secundă; - Min. 4095 VLAN-uri; - Max. 16.000 instanțe VRF; - Min. 64 căi ECMP; - Min. 512 port channel; - Min. 32 link-uri într-un port channel; - Min. 4 sesiuni SPAN active; - Min. 3967 instanțe RPVST; - Min. 490 grupuri HSRP; - Min. 64 instanțe MST; - Grupuri IGMP snooping: min. 32.000; - Număr slice-uri: min. 1 slice; - Min. 5.000 reguli de filtrare ACL pe intrare și min. 2000 reguli pe ieșire; - IPv4: min. 256K route; - IPv6: min. 128K route; - Imagine pentru servicii Layer 3, OSPF, EIGRP, BGP și VXLAN; - Max. 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
Protocoale/standarde suportate	- 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;

Caracteristică	Cerințe tehnice minimale
	- IEEE 802.1ae MACsec, Cloudsec; - 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.
Administrare și cerințe de licențiere	- Configurare CLI, telnet, consolă; - Trebuie să dispună de o platformă de administrare prin intermediul căreia să poată fi realizate cel puțin următoarele tipuri de operațiuni: • Automatizarea provizionării; • Verificare și validare configurație cu posibilitatea remedierii problemelor identificate. Se solicită ca aplicația de administrare să fie dedicată pentru echipamentul ofertat (nu se acceptă aplicații de tip third-party provenind de la alți producători de cât cel al echipamentului ofertat); - Toate porturile vor fi active la viteza maximă (permanent); - Cu excepția cazului în care a fost specificat altfel, în situația în care platforma de administrare ori anumite dintre cerințele privind suportul și/sau serviciile/protocoalele/funcționalitățile solicitate în cadrul prezentului capitol (inclusiv cele de tip Layer 3, OSPF, EIGRP, BGP și VXLAN) necesită licențiere, modalitatea de licențiere va fi de tip perpetuu, cu dimensionarea în mod corespunzător a licenței ofertate pentru utilizarea în mod nerestricționat a tuturor facilităților menționate.
Elemente de conectică și accesorii	- 1 cablu consolă; - 2 cabluri de alimentare energie electrică tip C13-C14; - 1 kit de instalare 19'' cu toate cablurile de protecție (împământare), șuruburile, cât şi alte accesorii necesare instalării şi punerii în funcțiune; - 20 module optice 25G-LR-S SM conector LC sau compatibil; - 20 patch-uri FO SM LC-LC, cu lungimi diferite (compatibile transceiver ofertat), din care 10 buc. de min. 2m și 10 buc. de min. 3m; - 6 module optice QSFP28-100GB SMF conector LC exemplu: QSFP-100G-DR-S; - 12 patch-uri FO SM-LC compatibil transceiver QSFP28 ofertat de min. 2m.
Alimentare	Min. 2 surse de alimentare, redundante (cu suport pentru standardele românești)
Răcire/ventilație	- Răcire Back to Front; - Min. 4 ventilatoare redundante, hot-swappable (un ventilator defect nu va afecta performanțele echipamentului);
Format	Rack-mountable 19”
Alte cerințe (suport și garanție)	- Minim 5 ani

3.2.4.6 Echipament de interconectare pentru administrare

Caracteristică	Cerințe tehnice minimale
Descriere generală	Echipament de interconectare pentru administrare
Procesor	Min. 4 core
Memorie	Min. 8 GB memorie de tip RAM
Stocare internă	- Min. 16 GB disc SSD; - Min. 40 MB buffer.
Interfețe de rețea/porturi și conectori interfețe I/O	- Min. 48 interfețe 100M/1G Base-T, min. 4 interfețe 1/10/25G SPF28 și min. 2 interfețe 40/100G QSFP28 (interfețele suportă module optice atât min. 40 Gigabit Ethernet, cât și min. 100 Gigabit Ethernet); - Min. 1 port 10/100/1000 RJ45 pentru management şi consolă; - Min. 1 port USB tip A pentru stocare şi boot.
Performanțe/ funcționalități	- Capacitate min. 0.696 Tbps switching; - Min. 517 mpps switching capacity; - Latență maximă: 2 micro-secunde; - Min. 64 căi ECMP; - Min. 512 port channel; - Min. 32 link-uri într-un port channel; - Min. 4 sesiuni SPAN active; - Min. 3967 instanțe RPVST; - Min. 490 grupuri HSRP; - Min. 64 instanțe MST; - Max. 8000 rute multicast; - Grupuri IGMP snooping min. 8.000; - Reguli de filtrare ACL pe intrare (min. 3000/slice) și reguli pe ieșire (min. 2000/slice); - Imagine pentru servicii Layer 3, OSPF, EIGRP, BGP și VXLAN; - Max. 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.
Protocoale/standarde suportate	- 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 802.1ae MACsec, Cloudsec;

Caracteristică	Cerințe tehnice minimale
	- 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.
Administrare și cerințe de licențiere	Trebuie să dispună de o platformă de administrare prin intermediul căreia să poată fi realizate cel puțin următoarele tipuri de operațiuni: • Automatizarea provizionării; • Verificare și validare configurație cu posibilitatea remedierii problemelor identificate. Se solicită ca aplicația de administrare să fie dedicată pentru echipamentul ofertat (nu se acceptă aplicații de tip third-party provenind de la alți producători decât cel al echipamentului ofertat); - Toate porturile vor fi active la viteza maximă (permanent); - Cu excepția cazului în care a fost specificat altfel, în situația în care platforma de administrare ori anumite dintre cerințele privind suportul și/sau serviciile/protocoalele/funcționalitățile solicitate în cadrul prezentului capitol (inclusiv cele de tip Layer 3, OSPF, EIGRP, BGP și VXLAN) necesită licențiere, modalitatea de licențiere va fi de tip perpetuu, cu dimensionarea în mod corespunzător a licenței ofertate pentru utilizarea în mod nerestricționat a tuturor facilităților menționate.
Elemente de conectică și accesorii	- Min. 1 cablu consolă; - Min. 2 cablu de alimentare energie electrică tip C13-C14; - Min. 1 kit de instalare 19'' cu toate cablurile de protecție (împământare), șuruburile, cât şi alte accesorii necesare instalării şi punerii în funcțiune; - Min. 24 patch-uri RJ45 Cat 6, din care 12 buc de min. 2m și 12 buc. de min. 3m; - Min. 4 module QSFP-40GB LR SM LC-LC exemplu: QSFP-40G-LR4S; - Min. 8 patch-uri FO SM LC compatibil transceiver QSFP ofertat de min. 2m; - Min. 4 module optice QSFP-40GB MM LC-LC exemplu: QSFP-40G-SR4-S; - Min. 8 patch-uri FO MM-LC compatibil transceiver QSFP ofertat de min. 2m; - Min. 4 module optice QSFP28-100GB SMF conector LC exemplu: QSFP-100G-DR-S; - Min. 8 patch-uri FO SM-LC compatibil transceiver QSFP28 ofertat de min. 2m..
Alimentare	Min. 2 surse de alimentare, redundante (cu suport pentru standardele românești)
Răcire/ventilație	- Răcire Front to Back; - Min. 3 ventilatoare redundante, hot-swappable (un ventilator defect nu va afecta performanțele echipamentului);
Format	Rack-mountable 19”
Alte cerințe (suport și garanție)	- Minim 5 ani

3.2.4.7 Soluție de backup

Soluția de backup avută în vedere își propune generarea unui set de salvari de tip operațional stocate pe o soluție de stocare deduplicată a datelor pe disc și a unui alt set de date cu retenție pe termen mai lung, eventual cu evacuarea periodică a unei imagini salvate într-o locație sigură, folosind benzi magnetice.

Soluția software de backup trebuie să ofere o integrare avansată atât cu mediul virtual solicitat, cât și echipamentele de stocare a datelor de producție și de backup, în vederea obținerii unui proces de backup cu impact minim asupra performantei finale a platformei de producție.

Soluția de backup va fi instalată în centrul de date al Inspecție Muncii din București..

3.2.4.7.1 <u>Solutie de salvare deduplicată a datelor pe disc</u>

Caracteristică	Cerințe tehnice minimale
Cerinte generale	Solutia ofertata trebuie permita montarea intr-un rack standard de centru de date de 19”
Cerinte echipare	Solutia ofertata va fi echipata cu un spatiu raw total de minim 192TB cu discuri rotative si cel putin 60TB raw cu discuri flash capabile sa poata sustine o performanta constanta in citirea si scrierea datelor in sistem.
	Solutia ofertata va fi echipata cu cel putin 2 module de stocare dedicate pentru rularea sistemului de operare specializat al echipamentului si care nu vor fi parte din spatiul unde vor fi stocate datele salvate. Solutia ofertata va include si o licenta de replicare nativa, deduplicata a datelor catre un sistem similar la distanta (sau intr-o locatie de tip DR). Solutia ofertata va include suport atat pentru deduplicarea la destinatie, cat si pentru deduplicarea la sursa a datelor pentru cel putin 3 vendori de solutii software de backup: Veeam, Commvault si Veritas. Solutia ofertata va include suport pentru emularea de librarii virtuale cu tehnologie LTO, pentru cel putin LTO-3, LTO4 si LTO7. Solutia ofertata va include suport pentru criptarea datelor salvate. Solutia ofertata va fi echipata cu surse de alimentare redundante.
Echipare Interfete	Solutia ofertata trebuie sa includa: - Cel putin 1 port 1Gb RJ-45 pentru management IP. - Minim 4 porturi 25Gb SFP28 Ethernet - Minim 4 porturi 32Gb FC Toate porturile trebuie sa fie active si sa poata fi folosite in traficul de date de backup. Solutia ofertata va include suport pentru conectarea directa a serverelor pe porturile configurate.
Cerinte performanta	Solutia ofertata trebuie sa asigure o performanta cumulata de cel putin 100 TB/h, folosind eventual echipamente multiple, tehnologii de optimizare a traficului de date si algoritmi eficienti pentru deduplicarea datelor scrise pe disc

Cerinta pentru securitatea datelor	Solutia ofertata trebuie sa ofere stocarea datelor deduplicata pe diskurile instalate, asigurand un mod de integrare in infrastructura propusa care nu depinde de protocoale de tip DAS sau NAS (NFS si SMB), asigurand astfel si protectia a datelor de backup impotriva atacurilor de tip ransomware si cryptolocker.
	Solutia ofertata trebuie sa una specializata, de tip “appliance”, astfel incat datele stocate sa poata fi accesate doar printr-o interfata securizata care prezinta un numar minim de functii, legate strict de functionalitatea acestuia.

3.2.4.7.2 <u>Solutie de salvare a datelor pe benzi magnetice</u>

Caracteristică	**Cerințe tehnice minimale**
Cerinte generale	Solutia ofertata trebuie permita montarea intr-un rack standard de centru de date de 19”
Cerinte echipare	Solutia ofertata trebuie sa asigure: - Minim 40 de sloturi de benzi - Minim 100 de benzi LTO-9 - Minim 3 benzi de curatare - Minim 3 unitati de citire / scriere benzi magnetice in tehnologie LTO-9 cu conexiune nativa de tip FC, minim 8Gb, care sa includa suport pentru benzile de tip WORM (Write-Once-Read-Many) - Interfata web pentru administrarea de la distanta a librariei - 1 port de management 1Gb RJ-45 Benzile LTO-9 ofertate trebuie sa fie echipate cu coduri de bare Pentru a reduce gradul de utilizare a unitatilor de citire / scriere, libraria trebuie sa fie echipata cu un mecanism de adaptare automata a vitezei de scriere a datelor pe banda magnetica, functie de viteza de transmisie a datelor de catre servere.
Integrare in platforma de backup	Solutia ofertata va fie integrata cu solutia software de salvare a datelor propusa. Oferta va include toate echipamentele de interconectare necesare pentru transferul datelor între echipamentele de stocare/deduplicare și salvare pe benzi, în funcție de soluția tehnică ofertată, la viteza maximă cu care sunt echipate acestea
Cerinte pentru criptarea datelor	Solutia ofertata trebuie sa includa licente si eventualele module necesare pentru a permite criptarea hardware a datelor pe banda magnetica.
Cerinte pentru configuratie redundanta	Solutia ofertata trebuie sa includa suport si licentele necesare pentru configurarea intr-o arhitectura redundanta, prin care fiecarei unitati de citire / scirere i se pot aloca 2 cai redundante prin intermediul retelei SAN/FC, iar transferul datelor sa se poata face in mod transparent pentru aplicatia de backup fie pe o cale, fie pe cealalta, functie de disponibilitatea acestora.
Cerinte performanta	Solutia ofertata trebuie sa permita o viteza nativa de scriere de cel putin 2TB/h. In varianta maximala, solutia trebuie sa permita atingerea unei performante de cel putin 50TB/h.

Alimentare tensiune	Solutie ofertata trebuie sa fie echipata cu surse de alimentare redundante.
Cerinte fiabilitate	Fiabilitatea librariei ofertate va fi certificata de catre vendor prin urmatorii indicatori: - MTBF (Mean Time Between Failure) – minim 125.000 ore - MSBF (Mean Swaps Before Failure) – minim 1.000.000

3.2.4.8 Echipament pentru balansarea traficului

Caracteristică	**Cerințe tehnice minimale**
Descriere generală	Echipament de balansare de tip ADC, cu funcții de load-balancing și WAF.
Procesor	Min. 8 core
Memorie	Min. 32 GB memorie de tip RAM
Stocare internă	Min. 480 GB disc SSD
Interfețe de rețea/porturi și conectori interfețe I/O	- Min. 4 porturi 1/10 Gbps Ethernet RJ45; - Min. 4 porturi 10/25 Gbps Ethernet SFP+/SFP28.
Performanțe/ Funcționalități	Fiecare echipament va fi configurat și echipat pentru a asigura cel puțin următorii parametrii de funcționare: • Throughput, în regim de procesare generală L4: min. 20 Gbps; • Throughput, în regim de procesare generală L7: min. 17 Gbps; • Compresie HW: min. 15 Gbps; • Procesare criptografică HW internă (integrată): min. 10 Gbps; • Procesare SSL HW (integrată) de tip RSA (cu chei 2048 bit): min. 15.000 tranzacții pe secundă; • Procesare SSL HW (integrată) de tip EEC (ECDSA P-256): min. 10.000 tranzacții pe secundă; • Suport HTTP/2 *"full-proxy"*; • Optimizare TCP WAN/LAN/Mobile; • Suport pentru TLS 1.3 bazat pe RFC8446 cu listele de cipher-uri corespunzătoare; • Protocoale de rutare: BGP, ISIS, OSPF V2 și V3, RIP; • Procesarea de trafic: min. 1.8M cereri pe secunda L4 HTTP și 875k cereri pe secundă L7; - Echipamentul va putea funcționa ca proxy hardware, putând fi configurat pentru funcționare atât în *"full proxy mode"* cât și în mod *"reverse proxy mode"*, putând fi configurat pentru funcționarea strictă *"reverse proxy"* și va integra funcționalități de tip *"syn cookie protection"*; - Multipli algoritmi sau metode statice de balansare a traficului cum ar fi *"round-robin"*, *„ratio"* și "*priority"* (cu un număr minim de membri activi), precum și algoritmi sau metode dinamice de balansare a traficului cum ar fi: *"fastest-response"*, "*least-connections"*, combinația *"fastest-response/least-connections"*, precum si bazate pe resursele serverelor de aplicații (ex: utilizare CPU, încărcare memorie, gradul de încărcare al rețelei); - Echipamentul va dispune de următoarele capabilități: • Procesarea traficului TCP si UDP generat de diferite aplicații;

Caracteristică	Cerințe tehnice minimale
	• Procesarea cererilor bazate pe adresa IP sursa/destinație, SSL, "*hash persistence"*; • Utilizarea diferitelor metode pentru "*cookie persistence*": pasiv, insert, rewrite; • Utilizarea metodelor de persistenta a sesiunilor în funcție de orice variabilă din *header*-ul pachetelor TCP/UDP sau din „*payload"*; • NAT și NAPT, bazat pe IP sursa și/sau IP destinație; • Returnarea pachetelor bazată pe adresa MAC a ultimului hop (asigurarea rutării asimetrice); • Direcționarea traficului in funcție de URL, *"method"*, HTTP host, *"version"*, cookie, tipul browser-ului folosit de client; • Generarea regulilor noi pentru managementul traficului în funcție de anumite evenimente, folosind un limbaj de *"scripting"*; • Inserția XFF in *header*-e HTTP, cu adresa IP originară a clientului; • Redirectare URL către mai multe servere virtuale în funcție de "*HTTP response code"* sau *"URL pattern"*; • Agregarea și reutilizarea multiplelor sesiuni client într-o singură sesiune *"server-side"*; • Transformarea sesiunii HTTP 1.0 în sesiune HTTP 1.1 pentru consolidarea sesiunilor *"server-side"*; • Inspecția cererilor/răspunsurilor HTTP; • Blocarea codurilor de eroare generate de anumite servere de aplicații; • Blocarea atacurilor de tip DoS prin conexiuni proxy; • Utilizarea ambelor metode de securitate: pozitivă și negativă; • Filtrarea pachetelor OSI L3-L7; • Camuflarea informațiilor despre serverele de aplicații și mesajele generate de acestea ("*Resource cloaking*"); • Detectarea și blocarea anomaliilor de protocol TCP/UDP, pentru protecție DoS; • Definirea politicilor de blocare pentru atacuri tip DoS; • Monitorizarea aplicațiilor protejate pentru prevenirea, detectarea și raportarea anomaliilor de trafic precum și pentru protecția împotriva atacurilor L7 DoS; • Menținerea conexiunilor SSL și sesiunile SSL prin mirroring cu alte echipamente de tip ADC; • Dynamic TCP Tuning; • TCP Auto Buffer Tuning; • Conectarea cu instrumente de monitorizare third-party via open API; • Logging granular per aplicație; • Packet Filtering si ToS, QoS (*"marking"/"preservation"/"mimic"*); • Suport pentru limbaj programare pentru HTTP/2; • Realizarea de caching pentru HTTP/2; • Realizarea Bandwidth Control pentru UDP;

Caracteristică	Cerințe tehnice minimale
	• Definirea unui obiect pentru prezentarea aplicației prin utilizarea adresei IP și a unei liste cu porturile pentru servicii; • Combinarea mecanismelor detecție și de prevenire; • WAF prin intermediul cărora se vor putea: o Defini în mod automat politici de securitate; o Accepta prin intervenite manuală de tip "*false-positives";* o Defini politici de securitate diferite pentru diverse aplicații; o Suporta funcționalități de grupare a semnăturilor. În acest sens echipamentul va trebui să suporte cel puțin următoarele categorii de semnături: o Baze de date (min. Microsoft SQL, Oracle, MySQL, PostgreSQL, Sybase); o Sisteme de operare: (min. Windows, Linux, UNIX); o Limbaje și contexte de aplicație (min. .NET, PHP, Java); o Servere web (min. Apache, Microsoft IIS); • Mecanisme de: o Revenire (roll-back) a politicilor de securitate; o Versionare a politicilor de securitate; o Definire a politicilor de securitate în timp real, cu funcție de auto-învățare; o Definire a politici de securitate pe baza unor instrumente/aplicații de tip third-party pentru evaluarea vulnerabilităților (spre ex. prin import); • Politici predefinite pentru diferite aplicații (ex: MS SharePoint, Oracle Application 10g).
Protocoale/standarde suportate	Echipamentul va dispune de capabilitatea de monitoriza aplicații "content based", cum ar fi: - HTTP/HTTPS; - FTP (pasiv/activ); - POP3; - IMAP; - SIP; - SMTP, - Telnet; - RADIUS; - LDAP (cu TLS sau peste canal SSL); - SASP; - Oracle; - MSSQL; - SNMP DCA; - WMI; - RPC și SOAP.
Administrare și cerințe de licențiere	Configurarea modulelor (licențiere/provizionare) utilizând CLI/REST API; Cu excepția cazului în care a fost specificat altfel, în situația în care aplicația de administrare/aplicațiile care deservesc echipamentul ofertat, ori anumite

Caracteristică	Cerințe tehnice minimale
	dintre cerințele privind suportul și/sau serviciile/protocoalele/funcționalitățile solicitate în cadrul prezentului capitol necesită licențiere, modalitatea de licențiere va fi de tip perpetuu, cu dimensionarea în mod corespunzător a licenței ofertate pentru utilizarea în mod nerestricționat a tuturor facilităților menționate; În sensul celor de mai sus, licența WAF va avea activate capabilitățile menționate, inclusiv cele de tip *"threat intelligence"* care vor permite identificarea și blocarea celor mai noi tipuri de atacuri. Celelalte licențe vor fi disponibile autorității contractante dar se vor activa la momentul indicat de acesta, cu precizarea că, configurația solicitată nu va include și eventualele subscripții pentru serviciile de reputație.
Elemente de conectică și accesorii	- Fiecare echipament va fi echipat cu: • Min. 4 transceivere ce asigura fiecare cate un port optic 25 Gbps (pentru fibră optică de tip SM); • Min. 2 transceivere ce asigura fiecare cate un port optic 25 Gbps (pentru fibră optică de tip MM); • Min. 2 transceivere ce asigura fiecare cate un port electric 10 Gbps (pentru conversie RJ45 to FO); - 1 kit de instalare 19'' cu toate cablurile de protecție (împământare), șuruburile, cât şi alte accesorii necesare instalării şi punerii în funcțiune, racordării la sistemul cu energie electrică, precum și orice alte repere și subansambluri necesare în acest scop, inclusiv pentru interconectarea în/la mediile de comunicații.
Alimentare	- Min. 2 surse de alimentare, redundante (cu suport pentru standardele românești), clasa *"Platinum"* (sau echivalent), cu o putere de consum de max. 85W, 220VAC, 50Hz; - Cabluri IEC C13 la C14 de min. 1,5m.
Răcire/ventilație	Răcire Front to Back.
Format	Rack-mountable 19", max. 1U.
Alte cerințe (suport și garanție)	- Minim 5 ani

3.2.4.9 Rack complet echipat – 2 buc.

Caracteristica	Cerința tehnică minimală
Design	Design conceput pentru rutare optima a cablurilor combinata cu ventilare maxima.
Capacitate	• Minimum 42U orizontal • Incarcare minimum 1000 kg
Facilități pentru intreținerea ușoară a echipamentelor montate	• Permite montarea de sine telescopice care să permită extracția completa a echipamentelor montate. • Uși reversibile (balamalele pot fi montate atât pe stanga cât și pe dreapta).
Protecția accesului	Uși prevazute cu incuietoare cu cheie atat in fata cat si in spatele rack-ului.

Caracteristica	Cerința tehnică minimală
Ventilație	Uși perforate (minim 80% din suprafata) pentru a permite un flux optim de aer pentru racire și disiparea eficientă a caldurii.
Specificații	• Compatibil cu standardul EIA-310-E; • Înălțime: 42U (197cm); • Adâncime: minim 100 cm; • Lățime: min 60 cm; • Compatibil cu echipamentele ofertate; • Carcasă metalică; • Încărcare statică: min 800 kg; • Încărcare dinamică: min 600 kg; • Asigură protecție IP-20 pentru echipamentele găzduite; • Prevăzut cu roți și sistem de fixare statică; • Dotat cu cable management;
PDU	Va fi echipat cu cel puțin două PDU tip smart verticale pentru conectarea redundanta a tuturor echipamentelor instalate în rack-ul respective și va avea cel puțin conectori de tip IEC 320 C13 (min. 10A) si de tip IEC 320 C19 (min. 16A).
Alte cerințe (suport și garanție)	Minim 5 ani

Fiecare rack va fi echipat cu minim* un UPS cu următoarele specificații:

Caracteristica	Cerință tehnică minimală
Descriere generala	UPS, rackabil 19”, cu topologie Online Double Conversion, cu sistem PFC (Power Factor Correction), cu management, bypass intern
Capacitate de ieșire livrata	Minim 5.000 VA/ 4.500 Watts
Tensiune nominala de intrare	230V default
Tensiune nominala de ieșire	230V default (tensiune suportata intre: 200 – 240V), TDHu<2%
Frecventa de intrare	auto-selectata
Frecventa ieșire	50/ 60 Hz
Conexiuni ieșire	6 socket x IEC 320 C13 4 socket x IEC 320 C19 2 socket x IEC Jumpers
Conexiuni de intrare	Bloc terminal (hard-wire)
Randament	Minim 92% în mod on-line
Expandabilitate	Posibilitatea de a adaugă minim 10 module de baterii externe, hot-swappable, ce pot fi recunoscute automat de către UPS
Tip acumulatori	Sigilati, fără mentenanță, etanși, de tip lead-acid
Porturi de comunicații	Min 1 x USB, 1 x RJ-45 Serial

Conexiune rețea Ethernet	Card de management cu port RJ-45, 10/ 100 Mbps
Notificări	Notificare privind apariția defectelor la acumulatori
	Notificare privind absenta acumulatorilor
Cerințe de funcționare/ operare	Reglare automata a tensiunii de încărcare a acumulatorilor în funcție de temperatură, protecție împotriva descărcării totale
	Sa permită schimbarea acumulatorilor în timpul funcționarii UPS-ului și recunoașterea automata a bateriilor
	Testare automatică periodică
	Asigură predicția estimativă pentru înlocuirea acumulatorilor
	Ecran LCD încorporat, cu taste de navigare, pentru monitorizarea și configurarea locală a UPS-ului: min status UPS, parametrii sistem, evenimente
Mediu de operare/ funcționare	Temperatura de lucru: 0 – 40°C Umiditate relativa: 5% – 95%, fără condens
Accesorii	Toate accesoriile și șuruburile necesare montării în rack (kit de rack-are, șuruburi, etc.)
Alte cerințe (suport și garanție)	Minim 5 ani

*conform soluției tehnice propuse oferta va include un echipament(e) capabil să susțină funcționarea echipamentelor protejate până la oprirea acestora în siguranță. Oferta va include calculul de dimensionare a echipamentului(elor) propus și demonstrarea capacității solicitate.

