UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

Proiect co-finanțat din Fondul European de Dezvoltare Regională prin Programul Operațional Competitivitate 2014-2020

APROB
DIRECȚIA GENERALĂ PENTRU COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI
DIRECTOR GENERAL
Chestor de poliție
Mihai DĂNILĂ

DOCUMENT DESCRIPTIV

Achiziție sistem informatic central în cadrul proiectului *„Sistem Informatic Integrat pentru Emiterea Actelor de Stare Civilă” – SIIEASC*, cod SMIS 2014+ 120025

CUPRINS

INFORMATII GENERALE

I.1. Informații generale despre autoritatea contractantă

Ministerul Afacerilor Interne (MAI) funcționează în baza OUG nr. 30 din 2007, privind organizarea și funcționarea Ministerului Afacerilor Interne, aprobată cu modificări prin Legea nr. 15/2008, cu modificările și completările ulterioare și HG nr. 416/2007 privind structura organizatorică și efectivele Ministerului Afacerilor Interne, cu modificările și completările ulterioare.

Direcția Generală pentru Comunicatii și Tehnologia Informației (DGCTI) face parte din structura Aparatului central al Ministerului Afacerilor Interne și este unitatea de specialitate cu competență materială și teritorială generală în domeniul comunicațiilor și tehnologiei informației, denumit în continuare TIC.
Obiectivele generale ale DGCTI:

a) dezvoltarea domeniului TIC în scopul asigurării sprijinului de specialitate necesar îndeplinirii misiunii MAI pentru componentele ordine publică și siguranța cetățeanului, administrație și domeniile „suport", precum și implementarea prevederilor europene cu privire la Agenda Digitală, în vederea consolidării capacității instituționale a MAI;
b) eficientizarea utilizării resurselor materiale, financiare și umane din domeniul TIC de care dispune MAI.

Direcția pentru Evidența Persoanelor și Administrarea Bazelor de Date (DEPABD) este organizată și funcționează ca organ de specialitate al administrației publice centrale, cu personalitate juridică, în subordinea MAI, finanțată integral de la bugetul de stat, prin bugetul Ministerului Afacerilor Interne. Ca principală atribuție a DEPABD menționăm "organizează, coordonează și urmărește modul de aplicare, în mod unitar, de către serviciile publice comunitare de evidență a persoanelor, a reglementărilor legale în domeniul evidenței persoanelor, al stării civile și al schimbării pe cale administrativă a numelor persoanelor fizice".

1. Scopul și obiectivele proiectului

1.1. Obiectiv general

Ministerul Afacerilor Interne în parteneriat cu Ministerul Comunicațiilor și Societății Informaționale, Serviciul de Telecomunicații Speciale și Ministerul Dezvoltării Regionale și Administrației Publice derulează proiectul **"Sistemul Informatic Integrat pentru Emiterea Actelor de Stare Civilă" – SIIEASC**, finanțat prin Programul Operațional Competitivitate, *Axa prioritară 2* - Tehnologia Informației și Comunicațiilor (TIC) pentru o economie digitală competitivă, *OS 2.3* - Creșterea utilizării sistemelor de e-guvernare, *Acțiunea 2.3.1* – Consolidarea și asigurarea interoperabilității sistemelor

informatice dedicate serviciilor de e-guvernare tip 2.0 centrate pe evenimente din viața cetățenilor și întreprinderilor, dezvoltarea cloud computing guvernamental și a comunicării media sociale, a Open Data și Big Data – *SECȚIUNEA E-GUVERNARE ȘI INTEROPERABILITATE.*

Obiectivul general al proiectului constă în informatizarea sistemului de depunere a cererilor pentru emiterea și eliberarea efectivă a documentelor de stare civilă, precum și implementarea suportului necesar dezvoltării și accesării serviciilor electronice ce au la bază informații primare de stare civilă. Prin implementarea proiectului SIIEASC, pentru evenimentele de viață, așa cum sunt acestea descrise în SNADR (naștere, căsătorie, divorț, deces etc.) și grupate în categoria „stare civilă", vor fi furnizate servicii electronice, la nivelul 4 de sofisticare.

Obiectivele specifice ale proiectului SIIEASC sunt:

- Reducerea timpului necesar procesării tranzacțiilor informațiilor de stare civilă și a cheltuielilor de stocare a informațiilor pentru administrațiile locale și centrale legate de un număr de 5 servicii pentru cele 4 evenimente primare de viață: naștere, căsătorie, divorț, deces.
- Creșterea gradului de interoperabilitate a sistemelor centrale și locale care prelucrează informații de stare civilă specifice serviciilor corelate cu cele 4 evenimente de viață primare: naștere, căsătorie, divorț, deces.
- Eliminarea redundanțelor informaționale existente în sistemele locale și centrale care prelucrează informații de stare civilă.
- Digitizarea (scanarea și indexarea) documentelor de stare civilă emise în ultimii 100 de ani, aferente evenimentelor de viață primare. Activitatea de digitizare vizează actele de stare civilă întocmite în perioada de referință de către oficiile de stare civilă (aprox. 75.000.000 de documente).
- Stocarea electronică și gestiunea arhivistică a documentelor digitizate.
- Creșterea nivelului de colaborare și comunicare între comunitățile locale și instituțiile publice în problematica stării civile.
- Creșterea nivelului de colaborare, comunicare și mobilitate în vederea asigurării comunicațiilor operative oferite personalului M.A.I., din cadrul D.E.P.A.B.D. și D.G.C.T.I., cu atribuții în implementarea, operaționalizarea și ulterior, exploatarea SIIEASC prin soluția de comunicații VoIP colaborativă;
- Punerea în aplicare a serviciilor G2C/G2G prin implementarea suportului necesar dezvoltării serviciilor electronice ce au la bază informații primare de stare civilă.

Implementarea proiectului va avea ca rezultat dezvoltarea, instalarea, configurarea și integrarea unui sistem informatic centralizat care are rolul de a permite cel putin:

- Entităților care desfășoară activități de stare civilă și care efectuează în mod eficient și în siguranță, fluxul de activități de stare civilă prin mijloace informatice, în scopul de a crea, actualiza, stoca, păstra înregistrările, precum și de a elibera documentele de stare civilă aferente evenimentelor de stare civilă.

- Transmiterea şi primirea de cereri oficiale şi documente, verificarea statutului cetăţenilor în timpul procesului de emitere a documentului de stare civilă printr-o interfaţă web care trebuie să echilibreze accesul şi uşurinţa de utilizare, cu necesitatea de a proteja confidenţialitatea, integritatea şi disponibilitatea datelor personale ale cetăţenilor.

- Accesul facil al cetăţenilor într-un mod securizat la cele mai recente informaţii cu privire la reglementările, procedurile, deciziile, tarifele şi etapele necesare pentru obţinerea documentelor de stare civilă, imprimarea şi descărcarea de formulare electronice, trimiterea solicitărilor de informaţii pe bază de şabloane electronice.

- Securizarea accesului la aplicaţii / date / sisteme / infrastructură prin intermediul unui sistem informatic integrat, cu aplicarea politicilor de securitate, profilelor de identitate şi a soluţiilor de gestiune a accesului; integrarea şi comunicarea cu sistemele externe pentru notificări /consultări / vizualizări şi obţinerea datelor / informaţiilor din sistemul de stare civilă.

- Emiterea, arhivarea şi gestiunea întregului ciclu de viaţă al documentelor de stare civilă, conform legislaţiei în vigoare (Legea 119/1996, HG 64/2011 şi OG 41/2003, OUG 41/2016, HG 727/2013).

- Implementarea serviciilor online G2C / G2G ce au la bază informaţii primare de stare civilă.

- Gestionarea şi administrarea arhivei documentelor de stare civilă emise în ultimii 100 de ani, rezultatâîn urma activităţilor de digitizare a fondului de documente existent.

Situaţia actelor de stare civilă în perioada 1918 - 2017:

AN	ACTE_NAŞTERE	ACTE_CĂSĂTORIE	ACTE_DECES	TOTAL_AN
1918	198.442	93.035	506.176	797.653
1919	411.901	156.803	382.106	950.810
1920	408.194	163.225	325.866	897.285
1921	463.258	159.847	292.279	915.384
1922	476.259	141.702	301.965	919.926

AN	ACTE_NAȘTERE	ACTE_CĂSĂTORIE	ACTE_DECES	TOTAL_AN
1923	474.911	133.566	295.187	903.664
1924	474.412	129.635	302.139	906.186
1925	471.316	130.022	284.914	886.252
1926	465.005	143.837	297.655	906.497
1927	465.238	138.731	308.161	912.130
1928	476.051	126.440	284.634	887.125
1929	458.509	123.513	318.847	900.869
1930	477.057	128.018	266.684	871.759
1931	465.958	128.122	286.609	880.689
1932	509.770	133.358	292.630	935.758
1933	460.694	119.583	259.087	839.364
1934	472.310	132.859	295.468	900.637
1935	454.482	157.057	294.783	906.322
1936	484.067	137.892	282.224	904.183
1937	471.119	142.500	280.657	894.276
1938	461.813	137.698	276.694	876.205
1939	453.047	127.898	275.894	856.839
1940	420.787	135.678	285.842	842.307
1941	403.801	127.973	278.790	810.564
1942	365.333	120.607	309.606	795.546
1943	343.586	111.618	260.595	715.799
1944	366.012	90.761	303.442	760.215
1945	336.491	169.426	317.456	823.373

AN	ACTE_NAȘTERE	ACTE_CĂSĂTORIE	ACTE_DECES	TOTAL_AN
1946	393.633	183.944	289.922	867.499
1947	372.749	157.793	344.330	874.872
1948	381.402	177.870	246.576	805.848
1949	450.458	186.398	218.942	855.798
1950	721.906	218.258	202.926	1.143.090
1951	459.580	176.017	208.791	844.388
1952	467.273	179.062	195.247	841.582
1953	465.241	182.552	200.376	848.169
1954	463.898	208.016	193.032	864.946
1955	508.086	203.717	166.883	878.686
1956	465.690	210.333	173.791	849.814
1957	432.682	205.898	182.069	820.649
1958	412.956	210.852	159.150	782.958
1959	391.730	195.953	186.876	774.559
1960	370.264	200.407	161.216	731.887
1961	331.783	181.745	165.245	678.773
1962	312.403	185.944	170.438	668.785
1963	305.410	174.783	155.293	635.486
1964	295.149	170.774	151.778	617.701
1965	286.244	165.355	165.115	616.714
1966	286.051	170.949	155.318	612.318
1967	534.088	154.159	175.586	863.833
1968	538.857	148.322	187.017	874.196

AN	ACTE_NAȘTERE	ACTE_CĂSĂTORIE	ACTE_DECES	TOTAL_AN
1969	489.325	141.921	200.011	831.257
1970	438.162	149.417	193.097	780.676
1971	410.434	153.084	193.330	756.848
1972	397.433	158.510	187.772	743.715
1973	385.518	170.498	200.083	756.099
1974	435.445	178.078	190.151	803.674
1975	429.695	189.872	195.774	815.341
1976	430.769	197.756	203.469	831.994
1977	439.218	202.000	206.701	847.919
1978	427.818	202.533	214.607	844.958
1979	421.791	203.775	216.979	842.545
1980	431.946	185.707	231.109	848.762
1981	397.033	185.773	224.263	807.069
1982	355.894	177.783	223.534	757.211
1983	334.056	166.495	232.920	733.471
1984	359.696	167.332	233.591	760.619
1985	370.511	164.577	256.969	792.057
1986	429.890	170.799	243.111	843.800
1987	393.741	170.963	254.455	819.159
1988	394.113	176.147	255.024	825.284
1989	376.101	183.302	246.281	805.684
1990	331.286	194.903	248.152	774.341
1991	294.672	187.297	252.560	734.529

AN	ACTE_NAȘTERE	ACTE_CĂSĂTORIE	ACTE_DECES	TOTAL_AN
1992	273.701	176.700	263.876	714.277
1993	258.688	161.884	263.602	684.174
1994	256.883	156.853	265.019	678.755
1995	247.646	157.171	271.138	675.955
1996	238.840	153.660	284.485	676.985
1997	245.891	150.167	276.541	672.599
1998	248.769	149.250	266.345	664.364
1999	250.291	146.415	262.866	659.572
2000	253.784	142.207	253.077	649.068
2001	231.827	135.698	255.213	622.738
2002	240.400	140.056	266.947	647.403
2003	248.542	149.006	267.249	664.797
2004	235.499	152.330	258.180	646.009
2005	238.900	144.677	261.823	645.400
2006	234.994	151.056	255.858	641.908
2007	232.433	191.120	250.131	673.684
2008	237.061	146.920	249.982	633.963
2009	247.239	138.181	252.806	638.226
2010	231.453	116.730	251.295	599.478
2011	258.313	122.132	236.675	617.120
2012	248.189	117.869	254.121	620.179
2013	240.467	107.552	247.524	595.543
2014	252.102	126.540	250.321	629.789

AN	ACTE_NAȘTERE	ACTE_CĂSĂTORIE	ACTE_DECES	TOTAL_AN
2015	264.816	132.770	259.732	657.318
2016	254.072	139.887	258.547	652.506
2017	254.756	128.111	271.485	654.352
TOTAL	**37.680.571**	**15.932.349**	**24.781.088**	**78.394.008**
Acte întocmite la misiunile diplomatice în perioada (1968-2016)	**489.185**	**131.929**	**6.851**	**627.965**
TOTAL GENERAL	**38.169.756**	**16.064.278**	**24.787.939**	**79.021.973**

În perioada 1968-2017 au fost înregistrate acte de stare civilă şi la nivelul misiunilor diplomatice,acte care se află în păstrare în arhiva Direcţiei de Stare Civilă din cadrul Direcţiei Publice de Evidenţă a Persoanelor şi Stare Civilă a Sectorului 1 al mun. Bucureşti.

1.2. Entităţi implicate

Principalele entităţi care vor beneficia de implementarea proiectului sunt:

1. Autorităţi implicate în fluxurile de emitere a documentelor de stare civilăîn noul sistem:

   - Ministerul Afacerilor Interne (MAI) – DEPABD [1]
   - Consiliul Judeţean - Serviciul Public Judeţean de Evidenţă a Persoanelor [1]
   - Consiliul Local - Serviciul Public Comunitar Local de Evidenţă a Persoanelor [1]
   - Ofiţeri de Stare Civilă (UAT)

   -Număr de utilizatori UAT care actualizează sistemul – 6390 (ofiţeri de stare civila)

   - Ministerul Afacerilor Externe – 593 utilizatori

1 Aceste entităţi vor totaliza un număr de aproximativ 1500 de utilizatori.

- Ministerul Afacerilor Interne (MAI) - Direcția Generală de Pașapoarte – 505 utilizatori
- Notariat Public (CNARNN) – aprox. 3.000 utilizatori
- Ministerul Sănătății
- Ministerul Justiției
- Ministerul Afacerilor Interne (MAI)
- Parchetul de pe lângă Înalta Curte de Casație și Justiție
- Ministerul Apărării Naționale (MAPN)
- Laboratoare de Medicină Legale Județene/IML
- Ministerul Transporturilor

2. Beneficiari cu drept de consultare a unor date de stare civilă:

   - Ofițeri de Stare Civilă (UAT)

     -Număr de utilizatori UAT care accesează sistemul – 3747 utilizatori

   - Instituții ale statului;
   - Cetățeni.

1.3. Contextul proiectului

Prin implementarea acestui proiect se vor crea condițiile unei administrații moderne, eficace și eficiente, cât și premisele creșterii calității serviciilor oferite cetățenilor și reducerea timpului de soluționare a cererilor referitoare la furnizarea datelor cu caracter personal, în condițiile legii.

Interacțiunea instituțiilor publice cu societatea informațională determină reorganizarea proceselor instituționale (proceduri, metodologii de lucru, standarde și atribuții), regândirea strategică a managementului intern și asigurarea unui proces de continuă optimizare și perfecționare.

1.4. Situația actuală

Situația actuală privind înregistrareași eliberarea actelor de stare civilă cuprinde mai multe procese și proceduri, după cum urmează:

- Activitățile de stare civilă sunt efectuate la nivelul tuturor celor 3187 de unități administrativ-teritoriale din țară.

- Activitățile de stare civilă pot fi, de asemenea, efectuate şi de către şefii misiunilor diplomatice şi ai oficiilor consulare ale României din străinătate, comandanți de nave şi de aeronave care se află în afara teritoriului național, ofițerii militari de stare civilă desemnați prin ordine ale ministrului Apărării Naționale şi ministrului Afacerilor Interne, în limitele prevăzute de lege.

- În conformitate cu prevederile Legii nr.119/1996 cu privire la actele de stare civilă, republicată, cu modificările şi completările ulterioare, actele de stare civilă sunt întocmite prin utilizarea formularelor standardizate, securizate şi a procedurilor specifice (certificate).

- Actele de stare civilă sunt înscrisuri autentice prin care se dovedeşte naşterea, căsătoria sau decesul unei persoane. Pe baza actelor de stare civilă se eliberează certificate/extrase multilingvistice de stare civilă.

- Actele de stare civilă se întocmesc în interesul statului şi al persoanei şi servesc la cunoaşterea numărului şi structurii populației, a situației demografice, la apărarea drepturilor şi libertăților fundamentale ale cetățenilor.

- Actele de stare civilă (naştere, căsătorie şi deces) se întocmesc în registre de stare civilă, în două exemplare, ambele originale, exemplarul I, exemplarul II si se completeaza manual, cu cerneală specială de culoare neagră.

- Registrele şi certificatele/extrasele multilingvistice de stare civilă se păstrează în încăperi special amenajate, în dulapuri metalice închise, oferind astfel securitatea acestora.

- "Exemplarul I" al registrelor de stare civilă se păstrează la nivel local, în timp ce al doilea exemplar este trimis şi păstrat la nivel de județ. Intervalul de timp pentru păstrarea celor 2 registre este de 100 de ani; după expirarea acestei perioade, acestea sunt depozitate la nivelul Arhivelor Naționale.

- Operațiunile pentru întocmirea actelor de stare civilă implică şi transmiterea de comunicări de către alte instituții, în conformitate cu Metodologia pentru aplicarea unitară a dispozițiilor în materie de stare civilă, aprobată prin H.G. nr. 64/2011.

- Ofițerii de stare civilă înscriu mențiuni pe marginea actelor de stare civilă aflate în păstrare şi trimit comunicări de mențiuni pentru înscrierea în registrele de stare civilă - exemplarul I sau, după caz, exemplarul II.

- Orice modificare intervenită în statutul civil al unei persoane se comunică din oficiu, în termen de 10 zile, S.P.C.L.E.P. sau, după caz, ofiţerului de stare civilă din cadrul primăriei unităţii administrativ – teritoriale care a întocmit actul de naştere, de căsătorie sau de deces al persoanei la care această modificare se referă, în vederea înscrierii menţiunilor corespunzătoare (art. 8 din Legea 119/1996). În cazul în care exemplarul I al actelor de naştere, căsătorie sau de deces ale unei persoane a fost întocmit şi se află în păstrarea aceluiaşi S.P.C.L.E.P. sau ale aceleiaşi primării, ofiţerul de stare civilă operează menţiunea corespunzătoare pe marginea acestora, după care întocmeşte şi trimite comunicare de menţiune la structura de stare civilă din cadrul S.P.C.J.E.P., sau, după caz, D.G.E.P. a mun. Bucureşti – D.S.C. care are în păstrare registrele de stare civilă exemplarul II.

- Comunicările de menţiuni pentru registrele de stare civilă exemplarul I şi II se întocmesc pe formulare prevăzute de H.G. nr. 64/2011 pentru aprobarea Metodologiei cu privire la aplicarea unitară a dispoziţiilor în materie de stare civilă, cu modificările şi completările ulterioare, şi se expediază în termen de 10 zile (art. 88).

- Ofiţerul de stare civilă care primeşte comunicarea de menţiune o înregistrează în registrul de intrare – ieşire, după care operează menţiunea pe exemplarul I al registrului de stare civilă – art. 89 din HG nr. 64/2011.

- Pe comunicare se înscrie următorul text : «Operat menţiunea, numărul actului/anul, data operării», semnătura ofiţerului de stare civilă; efectuarea înscrierii menţiunii se consemnează în registrul de intrare – ieşire, prin înscrierea următorului text : «Operat menţiunea, actul numărul ...../anul».

- După înscrierea menţiunii pe exemplarul I al registrului cu acte de stare civilă, se trimite comunicare de menţiune la structura de stare civilă care are în păstrare exemplarul II.

- În cazul în care exemplarul II al registrului nu a fost predat, nefiind încheiat, operarea menţiunii se face şi în acesta, iar comunicarea se trimite structurii de stare civilă din cadrul S.P.C.J.E.P. respectiv D.G.E.P.M Bucureşti – DSC, pentru arhivare.

- În cazul în care exemplarul I al registrului de stare civilă este distrus sau pierdut, comunicările de menţiune se expediază pentru a fi operate pe exemplarul II al registrului; în comunicare se face menţiunea că pe actul de stare civilă exemplarul I nu s-a operat, registrul fiind pierdut sau distrus (art. 89 alin. 4 din HG nr. 64/2011).

- În cazul în care lipseşte şi registrul de stare civilă exemplarul II, despre aceasta se menţionează pe comunicare, după care se arhivează în dosarul de comunicări neoperabile, până la reconstituirea actului (art. 89 alin. 5 din HG nr. 64/2011).

- Comunicările de menţiuni se arhivează după înscrierea acestora pe exemplarele I şi II ale registrelor de stare civilă; pentru menţiunile neoperabile se ţine o evidenţă separată.

- Toate activităţile desfăşurate în cadrul acestui flux sunt în conformitate cu dispoziţiile H.G. nr. 64/2011 pentru aprobarea Metodologiei cu privire la aplicarea unitară a dispoziţiilor în materie de stare civilă, cu modificările şi completările ulterioare.

1.5. Beneficiile proiectului

Beneficiile implementarii proiectului se regăsesc,în primul rând,în calitatea serviciilor oferite către cetăţeni (G2C), dar şi la nivel guvernamental, instituţional şi de colaborare între instituţiile implicate în procesul de eliberare,precum şi în cel de declanşare a proceselor de eliberare a actelor de stare civilă.

1.5.1. Beneficii pentru cetăţean (G2C)

Punerea la dispoziţia cetăţeanului a unui **portal** (accesibil prin Internet) prin intermediul căruia acesta va beneficia, în condiţiile legii, de diverse servicii electronice (intermedierea transferului autentificat al datelor proprii de stare civilă către terţe instituţii prestatoare de servicii pentru cetăţean, descărcare formulare electronice, descărcare/transmitere formulare/cereri, obţinerea unui document în format electronic cu datele conţinute în registrele de stare civilă, verificarea datelor personale proprii, transfer unidirecţional/bidirecţional de informaţii către cetăţean, programarea on-line în vederea accesării serviciilor; serviciu de suport/helpdesk). Precizăm că, în prezent, în majoritatea cazurilor, informaţiile referitoare la desfăşurarea activităţilor de stare civilă sunt afişate la avizierul oficiului de stare civilă;

- Creşterea gradului de transparenţă a prelucrării datelor de stare civilă, oferind cetăţeanului atât posibilitatea de a vizualiza datele de stare civilă înregistrate în sistem, cât şi un instrument de monitorizare permanentă a stadiului soluţionării cererii. Precizăm că, în prezent, cetăţeanul nu are acces la aceste informaţii;

- Reducerea procentului de eroare în procesul de prelucrare a informaţiilor de stare civilă, prin asistarea şi prelucrarea automată a acestora, respectiv prin compararea datelor prezentate cu cele existente în Registrul Naţional de Evidenţă a Persoanelor (RNEP);
- Reducerea timpului necesar emiterii unui certificat/extras multilingv de stare civilă prin prelucrarea cu mijloace IT a datelor aferente, tipărirea automată a certificatelor/extraselor şi reducerea/eliminarea activităţilor executate manual de către operator;
- Asigurarea confidenţialităţii, integrităţii şi disponibilităţii datelor personale ale cetăţeanului în timpul prelucrării informaţiilor de stare civilă, prin utilizarea unor tehnologii avansate de securitate şi protecţie. Utilizarea de către ofiţerul de stare civilă a unei interfeţe web care va realiza un echilibru între activităţile specifice de protecţie a datelor şi cele necesare pentru o accesibilitate şi utilizare facilă a acestora;
- Accesul securizat al cetăţeanului la cele mai recente informaţii publice privind reglementări, proceduri, decizii, tarife şi paşii de urmat pentru obţinerea certificatelor/extraselor multilingve de stare civilă, tipărirea şi descărcarea de formulare, expedierea de solicitări de informaţii bazate pe formulare-tip;
- Servicii de tip e-guvernare oferite cetăţeanului prin interconectarea SIIEASC cu alte instituţii publice;
- Documentele necesare pe care cetăţeanul este obligat să le prezinte la desfăşurarea evenimentului de stare civilă (ex. alte certificate de stare civilă, copii de pe documente de identitate etc.), conform legislaţiei, vor fi necesare doar la prima înregistrare în sistem (vor fi scanate), ulterior acestea nu vor mai fi aduse de cetăţean, ele fiind descărcate/consultate direct din arhiva electronică. Arhiva electronică, astfel creată, va putea fi folosită în interesul cetăţeanului şi în derularea altor activităţi de emitere a documentelor;
- Pentru soluţionarea unor cereri ale cetăţenilor pe linie de stare civilă nu se vor mai prezenta documentele necesare în condiţiile în care pot fi descărcate/consultate direct din arhiva electronică. Arhiva electronică, astfel creată, va putea fi folosită în interesul cetăţeanului şi în derularea altor activităţi de emitere a documentelor;
- Toate taxele aferente serviciilor publice furnizate prin sistem vor putea fi achitate online, prin integrarea sistemului SIIEASC cu Sistemul naţional electronic de plată online a taxelor şi impozitelor utilizând cardul bancar (SNEP, www.ghiseul.ro) realizat prin HG nr. 1235/2010 cu toate modificarile ulterioare. Integrarea sistemelor

informatice se va implementa utilizand standardele si interfetele de interconectare puse la dispozitie prin intermediul sistemului SNEP.

- Gestionarea coerentă şi asistată, prin mijloace IT avansate, a unui volum important de activităţi pe linie de stare civilă. În acest context, prezentăm, statistica privind actele şi certificatele de stare civilă pentru anul 2017:

Acte de naştere	Acte de căsătorie	Acte de deces	Total	Certificate de naştere eliberate	Certificate de căsătorie eliberate	Certificate de deces eliberate	Total
254.756	128.111	271.485	654.352	569.886	205.114	346.919	1.121.919

1.5.2. Beneficii pentru instituţii publice (G2G)

- Asigurarea transferului de extrase de stare civilă, în format electronic, semnate cu semnătura calificată, între unităţile/structurile administraţiei publice locale şi centrale, conform legislaţiei; asigurarea fluxului de date de stare civilă între autorităţi şi cetăţean, pentru date înregistrate deja în sistem informatic. Se va asigura atât accesul oficiilor de stare civilă la SIIEASC, cât şi accesul altor instituţii abilitate la acest sistem. Solicitările cetăţenilor vor ajunge rapid şi sigur la autoritatea competentă să le soluţioneze;
- Reducerea timpului mediu de procesare pentru actualizarea informaţiilor de stare civilă în SNIEP;
- Creşterea acurateţei şi disponibilităţii datelor de stare civilă înregistrate în sistem;
- Reducerea cheltuielilor de stocare a informaţiilor de stare civilă pentru administraţiile publice care au atribuţii în domeniul de referinţă;
- Asigurarea accesului la informaţiile din SIIEASC (constituit la nivel central) tuturor oficiilor de stare civilă, respectiv tuturor serviciilor publice comunitare de evidenţă a persoanelor;
- Eliminarea redundanţei datelor din diverse sisteme informatice ale instituţiilor implicate şi posibilitatea integrării cu alte sisteme informatice legal-abilitate, beneficiare ale informaţiilor de stare civilă, care sunt funcţionale sau vor fi dezvoltate la nivel european, naţional şi local;

- Asigurarea unui mediu operaţional partajat, precum şi a unei securităţi crescute a datelor electronice, informaţiilor şi schimburilor de documente în cadrul şi între autorităţile publice şi, de asemenea, susţinerea serviciilor de interes naţional.

1.5.3. Beneficii generale

- reducerea birocraţiei prin eliminarea treptată a evidenţelor manuale, respectiv simplificarea fluxului de activităţi pe linie de stare civilă (eliminarea exemplarului nr. 2 a Registrelor de stare civilă, reducerea numărului de documente prezentate de cetăţean în format hârtie, eliminarea corespondenţei în format hârtie între instituţiile care procesează informaţii de stare civilă etc.);
- informații online / în timp real pentru cetățeni și operatorii sistemului;
- standardizarea datelor şi acurateţii informațiilor gestionate de sistem;
- flexibilitate în abordarea problemelor cetățenilor;
- asigurarea unui mediu electronic standardizat pentru centralizarea informației cu privire la documentele de stare civilă;
- colectarea informațiilor la nivel național, în timp real, și transpunerea/accesarea lor facilă de către toți operatorii implicați în procesul de emitere, aprobare și gestiune al acestor documente;
- asigurarea transparenței activităților desfășurate de instituțiile statului;
- simplificarea procesului de culegere, introducere, modificare, aducere la zi și eliberare a informațiilor destinate publicului larg;
- asigurarea unui mediu electronic de tip "one stop shop" pentru serviciile oferite de către DEPABD și instituțiile implicate (SPCLEP, spitale, notariate etc.) în relația cu documentele de stare civilă ale cetățenilor;
- oferirea către cetățeni, operatorii sistemului și instituțiile implicate a unui mediu electronic de încredere, alternativă la procesul actual consumator de timp și resurse;
- reducerea timpului necesar înregistrării, completării și depunerii documentației necesare pentru emiterea sau eliberarea unui document de stare civilă;
- asigurarea unui mediu electronic standardizat pentru centralizarea documentelor/informației aferente fiecărui tip de document gestionat de sistem;
- centralizarea, în format electronic, a informațiilor cu privire la documentele istorice de stare civilă din ultimii 100 de ani;

- evitarea aglomerării birourilor pentru emiterea şi aprobarea fluxurilor de documente de stare civilă, prin oferirea unui instrument modern de completare/ transmitere/ validare a informaţiilor necesare;
- posibilitatea interconectării/interoperabilizării cu sistemele informatice ale insituţiilor implicate (sistemul SNIEP etc.) pentru schimbul bidirecţional de date.
- optimizarea şi standardizarea fluxurilor asociate activităţilor de stare civilă.

2. Cerinţe funcţionale şi tehnice

2.1. Cerinţe funcţionale ce trebuie îndeplinite de SIIEASC

SIIEASC va trebui să respecte cerinţele legislative privind gestionarea procedurilor de stare civilă şi de documentare.

Acest capitol descrie procesele majore şi procedurile operaţionale pe care Furnizorul le va implementa:

1. **Înregistrarea naşterii** şi toate celelalte funcţii conexe, în conformitate cu cerinţele legale privind: înregistrarea naşterii copilului din căsătorie; înregistrarea naşterii copilului în afara căsătoriei; recunoaşterea nou-născutului de către tatăl biologic; înregistrarea bebeluşilor născuţi morţi; înregistrarea nou-născutului decedat în termen de 30 zile de la naştere; înregistrarea copilului găsit; înregistrarea unui copil nou-născut şi abandonat în spaţiile unităţilor medicale, înregistrarea naşterii după împlinirea termenului de 30 zile.

2. **Înregistrarea căsătoriei** şi toate celelalte funcţii conexe, în conformitate cu cerinţele legale în ceea ce priveşte căsătoria între doi cetăţeni români, căsătoria între un cetăţean român şi un cetăţean străin şi căsătoria între doi cetăţeni străini.

3. **Înregistrare decesului** şi toate celelalte funcţii conexe, în conformitate cu cerinţele legale în ceea ce priveşte decesul în România a oricărui cetăţean român sau cetăţean străin, inclusiv moartea prin sinucidere, accidente şi alte cauze violente, precum şi înregistrarea de deces, după expirarea celor 3 zile de perioadă legală pentru declararea decesului unei persoane sau în baza hotărârilor declarative de moarte.

4. **Transcrierea actelor** de stare civilă, precum şi toate celelalte funcţii conexe, în conformitate cu cerinţele legale în ceea ce priveşte certificatele de naştere străine, căsătorie şi deces.

5. **Eliberarea certificatelor** de stare civilă şi a extraselor multilingve ale actelor de stare civilă, la cerere, în conformitate cu cerinţele legale.

6. **Schimbarea numelui de familie şi prenumelui** şi toate celelalte funcţii conexe în conformitate cu cerinţele legale.

7. **Rectificarea actelor de stare civilă şi a menţiunilor înscrise pe marginea acestora,** precum şi toate celelalte funcţii conexe în conformitate cu cerinţele legale.

8. **Înregistrarea adopţiilor** şi toate celelalte funcţii conexe în conformitate cu cerinţele legale.

9. **Înregistrarea hotărârilor/certificatelor de divorţ**, constatarea desfacerii căsătoriei prin acordul soţilor de către ofiţerul de stare civilă şi toate celelalte funcţii conexe în conformitate cu cerinţele legale.

10. **Înscrierea menţiunilor în registrele de stare civilă şi toate celelalte funcţii conexe în conformitate cu cerinţele legale.**

11. **Reconstituirea şi întocmirea ulterioară a actelor de stare civilă şi toate celelalte funcţii conexe în conformitate cu cerinţele legale.**

12. **Anularea, modificarea sau completarea actelor de stare civilă şi a menţiunilor înscrise pe marginea acestora şi toate celelalte funcţii conexe în conformitate cu cerinţele legale.**

13. **Atribuirea, înscrierea şi gestionarea C.N.P. şi toate celelalte funcţii conexe în conformitate cu cerinţele legale.**

14. **Eliberarea adeverinţelor de către ofiţerul de stare civilă** (anexa nr. 9, anexa nr. 11, anexa nr. 12 la Metodologia cu privire la aplicarea unitară a dispoziţiilor în materie de stare civila, aprobată prin H.G. nr. 64/2011, cu modificările şi completările ulterioare).

15. **Emiterea extraselor de uz extern de către Direcţia pentru Evidenţa Persoanelor şi Administrarea Bazelor de Date.**

16. **Înscrierea menţiunilor privind înregistrarea numelui/prenumelui cu ortografierea limbii materne şi toate celelalte funcţii conexe în conformitate cu cerinţele legale.**

17. **Înscrierea menţiunilor privind modificările intervenite în statutul civil precum şi cele privind schimbarea numelui şi/sau prenumelui intervenite în străinătate şi toate celelalte funcţii conexe în conformitate cu cerinţele legale.**

18. **Înscrierea menţiunilor privind acordarea sau renunţarea la cetăţenia română şi toate celelalte funcţii conexe în conformitate cu cerinţele legale.**

19. **Înregistrarea actelor de stare civilă în caz de mobilizare, război ori participare la misiuni de menţinere a păcii sau în scop umanitar.**

20. **Înregistrarea naşterii, căsătoriei sau decesului în cazul în care are loc în tren, pe o navă ori o aeronavă.**

Gestiunea documentelor de stare civilă se va realiza, în mod centralizat, de către sistemul integrat, prin administrarea fluxurilor şi proceselor privitoare la emiterea actelor de stare civilă.

Furnizorul sistemului va face, în etapa de evaluare, o analiză a fluxurilor actuale şi va propune îmbunătăţiri ale acestora (se vor utiliza standarde şi/sau metode recunoscute internaţional).

Din punct de vedere al fluxurilor logice, următoarele tipuri de documente de stare civilă vor fi gestionate de sistemul propus:

Indicativ	**Denumire document de stare civilă/document necesar în activitatea de stare civilă**
1	Certificat de căsătorie
2	Act de identitate
3	Certificat medical constatator al naşterii
4	Declaraţie cu privire la numele de familie şi/sau al prenumelui copilului
5	Declaraţie cu privire la domiciliul copilului
6	Declaraţie de recunoaştere a copilului născut în afara căsătoriei

Indicativ	Denumire document de stare civilă/document necesar în activitatea de stare civilă
7	Dovada discernământului tatălui minor la momentul recunoaşterii
8	Certificat de naştere
9	Certificat de stare civilă eliberat de autorităţile străine, fotocopie, traducere legalizată, după caz
10	Paşaport
11	Documentul de identitate eliberat de Inspectoratul General pentru Imigrări
12	Declaraţia notarială a titularului documentului străin prin care se face legitimarea dacă din documentele prezentate nu rezultă în mod distinct care este numele de familie şi prenumele
13	Certificatul de căsătorie al părinţilor cetăţeni străini, în original, precum şi traducerea legalizată a acestuia
14	Fotocopia procesului-verbal întocmit de poliţist cu ocazia verificărilor efectuate la solicitarea unităţii sanitare în care a avut loc naşterea, certificată pentru conformitate de reprezentatul unităţii sanitare
15	Declaraţia scrisă a persoanei în cazul în care naşterea mamei nu este înregistrată în registrele de stare civilă
16	Procesul-verbal privind identitatea declarată de mamă, semnat de reprezentantul D.G.A.S.P.C., de reprezentantul poliţiei şi de cel al unităţii sanitare
17	Dispoziţie emisă de primar de stabilire a numelui
18	Declaraţie privind înregistrarea naşterii peste termenul legal de 30 zile
19	Referatul cuprinzând avizul conform al S.P.C.J.E.P. sau, după caz, al

Indicativ	Denumire document de stare civilă/document necesar în activitatea de stare civilă
	D.G.E.P.M.B. şi aprobarea primarului privind înregistrarea tardivă a naşterii
20	Expertiza medico-legală în cazul înregistrării naşterii unei persoane în lipsa certificatului constatator al naşterii
21	Raportul de anchetă socială/Adresa SPAS pentru efectuarea anchetei sociale
22	Delegaţia reprezentantului D.G.A.S.P.C. sau S.P.A.S.
23	Referat ofiţer de stare civilă privind reconstituirea/întocmirea ulterioară a actului
24	Adresă înaintare documente pentru aviz la S.P.C.J.E.P. sau, după caz, la D.G.E.P.M.B.
25	Declaraţia persoanei care solicită înregistrarea dacă a dat naştere unui copil
26	Rezultatul verificărilor efectuate în evidenţele Direcţiei Generale de Paşapoarte şi ale serviciului cazier judiciar, statistică şi evidenţe operative
27	Rezultatul verificărilor efectuate de către unităţile de poliţie la adresele la care persoanele neînregistrate declară că au locuit, precum şi, după caz, la unităţile de învăţământ la care declară că au fost înscrişi
28	Declaraţia persoanei a cărei naştere nu a fost înregistrată, precum şi, după caz, a părinţilor sau reprezentantului legal ai/al persoanei
29	Declaraţia a doi membri ai familiei, iar în lipsa acestora, a două persoane care cunosc persoana neînregistrată
30	Adresa IGP prin care certifică/nu certifică imaginea facială şi impresiunile papilare
31	Declaraţia privind înregistrarea naşterii copilului părăsit de mamă în maternitate

Indicativ	Denumire document de stare civilă/document necesar în activitatea de stare civilă
32	Proces - verbal întocmit în cazul găsirii sau părăsirii unui copil, precum şi a cadavrului neidentificat
33	Dispoziţie de plasament în regim de urgenţă emisă de instanţa de tutelă
34	Comunicarea poliţiei, în cazul părăsirii unui copil, cu privire la identitatea mamei
35	Declaraţie scrisă a persoanei care a găsit copilul/reprezentant SPAS
36	Expertiza medico-legală întocmită în cazul găsirii unui copil
37	Cerere de transcriere
38	Certificat de cetăţenie
39	Procură notarială
40	Extrasul multilingv al actului de naştere
41	Declaraţie că nu s-a mai solicitat transcrierea
42	Avizul prealabil al Direcţiei Judeţene de Evidenţă a Persoanelor
43	Aprobarea primarului
44	Adresa MAE cuprinzând verificări cu privire la înregistrarea naşterii în străinătate
45	Certificat medical constatator eliberat de autorităţile străine
46	Extras din jurnalul de bord
47	Extras din carnetul de drum

Indicativ	Denumire document de stare civilă/document necesar în activitatea de stare civilă
48	Cerere privind reconstiuirea/întocmirea ulterioară a actului
49	Dispoziţia primarului
50	Sentinţă judecătorească (la naştere, căsătorie şi deces, adopţie, divorţ, schimbare de nume ca urmare a schimbării sexului)
51	Sentinţă de recunoaştere a efectelor hotărârii străine
52	Declaraţia de căsătorie
53	Certificat medical prenupţial
54	Declaraţii ale soţilor că se pot căsători
55	Publicitatea la căsătorie
56	Extrase/copii de pe actele de căsătorie cu menţionarea regimului matrimonial la Registrul Naţional Notarial al Regimurilor Matrimoniale
57	Certificat de deces
58	Certificat de divorţ (stare civilă sau notar)
59	Aprobarea primarului pentru încheierea căsătoriei (diverse situaţii)
60	Convenţie matrimonială, fotocopie, traducere legalizată, după caz
61	Aviz medical
62	Aprobare părinţi
63	Hotărârea/Autorizare instanţă de tutelă

Indicativ	Denumire document de stare civilă/document necesar în activitatea de stare civilă
64	Proces - verbal întocmit de ofiţerul de stare civilă la naştere, căsătorie şi divorţ sau la atribuire C.N.P.
65	Document eliberat de misiuni diplomatice acreditate în România pentru căsătorie
66	Documente necesare căsătoriei eliberate de autorităţile străine
67	Declaraţie din partea soţilor cu privire la numele purtat după căsătorie/divorţ
68	Extrasul multilingv al actului de căsătorie
69	Cerere de divorţ
70	Declaraţie privind locuinţa comună
71	Declaraţie de stăruinţă sau de renunţare la procedură (pentru divorţ administrativ)
72	Certificat medical constatator al decesului
73	Declaraţie privind motivul neprezentării certificatelor de stare civilă/act de identitate
74	Documentul de evidenţă militară a celui decedat
75	Adresă transmitere documente de identitate/paşapoarte ale decedatului, cetăţean strain la Inspectoratul General pentru Imigrări/Direcţia Generală de Paşapoarte
76	Dovada eliberată de poliţie
77	Dovada eliberată de parchet
78	Extrasul multilingv al actului de deces

Indicativ	Denumire document de stare civilă/document necesar în activitatea de stare civilă
79	Cerere înscriere, pe marginea actului de stare civilă, a menţiunilor intervenite în străinătate
80	Sentinţă judecătorească/document administrativ/certificat de divorţ pronunţat/ă în străinătate, fotocopie, traducere legalizată, după caz
81	Sentinţă judecătorească pronunţată în străinătate/document administrativ de recunoaștere și/sau încuviințare purtare nume, fotocopie, traducere legalizată, după caz
82	Sentinţă judecătorească pronunţată în străinătate/document administrativ privind rectificarea, completarea sau modificarea, fotocopie, traducere legalizată, după caz
83	Sentinţă judecătorească pronunţată în străinătate/document administrativ de schimbare a numelui de familie și/sau a prenumelui, fotocopie, traducere legalizată, după caz
84	Cerere eliberare certificate de stare civilă/extrase multilingve ale actelor de stare civilă
85	Cerere rectificare act stare civilă
86	Cerere de schimbare a numelui
87	Monitorul Oficial al României, Partea a III-a, în care a fost publicat extrasul din cererea de schimbare a numelui/Dovadă scutire de publicitate
88	Referatul ofiţerului de stare civilă cu propunere de aprobare/respingere de către primar
89	Referatul D.J.E.P.cu propunere de aprobare/respingere

Indicativ	Denumire document de stare civilă/document necesar în activitatea de stare civilă
90	Dispoziţia Preşedintelui Consiliului Judeţean/ Primarului General al municipiului Bucureşti
91	Adresă de comunicare a schimbării numelui şi/sau a prenumelui la Direcţia Generală de Paşapoarte, Direcţia cazier judiciar, statistică şi evidenţe operative din cadrul Inspectoratului General al Poliţiei Române şi Direcţiei generale a finanţelor publice judeţene sau, după caz, Direcţiei Generale a Finanţelor Publice a Municipiului Bucureşti din cadrul Agenţiei Naţionale de Administrare Fiscală
92	Cerere de ortografiere/traducere nume în limba maternă
93	Cerere modificare CNP
94	Avizul S.P.C.L.E.P.
95	Aprobare D.E.P.A.B.D.
96	Cerere eliberare anexa nr. 9 la HG.. nr. 64/2011
97	Cerere certificate anexa nr. 11 din H.G. nr. 64/2011
98	Adeverinţă anexa nr. 12 din H.G. nr. 64/2011
99	Cazier judiciar
100	Cazier fiscal/Declaraţie pe propria răspundere
101	Declaraţia de consimţământ
102	Alte documente raportat la modificările legislative

Fluxurile de lucru vor fi implementate astfel încât să permită înregistrarea tuturor cererilor pe linie de stare civilă, potrivit legislaţiei în domeniu. Documentele specifice necesare pentru înregistrarea fiecărui tip de cerere şi iniţiere a procesului pentru aceasta sunt descrise în continuare.