3.2.4.10 Terminal interactiv

Terminalele interactive vor fi instalate în sediul fiecărui Inspectorat Teritorial de Muncă. Oferta va include transportul, instalare și configurarea terminalelor în fiecare ITM, astfel încât acestea să fie conectate și să funcționeze integrat cu sistemul REGES-ONLINE. Scopul terminanelor este de a oferi solicitanților de informații acces direct la sistem precum și de a asigura imprimarea de documentel acolo unde situația o cere (sunt solicitate) direct din sistem.

Terminalul interactiv va oferi minim următoarele funcționalități:

- Ecran tactil pe care va putea fi accesat doar sistemul REGES-ONLINE. Soluția trebuie să ofere o funcționalitate similară unui dispozitiv mobil, astfel încât solicitantul/utilizatorul să poată realiza operațiile necesare obținerii informațiilor din sistem sau imprimării documentelor/rapoartelor solicitate din sistem, pentru setul de documente ce va fi stabilit în etapa de analiză și proiectare a REGES-ONLINE. Dimensiunea ecranului va permite realizarea tuturor operațiilor în sistem.
- Modul de conectare la internet atât prin rețea LAN cât și wireless
- Camera web
- Scaner de documente, care sa permită scanarea documentelor de identitate și identificarea elementelor de securitate din acestea: poza, cnp, care, împreună cu camera web, să permită autentificarea utilizatorului și autorizarea acestuia pentru acces la datelor proprii, sau, după caz, validarea contului unui utilizator și apoi autentificarea și autorizarea acestuia

- Design-ul terminalului va fi ergonomic și va stabilit de către Achizitor în baza modelelor propuse de prestator (minim 3 modele)
- Interfața kiosk a terminalului va fi securizată, astfel încât utilizatorul să nu poată realiza decât operațiile pentru care acesta a fost proiectat
- Interfața kiosk va fi una facil de utilizat, cu pictograme de dimensiuni mari și va ghida, pas cu pas, utilizatorul în realizarea minim a acțiunilor de activare cont, accesare cont, generare rapoarte de muncă personale, imprimare rapoarte
- Posibilitatea de imprimare documente format A4, alb-negru, imprimanta utilizată trebuind să aibă o capacitate de minim 200 de pagini pentru realimentare.

Terminalele interactive vor fi livrate cu toate cablurile și accesoriile necesare, respectiv cu toate licențele software necesare, inclusiv pentru asigurarea protecției antivirus și rularea în sistem securizat. Terminalele vor beneficia de o perioadă de garanție de minim 60 de luni de la recepția acestora.

Prestatorul va asigura livrarea și instalarea terminalelor în locațiile indicate de Achiztor (orașe reședință de județ) precum și operaționalizarea acestora și interconectarea cu sistemul REGES-ONLINE, precum și testarea funcționării acestora conform cerințelor. Pe toată durata asigurării serviciilor de garanție și suport Prestatorul va asigura lunar livrarea și instalarea consumabilelor, în fiecare locație, pentru a acoperi un flux de imprimare de minim 20.000 de pagini/terminal lunar.

Pentru terminalele interactive garanția și suportul se vor asigura on-site și va fi de tip Next Business Day pentru toate componentele terminalului, inclusiv imprimanta.

3.2.5 Componentele de infrastructură software

Pentru toate produsele software nu se vor achiziționa licențe care vor expira după o anumită perioadă, degradând astfel performanțele sau capacitatea funcțională a sistemului ofertat și acceptat.

3.2.5.1 Componenta de virtualizare

Soluția ofertată trebuie să fie compatibilă cu echipamentele hardware ofertate. Compatibilitatea va fi demonstrată printr-o referință clară în specificațiile celor 2 producatori de tehnologie, din care să reiasă că este suportat un mediu de producție bazat pe cele 2 soluții.

Soluția de virtualizare va trebui să asigure:

- 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, direct de pe discurile din server, din rețea sau pe de pe un stick USB;
- suport pentru o gamă largă de sisteme de operare instalate la nivel de mașină virtuală minim toate sistemele de operare incluse în oferta tehnică;
- o densitate mare de mașini virtuale, oferind suport pentru configurații fizice generoase la nivel de host, prin configurarea cu până Ia 768 de CPU-uri logice și 16TB de memorie RAM;
- rularea de aplicații mari consumatoare de resurse, oferind support de configurare a mașinilor virtuale cu până la 256 procesoare virtuale și 6TB RAM;
- utilizarea disk-urilor rapide instalate pe server pentru configurarea ca read cache la nivel de mașină virtuală sau de disk, oferind astfel performațe deosebite pentru aplicațiile Tier 1 (simultan cu soluția de stocare hiper-convergentă);

- rate mari de consolidare a mașinior virtuale pe host-uri prin mecanisme de optimizare și supra alocare a memoriei pentru reducerea costurilor asociate infrastructurii fizice și de licențiere precum și pentru asigurarea continuității în funcționare a aplicațiilor în cazul unor întreruperi parțiale neplanificate;
- suport larg pentru aplicații terțe din partea ISV (Independent Software Vendors);
- crearea de grupuri virtuale de resurse (minim memorie şi procesor) pentru controlul și asigurarea performanțelor maşinilor virtuale care folosesc în comun respectivele grupuri de resurse;
- suport pentru Trusted Platform Module (TPM) 2.0 la nivel de hipervizor si pentru virtual Trusted Platform Module (TPM) 2.0 pentru mașinile virtuale, asigurând astfel o protecție și integritate sporită atât pentru hipervizor cât și pentru sistemele de operare guest;
- o securitate crescută prin încărcarea proceselor importante la nivel de hypervisor în zonele de memorie reziliente, prin utilizarea ultimelor funcționalități disponibile în noile versiuni de procesoare;
- criptarea traficului necesar migrării unei mașini virtuale în funcționare de pe un host pe altul, caracteristică ce poate fi setată la nivelul mașinii virtuale;
- funcționalitate de failover astfel încât, în cazul defectării unui host, mașinile virtuale care rulau pe acel host să fie restartate automat pe celelalte host-uri din cluster;
- capacități de failover astfel încât, în cazul defectării parțiale a 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 automant în mentenanță după evacuarea mașinilor virtuale;
- capacități de failover astfel încât, în cazul blocării sistemului de operare instalat într-o mașină virtuală, respectiva mașina virtuală să fie restartată automat pe același host pentru deblocarea sistemului de operare, a serviciilor și aplicațiilor;
- configurarea unei arhitecturi de funcționare continuă a unei mașini virtuale cu 2 procesoare virtuale, care chiar și în situația unei defectări hardware la nivelul hostului, permite rularea aplicațiilor din mașina virtuală fără pierderi de date.
- capacitate de failover care să detecteze problemele de acces la datastore la nivel de host și să restarteze automat mașinile virtuale afectate pe un alt host din cluster;
- posibilitatea de boot-are rapidă în cazul aplicării actualizărilor, prin eliminarea timpilor mari necesari inițializării hardware în timpul procesului de boot;
- gruparea mai multor volume de stocare cu performanțe similare în clustere pentru simplificarea managementului și plasarea inteligentă respectiv balansarea încărcării (în funție spațiul disponibil sau timpul de acces la sistemul de stocare) mașinilor virtuale în mod automat la nivel de cluster;
- comutatoare de reţea virtuale (switch-uri) administrate centralizat, la care să se conecteze maşinile virtuale şi interfețele de rețea fizice de pe fiecare host;
- creare de profile pentru host-uri (servere fizice) astfel încât instalarea pe mai multe host-uri să se facă foarte rapid, respectând o configuraţie prestabilită, configurabilă pentru eliminarea erorilor umane de configurare;
- o interfața unică de management la nivel de centru de date, bazată pe interfața web HTML 5, accesibilă de pe majoritatea sistemelor de operare și browser-erelor existente minim Firefox, Google Chrome, Microsoft Edge, pentru simplificarea managementului;
- comutatoare de reţea virtuale (switch-uri) administrate centralizat, Ia care să se conecteze maşinile virtuale şi interfețele de rețea fizice de pe fiecare host;
- criptarea traficului necesar migrării unei mașini virtuale în funcționare de pe un host pe altul, caracteristică ce poate fi setată la nivelul mașinii virtuale;

- identificarea automată a celei mai bune modalități de stocare a unei mașini virtuale, în funcție de nivelul de servicii asociat acesteia și să ofere informații în timp real privind conformitatea cu nivelul de servicii asociat;
- gruparea mai multor volume de stocare cu performanțe similare în clustere pentru simplificarea managementului și plasarea inteligentă respectiv balansarea încărcării (în funție spațiul disponibil sau timpul de acces la sistemul de stocare) mașinilor virtuale în mod automat la nivel de cluster;
- o soluție de management centralizat la nivel de centru de date (1 licență pentru fiecare centru de date), disponibilă ca appliance virtual pentru simplificarea instalării, actualizării și administrării precum și pentru reducerea costurilor asociate (ex. licență sistem de operare, licență bază de date). Oferta va include licențierea pentru un singur centru de date.
- o soluție de management centralizat la nivel de centru de date, care suporta nativ configurarea în înaltă disponibilitate pentru evitarea situațiilor de downtime la nivelul de management;

Soluția de virtualizare va fi licențiată pentru întreaga infrastructură hardware ofertată. Soluția de virtualizare ofertată va fi livrată cu suport pe o perioada de minim 5 ani cu un SLA de tip 24x7 asigurat direct de producător.

3.2.5.2 Componenta de sisteme de operare de tip server

Platforma de sistem de operare de tip server trebuie să ofere capabilități de serviciu de director, să aibă suport pentru rularea de mașini virtuale Windows și Linux, să ofere servicii web precum și capabilități de securitate integrate.

Platforma de sistem de operare de tip server trebuie să ofere suport pentru integrare cu serviciu de director și următoarele capabilități:

- Asistență în găsirea obiectelor în directoare mari;
- Suport pentru implementare serviciu de director în virtualizare;
- Suport pentru clonarea serverelor cu rolul de serviciu de director;
- Abilitatea de face o căutare în jos la o unitate organizatorică (OU - Organization Unit) din cadrul directorului;
- Serviciul de director pentru administrarea identităţilor va trebui să suporte LDAP;
- Monitorizarea, operaţiunile şi restaurarea directorului pentru administrarea identităţilor să poată fi delegate;
- Serviciul de director de management al identităţilor trebuie să aibă un singur root;
- Spaţiul de nume al serviciului de director pentru administrarea identităţilor să poată fi partiţionat într-un mod care să reflecte sau nu structura organizaţională a instituției;
- Convenţia de nume a organizaţiei să identifice unic persoanele folosind un identificator numeric unic ca valoare pentru atributul Relative Distinguished Name;
- Să ofere posibilităţi de audit al accesului la serviciul de director şi al modificărilor aduse serviciului de director;
- Serviciul de director să ofere abilitatea de a stoca certificate şi CRL-uri.

Platforma de sistem de operare de tip server trebuie să ofere instrumente facile de management cu următoarele capabilități:

- să ofere un shell cu linie de comandă şi limbaj de script;
- să ofere instrumente de diagnosticare puternice, care să permită vizibilitate permanentă asupra mediului serverului, fizic şi virtual, pentru a identifica şi rezolva rapid problemele care apar;

- să permită administrarea serverului şi replicare a datelor optimizate pentru control îmbunătăţit al serverelor de la locaţii de la distanţă, cum ar fi centrele de salvare date;
- să conțină Internet Protocol versiunea 6 (IPv6);
- sa ofere Network Load Balancing (NLB) și pe IPv6 şi si sa ofere suport pentru mai multe adrese IP dedicate, care permite găzduirea mai multor aplicaţii în același cluster NLB;
- să ofere capabilități de virtualizare la nivel hardware și suport pentru rularea de mașini virtuale cu sisteme de operare Windows sau Linux;
- să permită virtualizarea rolurile de server sub formă de maşini virtuale (VM) separate care rulează pe aceeaşi maşină fizică, fără a fi necesară achiziţia de software de la terţi;
- să ofere replicarea mașinilor virtuale către gazde situate în locații la distanță; capabilitatea de replicare să poată fi oferită între gazde care sunt membri ai unui cluster sau gazde independente
- să ofere posibilitatea de replicare a mașinilor virtuale și datelor de pe un echipament de stocare pe celălalt;
- să poată implementa mai multe sisteme de operare – Windows, Linux şi altele – în paralel pe un singur server;
- să ofere clustering-ul gazdelor sau al maşinilor virtuale care rulează pe gazde Windows Server şi backup-ul maşinilor virtuale în timp ce acestea rulează.

Platforma de sistem de operare de tip server trebuie să ofere capabilități de securitate integrate și integrarea cu elementele de infrastructură curente:

- să ofere un mecanism ce asigura că rețeaua şi sistemele nu sunt compromise de calculatoare virusate, izolând şi/sau depanând calculatoarele care nu se conformează politicilor de securitate stabilite;
- să ofere un mecanism de protecție împotriva aplicațiilor periculoase;
- să ofere flexibilitate criptografică crescută, suportând algoritmi de criptare standard şi definiţi de utilizator, permiţând crearea, stocarea şi preluarea mai facilă a cheilor criptografice;
- să conțină un modul pentru monitorizarea stării autorităților de certificare (CA);
- să ofere o protecție persistentă: să prevină accesul neautorizat asupra informațiilor, atât în timpul în care utilizatorul este conectat la rețeaua informatica a Achizitorului, dar și în afara ei, fiind conectat la rețele publice de tipul Internet.

În etapa de configurare a sistemului vor fi dezactivate serviciile ce nu sunt utilizate de sistemul proiectat/implementat. Se vor defini politici de actualizarea permanentă și în mod automat a sistemului de operare.

Oferta va include minim licențele necesare acoperirii în întregime a nucleelor fizice ale serverelor ofertate precum și pentru crearea unui număr nelimitat de mașini virtuale licențiate pe infrastructura livrată. Achizitorul nu va achiziționa nici o licență suplimentară pe durata derulării contractului necesare funcționării optime a sistemului. Oferta va include asumarea cerinței de către Ofertant. Soluția ofertata va include suport pe o perioada de minim 60 de luni, cu un SLA minim de tip 24x7 asigurat direct de producator.

3.2.5.3 Componenta de salvare date

Soluția software propusă trebuie să permită salvarea datelor provizionate în centrul de date principal, precum și replicarea acestora către centrul de date secundar, pentru un set de minim 300 de medii fizice sau virtuale și aplicații salvate în mod granular - fără a impune o limită pe numărul de sisteme pe care rulează acestea, pentru o perioadăde cel putin 60 de luni.

Soluția de backup ofertată va trebui să acopere următoarele cerințe minimale:

- integrare cu tehnologia de virtualizare ofertată

- va include licențele necesare pentru realizarea integrarii cu sistemul de salvare deduplicata a datelor pe disc ofertat, în vederea utilizării în cel mai eficient mod a facilităților de deduplicare partajată între cele 2 componente
- mecanismul utilizat pentru salvarea datelor pe solutia de backup deduplicat pe disk nu se va baza pe protocoale de tip DAS sau NAS, astfel incat sa asigure si protectia datelor salvate contra riscurilor de tip ransomware si cryptolocker
- va suporta backupul si restaurarea masinilor virtuale pentru sistemele de operare incluse în propunerea tehnică
- va include suport pentru crearea de snapshot-uri pe sistemele de stocare 32Gb si transportarea acestora catre echipamentul de stocare deduplicata
- va include suport pentru salvarea granulara a datelor folosind tehnologia de storage snapshot din solutia de stocare ofertata
- va crea arhive de backup care sunt auto-suficiente si usor de mutat/reamplasat.
- va oferi functionalitatea de a abstractiza (virtualiza) spatiile de stocare pentru backup – prin a creea un singur spatiu virtual ce va putea folosi mai multe extensii; Solutia software trebuie sa ofere aceasta funtionalitate pentru un numar nelimitat de extensii utilizate sau a numarului de utilizari;
- va stoca metadatele despre deduplicare impreuna cu fisierele de backup;
- nu va necesita instalarea de agenti in masinile virtuale pentru scopuri de backup/restore;
- va avea mecanime de notificare si informare referitor la succesul sau nereusita unei politici de backup și transmiterea notificarii prin e-mail
- trebuie sa ofere o interfață web prin care administratorii pot delega operatiile de restaurare catre utilizatori. Utilizatorii vor putea restaura pe baza permisiunilor lor, fisiere, masini virtuale
- va permite automatizarea prin REST API;
- va permite backupul configuratiei proprii si va permite reinstalarea intregii solutii daca acest lucru va fi necesar, fara a necesita mutarea sau transferul fisierelor de backup
- va oferi criptarea intregului trafic de retea intre toate componentele solutiei
- va oferi administratorilor posibilitatea recuperarii cheilor de criptare in cazul pierderii parolelor pentru politicile de backup si a backupurilor vechi
- va utiliza mecanisme pentru Change Block Tracking (CBT) si Resilient Change Tracking (RCT). Solutia va oferi suport CBT/RCT pentru hipervizorul ofertat, iar implementarea CBT/RCT va fi certificata de vendorul hipervizorului;
- va oferi mecanisme de control a incarcarii pe care operatiile de backup le aduc în mediul protejat. Astfel, daca latenta echipamnetelor de stocare va fi afectata in timpul ferestrelor de backup, trebuie să existe optiunea de a incetinii procesul de backup sau de a intrerupe temporar aceste procese pentru hypervizorul ofertat
- va oferi detectia automata a snapshoturilor orfane si va realiza consolidarea automata a acestora;
- va permite integrarea cu echipamentele de stocare ofertate. Prin integrare se va intelege posibilitatea realizarii operatiilor de backup din snapshoturile echipamentelor ofertate. De asemenea, integrarea va permite recuperarea masinilor virtualelor sau fisierelor din snapshoturile echipamentelor. Pentru operatiile de backup, snapshoturile nu vor fi montate cu ajutorul hipervizorului, iar datele vor fi copiate direct;
- va avea posibilitatea de a crea arhive de backup pe bandă, gestionand amplasarea acestei informatii;
- va oferi posibilitatea definirii unui server pentru salvarea pe benzi, altul decat serverul de backup;

- va permite copierea backupurilor intr-o alta locatie. Copiile astfel create vor putea avea setata o politica de retentie de tip GFS (Grandfather-father-son).
- Va permite creearea si copierea de puncte de restaurare (restore points) si a replica masini virtuale intr-o locatie secundara;
- va permite replicarea masinivor virtuale de productie direct din infrastructura de virtualizare ofertata, inclusiv posibilitatea de a realiza replicare asincrona continua.
- va permite ca un backup sa fie sursa pentru replicare a unei masini virtuale
- va permite pastrarea mai multor replici (sau puncte de recuperare) pentru masinile virtuale replicate;
- va permite accelerarea in cazul replicarii initiale, prin “seeding” folosind o masina virtuala diferita;
- va oferi mai multe optiuni pentru transportul datelor de backup – prin retea, folosind tehnica “hot-add”, sau direct SAN;
- va oferi posibilitatea de a realiza „ad-hoc” backup;
- va permite procesarea paralela a masinilor virtuale si a discurilor acestora.
- va permite restaurarea instantanee a masinilor virtuale, inclusiv pentru mai multe masini simultan, minim 10. Aceasta functionalitate va permite pornirea masinilor virtuale din orice backup, indiferent de tipul acestuia (full/incremental). Aceasta functionalitate va fi disponibila pentru echipamentele ofertate;
- va oferi mecanisme de migrare online pentru masinile virtuale restaurate instantaneeu, pentru reamplasarea acestora in productie;
- va permite recuperarea integral a unei masini virtuale, fisiere ale unei masini virtuale (granular) si a discurilor masinilor virtuale;
- va permite recuperarea fisierelor catre statia de lucru a utilizatorului sau direct in masina virtuala originala, fara a fi necesara instalarea vre-unui agent in masina de productie, indiferent de dimesiunea masinii sursa sau destinatie;
- va suporta pentru recuperare minim toate tipurile de fișiere din infrastructura ofertată
- va oferi posibilitatea indexarii fisierelor pentru masinile virtuale Microsoft Windows si Linux, permatand in acest mod cautarea fisierelor in arhivele de backup;
- va oferi posibilitatea de a recupera fisiere, obiecte ale aplicatiilor sau recuperarea instantanee, din snapshoturile echipamentelor de stocare ofertate
- va oferi mecanisme de verificare si testare a restaurarii, permitand testarea backupurilor realizate in mod automat. Verificarea va permite testarea aplicatiilor ce ruleaza in masinile virtuale, prin scripturi predefinite si customizabile. Procesul de verificare va trebui sa fie complet automatizat si va putea fi programat de administrator.

Soluția ofertata va include suport pe o perioada de minim 60 de luni, cu un SLA minim de tip 24x7 asigurat direct de producator.

3.2.5.4 Componenta de gestiune a bazelor de date, depozit de date, analiză și raportare

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 mentionați în cadrul prezentului caiet de sarcini.

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.

3.2.5.4.1 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 simpla operațiune de "publicare", fără a fi nevoie de redezvoltarea lor.

Modulul 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 intr-un cub cu mai multe dimensiuni, in vederea interogarii mai usoare a datelor si construirii de rapoarte si 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 îin Excel, fișiere CSV, o altă bazăde date, fișiere XML și altele;
  - Să permităa exportul datelor în documente tip PDF;
  - Să permită exportul datelor într-un feed de date;
  - Să ofere capabilitati 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 transparenta a datelor, a fisierelor de date si a fisierelor jurnal fara sa fie necesara modificarea aplicatiei. Functionalitatile de criptare sunt necesare pentru indeplinirea cerintelor si respectarea reglementarilor generale cu privire la confidentialitatea datelor. Criptarea trebuie sa ofere inclusiv instrumente de cautare in datele criptate utilizand sisteme de regasire intr-un interval sau cautarea partiala, fara modificarea aplicatiilor existente.
  - Auditarea operatiilor: auditarea trebuie sa includa informatii despre momentul in care au fost citite/accesate datele, in plus fata de orice modificare a datelor. Produsul trebuie sa ofere caracteristici precum configurarea imbunatatita si managementul auditurilor in server. Produsul sa defineasca specificatiile de audit in fiecare baza de date, astfel incat configuratia auditului sa poata fi adaptata pentru diversele baze de date.
  - Posibilitatea de a filtra evenimentele auditate; posibilitatea de a customiza operatia de audit in functie de evenimentele din baza de date.

- Posibilitatea adaugarii online a resurselor de memorie la masinile fizice care gazduiesc bazele de date pentru scalarea acestora la cerere.
- Colectarea datelor de performanta: facilitati de optimizare si depanare a performantei server-ului de baze de date, pentru a furniza administratorilor o perspectiva interactiva cu privire la performanta.
- Sistem de monitorizare extins al evenimentelor: sistem general de tratare a evenimentelor la nivel de server prin captarea, filtrarea si reglarea evenimentelor generate de procesele de server. Evenimentele trebuie sa poata fi captate si exportate in diferite formate de iesire, inclusiv Event Tracing for Windows (ETW), pentru corelarea cu aplicatiile sistemului de operare si ale bazelor de date, permitand astfel o monitorizare completa a sistemului.
- Posibilitatea comprimarii rapide a backup-urilor bazelor de date.
- Posibilitatea definirii limitelor si prioritatilor resurselor pentru diferite sarcini (workloads), si obtinerea unei perfomante crescute in executarea acestora. Modul de alocare a resurselor fizice ale server-ului trebuie să poata fi controlat de catre administratorul de sistem.
- Asigurarea continuitatii activității organizației: duplicarea datelor prin tehnologii de tip data mirorring

- Implementarea structurilor de date complexe:
  - Posibilitatea nativa de modelare a structurilor de date de tip arbore: metode incorporate pentru crearea si operarea pe noduri ierarhice.
  - Posibilitatea stocarii datelor binare mari, precum documente si imagini, ca parte integranta a bazei de date, pastrand in acelasi timp consecventa tranzactionala.
  - Cautare complexa la nivel de text, folosind indecsi specializati; efectuarea rapida a cautarilor in acest tip de date.
  - Managementul performant al coloanelor cu valori rare: modalitati eficiente pentru administrarea spatiilor necompletate dintr-o baza de date relationala, astfel incat valorile de tip NULL să nu consume spatiu 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 (CEP).
  - 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 efectuarii backup-ului in multiple fisiere simultan pentru a putea efectua operatia pe discuri diferite in paralel;
  - Posibilitatea efectuarii backup-ului direct intr-o solutie de cloud public, respectand normele de securitate;
  - Posibilitatea de a crea, modifica, sterge index-ul concurent cu activitatile utilizatorilor;

- Posibilitatea de a crea un snapshot al bazei de date;
- Modificarea schemei online.