2.1.1. Procesele pentru documente de naşteri

PROCES	ACTE NECESARE
La spital, ambii părinţi cu acelaşi nume de familie	1,2,3,4
La spital, ambii părinţi cu acelaşi nume de familie, domicilii diferite	1,2,3,4,5
La spital, părinţii cu nume de familie diferite	1,2,3,4
La spital, mamă necăsătorită	2,3 (6,7după caz)
La spital, mamă minoră	2,3,8 (6,7după caz)
La spital, mamă singură, tatăl recunoaşte copilul	2,3,4,5,6 (7 după caz)
Naştere acasă, în oricare din situaţiile prezentate anterior	1,2,3,8 (4,5,6,7după caz)
Naştere la spital sau acasă, unul sau ambii părinţi cetăţean/cetăţeni străini	1,2,3,9,10 (4,5,6,11,12,13după caz)
Înregistrarea naşterii în lipsa actului de identitate al mamei	1,2,3,14 (4,5,6,7,10,11, 12,13 după caz)
Înregistrarea naşterii în cazul în care naşterea mamei nu este înregistrată în registrele de stare civilă	2,3,15,16,17 (4,5,6,7,10,11, 12,13 după caz)

PROCES	ACTE NECESARE
Înregistrarea tardivă a naşterii după 30 zile copil cu vârstă până la 14 ani	2,3,18,19, 21,22,23,24 (1,4,5,6,7,10, 11,12,13, 20,21,22 după caz)
Înregistrarea tardivă a naşterii – copil cu vârstă între 14 şi 18 ani	2,3,18,19,20, 21,22,23,24,25,26,27,28,29,30 (1,4,5,6,7,10, 11,12,13,20,21,22 după caz)
Înregistrarea tardivă a naşterii persoanei majore	3, ,23,24, 26,27, 29,30 (20,21,22 după caz)
Copil părăsit de mamă în maternitate	3,17,31,32,33, 34
Copil găsit	17,32,33,35,36
Copil născut în străinătate (transcriere)	1,2,8,9,10,37,38,39,40,41,42,43 1, 5, 39 după caz)
Copil născut în străinătate şi neînregistrat la autorităţile locale sau la misiunile diplomatice sau înregistrat cu date nereale	2,44/45,18 , (4,5,6,7,10,11, 12,39 după caz)
Copil născut pe navă sau aeronavă	46/47
Înregistrare act ca urmare a reconstituirii sau întocmirii ulterioare	23,42,48,49

2.1.2. Procesele pentru documente de adopţie

PROCES	ACTE NECESARE
Adopţie în ţară, ambii părinţi cetăţeni români	2,8,50
Adopţie în ţară, unul sau ambii părinţi cetăţeni străini	2,8,9,10,50
Adopţie în străinătate	2,8,9,10,50,51

2.1.3. Procesele pentru documente de căsătorie

PROCES	ACTE NECESARE
Căsătorie ambii soţi români	2,8,52,53,54,55,56 (50,57,58,59,60 după caz)
Căsătorie ambii soţi români, unul sau ambii soţi minori	2,8,52,53,54,55,56,61,62, 63 (50,57,58,59,60 după caz)
Căsătorie viitorii soţi rude până la gradul IV	2,8,52,53,54,55,56,63 (59,60 după caz)
Căsătorie unul sau ambii soţi cetăţean/cetăţeni străini	2,8,9,10,52,53,54, 55,56,64,65/66 (50,57,58,59,60 după caz)
Căsătorie încheiată în străinătate (transcriere)	2,8,9,10,37,38,41, 42,43,67,68, (39 după caz)
Căsătorie încheiată pe nave în afara apelor teritoriale ale României	46
Înregistrare act ca urmare a reconstituirii sau întocmirii ulterioare	23,42,48,49 (2, 10 după caz)

2.1.4. Procesele pentru documente de divorţ

PROCES	ACTE NECESARE
Divorţ pe cale judiciară	1,2,10,50
Divorţ, prin acordul soţilor, pe cale administrativă	1,2,8,69,71 (10,64,70 după caz)
Divorţ, prin acordul soţilor, pe cale notarială	58

2.1.5. Procesele pentru documente de deces

PROCES	ACTE NECESARE
Deces la spital sau acasă	1,2/10, 8,72, (73,74,75 după caz)
Deces survenit din cauze violente	1,2/10, 8,72, 76/77 (73,74,75, după caz)
Deces declarat tardiv	1,2/10, 8,72,,76,77 (73,74,75, după caz)
Cadavru neidentificat	2,32,72,76,77
Declararea judecătorească a decesului	2,8,50
Deces produs în străinătate (transcriere)	1,2/10, 8,9,37, ,42,43,78 (39, după caz)
Deces produs pe navă/aeronavă în afara apelor teritoriale române	46/47
Înregistrare act ca urmare a reconstituirii sau întocmirii ulterioare	23,42,48,49 (1, 2, 8, 57 după caz)

2.1.6. Procesele pentru înscrierea menţiunilor privind modificările intervenite în străinătate (casătorie, deces, divorţ, recunoaştere filiaţiei, încuviinţare purtare nume, schimbare nume, rectificare, completare, modificare, regim matrimonial)

PROCES	ACTE NECESARE
Înscrierea menţiunilor privind căsătoria	9,79, 95
Înscrierea menţiunilor privind căsătoria şi decesul	9,79, 95
Înscrierea menţiunilor privind căsătoria şi divorţul	9,51,79,80, 95 (67 după caz)
Înscrierea menţiunilor privind decesul	9,79, 95
Înscrierea menţiunilor privind divorţul	79,80, 95 (51, 67 după caz)
Înscrierea menţiunilor privind recunoaşterea filiaţiei	9,79,81, 95 (51 după caz)
Înscrierea menţiunilor privind recunoaşterea filiaţiei şi Încuviinţarea purtării numelui	9,79,81, 95 (51 după caz)
Înscrierea menţiunilor privind încuviinţarea purtării numelui	9,79,81, 95 (51 după caz)
Înscrierea menţiunilor privind rectificarea, completarea sau modificarea	9,79,82 , 95(51 după caz)

Înscrierea menţiunilor privind schimbarea numelui/prenumelui	9,79,83, 95 (51 după caz)
Înscrierea menţiunilor privind regimul matrimonial	60, 2/10, 95

2.1.7. Alte procese de stare civilă

PROCES	ACTE NECESARE
Eliberarea certificatelor de stare civilă/extrase/extrase multilingve/eliberarea adeverinţei de înhumare/incinerare	2, ,84 (10, 39 după caz)
Rectificarea actelor de stare civilă şi a menţiunilor înscrise pe marginea acestora	2,23,42,49,85
Schimbarea numelui de familie şi prenumelui	1,2,8,86,87,88,89, 90,91, 99, 100 (63, 101 după caz)
Ortografierea numelui/prenumelui persoanelor fizice	1,8,23,43,57,92
Anularea, modificarea sau completarea actelor de stare civilă şi a menţiunilor înscrise pe marginea acestora	50
Atribuirea, înscrierea şi gestionarea C.N.P.	1,8,43,57,64,93,94
Întocmire extras uz extern DEPABD (căsătorie şi deces în România a unui cetăţean străin)	
Eliberarea Adeverinţei tip anexa nr. 9 la H.G. 64/2011	2, 96, (39 după caz)
Eliberarea certificatului care atestă componenţa familială (anexa nr. 12 din H.G. 64/2011)	2,97,98

În etapa de analiză vor fi identificate şi detaliate toate procedurile, fluxurile şi documentele necesare activităţii de stare civilă care vor fi gestionate de SIIEASC,potrivit reglementărilor legale în domeniu.

Totodată, pe perioada derularii contractului, Furnizorul va avea în vedere atât implementarea eventualelor modificări/actualizări ale cadrului normativ aferente domeniului stării civile la nivelul SIIEASC, cât şi dezvoltarea sistemului informatic astfel încât să fie posibilă trecerea la o nouă etapă, respectiv eliminarea documentelor completate olograf -fără costuri adiţionale pentru Autoritatea Contractantă.

2.2. Cerinţe generale

SIIEASC va trebui să asigure un schimb de informaţii automatizat, standardizat, uşor de gestionat şi să ofere un nivel de accesibilitate securizat. Asigurarea unui schimb consistent de informaţii şi date de stare civilă se poate realiza doar în condiţiile abordării multi-nivel pentru interoperabilitate:

- La nivel legal – baza legală pentru eliberarea documentelor de stare civilăşi actualizarea evidenţelor acestora, inclusiv prin susţinerea eliminării anumitor formulare tipizate imprimate şi identificarea unică a persoanelor;
- La nivel organizaţional – logistică pentru eliberarea documentelor, eliberarea documentelor de stare civilă, recunoaşterea instituţiilor care concură la eliberarea acestora;
- La nivel semantic – codificări, nomenclatoare, evidenţele existente de evidenţă a persoanelor etc.;
- La nivel tehnic – sintaxa, standarde de mesagerie, reţele, comunicaţii.

În plus, la nivel tehnic, soluția adoptată trebuie să îndeplinească următoarele cerințe:

- Platforma software să suporte standarde deschise, fiind necesar a fi compatibilă cu serverele care respectă specificațiile non-proprietare şi standardele existente.
- Nu sunt permise pierderi de date la transferul spre/dinspre baza de date.
- Aplicația va fi dezvoltată urmărind o arhitectură în trei straturi (interacțiunea dintre aplicație şi baza de date, logica de aplicație, interfața cu utilizatorul).
- Sistemul informatic trebuie proiectat, dezvoltat/configurat, instalat, testat şi operaționalizat ca un sistem complet integrat, scalabil, deschis, extensibil, flexibil, cu atribute înalte de securitate şi disponibilitate, interoperabil cu alte sisteme informaţionale, prin interfeţe care vor fi descrise mai jos.
- Utilizarea unei arhitecturi modulare care să permită o cuplare redusă între componente şi în care responsabilitățile fiecărei componente sunt specializate.
- Structura modulară documentată astfel încât să permită atât dezvoltarea, modificarea fiecarui modul în mod separat de celelalte, cât si adăugarea de noi module fără modificări în modulele software finalizate.
- Pentru maximizarea modularității sistemului informatic, cu excepția compresiei, decompresiei, criptării şi decriptării datelor, prelucrarea datelor nu se va realiza prin

proceduri stocate în interiorul SGBD ci prin alte mecanisme (de exemplu: utilizarea microserviciilor, migrarea dintr-un SGBD într-altul fără a necesita o convertire semantică în exteriorul SGBD).

- Se va respecta regula protecției datelor personale prin proiectare (privacy by design): sistemele ITC care prelucrează date cu caracter personal trebuie proiectate să asigure protecția datelor cu caracter personal în toate cele 3 situații:
    - **Protecția datelor stocate**, care presupune inclusiv posibilitatea stocării criptate-după caz, precum și accesul restricționat și jurnalizat, permis doar persoanelor sau proceselor automate autorizate, după caz;
    - **Protecția datelor în tranzit**, care presupune trimiterea lor securizată între sisteme ITC diferite sau între microservicii, după caz;
    - **Protecția datelor în timpul prelucrării**, care presupune: folosirea de metode de programare (programming patterns) care micșorează riscul accesului neautorizat la date atunci când sunt prelucrate în memorie; livrarea unui serviciu public în format electronic sau al executării unui act administrativ care presupune prelucrarea de date cu caracter personal, necesita cunoașterea identității persoanei doar la momentul inițierii prelucrării și la momentul încheierii ei (in etapele intermediare acestea sa fie anonimizate).
- Posibilitatea includerii de microservicii, cum ar fi, spre exemplu: module de precompletare (extragerea automata a informațiilor deja existente, odată identificați beneficiarul și serviciul care trebuie livrat), module de fluxuri de lucru (permit editarea fluxurilor de lucru și generarea automată a codului-sursă necesar pentru ca sistemul informatic existent să continue să livreze servicii, fără a fi necesară o rescriere majoră a lor), module de plăți electronice (serviciile care presupun achitarea unor taxe de către cetateni, vor folosi un modul specializat, astfel încât schimbarea modalităților de plată să implice doar schimbarea acestui modul, nu a întregului sistem informatic;), module de urmărire și raportare a executării serviciilor, modul de notificări (modul distinct pentru notificări primite/transmise pe parcursul executării serviciilor publice electronice.), modul de autentificare și, respectiv, modul de autorizare (autentificare unică, Single Sign-On) etc.
- Pentru a asigura uniformitate, fluxurile de lucru, managementul de caz și deciziile vor fi descrise folosind standardele internaționale deschise, respectiv BPMN (pentru fluxuri), CMMN (pentru managementul de caz) și DMN (pentru decizii).

- Produsele software create pentru uzul administrației publice vor fi descrise folosind limbajul standard de modelare UML.Pentru schimbul de date cu alte sisteme se solicită utilizarea de standarde deschise (ex. bazate pe XML/JSON).
- Sistemul va expune o interfață bazată pe servicii WEB prin care aplicațiile instituțiilor pot transmite și recepționa informație folosind un canal de comunicare *sistem la sistem*.
- Sistemul propus va permite importul/exportul informațiilor stocate în diverse formate (ex. bazate pe XML/JSON).
- Infrastructura hardware trebuie să conțină, atât pentru locația principală, cât și pentru cea secundară, cel puțin:
  - Sisteme de procesare și stocare
  - Sistem de securitate cibernetică
  - Sistem de asigurare continuă a energiei electrice și climatizare
  - Sisteme de securitate fizică (control acces, alarmare la efracție, supraveghere video)
  - Sisteme de detecție și semnalizare a incendiilor
  - Sisteme de stingere a incendiilor Infrastructura de rețea necesară în cadrul soluției centrale (între elementele ce compun sistemul propriu-zis)
  - Infrastructura și echipamente de rețea necesare conectării celor două locații (secundară și principală)
  - Comunicații VoIP colaborative

- Stabilirea cantităților necesare pentru componentele aferente sistemului de securitate integrat (atât pentru Centrul de date, cât și pentru Centrul de date secundar), cu respectarea prevederilor legale în vigoare și a normativelor interne, cade în sarcina candidaților calificați în etapa a II-a a procedurii de achiziție, înaintea derulării primei runde de dialog cu candidații.
- Analiza de risc pentru sistemul de securitate integrat (atât pentru Centrul de date, cât și pentru Centrul de date secundar), se face în conformitate cu OMAI nr. 67/2017, cu modificările și completările ulterioare.
- Sistemele și echipamentele livrate trebuie să fie noi, neutilizate și de ultimă generație.
- Furnizorul va trebui să prezinte specificațiile tehnice privind organizarea și dotarea camerei serverelor (datacenter) în care se vor instala echipamentele, atât pentru locația

principală, cât şi pentru cea secundară,astfel încât să fie asigurate condiţiile operaţionale optime pentru funcţionarea acestora.

Furnizorul va avea în vedere utilizarea standardelor internaţionale privind implementarea DataCenterelor, respectiv minimum Tier2 Level conform TIA 942 pentru spaţiile puse la dispoziţie de MAI .

Amenajările aferente celor 2 site-uri, conform specificaţiilor standardului TIA 942,vor fi în sarcina Furnizorului.

- Pentru locaţia secundară Furnizorul va efectua igienizarea şi astuparea ferestrelor existente în camera tehnică, în care se vor instala echipamentele livrate, prin utilizarea de materiale speciale, conform normativelor în vigoare, care vor asigura cel puţin: protecţie la incendiu, izolare termică, barieră antivapori. Furnizorul va avea în vedere la dotarea datacenter-ului greutatea echipamentelor ce vor fi instalate în cele două amplasamente.
- Furnizorul va trebui să precizeze care este puterea totală consumată de echipamentele livrate, precum şi caracteristicile de climatizare/ventilaţie necesare, pentru a le avea în vedere la amenajarea datacenter-ului.
- Pentru locaţie secundară se va livra un grup electrogen care va fi instalat în paralel cu grupul electrogen existent, pentru asigurarea redundanţei componentei de alimentare necesară funcţionării infrastructurii IT instalată în camera tehnică, precum şi proiectarea şi instalarea circuitelor electrice necesare funcţionării echipamentelor în parametrii.
- Furnizorul va avea în vedere că toate cerinţele şi caracteristicile hardware sunt minime şi obligatorii.
- În acelaşi timp, cerinţele nu sunt limitative, furnizorii având libertatea de a le dezvolta şi extinde, conform soluţiei pe care o au în vedere. Este, aşadar, necesar ca furnizorii să propună soluţii complete şi integrate, care să îndeplinească în totalitate cerinţele beneficiarului.
- Furnizorii au obligativitatea de a include în propunerea tehnică şi comercială toate componentele hardware, software şi de servicii pe care le consideră necesare, chiar dacă acestea nu sunt individualizate sau solicitate în mod explicit.

Prezentul document descriptiv cuprinde regulile de bază care trebuie respectate astfel încât potenţialii furnizori/ofertanţi să elaboreze propunerea tehnică corespunzător cu necesităţile autorităţii contractante/beneficiarului. Cerinţele impuse prin Documentaţia descriptivă sunt considerate ca fiind minimale. Cerinţele tehnice care indică o anumită origine, sursă,

producţie, un produs special, o marcă de fabricaţie sau de comerţ, un brevet de invenţie, o licenţă de fabricaţie sunt menţionate doar pentru identificarea cu uşurinţă a tipului de produs şi nu au ca efect favorizarea sau eliminarea anumitor operatori economici sau anumitor produse. Aceste cerințe vor fi considerate ca având menţiunea "sau echivalent".

- Furnizorul va prelua si stoca la nivelul nucleului central al sistemului SIIEASC, datele și fișierele puse la dispoziție în acest scop de către Beneficiar (rezultate în urma procesului de digitizare), în integralitatea lor.

Operatorii din cadrul instituțiilor implicate vor accesa platforma prin intermediul unei interfețe web.

Pentru accesarea sistemului, toți operatorii vor naviga către pagina principală a sistemului și se vor autentifica în conformitate cu cerințele regulamentului 910/2014 al CE,înainte de a putea efectua orice operațiune în cadrul sistemului integrat.

Astfel, pentru înregistrarea informațiilor furnizate de către cetățeni în vederea înregistrării unei noi cereri, operatorii vor avea la dispoziție o interfață dedicată care va afișa, în formă standardizată (tabelară), un formular electronic ale cărui câmpuri vor trebui completate corespunzător. Completarea câmpurilor va fi validată în mod automat de către sistem în vederea eliminării posibilelor probleme (ex. greșeli tipografice sau de format – litere în câmpuri dedicate cifrelor etc).

SIIEASC se va integra cu sistemele informatice ale altor instituții – Ministerul Justiției, Ministerul Sănătății etc. – în vederea validării datelor introduse şi punerii la dispoziție a informațiilor către aceste instituții.

În urma completării unei cereri de către operator, sistemul va porni un flux pentru aprobarea şi validarea cererii înregistrate în sistem. Validarea se face prin autentificarea unui utilizator cu rol de aprobare, care poate semna digital cererea pentru a garanta autenticitatea acesteia.

Sistemul va fi operat şi gestionat de către următoarele categorii de utilizatori, având rolurile menționate mai jos:

- Administrator sistem. Utilizatori ce au acces la informațiile de tip administrativ ale sistemului. Au rolul de a gestiona utilizatorii sistemului, buna funcționare a fluxurilor, emiterea rapoartelor etc.

- Ofițeri stare civilă. Această categorie de utilizator aprobă diversele fluxuri inițiate de către operatorii aflați în cadrul instituțiilor partenere și emit documentele cu privire la starea civilă.

- Operatori date. Această categorie de utilizator este responsabilă de inițierea fluxurilor, pe baza drepturilor alocate acestora. Operatorii au acces numai la fluxurile care depind de aceștia (spitale, notariate publice etc.).

- Utilizatori finali. Această categorie de utilizator are dreptul doar să interogheze datele aflate în sistemși numai în scopurile pentru care li s-a conferit accesul la aceste informații. Interogarea datelor se face numai pe bază de autentificare, conform regulamentului 910/2014 al CE, iar fiecare interogare este auditatășsi trasatăîn integralitate de către sistemul de gestiune al documentelor de stare civilă propus.

Sistemul trebuie să includă un motor de creare și modelare fluxuri de lucru care să permită schimbul de date / informații și documente între utilizatorii sau sistemele implicate în procesele de emitere acte de stare civilă. Utilizatorii trebuie să fie notificați cu mesaje care expun toate informațiile necesare pentru a lua o decizie rapidă. De asemenea, toate acțiunile fiecărui utilizator în sistem și interacțiunile cu alte sisteme IT trebuie să poată fi auditate.

Sistemul va permite autentificarea utilizatorilor în condițiile specificate în regulamentul european EIDAS – nr. 910/2014.

Pentru a asigura disponibilitatea și accesul la sistem, întreaga soluție trebuie să fie construită în regim de înaltă disponibilitate (24 de ore pe zi, 7 zile pe săptămână):

- Servere de aplicații și baze de date în clustere activ - activ;
- Redundanță la nivelul echipamentelor de rețea (switch-uri, routere);
- Sistemul de operare trebuie să suporte *failover* și /sau *load balancing* pentru serviciile instalate care asigură accesul concurențial.

Sistemul trebuie să aibă un mecanism de căutare bazat pe criterii de căutare diferite, asigurând urmărirea informațiilor în cadrul aplicațiilor SIIEASC.

Sistemul trebuie să aibă funcții și capabilități de prelucrare a unui volum mare de date, de raportare și statistici Sistemul trebuie să aibă un mediu central de stocare a documentelor și o soluție de gestiune a conținutului digital, care să permită cel puțin:

- căutare în arhivă (metadate și conținut);

- suport pentru standarde deschise;
- scalabilitate ridicată.

Sistemul trebuie să aibă o soluţie de back-up şi restaurare pentru toate datele critice (date, aplicaţii, log-uri de sistem, etc) fiind capabil să fie restabilit în orice moment.

Interconectarea cu alte sisteme existente

Interconectarea SNIEP-SIIEASC

Pe partea de interconectare a SIIEASC cu SNIEP, se are în vedere migrarea din SNIEP parţială/totală a unor funcţionalităţi/date servicii Web, precum şi a unor funcţionalităţi de import/export date, adaptate la necesităţile SIIEASC şi SNIEP.

Interconectarea SIIEASC -sistem informatic Ministerul Justitiei

Interconectarea SIIEASC – sistem informatic MAE

Fluxuri de schimb de date între SIIEASC şi sistemul de gestiune a serviciilor consulare MAE:

- MAE -> SIIEASC: Cereri pentru procurarea de acte de stare civilă din România;
- MAE -> SIIEASC: Cereri de coduri numerice personale precalculate, în vederea înscrierii lor în certificatele de stare civilă;

Interconectarea SIIEASC – sistem SIUI al CNAS

- In vederea actualizării (dobândire/pierdere) statutului de asigurat din SIUI in raport cu evenimentele de viaţă (naştere/deces) tratate prin SIIEASC, este necesara interconectarea si schimbul de date intre cele doua sisteme, inclusiv din punct de vedere al fluxului de lucru de la nivelul DEPABD-CNUPPE de personalizare a CEAS.
- Este necesară implementarea unor mecanisme specifice care să permită alimentarea permanentă a Sistemul Informatic Unic Integrat al Asigurărilor Sociale de Sănătate din România cu informaţii actualizate care să reflecte cu acurateţe situaţia asiguratului în concordanţă cu evenimentele de stare civilă care individualizează fiecare persoană. Astfel, informaţiile relevante înscrise în cadrul SIIEASC, ce reprezintă sursa primară

de date referitoare la statutul civil al persoanei, respectiv cele referitoare la naştere, transcrierea actelor de stare civilă emise în străinătate, schimbarea numelui (pe cale administrativă ori ca urmare a modificărilor intervenite în statutul civil), precum şi cu privire la decesele intervenite, constituie un instrument deosebit de important atât în procesul de debirocratizare şi asigurare a serviciilor medicale de calitate asiguraţilor cât şi în domeniul fiscal prin reducerea eventualelor neconcordanţe sau vulnerabilităţi în materia acordării de servicii medicale persoanelor care nu au calitatea de asigurat.

Interconectarea SIIEASC – sistem informatic INS

- În conformitate cu prevederile articolului I pct. 11 din Regulamentul 2015/759 al Parlamentului European şi al Consiliului de modificare a Regulamentului (CE) nr. 223/2009 privind statisticile europene "Pentru a reduce sarcina pentru respondenţi, institutele naţionale de statistică [...] au dreptul de a accesa şi utiliza, imediat şi gratuit, toate registrele administrative şi de a integra respectivele registre administrative în statistici, în măsura în care acest lucru este necesar pentru elaborarea, producerea şi difuzarea de statistici europene". De asemenea, "institutele naţionale de statistică sunt consultate şi participă la proiectarea iniţială, dezvoltarea ulterioară şi întreruperea registrelor administrative realizate şi întreţinute de alte organisme, facilitând astfel utilizarea ulterioară a respectivelor registre în scopul producerii de statistici europene".
- În prezent oficiile de stare civilă realizează o serie de activităţi în domeniul comunicării periodice către structurile judeţene de statistică a informaţiilor relevante cu privire la evenimentele de stare civilă înregistrate pe raza acestora.
- În acest context, în vederea eficientizării sarcinilor ce revin oficiilor de stare civilă, proiectul SIIEASC permite implementarea unui instrument informatic dedicat elaborării şi furnizării în mod unitar, în sistem informatic, a situaţiilor statistice sau nominale, după caz, care fac obiectul evenimentelor de stare civilă necesare Institutului National de Statistică în scopul emiterii materialelor oficiale de informare în domeniul statistico-demografic, documente ce constituie elemente de referinţă în procesul de adoptare a politicilor şi strategiilor publice.

Interconectarea SIIEASC – Registrul electoral

- În aplicarea prevederilor Legii nr. 208/2015 privind alegerea Senatului şi a Camerei Deputaţilor, precum şi pentru organizarea şi funcţionarea Autorităţii Electorale

Permanente, cu modificările și completările ulterioare, evenimentele referitoare la decesul persoanelor, schimbarea numelui, punerea sub interdicție sau pierderea cetățeniei române implică necesitatea actualizării Registrului electoral, astfel că unele operațiuni de actualizare a sistemului informatic electoral sunt realizate punctual de către persoanele nominalizate de primarii unităților administrativ-teritoriale, aceste persoane fiind desemnate inclusiv din rândul personalului oficiilor de stare civilă sau al serviciilor publice comunitare de evidentă a persoanelor, aspect ce determină, în prezent, supraîncărcarea sarcinilor personalului cu atribuții în aceste domenii.

- Prin urmare, pentru derularea în condiții optime a acțiunilor de importanță națională din categoria proceselor electorale, intens mediatizate și cu impact în rândul populației și societății civile, se impune eficientizarea cadrului de cooperare inter-instituțională și armonizare a datelor referitoare la evidenta persoanelor cu drept de vot, prin valorificarea informațiilor relevante cuprinse în SIIEASC, fapt care va permite eliminarea unor posibile inadvertențe sau actualizarea cu întârziere a listelor electorale.

Interconectarea SIIEASC – sistem informatic UNNPR

- În vederea asigurării unui nivel înalt de calitate a serviciilor notariale oferite cetățenilor, este necesară valorificarea informațiilor ce fac obiectul SIIEASC, în scopul alimentării permanente a sistemului informatic aflat în administrarea UNNPR cu informații privind regimul matrimonial, decesele intervenite precum și desfacerea căsătoriei, în concordanță cu dispozițiile Legii nr. 119/1996 cu privire la actele de stare civilă, republicată, cu modificările și completările ulterioare, urmând ca în cadrul SIIEASC să fie înregistrate informațiile corespunzătoare divorțurilor încheiate la nivelul birourilor notariale precum și buletinele statistice de divorț aferente.

Alte detalii referitoare la sistemele cu care se va interconecta SIIEASC, fără a ne limita la cele enumerate anterior, vor fi furnizate ofertanților în etapa de dialog competitiv și ulterior detaliile în faza de analiză, după contractarea implementării sistemului.

2.3. Prevederi de securitate

Pentru asigurarea îndeplinirii cerinţelor de securitate legate de constrângerile privind prelucrarea datelor cu caracter personal, trebuie să se respecte următoarele reguli aferente sistemului informatic:

- **Confidenţialitate** - asigurarea protecţiei datelor împotriva acceselor neautorizate.
- **Integritate** - asigurarea protecţiei, exactităţii şi completitudinii datelor şi a soluţiilor furnizate pentru stocarea şi gestionarea acestora, dar şi asigurarea împotriva manipulării frauduloase a datelor/informaţiilor.
- **Disponibilitate** - sistemul trebuie să asigure un proces de redundanţă pentru a proteja utilizatorii de eventualele defecţiuni care pot surveni în timpul funcţionării, precum şi asigurarea datelor, componentelor funcţionale şi serviciilor asociate către utilizatorii autorizaţi la momentul solicitării. Sistemul va oferi o redundanţă atât în modul de implementare a sistemului în mediul de producţie, prin soluţii de clusterizare şi balansare, cât şi prin implementarea site-ului secundar.

Asigurarea controlului centralizat al tuturor aspectelor legate de securitate (autentificare, autorizare, auditare etc.), bazat pe separarea clară între control şi date/informaţii. În acest fel, este posibil să se obţină două avantaje majore:

- Descentralizarea serviciilor, simplificarea activităţilor administraţiei locale şi aducerea serviciilor mai aproape de cetăţeni, asigurarea autonomiei organizaţiilor implicate fără incidente de securitate şi garantează un control strict al administraţiei centrale (MAI) al tuturor serviciilor descentralizate;
- Centralizarea soluţiilor de securitate pentru a nu pierde controlul asupra aspectelor de securitate legate de gestionarea datelor critice cu caracter personal.Accesul la servicii poate fi dezactivat în timp real, atât pentru un anumit utilizator, cât şi pentru o anumită staţie de lucru.

Ca functionalităţi care trebuie îndeplinite, pentru respectarea cerinţelor de securitate, vor fi asigurate:

- Soluţiile de securitate implementate vor asigura funcţionarea SIIEASC în condiţii de siguranţă şi securitate, asigurând posibilitatea inventarierii şi evaluării riscurilor specifice, minimizării acestora sau contracararea, prin proceduri, măsuri şi soluţii şi instrumente informatice, precum şi prin măsuri şi proceduri administrative;

- Securitatea sistemului trebuie administrată la nivel central şi va dispune de mecanismele de administrare şi monitorizare a funcţionării infrastructurii;
- Soluţia de securitate trebuie să asigure acelaşi nivel de securitate şi pentru viitoarele aplicaţii dezvoltate, interne sau externe, cu care se va integra SIIEASC;
- Politicile de securitate vor asigura posibilitatea definirii, activării sau restricţionării drepturilor utilizatorilor finali, în ceea ce priveşte accesul la date, prelucrarea acestora, precum şi evidenţa actiunilor legate de emiterea şi prelucrarea documente şi datelor de stare civilă;
- Autentificarea şi controlul accesului utilizatorilor în sistem se va realiza în mod centralizat şi integrat pentru toate componentele funcţionale ale sistemului;
- Conceptul de securitate implementat pentru sistemul informatic va include,obligatoriu,diverse mecanisme şi proceduri, cum ar fi:
  - proceduri unitare de autentificare în sistem, cu asigurarea auditării operaţiilor de acces;
  - proceduri privind identificarea, raportarea şi remedierea incidentelor de securitate;
  - mecanisme de securizare a comunicaţiilor sistemului informatic;
  - politici centralizate de gestionare a utilizatorilor şi activităţilor desfăşurate de aceştia în sistem;
  - proceduri pentru securizarea, monitorizarea, administrarea tuturor componentelor funcţionale şi a componentelor de aplicaţie utilizate în cadrul SIIEASC.

În cadrul proiectului vor trebui să fie implementate măsuri de securitate care să faciliteze implementarea unor politici de securitate, conform cerinţelor noului Regulament General privind Protecţia Datelor (GDPR), cel puţin referitoare la:

- Securitate adecvată – protecţia împotriva prelucrării neautorizate sau ilegale, împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin măsuri tehnice sau organizatorice
- Pseudonimizare şi 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 informaţii suplimentare
- Capacitatea de a asigura confidenţialitatea, integritatea, disponibilitatea şi rezistenţa continue ale sistemelor şi 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 pe bază de cartele de acces; vor fi implementate diferite politici de securitate, acces în funcție de orar, 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
- 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.

Având în vedere numărul mare de tipuri de documente, accesul operatorilor la inițierea fluxurilor și la informații cu caracter personal, în ceea ce privește cetățenii care depun cererile, va fi limitat pe bază de roluri, gestionate de sistemul central de gestiune al utilizatorilor.

3. Descrierea tehnică a proiectului

3.1 Arhitectura sistemului informatic și de comunicații

3.1.1. Arhitectura funcțională

Din punct de vedere al soluției tehnice care va fi furnizată, aceasta va trebui să asigure un sistem unitar de acces la informațiile de stare civilă, atât instituțiilor publice care participă la emiterea actelor de stare civilă, cât și celor care validează/notifică producerea unui eveniment care are impact asupra activităților de emitere. Totodată, soluția va asigura și posibilitatea de

consultare a datelor şi informaţiilor de stare civilă instituţiilor publice centrale şi locale interesate dar şi cetăţenilor care doresc să consulte datele şi documentele necesare înregistrării actelor de stare civilă, cât şi obţinerea certificatelor de stare civilă în format electronic, semnate digital.

Totodată, este necesară realizarea unei soluţii complete de stocare, indexare şi gestiune a documentelor suport care să asigure atât înregistrarea noilor acte de stare civilă şi eliberarea certificatelor corespunzătoare cât şi preluarea/gestionarea fondului arhivistic digitizat pentru ultimii 100 de ani. Digitizarea fondului arhivistic pentru ultimii 100 de ani nu face obiectul implementarii nucleului central din proiect.

Pentru asigurarea tuturor fluxurilor şi proceselor de digitizare a fondului arhivistic, de întocmire a noilor acte de stare civilă şi eliberare a certificatelor corespunzătoare, cât şi de consultare a acestor date, vor fi necesare următoarele componente mari funcţionale şi de suport:

- Portal (cu servere web si reverse Proxy în DMZ)
  - O componentă de acces pentru autorităţile emitente a actelor de stare civilă
  - O componentă de acces pentru instituţiile publice locale şi centrale pentru consultarea datelor şi actelor de stare civilă
  - O componentă de acces pentru cetăţeni pentru consultarea datelor necesare eliberării certificatelor de stare civilă şi pentru obţinerea acestora în format electronic semnate digital.
- Platforma de aplicaţii
- Managementul fluxurilor şi proceselor de eliberare a documentelor de stare civilă
- Indexare documente electronice
- Stocare şi gestionare documente în format electronic
- Analiză şi raportare
- Sistem de Gestiune a Bazelor de Date
- Sistemul de securitate:
  - Securizare acces servicii electronice externe
  - Securitate utilizatori – managementul profilelor şi controlul accesului
  - LDAP
  - Monitorizare loguri şi trafic de reţea
- Integrare, consolidare şi replicare de date

- Backup date, sisteme şi aplicaţii
- Monitorizare date, sisteme şi aplicaţii
- Asistenţă tehnică şi instruire utilizatori

Arhitectura logica – componente functionale

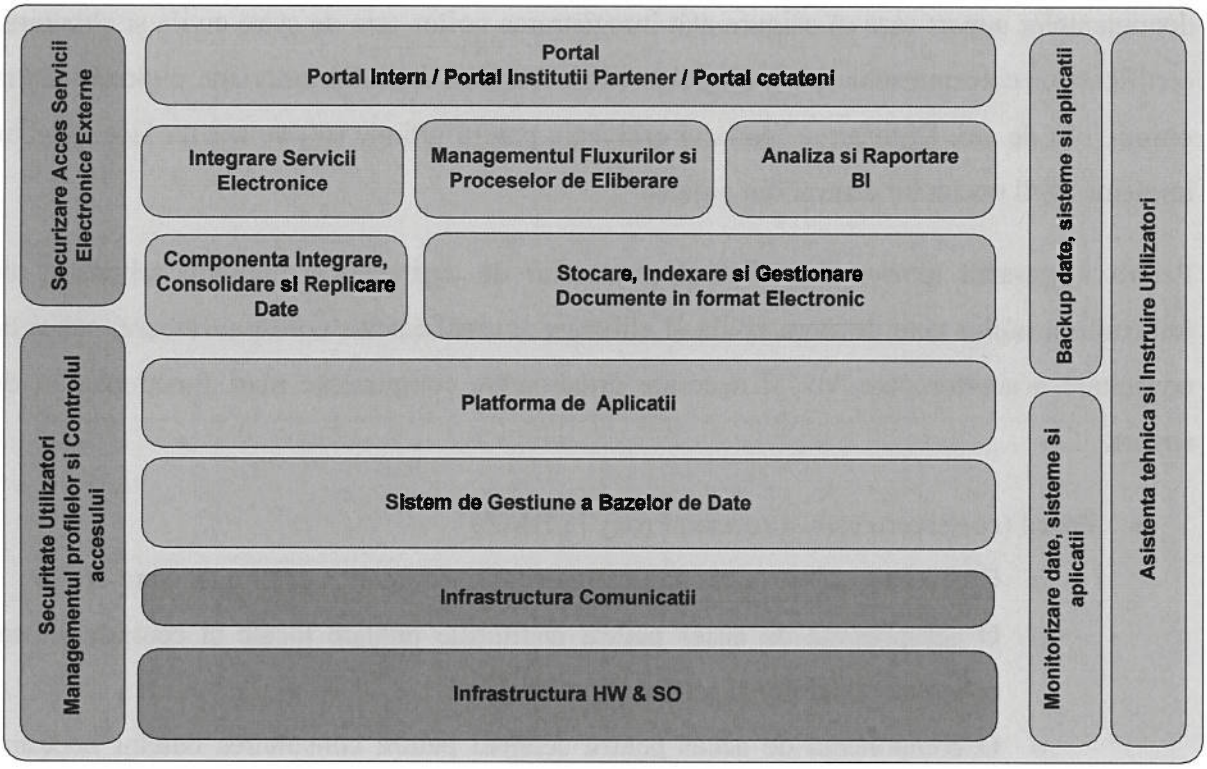

Fig. 1 Arhitectura funcţională SIIEASC

Nodul central al SIIEASC va fi instalat în două locaţii: site-ul principal din Data Center şi site-ul secundar.

Site-ul secundar va fi constituit din sisteme structural identice din punct de vedere funcţional cu cele din site-ul principal şi va fi dimensionat ţinând cont de cerinţele de disponibilitate a serviciilor. Este în responsabilitatea potenţialului furnizor crearea unei configuraţii valide pentru site-ul secundar în conformitate cu cerinţele funcţionale şi cerinţele tehnice ale componentelor software şi ale echipamentelor.

Ofertantul va propune în ofertă cantităţile necesare pentru echipamentele incluse în condiţiile asigurării echivalenţei arhitecturii între cele două locaţii

Sistemul din site-ul secundar va fi implementat folosind arhitectura de replicare a datelor din site-ul principal pentru toate componentele funcţionale, utilizând componenta 'Consolidare şi

replicare de date' și va fi implementat astfel încât, în cazul nefuncționării site-ului principal, sistemul să fie funcțional din această locație. Din acest motiv, licențele ofertate vor da posibilitatea ca sistemul din site-ul secundar să fie instalat și să funcționeze în mod activ.

Ofertantul va include în ofertă detalierea unei scheme de arhitectură amanuntita pentru mediul din site-ul secundar,cu precizarea exactă a echipamentelor și licențelor incluse în ofertă.

Ofertantul trebuie să descrie foarte clar abordarea propusă, din punct de vedere tehnic și metodologic, în vederea realizării acestei arhitecturi ce va avea în vedere transferul de date în timp util și fără pierderi.

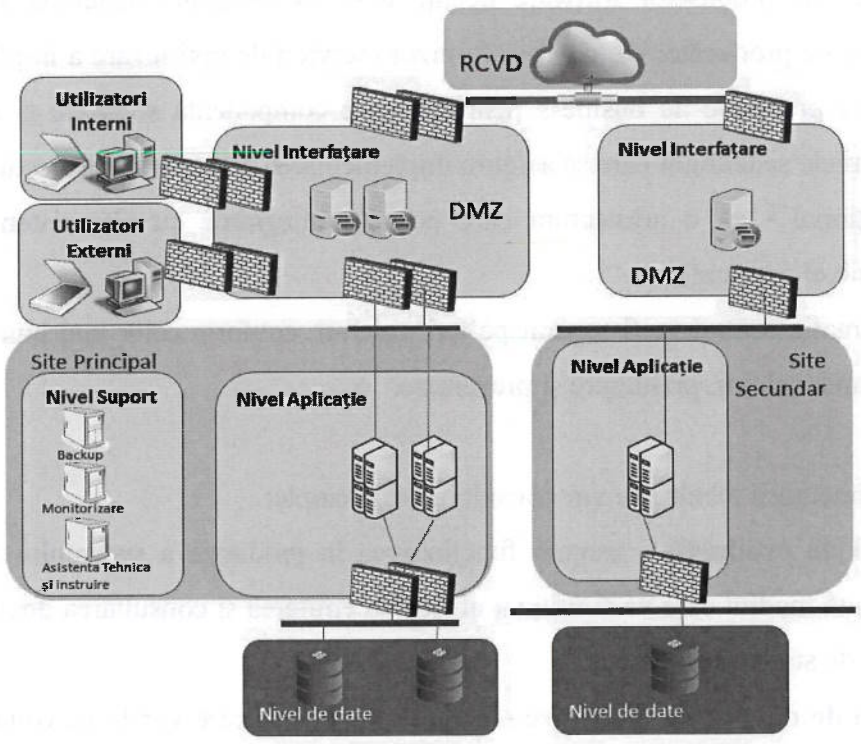

Fig. 2 Arhitectura funcțională site secundar

3.1.2. Arhitectura tehnică

Software standard

Platformele pe care vor rula aplicațiile (serverul de aplicație, bază de date, componente de integrare servicii electronice, managementul fluxurilor electronice de lucru și proceselor de eliberare etc.) vor trebui să fie integrate cu soluțiile de securitate pentru management al accesului și cu soluțiile de indexare, stocare și gestiune a documentelor electronice.
Platformele pe care vor rula aplicațiile (serverul de aplicație, bază de date, componente de integrare servicii electronice, managementul fluxurilor electronice de lucru și proceselor de eliberare etc.), soluțiile de securitate pentru management al accesului și soluțiile de indexare, stocare și gestiune a documentelor electronice trebuie să fie produse COTS, care au asigurate accesul la: versiuni noi ale produselor softtware licențiate, patch-uri de securitate, upgrade-uri cu îmbunătățiri ale produselor software licențiate și, totodată,care beneficiază de servicii expert furnizate de producător/distribuitor/furnizor (servicii de optimizare a implementării în conformitate cu procesele de business pentru fiecare componentă software și de integrare între componentele sistemului care să asigure implementarea cu succes a proiectului – proiect de interes național - cu o arhitectură care permite integrarea cu alte sistemeși servicii electronice la nivel național).
Sistemul informatic central va fi separat pe trei niveluri, conform celor mai bune practici în domeniu: stocarea datelor, prelucrare și prezentare.