Sistemul de analiza si raportare trebuie sa dispuna cel putin de urmatoarele caracteristici:

- Posibilitatea de a prelua, consolida, curata si agrega informatii si date provenite din diverse surse de date, structurate sau nestructurate;
- Posibilitatea de a pastra datele pe o perioada nedefinita;
- Posibilitatea de a afisa datele/informațiile vehiculate prin intermediul unui/unor dashboard-uri care să permită dispunerea flexibilă (de ex. ordonare, redimensionare, ștergere, adăugare, salvare în funcție de configurația aleasă de fiecare utilizator în parte) a mai multor widget-uri reprezentative ce vor putea fi grupate pe mai multe categorii/tab-uri, prin intermediul cărora vor fi afișate rezultatele atât rapoartelor, graficelor, tabelelor, valorilor anumitor indicatori etc.;
- Posibilitatea de a prezenta indicatorii pe harta, cu posibilitatea de a face drill la nivel de judet/regiune;
- Posibilitatea de o combina reprezentari de tip grafic cu reprezentari de tip tabular, in aceeasi pagina;
- Posibilitatea de a putea combina reprezentari de tip harta cu reprezentari de tip graphic in aceeasi pagina;
- Afisare totaluri pentru graficele centralizatoare;
- Flexibilitate in a afisa valori atat pe orizontala, cat si pe verticala;
- Posibilitatea de a putea selecta un judet din harta Romaniei rezultand astfel o modificare corespunzatoare a valorilor prezentate pe grafic (se vor prezenta doar valorile corespunzatoare respectivului judet);
- Posibilitatea de a modifica dimensiunea textului si de a incadra imaginile si graficele in pagini;
- Posibilitatea de a introduce filtre si criterii de selectie multiple;
- Posibilitatea de a urmări datele pe an calendaristic, trimestrial și lunar;
- Posibilitatea de a putea selecta luni diferite pentru afișare;
- Posibilitatea de a exporta datele in fisiere de tip Excel, PDF, CSV, imagini sau alte tipuri de fisiere;
- Posibilitatea de a importa fisiere de tip .xls, .xlsx, .csv, .txt;
- Posibilitatea de a se conecta la diverse tipuri de surse de date prin conectori dedicati cum ar fi Oracle, Mysql, DB2, SQL Server;
- Posibilitatea de a funcționa în cadrul browserelor Mozilla Firefox, Google Chrome, Safari, fără a se limita la acestea;
- Posibilitatea de a fi utilizata atat pe computer de birou, cat si laptopuri si dispozitive mobile inteligente (telefoane mobile si tablete) fara a fi necesare instalari de componente suplimentare;
- Posibilitatea de a seta drepturi diferite de acces/vizualizare a datelor la nivel de utilizator/grup de utilizatori;
- Posibilitatea de a seta drepturi de vizualizare sau creare rapoarte/dashboarduri;
- Posibilitatea de a construi rapoarte/dashboarduri noi fără a avea nevoie de cunostinte avansate de programare;
- Posibilitatea de a proiecta un model de date la nivelul Data Warehouse independent de modelul surselor de date;

- Posibilitatea de a putea prezenta situatiile raportate la un anumit moment asa cum au fost ele prezentate chiar daca ele au suferit modificari intre timp;
- Posibilitatea de a implementa procese complet automatizate de preluare, transfer si incarcare a datelor (ETL);
- Posibilitatea de a programa lansarea in executie a proceselor de incarcare a datelor la un anumit moment sau in functie de anumite conditii predefinite;
- Posibilitatea de a transmite alerte pe mail in cazul in care procesul de incarcare a datelor se intrerupe din diverse motive;
- Posibilitatea de a relansa procesele de incarcare a datelor de la pasul unde acestea s-au oprit;
- Posibilitatea de scalare a soluției in functie de modul de licentiere ofertat (per user/per processor/per record etc), inclusiv prin introducerea de noi surse de date si/sau noi tipuri de rapoarte.dashboard-uri.

Componenta de realizare a rapoartelor și dashboard-urilor trebuie să îndeplinească următoarele cerinte minime obligatorii, grupate mai jos dupa tipurile principale de functionalitati:

- Componenta trebuie sa ofere posibilitatea creearii unui model de date In-Memory,
- Componenta trebuie sa permita asocierea automata rezultand astfel un raspuns instant selectiilor utilizatorilor;
- Componenta trebuie sa permita o dezvoltare facila a rapoartelor si dashboardurilor cu ajutorul unor ferestre de tip wizard cu multe optiuni;
- Componenta trebuie sa permita ca mare parte din dezvoltarea de rapoarte si dashboarduri sa se faca prin click-uri si drag-and-drop;
- Componenta trebuie sa ofere o capacitate de vizualizare de inalta performanta folosind stiluri de dashboard indicatoare, grafice si tabele;
- Componenta trebuie sa permita utilizatorilor sa poata impartasi informatiile cu colegii prin emailuri integrate, rapoarte si printuri si sa permita lucrul colaborativ;
- Componenta trebuie sa permita integrarea unitara cu aplicatiile Microsoft Office (inclusiv e-mail);
- Componenta trebuie sa permita reprezentarea multidimensională;
- Componenta va permite utilizatorilor sa poata analiza intregul volum de date pana la nivelul tranzactiei;
- Componenta trebuie sa permita ca aplicatiile, rapoartele si graficele sa poata fi de asemenea personalizate pentru nevoi specifice si sa poate fi distribuite printre grupurile de utilizatori;
- Componenta trebuie sa permita deschiderea modelului de date pentru actualizari de date in timp real din sistemele sursa, utilizatorii finali beneficiind de vizibilitate in timp real, prin intermediul masurilor, diagramelor si alertelor disponibile in aplicatie;
- Componenta trebuie sa permita incarcarea incrementala a datelor;
- Din punct de vedere al securitatii, componenta va permite monitorizarea persoanelor cu acces la analize, la masuratorile individuale, precum si la datele din cadrul aplicatiei;
- Securitatea componentei va trebui sa poata fi configurata pe utilizator sau pe grup pentru a lucra dupa modelele standard de securitate Active Directory, LDAP sau altele;
- Componenta trebuie să includă clienți Windows, Java, Web browser zero-footprint, client AJAX-based, clienți mobile sau echivalent;
- Componenta trebuie sa permita lucrul atat on-line (server based) cat si off-line;

- Componenta trebuie sa permita utilizatorilor, care o acceseaza de pe dispozitive mobile, sa interactioneze, sa analizeze si sa interogheze o aplicatie dezvoltata/seturile de rapoarte;
- Componenta va permite definirea mai multor tipuri de utilizatori:
  - Utilizatori care vor avea doar drept de a accesa/vizualiza rapoartele si dashboardurile (fara a le modifica ca si continut si fara a putea dezvolta unele noi);
  - Utilizatori care vor avea dreptul sa creeze rapoarte si dashboarduri noi pe care le vor putea expune spre vizualizare;
  - Utilizatori care vor administra componenta software;
- Componenta trebuie sa includa posibilitatea de a interactiona in dashboard (OnClick, OnHover, Drill Down, Right Mouse Click, On load etc);
- Componenta trebuie sa ofere posibilitatea utilizatorilor de a-si definei propriile filtre;
- Componenta trebuie sa includa posibilitatea de a filtra si sorta datele (la nivel de raport/set de rapoarte);
- Componenta trebuie sa includa posibilitatea de a crea vizualizari de tip tabel sau grafic (de diverse forme) prin functia de drag and drop integrata;
- Componenta trebuie sa includa posibilitatea de a crea dimensiuni pentru a asigura comparabilitatea datelor;
- Componenta trebuie sa includa definirea si utilizarea unor date calendaristice prestabilite sau selectate dintr-un meniu de tip calendar;
- Componenta trebuie să includă posibilitatea de a exporta datele in cel putin urmatoarele formate: XLS, PDF, CSV si altele;
- Componenta trebuie sa ofere API-uri pentru extinderea functionalitatilor de vizualizare si de conectare la surse de date externe;
- Componenta trebuie sa permita prezentarea indicatorilor in diverse vizualizari (grafice de tip Pie, Bar, Line, Harti, Gauge) si posibilitatea de grupare a 2 sau mai multe grafice pentru a prezenta acelasi indicator sub diverse forme (grafic si tabel);
- Componenta trebuie sa includa elemente specifice interfetei cu utilizatorul (campuri de text, butoane normale, butoane de tip radio, butoane de tip check, drop down lists, label-uri care pot fi umplute cu text, frame-uri pentru a incadra un grafic, linii, forme geometrice, etc);
- Componenta trebuie să includa un wizard pentru a creea si edita interogari (queries);
- Componenta va permite stocarea datelor ce urmeaza a fi raportate in memorie, rezultand astfel o viteza foarte mare de raspuns la rularea rapoartelor si a dashboard-urilor;
- Componenta va permite introducerea de campuri calculate, oferind fie posibilitatea de a alege operatiuni matematice dintr-o lista predefinita fie de a crea operatiuni matematice prin scrierea de linii de cod;
- Raportare "ad hoc": utilizatorii vor putea edita propriile rapoarte pe baza unui model (template), fara sa detina cunostinte de baze de date sau despre structura acestora;
- Interogare si analiza ad-hoc si self-service a datelor: facilitati de interogare a datelor disparate in momentul solicitarii rapoartelor.

Componenta de integrare a datelor trebuie sa indeplineasca urmatoarele cerinte minimale:

- trebuie să aibe capabilități de integrare date (extragere-transformare-incarcare ETL) prin care sa se poate conecta la sisteme sursa de date, sa extraga datele, sa le transporte de la locatia sistemelor

sursa la locatia/mediul Data Warehouse, sa le transforme in functie de necesitatile de business si sa le incarce in tabelele de la nivelul componentei de baza de date (Data Warehouse);

- trebuie să aibă functionalități de extragere a datelor din diferite surse de date (minim SQL Server, Oracle, SAP, Excel, Web services, DB2, XML sau echivalent), realizarea de filtrari, agregari si diferite alte transformari asupra datelor si in final stocarea datelor in data warehouse;
- în cadrul maparilor de date trebuie sa permita definirea de filtre si de restrictii asupra campurilor implicate;
- trebuie să suporte modalitati diferite de incarcare a datelor:
- încarcare masiva de date (de tip Bulk);
- încarcare incrementala;
- trebuie să permită pastrarea istoricului diverselor versiuni ale maparilor de date;
- trebuie să permită definirea si incorporarea de componente reutilizabile suplimentare;
- trebuie să poată pune la dispozitie, sub o forma tehnica accesibila date provenite din sisteme externe pentru a fi consumate de sistemele interne;
- trebuie să ofere un nivel de abstractizare și separare a surselor de date intr-o arhitectura de tip SOA;
- trebuie să permită ca procesul de integrare sa foloseasca doua concepte larg folosite pentru a rezolva cerinte de integrare de date: procesarea datelor folosind ETL si publicarea datelor folosind o arhitectura SOA;
- procesele ETL vor fi folosite pentru a procesa datele din surse de date diverse existente.

Va fi considerată dezvoltarea a minim 20 rapoarte 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 REGES-ONLINE, 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 Caiet de Sarcini.

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 ofertata va include suport pe o perioada de minim 60 de luni, cu un SLA minim de tip 24x7 asigurat direct de producator.

3.2.5.5 Componenta de monitorizare a infrastructurii hardware, software și de aplicații

Soluția de monitorizare a infrastructurii trebuie să detecteze și să remedieze imediat, pe cât posibil automat, problemele de funcționare care afectează utilizarea în bune condiții a sistemului informatic.

- Soluția trebuie să monitorizeze performanța funcționării aplicațiilor corelată cu performanța funcționării infrastructurii, oferind următoarele funcționalități minime:
    - Identificarea impactului partajării de resurse asupra performanței aplicațiilor web;
    - Monitorizarea tranzacțiilor aplicațiilor web – Java / .Net și medii SOA – pentru toți utilizatorii în regim de 24 ore/zi și 7 zile/săptămâna și sa detecteze eventualele probleme înainte ca acestea sa afecteze utilizatorul final;

- Să asigure implementarea unei strategii de monitorizare în timp real a performanțelor aplicațiilor web utilizate ce va permite:
    - monitorizarea experienței utilizatorului prin urmărirea tranzacțiilor de tip „end-to-end”;
    - identificarea și prioritizarea problemelor care ar afecta calitatea serviciilor către utilizatorul final;
    - determinarea rapidă a sursei problemelor de performanță – indiferent dacă acestea sunt generate de aplicație (erori la nivel de cod), de componentele de infrastructură software (baze de date, server aplicații etc.) sau de componentele de infrastructură hardware (servere, sistem de stocare SAN, echipamente comunicații etc.);
    - prioritizarea și trierea incidentelor care afectează activitatea utilizatorilor;
    - monitorizarea în timp real a performanțelor aplicațiilor și experienței utilizatorilor – inclusiv pentru aplicațiile securizate prin SSL;
    - stabilirea de profile de comportament normal pe baza datelor adunate în timp și evidențierea abaterilor de la funcționarea normală a aplicațiilor;
- Să asigure monitorizarea și analizarea în detaliu a performanțelor aplicaților web, până la nivel de cod sursă;
- Să indice impactul asupra performanței generat de modificările realizate în aplicații (update-uri, patch-uri, noi versiuni etc), permițând astfel identificarea cu ușurință a problemelor de performanță generate de aceste modificări;
- Să ofere o vedere cronologică asupra performanței funcționării aplicației corelată cu arhitectura aplicației și relațiile dintre componente, care să identificarea rapidă a problemelor de performanță cauzate de modificările arhitecturale din cadrul aplicațiilor;
- Pentru optimizarea proceselor de diagnosticare și stocare, să ofere flexibilitatea culegerii datelor de diagnosticare de detaliu doar pentru tranzacțiile cu erori/probleme;
- Să monitorizeze proactiv 100% din tranzacțiile cu utilizatori reali, să detecteze tranzacțiile eșuate, și să colecteze parametri de monitorizare pentru diagnosticarea problemelor de performanță care afectează utilizatorii finali, fără a fi necesară instalarea de componente software pe stațiile de lucru ale utilizatorilor;
- Să realizeze o viziune unică, prin care să prezinte întreaga tranzacție reală a utilizatorului final și să descompună timpul necesar procesării tranzacției în timpii necesari pentru: componentele aplicației, instrucțiunile SQL, sistemele backend și componente terțe externe;
- Să poată detecta Memory Leaks și să izoleze componentele exacte care creează Memory Leaks;
- Să înregistreze proactiv toate apelurile SQL și să le raporteze pe cele cu performanțe lente. Monitorizarea execuției instrucțiunilor SQL trebuie făcută din aplicația monitorizată – fără a utiliza un agent de baze de date extern;
- Să asigure capacitatea de a monitoriza performanța aplicațiilor până la nivelul metodei de execuție (metoda Java / .Net), 24x7, în mediile de producție cu impact neglijabil asupra aplicațiilor monitorizate;
- Să identifice și să raporteze eventualele erori apărute în timpul executării funcționalităților aplicației și să identifice locul exact al erorii în cadrul stivei de apeluri de tranzacții;
- Să asigure cel puțin 2 niveluri de praguri de alertă care pot fi setate pentru parametrii monitorizați. De asemenea, la detectarea unei probleme de performanță/funcționare, să asigure declanșarea automată de acțiuni automate complexe, ca de exemplu: re-configurare rețea, re-configurare aplicație sau re-alocare resurse mașini virtuale în cazul încălcării pragurilor de alertă – acțiunile fiind diferențiate în funcție de tipul de prag încălcat.
- Soluția trebuie să monitorizeze soluția de virtualizare, oferind următoarele funcționalități minime

- Să permită identificarea și diagnosticarea problemelor de performanță la nivelul infrastructurii de virtualizare ofertate;
- Să ofere capabilități de analiză a proceselor active pentru a determina care dintre acestea afectează performanțele mașinilor virtuale și care mașini virtuale nu utilizează eficient resursele;
- Să includă o interfață predefinită de prezentare în timp real în format tabelar și grafic a metricilor (parametrilor de funcționare) a infrastructurii de virtualizare care să conțină date intuitive, cu panouri de control dedicate care să prezinte o imagine de ansamblu și de detaliu a infrastructurii de virtualizare;
- Să asigure monitorizarea metricilor de performanță pentru fiecare mașină virtuală – cel puțin încărcare CPU, memorie, disc, interfață de rețea să asigure declanșarea de acțiuni automate complexe, ca de exemplu: re-configurare rețea sau re-alocare resurse mașini virtuale pe baza datelor detectate astfel încât să asigure remedierea automată a problemelor de performanță;
- Să asigure monitorizarea apariției unui anumit text în fișiere de jurnal (log) și să asigure declanșarea de acțiuni automate complexe, ca de exemplu: re-configurare rețea sau re-alocare resurse mașini virtuale pe baza datelor detectate în fișierele jurnal (log);
- Să asigure posibilitatea de a determina în mod automat performanța "normală" de funcționare a componentelor de infrastructură monitorizate și să determine modele de funcționare normală bazate pe oră, zi, săptămână etc. De asemenea, soluția trebuie să asigure capacitatea de a genera alarme / evenimente în cazul depășirii valorilor normale de funcționare;
- Să realizeze identificarea configurației hardware și software a serverelor și a stațiilor de lucru și să detecteze automat orice modificare a configurației acestora (modificare configurație hardware, instalare / dezinstalare software etc) cu generarea automată a unei alerte;
- Soluția trebuie să permită administrarea și monitorizarea sistemelor de operare care stau la baza aplicațiilor, bazelor de date, dispozitivelor de rețea din infrastructura IT. În acest sens, va permite colectarea parametrilor de funcționare la nivel de CPU, memorie, intrări/ieșiri, tendințe de utilizare a spațiului de stocare, precum și a proceselor care rulează pe fiecare server / mașină virtuală.
- Toate aceste date vor fi agregate cu datele legate de diverse evenimente, date de monitorizare a aplicațiilor, bazelor de date și infrastructurii de virtualizare pentru furnizarea unei monitorizări globale a performanței aplicațiilor.
- Soluția trebuie să ofere o perspectivă similară (model unificat) a colecțiilor de resurse monitorizate indiferent de sistemul de operare monitorizat.
- Soluția trebuie să asigure capabilități de diagnosticare grafică afișând metrici în timp real și oferind posibilitatea de a naviga la metrici conexe efectuând click pe reprezentările grafice (drill-down).
- Monitorizarea conținutului fișierelor log și să genereze alarme atunci când identifică anumite expresii definite;
- Monitorizarea timpului de răspuns la accesarea diferitelor URL-uri;
- Identificarea blocajelor la nivelul sistemelor de operare prin monitorizarea fluctuațiilor la nivel de procese;
- Prezentarea parametrilor de funcționare (CPU, memorie rețea, utilizare disc) în timp real pentru un număr configurabil de sisteme, astfel încât să ofere o imagine de ansamblu asupra stării de funcționare a infrastructurii IT la nivel de sistem de operare, cu afișarea alarmelor pe diferite niveluri de severitate.
- Soluția trebuie să poată monitoriza platforme eterogene de baze de date – cel puțin bazele de date oferite.
- Soluția trebuie să asigure următoarele funcționalități minime:

- monitorizarea bazelor de date care rulează atât pe infrastructură fizică, cât și pe infrastructură virtuală;
- monitorizarea componentele bazelor de date pentru a asigura funcționarea acestora în limitele capacității resurselor;
- identificarea automată a degradărilor performanței execuției de fraze SQL;
- declanșarea automată de alarme atunci când anumite valori de referință sunt încălcate. În cazul apariției unei alarme, platforma trebuie să asigure declanșarea de acțiuni automate complexe, ca de exemplu: alocare resurse suplimentare pentru baza de date sau configurări / reconfigurări complexe ale bazei de date;
- monitorizarea instanțelor de baze de date din sistem cu ajutorul unei singure instanțe de monitorizare;
- colectarea de date fără necesitatea instalării unui agent local, ci prin agenți la distanță, asigurând astfel un consum minim de resurse – fiind acceptabil un consum de resurse pentru monitorizare de 1% ÷ 3 % CPU;
- mecanism pentru programarea perioadelor de ne-funcționare planificată (ex: mentenanță), în care generarea de alarme va fi suspendată pentru a nu genera alarme false.

Licențierea trebuie să acopere toate cerințele generale și specifice, pentru toate echipamentele furnizate în cadrul contractului. Soluția ofertata va include suport pe o perioada de minim 60 de luni, cu un SLA minim de tip 24x7 asigurat direct de producator.

3.2.5.6 Componenta de gestiune și securizare a accesului

- Soluția trebuie să asigure gestionarea si protejarea conturilor privilegiate impotriva compromiterii acestora si folosirea acestora de atacatori
- Solutia trebuie sa ofere un panou central web pentru gestionarea conturilor privilegiate, care să ofere minim informații privind :
  - gestionarea certificatelor
  - gestionarea grupurilor
  - gestionarea cheilor (SSH)
  - gestionarea conexiunilor
  - generarea si vizualizarea de rapoarte
  - auditarea actiunilor utilizatorilor privilegiati (login, logout), folosirii cheilor, sesiunilor si a certificatelor.
- Solutia trebuie sa ofere un sistem pentru scanarea retelei si descoperirea activelor IT critice si inregistrarea in solutie a conturilor privilegiate folosite de aceste active IT. Solutia trebuie sa fie capabila sa scaneze minim sistemele de operare și virtualizare ofertate, dispozitive de retea si baze de date.
- Solutia trebuie sa foloseasca criptare de tip AES 256, sau echivalent pentru securizarea datelor si credentialelor conturilor privilegiate
- Solutia trebuie sa permita crearea de politici pentru resetarea de parole pentru conturile privilegiate la anumite intervale de timp sau evenimente
- Solutia trebuie sa permita elevarea de privilegii doar pentru un anumit timp

- Solutia trebuie sa gestioneze, monitorizeze si sa crezee conexiuni de tip Windows RDP, SQL, VNC, si SSH/Telnet direct din platforma web catre diverse active IT. De asemenea solutia trebuie sa inregistreze astfel de sesiuni pentru investigatii ulterioare
- Solutia trebuie sa includa un sistem pentru analiza comportamentul utilizatorilor privilegiati pentru detectarea anomaliilor și să utilizeze aceste date pentru a genera modele de baza pentru detectarea riscurilor de compromitere sau furt a unui cont
- Solutia trebuie sa fie capabila sa trimita notificari in cazul in care sunt detectate actiuni si evenimente suspicioase sau anomalii in folosirea conturilor privilegiate.
- Solutia trebuie sa detecteze vulnerabilitati SSL
- Solutia trebuie sa genereze rapoarte cu privire la parole activate sau expirate, utilizatori și acces, GDPR, certificate. De asemenea trebuie sa permita administratorului sau utilizatilor din platforma sa isi extraga rapoarte customizate in functie de nevoi
- Solutia trebuie sa permita exportul rapoartelor in format PDF si EXCEL, precum și trimiterea unui raport pe email
- Solutia trebuie sa permita programarea generarii de rapoarte si trimiterea acestora utilizatorilor selectati
- Solutia trebuie sa auditeze complet toate evenimentele si actiunile ce au loc si sa furnizeze date privind status, evenimente, acțiuni, rezultat.
- Solutia trebuie sa auditeze si monitorizeze toate sesiunele de conexiune incepute de utilizatori (minim conexiune RDP, conexiune VNC, remote) si de asemenea sa permita administratorului sa le blocheze in timp real.
- Solutia tre buie sa auditeze si monitorizeze cheile si certificatele utilizate în sistem si sa furnizeze date complete despre starea acestora.
- Solutia trebuie sa permita crearea sau adaugarea de utlizatori atât manual cât și prin import din fișiere, AD, LDAP sau prin integrare API cu alte sisteme
- Solutia trebuie sa permita configurarea acestor utilizatori cu privilegii si roluri
- Solutia trebuie sa suporte autenficare de tip 2FA
- Solutia trebuie sa permita administratorului sa blocheze sau sa suspende conturi de utilizatori in timp real
- Solutia trebuie sa permita gestionarea de certificate in mod centralizat din consola web.
- Solutia trebuie sa permita adaugarea de resurse IT in platforma prin import, manual sau automat
- Solutia trebuie sa furnizeze o lista toate resursele existente și tipul acestora
- Solutia trebuie sa permita efectuarea urmatoarelor actiuni pe resursele introduse in platforma:
    - Descoperire Resurse
    - Gestionare
    - Configurare
    - Partajare
    - Restrictionare RDP
    - Resetare Parole
    - Asociere Politica Parole
    - Customizare Atribute Resurse

- Exportare Parole

- Solutia trebuie sa permita efectuare urmatoarelor actiuni asupra parolelor si conturilor de utilizatori:
  - Descoperire Conturi
  - Gestionare
  - Configurare
  - Partajare
  - Restrictionare RDP
  - Resetare Parole
  - Asociere Politica Parole
  - Export Parole
  - Asociere Chei
  - Creare si implementare chei
- Solutia trebuie sa suporte integrarea pentru schimb de date folosind API-uri, minim REST API

Licențierea trebuie să acopere toate cerințele generale și specifice, perpetuu, pentru minim 50 de utilizatori. Soluția ofertata va include suport pe o perioada de minim 60 de luni, cu un SLA minim de tip 24x7 asigurat direct de producator.