În definirea arhitecturii tehnice se vor considera următoarele:

a) **Mediul de producție** - asigură funcționarea în producție a sistemului SIIEASC și reprezintă mediul care va fi utilizat efectiv la emiterea și consultarea documentelor și datelor de stare civilă
b) **Mediul de dezvoltare și testare** – asigură mediul pe care vor fi dezvoltate și testate toate componentele dezvoltate ale sistemului într-un mod integrat, înainte ca acestea să fie trecute în producție. Pentru dezvoltare și testare se va respecta arhitectura mediului de producție, inclusiv un nivel corespunzător/suficient de disponibilitate a componentelor funcționale în clustere
c) **Site secundar** – asigură funcționarea SIIEASC în cazul producerii unui dezastru în mediul de producție și reprezintă mediul care va asigura continuitatea funcționalităților din site-ul principal. Mediul din site-ul secundar va respecta

arhitectura mediului de producție la nivelul componentelor funcționale (excluzând nivelul suport) și va fi dimensionat ținând cont de cerințele de disponibilitate a serviciilor. Este în responsabilitatea potențialului furnizor crearea unei configurații valide pentru site-ul secundar în conformitate cu cerințele funcționale și cerințele tehnice ale componentelor software și ale echipamentelor.

Resursele de procesare alocate mediului de productie nu trebuie partajate cu alte medii, fiind rezervate rularii solutiei in regim normal.

Din punct de vedere al resurselor de stocare, acestea vor putea fi accesate simultan din toate mediile, dar vor fi alocate volume si spatii diferite pentru fiecare mediu in parte, asigurandu-se ca aceasta configurare nu impacteaza performanta, stabilitatea si securitatea mediului de productie.

În dezvoltarea sistemului va trebui să se țină cont de numărul mare de utilizatori și de volumul mare de date și acte de stare civilă care vor fi digitizate stocate și gestionate în vederea asigurării accesului irapid și facil la date, respectiv exploatarea eficientă a sistemului, având în vedere creșterea constantă a volumului de date și a documentelor ce vor fi digitizate după implementarea sistemului.

Dimensionarea mediilor

Soluția hardware furnizată va trebui să fie asigurată de soluții de tip server enterprise care să permită virtualizarea/partiționarea resurselor.

Pentru **dimensionarea mediului de producție** trebuie luate în considerare următoarele:

a) Pentru portalul la care vor avea acces cetățenii este estimat un număr de utilizatori concurenți = 1.000;
b) Pentru portalul intern numărul maxim de utilizatori este de 20.000 din care numărul estimat de utilizatori concurenți este de 4000;
c) Pentru portalul de acces pentru instituțiile publice locale și centrale pentru consultarea datelor și actelor de stare civilă numărul estimat de utilizatori concurenți este de 4000;
d) Volumul mare de documente digitizate pentru actele de stare civilă din ultimii 100 de ani, rezultatul va fi stocat și gestionat de componenta Indexare, Stocare și Gestionare Documente în format Electronic care va asigura si funcționalități de indexare si regăsire a documentelor si datelor de stare civila din arhiva.

e) Volumul mare al datelor de stare civilă şi a documentelor aferente, ce vor fi înregistrate în sistem, a log-urilor generate de accesul utilizatorilor şi care trebuie stocate cel puţin 2 ani, în conformitate cu prevederile legale actuale.

În acelaşi timp, pentru asigurarea disponibilităţii serviciilor de eliberare a actelor de stare civilă, sistemul trebuie săpermită o disponibilitate de tipul 365x7x24.

Pentru a atinge nivelul de disponibilitate toate componentele funcţionale principale vor trebuie sa fie asigurate in sisteme de tip cluster activ-activ.

Pentru **dimensionarea mediului din site-ul secundar** trebuie luate în considerare următoarele:

a) numărul maxim de utilizatori este 20.000;

b) numărul de utilizatori concurenţi este 200 (dintre care utilizatori de eliberare şi consultare din instituţiile publice – 100).

Dimensionarea componentelor funcţionale ale **mediului de dezvoltare şi testare** va trebui să asigure dezvoltarea componentelor pentru un număr de minimum 50 de utilizatori.

3.2. Funcţionalităţi ale sistemului

3.2.1. Funcţionalităţi front-office şi back-office

Sistemul trebuie să respecte cerinţele legislative privind procedurile de gestionare a datelor de stare civilă şi va trebui să asigure principalele procese descrise la cap.2.1.

3.2.2. Managementul utilizatorilor şi accesul la sistem

Pentru asigurarea managementului utilizatorilor (administratori de sistem, ofiţeri de stare civilă, operatori de date, utilizatori finali) şi accesului la sistemul SIIEASC, se vor avea în vedere următoarele:

- identificarea în mod unic a fiecărui utilizator în sistem prin crearea de conturi unice şi personalizate de acces;
- gestionarea centralizatăşi unitară a accesului utilizatorilor în sistem si autorizarea utilizatorului doar la componentele şi modulele funcţionale ale sistemului conform cu drepturile de acces stabilite in raport cu atribuţiile specifice;

- accesul la sistem se va putea realiza doar prin autentificarea utilizatorilor, excepție făcând accesul la acele informații de interes public publicate în portal.

Asigurarea accesului la sistem se va realiza diferențiat pe diferitele tipuri de utilizatori și conform atribuțiilor instituțiilor din care fac parte, astfel:

- controlul accesului la date şi servicii trebuie să ia în considerare cerinţele referitoare la politicileinstituţiilor cu atribuţii privind actualizarea informaţiilor despre persoană şi accesul la date cu caracter personal;
- în scopul realizării şi menţinerii unui nivel adecvat de acces la date şi servicii, se vor lua în considerare cel puţin următoarele:
  - 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 acţiune în sistem;
  - capabilitatea de a înregistra operaţiile/tranzacţiile realizate de fiecare utilizator autentificat în vederea realizării unui audit;
  - să furnizeze suport pentru utilizatori şi sesiuni de autentificare;
  - să aibă capabilităţi de management pentru identificare şi autentificare, să transmită aceste date într-o formă securizată;
  - capabilitatea de a seta durata sesiunii unui utilizator în cazul în care acesta nu mai utilizează aplicaţia, pentru a preîntâmpina accesul neautorizat la sistem altor persoane;
  - să ofere o soluţie de tip Single-Sign On pentru autentificarea unitară a utilizatorilor;
  - capabilitatea de a înregistra evenimente definite de securitate şi să transmită mesaje de alertă administratorilor de securitate;
  - în scopul protejării reţelei, este necesară încorporarea unor controale pentru a restrânge capacitatea de conectare a utilizatorilor. Astfel de controale pot fi realizate prin intermediul porţilor de reţea (gateway-urilor, VPN, etc.) care filtrează traficul pe baza unor reguli sau tabele prestabilite. Restricţile aplicate trebuie să ţină cont de cerinţele de acces la resursele respective.

3.2.3. Confidenţialitatea datelor

Pentru asigurarea confidenţialitatii datelor şi informaţiilor prelucrate, SIIEASC trebuie să asigure:

a) O infrastructură software şi hardware,precum şi realizarea unei arhitecturi care să implementeze instrumente prin care se asigură stabilitatea, integritatea şi disponibilitatea datelor;

b) Criptarea datelor, atât în trafic, prin securizarea comunicaţiilor, cât şi în modul de stocare al acestora (stocarea lor în mediul de producţie şi,în plus,în orice alt mediu în care datelor nu sunt anonimizate).

Confidenţialitatea datelor este prezentată în cadrul soluţiilor de securitate solicitate şi, în plus, va asigura:

- Utilizatorii de aplicaţie vor fi găzduiţi într-un sistem central.
- Autentificarea utilizatorilor în sistem se va face în mod unic, pe bază de conturi unice de utilizatori şi prin metode de autentificare pe bază de parole sau certificate digitale,în funcţie de nivelul de acces al utilizatorului.
- Autorizarea utilizatorilor se va face pe bază de rol şi/sau funcţie.
- Traficul utilizatorilor va trece prin mai multe sisteme de filtrare:
    - La nivel de reţea în Datacenter, traficul va trece prin firewall-uri, IDS, IPS şi sisteme de autentificare şi autorizare dedicate. În plus, reţeaua de date va fi împărţită în mai multe zone (ex: acces internet, DMZ, zona de management şi administrare, zona de aplicaţii, zona bazelor de date, zona de audit şi monitorizare etc.);
    - La nivel de aplicaţie, traficul va fi filtrat folosind metode de genul ReverseProxy şi sisteme tampon (dacă acestea sunt compromise se întrerupe legătura la serverele de date).
- Acţiunile efectuate (citire, scriere, modificare, ştergere etc.) la nivelul aplicaţiei, atât din punct de vedere al datelor utilizatorilor, cât şi a datelor de management (acţiuni efectuate de administratori) sunt logate în sistemul de audit. Accesul în sistemul de audit se va face strict pe baza nevoii de cunoaştere.

Pe lângă cerinţele enunţate mai sus, instrumentele proiectate pentru asigurarea confidenţialităţii datelor trebuiesă:

- ofere suport pentru criptarea traficului prin reţea între utilizator, aplicaţia de business şi baza de date, pentru a elimina posibilele încercări de interceptare a datelor când sunt transmise prin mediile de comunicaţie;
- asigure confidenţialitatea informaţiilor vehiculate, în conformitate cu modul de exploatare, pe verticală şi pe orizontală, a resurselor informaţionale ale sistemului;
- blocheze încercarea de utilizare neautorizată a resurselor, a serviciilor sau informaţiilor, să înregistreze evenimentul într-un fişier sau tabelă de supraveghere şi să semnaleze aceste evenimente personalului administrativ;
- nu permită persoanelor neautorizate modificarea sau alterarea semantică a informaţiilor;
- asigure calitatea şi consistenţa datelor, să facă identificarea sursei datelor iniţiale şi a persoanelor ce au introdus datele iniţiale, precum şi identificarea surselor şi persoanelor care modifică ulterior aceste date şi a elementelor/datelor modificate la nivelul fiecărei operaţii.

3.2.4. Integrarea componentelor

Datorită importanţei proiectului, un proiect de interes naţional, şi care se va integra cu alte proiecte existente la nivel naţional (ex SNIEP etc.), sistemul va fi dezvoltat şi implementat într-o arhitectură care va include componente importante precum managementul fluxurilorşi proceselor, platforma de schimbare de mesaje electronice între aplicaţii şi componente de acces securizat la servicii electronice.

Soluţiile de interconectare şi interoperabilitate implementate prin acest proiect vor asigura fundaţia şi vor oferi posibilitatea de a extinde proiectul pentru a asigura schimbul de date între acesta şi alte sisteme naţionale.

Soluţia propusă ar trebui să permită integrarea şi interoperabilitatea pentru a realiza schimbul de date unidirecţional sau bi-direcţional,între sistemul propus şi celelalte sisteme implicate, într-un format standardizat şi cu respectarea cerinţelor de securitate.

Interoperabilitate

Soluția va fi pregătită pentru asigurarea interoperabilității și recunoașterii evenimentelor de stare civilăîn schimbul de date inter-state UE. În acest sens, SIIEASC va dezvolta servicii web care săpermită schimb de date de stare civilăîntre statele membre, prin API-uri și tehnologii de marsh-alizare/demarsh-alizare și persistență, mapând modelul existent de date la ISA Core Person Vocabulary și generând formate de reprezentare XML/JSON.

Ghidul practic de mapare este descris de către ISA în manualul „ISA Handbook for using Core Vocabularies", disponibil la adresa :

http://ec.europa.eu/isa/ready-to-use-solutions/isa2/core-vocabularies_en.htm

Programele și soluțiile ISA de interoperabilitate se pot consulta aici:

http://ec.europa.eu/isa/

Pentru asigurarea compatibilității din punct de vedere al autentificării și semnăturii electronice, sistemul va ține seama de specificațiile EIDAS.

3.2.5. Parametrii tehnici

Pentru **dimensionarea mediului de producție al sistemului** trebuie luate în considerare următoarele:

a) Pentru portalul la care vor avea acces cetățenii, numărul estimat de utilizatori concurenți este de 1.000;
b) Pentru portalul intern,numărul maxim de operatori de date este de 20.000 din care numărul estimat de utilizatori concurenţi este de 4000

Pentru portalul de acces pentru instituțiile publice locale și centrale pentru consultarea datelor și actelor de stare civilă,numărul estimat de utilizatori concurenţi este de 4000;

Numărul de acte de stare civilă care vor face obiectul procesului de digitizare este de minim 50.000.000 din aproximativ 75.000.000 pentru procesare și rezultatul va fi stocat și gestionat de componenta Indexare, Stocare și Gestionare Documente în format Electronic care va asigura și funcționalități de indexare și regăsire a documentelor și datelor de stare civilă din arhivă.

Registrele de stare civilă vor fi scanate pagină cu pagină la rezolutie de 300dpi, astfel încât să fie obținute imagini digitale fidele ale acestora pe hârtie (copie fidelă a registrelor) și vor fi livrate în format jpeg, fără compresie. De asemenea, fiecare act în parte va avea si imaginea sa în format PDF (copie procesată).

Pentru **dimensionarea mediului din site-ul secundar** trebuie luate în considerare următoarele:

-numărul maxim de utilizatori este 20.000;

-numărul de utilizatori concurenți este 200 (dintre care utilizatori de eliberare și consultare din instituțiile publice – 100).

4. Prezentarea infrastructurii hardware

Cerințe generale privind platforma hardware

- Infrastructura hardware va fi instalată în cele două locații (site principal și site secundar) care vor găzdui toate componentele hardware necesare pentru rularea, în bune condiții, a aplicațiilor descrise mai sus;
- Toate echipamentele și UPS-urile oferite pentru nodul central si site-ul secundar trebuie să aibă suport pentru rack și toate accesoriile necesare incluse; furnizorul va asigura instalarea acestora in rack-uri;PDU-urile utilizate /instalate în rack-uri vor fi cu management;
- Fiecare Rack trebuie să fie complet utilat, inclusiv cu Consolă de management general de tip KVM montată în rack care va include monitor de min. 17 inch, rezoluție minimă 1280x1024, tastatură cu dispozitive integrate de tip touch-pad și/sau track-point si switch KVM pentru managementul serverelor. Gradul maxim de ocupare a rack-urilor să fie de 75%;
- Vor fi asigurate toate dotările auxiliare necesare functionalitatii complete a DataCenter-ului (site principal) și respectiv site-ul secundar.

Infrastructura hardware care va fi furnizată constă în:

- <u>Infrastructura mediului din site-ul principal</u>
  - sisteme comunicații;
  - sisteme de procesare;
  - sisteme de stocare;
  - surse neintreruptibile de alimentare cu energie electrică;
  - sistem de răcire și climatizare;
  - sistem de control acces, alarmare la efracție și supraveghere video;
  - sisteme de detecție și semnalizare a incendiilor;
  - sisteme de stingere a incendiilor;
  - grup electrogen;

- Infrastructura mediului din site-ul secundar

Va respecta arhitectura mediului de producție la nivelul componentelor funcționale (excluzând nivelul suport) și va fi dimensionat ținând cont de cerințele de disponibilitate a serviciilor.Este în responsabilitatea potențialului furnizor crearea unei configurații valide pentru site-ul secundar în conformitate cu cerințele funcționale și cerințele tehnice ale componentelor software și ale echipamentelor.

4.1. Prezentare sistem comunicații nucleu central

1. Componenta de comunicații și securitate

Componenta de comunicații și securitate trebuie să asigure o lățime de bandă în concordanță cu cerințele mediului de producție (minim 10 Gbps) pentru a asigura accesul rapid la date si schimbul de date între acesta și alte sisteme naționale care prelucrează date personale, precum și între site-ul primar și cel secundar, în contextul constrângerilor impuse de scopul site-ului secundar. Astfel că, traficul agregat de la utilizatorii finali către sistemul central va fi expus simultan către cele două noduri componente prin conexiuni de minim 10 Gbps într-o arhitectură redundantă și, în același timp, replicarea între cele două noduri ale sistemului central se va realiza printr-o conexiune dark-fiber care să ofere o bandă garantată de minim 10 Gbps.

Soluția trebuie să fie structurată pe un model arhitectural cu trei niveluri, denumite în continuare Interconectare, Agregare și Acces, care trebuie să asigure scalabilitate, performanță, flexibilitate și reziliență.

Nivelul Interconectare trebuie să îndeplinească următoarele cerințe:

1. Să ofere suport pentru comunicația nestingherită în cadrul nodului central SIIEASC, între site-ul principal și cel secundar, între sistemul informatic central SIIEASC și utilizatorii finali, dar și alte sisteme;
2. Să ofere suport pentru comunicația la nivel ISO-OSI 3, între diferite zone ale nivelurilor Acces și Agregare, precum și alte rețele prezente sau viitoare din cadrul Centrului de Date;
3. Să ofere posibilitatea extinderii în viitor a Centrului de Date către un alt centru de date și să permită funcționarea de tip activ-activ cu acesta prin tehnologii și protocoale existente.

Routere interconectare nod principal SIIEASC(site principal și secundar)

- Să poată asigura servicii de tip VPN (L2VPN, L3VPN, DMVPN)
- IPv4, IPv6, L3VPN
- multicast de Layer 2 și Layer 3, IPoDWDM;
- liste de access control Layer 2 și Layer 3 (ACL)

- hierarchical quality of service (HQoS), MPLS Traffic Engineering Fast Reroute (MPLS TE-FRR), Multichassis Link Aggregation (MC-LAG), Integrated Routing și Bridging (IRB)
- minim 4 porturi WAN 10 Gbps echipate cu SFP+
- minim 2 porturi OOB Ethernet pentru aplicații de cluster
- surse de alimentare redundante
- suport pentru adaptoare modulare cu capabilități de 20Gbps, respectiv 40 Gbps
- throughput 120Gbps
- Routing IPv4 și Multicast: OSPF, BGP, RIPv2, EIGRP Static routes, IS-IS, Multicast;
- Routing IPv6: RIPng, BGP, OSPFv3, EIGRP
- Securitate: Stateful Firewall, Attack detection, DOS protection, GRE Tunnels, AES encryption, autentificare MD5;
- Management port: port dedicat de management Ethernet;
- Suport pentru legături WAN multiple;
- Suport pentru rute statice;
- Suport pentru rutare pe bază de politici;
- Suport pentru prioritizare trafic și shaping până la nivel de aplicație.
- Capabilități IPSec;
- Surse redundante de alimentare;

Sistem de securitate pentru comunicații nod principal SIIEASC(site principal și secundar)

- criptare in hardware prin tunele IPSec peste infrastructura IPv4 si IPv6
- functii de NAT, object-based NAT si twice-nat;
- functii de context-aware firewall si identity-based firewall in concordanta cu sistemul de management al utilizatorilor;
- capacitate de configurare ca identity-firewall, daca exista o baza externa de utilizatori precum ActiveDirectory;
- Echipamentul va putea utiliza servicii de autentificare-autorizare-accounting (AAA) folosind minim urmatoarele protocoale: Kerberos, LDAP, RADIUS;
- Capacitate maxima de inspectie de tip stateful firewall de minimum 30Gbps.

- capacitate de criptare de minim 8Gbps si posibilitate de stabilire a minimum 5000 de conexiuni VPN simultan, indiferent daca conexiunea este de tip remote-access VPN sau site-to-site VPN
- capacitate de inspectie IPS, detectie si control la nivel de aplicatie cu o capacitate de procesare de minim 10Gbps (pachete 1024 bytes, trafic HTTP) cu toate cele 3 functii activate simultan;
- echipamentul va permite un numar de sesiuni concurente de minim 9,000,000, cu functionalitatile de detectie si control la nivel de aplicatii activate;
- Echipamentul va suporta protocol IKEv1 cat si IKEv2; De asemenea va putea utiliza suita de criptari de generatie noua, ce foloseste criptare cu AES-GCM, AES-GMAC cu chei de minim 256biti, algoritmi de hashing SHA-384, SHA-512;
- minim 12 interfete 10Gbps de tip SFP+ echipate cu module de tip 10G suportate de producatorul echipamentului.
- Modulele disponibile echipamentului propus trebuie sa detina si functia de fail-to-wire, ca in cazul unui defect critic al echipamentului, legatura fizica intre echipamentele adiacente sa nu fie intrerupta;
- Interfetele trebuie sa permita formarea de Etherchannels conform 802.3ad atat intre interfetele unui modul cat si intre interfetele modulelor aditionale, fara limitari;
- Sistemul trebuie sa dispuna de mecanisme de alocare a resurselor (numar maxim de conexiuni permise, numar maxim de adrese MAC, numar maxim de sesiuni IPSec, etc) catre firewall-uri virtuale;
- Capacitate de stocare interna dedicata si containerizata (separata fizic) pentru esantioane de fisiere captate in tranzit pentru functia de detectie si protectie antivirus si antimalware ;
- Va avea capabilitatea de filtrare a continutului web ce are ca destinatie internetul public, filtrarea facandu-se local sau printr-un serviciu specializat furnizat de producator; Functia de filtrare web e necesar sa tina cont de reputatia actualizata a site-urilor vizitate, nu doar filtrare prin blacklist. Actualizarea reputatiei va trebui realizata de algoritmul intern al echipamentului sau de actualizarea acesteia de catre producator intr-un mod regulat sau cand se detecteaza deteriorarea iminenta a reputatiei.

- Se vor suporta functionalitati de IPS. Trebuie să fie disponibile posibilitati de scriere de reguli IPS personalizate, intr-un format compatibil cu regulile de compunere pentru solutia open-source IPS Snort.
- Odată cu configurarea si activarea functiilor de IPS, sistemul va dispune de o functie de inspectie preliminara a unui flux de date, iar apoi, daca fluxul de date este conform cu politica de acces, daca sursa si destinatia sunt de incredere, daca protocolul este cel desemnat, daca nu exista evenimente de IPS detectate in fluxul de date si banda acestuia creste peste un anumit prag, fluxul sa fie redirectionat direct, fara inspectie IPS ulterioara. Aceasta functionalitate este necesara operational, pentru transferuri programate de date, cunoscute, cu volum mare, dar pentru care nu dorim sa avem o politica de excludere din inspectia IPS, dar nici sa avem impact major in performanta transferului sau asupra sistemului;
- Se vor suporta functii de detectie si protectie antivirus si antimalware pentru fisierele care-l tranziteazaEchipamentul se cere sa fie capabil sa mentina confidentialitatea fisierelor inspectate, sa nu necesite metode de exportare a fisierelor sau continutului acestora din echipament in timpul inspectiei
- Trebuie a fi insotit de aplicatie de management accesibila prin http/https, fara limitari de sistem de operare ce o pot accesa. Aplicatia capteaza, coreleaza si afiseaza in rapoarte evenimentele detectate de echipament si trebuie sa permita configurarea unitara a politicilor de securitate pe toate echipamentele din cadrul solutiei.
- Se va suporta optiunea de a trimite fisiere suspicioase, captate, catre analiza sandbox, iar raportul acestora, scorul asociat si indicatorii de risc sa se trimita catre aplicatia de management automat; Trimiterea fisierelor pentru analiza in sandbox, trebuie sa fie la latitudinea operatorului, nu automat. De asemenea operatorul trebuie sa poata configura ce tipuri de fisiere sunt foarte riscante (exe, dll, scr).
- Se va avea capacitatea de catalogare a traficului si asocierea acestuia la o lista de aplicatii cunoscute si actualizate de producator. Catalogarea traficului trebuie sa fie raportata in sistemul de management;
- Se va instala un echipament similar pentru redundanta si functionare in mod active/standby; De asemenea echipamentele se vor configura in mod cluster activ-activ, in care o stiva de minim 2 echipamente sa poata balansa incarcarea cu trafic;

- Va contine memorie interna, pentru stocarea in timp real a evenimentelor IPS si/sau procesarea catalogarii traficului catre tipurile de aplicatii, separata fizic de capacitatea de stocare a esantioanelor fisierelor captate;
- Se vor suporta minim urmatoarele protocoale de rutare: BGP, IS-IS, OSPFv2, OSPFv3, PIM-SM bidir;
- Se va permite configurarea de VLAN-uri.
- Se va dispune de port serial pentru administrarea locala si de asemenea de un port RJ45 dedicat exclusiv pentru management OOB, la care se adauga posibilitatea de administrare de la distanta prin telnet sau ssh v2.
- Se va dispune de accesorii ce vor permite instalarea in rack de telecomunicatii cu latimea de 19";
- Sistem de operare dedicat, securizat. Nu se accepta solutii care se instaleaza pe sisteme de operare de uz general;
- Este necesar a avea din design, mecanisme de protectie impotriva alterarii, inlocuirii sau interventiilor neautorizate asupra software-ului ce ruleaza pe sasiu. Aceste mecanisme trebuie sa includa minim: semnarea criptografica imaginilor software de la producator, lansarea in executie controlata (secure boot) prin verificarea ca imaginea semnata criptografic este lansata pe plaforma hardware destinata acesteia si minim un chip TPM (trusted platform module) instalat in fabrica, prin care platforma hardware este identificata unic si autentic.

Nivelul Agregare trebuie să îndeplinească următoarele cerințe:

- Să conecteze toate componentele nivelului Acces;
- Să asigure o comunicație redundantă și scalabilă între componentele nivelului Acces;
- Să permită extinderea în viitor a nivelului Acces cu cel puțin 100%.

Infrastructură de comunicații datacenter nivel agregare (site principal și secundar)

- Soluția propusă și dimensionarea acesteia trebuie să permită integrarea și interoperabilitatea pentru a realiza schimbul de date unidirecțional sau bi-

direcțional, între nivelul de agregare și nivelurile superioare și inferioare, cu respectarea cerințelor de securitate și standardizare.

- Dimensionarea trebuie să se facă astfel încât să nu creeze latențe, limitări virtuale de bandă sau zone de constrângere a traficului vehiculat de către întreg sistemul.
- Având în vedere caracterul critic al sistemului, este necesară implementarea unei arhitecturi balansate, precum și asigurarea redundanței tuturor conexiunilor între echipamente

Nivelul Acces trebuie să îndeplinească următoarele cerințe:

- trebuie să asigure o arhitectură unitară și uniformă pentru accesul echipamentelor de tip Server la nivelurile superioare si inferioare, asigurând o bandă de minim 10 Gbps/port, iar numărul și tipul de interfețe de rețea trebuie să fie corelat cu infrastructura de servere proiectată, asigurându-se o rezervă de porturi de 40% din necesarul proiectat.

Infrastructură de comunicații datacenter nivel acces (site principal și secundar)

- Soluția propusă și dimensionarea acesteia trebuie să permită integrarea și interoperabilitatea pentru a realiza schimbul de date unidirecțional sau bi-direcțional, între nivelul de acces și nivelurile superioare și inferioare, cu respectarea cerințelor de securitate și standardizare.
- Dimensionarea trebuie să se facă astfel încât să nu creeze latențe, limitări virtuale de bandă sau zone de constrângere a traficului vehiculat de către întreg sistemul.
- Având în vedere caracterul critic al sistemului, este necesară implementarea unei arhitecturi balansate acolo unde este tehnic imperios, precum și asigurarea redundanței tuturor conexiunilor între echipamente

2. Componenta colaborativă

Prin intermediul componentei colaborative, se doreste implementarea unei soluții care să asigure servicii colaborative punct la punct și punct la multipunct de tip voce, grup de chat, share de conținut de documente și imagini, prezență, în echipă prin intermediul unui singur instrument folosind dispozitive mobile cu acces la internet. Această soluție de comunicații IP colaborativă va permite conectarea în siguranță, din internet a clienților software (instalați pe dispozitive mobile din dotarea Achizitorului) în vederea îmbunătățirii serviciilor de comunicații colaborative oferite personalului M.A.I., din cadrul D.E.P.A.B.D. și D.G.C.T.I,

cu atribuții în implementarea, operaționalizarea și exploatarea SIIEASC. Clienții soft instalați pe dispozitivele mobile vor putea efectua / primi apeluri prin intermediul echipamentelor livrate în cadrul soluției, echipamente ce vor fi instalate într-o zonă publică demilitarizată a M.A.I., comunicațiile astfel efectuate fiind criptate.

Soluția va conține o componentă hardware (echipament de comutație voce) și o componentă software (suită de aplicații software – C.O.T.S.) și va permite administrarea centralizată, se va conecta la nivel de interfață fizică ISDN, protocol QSIG (minim 40 canale), cu Rețeaua Națională de Voce a M.A.I. (R.N.V. – M.A.I.) , protocol ISDN Public (minim 40 canale) și va oferi minim următoarele:

A. Servicii în rețea la nivelul R.N.V. a M.A.I.:

- Account Code
- Authorization Code for Extension
- Basic Calls
- Callback
- Call Diversion
- Call Metering
- Calling/Connected Line Identity
- Customer Identity Storage (CID)
- Direct Indialling
- DNIS for ACD
- Extension Status Indication
- Facility Restriction Level/Travelling Class Mark (FRL/TCM)
- Follow-me
- Incoming Automatic Inter-PABX Calls
- IP networking
- Manual Extending
- Name Identity
- Outgoing Automatic Call
- Outgoing call via Operator
- QSIG Call Offer
- Release Principles
- Rerouting
- Transfer

Pentru asigurarea acestor servicii, soluția va fi integrată cu R.N.V. a M.A.I., prin integrare se înțelege armonizarea protocoalelor și modelelor de comunicație, precum și armonizarea funcționalității cu R.N.V. a M.A.I.

B. Funcționalități la nivel de clienți software

- primirea de apeluri / mesaje / notificări, chiar dacă aplicația nu este deschisă pe dispozitivul clientului;
- redirectionarea apelurilor în caz de ocupat, fără răspuns dar și pentru orice apel;
- vizualizarea apelurilor efectuate, primite, pierdute ;
- transfer, parcare și redirecționare a apelurilor;
- răspuns automat și punere în așteptare;
- vizualizarea statusului celorlalți utilizatori (absent / ocupat / etc.);

- mesagerie instant cu opțiunea de arhivare a transcrierilor sesiunii;
- crearea de grupuri de apel;
- crearea de grupuri de mesagerie;
- inițierea de sesiuni de apel de către orice utilizator al soluției, cu adăugarea de participanți, în timpul derulării apelului;
- vizualizarea și editarea documentelor de tip ***.doc***, ***.ppt etc.*** în timpul unei sesiuni de apel de către toți participanții la sesiune;
- vizualizarea documentelor de tip ***.pdf***, ***etc.*** în timpul unei sesiuni de apel de către toți participanții la sesiune;
- transfer de fișiere (***.doc, .pdf, .ppt***);
- transfer de fișiere media (*audio, video, foto*).

C. **Remote Authentication in Dial-In User Service** pentru protocolul AAA (Authentication, Authorization și Accounting), prin care să fie asigurată pentru echipamentele soluției și / sau clienții soft ai soluției, următoarele facilități:
   - Authentication — proces care permite identificare (unic definit) obiectului după datele sale;
   - Authorization — proces de definire a competențelor obiectului de identificare pentru a avea acces la anumite facilități sau servicii;
   - Accounting — proces care permite culegerea informației (datelor de acreditare) de utilizare a resurselor.

Componenta hardware (echipament de comutație voce) va conține redresor stabilizat cu funcționare în tampon/baterie, tablou de comutare și distribuție c.a./c.c. și baterie de acumulatori cu gel dimensionată pentru asigurarea a minim 4 ore de funcționare de la întreruperea tensiunii de rețea (220 Vc.a.).

Soluția va fi livrată, pentru cele două site – uri (principal și secundar), cu:

- trunchiuri analogice (minim 10 porturi);
- trunchiuri IP SIP pentru conectarea la R.N.V. a M.A.I. (minim 20 canale);
- trunchiuri IP SIP inclusiv cu toate prerechizitele recomandate de producator (software, hardware etc.), pentru conectarea la operatorii publici de telecom (minim 20 canale) prin Internet, coroborat cu cerințele de customizare precizate.

Din punct de vedere tehnic și funcțional, soluția va fi implementată atât în site-ul principal cât și în site-ul secundar. Pentru dimensionarea soluției, atât în site – ul principal, cât și în site – ul secundar, trebuie luate în considerare următoarele:

a) Numărul de utilizatori ai soluției - aproximativ 410;
b) Numărul de convorbiri simultane 150;
c) Din punct de vedere hardware, soluția trebuie să permită un număr de aproximativ 1.000 de utilizatori fără a fi nevoie de dezvoltări ulterioare;
d) Capacitate de stocare log – uri pentru o perioadă aprox. 6 luni.

Soluția trebuie dimensionată și configurată astfel încât serviciile oferite să poată fi furnizate și de site-ul secundar, în cazul nefuncționării site – ului principal.

4.2. Prezentare sisteme de procesare și stocare

Pentru sistemul central SIIEASC vor fi livrate următoarele tipuri de sisteme de procesare:

- Servere pentru componentele din zona DMZ și componentele de suport:
  - Servere Web și Reverse proxy
  - Indexare Documente Electronice
  - Backup date, sisteme și aplicații
  - Monitorizare date, sisteme și aplicații
  - Asistență tehnică și Instruire Utilizatori
  - Monitorizarea logurilor și a traficului de rețea

Configuraţie minimă per server din punct de vedere al performantei:

Dotat cu minim 4 procesoare în arhitectură de tip x86,64 biti, multicore

256 GB memorie DDR4 cu posibiltate de extindere, ECC memory,

4 interfete de retea tip 10Gigabit Ethernet BaseT;

2 interfete plăci FC 16 Gbps single port;

Minim 2 x 600 GB SAS , 10.000 rpm, 12 Gbps, hot plug

Controller RAID cu posibilitati de configurare RAID 0, 1, 5, 10

Surse de alimentare şi ventilatoare în configuraţie redundantă

Certificate de producător pentru compatibilitate cu sistemul de operare ofertat.

- Servere pentru componentele funcționale corespunzătoare componentelor de aplicații și securitate utilizatori:
  - Portal Intern, Portal Instituții Partenere și Portal Cetățeni
  - Platforma de aplicații
  - Managementul Fluxurilor şi Proceselor de Eliberare
  - Stocare și Gestionare Documente în Format Electronic
  - Analizăși Raportare
  - Consolidare şi replicare date
  - Securizare acces servicii electronice
  - Securitate Utilizatori (Managementul profilelor, Controlul Accesului si LDAP)

Configuraţie minimă per server din punct de vedere al performantei:

Dotat cu minim 4 procesoare în arhitectură de tip x86, 64 biti, multicore

256 GB memorie DDR4, cu posibilitate de extindere, ECC memory,

4 x porturi 10 gigabit Ethernet si Modul Dual Port QDR (40Gb/s)

2 x 400 GB SSD

Surse de alimentare şi ventilatoare în configuraţie redundantă

Certificate de producător pentru compatibilitate cu sistemul de operare ofertat.

- Servere pentru SGBD

Configuraţie minimă per server din punct de vedere al performantei:

Dotat cu minim 2 procesoare în arhitectură de tip x86, 64 biti, multicore

256 GB memorie DDR4 cu posibiltate de extindere, ECC memory

4 x 1Gb Ethernet

2 x 10 Gb SFP+ Ethernet

5 x adaptoare dual port Fiber Channel (8Gbit/sec) si dual port QDR (40Gbit/sec)

4 x 600 GB SAS. 10.000 rpm

Surse de alimentare şi ventilatoare în configuraţie redundantă

Certificate de producător pentru compatibilitate cu sistemul de operare ofertat.

Toate sistemele de procesare vor fi insotite de sisteme de operare atat la nivelul de masina fizica cat si la nivelul de masina virtuala.

Din punctul de vedere al sistemelor de stocare, vor fi asigurate minim următoarele tipuri de echipamente de stocare pentru:

- zona de aplicaţii
- zona de date
- arhivarea documentelor şi actelor de stare civilă
- soluţie de stocare pe bandă

Configuraţie minimă de stocare pentru zona de aplicaţii:

Se solicită redundanţă totală la nivelul componentelor şi a căilor de date cu facilităţi de înlocuire a componentelor fără downtime şi fără oprirea accesului la date.

Surse şi ventilatoare în configuraţie redundantă şi baterie pentru protecţia memoriei cache.

2 controllere instalate şi active

Memorie cache per controller 8 GB

Discuri:

- Minim 160 TB raw SAS-2, 7200RPM

- Minim 4 TB SSD optimizat citire
- Minim 600 GB SSD optimizat scriere

Interfaţă reţea: ModulDual Port QDR 4x QDR (40Gb/s) sau minim 4 porturi 10GbE

Consola de management ce permite administrarea, monitorizarea, configurarea sistemului/componentelor.

Configuraţie minimă de stocare pentru zona de date:

Se solicită redundanţă totală la nivelul componentelor şi a căilor de date cu facilităţi de înlocuire a componentelor fără downtime şi fără oprirea accesului la date.

Surse şi ventilatoare în configuraţie redundantă

2 controllere instalate şi active scalabil la 8 controllere

Discuri:

- Minim 36 discuri x 8 TB, 7200 rpm; arhitectura discurilor sa fie SAS sau FC
- Discurile sa poata fi inlocuite fara a intrerupe activitatea solutiei de stocare sau a bazei de date

Interfaţă reţea:

- Minim 16 x 8 Gb/sec Fiber Channel sau minim 6 porturi x 40Gb/sec
- Latime de banda totala activa de cel putin 120Gb/sec
- Interfetele de retea sa fie redundante

Management:

- Sistem incorporat de monitorizare a tuturor functiilor critice
- Porturi Ethernet dedicate administrarii
- Verificarea automata a conectivitatii

Configuraţie minimă de stocare pentru zona de arhivare a documentelor şi a actelor de stare civilă:

Tip storage: Unified (SAN+NAS) dual-controller

Caracteristici generale

- Sistem de stocare centralizata cu arhitectura dual controller;
- Sistemul de stocare trebuie sa utilizeze o arhitectura care sa combine memorie RAM, discuri SAS3 si dispozitive Flash sau SSD pentru maximizarea performantei;
- Sistemul de stocare va putea fi echipat atat cu discuri de mare capacitate in tehnologie NL-SAS2 7200 rpm, discuri de mare performanta in tehnologie SAS2 10k RPM, cat si unitati de tip SSD;
- Operatiunile de scriere se vor putea executa pe medii de stocare cu timp de raspuns cat mai mic;

Fiabilitate

- Sistemul de stocare trebuie sa poata functiona in configuratie activ-activ cu doua controlere, pentru a evita aparitia unor zone critice de defectare. Sistemul tebuie sa permita replicarea parametrilor de configurare intre cele doua controlere, astfel incat in situatia in care unul dintre cele doua controlere este scos din productie (din cauza unor defectiuni sau operatiuni de mentenanta), celalalt sa poata prelua sarcinile si resursele asignate anterior controlerului inactiv;
- Administratorul sistemului de stocare va putea vizualiza si analiza in timp real sistemul de stocare si de transport al datelor, astfel incat problemele aparute sa poata fi diagnosticate si rezolvate in cel mai scurt timp;
- Eventualele operatiuni de upgrade al sistemului de operare a controlerelor nu trebuie sa impacteze disponibilitatea sistemului de stocare;
- Sistemul de stocare trebuie sa suporte modificarea in timp real, fara intreruperi, a parametrilor de functionare;
- Sistemul de stocare trebuie sa ofere metode de izolare a defectelor diverselor componente.

Capacitate de stocare, scalabilitate si flexibilitate

- Sistemul de stocare oferit trebuie sa dispuna de o capacitate instalata de 160TB brut (*raw*), obtinuta cu discuri avand capacitate unitara de maxim 8TB – 7200 rpm, astfel incat distributia datelor pe volumul de stocare sa fie optima din punct de vedere al operatiilor de citire;
- Sistemul de stocare oferit trebuie sa dispuna de o capacitate instalata de minim 12TB brut (*raw*), format din SSD-uri si/sau dispozitive Flash, care va avea rol de a accelera scrierile si citirile;
- Sistemul trebuie sa permita cresteri ulterioare ale capacitatii de stocare, aceasta putand fi extinsa pana la minim 250TB;
- Sistemul de stocare trebuie sa suporte minim urmatoarele tipuri de discuri: SAS2, SAS3, Flash sau SSD;
- Fiecare controler al sistemului de stocare trebuie sa fie echipat standard cu minim 2 porturi Ethernet 10Gb si 2 porturi FC 16Gbps;
- Sistemul de stocare trebuie sa fie compatibil cu rack-uri de 19 inch, sa contina accesoriile necesare instalarii si sa poata fi montat in rack-ul component al solutiei oferite;

Monitorizare, administrare, avertizare

- Sistemul de stocare trebuie sa ofere facilitati de monitorizare si analiza in timp real a functionarii;
- Sistemul de stocare trebuie sa ofere metode de diagnosticare si monitorizare de la distanta prin protocoale de tip HTTPS sau SMTP;
- Discurile sistemului de stocare trebuie sa fie usor de accesat si sa poata fi inlocuite fara a intrerupe functionarea sistemului (hot-swap/hot-plug);

Protectia datelor

- Sistemul de stocare trebuie sa asigure integritatea datelor;
- Sistemul de stocare trebuie sa suporte minim urmatoarele mecanisme de protectie a datelor: RAID0, RAID1, RAID simpla paritate echivalent RAID5, RAID dubla paritate echivalent RAID6;
- Sistemul de stocare trebuie sa suporte existenta simultana a mai multor niveluri de RAID;
- Sistemul de stocare trebuie sa suporte discuri de diferite viteze simultan, pentru a optimiza performantele si capacitatea de stocare;
- Sistemul de stocare trebuie sa asigure mecanisme de verificare continua in background a starii discurilor instalate;
- Sistemul de stocare trebuie sa includa facilitati de backup si restaurare a datelor;
- Sistemul de stocare trebuie sa poata fi administrat de la distanta;
- Sistemul de stocare trebuie sa permita realizarea unui numar mare de copii de siguranta a datelor, fiind inclusa facilitatea de protectie la scriere a unor asemenea copii si in mod integrat cu baze de date uzuale si aplicatii;
- Replicarea datelor trebuie sa se poata face manual la cerere sau programata la intervale fixe;

Datorită cerințelor de performanță și disponibilitate necesare implementării proiectului și ținând cont de timpii de răspuns necesari furnizării rapide a datelor din bazele de date, se dorește separarea celor 3 zone de stocare: aplicații, baze de date și arhivare. Fiecare zonă are cerințe de performanță specifice tipurilor de operații de citire/scriere aferente acestor zone, cerințele fiind diferite pe nodurile de stocare a bazei de date care necesită operații de IO foarte rapide față de cele de aplicații sau cele aferente arhivei electronice în care accesul se face doar pe bază de legătură directă către documentul digitizat.

Nota: Se accepta si o solutie de stocare unica ce va permite segmentarea celor trei zone atata timp cat se asigura cumulul cerintelor specificate pentru fiecare tip de echipament de stocare solicitat si un management complet independent pentru fiecare zona.
Solutia trebuie sa ofere:

- Deduplicare;
- Realizarea de snapshot-uri;
- Posibilitatea replicării volumelor indiferent de serviciu oferit (sincron sau asincron).

Cerinte tehnice echipamente de conectare sisteme de stocare centralizată (SAN)

Se dorește furnizarea unor echipamente de tip **switch SAN**, având următoarele caracteristici tehnice minimale:

- vor fi echipate cu porturi minim 24 porturi FC 16 Gbps per switch
- porturile switch-urilor SAN vor fi echipate cu conectori tip SFP.
- echipamentele vor fi furnizate cu kit pentru montarea în rack standard 19".
- switch-urile SAN vor fi furnizate cu cabluri FC de lungimi corespunzătoare în vederea conectării tuturor echipamentelor componente ale soluției furnizate, care necesită conectivitate la SAN.

Solutia de stocare pe banda

- Furnizorul va oferta o solutie de backup şi arhivare pentru care va oferi si numarul de benzi necesare pentru un an pentru o capacitate de minim 100TB brut (fiecare set va permite un backup zilnic al datelor-fise scanate şi metadate)

4.3 Infrastructura mediului din site-ul secundar

Infrastructura mediului din site-ul secundar trebuie să fie asigurată astfel încât să permită asigurarea disponibilității serviciilor în situația în care mediul de producție nu este disponibil. Aceasta va trebui să asigure toate componentele funcționale ale sistemului, cu necesarul de resurse de procesare solicitate în capitolul „Arhitectura tehnică". Va trebui asigurat un spațiu de stocare pe disk necesar pentru a se putea aplica toate modificările efectuate pe mediul de producție, utilizând backup-ul săptămânal integral al aplicațiilor, cât și spațiul necesar operațiilor de replicare a datelor, utilizând componenta de replicare a bazei de date. Se acceptă virtualizare/partiționare a resurselor de procesare utilizate în acest site.

Astfel, în mediul secundar se vor utiliza toate echipamentele de procesare, stocare, de comunicaţii şi securitate implementate în mediul de producţie necesare funcţionării şi conectivităţii mediului. Aceste echipamente vor asigura necesarul de infrastructură pentru asigurarea preluării - de către mediul din site-ul secundar - funcţionării aplicaţiilor necesare pentru toate fluxurile de emitere a documentelor de stare civilă şi de consultare a datelor copiate din baza de date de producţie şi a metadatelor corespunzătoare documentelor digitizate şi indexate.

4.4 Amenajare Centre de date

Având în vedere că activităţile propuse a se realiza în cadrul acestui contract pot face parte din categoria lucrărilor de investiţii este necesar să se ţină cont de parcurgerea etapelor, prevăzute de legislaţia în vigoare, după caz.

În urma dimensionării componentei hardware a sistemului informatic, operatorii economici vor evalua necesarul şi impactul lucrărilor ce vor fi efectuate, asupra clădirilor în care se află cele două spaţii care vor fi supuse amenajării pentru a găzdui echipamentele din cadrul sistemului informatic, în vederea îndeplinirii cerinţelor de la punctele 4.4.1. şi 4.4.2.

Ulterior acestei evaluări, operatorii econonomici vor prezenta pentru fiecare locaţie în parte şi pentru fiecare componentă care face obiectul amenajării, dacă sunt sau nu necesare următoarele documente/avize etc elaborate conform legislaţiei în vigoare:

- expertize tehnice;
- servicii de proiectare, execuţie şi recepţie a lucrărilor care necesită emiterea, în condiţiile legii, a autorizaţiei de construire;
- expertize tehnice locale;
- certificat de urbanism şi obţinerea avizelor menţionate în acesta;
- notă conceptuală;
- temei de proiectare;
- documentaţia de avizare a lucrărilor de intervenţii (DALI);
- proiect pentru autorizarea executării lucrărilor/proiectului tehnic de execuţie şi detaliilor de execuţie (PT + DDE), ulterior obţinerii avizului CTE al MAI;

- avizarea lucrărilor în Consiliul Tehnico - Economic al M.A.I. şi obţinerea avizului C.T.E.;
- obținerea autorizației de construire;
- alte documente necesare conform legislației incidente.

Obținerea tuturor avizelor şi elaborarea documentelor necesare va intra în sarcina operatorului economic declarat câştigător.

4.4.1 Centrul de date principal

Furnizorul va amenaja Centrul de date necesar proiectului într-un spaţiu de aproximativ 100 mp, pus la dipoziţie de MAI. Amenajarea se va face conform **standardului TIA 942 nivel minim Tier2.**

Implementarea Centrului de date se va face într-un spaţiu dedicat. Toate echipamentele externe ale sistemelor infrastructurii de suport fizic vor fi amplasate în imediata apropiere a clădirii care găzduieşte Centrul de date.

Echipamentele furnizate pentru dotarea Centrului de date vor fi conforme cu normele europene. Pentru echipamentele exterioare se va ţine seama de normele naţionale şi europene privind acustica urbană şi limitele admisibile ale nivelului de zgomot.

Activităţi desfăşurate de furnizor:

- Evaluarea arhitecturii generale a spaţiului Centrului de date şi a caracteristicilor generale de construcţie, inclusiv analiza potenţialelor neconformităţi cu cerinţele standardelor;
- Evaluarea specificaţiilor pentru sistemul electric, incluzând furnizarea energiei electrice, sistemele electrice de backup şi distribuţia electrică pentru subsistemele de suport ale Centrului de date;
- Evaluarea specificaţiilor pentru sistemul mecanic, incluzând sistemele de aer condiţionat;
- Evaluarea specificaţiilor pentru sistemul de monitorizarea a mediului;
- Evaluarea specificaţiilor pentru sistemele de securitate fizică;
- Evaluarea specificaţiilor pentru sistemul de cablare structurată.

Evaluarea specificaţiilor pentru sistemul de protecţie şi stingere a incendiilor.

Procesul de definire a cerinţelor va fi bazat pe analiza modului în care Centrul de date propus va putea să suporte necesităţile obiectivelor de business, începând din faza iniţială (punere în funcţiune) şi pe parcursul ciclului său de viaţă (capacitatea maximă proiectată), adresând discipline cum ar fi:

- Scalabilitate în adaptarea la cerinţele de business şi evoluţie a tehnologiilor TI;
- Flexibilitate pentru a suporta schimbările generate de adoptarea noilor tehnologii TI;
- Controlul costurilor pentru a se realiza optimizarea cheltuielilor pe durata ciclului de viaţă a Centrului de date, inclusiv costurile de pregătire, investiţia în realizare şi costurile de operare.

Planificarea lucrărilor care vor fi prestate în Centrul de date

În această fază, utilizând rezultatele etapei de evaluare, se va realiza planificarea Centrului de date, în concordanţă cu cerinţele specifice ale beneficiarului şi asigurându-se maximizarea eficienţei energetice pentru toate susbsistemele de infrastructură fizică şi TI.

Faza de planificare va utiliza datele din etapa precedentă pentru a pregăti elementele necesare proiectului final:

- Configuraţiile hardware şi de infrastructură, configuraţiile reţelei de date, inventarul pentru servere, echipamente de stocare, reţea şi alte echipamente TI;
- Infrastructura existentă a clădirii pentru asigurarea puterii şi capacităţii de răcire, împreună cu schemele arhitecturale şi ale instalaţiilor de suport fizic;

Evaluările clădirii realizate on-site vor oferi informaţii suplimentare de planificare, inclusiv necesarul de spaţiu pentru echipamentele de suport, stabilindu-se elementele arhitecturale, structurale, mecanice şi electrice ale noului Centru de date.

Proiectarea detaliată a activităţilor care vor fi prestate în Centrul de date

Rezultatele activităţilor din faza de planificare vor fi utilizate în documentarea proiectării detaliate, astfel încât să poată fi obţinute aprobările necesare, iar implementarea Centrului de date să poată fi realizată fără, sau cu modificări minime, ale proiectului de execuţie.

Pe parcursul fazei de proiectare, detaliile din etapa de planificare vor fi materializate în planuri detaliate de implementare pentru instalarea cablării electrice, a sistemului de conducte

pentru sistemul de răcire, de amplasare a echipamentelor, a detaliilor arhitecturale (pereţi, uşi), echipamentelor de monitorizare mediu, a sistemului de detecţie si semnalizare a incendiilor, sistemului de stingere a incendiilor,sistemului de control acces, sistemului de alarmare la efracţie şi sistemului de supraveghere video. Faza de proiectare a soluţiei va acoperi următoarele zone şi va trebui să fie materializată printr-un proiect de execuţie în concordanţă cu reglementările şi standardele în vigoare la data realizării, cu respectarea legislației naționale în vigoare.

- Arhitectura: Planurile de amplasare și detaliile pentru pereți, tavane, spații, compartimentări; elementele generale ale proiectului de construcție;
- Sisteme mecanice: detalii, scheme şi specificaţii pentru sistemul de climatizare, sistemul hidraulic şi planurile pentru realizare, amplasare echipamente, planificare;
- Sistemele electrice: scheme şi specificaţii pentru echipamentele electrice, amplasare, planificare, scheme monofilara şi detalii, incluzând sistemele de susţinere în cazul căderilor de tensiune etc.;
- Sisteme de control acces , alarmare la efracţie, supraveghere video, detecţie şi semnalizare a incendiilor şi stingere a incendiilor : detalii, scheme și specificații, planurile pentru realizare, inclusiv proiect tehnic;

Implementare, punere în funcțiune și testarea Centrului de date

Proiectul de implementare va include următoarele elemente:

- Asigurarea de către furnizor a amenajărilor de arhitectură şi construcţii, a pereţilor, uşilor şi a celorlalte lucrări de pregătire ale spaţiului, precum şi a pardoselii supraînălţate şi asigurarea serviciilor de instalare a echipamentelor infrastructurii de suport în Centrul de date.
- Instalarea sistemului de suport de cabluri, a cablurilor şi circuitelor electrice din sala de calculatoare pentru a suporta necesarul de putere al Centrului de date; se va asigura integrarea cu sistemele electrice existente ale beneficiarului.
- Instalarea echipamentelor externe ale sistemului de răcire, a sistemului de conducte al circuitului hidraulic şi a sistemului de control al mediului din Centrul de date.
- Instalarea rack-urilor pentru echipamente, a echipamentelor interioare ale sistemului de răcire, a sistemului UPS şi de distribuţie protejată a energiei electrice la rack-uri, a soluţiilor de monitorizare.

- Testarea infrastructurii de suport şi a soluţiilor de monitorizare.

Cerințe tehnice minimale pentru proiectarea și implementarea Centrului de date

Generalități

La implementarea proiectului Centrului de date, următoarele cerinţe sunt obligatorii:

Spaţiul dedicat Centrului de date va cuprinde:

- Data Room:
  - Suprafața de circa 100 mp;
  - 10 rackuri, aşezate pe rânduri; rândurile multiplu de 2;
  - O incintă pentru monitorizarea şi administrarea infrastructurii,
  - Rack-uri dotate cu:
    - Kit-uri antiseismice;
    - Sisteme de distribuţie a alimentării de tip PDU;
  - UPS-uri cu montare în rack;
  - Servere cu montare în rack;
  - Echipamente de comunicaţii cu montare în rack şi conectica cablării structurate a clădirii şi a Centrului de date;
  - Cablare structurată;
  - Sistemul UPS de rezervă
  - Echipamente interioare de climatizare;
  - Tablouri electrice de distribuţie;
  - Componente ale sistemului de detecţie şi semnalizare a incendiilor,
  - Componente ale sistemului de stingere a incendiilor,
  - Componente ale sistemelor decontrol acces, alarmare la efracţie şi de supraveghere video.

- Un spaţiu exterior, pentru echipamentele externe ale sistemului de răcire, situat în vecinătatea clădirii Centrului de date. Acesta cuprinde o platformă de beton, care va fi pregatită şi finalizată de furnizor şi va fi disponibilă la începerea serviciilor de instalare a echipamentelor exterioare, cu respectarea normelor de protecţie a mediului, de poluare fonică, etc.
- Fiecare rack va fi conectat la un dulap de distributie prin conexiuni UTP minim cat.7, respectiv conexiuni de fibra optica, astfel incat conectarea echipamentelor din rack-uri diferite sa se faca prin patch-cord-uri la nivelul dulapului de distributie. Pozarea

cablurilor de cupru si fibra optica se va realiza prin canale de cablu instalate pe trasee diferite.

Standarde și normative

În proiectare și implementare se vor respecta cerințele următoarelor standarde și normative, după caz, fara a se limita la:

- ANSI/TIA-942 Telecommunications Infrastructure Standard for Data Centres:
  - Scopul standardului este de a oferi cerințele și recomandările pentru proiectarea și implementarea de Centre de date.
  - Standardul se adresează proiectanților care au nevoie de o înțelegere cuprinzătoare a proiectării Centrelor de date, incluzând planificarea locației, proiectarea sistemului de cablare și a rețelei de date.
  - Standardul specifică proiectarea cablării, a rețelei, a locației, conține anexe de informare cu privire la bunele practici și recomandări pentru cerințele de disponibilitate, definirea spațiilor, a rack-urilor și cabinetelor.
- EN 50173-5 Data Centre Cabling:
  - Scopul standardului este de a oferi un sistem de cablare generic pentru centre de date, care să suporte o gamă largă de aplicații existente sau emergente pentru LAN, SAN și WAN, care să fie scalabil, astfel încât să suporte creșterea viitoare pe durata de viață planificată a centrului de date și să fie suficient de flexibil pentru a face modificări în mod ușor și eficient.
- ANSI/TIA-568-C.0, Generic Telecommunications Cabling for Customer Premises:
  - Standardul defineste planificarea si instalarea unui sistem de cablare structurata pentru toate tipurile de premise ale clientilor. El specifica un sistem care suporta o cablare de telecomunicatii generica intr-un mediu care imbina o diversitate de produse si de producatori.
  - Standardul specifica cerintele pentru un sistem de cablare de telecomunicatii generic, incluzand:
    - Structuri ale sistemului de cablare,
    - Topologii si distante,
    - Instalare, performanta si testare,

        - Transmisie prin fibra optica si cerinte de testare.

- ANSI/TIA-568-C.1, Commercial Building Telecommunications Standard:
    - Standardul defineste planificarea si instalarea unui sistem de cablare structurata intr-o cladire comerciala si intre cladirile comerciale din cadrul unui campus.
    - Standardul defineste structurile sistemului de cablare incluzand:
        - Facilitatile de intrare a furnizorilor de comunicatii,
        - Salile de echipamente,
        - Salile de telecomunicatii,
        - Cablare backbone,
        - Cablare orizontala,
        - Zona de lucru (spatiul care contine prizele de comunicatii).
- ANSI/TIA-568-C.2 Balanced Twisted-Pair Telecommunications Cabling and Components Standard:
    - Standardul include specificatiile pentru componente si cablare, precum si cerintele de testare pentru cablarea cu cupru (perechi torsadate), incluzand categoria 3, 5e, 6 si 6A.
- ANSI/TIA-568-C.3 Optical Fiber Cabling Components:
    - Scopul standardului este de a specifica cerintele de performanta pentru cablu si componente de fibra optica pentru cablarea cu fibra optica.
- ANSI/TIA/EIA-569-B Commercial Building Standard for Telecommunications Pathways and Spaces:
    - Scopul standardului este de a asigura operabilitatea, flexibilitatea, administrarea si longevitatea sistemului de cablare intr-un mediu complex de transmisii de telecomunicatii de voce si date (voce, date, video, securitate, semnale de control, etc.) descriind elementele de proiectare arhitecturala a sistemelor de suport pentru cabluri si spatiilor dedicate pentru echipamentele de telecomunicatii.
- ANSI/TIA/EIA-606-A Administration Standard for Commercial Telecommunications Infrastructure:

- Standardul se refera la administrarea infrastructurii de comunicatii pentru cladire, incluzand documentatia de baza si actualizarea periodica a planurilor, etichetelor si inregistarilor. Administrarea va fi in sinergie cu sistemele de voce date si video precum si cu celelalte sisteme de semnalizare din cladire, incluzand sistemele de securitate, audio, alarme si management al energiei.

- J-STD-607-A Commercial Building Grounding and Bonding Requirements for Telecommunications:
  - Standardul specifica o infrastructura uniforma de impamantare si legare la masa in cladirile comerciale.
- ISO/IEC 11801, Generic Cabling for Customer Premises:
  - Standardul specifica un sistem de cablare generic, independent de aplicatie, capabil sa suporte o gama larga de aplicatii. El ofera o schema flexibila de cablare, astfel incat modificarile sunt atat usor de realizat cat si economice. Standardul de cablare generica:
    - Specifica o structura de cablare care suporta o larga varietate de aplicatii,
    - Specifica clasele de canal E si F, bazate pe componente cu performante mai mari, capabile sa suporte aplicatii viitoare,
    - Specifica cerintele componentelor si specifica implementarile de cablare care asigura legaturi permanente si canale care satisfac sau depasesc cerintele pentru clasele de cablare.
- BS EN 62040 Specification for UPS Systems
- BS EN 62040-1-1 UPS Safety Requirements
- IEC 60529 Degrees of Protection provided by Enclosures
- EN 61000 Electro Magnetic Compatibility Standard
- EMC Directive 89/336/EEC

Cerinţe pentru proiectarea şi implementarea Centrului de date

Centrul de Date va fi proiectat şi implementat conform recomandarilor standardului ANSI/TIA-942, minimum clasificarea **TIER 2**.

Pentru sistemele electrice şi mecanice (sistemul de răcire) de suport se vor alege soluţii care să garanteze consum minim de energie şi eficienţă energetică în funcţionare, chiar în condiţii de încărcare a echipamentelor IT şi de comunicaţii de 30-40%. Se cere dimensionarea corectă a sistemelor infrastructurii de suport a Centrului de date, fiind unanim acceptat că supradimensionarea duce la creşterea masivă a pierderilor şi la ineficienţă energetică.

Soluţia propusă pentru Centrul de date trebuie să fie adaptabilă, flexibilă şi modulară şi să permită instalarea de rack-uri de servere cu mari densităţi de putere, fără oprirea sau modificarea configuraţiei iniţiale de rack-uri, prin creşterea capacităţii de putere şi de răcire şi prin soluţii de izolare a culoarului de aer cald sau rece. Soluţia trebuie să asigure integrarea în rack-uri a unor servere cu densităţi de putere de până la 15 KW/rack (pentru unele rack-uri). Soluţia trebuie să asigure parametrii optimi de mediu (capacitate de răcire şi flux de aer rece) pentru configuraţii de rack-uri cu diverse puteri TI (mici, medii şi mari).

Sistemele de securitate fizică vor fi proiectate şi dimensionate astfel încât să respecte specificaţiile din standardul ANSI/TIA-942 precum şi legislaţia română în domeniu.

Cerinţe tehnice pentru sistemele de suport ale Centrului de date

Arhitectură şi construcţii

Data Room

Spaţiul sălii de calculatoare va fi amenajat în următoarele condiţii:

- Pereţii interiori şi exteriori ai sălii de calculatoare finisaţi, finisarea lor asigurând:
  - protecţia antiincendiu (F90 minimum),
  - izolarea termică (cu vată minerală),
  - bariera antivapori
  - acoperiţi cu vopsea antistatică.
- Ferestrele exterioare vor fi blocate şi vor asigura izolaţia termică necesară pentru a minimiza schimbul de caldură cu exteriorul.
- Tavanul şi grinzile vor fi predate finisate, placate cu gips-carton şi vata minerală şi acoperite cu vopsea antistatică.
- Uşile prin care se delimitează perimetrul Centrului de date vor fi metalice, antifoc, cu acelasi grad de protectie ca şi al peretilor. Vor fi instalate usi antifoc, cu dimensiuni

deschidere minime 900 x 2130 mm, cu deschidere spre sensul de evacuare în caz de incendiu. În interior uşile vor fi dotate cu bara antipanică, pentru deschiderea lor. Toate uşile Centrului de date vor fi prevăzute cu dispozitive de deblocare conectate la sistemul de control de acces şi detecţie/stingere incendii.

- Planşeul în spaţiul Centrului de date va realizat din şapă autonivelantă şi va fi predat uscat şi curat (desprafuit) şi acoperit cu vopsea antistatică.

Pardosela tehnologică din Centrul de date

Pardoseala supraînălţată va fi realizată pe o structură de suport, metalică şi va suporta minimum 1200 kg/mp. Înainte de instalarea pardoselii supraînălţate, planşeul va fi acoperit cu vopsea antistatică. Această vopsea va fi compatibila cu răşina epoxidică utilizată pentru lipirea suporţilor verticali ai structurii pardoselii supraînalţate. Pardoseala supraînalţată va avea înălţimea maximă de 40 cm.

- Structura portantă de suport va fi formată din:
  - coloane verticale reglabile cu cap profilat pentru a fixa traversele orizontale cu şuruburi şi picior profilat pentru fixare în planşeu cu şuruburi, din oţel ambutisat, protejat anticoroziv,
  - traverse orizontale, realizate din oţel profilat, protejat anticoroziv care se fixează cu şuruburi de capul profilat al coloanei reglabile.
- Panourile pardoselii supraînălţate vor fi cu dimensiuni standard de 600x600 mm, realizate din conglomerat, ignifuge şi antistatice.
- Podeaua va fi prevăzută cu sistem echipotenţial.

Planul de amplasare a echipamentelor

Echipamentele IT şi de comunicaţii din sala de calculatoare vor fi amplasate în rack-uri standard de servere de 19" cu lăţimea de 60-75 cm şi adâncimea minimă de 100 cm şi în rack-uri de comunicaţii de 19" cu lăţimea minima de 75 cm şi adâncimea minimă de 100 cm. Toate rack-urile vor avea înălţimea de minim 42 U.

Rack-urile de servere şi comunicaţii vor fi aşezate în rânduri continue, respectându-se realizarea de culoare calde şi reci pentru circulaţia fluxurilor de aer şi minimizarea amestecului aerului cald cu cel rece.

Va exista un spaţiu pentru mentenanaţă, atât în faţa rack-urilor cât şi în spatele acestora, astfel încât intervenţia la echipamente să fie facilă, în condiţii de ergonomie, conform recomandărilor furnizorilor.

Rack-urile vor fi livrate în configuraţia pentru ocupare maximă cu echipemente IT şi vor fi prevăzute cu kituri de ranforsare seismică .

La momentul punerii în funcţiune, media ocupării rack-urilor cu echipamente IT va fi de maxim 75%.

La intrarea în sala de calculatoare, în dreptul uşii de acces se va lăsa un spaţiu liber minim de 120x120 cm, spaţiu necesar manipularii şi transportului rack-urilor şi echipamentelor în sau din sala de calculatoare.

Furnizorul va prezenta soluţia de amplasare care să prevadă, în condiţiile dimensiunilor sălii, distribuţia în cadrul Centrului de date a unui număr maxim de rack-uri de servere şi de comunicaţii.

Furnizorul va asigura o compartimentare, în cadrul Centrului de date, pentru o încăpere de unde se va face administrarea infrastructurii, cu o sprafaţă de 10 mp. Pentru această compartimentare, climatizarea se va face independent de cea a Centrului de date.

Sistemul de alimentare electrica si protectie la caderi de tensiune

Alimentarea cu energie electrica a Centrului de date va fi realizata de la tabloul general al cladirii. Pentru echipamentele vitale, in tabloul electric general al cladirii vor exista conexiuni protejate la caderi de tensiune prin generatorul Dieselprevazut in proiect. Pentru Data Room a Centrului de date vor fi instalate tablouri electrice pentru alimentarea cu energie electrica a echipamentelor, astfel:

- un circuit trifazic pentru conectarea sistemului UPS redundant, care va alimenta rack-urile de echipamente, echipamentele sistemelor de securitate, cu o putere minima de 250 KVA,
- un circuit trifazic care va alimenta echipamentele externe ale sistemului de climatizare, cu o putere suficienta alimentarea instalatiilor de răcire propuse.

Circuitele electrice de la tabloul general al cladiriivor fi aduse la locul de instalare al tablourilor electrice de catre Furnizor, care va realiza tabloul sau tablourile electrice de distributie şi care va asigura toate automatizările necesare, va asigura echiparea cu circuitele

de protectie necesare si va asigura conectarea echipamentelor furnizate, inclusiv conectarea duala a rack-urilor de echipamente.

Alimentare electrică de rezervă

Circuitele electrice pentru Centrul de date vor fi protejate împotriva anomaliilor de alimentare cu energie electrică de către generatorul prevăzut în proiect.

Dimensionarea Sistemului de alimentare electrică şi protecţie la căderi de tensiune

Sistemul de alimentare electrică şi protecţie la căderi de tensiune va fi dimensionat pentru o încarcăre de 200 KW, pentru sarcina IT şi comunicaţii. Va fi luată în considerare o marjă de eroare de 10-15%. La dimensionarea sistemului de alimentare electrică şi protecţie la căderi de tensiune se vor lua în considerare şi echipamentele infrastructurii de suport care vor asigura continuu condiţiile de mediu şi operare pentru Centrul de date, respectiv alimentare protejată pentru echipamentele infrastructurii de suport (sistemul de răcire) care trebuie sa funcţioneze continuu, chiar şi în intervalul de la căderea tensiunii de reţea şi pornirea şi preluarea sarcinii de către sistemul electric de rezervă (grupul generator Diesel standby).

Acest sistem de alimentare va asigura alimentarea cu energie electrică în parametrii funcţionali, într-un interval de temperatură exterioară de la -40°C la +50°C.

Sistemul UPS (uninterruptible power supply) cu distribuţie electrică modulară integrată

Rack-urile de echipamente din Centrul de date vor fi protejate la anomalii de alimentare cu energie electrică de un sistem UPS (Uninterruptible Power Supply). Sistemul UPS oferit trebuie să fie eficient din punct de vedere energetic într-o plaja largă de încărcare la ieşire şi să aibă integrat sistemul de distribuţie electrică pentru rack-urile de echipamente.

Sistemul UPS trebuie:

Sa utilizeze o arhitectura modulara si scalabila, atat pentru putere cat si pentru timpul de sustinere pe baterii, instalata in rack-uri cu dimensiunile fizice ale rack-urilor standard de servere, pentru a putea fi integrat in randurile de rack-uri de echipamente.

- Să utilizeze o arhitectură robustă, industrială, de tip online, cu dublă conversie, modulară şi scalabilă, cu MTBF ridicat, atât pentru putere cât şi pentru timpul de susţinere pe baterii.

- Să fie un sistem bazat pe tehnologia "transformer-free".
- Sa dispuna de accesorii optionale care sa faca posibila integrarea intr-o solutie de racire pentru densitati mari de putere impreuna cu rack-urile de echipamente protejate.
- Sa contina bypass static integrat. Acesta va asigura tranferul fara intrerupere a sarcinii de pe UPS pe intrarea de bypass daca este necesara mentenanta sistemului sau daca sistemul UPS nu poate sa sustina sarcina critica.
- Sistemul trebuie să poată ajusta automat puterea nominală furnizată în funcţie de temperatura mediului ambiant în care funcţionează: 110% la 25°C şi 100% la 40°C.
- Clasificare VFI conform IEC/EN 62040-3, EN-50091-3.
- Tehnologie 100% digitală.
- Sa contina bypass mecanic de mentenanta integrat. Acesta va permite izolarea totala a sistemului UPS in timpul activitatilor de testare sau mentenanta, asigurand siguranta personalului, timp in care sarcina este sustinuta de reteaua externa de alimentare bypass.
- Modulul de baterii trebuie sa fie astfel realizat incat sa permita inlocuirea de catre utilizator, fara a fi necesara oprirea sistemului. Fiecare modul de baterii trebuie sa permita monitorizarea tensiuni si temperaturii pentru a fi utilizate de sistemul de diagnosticare al bateriilor si de circuitul de incarcare cu compensare functie de temperatura.
- Sa contina un sistem de management al bateriilor care sa monitorizeze continuu starea fiecarui modul de baterii si care sa transmita notificari in situatia defectării sau deteriorării a capacităţii modulului.

Furnizorul va asigura si solutia de alimentare a rack-urilor de echipamente, de la sistemul de distributie modular al sistemului UPS si va furniza si barele de distributie (PDU - Power Distribution Unit) din rack-uri, capabile sa sustina minimum 3,5 KW. Sistemul va permite adaugarea de noi circuite de alimentare duale pentru rack-uri, sau inlocuirea cu circuite de puteri mari (11 KW sau 22 KW în funcție de capacitatea prognozată pentru fiecare rack) pentru a se asigura cresterea densitatii de putere in rack-urile in care se vor instala echipamente noi sau inlocui cele existente. Adaugarea sau inlocuirea de circuite electrice de distributie trebuie sa poate efectua fara oprirea sistemului UPS.

Sistemul de răcire pentru Centrul de date

Sistemul de răcire oferit pentru Centrul de date trebuie să fie eficient din punct de vedere energetic şi să aibă funcţionare eficientă într-o plaja largă de variaţie a încărcării termice ale echipamentelor instalate în rack-uri. Se doreşte atingerea unui factor PUE (Power Usage Effectiveness) sub 1,6. De aceea, toate componentele sistemului de răcire, inclusiv proiectarea sistemului de răcire vor trebui să contribuie la atingerea acestui scop, prin integrarea în soluţie de module de tip „free cooling" pentru agentul de răcire. Echipamentele de răcire din sală trebuie să aibă consum energetic minim şi să fie adaptabile, funcţie de încărcarea termică dinamică a echipamentelor IT şi comunicaţii, prin controlul puterii ventilatoarelor pentru asigurarea debitului de aer rece, minimizarea lungimii căilor fluxurilor de aer şi minimizarea sau eliminarea amestecului fluxurilor de aer rece şi cald.

Soluţia de climatizare trebuie să asigure răcirea echipamentelor cu mari densităţi de putere din sala Centrului de date, inclusiv pentru rack-uri cu densităţi de putere de 10-20 KW/rack.

Toate echipamentele oferite vor fi din gama profesională, dedicate soluţiilor de răcire pentru Centre de date şi vor permite integrarea într-un sistem de administrare şi monitorizare, care va permite monitorizarea eficienţei energetice a infrastructurii Centrului de date.

Dimensionarea sistemului de răcire a Centrului de date

Va fi luată în considerare o marjă de eroare de 10-15%. La dimensionarea sistemului de răcire vor fi luate în considerare şi echipamentele infrastructurii de suport care generează încărcare termică în Centrul de date. Infrastructura de suport trebuie să funcţioneze continuu, chiar şi în intervalul de timp de la căderea tensiunii de reţea şi pana la pornirea şi preluarea sarcinii de către sistemul electric de rezervă (grupul generator Diesel standby).

Echipamente de racire cu montaj la exterior (chillere)

Echipamentele de racire trebuie să poată fi integrate într-un sistem de răcire modular şi scalabil, pentru a asigura capacitatea de răcire pentru încărcarea termică iniţială şi să permită în viitor un upgrade pentru susţinerea încărcării termice finale specificate mai sus. Pentru asigurarea funcţionării continue se doreşte asigurarea redundanţei N+1 (un echipament va fi în standby pentru a prelua funcţionalitatea în caz de defectare a altui echipament din sistem). Echipamentele vor fi din clasa de mare eficienţă energetică şi vor putea funcţiona, în intervalele cu temperaturi scăzute, în regim „free cooling".

Instalarea inițială va asigura redundanța necesarului de răcire, iar infrastructura va fi proiectată și realizată astfel încât să se poată ajunge la cel mult 3 echipamente, în configurație redundantă 2+1.

Echipamentul de producere apa racita (chiller) ofertat trebuie sa aiba specificatiile tehnice de mai jos, considerate minimale:

- Să fie din categoria echipamentelor profesionale, destinate centrelor de date, proiectate astfel încât să combine cele mai bune perfomanțe în condiții eficiente, cu un impact scăzut asupra mediului.
- Să conțină un modul de tip „free cooling", care să asigure un consum minim de energie electrică în perioadele cu temperatură scăzută, fără a se utiliza compresoarele.
- Toate funcțiile chiller-ului cu „free cooling" trebuie să fie administrate și monitorizate de un controller cu microprocesor. Controlul vitezei ventilatorului, pornirea compresoarelor și repartizarea capacității de răcire trebuie să fie astfel administrate încât să se economisească la maxim consumul de energie electrică.
- Echipamentul să poata funcționa cu apă sau cu un amestec apa - etilen glycol, în diferite proporții, astfel încât să se asigure funcționarea sigură și la capacitatea de răcire proiectata în limite de variație a temperaturii exterioare între -25^{O}C și +45^{O}C.
- Chiller-ul trebuie să asigure capacitatea de răcire pentru o funcționare la capacitatea maximă estimată a echipamentelor instalate în rack-uri, la o temperatură exterioară de maxim 45^{O}C și o funcționare în mod „free cooling", fără pornirea circuitelor frigorifice, până la o temperatură exterioară maximă de 17^{O}C.
- Chiller-ul să fie echipat cu două compresoare de tip „Hermetic Scroll", cu un coeficient de performanță ridicat, nivel de zgomot scăzut și protecție termică internă.
- Chiller-ul să fie echipat cu presostate duble pentru protecția compresoarelor la suprapresiune sau subpresiune.
- Sistemul să fie livrat cu un controller care să permită monitorizarea tuturor parametrilor de funcționare sau a alarmelor de funcționare. De asemenea, trebuie să permită interconectarea a două sau mai multor echipamente, asigurând funcționarea acestora în cascadă, în funcție de capacitatea de răcire necesară la un moment dat, cât și funcționarea acestora prin rotație cu echipamentul de rezervă, pentru a se realiza uzura uniformă a fiecărui echipament. Controllerul va asigura funcționarea/pornirea

secvenţială decalată, pentru a nu porni două echipamente în acelaşi timp (pentru a se evita curenţii de pornire mari în acelaşi timp) şi va asigura şi pornirea automată a lor (autorestart) după oprirea lor la fluctuaţii de tensiune sau la căderi de tensiune, în aceleaşi condiţii (cascadare, rotaţie, pornire secvenţială decalată) precum şi comanda echipamentelor hidraulice.

- Să aibă două circuite frigorifice independente, pentru a asigura atât o funcţionare eficientă din punct de vedere energetic la încărcare parţială, cât şi creşterea redundanţei şi fiabilităţii echipamentului.
- Chiller-ul trebuie să funcţioneze cu zgomot redus, fără a depăşi nivelul de zgomot de 47 dB(A) măsurat la 10 metri de echipament sau maximul prevăzut de normativele în vigoare în mediul urban..
- Să permită monitorizarea şi să transmită parametrii de stare, alarmele sau atenţionările cel puţin pentru:
  - stare: operare sau standby;
  - valori temperaturi apă tur şi retur;
  - mod funcţionare: mecanic sau „free cooling";
  - număr de compresoare în funcţionare;
  - stare şi alarme alimentare electrică;
  - stare şi alarme controller;
  - stare şi alarme compresoare;
  - stare şi alarme ventilatoare;
  - stare şi alarme circuite hidraulice.

Furnizorul va asigura proiectarea şi implementarea soluţiei complete pentru echipamentele chiller, cu toate accesoriile şi componentele necesare conectării lor în circuitul hidraulic şi în sistemul de administrare şi monitorizare a infrastructurii de suport a Centrului de date. Circuitul hidraulic va fi proiectat şi realizat pentru puterea maximă IT a Centrului de date, dar va permite adăugarea, dacă va fi necesar, a unor chiller-e adiţionale, pentru asigurarea redundanţei şi creşterea capacităţii de răcire. Circuitul hidraulic va fi izolat termic pe întreaga lungime a sa.

Pompele de recirculare pentru agentul frigorific din circuitul hidraulic vor fi alimentate de către sistemul UPS, pentru a se asigura funcţionarea neîntreruptă a sistemului de răcire.

Echipament de distribuţie agent de răcire în Data Room

Echipamentul de distribuţie a agentului de răcire asigură distribuţia centralizată şi sigură a apei răcite sau a amestecului apă-glycol către echipamentele de răcire din sala Centrului de date, asigurând modularitatea şi scalabilitatea soluţiei de răcire.

Echipamentul de distribuţie a agentului de răcire ofertat trebuie să aibă specificaţiile tehnice de mai jos, considerate minimale.

- Să poată fi amplasat în sala de calculatoare sau într-un spaţiu adiacent, cu valvele de izolare şi de reglaj uşor accesibile. În cazul în care va fi instalat în sala de calculatoare, adâncimea nu va fi mai mare de 75 cm şi lăţimea va fi de maximum 110 cm, din cauza constrângerii spaţiului disponibil.
- Să aibă posibilitatea de a conecta ţevile de tur şi retur ale circuitului frigorific de la chillere în partea superioară sau în cea inferioară, pe sub pardoseala supraînalţată.
- Să poată asigura distribuţia agentului de răcire spre echipamentele de răcire din sală prin ţevi flexibile, izolate termic, instalate sub pardoseala supraînalţată.
- Să aibă posibilitatea de conectare a până la 12 echipamente de răcire, fiecare circuit tur şi retur să poată fi izolat şi balansat individual, pentru a se asigura operarea optimă, mentenanţa echipamentelor de răcire sau adăugarea de noi echipamente de răcire fără a fi necesară oprirea sistemului de răcire.
- Să permită conectarea circuitelor hidraulice (tur şi retur) către echipamentele de răcire cu ţevi flexibile, în conformitate cu recomandările producătorului echipamentelor pentru răcire.
- Să poată funcţiona cu apă sau cu un amestec apă-glycol.

Echipamentul va fi livrat cu toate accesoriile necesare pentru conectarea la circuitul hidraulic al echipamentelor de producere a apei răcite precum şi cu toate componentele circuitelor hidraulice de distribuţie pentru echipamentele de răcire ofertate pentru soluția de răcire a Centrului de date pentru încărcarea proiectată inițială, inclusiv elementele de fixare şi izolare a acestor circuite.

Echipamentul va fi livrat cu toate echipamentele şi instlalaţiile necesare necesare pentru umidificare si evacuare condens in condițiile respectării standardului pentru proiectarea centrelor de date.

Echipamentele profesionale de răcire în rând pentru sala Centrului de date

Echipamentele de racire pentru rack-urile de servere si echipamente de stocare date vor fi instalate in randurile de rack-uri. Aceasta amplasare a echipamentelor de racire profesionale pentru centre de date a fost luata in considerare din urmatoarele motive:

- Spaţiul sălii de calculatoare nu permite instalarea de echipamente profesionale de răcire perimetrale, cu livrarea aerului rece prin grile în pardoseala supraînălţată, situate în faţa rack-urilor, fără a avea limitări asupra debitelor fluxurilor de aer şi asigurării condiţiilor de răcire pentru densităţi mari de putere în rack-uri;
- Echipamentele de răcire în rând minimizează lungimea fluxurilor de aer, prin furnizarea aerului rece în faţa şi recuperarea aerului cald din spatele rack-urilor de echipamente. În acest fel, puterea necesară pentru ventilatoare pentru circulaţia volumului de aer este diminuată şi creşte eficienţa energetică a sistemului de răcire;
- Amplasarea în rând permite mai uşor adoptarea de soluţii pentru izolarea fluxurilor de aer cald sau rece în interiorul sălii de calculatoare şi se maximizează eficienţa energetică globală a sistemului de răcire.

Echipamentele de răcire profesionale în rând ofertate trebuie să aiba specificaţiile tehnice de mai jos, considerate minimale:

- Alimentare electrica 200-240V, 50/60 Hz.
- Capacitate de răcire minimum 18 KW.
- Să permită conectarea echipamentului la sistemul UPS, pentru a se asigura ventilaţia şi răcirea continuă, chiar şi în fereastra de timp de la căderea tensiunii de la reţeaua urbană şi transferul alimentării electrice pe sistemul electric de rezervă pentru eliminarea pericolului creşterii excesive a temeperaturii datorită densităţii mari de putere TI şi comunicaţii din sala de calculatoare.
- Refularea aerului rece să se facă frontal, orizontal, pe toata înălţimea echipamentului.
- Colectarea aerului cald trebuie să se facă în partea din spate a echipamentului de răcire, pe toată înălţimea echipamentului.
- Ventilatoarele să fie cu viteză variabilă, cu posibilitatea modulării vitezei în intervalul 30-100%. Acestea vor fi dotate cu soft-start, pentru a minimiza curenţii de pornire, cu impact de suprasarcină asupra sistemului UPS de la care sunt alimentate. Echipamentele trebuie să poată funcţiona chiar în condiţiile defectării unui ventilator.

Un ventilator defect trebuie să poată fi înlocuit fără a fi necesară oprirea echipamentului de răcire.

- Fiecare echipament de răcire trebuie să poata furniza un debit minim de 75 m^3/min, iar la defectarea unui ventilator trebuie să nu se diminueze debitul de aer al echipamentului cu mai mult de 15%.
- Echipamentul de răcire va fi prevăzut cu o valvă controlată de microprocesor, care va asigura reglarea cantităţii de lichid de răcire care circulă prin serpentină pentru menţinerea condiţiilor optime de răcire.
- Echipamentul de răcire va funcţiona cu apă sau cu un amestec de apă şi glycol. Conectarea la echipamentul de distribuţie a ţevilor circuitului hidraulic se va face în mod obligatoriu în partea inferioară.
- Echipamentele de răcire vor fi livrate standard cu câte un senzor de temperatură care să poată fi instalat pe rack-urile adiacente pentru a oferi informaţiile privind temperatura la intrarea în rack, parametru care să fie utilizat pentru controlul funcţionării echipamentului de răcire.
- Echipamentele vor fi prevăzute cu o pompă şi un circuit de evacuare a condensului, capabilă să pompeze apa rezultată în afara spaţiului sălii de calculatoare. Funcţionarea incorectă a circuitului de evacuare a condensului va fi semnalată prin transmiterea unei alarme.
- Fiecare echipamente va avea instalat câte un detector de lichide, conectat la controller. Acesta va transmite alarme în cazul detecţiei scurgerii de agent de răcire pe pardoseală
- Echipamentele vor avea două surse de alimentare şi vor putea să fie alimentate pe două circuite electrice distincte, cu cordoane electrice cu conectori IEC 309, pentru a se putea asigura continuarea răcirii în cazul defectării unei surse de alimentare sau întreruperii unei căi de alimentare cu energie electrică.
- Echipamentele vor avea un panou frontal, gestionat de un controller cu microprocesor, cu ecran LCD şi taste. Panoul va permite monitorizarea şi configurarea echipamentului pe baza unui meniu ale cărui funcţii vor include rapoarte de stare şi vor permite setarea parametrilor operaţionali, navigarea prin meniuri, selectarea obiectelor şi introducerea informaţiilor alfanumerice. În plus, panoul frontal trebuie să aibă LED-uri care să indice starea de operare a echipamentului, existenţa

alarmelor sau atenţionărilor şi să atenţioneze utilizatorul dacă au aparut noi alarme critice. Orice alarmă critică trebuie să fie avertizată şi sonor. De asemenea, controllerul va oferi informaţii asupra timpului de utilizare pentru componentele majore ale echipamentului.