3.2.5.7 Componenta de integrare, extragere, transformare și încărcare date

Din punct de vedere tehnic, pentru realizarea nevoilor de interconectare și integrare cu sisteme externe, se va utiliza o subcomponentă de integrare aplicatii ce va oferi suport pentru:

- modelarea şi execuţia proceselor de afaceri rezultate ca urmare a orchestrării de servicii standard reutilizabile;
- integrarea sistemelor informatice utilizând o soluţie de tip magistrală de mesaje (Service Bus) cu capabilităţi extinse de conectare la soluţii tehnologice eterogene;
- monitorizarea proactivă a fluxurilor în execuţie prin accesul direct, sub formă de tablouri de control, la indicatorii cheie de execuţie;
- capturarea şi tratarea de evenimente provenite din surse diferite;
- securizarea accesului la serviciile şi fluxurile modelate pe baza unor politici de acces definite şi administrate centralizat.

Această platformă de integrare trebuie să respecte următoarele cerinte:

- Va oferi suport complet pentru dezvoltarea, testarea, execuţia, monitorizarea, optimizarea şi administrarea proceselor de integrare;
- Va oferi suport pentru soluţii moderne şi deschise de integrare conform principiilor şi conceptelor arhitecturilor Service Oriented Architecture (SOA) şi Event Driven Architecture (EDA);
- Va fi bazată pe standardele deschide de interoperabilitate a aplicaţiilor WS-I Basic Profile, WSDL (Web Services Description Language), WS-*, XML, SOAP sau echivalente;
- Va permite modelarea declarativă a proceselor de integrare utilizând standardul OASIS (Organization for the Advancement of Structured Information Standards) BPEL (Business Process Execution Language);
- Va permite comunicaţii sincrone şi asincrone inter-aplicaţii;

- Va oferi mecanisme transparente de persistenţă a stării proceselor şi informaţiilor de audit într-o bază de date relaţională;
- Va permite folosirea canalelor de notificare moderne (email, SMS) pentru informarea utilizatorilor despre evenimentele semnificative apărute în aplicaţii;
- Va suporta transformări şi manipulări de date complexe pentru implementarea logicii proceselor de business;
- Sistemul va include capabilităţi extinse de transformare a mesajelor XML utilizând standarde deschise W3C Extensible Stylesheet Language (XSL), XPath şi XQuery sau echivalente;
- Va oferi soluţii de conectare predefinite la principalele tipuri de tehnologii: baze de date relaţionale, cozi de mesaje (JBossMQ, Oracle AQ, IBM Websphere MQ, MSMQ sau echivalente), sisteme de fişiere, etc;
- Va oferi un cadru de dezvoltare pentru noi soluţii de conectare la sisteme externe bazat pe standarde deschise;
- Va oferi servicii de transport cu suport pentru persistenţa datelor;
- Va oferi servicii de transport cu suport pentru garantarea livrării datelor;
- Va oferi un modul centralizat de gestiune şi aplicare a politicilor de securitate peste portofoliul de fluxuri electronice instalat;
- Va oferi servicii de securitate la nivel de aplicaţie;
- Pentru asigurarea securităţii la nivel transport, soluţia va permite utilizarea protocolul Secure Socket Layer (SSL) şi a certificatelor compatibile X.509;
- Va permite implementarea de servicii de securitate specifice lucrului cu serviciile web standard:
    - autentificarea accesului la servicii;
    - autorizarea accesului la servicii;
- Soluţia va fi bazată pe standardele deschise de securitate a serviciilor web, precum WS-Security, WS-Policy and WS-Security Policy, Security Assertation Markup Language (SAML) sau echivalente;

Platforma trebuie să fie integrată cu serviciile centrale de infrastructură existente ale Beneficiarului, cum ar fi, fără a se limita la:

- Active Directory, LDAP
- DNS
- DHCP
- NTP
- Email

Soluţia va putea securiza totalitatea apelurilor către serviciile existente printr-un mod de funcţionare de tip poartă de acces (gateway) fără să fie necesară modificarea proceselor instalate;

- Să ofere mecanisme de grupare a serverelor în clustere pentru toate componentele platformei de integrare atât în topologii de tip activ-activ cât şi activ-pasiv;
- Posibilitatea stopării temporare a unui nod din cluster pentru mentenanţă şi suport, sistemul în acest timp fiind disponibil pentru activităţi normale;
- Mecanisme de balansare a încărcarii sistemului între resursele administrate în cadrul aceluiaşi cluster;
- Mecanisme de scalare a sistemului pe orizontală (Scale Out).

Serviciile de implementare integrare cu sistemele operaționale vor include, fără a se limita la:

- Analiză, proiectare soluție integrare
- Dezvoltare, configurare, customizare, integrare
- Probe tehnologice, inclusiv testare integrată
- Documentarea interfețelor
- Instalare pe mediile platformei ESB,
- Instruirea personalului de exploatare
- Punere în funcțiune și transfer în operațional
- Platforma va expune un API restfull în care sunt disponibile toate funcţionalităţile de bază ale REGES-ONLINE
- Platforma se va integra cu platformele existente în cadrul Inspecției Muncii, precum și cele menționate ca urmând a fi implementate pentru schimbul de date referitor la funcții și funcționari publici
- în cadrul proiectului se vor implementa interfeţe cel puţin cu toate aplicaţiile Inspecției Muncii şi externe menţionate în acest document.

Indicatori de performanţă necesari pentru interfeţele de integrare:

- Interfeţele sincrone expuse de sistem vor trebui să execute într-un timp maxim de 2 secunde (răspunsul primit de sistemul solicitat pentru a fi dat în termen de 2 secunde după apelul iniţial, inclusiv timpul pentru comunicarea în reţea);
- Interfeţele asincrone (cum ar fi MQ) vor trebui să dea mesajul iniţial de confirmare în timp aproape real (<500ms) şi timpul de executare al fiecărui mesaj va fi de max. 3 sec; în aceste interfeţe numărul mesajelor care aşteaptă să fie procesate nu va fi mai mare de 5000, cu un timp de aşteptare de aprox. 1 oră;
- Interfeţele automate de tip batch vor fi programate pentru executare la un moment convenit cu beneficiarul care nu va afecta performanţa totală a sistemului, respectiv toţi indicatorii de performanţă stabiliţi;
- Pentru interfeţe de tip batch zilnice, timpul de execuţie nu trebuie să depășească 2 ore;
- Pentru interfeţe de tip batch lunare, timpul de execuţie nu trebuie să depășească 5 ore;

Soluția va oferi funcționalități pentru schimbul de evenimente cu sisteme terțe, evenimente ce vor putea fi consumate de acestea, respectiv sistemul va trebui să poată primi mesaje din exterior și declanșa fluxuri corespunzătoare în cadrul REGES-ONLINE. Prestatorul va asigura implementarea integrărilor identificate în etapa de analiză.

Soluția va fi dimensionată pentru cel puțin 16 nuclee. Licențierea va permite acces la update-uri de produs și upgrade-uri de versiuni software, pe o perioada de minim 60 de luni de la recepția platformei.

Prestatorul va configura și va dezvolta funcționalități de integrare care să ofere atât posibilitatea preluării de date din alte sisteme, validarea datelor existente, cât și expunerea unor servicii de transmitere a datelor către alte sisteme.

Integrarea sistemului dezvoltat va fi realizată atât cu sisteme interne cât și cu sisteme externe ale Beneficiarului așa cum sunt menționate în Caietul de sarcini. De asemenea se va asigura interfațarea, integrarea și interoperabilitatea REGES-ONLINE – SIAMC pentru schimbul de date și pentru a asigura mecanisme de autentificare și autorizare comune între cele două sisteme (single sign-on). Astfel, în cadrul proiectului se vor configura interfețele necesare pentru a asigura această intregrare.

Specificațiile detaliate de integrare și interoperabilitate vor rezulta în urma etapei de analiză și în funcție de stadiul de implementare al celorlalte sisteme informatice.

3.2.5.8 Componenta de generare/mascare și administrare a datelor de test

Soluția trebuie să asigure clasificarea și mascarea datelor de test din cadrul sistemului. Soluția trebuie să fie compatibilă cu soluția de baze de date ofertată. Oferta va include demonstrarea compatibilității.

Clasificarea datelor

- La nivelul platformei trebuie să existe metode pre-definite de descoperire a datelor sensibile pentru cele mai uzuale scenarii
- Soluția trebuie să permită adăugarea/dezvoltarea de metode de descoperire a datelor pentru a scana anumite tipuri de date
- Soluția trebuie sa aiba reguli predefinite de detecție și clasificare în funcție de reglementări, minim GDPR, PCI-DSS
- Soluția trebuie să permită adaugarea/dezvoltarea de metode de clasificare a datelor cu caracter personal
- Soluția trebuie să aibă posibilitatea de a atribui etichete / categorii datelor clasificate
- Soluția trebuie să aibă posibilitatea de a gestiona și de a reduce rezultatele fals pozitive
- Soluția trebuie să permită crearea de politici și alerte de clasificare a datelor
- Soluția trebuie să permită exportul rezultatelor scanării în excel / pdf
- Soluția trebuie să permită integrarea cu motorul de mascare – adaugarea de tabele și coloane din modulul de clasificare în modulul de mascare

Mascarea datelor

- Soluția trebuie să ofere mai multe metode de mascare built-in, oferta va preciza metodele suportate
- Soluția trebuie să permita mascarea consistentă a datelor
- Soluția trebuie să pastreze integritatea relaționala (PK-FK)
- Soluția trebuie să aiba capacitatea de a masca indexuri unice
- Soluția trebuie să aiba capacitatea de a adăuga metode de mascare personalizate fără a dezvolta cod
- Soluția trebuie să permită mascarea deterministă pentru coloane complexe
- Soluția trebuie să permită mascarea condiționată
- Soluția trebuie să pemită mascarea bulk (sa permita mascarea similara unui grup de coloane)
- Soluția trebuie să pemită atribuirea automată a metodei de mascare după categorie
- Soluția trebuie să permită repornirea operațiunii de mascare in eventualizatea apariției unei erori în procesul de mascare
- Soluția trebuie sa permita previzualizarea rezultatului operatiunii de mascare.

Soluția ctrebuie să acopere necesarul de clasificare și mascare a datelor pentru mediul de test ofertat, pe toată durata contractului și a perioadei de garanție ofertate. Soluția ofertata va include suport pe o perioada de minim 60 de luni, cu un SLA minim de tip 24x7 asigurat direct de producator.

3.2.5.9 Componenta de securizare pentru prevenirea pierderii datelor

Soluția propusă va permite detectarea și descoperirea datelor senzitive la nivel de rețea, aplicații și endpoint.

Aceasta va fi capabila de a asigura protecția datelor, împiedicând pierderea / înstrăinarea acestora, prin canalele de comunicare email, web, dar si prin dispozitivele de stocare amovibile. Soluția propusa va fi capabila sa analizeze cum sunt folosite datele de către utilizator, oferind funcții de educare a acestuia pentru a lua deciziile corecte privind stocarea, folosirea si transmiterea datelor senzitive. Totodată, soluția trebuie sa fie capabila sa prioritizeze incidentele de securitate in funcție de riscul pe care îl reprezintă.

Sistemul trebuie sa îndeplinească următoarele cerințe si funcționalități:

- Sistemul trebuie să aibă capacitatea de a utiliza o singură politică pentru a scana date ori de câte ori acestea sunt stocate, transmise sau utilizate, atât în rețea, cât și în endpoint si de a aplica automat răspunsul potrivit pentru amenințarea detectată;
- Sistemul trebuie sa dețină o interfață centralizata pentru editarea politicilor și gestionarea politicilor, pentru toate produsele (în cadrul monitorizării și prevenirii rețelei și al endpoint-ului);
- Sistemul trebuie sa permită definirea politicilor pe baza oricăruia dintre următoarele: conținut, expeditor/destinatar, caracteristicile fișierului și protocolul de comunicare;
- Sistemul trebuie sa permită configurarea gravității incidentelor pe baza cantității datelor expuse;
- Sistemul trebuie sa poată accepta reguli de detectare a includerii și excluderii bazate pe datele din serviciile de directoare pentru a aplica politica bazată pe expeditori și destinatar/destinație;
- Sistemul trebuie sa ofere capabilitatea de a implementa politici de detectare predefinite pentru a acoperi reglementările și cele mai bune practici de detectare, inclusiv dicționare predefinite pentru reglementările specifice industriei/tarii;
- Sistemul trebuie sa ofere capabilități identice de detectare pentru toate amenințările acoperite (de exemplu, atât pentru produsele bazate pe rețea, cât și pentru cele finale, dar și pentru monitorizarea și prevenirea exfiltrării datelor, cât și pentru descoperirea și protecția datelor);
- Capacitățile de detectare ale sistemului trebuie sa se poată aplica pentru conținutul limbilor europene și asiatice (japoneză, chineză simplificată, chineză tradițională, chirilică și coreeană);
- Sistemul trebuie sa poată inspecta recursiv conținutul arhivelor comprimate (de exemplu ZIP, TAR, RAR) și sa detecteze conținutul amprentat;
- Sistemul trebuie sa poată face față fișierelor sau atașamentelor foarte mari (20 MB și mai mari) în timpul procesului de detectare a conținutului amprentat;
- Sistemul trebuie sa fie capabil sa își amintească încălcările utilizatorilor în timp și sa creeze incidente atunci când este atins un prag definit;
- Sistemul trebuie sa ofere o metodă pentru amprentarea datelor, cum ar fi înregistrările clienților;
- Sistemul trebuie sa ofere conexiune ODBC la baze de date pentru amprentare;
- Sistemul trebuie sa ofere posibilitatea de a limita privilegiile de acces pentru amprentarea datelor structurate;
- Sistemul trebuie să ofere unelte/modalități de control pentru a valida precizia unei amprente digitale în momentul creării acesteia;
- Sistemul trebuie să permită prin metoda de detectare a datelor cu amprentă să fie specificate ce coloane de date constituie o potrivire per-politică;
- Sistemul trebuie să fie capabil sa facă distincția între diferite tipuri de numere
- Sistemul trebuie să poată limita privilegiile de acces pentru amprentarea datelor nestructurate;

- Sistemul trebuie să ofere măsuri de control pentru a valida precizia unei amprente digitale în momentul creării acesteia;
- Sistemul trebuie să poată acceptă potrivirea conținutului unor documente specifice, cum ar fi codul sursă, documentele de marketing sau cele financiare;
- Sistemul trebuie să permită specificarea de text si expresii șablon care sa poată fi excluse din detecția politicilor si regulilor de DLP;
- Sistemul trebuie sa poată detecta conținutul descris in reguli complet personalizabile cu cuvinte și fraze cheie;
- Sistemul trebuie să poată detecta prezența transmisiilor sau fișierelor criptate;
- Sistemul trebuie să poată accepta detectarea pe baza unui anumit tip de document, chiar dacă expeditorul a modificat extensia de fișier;
- Sistemul trebuie sa fie capabil sa detecteze și inspecteze fișierele de imagine utilizând un motor OCR încorporat în sistemul DLP;
- Sistemul trebuie să poată trimite alerte prin e-mail;
- Sistemul trebuie să ofere posibilitatea de a furniza notificări pe ecran utilizatorilor pentru încălcările politicilor pe endpoint-uri;
- Acțiunile de răspuns automatizate trebuie sa poată fi definite de diferiți parametri, cum ar fi politica încălcată, gravitatea incidentului, numărul de potriviri găsite, protocolul de comunicare utilizat, starea conectată a endpoint-ului și produsul utilizat;
- Sistemul trebuie să ofere funcționalități de automatizare a fluxului de lucru pentru urmărirea remedierii unui incident, minim coduri de stare, atribute, cozi de alocare, gravitate;
- Sistemul trebuie sa poată afișa o indicație clară a modului în care transmisia sau fișierul au încălcat politica în incidentul declanșat, inclusiv identificarea clară a conținutului care a motivat potrivirea;
- Sistemul trebuie să permită vizualizarea informațiilor de identitate despre expeditor și destinația transmiterii
- Sistemul trebuie sa permită deschiderea atașamentelor originale ale unui eveniment direct din interfața de utilizare
- Fiecare utilizator din fluxul de lucru trebuie sa poată fi desemnat să remedieze un anumit set de incidente
- Gestionarii de incidente trebuie sa poată primi notificări automate despre incidentele noi de examinat;
- Sistemul trebuie să ofere capabilitatea de a defini și urmări un „caz” sau un set de incidente care s-au relaționat după o investigație;
- Sistemul trebuie să permită ștergerea incidentelor. Această acțiune va fi înregistrată în jurnalul de audit;
- Sistemul trebuie să permită controlul accesului la incidente pe baza rolului și a politicii încălcate;
- Sistemul trebuie să includă funcția de definire a unui rol care nu are drepturi de vizualizare a informațiilor de identitate pentru a proteja confidențialitatea angajaților;
- Sistemul trebuie să permită crearea de roluri separate pentru administrarea tehnică a serverelor, administrarea utilizatorilor, crearea și editarea politicilor, remedierea incidentelor și vizualizarea incidentelor pentru date în repaus, în mișcare sau la endpoint;

- Soluția trebuie să ofere o metodă de investigare a oricăror modificări neautorizate sau neregulate aduse sistemului;
- Sistemul trebuie să permită ascunderea datelor probatorii (datele tranzacțiilor) în vizualizarea incidentului;
- Sistemul trebuie să permită crearea mai multor utilizatori și atribuirea de diferite roluri acestora;
- Sistemul trebuie sa permită ca autentificarea utilizatorului să fie controlată într-un director extern, minim Active Directory;
- Sistemul trebuie sa permită integrarea cu directoare pentru rezolvarea identității expeditorului sau proprietarului fișierului;
- Arhitectura sistemului trebuie să accepte site-uri la distanță și utilizatori de rețea distribuiți în mai multe locații diferite;
- Sistemul trebuie să permită configurarea și gestionarea tuturor componentelor de rețea printr-o interfață centralizată;
- Sistemul trebuie să ofere o capacitate ridicată de disponibilitate/failover;
- Sistemul trebuie să ofere rapoarte despre traficul de sistem, performanța și valorile de transfer;
- Sistemul trebuie să stocheaze datele și jurnalele capturate într-o bază de date centralizată;
- Sistemul trebuie să permită gestionarea de patch-uri de securitate;
- Sistemul trebuie să permită securizarea orice legătură de comunicare între acesta și endpoint-ul pe care rulează agentul;
- Fiecare conectare la sistem și modificare a politicilor de sistem sau incidentelor trebuie să fie relatate într-un jurnal de audit;
- Sistemul trebuie să ofere o vizualizare generală de tip „tablou de bord” concepută pentru a fi utilizată de directori care pot combina informații din date în mișcare (rețea), date în repaus (stocare) și date la endpoint într-o singură interfață;
- Sistemul trebuie să permită vizualizarea detaliată a incidentului dintr-un raport (de tip drilldown). Aceasta caracteristică trebuie să fie posibilă prin interconectarea și corelareea dintre incidente, politici și rapoarte;
- Sistemul trebuie să permită clasificarea traficul în protocoale fără a se baza pe anumite numere de port;
- Sistemul trebuie s[monitorizeze traficul web, inclusiv poșta web, postările web și alte protocoale utilizând HTTP și HTTPS, inclusiv fișiere încărcate;
- Soluția trebuie să permită monitorizarea/prevenirea imprimării în rețea a informațiilor confidențiale;
- Sistemul trebuie să poată oferi detalii geografice despre site-ul web pentru a rezolva/clasifica destinația transmisiei HTTP/S;
- Soluția trebuie să asigure nativ inspecția comunicațiilor SSL;
- Sistemul trebuie să fie capabil sa blocheaze e-mailurile de ieșire care încalcă politica instituției privind datele confidențiale;
- Sistemul trebuie să fie capabil sa pună în carantină e-mailurile care încalcă politica instituției privind datele confidențiale;
- Sistemul trebuie să permită notificarea expeditorilor și administratorilor de securitate despre un e-mail blocat sau pus în carantină;

- Soluția trebuie să fie capabila sa blocheze conștient conținutul transmisiilor de rețea prin HTTP în mod nativ și sa furnizeze notificări;
- Sistemul trebuie să permită blocarea conținutului sensibil pentru a preveni pierderea confidențială a datelor;
- Sistemul trebuie să permită definirea fișierelor, platformelor, bazelor de date, aplicațiilor și altor dispozitive acoperite;
- Sistemul trebuie să fie capabil să scaneze alte tipuri de ținte, inclusiv depozite personalizate și sa asigure raportarea completă cu privire la încălcările politicii constatate în respectivele depozite;
- Sistemul trebuie să fie capabil să copieze automat fișiere care încalcă politica;
- Sistemul trebuie să fie capabil să pună în carantină și sa șteargă automat fișiere care încalcă politica;
- Sistemul trebuie să includă o modalitate de a informa proprietarii de fișiere despre fișierele în carantină, inclusiv detalii despre motivul pentru care fișierul a fost pus în carantină. Ex: politica pe care a încălcat-o;
- Sistemul trebuie să fie capabil sa afișeze locația fișierului original și detaliile politicii pe care fișierele le încalcă;
- Sistemul trebuie să fie capabil sa se integreze cu serviciile de directoare pentru a permite încălcărilor politicii de date în repaus să fie asociate cu o anumită unitate individuală;
- Sistemul trebuie să furnizeze un raport care să acopere datele în repaus în întreaga organizație;
- Sistemul trebuie să poată oferi o singură interfață de gestionare pentru toate configurațiile și controlul scanării, la nivel de organizație;
- Sistemul trebuie să lase neschimbat atributul „ultimul accesat” al fișierelor scanate pentru a nu perturba procesele de backup ale organizației;
- Sistemul trebuie să accepte scanarea repetată programată automat;
- Sistemul trebuie sa accepte scanarea diferențială pentru a reduce volumul de date de scanat
- Sistemul trebuie sa poată rula mai multe scanări în paralel
- Sistemul trebuie sa poata scana locații la distanță cu lățime de bandă redusă
- Sistemul trebuie sa ofere atât opțiuni de implementare fără agent, cât și pe bază de agent
- Comunicațiile dintre sistem și agent trebuie sa fie criptate
- Soluția de endpoint trebuie sa poata detecta încercările utilizatorilor de a copia date confidențiale pe dispozitive de stocare amovibile (de exemplu, unități USB, dischetă, CD/DVD)
- Soluția de endpoint trebuie sa poata afișa detalii complete despre incident, inclusiv numele fișierului, informațiile utilizatorului, detaliile potrivirii politicii și o copie a fișierului original care a încălcat politica
- Soluția trebuie să poată asigura monitorizarea și protecția continuă a datelor confidențiale, indiferent dacă utilizatorul se află în sau în afara rețelei;
- Soluția trebuie poată monitoriza/proteja utilizatorii la distanță care pot fi deconectați pentru o lungă perioadă de timp sau pot fi conectați numai printr-o conexiune lentă;
- Soluția de endpoint trebuie să poată proteja conținutul confidențial indiferent de tipul de fișier sau de locația fișierului;
- Soluția de endpoint trebuie să poată realiza detectarea bazată pe amprentarea conținutului, chiar dacă endpoint-ul este în afara rețelei instituției;

- Soluția de endpoint trebuie să realizeze actualizări automate ale agenților și modificări de politică fără a necesita instrumente terțe;
- Soluția de endpoint trebuie să permită instalarea acesteia pe sisteme de operare minim Microsoft Windows (32/64) si Apple OS;
- Soluția de endpoint trebuie să asigure agentul împotriva manipulării utilizatorului final;
- Endpoint-ul trebuie să includă un bypass local/la distanță.

Soluția trebuie să asigure descoperirea și protecția datelor senzitive la nivel de rețea, pentru un număr de minim 2.000 de echipamente IT. Soluția ofertata va include suport pe o perioada de minim 60 de luni, cu un SLA minim de tip 24x7 asigurat direct de producator.

3.2.5.10 Portal extern

Portalul extern va fi construit pe o soluție de tip CMS (Content Management System) ce va permite actualizarea și administrarea facilă a conținutului.

Platforma CMS propusă trebuie să asigure minim:

- Publicarea de diferite documente și informații în format cel puțin doc, docx, pdf, png, jpg, formate Excel, formate fișiere audio/video
- Definirea de pagini ale website-ului. Definirea paginilor și a meniurilor trebuie să presupună inclusiv posibilitatea de ștergere/ adaugare/ modificare
- Definirea de meniuri în cadrul website-ului
- Definirea de drepturi de access la meniuri și secțiuni
- Mecanisme de tip WYSIWYG pentru adăugarea și editarea conținutului
- O zona publică, cu informații generale, disponibilă fără autentificare pentru utilizatorii externi
- Posibilitatea de alegere a
- s paletei de culori, imaginilor și altor elemente graficie, statice sau dinamice, în definirea paginilor
- Posibilitatea de editare, adăugare/ștergere/modificare și publicare de noi pagini
- Posibilitatea de definire pagini înistem multi-limbă, cel putin in limbile Română și Engleză
- Posibilitatea publicării conținutului site-urilor prin feed-uri de tip RSS
- Un asistent de creare site-uri ce permite setarea permisiunilor, crearea de șabloane de conținut și adaugarea de teme personalizate
- Un mecanism configurare/scripting de tip linie de comanda pentru administratori.
- Un model programatic și servicii web care să permită personalizarea rapidă și/sau dezvoltarea de noi funcționalități precum si un mecanism dedicat pentru monitorizarea si depanarea solutiilor dezvoltate prin scriere de cod personalizat.
- Securizarea eficientă a site-ului web folosind cele mai noi metode disponibile. Astfel, ofertantul trebuie să asigure rezolvarea a cel puțin celor mai comune probleme fără a se limita la aceste:
    - interfața de administrare a site-ului trebuie să fie protejată cu utilizator și parolă. Fiecare utilizator are drepturi proprii de acces la fiecare modul în parte la nivel de adăugare/editare/ștergere/modificare;
    - modulul de administrare trebuie să fie bazat de roluri, la nivel de acțiune, putând fi ascunse funcționalitățile ce nu sunt permise unui anumit rol;

- Administrarea portalului trebuie să fie realizată în mod simultan de mai multe persoane. Aceste persoane desemnate “administratori” vor avea roluri predefinite, în funcție de preferințe, astfel interfața de administrare a portalului trebuie să permită configurarea drepturilor de acces a persoanelor cu responsabilități în crearea, editarea, ștergerea, aprobarea conținutului sau în administrarea platformei;
- parolele administratorilor trebuie să fie codate în baza de date în baza unui algoritm de codare;
- toate interogările de tip SQL trebuie să fie protejate împotriva injectărilor de tip “sql injection”;
- formularele ce permit introducerea de date sunt validate și sunt securizate cu ajutorul codului CAPTCHA;
- site-ul web trebuie să dispună de functionalități de audit;
- sistemul trebuie să păstreze istoricul modificărilor efectuate (ce utilizator, ce informație si când a adăugat/modificat/șters).
- Zona publică va fi separată de cea de administrare, care va fi accesibilă exclusiv din intranet (URL distinct).
- Soluția va include mijloace de prevenire a atacurilor de tip DoS, SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF) fara a se limita la acestea.
- Preluarea automată de date din surse externe trebuie prevăzută cu un mecanism de verificare și validare a acestora din punct de vedere al securității, iar interacțiunea cu celelalte baze de date se va realiza securizat (configurare network encryption + certificate).

Ofertantul va asigura identificarea și implementarea soluțiilor, cu consultarea prealabilă a beneficiarului.

Oferta va evidenția riscurile și punctele de vulnerabilitate ale soluției. Se vor propune eventuale măsuri adiționale de optimizare a nivelului de securitate si metode proactive în vederea prevenirii si identificării rapide a atacurilor.

3.2.6 REGES-ONLINE

3.2.6.1 Cerințe generale

Sistemul va trebui să permită îndeplinirea obligațiilor angajatorilor conform prevederilor art. 34 din Legea nr. 53/2003, republicată, cu modificările și completările ulterioare – Codul muncii, Hotărârii Guvernului nr. 905/2017 privind registrul general de evidență a salariaților, precum și a actelor normative care vor reglementa activitățile privind registrul general de evidență a salariaților la momentul implementării și pe durata perioadei contractuale de asigurare a mentenanței și suportului tehnic.

Sistemul va pune la dispoziția persoanelor fizice, salariaților și foștilor salariați, posibilitatea vizualizării istoricului propriilor relații de muncă într-un mediu securizat. Astfel, fiecare salariat persoană fizică din România va avea posibilitatea să acceseze sistemul și să fie informat dar și să-și verifice propriile informații. Se va îmbunătăți în acest fel transparența și se va asigura un nivel în plus de validare a informațiilor adăugate de angajatori, de la persoane interesate direct ca informațiile să fie corecte, respectiv de la angajați..

Implementarea registrului general de evidenţă a salariaţilor, REGES-ONLINE:

- Va determina eficientizarea cheltuielilor atât pentru instituțiile publice cât și pentru angajatori, prin crearea unui sistem de lucru unitar va elimina informațiile redundante și va scădea birocrația, va permite utilizatorilor modalități moderne de utilizare și interpretare a informațiilor, permițându-le astfel să ia decizii rapide;

- Va asigura un suport decizional și sporirea numărului de instituții care utilizează informațiile, cu o contribuție benefică în domeniul politicilor salariale și a colectării taxelor, va putea pune la dispoziția autorităților competente informații referitoare la salariile înregistrate, centralizate și în timp real;
- Va permite integrarea sistemului informatic nou creat cu bazele de date deținute de autorități sau instituții publice, cu versiunile precedente ale sistemului REGES/REVISAL sau cu alte surse de date administrative la nivel național;
- Va asigura o îmbunătățire majoră a securității sistemului astfel încât să se asigure un grad ridicat de protecție a datelor.

Pentru asigurarea managementului utilizatorilor și accesului la sistemul REGES-ONLINE, se vor avea în vedere următoarele:

- identificarea în mod unic a fiecărui utilizator în sistem prin crearea de conturi unice și personalizate de acces;
- gestionarea centralizată și unitară a accesului utilizatorilor în sistem prin autorizarea utilizatorilor doar la componentele și modulele funcționale ale sistemului conform cu drepturile de acces și atribuțiile specifice;
- accesul la sistem se va putea realiza doar prin autentificarea utilizatorilor, excepție făcând doar informațiile disponibile în portalul public.

În scopul realizării şi menţinerii unui nivel adecvat de acces la date şi servicii, se vor avea în considerare cel puţin următoarele aspecte:

- cerinţele de securitate ale aplicaţiilor;
- politicile departamentale şi de instituţii publice privind diseminarea informaţiilor;
- cerinţele contractuale şi legale, în vederea protejării împotriva accesului neautorizat la date şi servicii;
- capabilitatea de a solicita utilizatorilor să se identifice unic înainte să le fie permisă orice acțiune în sistem;
- capabilitatea de a înregistra operaţiile/tranzacțiile efectuate de fiecare utilizator autentificat în vederea realizării auditului;
- capabilitatea de a seta durata sesiunii unui utilizator în cazul în care acesta nu mai utilizează aplicaţia, pentru a preîntâmpina accesul neautorizat la sistem a altor persoane;
- capabilitatea de a înregistra evenimente definite de securitate şi de a transmite mesaje de alertă administratorilor de securitate.

Pentru a atinge nivelul de disponibilitate necesar, toate componentele funcționale principale vor fi asigurate în sisteme de tip „cluster redundant”.

Sistemul va dispune de o interfață web în care se va putea completa registrul atât dintr-un browser web obișnuit cât și utilizând dispozitive mobile.

Sistemul va pune la dispoziția micilor angajatori modele de contracte de muncă pe care aceștia le pot utiliza.

3.2.6.2 Cerințe funcționale

Procesele descrise în ceea ce urmează reprezintă o analiză preliminară. Ofertantul devenit prestator va realiza o analiză de business aprofundată în vederea proiectării REGES-ONLINE, luând în considerare legislația în vigoare la momentul implementării contractului. Oferta va include asumarea cerinței de către ofertant.

3.2.6.2.1 Portal extern

Componenta de Portal va asigura principalul punct de acces direct pentru utilizatori și va servi ca principalul mod de informare a vizitatorilor și utilizatorilor.

Prin intermediul portalului se vor putea pune la dispoziție mai multe categorii de conținut:

- informații și noțiuni de bază pentru managementul afacerilor, de interes pentru salariați și angajator cum ar fi:
    - angajarea (ce trebuie să știi pentru a angaja, crearea contractelor)
    - expunerea elementelor de bază (ce trebuie să știi pentru gestionarea contractelor, actelor adiționale, concediilor)
    - siguranța la locul de muncă (ce trebuie să știi despre protecția muncii și siguranța salariaților, raportarea evenimentelor și accidentelor de muncă),
    - gestionarea salariaților (ce trebuie să știi pentru a gestiona problemele la locul de muncă și schimbările de personal)
    - informații pentru tineri (primul loc de muncă, salariul minim, drepturi de bază, condiții speciale, formare profesională, etc.).
- pentru micii angajatori modele de contracte de muncă pe care aceștia le pot utiliza
- știri/anunțuri privind activități/reglementări noi din domeniu
- informări privind aplicația REGES-ONLINE.

În dezvoltarea portalului se vor avea în vedere minim următoarele aspecte de design și funcționale:

- Designul trebuie să fie sobru, elegant si aerisit și să respecte identitatea vizuală a Achizitorului, conform reglementărilor în vigoare pentru design-ul site-urilor guvernamentele
- Interfețele grafice vor oferi utilizatorilor experiențe de navigare coerente, vor fi intuitive si ușor de folosit
- Se va implementa un mecanism de căutare în site-ul web, atât în cadrul structurii și meniurilor cât și a conținutului introdus și indexat
- Prestatorul va prezenta propriile variante de design pentru homepage și pentru paginile de conținut (după perioada de analiză), minim 3 variante, machetele fiind apoi ajustate iterativ pentru a răspunde necesităților proiectului.
- pentru toate temele, imaginile, pozele, icon-uri, widget-uri, flash-uri, filme, etc. utilizate de Prestator (altele decât cele furnizate de autoritatea contractantă) trebuie să existe dreptul legal de utilizare a acestora în acest scop (fie dreptul dezvoltatorului aplicației de a utiliza si redistribui fisierele respective, fie dreptul de autor al acestuia). La momentul livrării Prestatorul va menționa sursa acestora (numele producătorului si datele de contact ale acestuia), și modalitatea achiziționării (copie după factură/contract), după caz. Prestatorul va transfera Achizitorului drepturile de utilizare și reutilizare ori de câte ori va fi nevoie a acestor resurse
- Designul portalului va utiliza soluții de tip one-site, responsive/ adaptive web design (mobile first), urmărind redarea corectă a conținutului pentru utilizatorii diferitelor tipuri de terminale:
    - Mobile (tablete si smartphone), orientate portrait sau landscape;
    - Terminale de tip desktop și laptop;
    - Toată gama de browsere utilizate la nivel mondial, acoperind minimum 90% din numărul total de utilizatori;

- Formatul paginilor va ține seama de necesitatea redării conținutului pentru persoane cu handicap vizual/auditiv (O.U.G. nr. 112 /2018 privind accesibilitatea site-urilor web şi a aplicaţiilor mobile ale organismelor din sectorul public).

In cadrul implementarii se vor realiza minim următoarele servicii de configurare a portalului:

- Crearea și introducerea conținutului pentru toate paginile portalului, conform design-ului agreat
- Implementarea unui unui motor de monitorizare a trafic pentru minim număr vizitatori, de unde acceseaza (județ, țara), număr pagini accesate, statistica pe pagini accesate.
- La crearea paginilor portalului se va avea în vedere respectare a prevederilor OUG 112/2018 privind transpunerea Directivei 2102/2016 privind accesibilitatea site-urilor web și a aplicațiilor mobile ale organismelor din sectorul public, precum și respectarea prevederilor Directivei (UE) 2019/882 a Parlamentului European și a Consiliului din 17 aprilie 2019 privind cerințele de accesibilitate aplicabile produselor și serviciilor. Oferta va prezenta modalitățile concrete prin care se va asigura respectarea cerințelor din această ordonanță.
- Crearea și configurarea rolurilor și gestionarea utilizatorilor pentru adăugarea, administrarea și gestionarea paginilor și conținutului portalului
- Configurarea operațiunilor de back-up/ restore, manual sau programat, atât pentru bazele de date, cât și pentru fișierele core a portalului, conform celor mai bune practici în domeniu

Serviciile de implementare vor include dezvoltarea, instalarea și configurarea portalului extern, precum și încărcarea conținutului inițial, integrarea cu restul componentelor soluției, pentru asigurarea accesului utilizatorilor la sistem sau publicarea informațiilor în conturile utilizatorilor, ca răspuns la solicitările transmise, în funcție de soluția tehnică propusă.

3.2.6.2.2 Aplicație mobilă

Prestatorul va dezvolta și întreține pe durata contractului și a perioadei de suport tehnic și garanției o aplicație de mobil nativă pentru iOS și Andoid. Prestatorul va asigura găzduirea aplicației și disponibilitatea aceteia în magazinele on-line Apple și Google, pe toată durata contractului și a perioadei de suport și garanție ofertate, inclusiv eventualele actualizări necesare în aceasta perioadă pentru respectarea cerințelor tehnice și juridice a celor 2 magazine.

Aplicația va fi disponibilă pentru descărcare gratuită. La finalul perioadei de garanție și suport, Prestatorul va transfera pachetele de instalare, actualizate la ultima versiune, Achizitorului pentru ca acesta să le poată înregistra și găzdui în nume propriu ulterior, dacă va fi cazul.

Aplicația mobilă va asigura minim următoarele funcționalități aferente REGES-ONLINE:

- Înrolarea unui utilizator și asocierea dispozitivului unui cont
- Accesului unui utilizator de tip angajat la datele proprii, formatul datelor fi stabilit în etapa de analiză
- Primirea de notificări din partea sistemului, inclusiv notificări necesare autentificării în 2 pași.

3.2.6.2.3 Pagina de start

Platforma REGES-ONLINE va asigura înrolarea și autentificarea tuturor angajatorilor și beneficiarilor de lucrări*, indiferent de forma contractuală de lucru cu persoanele angajate (contract de muncă sau zilier de exemplu), precum și a angajaților/ persoanelor fizice care interacționează cu Inspecția Muncii / Inspectoratele teritoriale de muncă.

După autentificare, angajatorul sau beneficiarul de lucrări va trebui să poată alege operațiile pe care dorește să le realizeze/ la care are acces, fie operații specifice REGES-ONLINE pentru angajații cu un contract individual de muncă fie operații specifice SIAMC care privesc relațiile de muncă cu zilieri sau alte acțiuni

specifice altor aplicații ale Inspecției Muncii ce relaționează cu angajatorii, beneficiarii de lucrări sau angajații / persoanele fizice care necesită o formă de autentificare și autorizare pentru accesul la servicii IM/ITM.

În acest sens platforma REGES-ONLINE va trebui să asigure:

- O pagină de pornire, sau orice altă soluție tehnică ce asigură ergonomia aplicației, din care utilizatorul să poată selecta acțiunile pe care dorește să le realizeze/ la care are acces con
- Instrumentele pentru autentificarea utilizatorului în aplicațiile terțe ale Inspecției Muncii pentru acțiunile nespecifice REGES-ONLINE, minim sistemul SIAMC
- Documentația tehnică detaliată necesară integrării cu sistemele terțe, în vederea autentificării utilizatorilor și suport pentru prestatorul/prestatorii de servicii care vor dezvolta și implementa sistemele ce necesită integrare.

Notă: în cazul unei organizații care acționează exclusiv ca beneficiar de lucrări nu se va permite accesul la operații specifice REGES-ONLINE.Dacă modul de operare al organizației se modifică și aceasta urmează să acționeze și ca angajator, sistemul va permite autentificarea cu același set de credențiale și accesul reprezentantului organizației și la funcționalitățile REGES-ONLINE.

3.2.6.2.4 Înregistrarea şi autentificarea utilizatorilor

Platforma REGES-ONLINE trebuie să permită înregistrarea și autentificarea utilizatorilor persoane fizice, persoane juridice (persoane fizice, salariați/foști salariați și angajatori prin asumarea de către angajator a atribuţiilor specifice, prin desemnarea unuia sau mai multor angajaţi cărora să le repartizeze, prin fişa postului, atribuţii privind activitatea de resurse umane şi salarizare, prin contractarea unor servicii externe specializate în resurse umane şi salarizare – prestatori profesioniști) cu cel puțin următoarele funcționalități:

- Posibilitatea de înregistrare/înrolare online utilizând o zonă dedicată prin care va fi necesară furnizarea datelor de identificare și contact, de exemplu:
    - Prenume, Nume
    - CNP/Pașaport
    - Adresa de mail validă
    - Nr. de telefon valid
    - optarea pentru una dintre modalitățile de validare a identității solicitantului – prestatorul va implementa toate modalitățile menționate:
        - prezența fizică la ghișeu cu actul de identitate
            - pentru acest caz, operatorul ITM/IM va putea încărca un scan al documentului de identitate prezentat de către solicitant fizic la ghișeu, împreună cu semnătura olografă a acestuia
            - alternativ, utilizatorul își va putea încărca singur documentul urmând ca operatorul ITM să verifice corespondența între documentul încărcat și cel prezent la ghișeu
            - sistemul va înregistra identitatea utilizatorului care a încărcat documentul precum și marcarea validării de la ghișeu a operatorului ITM
        - mecanism automat de verificare prin încărcarea pozei actului de identitate cu identificarea elementelor necesare, a pozelor din mai multe unghiuri/video a persoanei – fără necesitatea intervenției unui operator uman
        - utilizarea unui sistem terț, în care utilizatorul este deja înregistrat și care i-a validat identitatea. Sistemele terțe astfel acceptate trebuie să fie minim: Spațiul Privat

Virtual al ANAF sau Platforma Software Centralizată pentru Identificare Digitală - PSCID

- Integrarea cu Direcția Generală pentru Evidența Persoanelor pentru verificarea datelor personale introduse de către utilizator pentru profilul personal sau a datelor înscrise în registru pentru un angajat
- Integrarea cu baza de dată națională a Inspectoratului Generali pentru Imigrări, cu soluția tehnică identificată în etapa de proiectare a sistemului, pentru verificarea datelor introduse de către utilizator pentru cetățenii străini care se identifică cu pașaport. Autoritatea Contractantă va fi responsabilă pentru încheierea protocolului instituțional în temeiul legii, de colaborare cu IGI.
- Pentru autentificarea utilizatorilor înregistrați cu succes se vor implementa mai multe mecanisme de autentificare de tipul autentificare în mai mulți factori prin:
    - transmiterea unui cod de tip OTP pe adresa de mail sau prin aplicația mobilă
    - posibilitatea de conectare la aplicații de autentificare prin token
    - posibilitatea de verificare a autenticității încercării de conectare de către sistem în funcție de dispozitiv și locație.

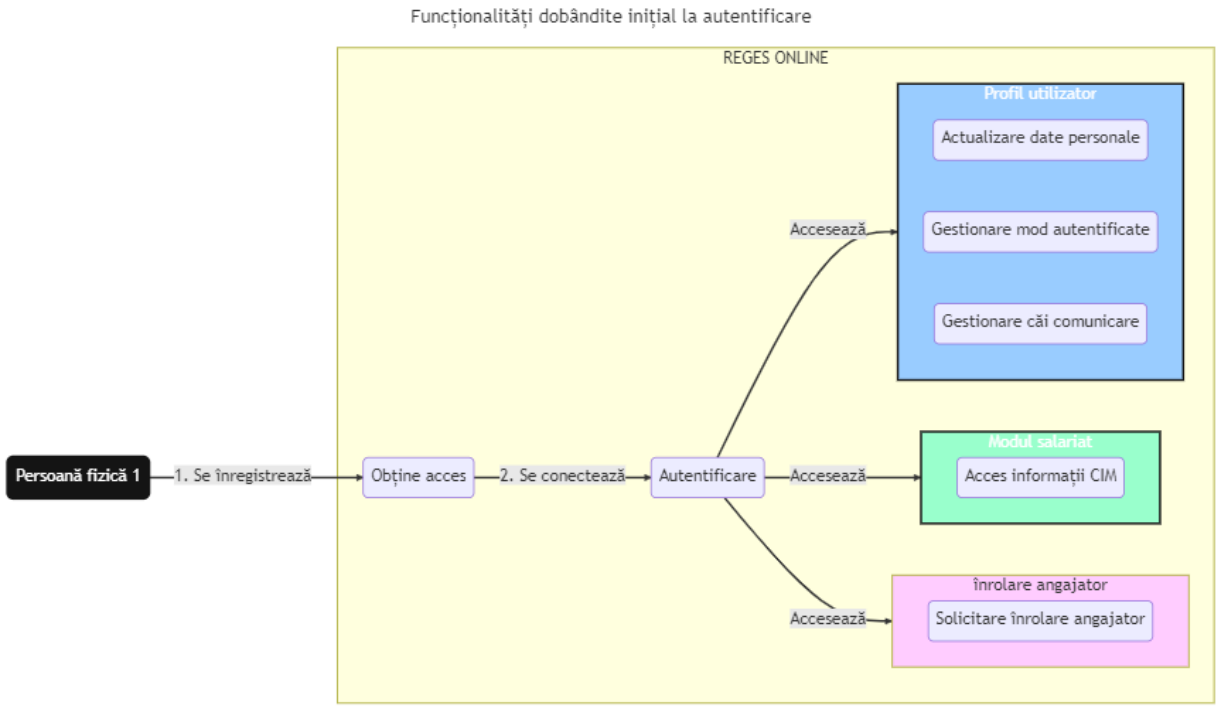
3.2.6.2.4.1 Accesarea funcționalităților REGES-ONLINE

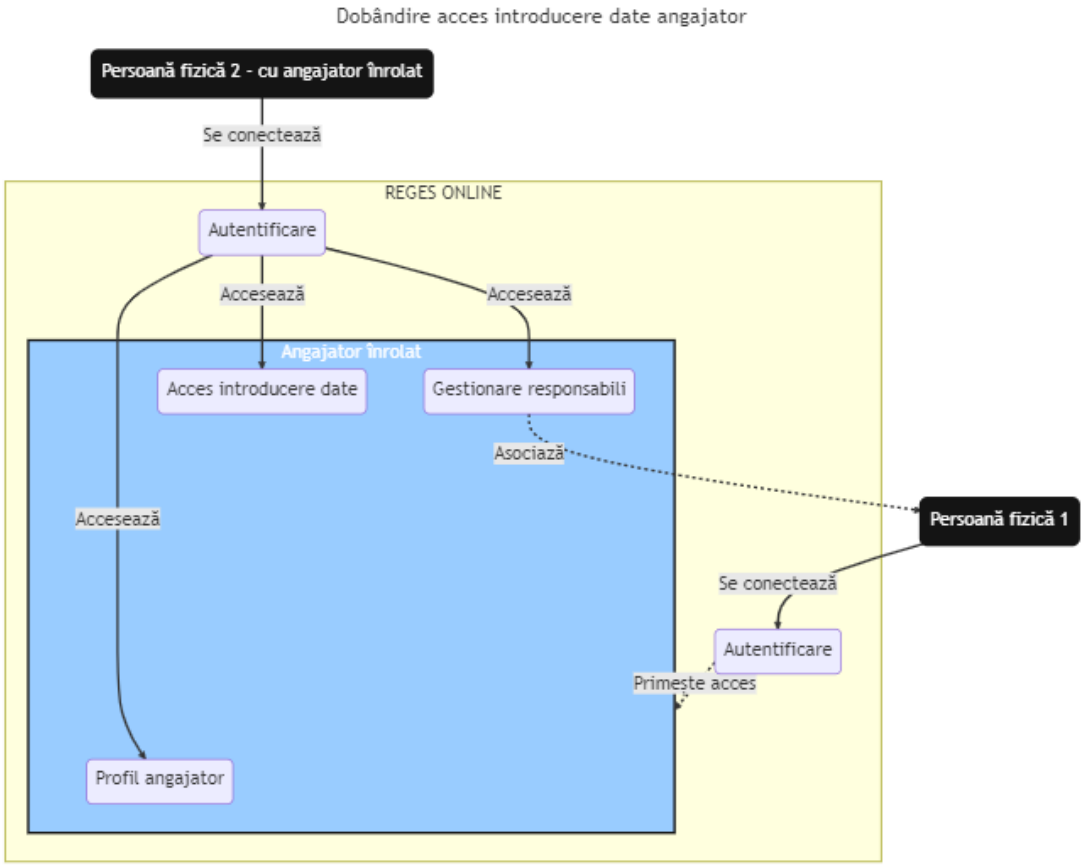
Accesarea funcționalităților REGES-ONLINE va trebuie să poată fi realizată în mod securizat doar de către persoanele înregistrate cu succes, după stabilirea identității utilizatorului.