- Alarmele şi evenimentele trebuie să fie memorate şi insotite de data şi timpul producerii evenimentelor precum şi conditiile de operare ale echipamentului in momentul producerii evenimentului. Echipamentul va transmite cel putin urmatoarele alarme:
  - eroare de comunicaţie internă a echipamentului;
  - pierderea comunicaţiei în grup;
  - defect de răcire;
  - defectare senzori temperatură;
  - temperatura fluid tur sau retur în afara parametrilor setaţi;
  - senzori defecţi;
  - filtru aer colmatat;
  - pompa condens defectă;
  - detecţie scurgeri lichid;
  - defectare ventilator;
  - defectare sursa alimentare;
  - parametrii aer ieşire/intrare în afara celor setaţi.
- Echipamentele de răcire vor avea interfaţă de reţea Ethernet care să permită administrarea, monitorizarea şi notificarea evenimentelor într-o reţea cu protocol TCP/IP şi care să permită integrarea într-un sistem de management a infrastructurii fizice de suport a Centrului de date.
- Echipamentele de răcire trebuie să aibă aceeaşi înălţime şi adâncime ca şi rack-urile de servere furnizate, pentru a permite alinierea în faţă, spate şi înălţime şi a se putea implementa o soluţie de închidere şi izolare a culoarului de aer (cald sau rece). Astfel se poate realiza o soluţie care să permită instalarea de echipamente cu densităţi mari de putere. Ele vor fi astfel distribuite încât să se asigure atât fluxul de aer cât şi capacitatea de răcire necesare obţinerii condiţiilor optime de funcţionare a echipamentelor susţinute cât şi a redundanţei N+1. În situaţia defectării sau opririi unui echipament, celelalte echipamente trebuie să susţina răcirea corespunzătoare a tuturor rack-urilor.

- Echipamentele trebuie să fie livrate cu elementele necesare realizării canalelor de cablu pentru distribuţia circuitelor electrice de alimentare şi a cablării de date, sistem de susţinere deasupra rack-urilor şi care să se integreze cu cel al rack-urilor de echipamente.

Vor fi livrate şi instalate echipamentele de răcire, cu toate accesoriile necesare pentru conectarea în circuitul hidraulic, la sistemul de administrare şi monitorizare a infrastructurii Centrului de date şi accesoriile necesare realizării sistemului de susţinere a cablurilor electrice şi a sistemului de cablare structurată pozat pe deasupra rândurilor de rack-uri. Numărul lor trebuie să asigure soluţia de răcire a Centrului de date pentru încărcarea iniţială proiectată şi să asigurare redundanţa N+1 pentru echipamente.

Sistemul de management centralizat al infrastructurii Centrului de date

Sistemul de management centralizat trebuie să poată monitoriza parametrii de funcţionare pentru echipamentele propuse în soluţia pentru Centrul de date (UPS, distribuţie electrică modulară, unităţi de răcire, sistem de monitorizare a temperaturii şi umidităţii la nivel de rack).

Sistemul de management centralizat ofertat trebuie să aibă specificaţiile tehnice de mai jos, considerate minimale.

- Sistemul de management va fi livrat cu un server montabil în rack, cu accesoriile de instalare, pe care va rula aplicaţia de management centralizat.
- Sistemul de management va asigura monitorizarea centralizată prin utilizarea unei console grafice a alarmelor şi stărilor generale ale parametrilor echipamentelor de infrastructură a Centrului de date.
- Va efectua monitorizarea şi va asigura notificarea in timp real a evenimentelor care apar la echipamentele infrastructurii Centrului de date, asigurând eficienţa în luarea deciziilor, reducerea timpilor de reparare şi maximizarea disponibilităţii.
- Va asigura suport pentru echipamente de infrastructură de la producători diferiţi, ofertati in cadrul solutiei.
- Interfaţa utilizator trebuie să permită filtrarea evenimentelor critice, de atenţionare sau normale.
- Va detecta automat echipamentele şi va permite configurarea în grup pentru pragurile de alarmă.

- Va permite accesul la informaţiile curente şi istorice şi va permite efectuarea de analize asupra tendinţelor, pentru a se detecta din timp posibilele situaţii critice. Informaţiile vor fi stocate într-o bază de date centralizată a aplicaţiei, de unde va fi posibilă sortarea după tip eveniment, dată, tip echipament şi sau grup de echipamente.
- Să aibă posibilitatea integrării cu aplicaţii de administrare a operării, schimbărilor, capacităţii şi eficienţei energetice.
- Să permită administratorilor accesul Web, prin comunicaţii criptate, pentru a putea monitoriza 24 de ore din 24 starea echipamentelor infrastructurii de suport a centrului de date.

Sistemul de management centralizat va fi livrat cu toate accesoriile necesare pentru instalare şi operare în rack în sala de calculatoare a Centrului de date.

Sistemul de securitate integrat al Centrului de date

Echipamentele vor fi conforme EN54. Sistemul de detecţie şi semnalizare a incendiilor este tratat în seria de standarde SR EN 54. Standardele din această serie intră sub incidenţa directivei europene referitoare la produsele pentru construcţii 89/106/EEC. Pentru sistemul de stingere a incendiilor se va respecta SR EN 12094.

Sistemul de securitate integrat destinat Centrului de date va fi format din urmatoarele sisteme:

1.Sistem de control acces cu urmatoarele specificatii minime:

- Sa permita integrarea cu celelalte sisteme de securitate din cadrul Centrului de date, cu management din interfata unica
- Sa contina filtre de control acces dublu sens, cu functie anti passback
- Sa permita integrarea si managementul useri-lor cu tehnologie de tip Active Directory sau echivalent
- Sa fie sistem modular ce permite extensia ulterioara a sistemului fara a afecta functionarea sistemului initial
- Dotat cu electromagneti de forta si amortizoare hidraulice, cu montaj aplicat, butoane de urgenta si monitorizare a starii usii.
- Programare software a usilor care se vor dezarma in caz de urgenta si sunt pe calea de evacuare.

2.Sistem de supraveghere video IP

- Cuprinde camere IP, tip DOME, rezolutie HD, iluminare IR, compresi H.264
- NVR si storage pentru stocare minim 30 zile
- Sa permita integrarea cu celelalte sisteme de securitate, cu management din interfata unica

3.Sistem de alarmare la efractie

- Centrala de alarmare cu posibilitate de extensie a zonelor
- detectori PIR in dubla tehnologie, PIR+MW, montaj pe perete
- detectori de soc
- detectori de umiditate
- contacte magnetice de uz industrial, metalice cu cablul protejat in bucla metalica.
- Sa permita integrarea cu celelalte sisteme de securitate, cu management din interfata unica

4. Sistem de detecție și semnalizare a incendiilor

Dimensionarea și execuția instalației de detectare, semnalizare și avertizare incendiu-IDSAI și amenajarea spațiilor necesare instalării echipamentelor aferente se stabilește de proiectant în conformitate cu prevederile SR EN 54, corelat cu prevederile Normativul privind securitatea la incendiu a construcțiilor partea a III-a – instalații de detectare, semnalizare și avertizare incendiu Indicativ P118/3 – 2015 pe baza destinației construcției, caracteristicilor specifice ale produselor utilizate și în funcție de pericolul prognozat.

Documentația tehnico-economic se elaborează pe baza scenariului de securitate la incendiu, stabilindu-se măsurile, tehnicile, procedeele și organizarea instalațiilor de detectare, semnalizare și avertizare incendiu. De asemenea, tipul de acoperire va fi totală.

Instalația de detectare, semnalizare și avertizare incendiu trebuie proiectată astfel încât activarea sistemelor de stingere a incendiilor să nu pună în pericol persoane aflate în zona protejată. Se vor lua măsuri de protecție a acestora atât în cazul alarmelor reale cât și în cazul alarmelor false.

În cadrul instalației se vor utiliza doar produse introduse legal pe piață, în baza prevederilor HGR nr.668/2017.

5.Sistem de stingere a incendiilor

Alegerea tipului de instalație de stingere a incendiului, a substanței de stingere utilizată și valorile intensităților de stingere, protecție și răcire, trebuie să corespundă naturii produselor combustibile din spațiul protejat, condițiilor specifice concrete ale incintei respective, importanței și valorii produselor protejate, tipului de construcție etc.

La dimensionarea și execuția instalației de stingere se vor respecta prevederile Normativului privind securitatea la incendiu a construcțiilor, partea a II-a – Instalații de stingere, indicativ P 118/2-2013.

În cadrul instalației se vor utiliza doar produse introduse legal pe piață, în baza prevederilor HGR nr.668/2017.

- Detectie ultrarapida prin aspiratie, atat in rack-uri cat si sub pardoseala
- Conditionare la actionarea electrovanelor de evacuare a gazelor
- Sistem de eliminare al gazelor arse

NOTĂ

1. În conformitate cu prevederile legale, legea 333/2003, OMAI nr. 5/2017 și OMAI nr. 67/2017, numărul de repere aferente celor 2 locații vor rezulta în urma analizei de risc, sens în care analiza de risc se va realiza cu respectarea normelor în vigoare menționate anterior .

2. Analiza de risc se va face in conformitate cu OMAI nr. 5/2017 și OMAI nr. 67/2017.

3. Instalarea și operaționalizarea sistemelor de securitate fizică se va face de către Implementator în baza unui Proiect Tehnic avizat și livrat Beneficiarului în conformitate cu prevederile legii nr. 333/2003 si H.G. 301/2012 și normativelor interne.

4. Evaluarea riscurilor de incendiu din obiectiv se va efectua în conformitate cu legea 307/2006 art.19 lit.b.

   Evaluarea riscului de incendiu se va realiza în baza Scenariului de Securitate la incendiu – aprobat prin procedura proprie a MAI și a normelor tehnice de securitate la incendiu, respectiv Normativul de Siguranță la foc a construcțiilor indicativ P118/1999, având în vedere prevederile SR 10903/2, privind evaluarea sarcinii termice și a densității de sarcină termică, Normativul privind securitatea la incendiu a construcțiilor, Partea a II-a - Instalații de stingere", indicativ P118/2-2013, Normativul privind securitatea la incendiu a construcțiilor partea a III-a – instalații de detectare, semnalizare și avertizare incendiu Indicativ P118/3 – 2015 corelat cu prevederile art.19, lit.(b) din Legea nr.307/2006 privind apărarea împotriva incendiilor, cu completările și modificările ulterioare.

Cerinte minime obligatorii

Cerințe generale

- Soluţia pentru proiectarea şi implementarea Centrului de date oferita va fi de tip integrat, beneficiind de soluţii tehnice avansate, modulare şi scalabile, construite pe baza unor standarde deschise, de actualitate.
- Toate echipamentele furnizate trebuie să poată fi monitorizate din aplicaţia de management centralizat.
- Soluţia pentru Centrul de date trebuie să includă toate componentele hardware şi software necesare realizării unei soluţii integrate şi funcţionale incluzând cel puţin, dar fără a se limita la: rack-uri şi accesorii de management fluxuri de aer, sistem de protecţie a alimentării cu energie electrică (UPS) şi distribuţie electrica integrată, sistem de răcire, sistem de monitorizare a mediului (temperatura, umiditate, scurgeri de lichide), sistem de administrare, operare şi management.
- Soluţia ofertată trebuie să permită adăugarea ulterioară de noi module de infrastructură de suport fără a fi nevoie de reproiectarea în totalitate a soluţiei.
- Pentru soluţia de Centru de date se vor utiliza standarde deschise, neproprietare, pentru a permite interconectarea facilă cu alte sisteme şi pentru a permite adăugarea ulterioară de noi facilităţi infrastructurii de suport.

Performanță, calitate și fiabilitate

Din punct de vedere performanta, calitate si fiabilitate solutia propusa trebuie sa satisfaca urmatoarele cerinte minime si obligatorii:

- Să fie o soluţie integrată de infrastructură de suport care să asigure atingerea unui factor PUE (Power Usage Effectiveness) mediu sub 1,8 pentru Centrul de date.
- Să asigure performanţa şi eficienţa energetică pentru întreaga infrastructură de suport, atât pentru sistemul electric cât şi pentru cel de răcire, într-o plajă largă de variaţie a încarcării de putere IT, specifică sistemelor High-performance computing (HPC).
- Platforma pentru infrastructura de suport a Centrului de date trebuie să asigure un grad crescut de flexibilitate, astfel încât eventuale noi cerinţe ale beneficiarului să poată fi uşor aplicate.
- Pentru asigurarea unui nivel corespunzator de disponibilitate şi fiabilitate a soluţiei oferite se solicită în mod obligatoriu satisfacerea următoarelor cerinţe:
    - posibilitatea de a se asigura upgrade la redundanţa 2N pentru echipamentele din sistemul electric şi sistemul de răcire,
    - alarmare în timp real a defectelor,

- atenţionare a necesităţii efectuării mentenanţei preventive a echipamentelor, atingerea limitei de operare sau deterioararea parametrilor operaţionali,
- posibilitatea de a se înlocui module sau subansamble defecte fără a fi necesară întreruperea operării Centrului de date.

4.4.2. Datacenter site secundar

Echipamentele aferente site-ului secundar vor fi instalate în datacenter-ul existent în locaţia MAI din str. Leaota nr.2A, Bucureşti.

Echipamentele furnizate pentru dotarea datacenter-ului vor fi conforme cu normele europene. Pentru echipamentele exterioare se va ţine seama de normele naţionale şi europene privind acustica urbană şi limitele admisibile ale nivelului de zgomot.

Activităţi desfăşurate de furnizor:

- Evaluarea arhitecturii generale a spaţiului Centrului de date şi caracteristicile generale de construcţie, inclusiv analiza potenţialelor neconformităţi cu cerinţele standardelor;
- Evaluarea specificaţiilor pentru sistemul electric, incluzând furnizarea energiei electrice, sistemele electrice de backup şi distribuţia electrică pentru subsistemele de suport ale Centrului de date;
- Evaluarea specificaţiilor pentru sistemul mecanic, incluzând sistemele de aer condiţionat;
- Evaluarea specificaţiilor pentru sistemul de monitorizarea a mediului;
- Evaluarea specificaţiilor pentru sistemele de control acces, alarmare la efracţie şi supraveghere video.
- Evaluarea specificaţiilor pentru sistemul de cablare structurată.
- Evaluarea specificaţiilor pentru sistemul de detecţie şi semnalizare a incendiilor.
- Evaluarea specificaţiilor pentru sistemul de stingere a incendiilor.

Planificarea lucrărilor care vor fi prestate în Centrul de date

În această fază, utilizând rezultatele etapei de evaluare, se va realiza planificarea Centrului de date, în concordanţă cu cerinţele specifice ale beneficiarului şi asigurându-se maximizarea eficienţei energetice pentru toate susbsistemele de infrastructură fizică şi TI.

În această fază, utilizând rezultatele etapei de evaluare, se va realiza planificarea Centrului de date secundar, în concordanţă cu cerinţele specifice ale beneficiarului şi asigurându-se maximizarea eficienţei energetice pentru toate susbsistemele de infrastructură fizică şi TI.

Faza de planificare va utiliza datele din etapa precedentă pentru a pregăti elementele necesare proiectului final:

- Configuraţiile hardware şi de infrastructură, configuraţiile reţelei de date, inventarul pentru servere, echipamente de stocare, reţea şi alte echipamente TI;
- Infrastructura existentă a clădirii pentru asigurarea puterii şi capacităţii de răcire, împreună cu schemele arhitecurale şi ale instalaţiilor de suport fizic;
- Evaluările realizate on-site ale clădirii, oferind informaţii suplimentare de planificare, inclusiv necesarul de spaţiu pentru echipamentele de suport, stabilindu-se elementele arhitecturale, structurale, mecanice şi electrice.

Proiectarea detaliată a activităţilor care vor fi prestate în Centrului de date

Rezultatele activităţilor din faza de planificare vor fi utilizate în documentarea proiectării detaliate, astfel încât să poată fi obţinute aprobările necesare, iar implementarea Centrului de date să poată fi realizată fără, sau cu modificări minime, ale proiectului de execuţie.

Pe parcursul fazei de proiectare, detaliile din etapa de planificare vor fi materializate în planuri detaliate de implementare pentru instalarea cablării electrice, a sistemului de conducte pentru sistemul de răcire, de amplasare a echipamentelor, a detaliilor arhitecturale (pereţi, uşi), echipamentelor de monitorizare mediu, a specificaţiilor tehnice pentru sistemul de detecţie/stingere incendii şi cerinţelor de asigurare a securităţii fizice. Faza de proiectare a soluţiei va acoperi următoarele zone şi va trebui să fie materializată printr-un proiect de execuţie în concordanţă cu reglementările şi standardele în vigoare la data realizării:

- Sisteme mecanice: detalii, scheme şi specificaţii pentru sistemul de climatizare, sistemul hidraulic şi planurile pentru realizare, amplasare echipamente, planificare;
- Sistemele electrice: scheme şi specificaţii pentru echipamentele electrice, amplasare, planificare, scheme monofilara şi detalii, incluzând sistemele de susţinere în cazul căderilor de tensiune etc.;

- Sistemul de control acces, alarmare la efracţie şi supraveghere video. sistemul de detecţie şi semnalizare a incendiilor, sistemul de stingere a incendiilor: detalii, scheme şi specificaţii, planurile pentru realizare, inclusiv proiect tehnic.

Implementare, punere în funcțiune și testarea Centrului de date

Proiectul de implementare va include următoarele elemente:

- Asigurarea de către furnizor a igienizării şi astupării ferestrelor existente în camera tehnică, în care se vor instala echipamentele livrate, prin utilizarea de materiale speciale, conform normativelor în vigoare, care vor asigura cel puţin: protecţie la incendiu, izolare termică, barieră antivapori. Instalarea sistemului de suport de cabluri, a cablurilor şi circuitelor electrice din sala de calculatoare pentru a suporta necesarul de putere al Centrului de date secundar; se va asigura integrarea cu sistemele electrice existente ale beneficiarului.
- Instalarea echipamentelor externe ale sistemului de răcire, a sistemului de conducte al circuitului hidraulic şi a sistemului de control al mediului din Centrul de date secundar.
- Instalarea rack-urilor pentru echipamente, a echipamentelor interioare ale sistemului de răcire, a sistemului UPS şi de distribuţie protejată a energiei electrice la rack-uri, a soluţiilor de monitorizare.
- Testarea infrastructurii de suport şi a soluţiilor de monitorizare.

Cerințe tehnice minimale pentru proiectarea și implementarea Centrului de date secundar

Generalități

La implementarea proiectului Centrului de date secundar, următoarele cerinţe sunt obligatorii.

Spaţiul dedicat Centrului de date secundar va cuprinde :

- Spaţiul camerei tehnice:
  - Suprafața de circa 35 mp;
  - Rack-urile cu servere,
  - Rack-urile cu echipamente de comunicații, LAN şi conectica cablării structurate a clădirii şi a Centrului de date,

- Rack-urile dotate cu:
  - Kit-uri antiseismice;
  - Sisteme de distribuţie a alimentării de tip PDU;
- UPS-uri cu montare în rack ,
- Echipamentele interioare de climatizare,
- Componente ale sistemului de detecţie şi semnalizare a incendiilor,
- Componente ale sistemului de stingere a incendiilor
- Componente ale sistemelor de securitate fizică (control acces, alarmare la efracţie şi supraveghere video)
- Tablourile electrice de distribuţie.

- Un spaţiu exterior, pentru echipamentele externe ale sistemului de răcire, situat în vecinătatea clădirii Centrului de date secundar. Acesta cuprinde o platformă de beton, care va fi pregatită şi finalizată de furnizor şi va fi disponibilă la începerea serviciilor de instalare a echipamentelor exterioare, cu respectarea normelor de protecţie a mediului,etc.
- Fiecare rack va fi conectat la un dulap de distributie prin conexiuni UTP minim cat.7, respectiv conexiuni de fibra optica, astfel incat conectarea echipamentelor din rack-uri diferite sa se faca prin patch-cord-uri la nivelul dulapului de distributie. Pozarea cablurilor de cupru si fibra optica se va realiza prin canale de cablu instalate pe trasee diferite.

Standarde şi normative

În proiectare şi implementare se vor respecta cerinţele următoarelor standarde şi normative, după caz:

- ANSI/TIA-942 Telecommunications Infrastructure Standard for Data Centres:
  - Scopul standardului este de a oferi cerinţele şi recomandările pentru proiectarea şi implementarea de Centre de date.
  - Standardul se adresează proiectanţilor care au nevoie de o înţelegere cuprinzătoare a proiectării Centrelor de date, incluzând planificarea locaţiei, proiectarea sistemului de cablare şi a reţelei de date.

- Standardul specifică proiectarea cablării, a rețelei, a locației, conține anexe de informare cu privire la bunele practici și recomandări pentru cerințele de disponibilitate, definirea spațiilor, a rack-urilor și cabinetelor.

- EN 50173-5 Data Centre Cabling:
  - Scopul standardului este de a oferi un sistem de cablare generic pentru centre de date, care să suporte o gamă largă de aplicații existente sau emergente pentru LAN, SAN și WAN, care să fie scalabil, astfel încât să suporte creșterea viitoare pe durata de viață planificată a centrului de date și să fie suficient de flexibil pentru a face modificări în mod ușor și eficient.

- ANSI/TIA-568-C.0, Generic Telecommunications Cabling for Customer Premises:
  - Standardul defineste planificarea si instalarea unui sistem de cablare structurata pentru toate tipurile de premise ale clientilor. El specifica un sistem care suporta o cablare de telecomunicatii generica intr-un mediu care imbina o diversitate de produse si de producatori.
  - Standardul specifica cerintele pentru un sistem de cablare de telecomunicatii generic, incluzand:
    - Structuri ale sistemului de cablare,
    - Topologii si distante,
    - Instalare, performanta si testare,
    - Transmisie prin fibra optica si cerinte de testare.

- ANSI/TIA-568-C.1, Commercial Building Telecommunications Standard:
  - Standardul defineste planificarea si instalarea unui sistem de cablare structurata intr-o cladire comerciala si intre cladirile comerciale din cadrul unui campus.
  - Standardul defineste structurile sistemului de cablare incluzand:
    - Facilitatile de intrare a furnizorilor de comunicatii,
    - Salile de echipamente,
    - Salile de telecomunicatii,
    - Cablare backbone,
    - Cablare orizontala,

- Zona de lucru (spatiul care contine prizele de comunicatii).

- ANSI/TIA-568-C.2 Balanced Twisted-Pair Telecommunications Cabling and Components Standard:
  - Standardul include specificatiile pentru componente si cablare, precum si cerintele de testare pentru cablarea cu cupru (perechi torsadate), incluzand categoria 3, 5e, 6 si 6A.
- ANSI/TIA-568-C.3 Optical Fiber Cabling Components:
  - Scopul standardului este de a specifica cerintele de performanta pentru cablu si componente de fibra optica pentru cablarea cu fibra optica.
- ANSI/TIA/EIA-569-B Commercial Building Standard for Telecommunications Pathways and Spaces:
  - Scopul standardului este de a asigura operabilitatea, flexibilitatea, administrarea si longevitatea sistemului de cablare intr-un mediu complex de transmisii de telecomunicatii de voce si date (voce, date, video, securitate, semnale de control, etc.) descriind elementele de proiectare arhitecturala a sistemelor de suport pentru cabluri si spatiilor dedicate pentru echipamentele de telecomunicatii.
- ANSI/TIA/EIA-606-A Administration Standard for Commercial Telecommunications Infrastructure:
  - Standardul se refera la administrarea infrastructurii de comunicatii pentru cladire, incluzand documentatia de baza si actualizarea periodica a planurilor, etichetelor si inregistarilor. Administrarea va fi in sinergie cu sistemele de voce date si video precum si cu celelalte sisteme de semnalizare din cladire, incluzand sistemele de securitate, audio, alarme si management al energiei.
- J-STD-607-A Commercial Building Grounding and Bonding Requirements for Telecommunications:
  - Standardul specifica o infrastructura uniforma de impamantare si legare la masa in cladirile comerciale.
- ISO/IEC 11801, Generic Cabling for Customer Premises:
  - Standardul specifica un sistem de cablare generic, independent de aplicatie, capabil sa suporte o gama larga de aplicatii. El ofera o schema flexibila de

cablare, astfel incat modificarile sunt atat usor de realizat cat si economice. Standardul de cablare generica:

- Specifica o structura de cablare care suporta o larga varietate de aplicatii,
- Specifica clasele de canal E si F, bazate pe componente cu performante mai mari, capabile sa suporte aplicatii viitoare,
- Specifica cerintele componentelor si specifica implementarile de cablare care asigura legaturi permanente si canale care satisfac sau depasesc cerintele pentru clasele de cablare.

- BS EN 62040 Specification for UPS Systems
- BS EN 62040-1-1 UPS Safety Requirements
- IEC 60529 Degrees of Protection provided by Enclosures
- EN 61000 Electro Magnetic Compatibility Standard
- EMC Directive 89/336/EEC

Pentru sistemele electrice şi mecanice (sistemul de răcire) de suport se vor alege soluţii care să garanteze consum minim de energie şi eficienţă energetică în funcţionare, chiar în condiţii de încărcare a echipamentelor IT şi de comunicaţii de 30-40%. Se cere dimensionarea optimă a sistemelor infrastructurii de suport a Centrului de date, fiind unanim acceptat că supradimensionarea duce la creşterea masivă a pierderilor şi la ineficienţă energetică.

Soluţia propusă pentru Centrul de date trebuie să fie adaptabilă, flexibilă şi modulară şi să permită instalarea de rack-uri de servere cu mari densităţi de putere, fără oprirea sau modificarea configuraţiei iniţiale de rack-uri, prin creşterea capacităţii de putere şi de răcire şi prin soluţii de izolare a culoarului de aer cald sau rece. Soluţia trebuie să asigure integrarea în rack-uri a unor servere cu densităţi de putere de până la 15 KW/rack (pentru unele rack-uri). Soluţia trebuie să asigure parametrii optimi de mediu (capacitate de răcire şi flux de aer rece) pentru configuraţii de rack-uri cu diverse puteri TI (mici, medii şi mari).

Sistemele de securitate fizică vor fi proiectate şi dimensionate astfel încât să respecte specificaţiile din standardul ANSI/TIA-942 precum şi legislaţia română în domeniu.

Cerințe tehnice pentru sistemele de suport ale Centrului de date secundar

Sistemul de alimentare electrică şi protecţie la căderi de tensiune

Alimentarea cu energie electrică a Centrului de date secundar va fi realizată de la tabloul general al clădirii. Toate echipamentele din Centrul de date secundar, inclusiv sistemul de răcire aferent acestuia vor fi protejate împotriva anomaliilor de alimentare cu energie electrică prin generatorul prevăzut în proiect. In Centrul de date secundar vor fi instalate circuite electrice pentru alimentarea cu energie electrică a echipamentelor, astfel:

- un circuit trifazic pentru conectarea sistemului UPS redundant, care va alimenta rack-urile de echipamente IT şi sistemele de securitate.
- un circuit trifazic care va alimenta echipamentele externe ale sistemului de climatizare, cu o putere suficientă pentru funcţionarea instalaţiilor de răcire propuse;

Furnizorul va realiza proiectarea şi instalarea circuitelor electrice menţionate mai sus de la tabloul general al clădirii la Centrului de date secundar. Acesta va instala tablourile electrice necesare, automatizările, circuitele de protecţie, conectarea dual a rack-urilor şi a echipamentelor furnizate.

Alimentare electrică de rezervă

Circuitele electrice pentru Centrul de date secundar vor fi protejate împotriva anomaliilor de alimentare cu energie electrică de către generatorul prevăzut în proiect.

Dimensionarea Sistemului de alimentare electrică şi protecţie la căderi de tensiune

Sistemul de alimentare electrică şi protecţie la căderi de tensiune va fi dimensionat pentru o încarcăre de minim 200 KVA, pentru asigurarea continuităţii în funcţionare a Centrului de date secundar în condiţii optime. La dimensionarea sistemului de alimentare electrică şi protecţie la căderi de tensiune se vor lua în considerare şi echipamentele infrastructurii de suport care vor asigura condiţiile de mediu şi operare pentru Centrul de date secundar, respectiv alimentare protejată şi pentru echipamentele infrastructurii de suport (sistemul de răcire).

Acest sistem de alimentare va asigura alimentarea cu energie electrică în parametrii funcţionali, într-un interval de temperatură exterioară de la -40°C la +45°C.

Sistemul UPS (uninterruptible power supply) cu distributie electrica modulara integrata

Rack-urile de echipamente din Centrul de date vor fi protejate la căderi de tensiune de un sistem UPS (Uninterruptible Power Supply). Sistemul UPS oferit trebuie să fie eficient din

punct de vedere energetic într-o plajă largă de încărcare la ieşire şi să aibă integrat sistemul de distribuţie electrică pentru rack-urile de echipamente.

Sistemul UPS trebuie sa aiba specificatiile tehnice de mai jos care sunt considerate minimale.

- Să utilizeze o arhitectură robustă, industrială, de tip online cu dublă conversie, modulară şi scalabilă, cu MTBF ridicat,atât pentru putere cât şi pentru timpul de susţinere pe baterii.
- Să fie un sistem bazat pe tehnologia "transformer-free".
- Să fie instalat în rack-uri cu dimensiunile fizice ale rack-urilor standard de servere, pentru a putea fi integrat în rândurile de rack-uri de echipamente.
- Soluţia modulară trebuie să permită o scalabilitate până la 100 kW.
- Modulele de putere trebuie să permită upgrade de capacitate în paşi de maximum 10-20 KW, iar adăugarea de module de putere şi baterii sau înlocuirea modulelor defecte să poată fi efectuată fără oprirea sistemului UPS.
- Sistemul trebuie să poată ajusta automat puterea nominală furnizată în funcţie de temperatura mediului ambiant în care funcţionează: 110% la 25°C şi 100% la 40°C.
- Clasificare VFI conform IEC/EN 62040-3, EN-50091-3.
- Tehnologie 100% digitală.
- Sistemul trebuie să dispună de software integrat pentru managementul avansat al bateriilor (circuit de încărcare cu compensare funcţie de temperatură, testarea automată a bateriilor, determinarea exactă a timpului de back-up corelat cu diferenţele de temperatură şi ciclul de încărcare-decărcare). Fiecare modul de baterii trebuie să permită monitorizarea tensiunii şi temperaturii pentru a fi utilizate de sistemul de diagnosticare al bateriilor şi de încărcare.
- Să fie instalat în rack-uri cu dimensiunile fizice similare rack-urilor standard de servere.
- Să conţină bypass de mentenanţă şi sistem de distribuţie electrică pentru echipamentele IT şi de comunicaţii integrate în sistemul UPS.
- Să dispună de accesorii opţionale care să facă posibilă integrarea într-o soluţie de răcire pentru densităţi mari de putere împreuna cu rack-urile de echipamente protejate.
- Să aibă eficienţa AC-AC mai mare de 94% pentru sarcina la ieşire=100%.

- Să fie dimensionat cu o capacitate inițială de minimum 80 KW, în redundanță N+1 și să permită upgrade pentru o capacitate de minimum 100 KW.
- Amprenta la sol, în configurația finală, nu o va depăși pe cea a unui rack de servere standard, pentru un timp de susținere de minimum 6 minute la o încărcare de 80 KW. Pentru creșterea timpului de susținere trebuie să aibă opțiunea de instalare de rack-uri adiționale, similare cu cele ale sistemului UPS, pentru baterii.
- Tensiune alternativă nominală la intrare: 220/380, 230/400, 240/415 V cu L1, L2, L3, N, PE (R, S, T, nul, împământare), selectabilă.
- Să conțină bypass static integrat. Acesta va asigura transferul fără întrerupere a sarcinii de pe UPS pe intrarea de bypass dacă este necesară mentenanța sistemului sau dacă sistemul UPS nu poate să susțină sarcina critică.
- Să conțină bypass mecanic de mentenanță integrat. Acesta va permite izolarea totală a sistemului UPS în timpul activităților de testare sau mentenanță, asigurând siguranța personalului, timp în care sarcina este susținută de rețeaua externă de alimentare bypass.
- Să utilizeze baterii VRLA (Valve Regulated Lead Acid), fără mentenanță.
- Modulul de baterii trebuie să fie astfel realizat încât să permită înlocuirea de către utilizator, fără a fi necesară oprirea sistemului. Fiecare modul de baterii trebuie să permită monitorizarea tensiunii și temperaturii pentru a fi utilizate de sistemul de diagnosticare al bateriilor și de circuitul de încărcare cu compensare funcție de temperatură.
- Încărcarea bateriilor nu va depăși 10% din puterea de ieșire a sistemului UPS în condiții de încărcare 100% la ieșirea acestuia.
- Circuitul de încărcare al bateriilor va conține un circuit de compensare în funcție de temperatura bateriilor, pentru a optimiza durata de viață a acestora.
- Să conțină un sistem de management al bateriilor care să monitorizeze continuu starea fiecărui modul de baterii și care să transmită notificări în situația defectării sau deteriorării capacității unui modul.
- Să conțină un sistem de protecție a bateriilor, cu circuite de monitorizare și control, care să limiteze nivelul de descărcare a bateriilor.

- Sistemul UPS să fie controlat de două module de control, redundante, care să poată fi înlocuite, în caz de defectare, fără a fi necesară oprirea sistemului UPS. Fiecare modul de control trebuie să aibă căi de comunicaţii separate, izolate optic de cele ale modulelor de putere şi comutare statică şi va fi alimentat din surse de alimentare redundante.
- Să aibă un panou frontal, accesibil, care să permită afişarea parametrilor sistemului UPS şi a componentelor sale, a parametrilor electrici de ieşire şi intrare, a evenimentelor şi alarmelor, cu data şi ora producerii lor. Panoul va avea butoane prin care să se poată selecta parametrii sau evenimentele care doresc a fi vizualizate precum şi posibilitatea de a efectua programarea sau controlul unor funcţii ale sistemului UPS.
- Distribuţia electrică se va amplasa pe un traseu pe deasupra rack-urilor, iar lungimea cablurilor electrice va fi minimă, pentru a se minimiza pierderile şi degajările termice.
- Sistemul UPS trebuie să permită extinderea distribuţiei modulare cu circuite electrice monofazice sau trifazice suplimentare, dacă va fi necesar în viitor. Extinderea trebuie să poată fi făcută prin instalarea unui sistem de distribuţie modular suplimentar, independent sau montabil în rack standard. Sistemul de distribuţie modular suplimentar trebuie să fie conectat la sistemul de monitorizare şi administrare a infrastructurii.
- Sistemul UPS trebuie să aibă integrată o interfaţă de reţea Ethernet Web/SNMP care să permită integrarea într-un sistem de management a infrastructurii fizice de suport a Centrului de date secundar şi care să permită monitorizarea şi administrarea sistemului UPS, inclusiv sistemul de distribuţie electrică modulară, în mediu de reţea TCP/IP.

Furnizorul va asigura şi soluţia de alimentare a rack-urilor de echipamente de la sistemul de distribuţie modular al sistemului UPS şi va furniza şi barele de distribuţie (PDU - Power Distribution Unit) din rack-uri, capabile să susţină minimum 3,5 KW. Fiecare bară de distribuţie va fi conectata la câte un circuit electric de distribuţie distinct şi va avea prize IEC 320-C19 şi prize IEC 320-C13, în conformitate cu tipurile de echipamente ofertate şi cu o rezervă de minim o priză 320-C19 şi minim 3 prize IEC 320-C13. Fiecare bară de alimentare va fi monitorizată prin cardul SNMP şi va include şi posibilitatea instalării unui senzor de temperatură şi umiditate. Sistemul va permite adăugarea de noi circuite de alimentare, duale, pentru rack-uri, sau înlocuirea cu circuite de puteri mari (11 KW sau 22 KW în funcţie de

capacitatea prognozată pentru fiecare rack), pentru a se asigura creşterea densităţii de putere în rack-urile în care se vor instala echipamente noi sau se vor înlocui cele existente. Adăugarea sau înlocuirea de circuite electrice de distribuţie trebuie să poată efectua fără oprirea sistemului UPS.

Sistemul de racire pentru Centrul de date

Sistemul de răcire oferit pentru Centrul de date secundar trebuie să fie eficient din punct de vedere energetic şi să aibă funcţionare eficientă într-o plaja largă de variaţie a încărcării termice ale echipamentelor instalate în rack-uri. Se doreşte atingerea unui factor PUE (Power Usage Effectiveness) sub 1,6. De aceea, toate componentele sistemului de răcire, inclusiv proiectarea sistemului de răcire vor trebui să contribuie la atingerea acestui scop, prin integrarea în soluţie de module de tip „free cooling" pentru agentul de răcire. Echipamentele de răcire din sală trebuie să aibă consum energetic minim şi să fie adaptabile, funcţie de încărcarea termică dinamică a echipamentelor IT şi comunicaţii, prin controlul puterii ventilatoarelor pentru asigurarea debitului de aer rece, minimizarea lungimii căilor fluxurilor de aer şi minimizarea sau eliminarea amestecului fluxurilor de aer rece şi cald.

Soluţia de climatizare trebuie să asigure răcirea echipamentelor cu mari densităţi de putere din sala Centrului de date, inclusiv pentru rack-uri cu densităţi de putere de 10-20 KW/rack.

Toate echipamentele oferite vor fi din gama profesională, dedicate soluţiilor de răcire pentru Centre de date şi vor permite integrarea într-un sistem de administrare şi monitorizare, care va permite monitorizarea eficienţei energetice a infrastructurii Centrului de date.

Dimensionarea Sistemului de racire a Centrului de date

Va fi luată în considerare o marjă de eroare de 10-15%. La dimensionarea sistemului de răcire vor fi luate în considerare şi echipamentele infrastructurii de suport care generează încărcare termică în Centrul de date secundar. Infrastructura de suport trebuie să funcţioneze continuu, chiar şi în intervalul de timp de la căderea tensiunii de reţea şi pana la pornirea şi preluarea sarcinii de către sistemul electric de rezervă (grupul generator Diesel standby).

Echipamente de racire cu montaj la exterior (chillere)

Echipamentele de racire trebuie să poată fi integrate într-un sistem de răcire modular şi scalabil, pentru a asigura capacitatea de răcire pentru încărcarea termică iniţială şi să permită în viitor un upgrade pentru susţinerea încărcării termice finale specificate mai sus. Pentru asigurarea funcţionării continue se doreşte asigurarea redundanţei N+1 (un echipament va fi

în standby pentru a prelua funcţionalitatea în caz de defectare a altui echipament din sistem). Echipamentele vor fi din clasa de mare eficienţă energetică şi vor putea funcţiona, în intervalele cu temperaturi scăzute, în regim „free cooling".

Sistemul de răcire livrat și instalat va fi similar cu cel din site-ul principal.

Sistemul de securitate integrat al Centrului de date secundar

Echipamentele vor fi conforme EN54. Sistemul de detectare şi de semnalizare a incendiilor este tratat în seria de standarde SR EN 54. Standardele din această serie intră sub incidenţa directivei europene referitoare la produsele pentru construcţii 89/106/EEC. Pentru sistemul de stingere se va respecta SR EN 12094.

Sistemul de securitate integrat din cadrul Centrului de date va fi format din urmatoarele sisteme:

1.Sistem de control acces cu urmatoarele specificatii minime:

- Sa permita integrarea cu celelalte sisteme de securitate din cadrul Centrului de date, cu management din interfata unica
- Sa contina filtre de control acces dublu sens, cu functie anti passback
- Sa permita integrarea si managementul useri-lor cu tehnologie de tip Active Directory sau echivalent
- Sa fie sistem modular ce permite extensia ulterioara a sistemului fara a afecta functionarea sistemului initial
- Dotat cu electromagneti de forta si amortizoare hidraulice, cu montaj aplicat, butoane de urgenta si monitorizare a starii usii.
- Programare software a usilor care se vor deschide in caz de urgenta si sunt pe calea de evacuare.

2.Sistem de supraveghere video IP

- Cuprinde camere IP, tip DOME, rezolutie HD, iluminare IR, compresie H.264
- NVR si storage pentru stocare minim 30 zile
- Sa permita integrarea cu celelalte sisteme de securitate, cu management din interfata unica

3.Sistem de alarmare la efractie

- Centrala de alarmare cu posibilitate de extensie a zonelor
- detectori PIR in dubla tehnologie, PIR+MW, montaj pe perete
- detectori de soc
- detectori de umiditate
- contacte magnetice de uz industrial, metalice cu cablul protejat in bucla metalica.
- Sa permita integrarea cu celelalte sisteme de securitate, cu management din interfata unica

4.Sistem de detecție și semnalizare a incendiilor

Dimensionarea și execuția instalației de detectare, semnalizare și avertizare incendiu-IDSAI și amenajarea spațiilor necesare instalării echipamentelor aferente se stabilește de proiectant în conformitate cu prevederile SR EN 54, corelat cu prevederile Normativul privind securitatea la incendiu a construcțiilor partea a III-a – instalații de detectare, semnalizare și avertizare incendiu Indicativ P118/3 – 2015 pe baza destinației construcției, caracteristicilor specifice ale produselor utilizate și în funcție de pericolul prognozat.

Documentația tehnico-economic se elaborează pe baza scenariului de securitate la incendiu, stabilindu-se măsurile, tehnicile, procedeele și organizarea instalațiilor de detectare, semnalizare și avertizare incendiu. De asemenea, tipul de acoperire va fi totală.

Instalația de detectare, semnalizare și avertizare incendiu trebuie proiectată astfel încât activarea sistemelor de stingere a incendiilor să nu pună în pericol persoane aflate în zona protejată. Se vor lua măsuri de protecție a acestora atât în cazul alarmelor reale cât și în cazul alarmelor false.

În cadrul instalației se vor utiliza doar produse introduse legal pe piață, în baza prevederilor HGR nr.668/2017.

5.Sistem de stingere a incendiilor

Alegerea tipului de instalație de stingere a incendiului, a substanței de stingere utilizată și valorile intensităților de stingere, protecție și răcire, trebuie să corespundă naturii produselor combustibile din spațiul protejat, condițiilor specifice concrete ale incintei respective, importanței și valorii produselor protejate, tipului de construcție etc.

La dimensionarea și execuția instalației de stingere se vor respecta prevederile Normativului privind securitatea la incendiu a construcțiilor, partea a II-a – Instalații de stingere, indicativ P 118/2-2013.

În cadrul instalației se vor utiliza doar produse introduse legal pe piață, în baza prevederilor HGR nr.668/2017.

- Detectie ultrarapida prin aspiratie, atat in rack-uri cat si sub pardoseala
- Conditionare la actionarea electrovanelor de evacuare a gazelor
- Sistem de eliminare al gazelor arse

NOTĂ

- În conformitate cu prevederile legale, legea 333/2003, OMAI nr. 5/2017 şi OMAI nr. 67/2017, numărul de repere aferente celor 2 locaţii vor rezulta în urma analizei de risc, sens în care analiza de risc se va realiza cu respectarea normelor în vigoare menţionate anterior .
- Analiza de risc se va face in conformitate cu OMAI nr. 5/2017 şi OMAI nr. 67/2017.
- Evaluarea riscurilor de incendiu din obiectiv se va efectua în conformitate cu legea 307/2006 art.19 lit.b.

  Evaluarea riscului de incendiu se va realiza în baza Scenariului de Securitate la incendiu –aprobat prin procedura proprie a MAI şi a normelor tehnice de securitate la incendiu, respectiv Normativul de Siguranță la foc a construcțiilor indicativ P118/1999, având în vedere prevederile SR 10903/2, privind evaluarea sarcinii termice şi a densității de sarcină termică, Normativul privind securitatea la incendiu a construcțiilor, Partea a II-a - Instalaţii de stingere", indicativ P118/2-2013, Normativul privind securitatea la incendiu a construcțiilor partea a III-a – instalații de detectare, semnalizare şi avertizare incendiu Indicativ P118/3 – 2015 corelat cu prevederile art.19, lit.(b) din Legea nr.307/2006 privind apărarea împotriva incendiilor, cu completările şi modificările ulterioare.
- Autorizarea persoanelor care efectuează lucrari impotriva incendiilor se va face in conformitate cu OMAI 87/2010.