Un utilizator autentificat cu succes va avea acces în mod implicit cel puțin la următoarele funcționalități:

- Modulul salariat
- posibilitatea de înrolare a unui angajator nou folosind funcționalitățile descrise în Modulul angajator

Posibilitatea adăugării de salariați, contracte de muncă și orice alte informații conexe relațiilor de muncă, va fi dobândit doar în urma asocierii unui utilizatorului cu entitatea juridică corespunzătoare.





3.2.6.2.4.2 Profilul unui utilizator

Utilizatorii autentificați în sistem trebuie să-și poată vizualiza și gestiona minim datele personale, tipul de securitate pentru autentificare dorit precum și preferințele privind modalitatea de autentificare, comunicările primite din partea sistemului, limba de utilizare a sistemului.

Astfel platforma dezvoltată trebuie să dispună de următoarele funcționalități:

- posibilitatea de modificare a datelor din profil
    - pentru schimbarea numelor sau a tipului actului de identitate se va avea în vedere realizarea unei verificări automate minim cu sistemele IT ale Direcției Generale Pentru Evidența Persoanelor, Inspectoratului General pentru Imigrări
- posibilitatea de a stabili dacă dorește autentificare avansată de tip 2FA sau autentificare simplă prin nume de utilizator și parolă
- posibilitatea modificării modalităților de notificare în afara sistemului (email sau aplicație mobilă) șia tipurilor de notificări ce să fie transmise, minim pentru transmiterea codurilor necesare pentru autentificarea în 2 pași (2FA)
- posibilitatea stabilirii limbii în care să fie afișată interfața sistemului pentru utilizator.

3.2.6.2.5 Modul salariat

Scopul modulului este punerea la dispoziția persoanelor fizice, salariaților/foștilor salariați a posibilității vizualizării înregistrărilor/istoricului propriilor relații de muncă într-un mediu securizat. Astfel, fiecare persoană fizică, salariat/fost salariat din România, va avea posibilitatea să acceseze sistemul și să își verifice propriile informații privind relațiile de muncă curente / precedente. Informațiile la care va avea acces salariatul vor fi minim: contractele de muncă și toate operațiunile conexe privind relația de muncă cu angajatorul (detașări, sporuri, acte adiționale, transferuri, încetări etc.). Dreptul de acces se va limita la

vizualizarea, descărcarea şi tipărirea acestor date, precum şi la generarea online şi descărcarea unui extras din registru.

Se urmărește astfel îmbunătățirea transparenței și asigurarea unui nivel suplimentar de validare a informațiilor introduse de către angajatori direct de la persoane interesate - angajați.

Din punct de vedere funcțional acest modul trebuie să asigure minim:

- Posibilitatea vizualizării informațiilor introduse de către angajatori, minim:
    - datele introduse din 2006 conform Hotărârii Guvernului nr. 161/2006 vor fi importate în platformă și vor fi accesibile salariaților sub forma unei arhive electronice
    - datele introduse conform Hotărârii Guvernului nr. 500/2011 și datele înregistrate conform dispozițiilor HotărâriiGuvernului nr. 905 din 2017 – actualul mod de lucru
    - datele noi introduse de către responsabilii angajatorilor utilizând noul sistem REGES-ONLINE, în timp real. În momentul adăugării, modificării, corecției datelor privind un contract de muncă în derulare utilizatorul salariat va fi notificat automat de către sistem asupra operațiunii realizate, conform schemei de notificări selectate
- Posibilitatea vizualizării direct din interfața platformei a istoricului modificărilor asupra unei operațiuni realizate de către angajator, cel puțin în ceea ce privește informații de tip modificare și momentul realizării modificării.
- Posibilitatea de a descărca un extras al datelor introduse de către angajator(i) minim în format .xlsx, .csv, .pdf.
- Vechimea în muncă sau în specialitate poate fi dovedită cu extrasul generat online din registru conform dispozițiilor legale aplicabile
- Se va avea în vedere afișarea în pagina de vizualizare sau de descărcare a extrasului generat online a dispozițiilor legale aplicabile.

3.2.6.2.6 Modul Angajatori

Scopul modulului de angajatori este realizarea operațiilor referitoare la salariați și contracte de muncă la nivel de angajator, în condițiile prevăzute de legislația în vigoare, de către utilizatori desemnați.

Sistemul REGES-ONLINE trebuie să permită îndeplinirea obligațiilor angajatorilor, în conformitate cu prevederile art. 34 din Legea nr. 53/2003, republicată, cu modificările și completările ulterioare – Codul muncii, respectiv în cazul în care există modificări, conform legislației în vigoare la data implementării sistemului și pe durata perioadei de suport tehnic și garanție ofertate.

Astfel, sistemul trebuie să permită:

- înființarea registrului general de evidență a salariaților, la nivel de angajator, prin înregistrarea în sistem a datelor referitoare la aceștia;
- înregistrarea corecției datelor referitoare la angajatori;
- înregistrarea modificării datelor referitoare la angajatori;
- înregistrarea de către angajator a unor înregistrări referitoare la nomenclatoare;
- înregistrarea încetării activității angajatorului;
- vizualizarea istoricului înregistrărilor referitoare la angajator, salariați și contracte de muncă;
- înregistrarea în registrul angajatorilor a datelor referitoare la salariați și contractele de muncă ale acestora;
- preluarea în platformă a tuturor angajatorilor și datele transmise de către aceștia, cu istoric, din baza de date constituită în temeiul dispozițiilor Hotărârii Guvernului nr. 161/2006 privind întocmirea şi completarea registrului general de evidenţă a salariaţilor;
- preluarea în platformă a tuturor angajatorilor și datele transmise de către aceștia, cu istoric, din baza de date constituită în temeiul dispozițiilor Hotărârii Guvernului nr. 500/2011, actualizată;
- credențialele utilizatorilor existenți să fie migrate și asociate entităților de angajatori;
- accesul salariaților sau al foștilor salariați la datele din registru, cu asigurarea măsurilor de protecție a datelor cu caracter personal; vizualizarea, descărcarea şi tipărirea acestor date, precum şi la generarea online şi descărcarea unui extras din registru.

Modulul angajatori REGES-ONLINE va înlocui modul actual de lucru cu aplicația off-line Revisal prin generarea de fișiere .rvs și încărcarea acestora în sistem, toate operațiile urmând a fi realizate on-line, direct în sistem.

În dezvoltarea modulului se vor avea în vedere următoarele principii:

- informarea utilizatorilor
    - sistemul trebuie să afișeze mesaje de informare/atenționare pentru utilizatori în paginile de lucru
    - sistemul trebuie să dispună de un mecanism de transmitere notificări pe baza unor evenimente
    - Mesajele de informare, notificările și regulile în urma căror acestea sunt declanșate nu sunt descrise exhaustiv în prezentul caietul de sarcini ci vor fi stabilite în etapa de analiză
- sprijinirea verificării corectitudinii datelor colectate. Sistemul trebuie să sprijine verificarea datelor introduse de către utilizatori prin cel puțin următoarele mecanisme:

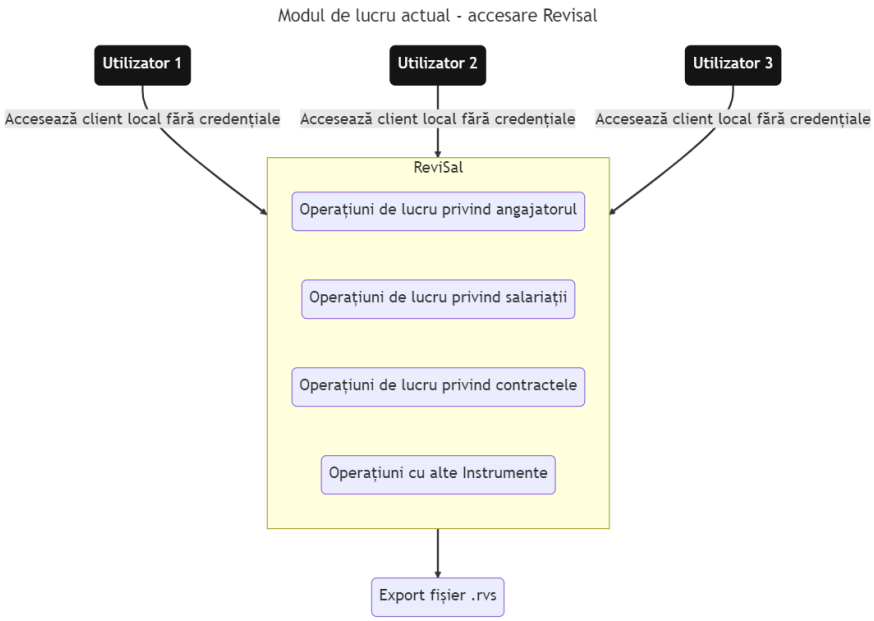
- integrarea cu sistemele informatice minim ale Direcției Generale Pentru Evidența Persoanelor, ONRC, IGI și ANAF, pentru furnizarea datelor de identificare ale entităților (persoane și angajatori) în scop de verificare a a datele introduse în sistem
- reguli de verificare și validare atât pentru formatul câmpurilor (ex. CNP, date) cât și din punct de vedere a succesiunii evenimentelor și constrângerile existente în legislație de exemplu: (introducerea unui spor/act adițional la un contract de muncă să poată fi realizate doar în perioada de valabilitate a contractului de muncă în vigoare)

- transparența privind informațiile introduse
  - informațiile introduse sau generate în cadrul modulului vor putea fi accesate, transmise, editate, corectate/modificate și exportate în timp real la solicitarea utilizatorului prin interacțiunea cu platforma în urma autentificării
  - toate operațiunile realizate de către utilizatori să fie jurnalizate în sistem – iar accesul la aceste informații să se poată face de către ceilalți utilizatori (operatori IM/ITM și useri externi cu acces pe baza unui protocol încheiat în temeiul legii) în funcție de nivelul de acces.

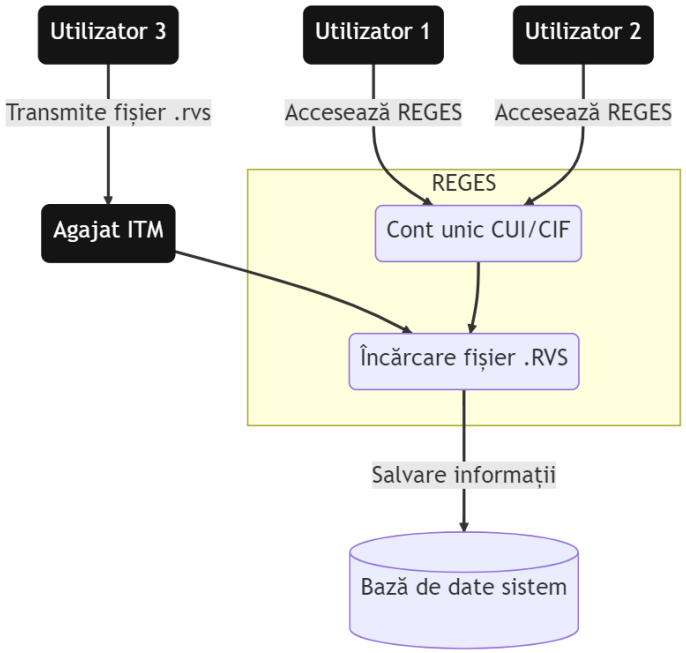
3.2.6.2.6.1 Accesul angajatorilor la REGES-ONLINE

Se urmărește ca REGES-ONLINE să asigure atât transparența cât și responsabilizarea utilizatorilor care introduc sau gestionează datele din sistem. Astfel pentru a se putea realiza managementul utilizatorilor și accesului la sistemul REGES-ONLINE, se vor avea în vedere următoarele:

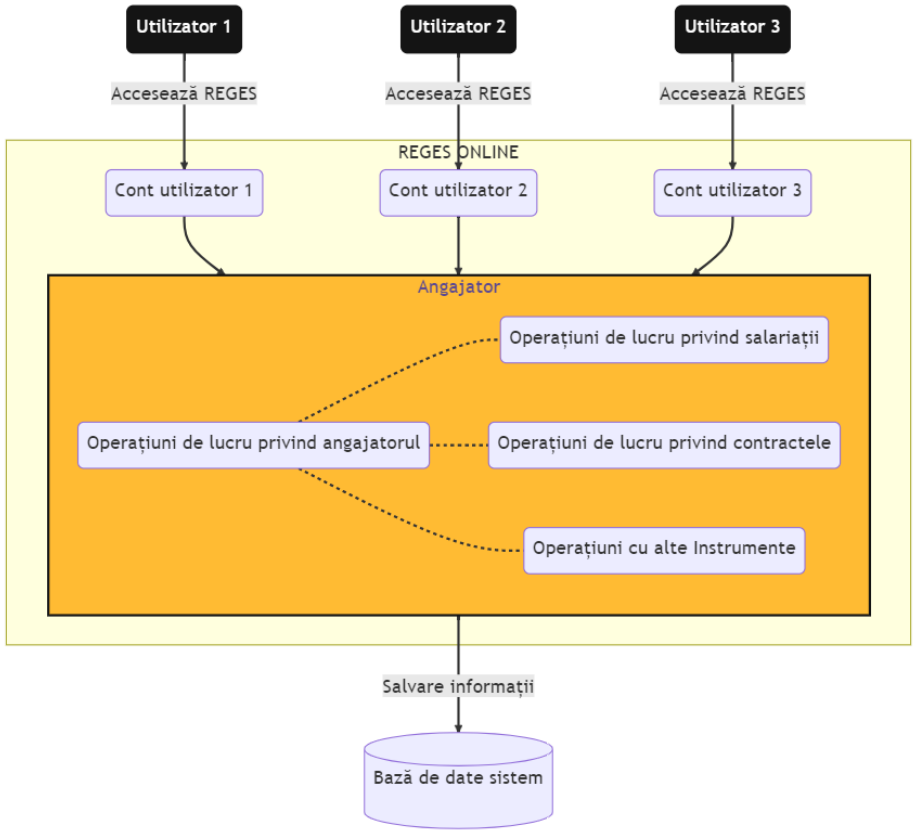
- identificarea în mod unic și nominal a fiecărui utilizator în sistem prin crearea de conturi nominale de acces – procesul de introducere/colectare a datelor nu se va mai putea realiza prin intermediul unor conturi impersonale bazate doar pe CUI/CIF și partaje de mai multe persoane;
- gestionarea centralizată și unitară a accesului utilizatorilor în sistem prin autorizarea utilizatorului doar la componentele și modulele funcționale ale sistemului conform cu drepturile de acces și atribuțiile specifice;
- toate procesele de introducere sau gestionare a datelor se va putea realiza doar de către utilizatori autentificați și autorizați, excepție făcând doar informații de interes public disponibile pentru publicul larg.



Modul de lucru actual - accesare REGES



Modul de lucru dorit REGES - ONLINE



3.2.6.2.6.2 Migrarea conturilor angajatorilor existenți

REGES-ONLINE trebuie să permită migrarea conturilor angajatorilor existenți, minim:

- Preluarea în platformă a tuturor entităților de angajatori și datele introduse de către aceștia în sistemul actual, la trecerea în producție a REGES-ONLINE și înlocuirea sistemului actual cu acesta;
- Credențialele utilizatorilor existenți de forma (CUI/CIF parolă) să fie migrate și asociate entităților angajatori corespunzătoare având în vedere următoarele:
    - acest tip de utilizator va fi folosit doar pentru migrarea la noul mod de lucru folosind conturi nominale pentru toți utilizatorii – nu se vor putea realiza operațiuni de introducere/modificare date privind salariații și contractele de muncă cu acest nivel de acces
    - utilizând acest tip de credențiale – angajatorii trebuie să își poată asocia firmei primul cont de tip utilizator nominal, care ulterior să poată gestiona organizația, datele și utilizatorii asociați acesteia
    - conturile nominale reprezintă un tip de utilizator nou care va urma procesul de înrolare comun cu cel al salariaților/angajaților – un utilizator putând fi în același timp salariat/angajat cât și persoană desemnată să gestioneze date pentru unul sau mai mulți angajatori, accesul la aceste funcționalități se va acorda numai prin asocierea utilizatorului la entitatea angajator respectivă
- pentru situațiile în care există angajatori care au pierdut datele de acces ale acestor conturi generice să existe un mecanism de regenerare/recuperare parolă disponibil direct în REGES-ONLINE. Având în vedere faptul că pentru aceste conturi nu există adrese de e-mail în sistem va fi identificată în etapa de analiză procedura de lucru IM/ITM necesară pentru a stabili modalitatea de solicitare/resetare a parolei.

3.2.6.2.6.3 Înrolarea angajatorilor noi

Procesul de înrolare a unui nou angajator (altul decât cei de la cap 3.2.6.2.3.2) trebuie să poată fi realizat integral online, urmând porcesul descris mai jos, sau un proces echivalent care poate fi identificat în etapa de analiză derulată de Prestator:

(a) <u>Inițierea procesului de înrolare de către un angajator</u>

- solicitantul creării unei noi entități de angajator trebuie să fie autentificat în sistem folosind contul nominal personal
- platforma va permite ca utilizatorul astfel conectat să acceseze o secțiune specifică înrolării noilor angajatori
- solicitarea de înrolare se va realiza prin completarea unui formular web. La completarea și/sau salvarea formularului vor fi utilizate mecanisme de verificare și validare a datelor atât prin definirea unor reguli privind unicitatea datelor introduse la nivelul platformei cât și prin integrarea cu Direcția Generală Pentru Evidența Persoanelor, ONRC și ANAF, IGI, pentru validarea informațiilor specifice angajatorului furnizate de aceste instituții, precum și cu Registrul Național al ONG-urilor de pe lângă Ministerul Justiției (fundații, asociații, persoane juridice străine, federații, uniuni)
- platforma va solicita și va permite încărcarea documentelor justificative conform legislației în vigoare – documentelor încărcate vor fi semnate cu semnătură electronică extinsă (semnătură electronică avansată, semnătură electronica calificată), semnătură ce va fi verificată de sistem la încărcare
- la transmiterea solicitării aceasta trebuie să fie înregistrată de către sistem. Numărul de înregistrare va fi afișat în profilul utilizatorului cât și comunicat printr-o notificare pe adresa de email a acestuia. Solicitarea va fi transmisă automat către ITM-ul responsabil, determinat de adresa câmpului de domiciliu/sediu social a angajatorului.

(b) Procesarea solicitării de înrolare de către ITM

- Platforma trebuie să permite definirea de grupuri de utilizatori asociate fiecărui Inspectorat Teritorial de Muncă (ITM), cu minim următoarele funcționalități:
    - gestionarea grupului de utilizatori căruia i se va conferi accesul de preluare a solicitărilor de înrolare trebuie să poată fi realizată de către utilizatorii ITM autorizați în acest sens de către administratorii REGES-ONLINE
    - prin intermediul sistemului de roluri de permisiuni platforma trebuie să permită configurarea a cel puțin 2 niveluri de acces pentru această activitate:
        - operator (responsabili nominalizați conform fișei postului)
        - coordonator (șef de serviciu, conducător departament etc.)
    - Platforma trebuie să le permită utilizatorilorilor ITM desemnați:
        - vizualizarea listei de solicitări primite cu toate detaliile aferente
        - posibilitatea de preluare a solicitării direct de către operator și/sau de nominalizare a persoanei responsabile de către coordonator
        - verificarea datelor introduse și a documentelor încârcate
        - aprobarea/respingerea/solicitarea de clarificări după caz
            - aprobarea presupune acordarea accesului utilizatorului solicitant de a gestiona activitatea entității de angajator
            - solicitarea de clarificări, care presupune:
                - posibilitatea de a completa un mesaj cu motivul solicitării de către operatorul ITM și transmiterea acestui mesaj atât prin sistemul de mesagerie/ notificare intern sistemului cât și prin email
                - posibilitatea utilizatorului de a completa un mesaj de răspuns și a încărca documente justificative, dacă este cazul, urmând ca sistemul să notifice operatorul cu privire la primirea răspunsului
                - posibilitatea de a relua procesul de solicitare/răspuns la clarificări ori de câte ori este nevoie până la rezoluția finală a solicitării (aprobare sau respingere)
            - în cazul unei respingeri utilizatorul trebuie să poată relua procesul de înrolare pentru entitatea angajatoare, noua solicitare primind un număr de înregistrare distinct.

3.2.6.2.6.4 Gestionare profil angajator

Platforma va permite ca în urma înrolării și asocierii utilizatorului cu entitatea angajatoare, acesta să poată gestiona profilul entității de angajator cel puțin prin:

- Modificarea datelor aferente entității angajatoare, prin încărcarea documentelor justificative privind modificarea operată
- Corecția datelor aferente entiății angajatoare – pentru situațiile în care au fost realizate erori umane
- Un mecanism de verificare periodică a entității angajatoare cu surse externe, minim Direcția Generală Pentru Evidența Persoanelor ,ONRC, ANAF, și/sau alt sistem care gestionează registre naționale relevante, în urma căruia să se afișeze o informare în profilul angajatorului în cazul în care este necesară actualizarea datelor entității în REGES-ONLINE pentru alinierea cu datele existente în aceste sisteme.

3.2.6.2.6.5 Vizualizare istoric angajator

Toate operațiunile efectuate asupra unei datelor unei entități angajator, precum și a datelor privind contractele de muncă asociate entității angajator, vor fi jurnalizate în sistem cu mimim următoarele informații:

- tipul operațiunii
- data operării
- utilizatorul care a efectuat modificare
- posibilitatea de a vizualiza integral versiunile anterioare a înregistrării

Platforma trebuie să permită ca istoricul operațiunilor realizate de către utilizatori să fie vizualizat direct în interfață de către utilizatorii cu acest drept, respectiv utilizatorii asociați angajatorului și operatorii ITM.

3.2.6.2.6.6 Gestionare nomenclatoare specifice

Platforma va permite ca pe lângă seturile de date uzuale și predefinte la nivelul sistemului, conform nevoilor identificate în etapa de analiză, utilizatorii asociați unei entități angajator să-și poată adăuga și gestiona propriile seturi de date specifice, de exemplu lista de sporuri, indemnizații și alte adaosuri specifice acestuia.

3.2.6.2.6.7 Încetarea activității angajatorului

Platforma trebuie să ofere posibilitatea de a declara încetarea activității angajatorului de către utilizatorul cu drept de admnistrare a entității angajator respective. Procesul de formalizare a încetării activității angajatorului în platformă, prin inactivare sau arhivare, va fi stabilit în etapa de analiză în vederea proiectării sistemului.

3.2.6.2.6.8 Gestionarea datelor salariaților și a contractelor de muncă

Pentru gestionarea datelor salariaților platforma trebuie să ofere minim următoarele funcționalități și pași de control:

- adăugarea unui salariat trebuie să fie condiționată de adăugarea unui contract de muncă
    - formularul de colectare date a datelor privind salariatul va conține elemente de identificare pentru care se vor stabili reguli de validare privind unicitatea, de respectare a formatului solicitat precum și posibilitatea de verificare a corectitudinii datelor introduse prin integrarea cu sistemul IT al Direcției Pentru Evidența Persoanelor
        - Platforma trebuie să dispună de un mecanism de verificare perioadică în urma căruia să afișeze informări în pagina salariaților unui angajator în cazul în care survin modificări în sistemul Direcției Pentru Evidența Persoanelor, cum ar fi de exemplul marcarea shimbării numelui unei persoane
    - pentru facilitarea procesului de adăugare a unei înregistrări de tip salariat, ori de câte ori este posibil, platforma trebuie să poată calcula și completa automat anumite informații în baza datelor introduse de către utilizator (de exemplu sexul și vârsta în baza CNP-ului)
    - pentru cetățenii străini - aceștia se vor identifica printr-un câmp dedicat în baza unui nomenclator privind cetățenia. Pentru aceștia înregistrarea inițială în platformă se va putea realiza pe baza pașaportului. Platforma va permite modificarea pașaportului cu actul de identitate (ulterior primiri actului de identitate de către angajator – proces realizat offline)
    - pentru cetățenii identificați ca străini de către sistem vor exista reguli și atenționări specifice – de exemplu în lipsa CNP-ului platforma să afișeze o atenționare în urma verificării zilei de naștere și a numelui astfel încât utilizatorul să fie atenționat privind posibilitatea dublării datelor

- modificarea și corecția datelor pentru salariați – aceste operațiuni trebuie semnalizate și jurnalizate diferit:
    - modificarea presupune actualizarea datelor de identificare ale salariatului din motive obiective (ex. schimbare act identitate)
    - corecția presupune îndreptarea de erori materiale, platforma trebuind să înregistreze motivul alterării datelor
- radierea salariaților și/sau contractelor – radierea presupune ștergerea logică din sistem a unui salariat, functionalități de corecție cu rol EXCLUSIV de marcare ca ERONATE a unor înregistrări de contract și/sau salariat care NU aparțin angajatorului considerat și care fac parte din componența registrului acestuia ca urmare a unor erori de operare. Înregistrarile radiate sunt blocate pentru orice operațiune de actualizare, acestea putând fi regăsite și vizualizate numai prin functionalitățile de vizualizare asociate contractelor/salariaților (Lista contracte, Lista salariați, Istoric contract, Istoric salariat).
- vizualizarea listei de salariați cu posibilitatea de a realiza operațiuni de căutare, sortare și filtrare pe baza mai multor criterii precum și exportul listei în format .xlsx, .csv și .pdf
    - posibilitatea de vizualizare și generare de către sistem, pe baza unor șabloane prestabilite a *Registrului de salariați* și *Raportului de salariat* în format .xlsx, .pdf și .docx
        - Beneficiarul va furniza șablonul/formatul acestor document precum și datele pe care trebuie să le conțină
        - Registrul de salariați trebuie să poată fi generat fie integral pentru toți salariații fie doar pentru cei selectați în urma realizării operațiunilor de căutare, sortare și filtrare a liste salariaților după criteriile stabilite în etapa de analiză

Pentru gestionarea contractelor de muncă sistemul trebuie să permită minim:

- <u>Adăugare contract</u> prin:
    - completarea formularului de colectare date ce va conține elemente de identificare pentru care se vor stabili reguli de validare privind unicitatea și de respectare a formatului solicitat precum și atenționarea în momentul în care se adaugă un contract nou pentru un salariat existent în baza de date – cu informare asupra verificării și actualizării datelor acestuia – dacă este cazul
    - Posibilitatea de a modifica sau corecta datele unui contract astfel:
        - modificarea se va putea realiza doar prin menționarea a minim nr/data si tipului documentului în baza căruia s-a realiza modificarea
        - corecția care presupune îndreptarea de erori materiale, platforma trebuind să înregistreze motivul alterării datelor.
- <u>Transfer salariat/contract</u> – platforma trebuie să permită raportarea operațiunilor de transferare a contractelor de muncă de la un angajator la altul pentru situațiile de transfer, mutare, schimbare gestiune, cesiune, fuziune etc. prin
    - completarea datelor de identificare ale angajatorului către care se transferă salariații/contractele, împreună cu date de începere și nr/tipul deciziei
    - notificarea de către sistem a responsabililor angajatorului către care se transmite solicitarea transferului
    - posibilitate de a accepta sau respinge prin selectare individuală a unui, mai multor sau a întregului grup de angajați/contracte solicitate pentru transfer

        - acceptarea va presupune completarea sau actualizarea unor informații obligatorii pentru formalizarea mutării în gestiunea celui căreia către se transferă (de ex. nr. Contract)
        - acceptarea și respingerea integrală/parțială vor presupune înștiințarea angajatorului care a solicitat transferul printr-o notificare transmisă automat de către sistem
        - respingerea va presupune păstrarea în gestiune a salariaților/contractelor solicitate – acestea având starea anterioară transferării
- Suspendare contract și operațiuni conexe (încetare, corecție, modificare, anulare și corecție suspendare contract)
    - Operațiunile de încetare a suspendării, modficare a suspendării, anularea suspendării, se vor realiza prin:
        - selectarea contractului ce urmează a fi suspendat
        - completarea informațiilor specifice operației, minim Temei, nr/dată tipul, date de început și sfârșit a suspendării. Datele complete introduse pentru aceste operații vor fi validate de sistem prin configurarea unui set de reguli ce vor fi stabilite în perioada de analiză.
    - Operațiunile de corecție vor permite îndreptarea datelor în cazul unor erori umane dar se vor supune regulilor de validare stabilite pentru celelalte operațiuni privind suspendarea unui contract
- Detașare contract și operațiuni conexe (încetare, corecție, prelungire, anulare și corecție încetare)
    - Detașarea va presupune crearea unui legături logice intre angajatorul care detașează și angajatorul către care se detașează cu posibilitatea de vizualizare a listei angajaților detașați și din profilului angajatorului la care se face detașarea astfel:
        - lista angajaților detașați va oferi opțiuni de căutare, filtrare sau sortare
        - modalitatea de realizare a acestei legături logice, va fi stabilită în perioada de analiză în vederea proiectării sistemului
    - Adăugarea unei detașări trebuie să se poată realiza prin menționarea angajatorului care va acorda drepturile cuvenite salariatului și a nr/data tip actului în baza căruia se face detașarea si modificarea
    - Operațiunile privind detașarea unui contract se vor realiza pe baza unui set de reguli ce vor fi stabilite in perioada de analiză. Un exemplu de astfel de regulă ce va trebui să fie validată de sistem la inițierea unei detașări: detașarea inițială se poate realiza pentru maxim 12 luni, cu posibilitatea de prelungire la maxim 6 luni (și apoi din 6 în 6 luni).
        - platforma trebuie să notifice responsabililor angajatorului și pe angajat cu privirea la apropierea termenului de încetare a detașării conform regulilor astfel definite
    - Încetarea unei detașări se va putea realiza doar în baza unui document justificativ, angajatorul fiind obligat să intrudcă detaliile privind documentul în sistem, minim nr/data/tipului actului. Lista va fi revizuită în etapa de analiză și proiectare a REGES-ONLINE
    - În mod similar anularea încetării unei detașări se va putea realiza doar prin introducerea unui motiv sau menționarea unui document justificativ, minim nr/data/tipului actului
- Încetare contract și operațiuni conexe (anulare, corecție, reactivare, corecție reactivare)
    - încetarea unui contract va fi posibilă doar pentru contractele active
    - la încetarea unui contract se vor completa o serie de informații specifice, minim temei, nr/data, tip document

- pentru contractele pe perioadă determinată sistemul va notifica angajatorul și angajatul cu un anumit nr. de zile înainte de încetarea/expirarea contractului
- la anularea încetării – se va solicita minim motivul anulării cu introducerea nr/tipului documentului justificativ pentru operarea modificării
- pentru reactivarea contractului sistemul va solicita nr/data – documentului justificativ pentru realizarea înregistrării

- Radierea contractului presupune ștergerea logică a contractului dar cu păstrarea în listă a contractului cu statusul radiat și a istoricului acestuia (tip modificare, momentul realizării modificării și utilizatorul care a efectuat operațiunile).
  - Platforma va afișa o informare/avertizare utilizatorului privind faptul că radierea se realizează doar asupra operațiunilor introduse greșit
- Schimbare gestiune registru
  - schimbarea gestiunii registrului se referă la transferul responsabilității de gestiune între două entități ale aceluiași angajator – ca o consecință a luării deciziei de delegare/revocare a competenței pentru una sau mai multe unități ale angajatorului fără personalitate juridică (sucursală, agenție, reprezentanță)
  - astfel platforma trebuie să permită entității angajator centrale de a putea gestiona drepturile/capacitățile de gestiune ale contractelor pentru entitățile arondate/sucursale
  - Descentralizarea sau centralizarea gestiunii atrage după sine și responsabilitatea privind eliberării extraselor privind istoricul declarat al muncii pentru salariați
  - În etapa de analiză se va identifica și implementa și posibilitatea modalității de eliberare a extrasului centralizat – de către personalitatea juridică centrală – utilizând datele introduse și de către entitățile arondate

Toate operațiunile (inclusiv radierea) asupra unui salariat sau a unui contract de muncă vor fi jurnalizate în sistem cu minim următoarele informații:

- tipul operațiunii
- data operării
- utilizatorul care a efectuat modificare
- posibilitatea de a vizualiza integral versiunea anterioară

Sistemul trebuie să permită ca istoricul operațiunilor realizate de către utilizatori să fie vizualizat direct în interfață de către utilizatorii cu acest drept, respectiv utilizatorii asociați angajatorului și operatorii ITM.

Asupra listei contractelor trebuie să se poată realiza operațiuni de căutare, sortare și filtrare pe baza mai multor criterii, stabilite în etapa de analiză, precum și exportul listelor în format minim .xlsx, .csv și .pdf.

Din punct de vedere al jurnalizării sistemul va oferi o funcționalitate de tip Istoricul unui contract care va permite vizualizarea istoricului contractului/contractelor unui salariat.

3.2.6.2.6.9 Gestionarea automată a datelor salariaților și a contractelor de muncă

REGES-ONLINE va oferi instrumente pentru gestionarea automată, securizată, a datelor salariaților și contractelor de muncă prin intermediul componentei de integrare date / API/ sau alta metoda identificată în etapa de analiză în funcție de soluția tehnică propusă.

Prestatorul va asigurarea programarea instrumentelor de integrare, documentarea acestora și suport pentru angajatorii care aleg să utilizeze aceasta modalitate de gestionare a datelor pe durata implementării contractului și a perioadei de suport și garanție. Prestatorul va asigura actualizarea continua a instrumentelor de integrare corelat cu actualizările REGES-ONLINE pe durata perioadei de suport și garanție ofertate.

Sistemul va asigura jurnalizarea actualizărilor realizate prin instrumentele de integrare.

3.2.6.2.7 Modul de evidență și control

Scopul modulului de evidență și control este de a sprijini activitatea de zi cu zi a inspectorilor de muncă IM/ITM.

Modulul de evidență și control ce urmează să fie dezvoltat în REGES-ONLINE va înlocui modul actual de lucru cu aplicația online REGES.

În dezvoltarea modulului se vor avea în vedere următoarele principii:

- confidențialitatea datelor – accesul la datele privind angajatorii, salariații și contractele de muncă se va putea face securizat numai de către utilizatorii autorizați în acest sens
- trasabilitatea accesării datelor – activitatea inspectorilor de muncă cu datele de natură sensibilă, fie că este vorba despre de evidență sau control trebuie să poată fi justificată cu sursa sarcinii de lucru: minim solicitări de la alte instituții, pregătirea planului de control, interogări necesare activității de control în teren, precum și alte verificări ad-hoc punctuale, platforma înregistrând acest motiv
- utilizatorul care a accesat, IP și momentul în timp (zi, data, ora, minut, secunda)

3.2.6.2.7.1 Funcționalități principale pentru utilizatorii angajați IM/ITM

Angajații Inspecția Muncii și ai Inspectoratelor Teritoriale de Muncă vor avea acces la sistem în special pentru:

- Verificarea și validarea solicitărilor de înrolare a noilor angajatori.
- Realizarea de interogări în funcție de specificul activității – de monitorizare evidență și control.

3.2.6.2.7.2 Gestionarea accesului utilizatorilor angajați IM/ITM

Platforma trebuie să permită ca accesul la informații, de către utilizatorii Inspecției Muncii și ai Inspectoratelor teritoriale de muncă – denumiți în continuare *Operatori,* să se realizeze în mod granulat, pe nivele de acces.

Astfel, platforma trebuie să permită gestionarea nivelelor de acces printr-un sistem de roluri, permisiuni și grupuri gestionabil direct de către utilizatori administratori ai Inspecției Muncii și ai Inspectoratelor teritoriale de muncă, din interfața aplicației.

Mai multe detalii privind cerințele funcționale de gestionare a accesului în aplicație sunt detaliate în Modulul de Administrare,

3.2.6.2.7.3 Procesarea solicitărilor de înrolare a noilor angajatori

Platforma trebuie să asigure operatorilor cu acest nivel de acces o zonă de lucru dedicată procesării solicitărilor de înrolare a noilor angajatori cu următoarele funcționalități:

  - afișarea solicitărilor trimise într-o listă cu posibilitatea de căutare, sortare și filtrare după mai multe criterii și cu posibilitatea de export. Solicitările vor putea fi vizualizate la nivelul fiecărui ITM, pe baza domiciliului/sediului completat de către utilizator în formularul de solicitare

- posibilitatea de a administra procesul de distribuire a solicitărilor într-un mod flexibil cel puțin prin:
  - preluarea solicitărilor direct de către operatorii care vor analiza și procesa solicitarea
  - alocarea/nominalizarea de către un utilizator cu drepturi de coordonare a operatorilor la solicitări
- posibilitatea de a verifica datele introduse de către solicitant în formularul web atât prin inspecție vizuală cât și prin utilizarea integrărilor cu minim sistemele IT a Direcției Generale Pentru Evidența Persoanelor, ONRC și ANAF, IGI și Registrul Național al ONG-urilor de pe lângă Ministerul Justiției (fundatii, asociatii, persoane juridice straine, federatii, uniuni)
- posibilitatea de a consulta documentele încărcate de către solicitant

- posibilitatea de a formaliza procesarea solicitării cu următoarele rezoluții:
    - Aprobare – caz în care i se va permite accesul utilizatorului de tip persoană nominală să gestioneze entitatea de angajator
    - Solicitare de clarificări - în cazul în care documentele încărcate nu corespund criteriile de verificare aferente procedurii de lucru
        - Solicitarea de clarificări și răspunsul la aceasta se vor realiza prin intermediul platformei
    - Respinse – dacă nu se răspunde conform/în termen conform procedurii de lucru IM/ITM

Toate operațiunile efectuate asupra unei solicitări, de la inițiere și până la finalizarea procesului de procesare vor fi jurnalizate în sistem cu mimim următoarele informații:

- tipul operațiunii
- data operării
- utilizatorul care a efectuat modificare
- posibilitatea de a vizualiza integral versiunea anterioară
- utilizatorul care a accesat, IP și momentul în timp (zi, data, ora, minut, secunda).

Platforma trebuie să permită ca istoricul operațiunilor realizate de către utilizatori să fie vizualizat direct în interfață de către utilizatorii cu acest drept, respectiv utilizatorii solicitanți și operatorii ITM.

3.2.6.2.7.4 Accesarea informațiilor în vederea evidenței sau a activității de control

Utilizatorii IM/ITM vor avea acces la o serie de informații și rapoarte pe baza datelor stocate în sistem.

Platforma trebuie să permită gestionarea accesului la aceste informații la nivel granular de către utilizatorii nominalizați prin acordarea permisiunii specifice din partea ITM. Mai multe detalii privind cerințele funcționale de gestionare a accesului în aplicație sunt detaliate în Modulul de Administrare.

Astfel, pentru utilizatorii IM/ITM platforma trebuie să pună la dispoziție o zonă de lucru care să permită cel puțin:

- posibilitatea de a vizualiza informații de complexitate mare sub forma de liste
- posibilitatea de a căuta, sorta și filtra aceste liste pe mai multe criterii – în funcție de setul de date afișat
    - câmpuri de căutare cu titlu de exemplu lista nefiind exhaustivă (necesarul exact privind criteriile de căutare/sortare/filtrare se vor stabili în perioada de analiză):
        - CUI/CIF/CNP
        - Nume/Prenume Salariat
        - Nr./Dată Contract
        - Denumire Angajator
        - CAEN Angajator
        - CNP Salariat
        - Nr. salariați – cu posibilitatea de a selecta intervale de forma mai mic, mai mare etc.
        - Județ
        - Cod COR (funcție)
- posibilitatea de a realiza interogări utilizând mai mulți termeni pentru același tip de criteriu (de exemplu mai multe CNP sau CUI/CIF)

- având în vedere caracterul sensibil al datelor, realizarea interogărilor se va putea realiza doar prin selectarea unui motiv dintr-un nomenclator și completarea de informații acolo unde este cazul, de exemplu dacă motivul selectat este o adresă din partea altei instituții, se va completa nr/data documentului
    - nomenclatorul motivelor de accesare va putea fi gestionat din zona de administrare a sistemului, direct din interfața acestuia
- posibilitatea de a salva criteriile interogării pentru a putea fi reutilizate ("save search as filter") și posibilitatea de a partaja criteriile interogării astfel salvate cu alți utilizatori – dacă aceștia au permisiunea de acces asupra seturilor de date

- posibilitatea de a accesa detaliile unui set de date prin click în cadrul listei, de exemplu, dar nu limitat la:
    - vizualizarea detaliilor unui contract de muncă după ce a fost selectat, inclusiv istoricul
    - vizualizarea profilului unui angajator după ce a fost selectat cu toate informațiile relevante angajatorului, de exemplu:
        - datele de identificare ale angajatorului
        - utilizatorii asociați angajatorului care au drept de a introduce date
        - unitățile fără personalitate juridică subordonate angajatorului (sucursală, agenție, reprezentanță) sau unitatea părinte, cu personalitate juridică – după caz și dacă există
        - salariații și contractele de muncă cu toate detaliile acestora
        - salariații detașați la alți angajatori
        - istoricul operațiunilor realizate de către utilizatorii responsabili cu introducerea datelor pentru angajator
- evidențierea/marcarea automată în interfață a anumitor date introduse de către responsabilii angajatorului dacă există abateri (pe baza unor reguli), de exemplu:
    - dacă adăugarea unui contract a fost realizată după data începerii contractului
    - dacă adăugarea/eliminarea unui utilizator al unui prestator de servicii la entitatea angajatorului se realizează după termenul stabilit prin lege
    - se va avea în vedere configurarea de rapoarte specifice activității de control pe baza acestor criterii – de exemplul, da rnu limitat la "top angajatori cu o frecvență ridicată de înregistrare întârziată a contractelor dintr-un județ". Lista rapoartelor specifice va fi realizată în etapa de analiză, estimarea fiind pentru minim 20 de astfel de rapoarte
- posibilitatea de a identifica ușor, pe baza unui raport, ce tipuri de date introduce un utilizator (persoană nominală) pentru toate entitățile de tip angajator cărăra le este asociat, scopul fiind identificarea cu ușurință a utilizatorilor ce aparțin firmelor de prestare a serviciilor de introducere date

Nota: și utilizatorii asociați entităților de angajatori trebuie să aibă acces la aceste informații – dar doar pentru operațiile realizate asupra angajatorului de care aparțin – pentru a sprijini o bună gestionare a activităților de introducere date atât pentru angajații intern (HR) cât și pentru firmele de prestare a serviciilor

Mai multe detalii privind cerințele funcționale generale privind lucrul cu datele vehiculate și procesate în sistem sunt prezentate în Modulul de raportare și analiză date.

3.2.6.2.8 Modul de raportare și analiză date

Sitemul trebuie să permită agregarea, analiza și interpretarea datelor coletate și gestionate. Serviciile de implementare a sistemului vor cuprinde inclus dezvoltarea, testarea și operaționalizarea acestui modul

conform cerințelor caietului de sarcini și a celor identificate în etapa de analiză și proiectare, în ceea ce privește tipurile de rapoarte și datele conținute de acestea.

Ca sursă a datelor se anticipează minim următoarele:

- date colectate utilizând aplicația Revisal realizată în baza Hotărârii Guvernului 161/2006 – acest set de date reprezintă o arhivă a contractelor de muncă înregistrate și trasnmise de la inițierea modului de lucru respectiv până în anul 2011
- date colectate de către sistemul actual începând cu 2011 (Hotărârea Guvernului nr. 500/2011 și Hotărârea Guvernului nr. 905/2017) – în acest set de date au fost preluate, conform dispozițiilor legale aplicabile contractele active din perioada 2006 și au fost și sunt introduse date noi
- date colectate de către viitorul sistem REGES-ONLINE așa cum va fi fost acesta proiectat și operaționalizat, inclusiv în ceea ce privește migrarea datelor istorice și compatibilitatea structurii bazei de date cu versiunile anterioare pentru păstrarea relevanței datelor

Structura actuală a bazei de date Revisal/Reges precum și Specificațiile Tehnice privind întocmirea și transmiterea Registrului General de Evidenta a Salariaților sunt anexate prezentului document, anexele 1 și 2.

3.2.6.2.8.1 Panoul de control pentru analiză și raportare

Sistemul trebuie să ofere o zonă dedicată pentru afișarea grafică a informațiilor statistice și a rapoartelor complexe sub forma de liste.

Panoul de control trebuie să dispună de următoarele funcționalități:

- existența unui set implicit de rapoarte uzuale dar și posibilitatea de a genera dinamic rapoarte noi, astfel:
    - rapoartele uzuale vor fi configurate de către prestator, ca parte a serviciilor de implementare, în baza nevoilor identificate în etapa de analiză
    - rapoartele dinamice se vor putea realiza de către utilizatorii IM/ITM, sistemul trebuid să permită definirea a minim:
        - denumirii raportului
        - selectarea seturilor de date (doar dintre cele la care utilizatorul are acces) și agregarea acestora în raport cu posibilitatea stabilirii ordinii coloanelor
        - adăugarea unui motiv pentru construirea raportului
        - rularea raportului sau salvarea acestuia pentru rulare ulterioară, partajarea cu alți utilizatori
        - jurnalizarea de către sistem a datelor accesate astfel în aplicație, rapoartelor rulare. Informațiile jurnalizate vor putea fi consultate atât de către utilizatorul care a generat solicitarea cât și de utilizatorii cu un nivel de privilegii de acces mai ridicat decât acesta, cum ar fi de exemplu Serviciul Informatic, anumite persoane cu atribuții de control în cadrul instituției, direct în interfața aplicației.
- afișarea grafică a informațiilor în panoul de control în diferite moduri, cu posibilitatea de extragere a acestora, minim grafice de tip Pie Chart, Bar Graph, histogramă, scatterplot
- exportul de date generate de rularea unui raport trebuie să se poată realiza în minim următoarele formate .xlsx, .pdf, .csv, .docx

- posibilitatea de a vizualiza datele în mod georeferențiat, în sensul alocării acestora peste harta județelor și a localităților
- urmărirea tendințelor de evoluție a evenimentelor și folosind tehnici de tip "machine-learning", evidențierea anomaliilor în comportamentul utilizatorilor

Achizitorul estimează ca va fi necesară dezvoltarea a minim 50 rapoarte de complexitate mare, din care cel puțin 5 rapoarte de tip tablou de bord (dashboard). Acestea vor fi definite pe parcursul fazei de analiza/colectare a cerințelor.

Exemple de afișare de informații statistice pe panoul de control în funcție de tipul de utilizator, pentru a ca ofertanții să înțeleagă gradul de complexitate și să dimensioneze corect efortul de realizare a acestora:

- pentru angajatori:
    - Evoluția numărului de contracte/salariați/angajatori pe luni/săptămâni/zile
    - Top salarii
    - Distribuție salariați/funcții/ocupații, etc.
- pentru IM/ITM:
    - Evoluția numărului de contracte/salariați/angajatori pe luni/săptămâni/zile;
    - Top salarii/angajatori pe domenii de activitate/ocupații/județe etc.;
    - Distribuții salariați/angajatori/funcții/ocupații/domenii de activitate/modificări ale elementelor contractelor individuale de muncă, contractelor individuale de muncă, contract individual de muncă la domiciliu, contracte de ucenicie, contracte de stagiu, contract de muncă cu clauză de telemuncă, contract de muncă temporară, etc.

3.2.6.2.9 Componenta de notificare și informare

Platforma trebuie să dispună de un mecanism de notificare/informare a tuturor categoriilor de utilizatori prin mesaje transmise atât în cadrul sistemului cât și prin e-mail și/sau aplicația mobilă. Componenta trebuie să funcționeze fără să necesite instalarea și punerea la dispoziție a unui server de email de către Achizitor. Mecanismul de notificări va fi interconectat cu baza de date a utilizatorilor – pentru preluarea modalității de contact și a preferințelor acestora în ceea ce privește temele de interes pentru care aceștia doresc să fie notificați.