Cerinte minime obligatorii pentru site-ul secundar

Cerinte generale

- Soluţia pentru proiectarea şi implementarea Centrului de date oferita va fi de tip integrată, beneficiind de soluţii tehnice avansate, modulare şi scalabile, construite pe baza unor standarde deschise, de actualitate.
- Toate echipamentele furnizate trebuie să poată fi monitorizate din aplicaţia de management centralizat.

- Soluţia pentru Centrul de date secundar trebuie să includă toate componentele hardware şi software necesare realizării unei soluţii integrate şi funcţionale incluzând cel puţin, dar fără a se limita la: rack-uri şi accesorii de management fluxuri de aer, sistem de protecţie a alimentării cu energie electrică (UPS) şi distribuţie electrica integrată, sistem de răcire, sistem de monitorizare a mediului (temperatura, umiditate, scurgeri de lichide), sistem de administrare, operare şi management.
- Soluţia ofertată trebuie să permită adăugarea ulterioară de noi module de infrastructură de suport fără a fi nevoie de reproiectarea în totalitate a soluţiei.
- Pentru soluţia de Centru de date secundar se vor utiliza standarde deschise, neproprietare, pentru a permite interconectarea facilă cu alte sisteme şi pentru a permite adaugarea ulterioară de noi facilităţi infrastructurii de suport.

Performanţă, calitate şi fiabilitate

Din punct de vedere performanta, calitate si fiabilitate solutia propusa trebuie sa satisfaca urmatoarele cerinte minime si obligatorii:

- Să asigure performanţa şi eficienţa energetică pentru întreaga infrastructură de suport, atât pentru sistemul electric cât şi pentru cel de răcire, într-o plajă largă de variaţie a încarcării de putere IT, specifică sistemelor High-performance computing (HPC).
- Platforma pentru infrastructura de suport a Centrului de date trebuie să asigure un grad crescut de flexibilitate, astfel încât eventuale noi cerinţe ale beneficiarului să poată fi uşor aplicate.
- Pentru asigurarea unui nivel corespunzator de disponibilitate şi fiabilitate a soluţiei oferite se solicită în mod obligatoriu satisfacerea următoarelor cerinţe:
    - posibilitatea de a se asigura upgrade la redundanţa 2N pentru echipamentele din sistemul electric şi sistemul de răcire,
    - alarmare în timp real a defectelor,
    - atenţionare a necesităţii efectuării mentenanţei preventive a echipamentelor, atingerea limitei de operare sau deterioararea parametrilor operaţionali, posibilitatea de a se înlocui module sau subansamble defecte fără a fi necesară întreruperea operării Centrului de date

5. Prezentare sistem software de bază

5.1. Componenta de Portal

6. Componenta de portal va trebui sa asigure zone de portal separate pentru urmatoarele tipuri de activitati si utilizatori:
   - acces pentru autoritatile emitente ale actelor de stare civila si pentru cele care participa la activitatile de validare/notificare in procesul de emitere
   - acces pentru Institutiile Partenere (locale si centrale) pentru consultarea datelor si actelor de stare civila
   - acces pentru cetateni pentru consultarea datelor necesare eliberarii actelor de stare civila cat si pentru obtinerea actelor de stare civila electronice.

Componenta de Portal va asigura principalul punct de acces direct pentru utilizatori la modulele sistemului de emitere, validare si consultare documente si date de stare civila si va trebui sa raspunda la urmatoarele cerinte minime:

- Să ofere suport pentru tehnologii şi standarde deschise;
- Interfaţă web standardizată, simplă şi intuitivă;
- Interfaţă cu utilizatorii bogată în funcţionalităţi care să ofere un nivel ridicat de accesibilitate, conform cu cerinţele nivelului de accesibilitate WCAG 2.0;
- Componenta de management de conţinut care să permită stocarea şi gestionarea într-o manieră sigură şi eficientă a tuturor secţiunilor ce vor fi publicate prin intermediul portalului;
- Să ofere suport multi-lingvistic pentru instalare şi prezentare;
- Să asigure şi varianta pentru mobil (accesare de pe smartphone, tabletă, etc.) a portalului, asigurând funcţionalitatea tuturor facilităţilor disponibile în varianta pentru desktop.
- Un framework unic de dezvoltare a portalului, astfel încât indiferent de tipul de conţinut publicat în portal sau de tipul de aplicaţii, modul de integrare al acestora în portal să fie consistent şi sigur;
- Conţinutul va fi optimizat pentru utilizarea browser-elor:Microsoft Edge, Firefox, Opera, Chrome, Safari etc. Se vor opera upgrade-urile necesare în cazul apariţiei unor noi versiuni de browsere pe toată durata garanţiei;

- Servicii şi extensii ale portalului modulare, care să permită dezvoltarea ulterioară de noi functionalităţi;
- Arhitectură orientată pe servicii, astfel incât toate serviciile implementate pentru gestionarea conţinutului în portal (publicare, căutare, versionare, etc.), să poata fi reutilizate şi incluse în alte aplicaţii;
- Administrarea şi dezvoltarea portalului se va putea realiza facil, utilizând doar un browser web;
- Personalizarea experienţei utilizatorilor prin posibilitatea personalizării interfeţei de portal (aranjare în pagină, alegere skin-uri etc);
- Să ofere acces către toate resursele prezente în cadrul portalului printr-o singură autentificare, la deschiderea sesiunii. Un utilizator autentificat in cadrul Portalului nu va trebui sa se mai autentifice la accesarea unei componente a sistemului. Este suficienta o singura autentificare;
- Să ofere functionalităţi Web 2.0, pentru a asigura interacţiunea dintre utilizatorii portalului si sistem;
- Grad ridicat de securitate a sistemului, care să garanteze confidenţialitatea şi securitatea datelor utilizatorilor cât şi a datelor din sistem împotriva accesului neautorizat, atât din afară cât şi din interiorul sistemului;
- Să ofere posibilitatea de a utiliza un director LDAP pentru a stoca şi administra utilizatorii portalului;
- Stoparea temporară a unui nod din cluster pentru mentenanţă şi suport nu trebuie să afecteze disponibilitatea sistemului pentru activităţi normale;
- Mecanisme de balansarea dinamică a încărcării sistemului între resursele administrate în cadrul aceluiaşi cluster;
- Mecanisme de scalare a sistemului pe orizontală (Scale Out) şi verticală (Scale Up), pentru asigurarea scalarii solutiei in situatia in care numarul de utilizatori va creste in viitor, fara modificarea configuratiilor solutiei;
- Suport pentru servicii web, pentru integrare si interoperabilitate;
- Să permită instalarea si functionarea componentei de Portal pe distribuţiile majore de sisteme de operare prezente pe piaţă: Windows, Linux şi UNIX.
- Rapoarte analitice asupra tuturor acţiunilor utilizatorilor, care să ofere posibilitatea de a analiza traficul şi activitatea utilizatorilor pe portal;
- Să conţină un motor de căutare performant, care se permită efectuarea de interogări în toate sursele de informaţie disponibile prin portal.

5.2. Server web (DMZ)

Pentru protejarea zonei de aplicatii, in zona de interfatare DMZ se vor instala punctele de intrare in sistem pentru utilizatori prin intermediul serverelor web al caror principal scop este:

- Să permită, din punct de vedere tehnic, vizualizarea layout-ului şi a resurselor Portal într-un browser Web;
- Să se integreze cu cel puţin o soluţie de tip Single-Sign On pentru autentificarea unitară a utilizatorilor;
- Să permită, din punct de vedere tehnic, accesarea aplicaţiei din browsere tradiţionale (Microsoft Edge, Mozilla Firefox, Opera, Chrome etc.), inclusiv de pe dispozitive mobile;
- Să asigure prin componentele software ale serverului Web funcţionarea în cluster pentru a asigura balansarea încărcării şi disponibilitatea maximă a aplicaţiei;
- Sa permita rularea pe distribuţiile majore de sisteme de operare prezente pe piaţă: Windows, Linux şi UNIX

5.3 Platforma de aplicatii

Asa cum s-a mentionat in descrierea arhitecturii solutiei, se solicita o arhitectura, modulară si care sa permită integrarea si interoperabilitatea cu alte sisteme si servicii. Astfel va fi necesara dezvoltarea mai multor aplicatii si servicii web, cel putin pentru modulele de emitere, validare si consultare documente si date de stare civila.

Componenta server de aplicatii va asigura infrastructura necesara executiei aplicatiilor moderne bazate pe standarde deschise, si trebuie sa asigure un set de servicii standard pe care toate aplicatiile dezvoltate si instalate sa il poata accesa si utiliza:

- servicii de clusterizare pentru o scalabilitate si disponibilitate ridicata;
- servicii de balansare si dirijare a incarcarii (load balancing);
- servicii de securitate pentru protejarea resurselor gazduite;
- servicii de management al tranzactiilor la nivelul aplicatiilor.

Pentru a raspunde acestor cerinte si celor prezentate in descrierea arhitecturii tehnice si celei functionale, cerintele corespunzatoare platformei de aplicatii sunt:

- Mecanisme de grupare a serverelor in clustere de servere de aplicatii atat in topologii

de tip activ-activ cat si activ-pasiv

- Stoparea temporara a unui nod din cluster pentru mentenanta si suport, nu trebuie sa afecteze disponibilitatea celuilalt nod (acest nod permitand executarea/ desfasurarea activitatilor curente)
- Mecanisme de balansare dinamica a incarcarii sistemului intre resursele administrate in cadrul aceluiasi cluster
- Mecanisme de scalare a sistemului pe orizontala si verticala
- Server web integrat
- Sa permita rularea pe sistemul de operare ofertat
- Consola de administrare a serverelor de aplicatii cu capabilitati de gestiune a schimbarilor de configuratii:
    - blocarea unei configuratii in vederea modificarii
    - salvarea unei configuratii fara aplicare efectiva
    - revenirea la o configuratie anterioara
    - istoricul modificarilor

5.4 Indexare Documente Electronice

Platforma software de indexare va asigura preluarea continutului digitizat si a metadatelor aferente si le va prelucra si valida inaintea incarcarii acestora in cadrul solutiei de Gestionare a Documentelor in Format Electronic. Platforma software de indexare va asigura actualizarea consistenta a continutului digital in cadrul sistemului.

Pentru indexarea fondului arhivistic este nevoie de o solutie (sau facilitate/opțiune inclusă în platformele furnizate) care sa permita preluarea documentelor in format electronic si indexarea acestora in componenta de Stocare si Gestionare Documente in Format Electronic.

Platforma software trebuie să conțină o componentă pentru captura, scanarea și indexarea documentelor (scanare/import document, procesare documente scanate), integrată cu celelalte componente (fluxuri de lucru, management de documente).

Solutia trebuie sa asigure cel putin urmatoarele functionalitati:

- Ofera functionalitati de imaging, captura si indexare de documente si fluxuri de lucru
- Procesarea imaginilor şi realizarea de activitati cu documente in fluxuri de lucru chiar din interfata aplicatiei. O solutie care sa ofere - captura, recunoastere, imaging si workflow.

- Clasificare inteligenta a documentelor si extragere de date – sa utilizeze Optical Character Recognition (OCR) pentru a extrage datele
- Completarea metadatelor pentru documentele scanate
- Sa se integreze cu Solutia de management a fluxurilor si proceselor pentru a oferi o platforma pentru procese de prelucrare a documentelor fizice cat si creare si administrare de fluxuri de lucru.
- Sa ofere capabilitati de validare de date pentru a asigura integritatea datelor prelucrate. Dacă validarea eşuează, nu se va trece la etapa următoare
- Scanarea si indexarea in format electronic a documentelor ce se doresc a fi stocate in solutia de gestiune documente; extragerea şi completarea automată a metadatelor.
- Să asigure trimiterea documentelor pe fluxuri de lucru;
- Salvarea documentelor scanate în diverse formate utilizate de beneficiar în care se pot efectua căutări, cum ar fi documente fisiere text, XML, HTML şi formate de imagini cum ar fi de ex. TIFF, JPG, PDF, GIF etc.
- După salvare, documentele şi metadatele vor putea fi utilizate imediat de celelalte componente ale sistemului (fluxuri de lucru, management documente);Modulul de scanare trebuie sa ofere utilizatorilor posibilitatea de a efectua scanari fara restrictii de volum;
- Sa se permita reducerea numarului de erori ce apar la introducerea datelor de catre operatorii de indexare (ex: prin posibilitatea de interfatare cu baze de date externe pentru a extrage si/sau valida informatii);

Platforma software nu trebuie să impună limitări în ceea ce priveşte alegerea echipamentelor de scanare şi numărul lor. Trebuie să poată fi folosit orice tip de echipament de scanare, fără a fi nevoie de licenţiere specială în acest sens.

5.5. Stocarea si Gestionarea Documentelor in Format Electronic

Aceasta solutie asigura gestionarea si stocarea continutului electronic rezultat in urma digitizarii documentelor de stare civila existente, impreuna cu indicatorii si metadalele preluate in urma procesului de digitizare. In acelasi timp, pentru noile documente de stare civila care vor fi eliberate, va asigura gestionarea si stocarea documentelor electronice a formularelor si documentelor scanate in urma procesului de eliberare.

Soluţia de stocare si gestionare a documentelor de stare civila si de pastrare a acestora trebuie să fie o soluţie matură, de tip enterprise si trebuie sa se integreze cu componentele solutiei si trebuie sa indeplineasca cerinţele tehnice şi funcţionale enumerate mai jos:

- Soluţia trebuie să permită gestionarea electronică a documentelor de lucru specifice activităţilor de eliberare si arhivare.
- Documentele gestionate trebuie să fie stocate, la nivel logic, într-un depozit securizat de documente/baza de date.
- Soluţia trebuie să asigure integrarea cu soluţia de management centralizat al utilizatorilor / LDAP pentru autentificarea şi managementul centralizat al utilizatorilor;
- Din punct de vedere al securităţii, soluţia trebuie să ofere funcţionalităţi atât pentru autentificarea utilizatorilor cât şi pentru autorizarea acestora.
- Accesul la documentele gestionate trebuie să se realizeze pentru utilizatorii autentificaţi pe baza unor drepturi de acces gestionate în cadrul soluţiei.
- Soluţia trebuie să permită declararea anumitor documente ca fiind publice. Utilizatorii trebuie să poată accesa documentele publice fără a fi necesară autentificarea lor în aplicaţie.
- Soluţia trebuie să permită gruparea documentelor în foldere, subfoldere şi organizarea acestora într-o structură arborescentă similară sistemelor de fişiere folosite de sistemele de operare.
- Fiecare document gestionat trebuie să aibă asociate câmpuri index predefinite şi câmpuri index specifice, definite de administratorii soluţiei.
- Soluţia trebuie să permită definirea de câmpuri index care se vor asocia fiecărui dosar sau document. Definirea câmpurilor index şi toate setările de configurare a acestora trebuie să poată fi realizate în interfaţa de administrare a soluţiei, fără a necesita programare.
- Tipurile de date acceptate de fiecare câmp index trebuie să fie cel puţin următoarele: text, dată calendaristică, număr întreg, număr real, listă de opţiuni. În cazul câmpurilor de tip listă de opţiuni, soluţia trebuie să permită atât valori predefinite cât şi popularea automată a listei cu valori noi introduse.
- Fiecare câmp index trebuie să poată fi declarat ca obligatoriu (necesită introducerea unei valori (documentul nu poate fi salvat fără completarea acestui câmp) sau opţional (nu necesită introducerea unei valori).

- Soluţia trebuie să permită importul manual al documentelor şi completarea câmpurilor index asociate.
- Câmpurile index trebuie să poată fi completate atât manual de către utilizatori cât şi automat pe baza unor reguli automate de clasificare şi catalogare. Motorul de catalogare automată trebuie să fie inclus în soluţia ofertată.
- Soluţia trebuie să permită importul simultan al unui număr mare de documente (loturi de documente) împreună cu metadatele asociate.Soluţia trebuie să permită conversia automată a următoarelor tipuri de documente:
    - documente create cu editoare de text
    - foi de calcul tabelar
    - prezentări
    - formate grafice
    - formate tabelă
- Soluţia trebuie să permită integrarea cu aplicaţii desktop cum ar fi Microsoft Windows Explorer, Microsoft Office (Word, Excel, Outlook), etc.
- Sistemul va putea permite definirea si utilizarea taxonomiilor.
- Soluţia trebuie să permită adăugarea de adnotari pe documente.
- Soluţia trebuie să ofere funcţionalităţi de gestionare a documentelor în mod offline.
- Soluţia trebuie să permită indexarea full-text a documentelor gestionate, motorul de indexare full-text trebuie să fie inclus în soluţia propusă.
- Soluţia trebuie să permită pentru fiecare document gestionat păstrarea unui istoric al acţiunilor realizate asupra sa.
- Soluţia trebuie să permită pentru fiecare document gestionat păstrarea unui istoric al versiunilor sale.
- Soluţia trebuie să permită pentru fiecare document gestionat păstrarea metadatelor.
- Soluţia trebuie să nu impună sau sa limiteze prin arhitectură, prin licentiere sau prin implementare numărul de dosare sau de documente care se pot adăuga.
- Pentru un acces uşor la documente, soluţia trebuie să permită transformarea dinamică în alte formate (ex: PDF, TIFF) a documentelor importate. Documentul astfel generat trebuie să fie asociat documentului original ca o nouă versiune a acestuia.
- Pentru integrarea cu alte sisteme, soluţia trebuie să dispună de API-uri şi să permită apelarea funcţionalităţilor prin intermediul serviciilor web.

- Soluţia trebuie să ofere şi posibilitatea de integrare cu alte aplicaţii de tip web pe bază de servicii web (SOAP, REST), să fie capabilă să consume servicii web şi să ofere un layer de servicii web pentru integrarea şi prezentarea informaţiilor astfel obţinute..
- Soluţia trebuie să permită trimiterea prin email a unor link-uri către documente din depozitul de documente.
- Soluţia trebuie să ofere capabilităţi de căutare a documentelor stocate în sistem şi afişare sub formă tabelară a rezultatelor căutărilor
- Soluţia trebuie să ofere posibilitatea de a interoga după toate valorile câmpurilor index/metadate conform schemelor de indexare definite.
- Soluţia trebuie să permită căutări după cuvintele din cadrul documentelor (full-text) şi căutări aproximative (fuzzy search).
- Soluţia trebuie sa permită efectuarea de căutări complexe, care să includă operatori logici sau folosirea caracterelor de substituţie (wildcards).
- Soluţia trebuie să pună la dispoziţie o interfaţă de administrare pentru crearea şi configurarea, activarea/dezactivarea fluxurilor de lucru. Fluxurile de lucru trebuie să poată fi dezvoltate utilizând o interfaţă grafică.
- Soluţia trebuie să permită iniţierea automată a fluxurilor de documente de la importul acestora în sistem, în concordanţă cu procedurile de lucru definite în cadrul organizaţiei.
- Soluţia trebuie să fie capabilă să trimită notificări automate pe email.
- Soluţia trebuie să suporte gestionarea întregului ciclu de viaţă al documentelor de la creare până la eliminarea acestora din sistem.
- Soluţia de trebuie să permită definirea unor categorii de retenţie în care se va specifica perioada de păstrare a documentelor şi acţiunile ce se întreprind asupra acestora pe parcursul şi la sfârşitul perioadei.
- Soluţia să permită vizualizarea fluxurilor de lucru în cadrul aplicaţiei;
- Soluţia de trebuie să permită definirea termenelor limită pentru fiecare etapă a fluxului de lucru;
- Soluţia de trebuie să permită redirecţionarea automată a sarcinilor în cazul în care utilizatorul şi-a delegat sarcina
- Soluţia de trebuie să permită definirea variabilelor pentru fluxurile de lucru;
- Soluţia de trebuie să permită generarea unui raport/tabel cu toate fluxurile de lucru şi toate informaţiile aferente;

- Soluţia de trebuie să permită configurarea atributelor unei sarcini (ex. Termen de finalizare, grad de urgenţă, tip sarcină, responsabil);
- Soluţia trebuie să permită gestionarea conţinutului digital (imagini scanate, etc.).
- Soluţia trebuie să pună la dispoziţia utilizatorilor toate funcţionalităţile platformei prin intermediul unor aplicaţii de tip standard (out-of-the-box).
- Sa permita rularea pe sistemul de operare ofertat
- Soluţia trebuie să poată utiliza oricare din următoarele sisteme de gestiune a bazelor de date: Microsoft SQL Server, Oracle Database, IBM DB2.
- Soluţia trebuie să permită accesul utilizatorilor şi administratorilor la funcţionalităţile oferite prin intermediul unui browser Web. Browserele suportate trebuie să fie ultimele versiuni pentru: Microsoft Edge, Mozilla Firefox, Google Chrome şi Apple Safari.
- Solutia trebuie sa ofere facilitati de delegare a taskurilor.

5.6 Analiza si Raportare

Prin modul in care este conceput SIIEASC, va fi nevoie de o componenta de analiza si raportare care va implementa urmatoarele principii, care sa asigure un maxim de beneficiu in procesele de raportare si analiza referitoare la situatia emiterii documentelor de stare civila:

- Viziune unica asupra datelor si documentelor;
- Viziune unica din punct de vedere semantic asupra datelor;
- Accesul facil pentru utilizatori la datele la care au acces;
- Acces la date in timp real pentru generarea rapoartelor;
- Infrastructura unitara.

Din punct de vedere tehnic componenta de raportare si analiza de business trebuie:

- Sa ofere posibilitatea prezentarii datelor in formate variate (tabele, tabele pivot, grafice, etc.), în funcţie de cerinţele utilizatorului. Datele ce vor fi afişate vor putea fi filtrate şi personalizate în funcţie de drepturile şi rolurile utilizatorului care accesează raportul, a criteriilor specifice fiecărui raport, precum şi pe baza criteriilor selectate de utlizator;
- Sa permita salvarea/generarea rapoartelor in formate diferite (Excel, PDF, Word, HTML, XML, CSV etc) şi în diferite moduri (afişare pe ecran, imprimare, e-mail, stocare pe disc);

- Să asigure generarea rapoartelor statistice, atât pentru rapoarte predefinite, cât şi pentru rapoarte dinamice, la cerere. Rapoartele vor putea fi definite, vizualizate, modificate sau chiar şterse dacă nu se mai utilizează;
- Să permită furnizarea rapoartelor legate de activitatea zilnică a utilizatorilor privind gestionarea actelor de stare civilă, situaţii statistice în funcţie de perioada selectată;
- Să permită generarea automată zilnică, săptămânal, lunar sau la intervale predefinite de timp a rapoartelor şi transmiterea acestora pe e-mail la grupuri predefinite de management, utilizatori etc.;
- Să permită organizarea rapoartelor pe categorii care vor corespunde domeniilor de activitate, pentru a facilita regăsirea lor.
- Mediul de lucru pentru utilizatorii finali sa fie in mediu web;
- Sa faciliteze accesul la informatie printr-un nivel de metadate care sa ascunda utilizatorilor finali complexitatea structurilor fizice de date;
- Nivelul de metadate expus utilizatorilor sa fie comun la nivelul tuturor modulelor sistemului de raportare si analiza;
- Utilizatorii sa isi poata crea propriile rapoarte (analize ad-hoc) fara sa fie nevoiti sa cunoasca in detaliu structurile fizice de date pe care le acceseaza;
- Sa ofere posibilitatea prezentării aceleiaşi informaţii in formate diferite: de exemplu tabel si grafic;
- Sa permităfacilitaţi avansate de formatare a rapoartelor;
- Sa ofere posibilitatea de a salva, organiza si partaja rapoartele cu alţi utilizatori;
- Sa ofere capabilităţi de drill-down pe diferite nivele de agregate;
- Accesul utilizatorilor la informaţie trebuie sa se facă si pe criteriul domeniului de valori (de exemplu un utilizator sa nu poată vedea decât rândurile la care acces);
- Să dispună de mecanisme de alertare pentru utilizatorii finali (cel putin prin aplicaţie, email si dispozitive mobile);Sa dispuna de mecanisme de optimizare a accesului utilizatorilor la informatie (cu impact minim asupra bazei de date);
- Din punctul de vedere al arhitecturii soluţiei de raportare, toate componentele sale trebuie sa fie strâns integrate, să facă parte dintr-un mediu unitar de lucru şi să utilizeze un sistem de securitate comun;
- Sa ofere posibilitatea agregărilor de date pentru acces rapid la rapoarte;
- Soluţia de raportare va fi utilizată de 150 de utilizatori, din care 50 utilizatori concurenţi;
- Realizarea de rapoarte să se facă în mod independent de sursele de date fizice

- Eventualele modificări în structurile fizice de date să poată fi capturate şi sincronizate cu uşurinţă în nivelul logic;
- Să ofere posibilitatea de a programa pentru rulare la un anumit moment a rapoartelor;
- Să permită integrarea cu diverse sisteme sursă/aplicaţii de raportare într-o manieră unificată;
- Să implementeze politici specifice de securitate pentru gestiunea accesului la rapoarte;
- Să dispună de propriul nivel de securitate pentru definirea accesului la rapoarte;

5.7 Sistem de Gestiune a Bazelor de Date

Bazele de date reprezinta o componenta critica in cadrul infrastructurii, de aceea, pentru bazele de date se solicita un sistem dedicat care sa contina toate componentele necesare (servere pentru bazele de date, sistemul de gestiune a bazelor de date, solutie de stocare, infrastructura de comunicatii) pentru a fi complet redundant, scalabil si capabil sa ofere performante ridicate.

Sistemul pentru gestiunea bazelor de date reprezinta componenta care permite stocarea si regasirea datelor solicitate de catre utilizatori prin intermediul aplicatiilor. Accesul la informatiile stocate in baza de date trebuie sa se efectueze in urmatoarele conditii:

- Datele sa poata fi protejate impotriva defectarii componentelor sistemului de baze de date;
- Functionarea aplicatiei sa nu fie afectata in cazul unor intreruperi ale unei componente din sistemul de baze de date;

Sistemul de baze de date trebuie sa contina toate elementele necesare functionarii optime si anume: servere pentru procesarea bazelor de date, sistemul de gestiune a bazelor de date, sistem dedicat pentru stocarea datelor, retea, conectica si toate echipamentele aditionale necesare implementarii si functionarii.

Tinand cont de importanta datelor prelucrate de SIIEASC si de volumul acestora, de cerintele de securitate cat si de diversitatea datelor, atat sub forma de date relationale cat si sub forma binara (documente, imagini, etc), este necesara furnizarea unui sistem unitar, robust si sigur de gestiune a bazelor de date.

Pentru a se asigura o platforma unitara de stocare a datelor este necesar un sistem performant de gestionare a datelor de tip relational, astfel:

- Sa fie un sistem de gestiune a bazelor de date de tip relational
- Sa ofere suport pentru proceduri stocate si triggeri
- Sa permită definirea de indecsi pentru acces rapid la date
- Sa permita rularea pe sistemul de operare ofertat
- Sa permitărestricționarea accesului la nivelul obiectelor bazei de date
- Sa permită minimizarea conflictelor de acces la date si garantarea simultaneitatii accesului la date
- Sa permită reorganizarea, mutarea si redefinirea de tabele fără blocarea activitatii
- Sa aiba posibilitatea de a suspenda temporar operatii consumatoare de resurse (de exemplu incarcari masive de date), cu reluarea ulterioara a acestora
- Sa permita prioritizarea modului de accesare a bazei de date in functie de utilizator
- Sa ofere suport date multimedia
- Sa ofere suport pentru tranzactii autonome
- Sa permită executia de instructiuni INSERT in mai multe tabele simultan
- Sa permită executia paralela a operatiilor de tip SELECT, INSERT, UPDATE, DELETE, MERGE, cu blocarea doar a inregistrarilor afectate, nu a intregii tabele
- Sa ofere mecanisme de restaurare rapida in caz de eroare, la nivel de tranzactie, tabela sau baza de date, fără a fi necesara intreruperea activitatii pe baza de date
- Sa permită limitarea numarului de conexiuni la baza de date prin folosirea unui mecanism de tip database connection pooling
- Sa permită recuperarea tranzactiilor aflate in lucru in momentul intervenirii unei caderi (roll-forward)
- Sa ofere suport pentru sincronizarea bidirectională a datelor între două sau mai multe instanțe ale bazei de date
- Sa ofere mecanisme de restrictionare a accesului utilizatorilor la nivel de inregistrare si coloana într-o tabela
- Sa permită salvarea/restaurarea, importul/exportul si arhivarea/dezarhivarea datelor in regim de lucru online
- Sa permita salvarea totala si/sau partiala a bazei de date
- Sa permită efectuarea de backup automat într-o forma unitara, centralizata si usor de administrat

- Sa permită efectuarea de backup numai pentru datele care au suferit schimbari de la ultimul backup si pentru datele nou create
- Sa ofere rapoarte locale si consolidate asupra intregului mediu de backup cat si a operatiunilor de backup
- Sa permită recuperarea totala si partiala a bazei de date de la un moment de timp specificat de utilizator
- Sa permită inregistrarea tuturor modificarilor bazei de date pentru a permite recuperarea bazei de date (inregistrarea tranzactiilor)
- Sa permită instalarea unei singure baze de date pe mai multe noduri (arhitectura de tip cluster activ-activ) pentru a asigura toleranta la defecte hardware sau nefunctionare planificata, scalabilitatea si disponibilitatea crescuta a sistemului
- Sa ofere mecanisme de criptare a datelor din baza de date
- Sa permită balansarea incarcarii intre noduri la nivelul cererilor si executiilor pe baza de date aflata in cluster
- Sa ofere disponibilitate de tip 24x7 pentru utilizatori in cazul aparitiei unei defectiuni hardware la unul din serverele cluster-ului de baza de date
- Sa permita reconectarea automata la nodul sau nodurile ramase disponibile dupa aparitia unei defectiuni.
- Sa ofere capabilități incluse de monitorizare si diagnosticare continua a starii bazei de date in scopul identificarii potentialelor probleme de performanta
- Pentru gestionarea mai usoara a drepturilor de acces, baza de date trebuie sa ofere mecanisme incluse care sa permită definirea de domenii asupra seturilor de date continute.

5.8 Componentele de securitate cibernetică

Din punct de vedere al componentelor necesare pentru a asigura cerintele de securitate prezentate in prezentul proiect, au fost identificate urmatoarele:

-Componenta de securizare acces servicii electronice – care va securiza accesul la serviciile electronice catre beneficiarii acestui sistem si pentru securizarea accesului integrarii la nivel de servicii web

*-Componenta de control al accesului utilizatorilor la sistem-Componenta de administrare unitara a profilelor de utilizato*r

-Componenta de administrare unitara a profilelor de utilizator

-Componenta de integrare cu alte sisteme

-Componenta de stocare centralizata a profilelor de utilizator (LDAP)

-Componenta de monitorizare a logurilor si traficului de retea

-Componenta de detectare a codului malitios (malware)

5.8.1. Securizare Acces Servicii Electronice

Datorita cerintelor de integrare ale sistemului SIIEASC cu sisteme externe, este necesara securizarea accesului la serviciile web expuse către aceste sisteme externe si de a scadea costurile operatiunilor administrative legate de controlul accesului la aceste servicii, prin implementarea unei componente de securizare a accesului la interfete web in mod centralizat.

Avand in vedere rolul important al acestei componente se doreste implementarea unei solutii de tip „COTS", care sa satisfaca cel putin urmatoarele cerinte functionale si tehnice:

- Modul centralizat de gestiune si control al politicilor de acces pentru serviciile web
- Suport pentru standardul Web Service Definition Language (WSDL)
- Autentificarea accesului la servicii
- Autorizarea accesului la servicii
- Controlul accesului la nivel aplicatie
- Suport pentru protocolul (SSL)/TLS si certificate compatibile X.509
- Mod de functionare de tip „transparent" (in-line) gateway fără modificarea serviciilor protejate
- Definirea declarativa a politicilor de access sa fie facuta utilizand o consola web-based
- Auditarea parametrizabila a apelurilor de servicii web
- Ofera capabilităţi de WS/API firewall si funcţii de control acces pe baza de politici de acces de tip RBAC
- Solutia trebuie sa detecteze atacuri de genul SQL-injection sau XPATH-injections
- Sa poată limita numarul de mesaje pe o perioada de timp
- Sa poată limita numarul de conexiuni concurente către un anumit serviciu web expus
- Sa poată preveni atacuri informatice specifice cunoscute;
- Solutia trebuie sa monitorizeze accesele in timp real si sa permită vizualizarea statisticilor pe perioade de timp.

- Sa aiba un mecanism de alertare in cazul detectarii de activitati/interogari cu un volum anormal de date
- Sa poată cripta si decripta mesaje XML/JSON
- Sa poată monitoriza si alerta in cazul in care unul sau mai multe servicii API expuse au performanțe deteriorate, conform unor limite configurabile;
- Sa poată prioritiza traficul pe baza clientului, utilizatorului si atribute de servicii
- Posibilitatea de monitorizarea modului in care politicile de acces sunt respectate
- Integrabilă cu software-ul de control al accesului la resurse
- Integrabilă cu platforma de executie a proceselor
- Integrabilă cu serverul de aplicatii
- Sa ruleze pe toate distributiile majore de sisteme de operare prezente pe piata (Windows, Linux, Unix)

5.8.2. Controlul accesului utilizatorilor la sistem

Sistemul informatic SIIEASC va fi compus din mai multe componente, fiecare indeplinind cerinte functionale specifice. Pentru a se asigura un control al accesului centralizat, unificarea experientei de utilizare dar si pentru a creste nivelul de securizare si a scadea costurile operatiunilor administrative legate de controlul accesului la aplicatiile si componentele sistemului, se doreste implementarea unei componente de securizare a accesului la interfete web in mod centralizat. Avand in vedere rolul important al acestei componente se doreste implementarea unei solutii de tip „COTS",care sa satisfaca cel putin urmatoarele cerinte functionale:

- Sa protejeze resursele impotriva acceselor neautorizate – atât din interiorul cat si din exteriorul retelei
- Nici o resursa web din interiorul sistemului nu trebuie sa poată fi accesata direct din exterior, orice acces realizandu-se prin intermediul serverelor web proxy
- Sa integreze controlul accesului pentru componentele sistemului
- Sa ceara utilizatorilor sa introduca date de identificare pentru accesul la aplicatii
- Sa permită impunerea unor filtre de acces (operațiuni de autorizare) pe diverse criterii
- Sa permită administratorului sistemului sa poata alege metode de autentificare si autorizare diferite in functie de alocarea grupurilor
- Sa ofere o interfață de administrare de tip web pentru accesul facil la configurari, care sa poată fi accesata doar de către administratorii de securitate ai solutiei

- Sa ofere SSO – autentificare unica pentru accesul la resurse; pe parcursul unei singure sesiuni de lucru utilizatorul fi autentificat o singura data , dupa care va putea accesa fără reautentificare toate aplicatiile web pentru care are drept de acces.
- Fiecare utilizator sa fie identificat de sistem pe baza unei sesiuni
- Sistemul sa permită administratorilor terminarea manuala a sesiunilor utilizatorilor
- Dupa un timp configurabil de inactivitate sesiunile utilizatorilor trebuie sa fie terminate in mod automat
- Numarul de sesiuni pe care un utilizator le poate deschide trebuie sa poată fi limitat de către administratori
- Toate evenimentele de acces – autentificari reusite, autentificari nereusite, autorizari reusite, autorizari nereusite trebuie sa poată fi auditate
- Datele colectate prin auditarea accesului trebuie sa fie stocata într-o baza de date pe care sa poată fi rulate in caz de nevoie rapoarte
- Toate componentele software ale solutiei de control acces trebuie sa permită rularea in mod disponibilitate ridicata folosind functionalitati native

Din punct de vedere tehnic, componenta de control al accesului utilizatorilor va trebui sa asigure:

- Stocarea configuratiilor si a politicilor de acces la resursele web sa se realizeze într-o baza de date, fără a exista nevoia unui depozitar proprietar de date
- Sa permită accesarea simultana a mai multor surse de identitati pentru realizarea autentificarii si autorizarii
- Toate politicile de control al accesului trebuie sa poată fi definite utilizand interfață web a solutiei, fără a necesita cunostinte de programare sau rularea de scripturi pe server
- Sa suporte cel putin urmatoarele metode de autentificare:
    - Nume de utilizator si parola
    - Certificate digitale x.509
    - API-uri de autentificare pentru dezvoltari
- Schimbarea comportamentului standard (refuza acces sau permite acces pentru resursele neprotejate)
- Nivelul de auditare trebuie sa fie configurabil (succes, nereusita, etc)
- Sa realizeze criptarea informatiei transferata intre componentele sistemului si clienti

- Solutia de control acces sa ofere integrare cu solutia de stocare a profilelor de utilizatori si cu cea de administrare unitara

Securizarea accesului privilegiat pentru echipamentele de tip comunicatii si servere

- Solutia trebuie sa aiba posibilitatea de a oferi acces pe baza de roluri definite pentru a evita accesul neautorizat sau al unui utilizator cu rol diferit la serverele critice.
- Solutia trebuie sa permită integrarea cu un server LDAP extern unde sunt tinuti utilizatorii.
- Solutia trebuie sa ofere posibilitatea de a oferi accesul la resurse pe baza unui program de timp care sa poată fi definit.
- Solutia trebuie sa ofere posibilitatea de a reduce controlat si granular privilegiile conturilor de tip "superuser" pentru administratorii de aplicatii Microsoft si "root" pentru UNIX/Linux.
- Solutia trebuia sa permită definirea de politici de acces la resurse pe baza criteriilor multiple: interval orar, metoda de acces, metoda de logare, etc.
- Solutia trebuie sa permită definirea de politici de acces individualizate pentru sisteme, in functie de rolul acestora.
- Solutia trebuie sa ofere posibilitatea elimintarii conturilor administrative comune prin implementarea functionalitatilor de delegare a sarcinilor administrative, administratorii avand drepturi doar la componentele necesare indeplinirii sarcinilor.
- Solutia trebuie sa ofere politici predefinite care sa fie in conformitate cu bunele practici de securitate.
- Solutia trebuie sa permită definirea de politici pentru implementarea unei functionalitati de tip firewall in functie de porturi, adresa sursa, tipul conectarii precum si timp. Aceasta functionalitate trebuie oferita atât pentru conexiunile egress cat si pentru cele ingress.
- Solutia trebuie sa permită definirea de politici de securitate ce pot fi distribuite pe grupuri de servere, indiferent de domeniul din care acestea fac parte
- Solutia trebuie sa ofere posibilitatea administrarii si definirii de politici intr-un mod centralizat, indiferent de sistemul de operare care ruleaza pe sisteme.
- Solutia trebuie sa suporte definirea de roluri, astfel încât pe baza grupurilor din care face parte utilizatorul, sa i se permită accesul la diferite functionalitati.
- Solutia trebuie sa suporte criptarea datelor transmise prin retea si a datelor aplicatiei

- Solutia trebuie sa ofere functionalitati de administrare a parolelor conturilor partajate si privilegiate.
- Solutia trebuie sa permită definirea de politici pentru asigurarea calitatilor parolelor: compozitie, dimensiune, perioada in care se va schimba automat parola.
- Regulile de acces trebuie sa poată fi create si modificate de către administratorul solutiei.
- Solutia trebuie sa ofere posibilitatea integrarii cu aplicatii dezvoltate in-house in vederea schimbarii parolelor.
- Solutia trebuie sa ofere suport prin SDK in vederea dezvoltarii ulterioare de noi module sau functionalitati
- Solutia trebuie sa suporte cel putin protocolul RDP, SSH pentru loginul automat.

5.8.3. Componenta de administrare unitara a profilelor de utilizator

Datorita specificului datelor cu caracter personal gestionate in cadrul SIIEASC si asa cum este prezentat si in capitolele privind *Managementul utilizatorilor şi accesul la sistem* si *Confidențialitatea datelor,* in cadrul sistemului este solicitata o componenta care sa asigure managementul centralizat al drepturilor de acces ale utilizatorilor in sistem, componenta care are un rol esential in arhitectura de securitate si administrare a sistemului. Se doreste implementarea unei solutii de tip „COTS",care sa satisfaca cel putin urmatoarelor cerinte functionale si tehnice:

- Sa ofere o imagine unitara a conturilor de acces asociate unui utilizator
- In functie de specificul fiecarui angajat in parte si de regulile din sistem, acestuia ii vor fi alocate in mod automat resurse (conturi de acces in sisteme)
- Orice schimbare in profilele de utilizatori, care ar putea avea impact asupra drepturilor de acces la alte sisteme (de exemplu schimbarea pozitiei, departamentului, etc) trebuie sa se reflecte in schimbarea rolurilor asociate utilizatorilor repectivi in mod automat
- In cazul in care un angajat este mutat pe o alta pozitie in organizatie, care implica schimbarea drepturilor de acces, componenta de administrare utilizatori trebuie sa ii revoce drepturile de acces la sistemele la care acesta nu mai are drept de acces conform noii pozitii si sa ii acorde drepturile suplimentare necesare
- In cazul in care angajatul pleaca din organizatie componenta de administrare utilizatori va trebui sa revoce toate drepturile de acces pe care utilizatorul le are in alte sisteme, astfel încât sa se previna tentativele de acces neautorizat

- Cand un utilizator pleaca din organizatie sau accesul nu mai este necesar in urma schimbarii rolului, solutia trebuie sa permită revocarea acestuia , conform cu politicile institutionale
- Trebuie sa expună o interfață web către utilizatori (self-service) care sa permită vizualizarea si modificarea informatiilor din profilul propriu
- Trebuie sa expună o interfață web către administratori care sa permită vizualizarea si modificarea informatiilor din profilul propriu si profilele angajatilor administrati
- Interfata expusa către utilizatori si administratori trebuie sa permită doar nivelul de acces de care acestia au nevoie, fără a afisa meniuri sau functionaliati neutilizabile de către acestia conform pozitiei si rolului in organizatie
- Sistemul trebuie sa permită lansarea de cereri pentru alocare de roluri si resurse
- Sa permită definirea drepturilor de acces pe baza unor template-uri
- Utilizatorii trebuie sa poată urmarii stadiul cererilor proprii - in timp real, la orice moment, folosind interfață grafica web
- Pentru eficientizarea operatiunilor de resetare a parolelor, utilizatorii trebuie sa isi poată configura intrebari si raspunsuri cheie pentru resetarea parolelor de acces la resurse dintr-un punct unic (interfață web)
- Pentru evitarea blocajelor in operarea sistemelor (de exemplu pentru situatiile in care utilizatorii sunt temporar indisponibili), solutia trebuie sa permită administrarea delegata a drepturilor de acces
- Solutia trebuie sa ofere posibilitatea rularii periodice a unor rapoarte de utilizare (numar resetari parole intr-un interval de timp, utilizatori care au un anumit tip de cont de acces, conturi inactive)
- Sa pastreze istoricul rapoartelor rulate; pentru fiecare rulare sa ofere detalii pentru fiecare utilizator inclus in raport
- Monitorizarea periodica a modificarilor aparute in system si actualizarea drepturilor de acces conform cu noile date
- Monitorizarea conturilor orfane in sistem si executarea unor acțiuni corective automate care sa previna utilizarea frauduloasa a acestora

Integrarea cu alte sisteme

Integrarea cu sistemele externe trebuie sa se realizeze fără a impacta functionarea acestora. Pentru sistemele din administrarea Beneficiarului cu care se va integra sistemul de referinta, va fi asigurat intregul suport tehnic necesar de catre Ofertant.