Componenta de notificare și informare trebuie să implementeze minim următoarele funcționalități:

- să suporte minim următoarele canale de comunicație
    - mesagerie internă accesibilă direct din interfața platformei de către utilizatori
        - utilizatorii să fie informați într-un mod facil asupra primirii unui nou mesaj și a numărului de mesaje necitite
    - transmiterea de mesaje externe platformei - prin email sau aplicația mobilă pentru evenimente
        - generate automat de către sistem – (de exemplu primirea numărului de înregistrarea după ce sistemul înregistrează solicitarea de înrolare a unui nou angajator).
        - declanșate de către utilizator (de exemplu solicitare înregistrare, autentificare, resetare parolă, solicitare de clarificări, răspuns de clarificări, notificarea unui salariat asupra faptului că i-a fost adăugat sau modificat un contract etc.)
        - să ofere posibilitatea utilizatorilor de a alege canalul de comunicație pe care îl doresc de tipul și/sau, aceste setări se vor aplica doar asupra mesajelor considerate non-critice (ex. se vor excepta resetările de parolă)

- să permită utilizatorului să stabilească din profilul propriu minim:
    - modalitatea de primire a codurilor de autentificare în doi pași, fie prim e-mail fie prin aplicația mobilă
    - modalitatea de primire a notificărilor/mesajelor de sistem, fie prim e-mail fie prin aplicația mobilă.
- să fie conceput astfel încât să permită transmiterea de notificări care să genereze acțiuni pro active din partea utilizatorilor - pe baza unui set de reguli identificate în etapa de analiză, de exemplu:
    - notificarea părților interesate atunci când se apropie termenul de încheiere a perioadei pentru care un utilizator persoană nominală poate efectua operațiuni de gestionare a salariaților și contractelor, pentru buna gestionare a prestatorilor de servicii de introducere date
    - notificarea responsabililor din partea angajatorului atunci când, o detașare sau un contract pe perioadă determinată urmează să se încheie
    - notificarea responsabililor din partea angajatorului asupra necesității actualizării cărții de identitate a cetățenilor străini care au fost introduși inițial cu datele pașaportului
- să permită compunerea dintr-o zonă de lucru dedicată din interfața platformei și transmiterea de notificări sau mesaje de către anumiți utilizatori IM/ITM cu nivel de acces sporit către un grup de utilizatori, de exemplu:
    - informări pentru toți angajatorii, toți salariații asupra unor modificări legislative care le poate afecta activitatea
    - informări asupra indisponibilității uneia dintre componente (transmitere alerte prin e-mail sau aplicația mobilă) sau a unuia dintre sistemele cu care noul REGES-ONLINE va fi interoperaționalizat (Direcția Generală Pentru Evidența Persoanelor, ONRC, ANAF, IGI, etc.)
    - mesajele de acest fel să poată fi trimise instant sau programate pentru o anumită oră/dată.

3.2.6.2.10 Modul administrare

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.

Operațiunile aferente modulului de administrare trebuie să poată fi realizate direct din interfața aplicației.

Accesul la funcționalitățile de administrare a utilizatorilor trebuie să fie permis doar administratorilor, în funcție de drepturile acordate rolului respectiv.

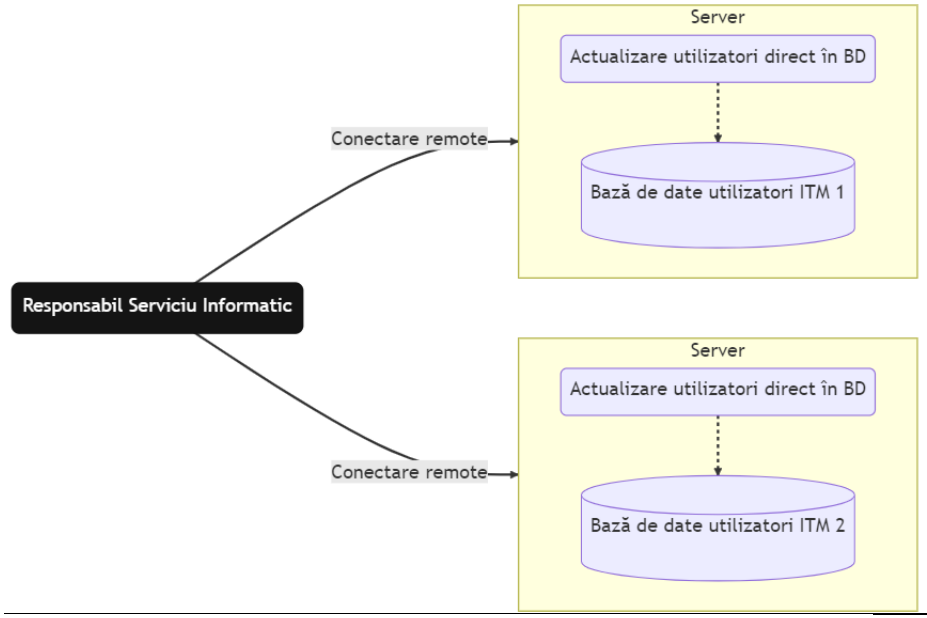
În plus, accesul în zona de administrare (și pentru accesul la anumite seturi de date ce se vor defini în etapa de analiză - de exemplu rapoartele accesate de către inspectorii de muncă) se va realiza în mod securizat doar prin rețeaua internă a IM/ITM (astfel accesul din afara instituției se va realiza în prealabil doar prin 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.

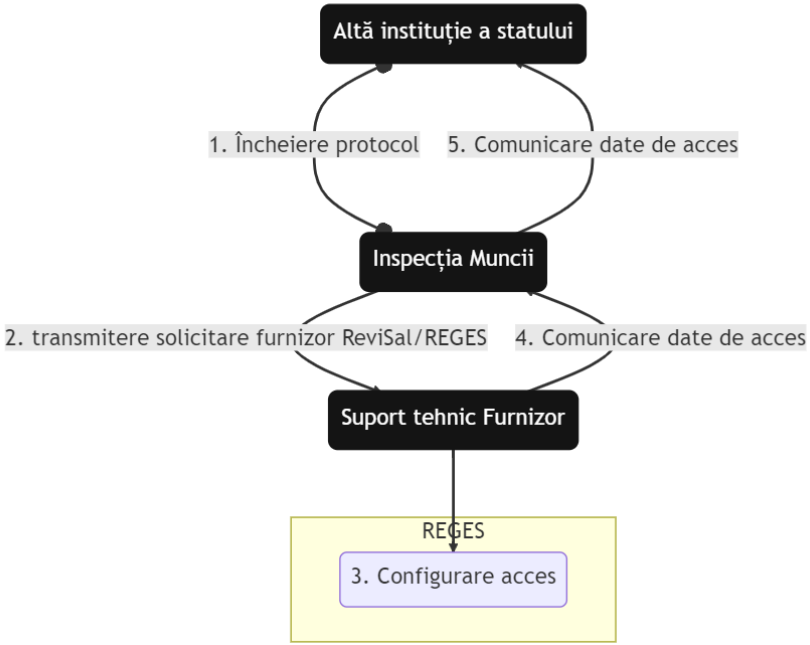
Prin modulul de administrare al viitoarei soluții REGES-ONLINE se urmărește îmbunătățirea actualului mod de lucru:

- prin înlesnirea modalităților de a realiza operațiuni simple de căutare, adăugare și modificare utilizatori
- prin dobândirea unui grad mai mare de independență în realizarea operațiunilor simple de actualizare a formularelor de colectare date și a nomenclatoarelor precum și a oferirii accesului granulat atât utilizatorilor din cadrul instituției cât și celor externi (pe baza unui protocol încheiat în temeiul legii).

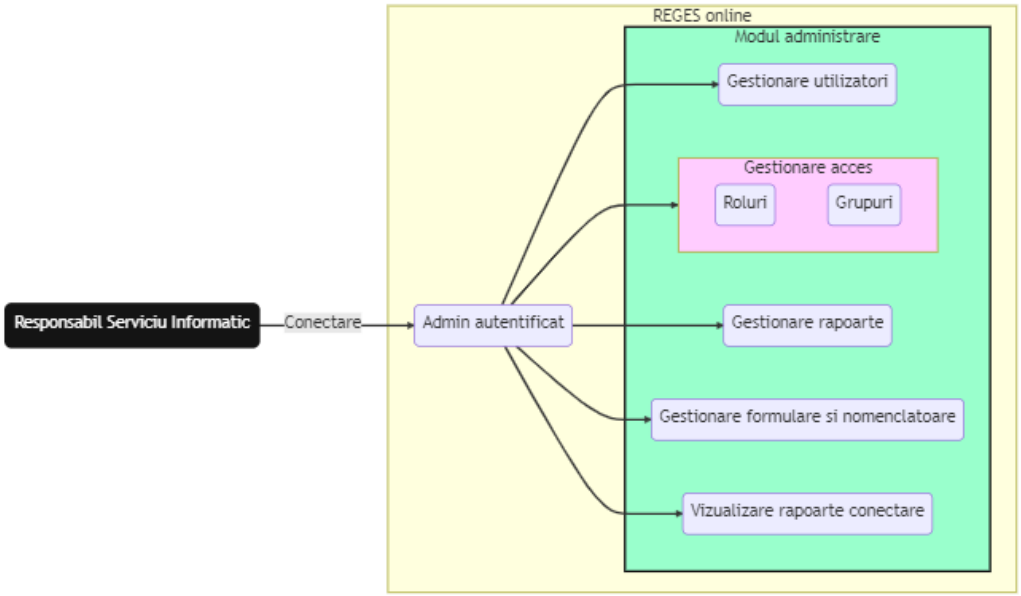
Modul de lucru actual gestiune utilizatori interni IM/ITM



Modul de lucru actual utilizatori externi



Modul de lucru dorit



3.2.6.2.10.1 Administrarea utilizatorilor

Sistemul trebuie să permită administrarea utilizatorilor cu cel puțin următoarele funcționalități:

- Administratorii sistemului să poată adăuga, modifica, suspenda/activa utilizatori, cu minim următoarele caracteristici:
    - generarea parolei inițiale trebuie să fie gestionată printr-un mecanism automat de către sistem, fără intervenția administratorilor REGES-ONLINE
        - de exemplu, la adăugarea unui cont, noul utilizator să primească un mesaj prin care să-și poată configura singur parola
        - formatul parolei din punct de vedere al cerințelor minime (nr de caractere, tipuri de caractere) va fi stabilit în perioada de analiză
    - mecanisme de resetare a parolei, automat, fără intervenția administratorilor REGES-ONLINE
    - mecanisme de vizualizarea a statusului utilizatorului: creat, modificat, suspendat, în curs de resetare parolă, inactiv, etc.
    - suspendarea unui utilizator presupune ca acesta să rămână în sistem dar fără a se putea autentifica sau a fi autorizat în sistem
    - suspendarea unui cont trebuie să se poată realiza pe o perioadă determinată prin introducerea datelor de început și sfârșit a suspendării
        - se va avea în vedere configurarea de notificări a utilizatorilor privind acțiunea de suspendare a contului
        - 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).
    - coroborat cu acțiunea de suspendare să existe și posibilitatea de a marca utilizatorii cu parola expirată - astfel încât, la următoarea conectare să fie obligați să-și schimbe parola
- Lista utilizatorilor să permită operațiuni de căutare, sortare și filtrare după diferite criterii (ex. Rol, grup utilizatori, prenume, nume, email/nume utilizator și stare – activ/suspendat) precum și posibilitatea de a fi exportată într-un fișier tabelar (.xlsx, .csv).
- Posibilitatea de import a mai multor utilizatori pe baza unui șablon prestabilit, direct din interfața de administrare a aplicației, acolo unde este cazul.
- Ca metodă complementară de management a utilizatorilor interni IM/ITM trebuie să existe și posibilitatea de integrare cu Active Directory configurat la nivelul Achizitorului. Gradul de integrare va fi stabilit în etapa de analiză pentru proiectarea sistemului.

3.2.6.2.10.2 Gestionarea accesului

Accesul la datele gestionate de REGES-ONLINE va fi accesibil doar următoarelor categorii de utilizatori:

- utilizatori interni ai IM și ITM, în funcție de nivelele de acces și rolurile definite în sistem
- 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

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 Autoritate Contractantă.

Astfel sistemul trebuie să permită:

- Adăugarea de noi roluri, sau modifica rolurile existente
- Asocia drepturi de acces rolurilor sau grupurilor astfel configurate
    - drepturile de acces vor fi atât cele prestabilite în urma dezvoltării soluției cât și permisiuni create dinamic utilizând modulul de raportare și care vor oferi acces la anumite seturi de date/rapoarte create de către utilizatori
- Adăugarea sau modificarea de grupuri de utilizatori. 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 numite seturi de date.
    - posibilitatea de a crea legături părinte-copil între grupuri
    - posibilitatea de a adaugă utilizatori la grupuri
        - 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.

3.2.6.2.10.3 Rapoarte referitoare la utilizatori

Soluția dezvoltată trebuie să asigure păstrarea și posibilitatea de consultare a:

- 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).

3.2.6.2.10.4 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).

Autoritatea Contractantă 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.

Structura actuală a bazei de date precum și *Specificațiile Tehnice privind întocmirea și transmiterea Registrului General de Evidenta a Salariaților* sunt anexate prezentului proiect tehnic.

Astfel sistemul dezvoltat trebuie să asigure:

- posibilitatea de a adăuga noi nomenclatoare
- posibilitatea de a putea adăuga/modifica lista de valori ai unui nomenclator

- posibilitatea de a crea legături de tip copil-părinte între nomenclatoare acolo unde este cazul (ex. structura ierarhică a codurilor COR).
- 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.

3.2.6.2.11 Registul prestatorilor de servicii

În vederea organizării unei evidențe centralizate, conform prevederilor legale, se va crea un registru al prestatorilor cu care angajatorii au încheiat contracte de prestări servicii pentru completarea și transmiterea datelor din registru. ~~, se va crea și se va menține un registru al prestatorilor~~.

Angajatorii pot contracta serviciul de completare şi transmitere a datelor din registru sau servicii de tip expert prin încheierea de contracte de prestări servicii cu prestatori care îşi desfăşoară activitatea în condiţiile prevederilor legale în vigoare, inclusiv ale prevederilor privind protecţia datelor cu caracter personal în care se vor înregistra persoanele care prestează servicii de operare date în registrul altor operatori economici. Angajatorii care au contractat serviciul de completare și transmitere au obligaţia de a notifica inspectoratul teritorial de muncă, în a cărui rază teritorială îşi au sediul/domiciliul, despre încheierea contractelor de prestări servicii precum şi datele de identificare ale prestatorului, conform prevederilor legale.

3.2.6.2.12 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.

3.2.6.2.13 Trasabilitate şi non-repudiere

Operațiunile efectuate în cadrul unei sesiuni de lucru pe datele din registru vor fi sigilate cu o cheie „hash” care garantează non-repudierea.

Operațiunile de tip „view-only” efectuate de către orice utilizator vor fi înregistrate într-un jurnal tip „log” astfel încât pentru orice vizualizare de date confidențiale din sistem să se cunoască ce utilizator, când și conform căror drepturi a efectuat acea vizualizare.

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.

3.2.6.2.14 Ergonomie în utilizare și feedback de la angajatori

Având în vedere că principalii utilizatori ai sistemului sunt angajatorii precum și faptul că obligația de transmitere a registrului este o activitate care va genera costuri în cadrul organizațiilor acestora, Inspecția Muncii solicită realizarea unui studiu de impact și de ergonomie a soluției tehnice în perioada de pilotare și rulare asistată a sistemului, concluziile acestui studiu urmând a fi implementate în sistema în vederea obținerii acceptanței finale pentru implementarea sistemului. Se vor analiza cel puțin următoarele elemente:

- Modul de lucru al personalului din departamentul resurse umane al angajatorilor pe categorii, mari, medii și mici;
- Modul de folosire a aplicației curente REVISAL și a altor aplicații de gestiune a resurselor umane, programe interne, fluxuri de lucru cu contractele de munca;
- Propuneri de optimizare a modului de lucru și îmbunătățire a modalității de completare a registrului.

Sistemul REGES-ONLINE va fi adaptat elementelor principale rezultate din analiza de impact în vederea obținerii acceptanței finale pentru etapa de implementare . În acest sens se vor efectua studii calitative de analiză a categoriilor țintă cărora se adresează sistemul REGES-ONLINE pentru a identifica ipoteze de îmbunătățire și de eficientizare a activității acestora precum și studii cantitative pentru a valida ipotezele identificate anterior pe categorii reprezentative. La finalul acestor activități, raportul studiului va fi prezentat Inspecției Muncii și analizat în vederea validării propunerilor ce urmează a fi implementate, precum și a modalității de implementare.

3.2.6.2.15 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.

De asemenea, se va solicita Prestatorului selectat să asigure și suport pentru utilizarea sistemului de către angajatori și salariați, prin punerea la dispoziției a unui centru de suport ce poate fi accesat telefonic, pe durata contractului și a perioadei de suport și garanție.

De asemenea, în etapa de proiectare tehnică va fi evaluată oportunitatea introducerii, la nivelul fiecărui inspectorat teritorial de muncă a unui terminal interactiv care să ofere informații și să permit consultarea datelor/ imprimarea de documente, pentru a degreva angajații ITM de o parte din interacțiunea cu publicul.

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;
- 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
- 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.

Nota:

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 caiet de sarcini, sistemul REGES-ONLINE 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.

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).

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 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 REGES-ONLINE 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 REGES-ONLINE.

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.).

4.2 Etapa de proiectare

Etapa de proiectare va avea la bază livrabilele aprobate de beneficiar în urma definitivării etapei de analiză 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 REGES-ONLINE, 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;

- 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 caiet de sarcini, 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 REGES-ONLINE 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 caietul de sarcini 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).

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 caiet de sarcini.

În cadrul fazei de dezvoltare, contractantul 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).

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 REGES-ONLINE

Manualele de utilizare vor conține prezentarea detaliată a modului de utilizare a fiecărei componente/modul al REGES-ONLINE, 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.

Pentru utilizatorii externi, manualele vor fi elaborate bilingv (limba română și engleză);

- 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 REGES-ONLINE 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 din partea producătorilor (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.

Toate echipamentele vor fi configurate de către Prestator conform soluției tehnice agreate cu Beneficiarul 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

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

Activitățile de instalare și configurare a infrastructurii software de bază 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 solicitate (de tip SLA)

4.4.3 Instalare și configurare sistem REGES-ONLINE

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

Activitățile de instalare și configurare a sistemului REGES-ONLINE se vor realiza de către reprezentanții Ofertantului sub supravegherea personalului Autorității Contractante.

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 REGES-ONLINE

Documentații tehnice complete

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

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 REGES-ONLINE.

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 cele 2 sisteme anterioare, testarea datelor

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 caiet de sarcini. Astfel, se va avea în vedere faptul că infrastructura hardware și sofware, precum și sistemul REGES-ONLINE 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 a REGES-ONLINE (GoLive), inclusiv migrarea și integrarea datelor

Etapa de lansare și punere în producție a REGES-ONLINE 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 caiet de sarcini 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 REGES-ONLINE – 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 REGES-ONLINE

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

- Crearea și actualizarea portalului extern
- Utilizarea modulelor de evidență și control, raportare și analiză date
- Funcționalități asociate modulelor salariat și angajator
- Notificări, informări și integrări cu alte sisteme
- Modalitatea de utilizare a documentației tehnice și de solicitare a suportului tehnic

Structura grupului de utilizatori ce vor participa la programul de formare:

- 2000 de utilizatori din partea IM și ITM-urilor

Fiecare persoană va participa la o instruire de 1 zi (8 ore).Prestatorul va organiza minim 2 sesiuni de 8 ore în fiecare oraș reședință de județ (40 de orașe reședință, în afară de București și Ilfov), pentru grupe de maxim 20 de cursanți. Cursanții din Inspecția Muncii, ITM București și ITM Ilfov vor fi instruiți la București, în grupe de maxim 20 de persoane, minim 6 sesiuni de 8 ore.

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 infrastructura hardware ofertată
2. Administrare infrastructura software de bază ofertate
3. Administrare și configurare platformă REGES-ONLINE
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 REGES-ONLINE, 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.

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 minimum 60 de luni (5 ani) de la data lansării și punerii în producție a REGES-ONLINE *(realizarea acceptanței finale).*

Garanția reprezintă perioada de timp în cadrul căreia contractantul are obligația asigurării și controlului calității funcționării REGES-ONLINE, 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 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 care

Operatorul economic 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
- iii) Dezvoltările și/sau configurările personalizate realizate de Prestator în vederea îndeplinirii cerințelor funcționale stabilite prin prezentul caiet de sarcini.

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 tip SA 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 HW 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 și asistență de specialitate din partea ofertantului pentru remedierea defectelor/deficiențelor constatate sau a incidentelor survenite în raport cu REGES-ONLINE. 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.

- Implică realizarea operațiunilor de modificare a parametrilor și configurărilor sistemului, ajustări în funcție de diverse modificări apărute la nivelul organizației Achizitorului, în limita a 300 zile om (în cei 5 ani).

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 și 12/5 pentru restul utilizatorilor de tip angajat sau angajator, canale de comunicație pe care să fie preluate și gestionate incidentele de la utilizatori (IM, ITM, angajatori, angajați, utilizatori de la alte instituții), cu respectarea următorului SLA:

Prioritate	**Descriere**	**Timp răspuns**	**Timp rezolvare (soluție provizorie)**	**Timp maxim 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 aplicațiile sistemului.	1 oră	6 ore	24 de ore (soluție finală sau nivel de funcționare Mediu
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 aplicațiile sistemului, însă **experimentează probleme/erori** care nu permit continuarea activității în integralitate	2 ore	12 ore	48 de ore
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**	4 ore	36 de ore	96 de ore

	degradată/redusă în mod semnificativ; - Utilizatorii **se pot conecta** și pot utiliza aplicațiile sistemului, însă **experimentează anumite probleme/erori** *(recuperabile)* de funcționare a acestora, fiind totuși posibilă continuarea activității.			
Minor	**Sistemul funcționează aproape de parametrii normali**, dar: - 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**;	8 ore	48 de ore	168 de ore

În vederea asigurării Autorității contractante cu privire la îndeplinirea la termen şi la parametrii de calitate solicitaţi a obligaţiilor contractuale ce revin Contractantului pe parcursul perioadei de garanţie, conform celor specificate în caietul de sarcini, Contractantul are obligaţia de a prezenta Autorității contractante, cu ocazia recepţiei cantitative și calitative finale aferente contractului o garanţie de bună funcţionare, emisă de o societate bancară sau societate de asigurări, sub formă de garanţie bancară sau poliţă de asigurare, în valoare de 2% din valoarea fără TVA a contractului.

Garanţia de bună funcţionare va face referire la denumirea, numărul şi data contractului şi va prevedea în mod clar şi fără echivoc, angajamentul irevocabil al emitentului de a plăti la prima cerere a Autorității contractante orice sumă solicitată de aceasta, până la concurenţa sumei maxime, în situaţia în care Contractantul nu şi-a îndeplinit obligaţiile contractuale ce îi revin în perioada de garanţie, în conformitate cu prevederile contractuale.

Sub sancţiunea atacării garanţiei de bună execuţie a contractului, garanţia de bună funcţionare trebuie prezentată Autorității contractante în original, în maxim 10 zile de la data semnării procesului-verbal final de recepţie cantitativă și calitativă pentru respectivul contract şi în orice caz, înainte de expirarea garanţiei de bună execuţie a contractului.

Perioada de valabilitate a garanției de bună funcționare va acoperi cel puțin perioada de garanție aferentă tuturor produselor hardware/software și serviciilor recepționate pe parcursul implementării contractului, plus două săptămâni.

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 caiet de sarcini depinde în mod decisiv de implicarea din partea prestatorului pe parcursul perioadei de execuție a unei echipe corespunzătoare.

Listă experți necesari:

- Manager proiect
- Analist de business
- Arhitect de sistem
- Expert infrastructură hardware (1 sau mai mulți)
- Expert infrastructură software(1 sau mai mulți)
- Expert baze de date
- Coordonator tehnic REGES-ONLINE
- Expert testare
- Expert securitate
- Coordonator suport tehnic

4.11 Grafic de implementare

Durata estimată de implementare a investiției este de maxim 15 luni de la intrarea in vigoare a contractului, care este estimată pentru **octombrie 2023**.

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 REGES-ONLINE, 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 3 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

4.11.1.1 Grafic estimat de implementare

Activitate	**Constrângeri de implementare/ Termen finalizare activitate**
Analiză și proiectare sistem informatic	Luna 5 a proiectului
Dezvoltare sistem informatic	Luna 10 a proiectului
Livrare, instalare și configurare infrastructură hardware, de comunicații și software de bază	Luna 5 a proiectului
Testare sistem informatic	Luna 12 a proiectului
Punere în producție sistem informatic	Luna 13 a proiectului
Instruire utilizatori și administratori	Luna 11 a proiectului
Asistență la pornire	Luna 15 a proiectului (Lunile 13-15 ale proiectului)
Suport tehnic, garanție și mentenanță	5 ani de la punerea în producție a sistemului informatic