Componentele de integrare aplicatii si colectare de date vor asigura indeplinirea cerintelor legate de integrarea cu diferitele aplicatii/sisteme nominalizate

Astfel, componentele tehnologice pentru integrarea/ interfatarea intre componentele functionale al sistemului SIIEASC si sistemele existente vor fi configurate pentru asigurarea in principal:

- suport complet pentru tot ciclul de viata al proceselor de integrare sisteme informatice: modelare, dezvoltare, testare, executie, optimizare, monitorizare si administrare;
- instrumente de transportare, rutare si transformare a mesajelor intre diferitele servicii si aplicatii care trebuie integrate;
- instrumentele necesare personalului non-tehnic pentru accesarea si modificarea prin intermediul unui browser web a regulilor de business;
- securizarea atat la nivelul canalelor si protocoalelor transport si comunicatie cat si la nivelul aplicatiilor si serviciilor prin asigurarea principalelor servicii de securitate cum ar fi autentificare, autorizare, criptare si non-repudiere;
- Extragerea si integrarea datelor din sisteme de tehnologii diferite.
- Trebuie sa permita auditarea si inregistrarea proceselor si serviciilor executate sau in curs de executie precum si a datelor transportate.
- Permita implementarea de reguli de verificare a datelor accesate astfel incat sa asigure consistenta si corectitudinea datelor finale
- Definirea de fluxuri de date compuse din activitati individuale de procesare a datelor care pot fi executate ordonat, secvential sau in paralel, permitand totodata reluarea activitatilor a caror executie nu s-a finalizat cu succes
- Să poată accesa si integra date din baze de date diferite: Oracle, Microsoft SQL Server, MySQL, IBM DB2, etc, şi să ofere suport pentru accesarea datelor aflate In fisiere (.txt, .csv, exml, etc)
- Să suporte modalităţi diferite de incărcare a datelor:
    - incărcare masivă de date (Bulk Load);
    - incărcare incrementală (Incremental Update);
    - incărcare a datelor captate printr-un mecanism de detectare a modificării datelor (Changed Data Capture);
- In cadrul mapărilor de date, să se permită definirea de filtre şi de restricţii asupra câmpurilor implicate

- Să ofere suport pentru web-services, atat pentru accesarea informatiei cat si pentru publicarea acestei, fara ca implementarea serviciilor web sa necesite scrierea de secvente de cod/programme
- Mediul de lucru să nu necesite cunoştinţe avansate de programare
- Să permită păstrarea istoricului diverselor versiuni ale mapărilor de date
- Trebuie sa ofere servicii de securitate specifice lucrului cu serviciile web standard:
    - autentificarea accesului la servicii;
    - autorizarea accesului la servicii.
- Să fie bazata pe standarde deschise de interoperabilitate a aplicaţiilor WS-I Basic Profile, WSDL, WS-*, XML, SOAP, UDDI.

Trebuie sa permita comunicatii sincrone si asincrone inter-aplicaţii.

5.8.4. Componenta stocare centralizata a profilelor de utilizatori - LDAP

Componenta de stocare a profilelor utilizatorilor, de tip director central LDAP, va fi apelata de toate modulele solutiei pentru preluarea datelor de autentificare la aplicatii. Se doreste implementarea unei solutii de tip „COTS" care sa indeplineasca urmatoarele cerinte tehnice si functionale:

Stocare centralizata profile utilizatori

- Stocarea utilizatorilor sa se realizeze in mod centralizat
- Sa permită accesarea datelor despre utilizatori atât din baze de date cat si din directoare LDAP, cu posibilitatea de agregare selectiva a profilelor si expunerea acestor informaţii in format LDAP către alte sisteme
- Sa asigure securitatea datelor private
- Pentru asigurarea unui nivel ridicat de acesibilitate, sa ofere o interfaţă grafica web pentru consultarea datelor despre utilizatori si operarea componentei
- Sa reprezinta sursa unica de profile de utilizatori pentru autentificarea in toate componentele functionale
- Directorul de utilizatori centralizat trebuie sa fie conform cu standardul LDAP v3 sau echivalent
- Componenta trebuie sa permită integrarea cu alte sisteme fără a utiliza agenti
- Sa permită protejarea datelor la acces – autentificare la interogarea directorului (nume utilizator si parola)

- Sa permită filtrarea accesului astfel încât fiecare utilizator sa poată citi doar datele de care are nevoie
- Filtrarea trebuie sa se poată realiza la nivel de atribut LDAP
- Sa permită criptarea parolei fiecarui utilizator in parte
- Sa permită integrarea cu celelalte componente ale sistemului general astfel încât sa existe o singura sursa de utilizatori pentru toate nivelele (aplicatie, baza de date, etc)
- Sa permita rularea pe sistemul de operare ofertat

5.8.5. Componenta de monitorizare a logurilor si a traficului de retea

Componenta de monitorizare a logurilor si traficului de retea va permite monitorizarea log-urilor de la componentele sistemului precum si a fluxurilor de comunicații prin preluarea traficului de la dispozitive de tip TAP. Acest modul va permite procesarea logurilor si a traficului de retea în timp real, prin probe dedicate, pentru extragerea, analiza şi detectarea eventualelor evenimente de securitate care pot afecta functionarea SIIEASC- detecţia rapidă a incidentelor de securitate, a utilizării incorecte a resurselor de reţea sau a performanţelor neoptimale.

Cerinte generale

- Solutia trebuie sa ofere capabilități de monitorizare real-time a device-urilor de securitate, switch-uri si routere de retea, Windows si Unix/Linux, servere de aplicatii, servere de baze de date si solutii de stocare
- Solutia trebuie sa identifice atacuri inclusiv in timpul colectarii datelor
- Pe toate segmentele de retea, solutia trebuie sa aiba posibilitatea de monitorizare permanenta si in timp real a traficului de date pentru detectarea anomaliilor si evenimentelor de securitate
- Solutia trebuie sa ofere posibilitatea colectarii de log-uri, iar arhitectura de stocare sa suporte stocarea datelor
- Solutia trebuie sa ofere monitorizarea traficului de reţea prin captura acestuia sau colectarea şi/sau generarea de metadate de tip flow
- Solutia trebuie sa ofere prin intermediul unei console centrale vizibilitate unificată asupra întregii infrastructuri de comunicaţii prin agregarea datelor primite pe baza traficului de retea si loguri de la diferite siteme, precum şi detecţia rapidă a

incidentelor de securitate, a utilizării incorecte a resurselor de reţea sau a performanţelor neoptimale

- Solutia trebuie sa ofere posibilitatea criptarii transmisiei datelor
- Solutia trebuie sa garanteze integritatea informatiilor colectate
- Solutia trebuie sa fie scalabila si sa acopere o gama larga de implementari, de la medii mici pana la medii distribuite. Solutia trebuie sa aiba optiunea de a adauga componente fără a fi nevoie de inlocuirea hardware-ului existent, a software-ului sau a licentelor
- Solutia trebuie sa fie dimensionata in acord cu sistemul dezvoltat plus o marje de 40% pentru scalabilitate ulterioara
- Solutia trebuie sa ofere posibilitatea instalarii in mediu virtual
- Solutia trebuie sa ofere licentele necesare atât pentru sistemele de operare, cat si pentru aplicatii terte, dupa caz.

Cerinte minime

- Solutia trebuie sa ofere o consola unica centralizata de administrare web pentru toate componentele
- Solutia trebuie sa colecteze datele in format brut cu performante ridicate de analiza in timp real
- Solutia trebuie sa ofere capabilităţi de alertare pentru regulile de corelare folosind cel putin: SMTP, SNMP si Syslog
- Solutia trebuie sa ofere posibilitatea de export si import a regulilor de corelare
- Solutia trebuie sa ofere o interfaţă pentru constructia de reguli pentru rapoarte, diagrame, alerte, corelari, suficient de flexibila si fără a fi nevoie de limbaje de script-ing
- Solutia trebuie sa ofere suport pentru descarcarea si instalarea actualizarilor aplicatiei direct din consola web sau din linia de comanda
- Solutia trebuie sa suporte ultimele versiuni pentru urmatoarele browsere web: Chrome, Microsoft Edge, si Mozilla Firefox
- Solutia trebuie sa ofere posibilitatea de a crea scripturi, filtre sau parsere personalizate pentru sursele de evenimente sau aplicatii ce nu sunt suportate nativ de aplicatie
- Solutia trebuie sa ofere functionalitati de auditare si log-uri ale sistemului
- Solutia trebuie sa permită detectarea atacurilor prin analiza traficului de reţea

- Solutia trebuie sa ofere conectivitate externa cu serviciile de cloud ale furnizorilor pentru descarcarea informatiilor aditionale: APT, definitii Botnet, retele malitioase, zero-day/compromitere, rapoarte suplimentare, parsere noi, reguli pentru rapoarte si diagrame etc
- Solutia trebuie sa permită detectarea atacurilor din interior prin stabilirea unui tip al comportamentului în reţea şi compararea în permanenţă a traficului observat în timp real cu tiparele observate în trecut precum si actualizarea permanenta a acestora
- Solutia trebuie sa permită introducerea în analiză a informaţiilor ce provin de la alte tipuri de tehnologii cum ar fi web-proxy, IDS/IPS, firewall sau NAC
- Solutia trebuie sa ofere capabilităţi DPI asupra traficului folosind soluţii de tip SPAN sau TAP
- Solutia trebuie sa permită generarea de rapoarte bazate pe trafic, servicii, protocoale, adrese IP, incidente de securitate sau utilizatori
- Solutia trebuie sa includa informaţii GeoIP in scopuri de investigatii
- Solutia trebuie sa ofere functionalitati de raportare. Rapoartele trebuie sa includa cel putin accesul bazat pe roluri: read&write, read only, no access
- Solutia trebuie sa suporte expresii regulate (RegEx) pentru crearea rapoartelor
- Solutia trebuie sa suporte o lista de variabile ce pot fi folosite la crearea rapoartelor
- Solutia trebuie sa ofere cel putin urmatoarele optiuni la afisarea rapartelor: tabular, area, bar, bubble, column, line, pie, step line, step area, spline area, spline
- Solutia trebuie sa permită adaugarea de informaţii aditionale rapoartelor: header, body text si comentariu
- Solutia trebuie sa ofere optiunea de a programa rularea rapoartelor: ad-hoc, ora de ora, zilnic, saptamanal, lunar
- Solutia trebuie sa ofere posibilitatea inestigatiei detaliate (drill-down) direct din raportul generat
- Solutia trebuie sa permită export-ul rapoartelor in cel putin urmatoarele formate: PDF si CSV
- Solutia trebuie sa ofere rapoarte, reguli si diagrame predefinite. Personalizarea rapoartelor, regulilor si diagramelor trebuie sa fie posibila
- Solutia trebuie sa ofere posibilitatea de a configura Identity Feed pentru a adauga domenii de tip Active Directory sau echivalent, statii si utilizatori pentru log-uri si sesiuni non-Windows, fără a fi nevoie de licente aditionale
- Solutia trebuie sa ofere posibilitatea de a exporta din interfaţă web log-urile colectate

- Solutia trebuie sa permită configurarea mesajului de login in aplicatie

Detectarea codului malitios (malware)

- Elemente ale acestei componente (agenți sau clienți în funcție de tehnologia aleasa) vor fi instalate pe toate sistemele livrate.
- Platforma de administrare centralizata pentru clientii/agentii instalati.
- Solutia trebuie sa ofere o componenta integrata de analiza malware, fără a fi nevoie de licente aditionale
- Permite identificarea atacurilor de tip APT, viruşi sau alte tipuri de malware specializat prin analiza traficului de reţea.
- Sa ofere capabilitati de integrare cu soluția de monitorizare şi traficului de retea
- Solutia trebuie sa ofere implicit cel putin urmatoarele tehnici de investigatie malware:
    a. analiza statica
    b. analiza in retea
    c. analiza sandbox

5.9. Backup date, sisteme si aplicatii

Avand in vedere importanta deosebita a SIIEASC este esentiala asigurarea unor instrumente si solutii de realizare a salvarii datelor, sistemelor si aplicatiilor, in acest sens furnizorul va trebui să realizeze implementarea unor strategii, proceduri si soluţii de backup care să se integreze atât cu echipamentul ofertat cât şi cu componentele functionale ale sistemului SIIEASC:

- Soluția trebuie sa includa posibilitatea replicarii datelor intr-o soluție similara, intr-o locație de protecție a datelor in caz de dezastru (site secundar).
- Soluția trebuie sa suporte replicare bidirecţionala şi de tip many-to-one.
- Soluția trebuie sa permita instalarea unui numar nelimitat de clienți de backup indiferent de tipul acestora – nivel de sistem de operare, aplicații sau clustere.
- Solutia trebuie sa identifice segmentele de date unice la nivelul tuturor agentilor de backup, pentru optimizarea traficului prin retea.
- Soluția trebuie să permită asistența pentru operațiile importante: instalare, creare activitati de backup / recovery, formatare medii de stocare, etc.
- Soluția trebuie să permită ștergerea automată a log-urilor şi cataloagelor vechi, cu posibilitatea de definire a perioadei de reținere pentru acestea
- Soluția trebuie să permită posibilitatea de restaurare a sistemului de operare şi a aplicațiilor deja instalate, inclusiv configurările existente

- Trebuie sa suporte toate configuratiile de stocare existente: DAS (Direct Attached Storage), NAS (Network Attached Storage), SAN (Storage Area Network)
- Din punct de vedere al fluxului de backup, pentru o optimizare a spatiului de stocare se va utiliza un mecanism de deduplicare sau compresie a datelor.
- Soluţia trebuie să permită utilizatorilor verificarea şi corectarea problemelor legate de securitate, disponibilitatea mediilor de stocare sau a conectărilor din reţea, înainte de a rula operaţiunile de backup
- Soluţia va oferi solutii software pentru protecţia continuă a datelor cu posibilităţi de salvare în sistem de salvari de siguranta precum şi o interfata de gestiune a back-up-ului.
- Soluţia de backup trebuie să asigure salvarea şi restaurarea datelor unice (nemodificate) cum sunt datele sistemului de operare, documentele şi alte date existente pe file servere, precum şi mediile virtuale.
- Se doreşte o soluţie de tip software care să asigure protecţia continuă a datelor şi care să restaureze datele corupte de viruşi, erori software sau erori umane prin capabilitatea de a relua datele de la un moment imediat anterior înainte de coruperea acestora.
- Solutia trebuie să ofere toate tipurile de backup: full, incremental şi diferenţial.
- Soluţia trebuie să permită integrarea cu sisteme de tip LDAP pentru autentificarea utilizatorilor.
- Solutia trebuie sa fie bazata pe un full backup initial, urmand ca backup-urile succesive sa transmita prin retea catre server doar segmentele unice de date modificate.
- Solutia trebuie sa foloseasca un format de scriere pe banda care sa permita refacerea datelor din catalogul intern al serverului de backup.
- Solutia trebuie sa ofere posibilitatea de a salva si restaura baze de date, sisteme de fisiere ale diferitelor sisteme de operare Unix, Linux, Windows;
- Solutia trebuiie sa fie flexibilă astfel încât să permită extinderi ulterioare in functie de dinamica dezvoltării SIIEASC.
- Solutia se va integra cu si va folosi solutia de stocare pe banda ofertata.

5.10. Monitorizare date, sisteme si aplicatii

Având în vedere complexitatea tehnică şi funcţională a sistemului informatic SIIEASC, precum şi importanţa acestuia, devine esenţială necesitatea implementării unei soluţii de

management de aplicații și infrastructură care să elimine discontinuitatea serviciilor oferite de IT către zona functionala, unificând în acest fel cele două componente.

Cerinte:

- Soluția trebuie să ofere o imagine globală a întregului sistem pentru a detecta proactiv, diagnostica și rezolva orice problemă de performanță și disponibilitate în ordinea priorității dictate de business.
- Soluția trebuie să ajute managerii IT și de aplicație să înțeleagă nivelurile acceptate ale serviciilor livrate către utilizatorii finali, pentru a asigura continuitatea sistemului în condiții optime.
- Sistemul trebuie să fie instalat şi implementat în nodul central. Soluţia ofertată va oferi o interfaţă grafică cu posibilitatea de a monitoriza disponibilitatea şi performanţa componentelor (timp mediu de răspuns între două componente, instantaneu şi istorie lunară, reprezentări grafice de instantanee, istoria de perturbări, processor, memorie şi degradare de performanţă).
- Sistemul va genera alerte clasificate în funcţie de gravitatea evenimentelor, cu privire la interfeţele, la aplicaţiile monitorizate; alertele se vor trimite destinatarilor desemnaţi prin email-uri de avertizare pentru evenimente critice.
- Trebuie sa ofere atat de interfete grafice web-based pentru administrare cat si de instrumente de tip linie de comanda.
- Colectarea informatiilor si evenimentelor trebuie sa se faca intr-o baza de date unica pentru analiza si raportare ulterioara;
- Platforma trebuie să permita administrarea, monitorizarea si auditul tuturor componentelor solutiei dintr-o singura interfata.
- Sa permita analiza in timp, pe baza de istoric, a performantelor sistemelor componente.
- Sa permita analiza performantelor in timp real.
- Platforma trebuie sa beneficieze de o interfata simpla, intuitiva in care subsistemele monitorizate sa fie grupate intr-o ierarhie arborescentă. In cadrul structurii arborescente administratorii trebuie sa poata selecta oricare dintre subsistemele solutiei pentru a vedea detaliile monitorizarii sau pentru a realiza operatii specifice de administrare.

- Informatiile de monitorizare trebuie sa fie prezentate atat sub forma tabelara cat si sub forma grafica, vizuala, folosind diagrame linie (line-chart), diagrame tip coloană (bar-chart), diagrame radiale (pie-chart), etc. in functie de optiunile administratorului.

- Sa permita definirea de alerte de functionare pentru fiecare dintre componentele sistemului care sa poata fi ulterior expediate utilizand diferite canale de comunicare cum ar fi mesaje de e-mail.

- Sa se poata configura astfel incat sa execute actiuni corective automate (fara a necesita interventia administratorilor) in cazul detectarii unei erori sau in cazul degradarii performantelor.

- Platforma trebuie sa permita gestionarea (vizualizarea si modificarea) porturilor utilizate de componentelor solutiei.

- Platforma trebuie sa permita configurarea setarilor de securitate (SSL, Keystores, certificate, metode de autentificare) ale componentelor solutiei.

- Platforma trebuie sa permita gestionarea fisierelor de jurnalizare (log files) si a informatiilor de diagnoza a solutiei. Fisierele de jurnalizare trebuie sa poata fi prezentate administratorilor sub formă tabelara in care acestia să aibă posibilitatea sa realizeze cautari, grupari după tipul mesajelor, grupari după data mesajelor, etc.

- Platforma trebuie să ofere instrumente pentru diagnoza problemelor si managementul incidentelor.

- Platforma trebuie sa permita configurarea capabilitatilor de back-up si recovery pentru componentele solutiei.

- Platforma trebuie sa permita configurarea capabilitatilor de scalare, inalta disponibilitate si a scripturilor de migrare intre diferite medii (test/dezvoltare, producţie) pentru componentele solutiei.

- Platforma trebuie sa ofere capacitatea de a consolida componentele sistemului SIIEASC tinand cont de constrangerile de natura tehnice si de business.

- Platforma trebuie sa ofere capacitatea de a realiza planuri de consolidare atat pentru resurse fizice cat si resurse virtuale pe scheme diferite de consolidare pe baza datelor istorice.

- Platforma trebuie sa permita integrarea cu un sistem centralizat de autentificare precum LDAP.
- Platforma trebuie sa ofere posibilitatea de a defini politici automate de oprire masini virtuale dupa o perioada de inactivitate.
- Portalul de tip self service trebuie sa permita configurarea acestuia cu elemente de design grafic specifice.
- Portalul de tip self-service trebuie sa ofere utilizatorilor finali informatii despre resursele utilizate (cpu, memorie,I/O, cota alocata, numar de request-uri la nivel de aplicatie).
- Trebuie sa ofere un depozit centralizat care sa cuprinda software, patch-uri si sa permita instalarea centralizata a acestora.
- Platforma trebuie să ofere posibilitatea de a vizualiza, inregistra, cauta, compara informatii de configurare.
- Platforma trebuie sa permita administrarea si monitorizarea cererilor de suport asociate incidentelor monitorizate.
- Platforma trebuie sa includa un mecanism integrat de inregistrare si urmarire a incidentelor aparute in infrastructura hardware si software.
- Sa permita crearea de panouri customizate, cu acces bazat pe roluri.
- Sa dispuna de un mecanism de alertare bazat pe reguli.
- Sa dispuna pentru fiecare tehnologie monitorizata de un set de reguli standard care sa poata fi customizate. De asemenea sa permita crearea de reguli noi.
- Sa dispuna de un mecanism avansat de notificare si de actiuni la aparitia unei alerte
- Sa ofere monitorizarea, controlul si diagnosticarea echipamentelor de retea, serverelor, sistemelor de operare si a altor echipamente de infrastructura IT. Solutia va trebui sa gestioneze infrastructura ca si suport pentru aplicatiile critice, din fiecare perspectiva, inclusiv vizualizarea nivelelor de servicii ale business-ului.

- Sa furnizeze grafice in timp real asupra proceselor cheie de sistem de operare, metrici si detalii ale metricilor de sistem destinate identificarii momentului de inceput al unei probleme si a ajuta la izolarea cauzei radacina:
- Capacitati grafice de diagnostic – vor putea fi vizualizate grafic, in timp real, procesele de baza pentru sistemele de operare, metrici si informatii derulante in metricii de sistem pentru a servi la identificarea momentului aparitiei unei probleme si a ajuta la izolarea cauzei de baza.
- Monitorizarea activitatii echipamentelor/device-urilor de stocare pe disc – informatii despre nivelul de utilizare, capacitate, severitate, despre discuri si sistemele de fisiere.
- Sa permita monitorizarea si urmarirea tranzactiilor de business peste toate nivelele aplicative (server de aplicatie, baze de date).
- Sa includa un modul integrat de testare functionala a serviciilor web si a tranzactiilor de business.
- Sa includa o componenta integrata pentru definirea,managementul si monitorizarea politicilor de securitate a serviciilor web.
- Sa permita colectarea si analiza configuratiilor componentelor software din platforma de integrare, permitand salvarea configuratiilor, compararea versiunilor de configuratie.
- Sa permita colectarea metricilor de rulare si a datelor de configurare a platformei de integrare intr-o sursa de date centrala permitand administratorilor sa analizeze datele stocate pentru a construi rapoarte si efectua analize.
- Sa permita auditarea fiecarei activitati de flux din platforma de integrare.
- Sa ofere capabilitati pentru managementul nivelului de servicii (SLA)

5.11Asistenta tehnica si instruire utilizatori

5.11.1 Asistenta tehnica (help desk)

Având in vedere numărul mare de utilizatori ai sistemului este necesara furnizarea și instalarea unei soluții de asistenta tehnica (help-desk) care sa limiteze cauzele și

efectele defectelor SIIEASC şi totodată să sigure monitorizarea SLA-ului stabilit. Sistemul va permite preluarea, înregistrarea si urmărirea sesizărilor (incidente/tickete) privind funcţionarea anormală a întregului sistem informatic. Sesizările vor putea fi preluate de către personalul IT specializat, prin telefon, e-mail, web sau alte canale de comunicare şi vor putea fi înregistrate în sistemul de Help-desk. Incidentele/ticketele se vor aloca personalului competent care comunica modalitatea de rezolvare a incidentului către solicitant. În perioada de suport şi garanţie sistemul va permite ca incidentele care nu pot fi gestionate de către personalul intern sa poată fi escaladate in exterior spre rezolvare de către implementator, in funcţie de tipul incidentului.

Sistemul va permite ca pe parcursul derulării activităţii de Help-Desk, specialiştii IT sa poată inregistra modalităţile de rezolvare pentru incidentele frecvent întâlnite sub forma de baza de cunoştinţe, astfel incat la reapariţia unui incident similar, modalitatea de rezolvare sa fie deja înregistrata in sistem.

Punerea la dispoziţie de către Furnizor a acestei soluţii presupune instalare, configurare şi asigurarea tuturor resurselor necesare operării (resurse umane, logistice etc.).

Este la latitudinea Furnizorului varianta utilizării unui spaţiu propriu sau a unuia închiriat, precum şi specificaţiile tehnice pentru infrastructura hardware/software şi de comunicaţii care va fi pusă la dispoziţie în perioada solicitată.

Autoritatea contractantă nu pune la dispoziţie spaţiu, hardware, echipamente de comunicaţii sau alte categorii de resurse, inclusiv personal, necesare implementării, operaţionalizării şi operării soluţiei de help-desk.

Sistemul va permite:

- micsorarea timpilor de nefunctionare a diverselor componente/sisteme;
- identificarea si corectarea punctelor vulnerabile ale sistemelor supervizate;
- creşterea vitezei de intervenţie a personalului IT;
- prioritizarea corecta a activităţii de rezolvare a incidentelor;
- urmărirea timpilor de intervenţie din partea furnizorilor si a modului in care aceştia isi respecta contractele de service si suport.

Soluţia de help-desk oferita va realiza gestionarea tuturor cerinţelor de service si suport ale organizatiei. Aceasta soluţie va asigura administrarea problemelor apărute in cadrul

organizaţiei, escaladarea si transferul acestora, managementul alertelor si va oferi opţiuni de căutare si raportare.

Cerinţe Generale:

- Solutia propusa trebuie sa se bazeze pe un pachet de aplicatii software care sa ofere functionalitati si procese specifice pentru managementul si administrarea incidentelor/ticketelor si a relatiilor cu solicitantii.
- Solutia propusa trebuie sa se bazeze pe un pachet de aplicatii software disponibile comercial (COTS –Commercial of the Shelf).
- Solutia trebuie sa fie conforma cu practicile ITIL v3 si sa acopere minim urmatoarele procese ITIL: Request Management, Incident Management, Problem Management
- Solutia trebuie sa contina functionalitati proprii de securitate si audit.
- Solutia trebuie sa aiba definite implicit rolurile de baza din ITIL pentru scurtarea perioadei de implementare si sa permita definirea unor alte roluri in functie de necesitati.
- Utilizatorii sa aiba posibilitatea sa isi aleaga din interfata aplicatiei rolul in care activeaza in solutie fara a fi nevoie sa iasa si sa reintre in sistem (conform ITIL, o persoana poate indeplini mai multe roluri). Rolurile pe care o anumita persoana poate sa le indeplineasca trebuie sa fie definibile doar de administratorul solutiei.
- Functionalitatile solutiei trebuie sa fie adaptate rolurilor pe care utilizatorii le indeplinesc, schimbarea rolului sa duca la schimbarea tipului de interfeta in care activeaza.
- Solutia trebuie sa dispune de mecanisme de securizare a accesului utilizatorilor la datele din aplicatie prin definirea de roluri cu nivele de acces diferite. Solutia trebuie sa permita definirea unui numar nelimitat de roluri in aplicatie. Solutia trebuie sa perminta atasarea unuia sau mai multor roluri pentru un utilizator.
- Soluţia trebuie să poată funcţiona pe oricare dintre platformele software următoare: Windows, UNIX şi distribuţii majore Linux.
- Soluţia trebuie să poata utiliza sisteme de gestiune a bazelor de date
- Accesul la aplicaţie trebuie sa se realizeze în intregime prin intermediul unei interfete WEB, accesibilă printr-un browser modern. Nu se admit soluţii tip client-server.

- Soluţia trebuie să suporte reguli de business flexibile care pot varia conform unor factori multipli.
- Soluţia va oferi suport complet pentru orchestrarea de procese (workflow).
- Solutia propusa trebuie sa permita integrarea folosind servicii si adaptori in conformitate cu standardele deschise.

Cerinte specifice

Aplicaţia trebuie sa fie accesibila prin interfaţa web securizata;

Sa dispună de mecanisme predefinite pentru implementarea functionalitatilor de Incident management, Problem management, Change management;

Sa fie uşor de exploatat astfel incat sa fie minimizata posibilitatea de apariţie a erorilor umane. Astfel:

- Trebuie sa asigure o interfaţa prietenoasa utilizatorului, facilitaţi de navigare confortabila utilizând mijloace naturale de căutare (meniuri bara, pop-up pull-down) si sa permită navigarea in toate modulele la care utilizatorul are acces fara deconectarea si reconectarea utilizatorului;
- Sa permită introducerea incidentelor/ticketelor de către utilizatori prin interfaţa web de către operatorul serviciului de asistenta;
- Sa permită ataşarea la incidentul introdus a documentelor electronice (de diverse formate);
- Sa permită configurarea unor fluxuri de operaţiuni pentru rezolvarea incidentelor/ticketelor in funcţie de tipologia acestora.
- Sa poată fi configurata astfel incat sa escaladeze automat incidentele/ticketele in funcţie de prioritatea lor sau in situaţia in care acestea nu respecta condiţiile de calitate (timpul maxim admisibil pentru rezolvare);
- Sa permită monitorizarea timpilor de rezolvare;
- Solutia trebuie sa permita identificarea la nivelul interfetei aplicatiei a solicitarilor pentru care nivelul de SLA (Service Level Agreement) definit a fost incalcat.
- Solutia trebuie sa permita configurarea de reguli automate de escaladare a cererilor si de notificare pentru a se asigura incadrarea in nivelul de SLA definit.
- Solutia trebuie sa permita afisarea la nivelul fiecareri solicitari a mometului in care SLA-ul agreat pentru rezolvarea acelei solicitari va fi depasit.

- Solutia trebuie sa permita oprirea contorului de timp la schimbarea status-ului in care se afla solicitarea (Hold).
- In definriea SLA-urilor timpul de rezolvare trebuie sa fie calculat tinand cont de un program de lucru care se poate defini (workshift).
- In cazul incidentelor trebuie sa permita definirea unei matrici flexibile de calcul a Prioritatii incidentelor in functie de nivelul de Urgenta si Impact conform specificatiilor ITIL.
- Solutia trebuie sa permita inregistrarea de relatii de tip Parinte-Copil intre incidente sau Probleme. De asemenea trebuie sa permita propagarea automata catre solicitarile copil a rezolutiei sau a altor informatii completate in solicitarea parinte.
- Solutia trebuie sa ofere posibilitatea deschiderea unei Probleme dintr-un Incident si relationarea Problemei cu unul sau mai multe Incidente.Analiştii sa poată salva soluţiile propuse intr-o baza de cunoştinţe cu arborescenta pe subiecte, puncte de interes etc;
- Baza de cunoştinţe trebuie sa dispună de facilitati de căutare după cele mai frecvente întrebări si Sa ofere metoda de căutare a informaţiei de tip „arbore de decizie" in baza de cunoştinţe;
- Baza de cunoştinţe sa permită definirea de drepturi diferite de acces la documentele publicate in funcţie de grupul de utilizatori;
- Trebuie sa permita introducerea de feedback-uri din partea utilizatorilor, pentru evaluarea si notarea calitatii raspunsurilor primite in urma interogarilor efectuate.
- La deschiderea unei solicitari de catre utilizatori trebuie sa se poata face mai intai o cautare in baza de cunostinte a unor posibile solutii astfel incat sa se reduca numarul de solicitari pentru care s-a dat deja o rezolvare.
- Toate activitatile de cautarile efectuate de utilizatori trebuie sa poata fie inregistrate si disponibile pentru analiza si determinarea graduli de utilitate al documentelor publicate.
- Solutia trebuie sa dispuna de raporate detaliate despre gradul de accesare al documentelor publicate precum si alti parametri
- Un solicitant trebuie sa poatea avea multiple incidente/tickete deschise simultan.
- Solutia propusa trebuie sa ofere suport complet integrat pentru toate canalele de contact, e-mail, portal web.
- Solutia propusa trebuie sa ofere capabilitati de a alocare a incidentelor/ticketelor bazata pe capabilitatile angajatilor.

- Solutia propusa trebuie sa permita inregistrarea si regasirea istoriei complete de comunicare (mesaje receptionate si emise) a solicitantului, de pe toate canalele de interactiune si zonele de cereri, informari si servicii.
- Solutia propuse trebuie sa ofere capabilitati de parsing pentru email-urile inbound pentru diverse campuri cum ar fi expeditorul, corpul e-mailului, in scopul procesarii acestora.
- Trebuie oferita posibilitatea utilizarii de sabloane pentru raspunsurile la emailuri.
- Solutia trebuie sa puna la dispozitie un instrument vizual care sa permita modificarea interfetei si a paginilor prezentate utilizatorilor, extinderea functionalitatilor si a fluxurilor de lucru, extinderea schemei bazei de date
- Solutia trebuie sa aiba incluse capabilitati de suport remote si capabilitati de self-service;
- Solutia trebuie sa dispuna de un instrument care sa permita analistilor sa se conecteze la distanta pe statia utilizatorilor, fara a necesita instalarea unor agenti pe acea statie, sa poata rula scripturi de reparare sau sa poata extrage date relevante despre starea sistemului (procese care ruleaza, loguri, servicii). Toate aceste activitati realizate de catre analist pentru rezolvarea problemei sa fie inregistrare si sa se salveze in logurile solicitarii.
- Solutia trebuie sa aiba un modul de "live chat" care sa permita un dialog direct intre utilizator si analist iar conversatia dintre acestia sa fie automat salvata ca si istoric al solicitarii
- Functionalitati de Raportare. Solutia trebuie sa aiba un modul dedicat de raportare care sa includa un set predefinit de raporte dar sa permita si dezvoltarea de rapoarte noi.
- Solutia trebuie sa permita rularea rapoartelor in functie de cerintele utilizatorilor si in contextul de lucru al fiecarui analist.
- Solutia trebuie sa pemita programarea rularii de rapoarte si expedierea acestora pe email.
- Solutia trebuie sa pemita exportul de rapoarte in format EXCEL si PDF.
- Modulul de raportare trebuie sa fie integrat nativ cu solutia de Helpdesk permitand autentificarea o singura data a utilizatorilor in aplicatie fara a mai cere o autentificare suplimentara atunci cand aceseaza un raport.
- Regulile de securitate aplicate asupra datelor din aplicatia Helpdesk trebuie sa se aplice automat si asupra rapoartelor.

5.11.2 Instruire utilizatori

Pentru desfăşurarea în bune condiţii a activităţii necesare utilizării sistemului este foarte important ca personalul care va opera sistemul să fie instruit corespunzător. Furnizorul trebuie să organizeze sesiuni de instruire şi să realizeze activităţi de instruire a personalului ce va utiliza noul sistem în vederea familiarizării corespunzătoare cu elementele de noutate ale aplicaţiei şi cu modul de operare a acesteia.

Sistemul va fi operat si gestionat de catre urmatoarele categorii de utilizatori, avand cel putin rolurile mentionate mai jos:

- Administrator sistem. Utilizatori ce au acces la informatiile de tip administrativ ale sistemului. Au rolul de a gestiona utilizatorii sistemului, gestiona buna functionare a fluxurilor, de a emite rapoarte etc.
- Ofiteri stare civila. Aceasta categorie de utilizator aproba diversele fluxuri initiate de catre operatorii aflati in cadrul institutiilor partenere si emit documentele cu privire la starea civila
- Operatori date. Aceasta categorie de utilizator este responsabila de initierea fluxurilor, pe baza drepturilor alocate acestora. Operatorii au acces numai la fluxurile care depind de acestia (spitale, norariate publice, etc.)

Se solicita servicii de instruire pe următoarele categorii:

- Administratori infrastructura hardware – cursuri specifice infrastructurii hardware si produselor ofertate.
    - cursul va avea o durată de minim 10 zile lucratoare (8 ore /zi)
    - cursul va fi dimensionat pentru 16 utilizatori
    - cursul va fi susţinut în limba română.
    - curicula va acoperi toate aspectele necesare utilizării în bune condiţii a sistemului.
- Administratori infrastructura software – cursuri specifice infrastructurii software ofertata.
    - cursul va avea o durată de minim 10 zile lucratoare (8 ore /zi)
    - cursul va fi dimensionat pentru 16 utilizatori
    - cursul va fi susţinut în limba română.

- curicula va acoperi toate aspectele necesare utilizării în bune condiţii a sistemului.

- Administratori solutie software specifică implementată– cursuri specifice aplicațieisoftware integrate oferite.
    - cursul va avea o durată de minim 5 zile (8 ore /zi)
    - cursul va fi dimensionat pentru 14 utilizatori
    - cursul va fi susţinut în limba română.
    - curicula va acoperi toate aspectele necesare utilizării în bune condiţii a sistemului.
- Administratori securitate sistem:
    - cursul va avea o durată de minim 5 zile (8 ore /zi)
    - cursul va fi dimensionat pentru 16 utilizatori
    - cursul va fi susţinut în limba română.
    - curicula va acoperi toate aspectele de securitate cibernetica a sistemului informatic
    - după încheierea cursului participanţii vor beneficia de un stagiu de pregătire aplicat în centrul de tip SOC în care se vor realiza activitățile descrise la capitolul Servicii dedicate asigurarii securitatii cibernetice a sistemului informatic. Stagiul de pregătire va avea o durată minimă de 5 zile, va fi realizat împreună cu instructorul cursului şi va fi de tipul hands-on.
- Administratori componenta de comunicații:
    - cursul va avea o durată de minim 10 zile lucrătoare (8 ore/zi)
    - cursul va fi dimensionat pentru 16 utilizatori
    - Instruirea trebuie să ofere participanţilor cunoştinţe relevante pentru echipamentele de tip firewall, router şi switch ofertate în cadrul contractului
    - Se vor pune la dispoziţia cursanţilor laboratoare în care vor exersa comenzi de administrare/configurare pentru aceste echipamente.
- Administratori componenta de comunicații colaborativă
    - cursul va avea o durată de minim 15 zile lucrătoare (8 ore/zi)
    - cursul va fi dimensionat pentru 5 utilizatori
    - cursul va fi susținut în limba română

- Instruirea trebuie să ofere participanților cunoștințe relevante pentru echipamentele ofertate pentru soluția de comunicații VoIP colaborativă, pentru instalarea, configurarea, customizarea, utilizarea și administrarea echipamentelor / soluției, conform recomandarilor de instruire ale producătorului acestora
- Se vor pune la dispoziția cursanților laboratoare în care vor exersa comenzi de administrare/configurare pentru aceste echipamente.

Instruirea administratorilor de sistem va acoperi toate componentele acestuia și cel puțin următoarelor teme de instruire:

- configurarea și administrarea sistemului SIIEASC;
- administrarea utilizatorilor sistemului SIIEASC;
- crearea și configurarea fluxurilor de lucru in cadrul sistemului SIIEASC
- crearea și administrarea formularelor utilizate de SIIEASC
- modalități de instalare și configurare a software-ului de baze de date și de aplicație;
- proceduri de administrare tipice pentru toate componentele instalate/configurate (ex: administrare soluție de backup, gestionare diferite tipuri de pagini portal, creare și administrare formulare, creare configurare fluxuri etc.);
- modalități de depistare si corectare a erorilor;

Se vor asigura instructori certificați de catre producatori pe produsele sau tehnologiile pentru care se face instruirea (produs/tehnologie ofertata).

Pentru fiecare curs de instruire a personalului tehnic, materialul (curricula cursului) trebuie sa respecte programa oficiala a producatorului pentru produsul/tehnologia ofertata si sa reflecte customizarile de aplicatie efectuate de furnizor asupra solutiei.

- Ofiteri stare civila – cursuri specifice solutiei integrate oferite.
  - cursul va avea o durată de minim 2 zile (8 ore /zi)
  - cursul va fi dimensionat pentru 140 utilizatori in regim train the trainers
  - cursurile vor avea maxim 20 persoane /curs
  - cursul va fi susţinut în limba română.

  Curicula va acoperi cel putin urmatoarele teme de instruire:
  - Prezentarea generală a soluției;
  - Prezentarea funcționalităților, modulelor/componentelor de sistem, interfețelor specifice SIIEASC;
  - Prezentarea fluxurilor implementate în sistem;
  - Exerciții practice privind utilizarea tuturor componentelor din sistem.

Se vor stabili:

a. etapele în desfășurarea proiectului în care vor avea loc activități de instruire;
b. strategia de instruire;
c. nivelul de cunoștințe al celor care vor susține ședințele de instruire conform cerințelor minime privind experiența profesională;
d. metodologia de instruire;

Se elaborează tematica și materialele sesiunilor de instruire. Perioadele de desfășurare a sesiunilor de instruire se vor stabili premergător etapei de testare și operaționalizării sistemului. Se vor asigura mediul informatic de instruire și toate resursele necesare desfășurării serviciilor de instruire.

Furnizorul va asigura toate resursele necesare desfăşurarii serviciilor de instruire, va elabora şi susţine cursurile si va tipări materiale de curs pentru toţi participanţii. De asemenea toate materialele sesiunilor de instruire vor fi livrate şi în format electronic;

Cazarea si transportul participanţilor la cursul de instruire vor fi puse la dispozitie de furnizor.

5.12 Solutia de virtualizare

Asa cum s-a solicitat si la descrierea dimensionarii sistemului, o data cu serverele furnizate va trebui livrata si o solutie de virtualizare pentru virtualizarea resurselor acestor servere. Soluția de virtualizare va trebui să fie certificata atât de producatorii serverelor cât și de producatorii produselor software care se vor instala pe masinile virtuale create cu aceasta solutie. În acest sens, serverele ofertate și produsele software trebuie sa suporte oficial soluția de virtualizare propusa.

Din punct de vedere tehnic şi funcţional, soluția de virtualizare va fi implementata atât în site-ul principal cât și în site-ul secundar și va fi capabila să asigure:

- o componentă informatică care să permită rularea unor aplicaţii de gestiune a datelor din sistemul SIIEASC într-un mediu virtual, care să ofere disponibilitate, securitate, scalabilitate şi portabilitate.
- soluţia de virtualizare va permite interconectarea maşinilor virtuale şi aplicaţiilor găzduite/dezvoltate pe acestea, cu echipamentele hardware şi aplicaţiile software livrate in cadrul proiectului.
- asigurarea unui înalt nivel de performanţă, disponibilitate, scalabilitate şi securitate pentru toate aplicaţiile şi informaţiile gestionate în mediul virtual, astfel încât să fie îndeplinite condiţiile necesare continuării acţiunilor pe linia prelucrării, actualizării şi schimbului de date.

Implementarea soluţiei de virtualizare are în vedere următoarele beneficii:

- Să reducă costurile hardware şi de operare, costurile de energie şi costurile totale de mentenanţă;
- Să asigure securitate, scalabilitate, portabilitate şi timp minim de răspuns;
- Să permită gestionarea (administrarea, furnizarea de informaţii etc.) optimă a informaţiilor aferente sistemului SIIEASC;
- Să asigure disponibilitate permanentă a serviciilor şi datelor;
- Sa asigure redundanta serverelor
- Să asigure o eficienţă ridicată de utilizare a resurselor şi să asigure un management performant al utilizării acestor resurse.
- Sa asigure optimizarea si eficientizarea administrarii serverelor.

6. Servicii de dezvoltare și implementare proiect

6.1 Serviciile de livrare, instalare si punere în funcțiune echipamente hardware și infrastructura software (central) site principal și site secundar

Pentru livrarea şi implementarea infrastructurii hardware si software solicitate vor trebui asigurate următoarele activităţi:

- livrarea echipamentelor şi infrastructurii software necesare funcţionării soluţiei informatice – nodul central (site principal şi site secundar) se va realiza la sediul DEPABD (site principal), respectiv DACTI (site secundar)
- livrarea documentaţiei tehnice a echipamentelor recepţionate
- instalare, configurare echipamente hardware
- instalare şi configurare infrastructura software
- livrarea documentaţiei tehnice infrastructurii software
- integrarea componentelor şi operaţionalizarea infrastructurii instalate
- elaborarea documentaţiei de testare infrastructură
- testarea echipamentelor furnizate şi a infrastructurii software instalate pe baza documentaţiei realizate
- recepţia echipamentelor şi infrastructurii software

În vederea pregătirii instalării, se va realiza inspecţia site-urilor şi se va documenta modalitatea de instalare.

Pentru asigurarea livrării cu succes a infrastructurii software a sistemului, trebuie să fie instalată infrastructura hardware corespunzătoare şi apoi finalizată arhitectura fizică a sistemului. Pentru fiecare mediu în parte vor trebui să fie instalate, conform arhitecturii, produsele furnizate, în modul de disponibilitate solicitat.

6.2 Serviciile de dezvoltare SIIEASC

Pentru asigurarea dezvoltării sistemului SIIEASC vor trebui asigurate cel puţin următoarele categorii mari de activităţi:

- ***Servicii de analiză a sistemului***

În cadrul acestei etape se va evalua situaţia existentă (domenii de activitate, modul de organizare a arhivei fizice şi modelul privind modelarea activităţilor de arhivare, atribuţii privind gestionarea actelor de stare civilă, structura organizatorică - relaţiile dintre acestea, diagrama de relaţii structurată pe tipuri de relaţii-ierarhice, funcţionale, coordonare, reprezentare, baza legală aferentă etc.), a categoriilor de informaţii specifice proiectului (categorii de date, nomenclatoare, fluxurile informaţionale şi procedurile legale pentru acoperirea necesarului informaţional), analiza sarcinilor şi cerinţelor utilizatorilor, analiza capacităţii de interconectare a aplicaţiilor/sistemelor existente implicate şi analiza constrângerilor de securitate.

Etapa de analiză detaliată a sistemului are ca obiective:

- Analiză detaliată a cerinţelor operaţionale
- Alinierea cerinţelor operaţionale cu specificaţiile tehnice
- Analiza fluxurilor informaţionale şi modelarea lor în vederea implementării fluxurilor tehnice
- Analiza proceselor tehnice şi de management a actelor de stare civilă
- Optimizare fluxuri pentru creşterea performanţei sistemului şi a procesului de gestionare a actelor de stare civilă

Livrabile:

- plan detaliat pentru implementarea sistemului;
- raport detaliat de analiză (identificare şi optimizare fluxuri de lucru, surse de date, nomenclatoare, cerinţe de configurare şi integrare etc.);

- ***Servicii de proiectare a sistemului***

Etapa de proiectare de detaliu a sistemului informatic are următorul obiectiv: pe baza cerinţelor documentate în cadrul Raportului de Analiză produs în cadrul etapei anterioare se rafinează cerinţele funcţionale identificate, se elaborează un set de specificaţii de proiectare care să stea la baza construcţiei noului sistem. Se vor proiecta procesele ce vor face obiectul implementării ţinând cont, pe de o parte de documentaţia de analiză şi pe de altă parte de specificul aplicaţiilor şi celorlalte subsisteme furnizate. În cadrul acestei etape se va realiza: proiectarea arhitecturii subsistemului software, proiectarea modelului de date, proiectarea interfeţelor grafice, proiectarea interfeţelor cu sistemele informatice existente, proiectarea

noilor procese de lucru pentru utilizarea sistemului informatic.

- Proiectarea modelului sistemului de date;
- Definirea serviciilor aferente noului flux funcţional de sistem;
- Definirea principalele funcţionalităţi de sistem;
- Proiectarea componentelor şi arhitectura de sistem.

Livrabile:

Proiectul tehnic de detaliu al sistemului informatic.

- ***Servicii de dezvoltarea şi configurarea componentelor de software:***

Având ca referință documentele de proiectare se dezvoltă/configurează și asamblează componentele software într-un sistem integrat, conform cu specificațiile de proiectare. În această etapă se va realiza: configurarea/dezvoltarea funcţionalităţilor deja existente în aplicaţiile ofertate astfel încât să răspundă cerințelor tehnice și funcționale specifice structurilor beneficiare, dezvoltarea funcţionalităţilor suplimentare, integrarea componentelor software, personalizarea interfeţelor grafice, dezvoltarea/configurarea interfeţelor de integrare cu alte sisteme şi programelor de incarcare date în vederea iniţializării sistemului.

De asemenea, se vor implementa fluxurile electronice de lucru prin derularea următoarelor activităţi:

a. se vor defini metadatele generale ale fluxurilor electronice;
b. se vor defini seturi de activităţi şi condiţii specifice proceselor şi metadatelor asociate;
c. se vor configura seturile de decizii cu opțiune pentru semnătura digitală;

Se finalizează procesul iterativ de rafinare a componentelor dezvoltate/configurate pentru satisfacerea cerințelor funcționale, integrarea și documentarea tuturor componentelor soluției, instalarea aplicației informatice integrate și integrarea în sistem a arhivei digitale.

Activităţile de instalare şi configurare a sistemului se vor derula la sediul Beneficiarului, facându-se astfel şi transferul de cunoştinte către specialiştii IT ai Beneficiarului.

- Servicii implementare call center
    - Implementarea soluției de help-desk
    - Consolidarea informaţiilor referitoare la elementele ce compun infrastructura IT într-o bază de date comună – CMDB
    - Înregistrarea modalităţilor de rezolvare pentru incidentele frecvent întâlnite sub formăde bază de cunoştinţe
    - Realizarea de proceduri de lucru pentru operarea sistemului help-desk

Livrabile:

- Soluția dezvoltată/configurată;

- Codul sursă documentat.

6.3 Testarea și asigurarea calității sistemului SIIEASC

Este necesar ca Furnizorul să planifice în detaliu, să pregătească şi să efectueze o serie de teste care să confirme că sunt asigurate cerinţele funcţionale şi nonfuncţionale ale sistemului, cerinţele reţelei de comunicaţii a sistemului, compatibilitatea sistemului cu specificaţiile de interfaţare ale sistemului cu sistemele externe.

6.3.1 Testarea

Pentru nodul central, beneficiarul se va asigura că Furnizorul a efectuat cu succes următoarele activități, cu rezultatele lor respective:

- toate componentele software de bază şi hardware-ul necesar au fost livrate corespunzător şi instalate;
- toate elementele de nodul central sunt pe deplin funcționale;
- aplicația SIIEASC a fost livrată şi instalată;
- sesiunile de instruire au fost livrate/efectuate;
- toate documentele necesare, manuale, CD-uri de instalare şi licenţele legate de acest proiect au fost livrate;
- interconectarea nucleului central cu sediile locale pentru verificarea funcionalitatilor platformei informatice pe nivele de acces

În cadrul acestei etape se va realiza testarea calității componentelor de sistem şi corectarea oricăror probleme sau disfuncționalități posibile. Activităţile desfăşurate presupun verificarea sistemului informatic dezvoltat, conform specificaţiilor rezultate şi agreate. Se vor realiza toate testele atât pe sistemul integrat cât şi pe fiecare componentă a acestuia, în conformitate cu **Documentația de testare** (metodologie de testare, plan de testare, scenarii de testare, raport de testare).

Testarea se va realiza utilizând scenariile de testare agreate în prealabil şi are ca scop validarea modalităţii corecte de implementare a funcționalităților solicitate şi proiectate.

Etapa de testare va include obligatoriu verificarea tuturor rapoartelor identificate/detaliate în etapa de analiza.

Testarea se va realiza în mai multe etape, după cum urmează:

- Testare funcțională;
- Testare de performanţă;
- Testare de stres (număr utilizatori concurenți, timp de răspuns, volum de date).

Procesul de testare de performanţă va avea la baza un flux de lucru, proceduri, strategie

de testare, modele pentru planul de test şi cazuri de test, tipuri de rapoarte dorite şi indicatori de performanţă.

Testele trebuie să acopere şi cerinţele de disponibilitate, scalabilitate, fiabilitate, robustețe, salvare şi restaurare, recuperare în caz de sezastru, estimări capacitate şi planificare, performanta, managementul configuraţiilor, extensibilitate/flexibilitate, siguranţă în funcţionare (reliability), securitate, managementul şi monitorizarea sistemului, managementul căderilor în sistem, operarea, conectivitatea şi calitatea serviciilor.

Livrabile:

- Metodologia de testare: va descrie modul în care se abordează testarea sistemului, obiectul activităţilor de testare, activităţile, mediile de testare, livrabilele, rolurile şi responsabilităţile pentru testare, procedurile de testare şi metoda de raportare.
- Planul de testare: conţine organizarea activităţilor şi resurselor necesare pregătirii şi efectuării nivelurilor de testare
- Specificaţii de testare: trebuie să conţină cel puţin cazurile de test, descrierea datelor de test (cu referire la datele de intrare şi la baza de date pe care se executa testele), scenariile de testare care vor acoperi cerinţele funcţionale (referitoare la operaţionalizarea cu succes a modulelor sistemului) şi non-funcţionale (disponibilitate infrastructura, salvare/restaurare, testare de performanta etc.).
- Raport de testare: trebuie să conţină rezultatele testelor efectuate conform planului de testare, precum şi concluzii şi recomandări

Beneficiarul va examina şi aproba planurile de testare propuse de Furnizor.

Planurile de testare trebuie să urmeze o metodologie standard în domeniu.

Planurile de testare trebuie să includă cel putin urmatoarele teste:

- teste funcţionale
- teste de arhitectură, teste non-funcţionale (cum ar fi LDAP, PKI)
- teste de conexiune
- teste de conectivitate şi interoperabilitate
- testele de conectare şi utilizare pentru site-urile locale
- teste de raportare statistice
- teste de securitate a reţelei
- teste de backup şi restaurare

Planurile de testare trebuie să includă cel puţin următoarele elemente:

- descrierea componentei de sistem testat
- obiectivele de testare
- descrierea mediului de testare
- rezultatele aşteptate ale testului
- test de abordare

- datele de test
- descrierea procedurilor de test
- cazuri de testare
- instrumente folosite de testare
- persoanele responsabile
- cerințe de intrare / ieşire

Platforma de testare

O bază de date de test cu simularea unei conexiuni la reţea va trebui să fie creată pentru testele funcţionale / de conectare cu baza de date. Un simulator de încărcare trebuie să fie pregătit pentru a testa procedurile în condiţii de maximă incărcare.

Soluție pentru generarea și managementul datelor de testare a sistemului

Testarea sistemului reprezintă un proces absolut necesar, nu doar înainte de lansarea în producţie, în scopul identificării şi remedierii erorilor, ci şi în timpul utilizării acestuia, înainte de utilizarea in producţie a oricăror noi funcţionalităţi, îmbunătăţiri ale celor existente sau patch-uri pentru remedierea unor erori detectate în timpul funcţionării sistemului.

Reglementările europene cu privire la protecţia datelor cu caracter personal (General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) impun reguli foarte stricte cu privire la gestionarea, de către instituţii şi companii, a datelor cu caracter personal – astfel încât instituţiile trebuie să cunoască în detaliu modul în care utilizează datele unei persoane, atât în sistemele de producţie, cât şi în sistemele de test sau dezvoltare.

Având în vedere necesitatea unor date de test de calitate pentru testarea eficientăşi relevantă a sistemului, se va utiliza o soluţie pentru generarea şi managementul datelor de testare.

Soluţia trebuie să îndeplinească următoarele caracteristici tehnice minime:

- Soluţia trebuie să dispună de capacitatea de profilare a datelor existente pentru descoperirea automată a modelului de date, a relaţiilor, a tendinţelor, a acoperirii şi a conţinutului sensibil
- Abilitatea de a edita modele şi relaţii de date
- Capacitatea de a crea sau de a genera noi date referenţial intacte în conformitate cu normele specifice de business. Regulile să poată fi importate dintr-o structură de bază de date dintr-un fişier existent sau definite de către utilizatori
- Soluţia trebuie să asigure generarea de date deschise(opendata) configurate de Beneficiar, în conformitate cu următoarele formate:
    - Baze de date

- Fișierele XML, HTML CSV, TXT, Excel

- Odată ce modelul de date a fost definit, soluția trebuie să permită să repete procesul de generare a datelor, în scopul de a recrea datele pentru testele repetate sau pentru a crea volume mari de date menținând în același timp integritatea logică și de business a datelor.
- Soluția trebuie să ofere posibilitatea utilizatorului să specifice legături între tabele, acolo unde acestea nu sunt deja definite în structura bazei de date
- Soluția trebuie să permită administratorilor crearea de sarcini administrative pe bază de proiect și versiuni ale proiectelor. Sarcinile să poată fi utilizate/selectate de către utilizatori în cadrul portalului de self-service.
- Soluția trebuie să fie capabilă să inlocuiască date sensibile, date de identificare personală, cu un conținut realist alternativ. O astfel de capacitate trebui să includă funcții cum ar fi:
    - Numărul & Data varianță - algoritmi de varianță pentru date si numere
    - Format de conservare - datele produse trebuie să aibă aceeași structură ca și datele originale.
    - Conservarea tipului de date - datele obținute trebuie să păstreze tipul de date al datelor originale
- Soluția trebui să ofere posibilitatea de a genera subseturi de date de la medii la mari foarte rapid
- Abilitatea de a înregistra, optimiza și cerințele de testare asociate cu datele de testare și cazuri de testare/căi care permit o acoperire maximă funcțională
- Soluția trebuie să ofere capacitatea de a identifica datele sensibile în baza de date și de a le marca în consecință pentru a permite utilizatorilor / administratorilor administrarea acestora
- Soluția trebui să fie capabilă de a reproduce modificările efectuate în baza de date sursă la baza de date țintă
- Soluția trebuie să poată păstra datele sincronizate și coerente în diferite baze de date
- Soluția trebuie să aibă capacitatea de a verifica dacă datele create sunt consistente, pentru a putea asigura că toate legăturile sunt valabile
- Soluția trebuie să dispună de posibilitatea modificării datelor generate
- Soluția trebuie să fie capabilă de a cuprinde tipuri de date complexe, cum ar fi codurile concatenate, checksum

- Soluția trebuie să permită o mascare a datelor
- Aplicația trebuie să ofere posibilitatea păstrării integrității datelor când se realizează procesul de mascare a datelor, indiferent dacă integritatea este definită la nivel fizic în baza de date sau la nivel logic
- Soluția trebuie să fie, de asemenea, capabilă să genereze date invalide, necesare pentru teste specifice
- Soluția trebuie să ofere posibilitatea apelări la algoritmi multipli pentru generarea datelor, astfel încât să poată genera date din unul sau mai multe câmpuri definite
- Soluția trebuie să fie scalabilă atât pe orizontală cât și pe verticală
- Soluția trebuie să dispună de capacitatea de a controla utilizarea funcțiilor și a accesului la date bazate pe utilizatori, roluri (acces bazat pe roluri) și grupuri (acces pe bază de grup)
- Soluția trebuie să dispună de rapoarte care pot pune în evidență datele vulnerabile, care trebuie mascate suplimentar.

Instrumente de testare

Furnizorul trebuie să precizeze toate instrumentele de testare (aplicații, scripturi etc.), destinate a fi utilizate în timpul procedurilor de testare. Furnizorul trebuie să furnizeze instrumentele de testare. Toate rezultatele testelor trebuie înregistrate și furnizate Beneficiarului după fiecare test.

Toate componentele HW / SW necesare testării vor fi descrise de furnizor și vor fi disponibile pentru toată perioada contractului (inclusiv pentru actualizări/testare, modificări). Același mediu de testare se va utiliza pentru a testa toate modificările cerute și/sau derivate din modificările legislative, pe perioada implementării contractului.

Punerea în aplicare a testarii

Toate testele se vor efectua de către Furnizor sub supravegherea Beneficiarului. Pentru cazurile de testare care necesită resurse externe sau acces la sisteme, Beneficiarul va asigura accesul la aceste resurse. Furnizorul va oferi toate instrumentele de testare, în cazul utilizării instrumentelor automate pentru testele de acceptanță.

Coordonarea testelor

Testele vor fi coordonate de către Beneficiar/Utilizatori, care vor revizui și aproba planul și specificațiile de testare înainte de execuția efectivă a testelor, vor controla că mediul de

testare e conform cu cerinţele, vor monitoriza efectuarea testelor şi se vor asigura de aplicarea procedurilor de management ale testării.

6.3.2 Asigurarea Calităţii

- Furnizorul trebuie să prezinte un plan pentru Asigurarea Calităţii, acceptabil pentru Beneficiar, ca parte a planului de proiect;
- Furnizorul trebuie să aloce timp suficient, în cadrul planului de proiect, pentru verificare şi validare în termeni de calitate, pentru serviciile prestate în cadrul contractului şi pentru livrabilele / documentele / rapoartele rezultate;
- Furnizorul va elabora procedurile standard de operare pentru toate aplicaţiile şi hardware-ul SIIEASC, cu instrucţiuni detaliate pentru a ajuta angajaţii în procesele de lucru diferite;

  Furnizorul va pune la dispoziţie manuale, documentaţii, proceduri complete privind concepţia, implementarea, testarea, instalarea, configurarea, administrarea şi utilizarea în integralitate a sistemului informatic. De asemenea Furnizorul va pune la dispoziţia Beneficiarului codul sursă documentat şi toate script-urile aferente soluţiei software SIIEASC dezvoltate/customizate. Codul sursa va fi pus la dispoziţia Beneficiarului imediat după etapa de testare funcţională, respectiv după acceptul acestuia de operaţionalizare. Codul sursă va fi furnizat cu titlu gratuit şi va fi însoţit de cedarea drepturilor de autor şi de proprietate intelectuală. De asemenea se va oferi codul sursa rezultat in urma modificarilor efectuate asupra sistemului in perioada de suport si garantie.

  Toate drepturile patrimoniale de autor asupra codului sursa dezvoltat se transferă către Beneficiar, conform art. 12 din OUG 41/2016.
- Furnizorul va oferi suport echipei de proiect a Beneficiarului pentru elaborarea tuturor documentelor necesare managementului implementarii proiectului (de exemplu: rapoarte de progres, cereri de rambursare etc. fara a se limita la acestea), conform prevederilor Ghidului solicitantului si Instructiunile aferente Programului operational Competitivitate.
- Toate documentele elaborate de Furnizor pe perioada de derulare a contractului vor fi redactate în limba română şi vor fi transmise atât în format electronic editabil cât şi pe suport hârtie.

6.4 Etape de realizare a sitemului informatic

Etapele de realizare ale sistemului informatic integrat sunt:

- **Etapa I**. (perioadă estimată maximă de implementare: 12 luni de la data intrării în vigoare a contractului)

  I.1 dezvoltarea aplicației care cuprinde următoarele activități:

  - analiza detaliată
  - proiectarea soluției informatice
  - servicii de livrare, instalare și punere în funcțiune echipamente hardware și infrastructura software aferente mediului de dezvoltare și testare
  - dezvoltarea/customizarea soluției informatice
  - testarea primei versiuni functionale a aplicației

  I.2. Amenajarea site-ului principal și site-ului secundar.

- **Etapa II**. (perioadă estimată maximă de implementare: 13 luni de la data recepției finale a Etapei I.), care cuprinde următoarele activități:
  - livrarea, instalarea și punerea în funcțiune echipamentelor hardware și infrastructurii software aferente mediului de producție - site principal și site secundar
  - instruirea administratorilor de sistem și trainerilor pentru utilizatorii finali
  - testarea integrală a soluției software și operaționalizarea sistemului IT

NOTĂ:

După fiecare etapă de mai sus, va avea loc o recepție la finalizarea etapei a serviciilor, lucrărilor după caz și bunurilor livrate în cadrul acesteia.

*Recepția la finalizarea **Etapei I** se va realiza după finalizarea primei etape mai sus definite, respectiv parcurgerea analizei de detaliu, proiectării, dezvoltării/customizării, testării primei versiuni funcționale a aplicației, inclusiv livrarea și instalarea platformei de dezvoltare și testare și executarea lucrărilor aferente amenajării celor 2 locații..*

Începerea Etapei II. mai sus definite, respectiv parcurgerea activităților de livrare, instalare și punere în funcțiune echipamente hardware și infrastructura software (aferente mediului de producție) - site principal și site secundar, instruire administratori de sistem și traineri pentru utilizatori finali, testarea integrală a soluției software și operaționalizarea sistemului IT, este condiționată de recepția fără obiecțiuni a Etapei I.

După finalizarea și recepționarea la finalizare, fără obiecții, a celor 2 etape de realizare, va avea loc Acceptanța finală a Sistemului, care atestă îndeplinirea tuturor obligațiilor cu privire la derularea contractului de către Furnizor. Acceptanța finală a Sistemului se consideră încheiată numai după semnarea fără obiecțiuni de către reprezentanții Achizitorului și cei ai Furnizorului a Procesului verbal de acceptanță finală a Sistemului

Plata produselor livrate/serviciilor prestate/lucrărilor executate se va realiza astfel:
- după semnarea Procesului verbal de recepție la finalizarea Etapei I, se vor plăti produsele livrate/serviciilor prestate/lucrărilor executate în cadrul acestei etape, ***dar nu mai mult de 25% din valoarea totală a contractului****. În cazul în care valoarea produsele livrate/serviciilor prestate/lucrărilor executate în cadrul acestei etape depășește* ***25% din valoarea totală a contractului,*** *diferența se va plăti după recepția la finalizarea Etapei II.*
- după semnarea Procesului verbal de recepție la finalizarea Etapei II, se vor plăti produsele livrate/serviciilor prestate/lucrărilor executate până la concurența valorii totale a contractului

6.5 Abordarea și metodologia proiectului

6.5.1 Riscuri și măsuri de gestionare a acestora

Principalele riscuri care pot să apară în derularea contractului identificate la nivelul autorității contractante și măsurile de gestionare aferente sunt următoarele:

- ***Nerespectarea condițiilor contractuale de către furnizori***

Întârzierile cauzate de furnizori vor fi evitate printr-o atentă și severă monitorizare a derulării contractelor și luarea imediată de măsuri în cazul apariției unor modificări de orice natură.

Măsuri de atenuare/gestionare ale riscului:

- prevederea unor clauze contractuale care să permită penalizarea furnizorilor, în cazul în care se încalcă condițiile contractuale;
- planificarea activitaților folosind marje de timp de siguranță, astfel încât să se poată apela la alt furnizor, fără o depășire a termenului de realizare;
- monitorizarea atentă a derulării activităților, verificându-se atât încadrarea în termenele stabilite, cât și verificarea respectarii întocmai a cerințelor contractuale.

- ***Deficiențe în comunicarea cu furnizorii***

În cazul în care vor exista deficiențe în relația cu furnizorii, se vor putea utiliza documentele utilizate în acest scop, astfel încât sa poată fi identificată clar cauza deficiențelor și să se poată remedia în cel mai scurt timp pentru a nu produce întârzieri. Managerul de proiect va monitoriza relația cu furnizorul astfel încât să se evite deficiențele în comunicare.

Măsuri de atenuare/gestionare ale riscului:

- stabilirea unei strategii de comunicare corespunzatoare în relația cu furnizorii;
- asigurarea trasabilitaăii interacțiunii cu furnizorii impact mediu

➢ ***Contractarea serviciilor cu întârziere din cauza procesului de derulare a procedurilor de achiziție publica***

Măsuri de atenuare/ gestionare ale riscului:

- organizarea procesului de derulare a achizițiilor publice pentru toate serviciile/bunurile ce urmeaza a fi contractate înca din prima luna de implementare a proiectului;
- elaborarea documentațiilor de atribuire într-un mod corect pentru evitarea respingerii de catre ANAP;
- organizarea comisiei de evaluare a ofertelor prin desemnarea unor persoane competente;
- publicarea proiectului de contract ce urmeaza a fi încheiat odata cu documentația de atribuire pentru evitarea unor întârzieri datorate unui eventual proces de negociere între parțile semnatare.

Furnizorul va identifica riscurile care pot să apară în perioada de implementare a contractului și va propune măsuri de prevenire/gestionare ale acestora.

6.5.2 Cerințe privind modalitatea de prezentare a propunerii tehnice

În vederea demonstrării unei abordări și a unei metodologii corespunzătoare pentru realizarea activităților și obținerea rezultatelor în cadrul proiectului, candidatul/ofertantul trebuie să facă dovada înțelegerii relației dintre obiectivele ce trebuie atinse și rezultatele ce urmează a fi obținute în contextul descris în prezentul document descriptiv.

Astfel, pentru a asigura uniformitate, acesta va trebui să propună o abordare și o metodologie - descrisă într-un capitol separat în propunerea tehnică - pentru realizarea activităților prezentate în detaliu care să se bazeze în mare măsură pe o metodologie sau serie de metodologii, metode și/sau instrumente testate, deschise și recunoscute la nivel internațional.

Metodologia trebuie să includă şi modalităţi de îmbunătăţire a rezultatelor şi/sau a activităţilor şi să utilizeze cele mai noi tehnici, instrumente sau metode recunoscute în domeniu.

În vederea optimizării utilizării resurselor, ofertantul trebuie să prezinte un **plan de implementare a proiectului,** care să conţină informaţii referitoare la durata, succesiunea logică şi cronologică a activităţilor, identificarea punctelor de reper (milestone-uri) pentru realizarea activităţilor în cadrul proiectului prin raportare la metodologia prezentată.

Toate activităţile principale vor fi incluse în calendarul activităţilor şi vor fi detaliate în subactivităţi, menţionându-se totodată resursele utilizate pentru realizarea acestora.

Corelarea logică şi cronologică a activităţilor în planul de implementare va fi foarte bine stabilită prin raportare la metodologia propusă. Durata activităţilor şi perioadele de derulare a acestora vor fi în totalitate corespunzătoare complexităţii activităţilor (modalitate de realizare, date de intrare, date de ieşire).

Propunerea tehnică va conţine, fără a se limita la acestea, descrierea următoarelor elemente:

- Metodologia de implementare a proiectului şi managementul proiectului la nivelul Furnizorului
- Arhitectura sistemului propus (software, hardware, funcţională)
- Descrierea soluţiei informatice propuse
- Descrierea tuturor componentelor soluţiei software (aplicaţii şi platforme/produse tehnologice)
- Descrierea tuturor componentelor hardware ce vor fi livrate, instalate, configurate
- Descrierea componentei de securitate cibernetică
- Descrierea serviciilor/lucrărilor de amenajare a celor două site-uri
- Descrierea componentei de comunicaţii
- Descrierea modului în care vor fi asigurate serviciile aferente dezvoltării şi implementării soluţiei
- Descrierea modului în care se va asigura implementarea (descrierea etapelor de implementare)
- Descrierea serviciilor de asistenţă tehnică
- Descrierea serviciilor de instruire
- Descrierea modului în care vor fi asigurate serviciile de garanţie şi suport, inclusiv asistenţă şi suport tehnic la darea în producţie
- Descriere SLA

Propunerea tehnică trebuie să cuprindă răspunsul la toate cerinţele din documentul descriptiv.

Totodată, candidații selectați vor prezenta o matrice de conformitate, care va conține cel puțin următoarele informații:

Nr. crt.	Cerințele din documentul descriptiv	Descrierea modalității de îndeplinire a cerințelor de către candidat	Referințe, observații, alte informații pe care candidat relevante
1.			
...			

7. Experți

Având în vedere faptul că, unul dintre criteriile de evaluare a ofertelor tehnice ce vor fi depuse în cadrul procedurilor de achiziții publice va fi CV-ul experților cheie, experții propuși de ofertantul ce va fi declarat câștigător nu vor putea fi schimbați pe întreaga perioadă a derulării contractului, decât în situații excepționale și în baza unui accept din partea Beneficiarului.

Profilele experților vor fi definite în documentațiile de atribuire, având în vedere complexitatea proiectului, iar echipa/echipele furnizorului/furnizorilor va/vor fi alcătuită/e din cel puțin următoarele categorii de experți cheie:

- **Arhitecți de soluție**

  - Experiența generală: Cel puțin 3 ani în domeniul IT. Experiența va rezulta din următoarele documente: fișa de post, contract de muncă, recomandare, CV sau orice alte documente similare din care rezultă informațiile solicitate.

  - Experiența specifică: Experiența ca expert cheie în realizarea a minim 1 proiect similar în calitate de arhitect de soluție (prin proiect similar se înțelege implementarea unui sistem informatic integrat multimodular pentru care s-a asigurat interoperabilitatea cu alte sisteme informatice

  - Certificare profesională în domeniul arhitecturilor de soluții complexe (TOGAF sau echivalent)

  - Certificare profesională privind managementul serviciilor IT (Information Technology Infrastructure Library – ITIL sau echivalent)

- **Experți tehnici**
  - **Specialiști soluție de securitate**

- **Experienţa generală**: Cel putin 3 ani in domeniul IT. Experienta va rezulta din urmatoarele documente: fişa de post, contract de muncă, recomandare, CV sau orice alte documente similare din care rezultă informaţiile solicitate.

- **Experienţa specifică:** Experienţa ca expert cheie în realizarea a minim 1 proiect similar în calitate de specialist securitate (prin proiect similar se înţelege implementarea unui sistem informatic integrat multimodular pentru care s-a asigurat interoperabilitatea cu alte sisteme informatice

- Studii post-universitare în domeniul securităţii sistemelor informatice

- Cunoaşterea unei metodologii recunoscute naţional/internaţional de auditare, control şi evaluare a securităţii sistemelor informatice (certificare Certified Information Systems Auditor – CISA sau echivalent)

  - **Analişti de business**

- **Experienţa generală**: Cel putin 3 ani in domeniul IT. Experienţa va rezulta din următoarele documente: fişa de post, contract de muncă, recomandare, CV sau orice alte documente similare din care rezultă informaţiile solicitate.

- **Experienţa specifică:** Experienţa ca expert cheie în realizarea a minim 1 proiect similar în calitate de analist de business (prin proiect similar se intelege implementarea unui sistem informatic integrat multimodular pentru care s-a asigurat interoperabilitatea cu alte sisteme informatice)

- Certificat de absolvire a unui curs de specialitate în domeniul analizei de business – curs recunoscut de instituţii/asociaţii recunoscute la nivel naţional sau internaţional

- Certificat de absolvire a unui curs de specialitate în domeniul modelării, analizei şi optimizării proceselor de business - curs recunoscut de instituţii naţionale/internaţionale

- **Experţi software- pentru:**

  - **Portal**

- **Experienţa generală**: Cel putin 3 ani in domeniul IT. Experienţa va rezulta din următoarele documente: fişa de post, contract de muncă, recomandare, CV sau orice alte documente similare din care rezultă informaţiile solicitate.

- **Experienţa specifică:** Participare ca expert cheie pe soluţia de portal la implementarea unui proiect similar (prin proiect similar se înţelege implementarea unui sistem informatic integrat multimodular pentru care s-a implementat soluţia de portal ofertată).

- Certificare profesională atestată /recunoscută național/ internațional de un producător de tehnologie pentru soluția de portal ofertată

- **Platforma de aplicații**

- **Experiența generală**: Cel puțin 3 ani în domeniul IT. Experiența va rezulta din următoarele documente: fișa de post, contract de muncă, recomandare, CV sau orice alte documente similare din care rezultă informațiile solicitate.
- **Experiența specifică:** Participare ca expert cheie pe platforma de aplicații la implementarea unui proiect similar (prin proiect similar se înțelege implementarea unui sistem informatic integrat multimodular pentru care s-a implementat platforma de aplicații ofertată).
- Certificare profesională atestată /recunoscută național/ internațional de un producător de tehnologie pentru platforma de aplicații ofertată

- **Managementul fluxurilor și proceselor de lucru**

- **Experiența generală**: Cel puțin 3 ani în domeniul IT. Experiența va rezulta din următoarele documente: fișa de post, contract de muncă, recomandare, CV sau orice alte documente similare din care rezultă informațiile solicitate.
- **Experiența specifică:** Participare ca expert cheie pe soluția ofertată, aferentă managementului fluxurilor și proceselor de lucru la implementarea unui proiect similar (prin proiect similar se înțelege implementarea unui sistem informatic integrat multimodular pentru care s-a implementat soluția ofertată, aferentă managementului fluxurilor și proceselor de lucru).
- Certificare profesională atestată /recunoscută național/ internațional de un producător de tehnologie pentru soluția ofertată, aferentă managementului fluxurilor și proceselor de lucru

- **Analiza si Raportare**

- **Experiența generală**: Cel puțin 3 ani în domeniul IT. Experiența va rezulta din următoarele documente: fișa de post, contract de muncă, recomandare, CV sau orice alte documente similare din care rezultă informațiile solicitate.
- **Experiența specifică:** Participare ca expert cheie pentru soluția de analiză și raportare implementată într-un proiect similar (prin proiect similar se înțelege implementarea unui sistem informatic integrat multimodular pentru care s-a implementat soluția de analiză și raportare ofertată).

- Certificare profesională atestată /recunoscută național/ internațional de un producător de tehnologie pentru soluția de analiză și raportare ofertată

- **Componentele de securitate**

- **Experiența generală**: Cel puțin 3 ani în domeniul IT. Experiența va rezulta din următoarele documente: fișa de post, contract de muncă, recomandare, CV sau orice alte documente similare din care rezultă informațiile solicitate.
- **Experiența specifică:** Participare ca expert securitate la implementarea unui proiect similar (prin proiect similar se înțelege implementarea unui sistem informatic integrat multimodular pe componentele de securitate pentru soluția ofertată)
- Certificare profesională atestată /recunoscută național/ internațional de un producător de tehnologie care să demonstreze specializarea pe componentele de securitate pentru soluția ofertată

- **Sistem de gestiune a Bazelor de Date**

- **Experiența generală**: Cel puțin 3 ani în domeniul IT. Experiența va rezulta din următoarele documente: fișa de post, contract de muncă, recomandare, CV sau orice alte documente similare din care rezultă informațiile solicitate.
- **Experiența specifică:** Participare ca expert cheie pe baze de date la implementarea unui proiect similar (prin proiect similar se înțelege implementarea unui sistem informatic integrat multimodular pentru care s-a implementat tehnologia SGBD ofertată)
- Certificare profesională atestată /recunoscută național/ internațional de un producător de tehnologie care să demonstreze specializarea în domeniul software-lui administrării bazelor de date pentru soluția ofertată

- **Backup date, sisteme și aplicații**

- **Experiența generală**: Cel puțin 3 ani în domeniul IT. Experiența va rezulta din următoarele documente: fișa de post, contract de muncă, recomandare, CV sau orice alte documente similare din care rezultă informațiile solicitate.
- **Experiența specifică:** Participare ca expert cheie pentru soluția de backup la implementarea unui proiect similar (prin proiect similar se înțelege implementarea unui sistem informatic integrat multimodular pentru care s-a implementat soluția de backup ofertată)
- Certificare profesională atestată /recunoscută național/ internațional de un producător de tehnologie pentru soluția de backup ofertată

- **Monitorizare date, sisteme şi aplicaţii**

- Experienţa generală: Cel puţin 3 ani în domeniul IT. Experienţa va rezulta din următoarele documente: fişa de post, contract de muncă, recomandare, CV sau orice alte documente similare din care rezultă informaţiile solicitate.

- Experienţa specifică: Participare ca expert cheie pentru soluţia monitorizare la implementarea unui proiect similar (prin proiect similar se înţelege implementarea unui sistem informatic integrat multimodular pentru care s-a implementat soluţia de monitorizare date sisteme şi aplicaţii ofertată)

- Certificare profesională atestată /recunoscută naţional/ internaţional de un producător de tehnologie pentru soluţia de monitorizare date sisteme şi aplicaţii ofertată

- **Soluţia de asistenţă tehnică**

- Experienţa generală: Cel puţin 3 ani în domeniul IT. Experienţa va rezulta din următoarele documente: fişa de post, contract de muncă, recomandare, CV sau orice alte documente similare din care rezultă informaţiile solicitate.

- Experienţa specifică: Participare ca expert cheie pentru soluţia de asistenţă tehnică la implementarea unui proiect similar (prin proiect similar se înţelege implementarea unui sistem informatic integrat multimodular pentru care s-a implementat soluţia de asistenţă tehnică ofertată)

- Certificare profesională atestată /recunoscută naţional/ internaţional de un producător de tehnologie pentru soluţia de asistenţă tehnică ofertată

- **Soluţia de virtualizare**

- Experienţa generală: Cel puţin 3 ani în domeniul IT. Experienţa va rezulta din următoarele documente: fişa de post, contract de muncă, recomandare, CV sau orice alte documente similare din care rezultă informaţiile solicitate.

- Experienţa specifică: Participare ca expert cheie pentru soluţia de virtualizare la implementarea unui proiect similar (prin proiect similar se înţelege implementarea unui sistem informatic integrat multimodular pentru care s-a implementat soluţia de virtualizare ofertată)

- Certificare profesională atestată /recunoscută naţional/ internaţional de un producător de tehnologie pentru soluţia de virtualizare ofertată

- **Experţi hardware**

- **Experienţa generală**: Cel puţin 3 ani în domeniul IT. Experienţa va rezulta din următoarele documente: fişa de post, contract de muncă, recomandare, CV sau orice alte documente similare din care rezultă informaţiile solicitate.

- **Experienţa specifică:** Participare ca expert cheie pentru componenta hardware la implementarea unui proiect similar (prin proiect similar se înţelege implementarea unui sistem informatic integrat multimodular pentru care s-a instalat, configurat infrastructura hardware).

- Certificare profesională atestată /recunoscută naţional/ internaţional de un producător pentru componenta hardware ofertată

- **<u>Formatori/Instructori</u>**

- Participarea ca expert cheie cu rol de coordonator instruire la cel puţin 1 proiect similar (prin proiect similar se înţelege implementarea unui sistem informatic integrat multimodular pentru care s-au asigurat servicii de instruire)

- Certificare de Formator emisă de instituţii recunoscute, ex. CNFPA sau echivalent

- **<u>Testeri pentru asigurarea testării sistemului informatic la cerinţele proiectului</u>**

- **Experienţa generală**: Cel puţin 3 ani în domeniul IT. Experienţa va rezulta din următoarele documente: fişa de post, contract de muncă, recomandare, CV sau orice alte documente similare din care rezultă informaţiile solicitate.

- **Experienţa specifică:** Participarea ca expert cheie cu rol de coordonator testare la cel puţin 1 proiect similar (prin proiect similar se înţelege implementarea unui sistem informatic integrat multimodular pentru care s-a asigurat interoperabilitatea cu alte sisteme informatice).

- Certificare profesională în domeniul testării aplicaţiilor informatice/sistemelor software (ISTQB Certified Tester sau echivalent)

- **<u>Expert calitate</u>**

- **Experienţa generală**: Cel puţin 3 ani în domeniul IT. Experienţa va rezulta din următoarele documente: fişa de post, contract de muncă, recomandare, CV sau orice alte documente similare din care rezultă informaţiile solicitate.

- **Experienţa specifică:** Participarea ca expert cheie în calitate de responsabil calitate la cel puţin 1 proiect similar (prin proiect similar se înţelege implementarea unui sistem

informatic integrat multimodular pentru care s-a asigurat interoperabilitatea cu alte sisteme informatice).

- Certificare ca auditor pentru sisteme de managementul calității ISO 9001 sau echivalent
- Certificare ca auditor pentru sistem de management al securității informatiei conform cu ISO 27001 sau echivalent

- **Expert stare civilă**

- Experiență acumulată în activitatea profesională în domeniul stării civile de cel puțin 3 ani, demonstrată prin adeverință/scrisoare de recomandare/similar de la instituția unde și-a desfășurat activitatea în acest domeniu.

- **Manager proiect**

- **Experiența specifică:** Participarea ca manager proiect în cel puțin 1 proiect similar (prin proiect similar se înțelege implementarea unui sistem informatic integrat multimodular pentru care s-a asigurat interoperabilitatea cu alte sisteme informatice).
- Certificare ca manager proiect recunoscută la nivel național/internațional

NOTĂ:

- *Expertul cheie are rol de coordonator pentru ceilalti experți*
- *Proiectul similar prezentat ca cerință de experiență la nivelul fiecarui expert cheie, se întelege a fi un proiect finalizat și recepționat de către Beneficiar, fără obiecții.*
- *În cazul în care experţii propuşi nu sunt vorbitori de limba română, furnizorul va asigura traducerea şi interpretarea de specialitate, în limba română pe toată durata contractului.*

8. Garanție și suport

În cadrul perioadei de garanție se vor asigura:

- majorarea perioadei de garanție cu timpul de nefuncționare a echipamentelor sau produselor software instalate, respectiv soluției software dezvoltate.
- în urma remedierii, reinstalarea și reconfigurarea echipamentelor se va face la sediul/sediile beneficiarului.
- rezolvarea bug-urilor care nu au fost identificate în timpul implementării/testarii și care apar în faza de producție;

- întreținerea și buna funcționare a sistemului furnizat în parametrii agreați (funcțional, performanță, disponibilitate, integritatea datelor etc.);
- instalarea/configurarea de noi versiuni ale aplicațiilor în urma efectuării corecțiilor;
- actualizarea manualelor de utilizare, administrare și altor documente în urma efectuării corecțiilor;
- remedierea oricarei neconcordante a produselor (solutiei) software fata de cerintele enuntate in documentația de atribuire adaugate in perioada de analiza/proiectare a sistemului sau descoperite in exploatarea curenta in faza de productie.
- transferului de cunoștințe de la furnizor către echipa Beneficiarului cu privire la actualizările aduse soluției și la activitățile de administrare și monitorizare aferente soluției SIIEASC.
- accesul la ultima versiune a produselor ofertate, pentru produsele software COTS livrate și va pune la dispozitie toate *patch*-urile care duc la fixarea unor probleme.
- aplicarea pe toata durata garantiei produselor, tuturor *patch*-urilor care duc la fixarea unor probleme sau facilitati de care utilizatorul are nevoie. Aceasta operatie se face de comun acord cu beneficiarul, fara a afecta stabilitatea/functionalitatea sistemului.
- serviciile de instalare si configurare a componentelor de sistem vor fi asigurate de furnizor prin personal certificat/autorizat.
- materialele necesare pentru desfășurarea activităților de intervenție, fără costuri suplimentare din partea beneficiarului;
- toate incidentele vor fi gestionate prin intermediul aplicației software de gestionare a tichetelor.

De asemenea, în perioada de garantie, Furnizorul va notifica si va pune la dispozitia Beneficiarului toate upgrade-urile aparute pentru solutia livrata in vederea functionarii acesteia in conformitate cu specificatiile tehnice ale compontelor de sistem.

Dacă în perioada desfășurării achiziției/implementării proiectului apar echipamente/produse software ca și end-of-life/end-of-sale/end-of-support ofertantul trebuie să le înlocuiască cu produse care să asigure minim funcționalitățile și performanța produselor ofertate inițial.

Garanția pentru Sistemul informatic central (hardware, software, amenajare site principal și site secundar, servicii de instalare hardware/software, servicii de dezvoltare software, instruire), inclusiv pentru fiecare componentă în parte, este de minim 36 luni de la data acceptanței finale a Sistemului. Acceptanța finală a Sistemului este considerată încheiată după semnarea, fără obiecțiuni, de către reprezentanții Achizitorului și cei ai Furnizorului a Procesului verbal de Acceptanță finală a Sistemului.

Indiferent de defectul produsului ofertat, ce necesită, dacă este cazul, a fi înlocuit în perioada de garanție, mediile de stocare de date de tip HDD, SSD, USB stick-uri, tape, defecte sau nu (indiferent de echipamentul în care este instalat) sau orice alt mediu amovibil, nu se vor returna furnizorului.

Pentru licențele software de bază se vor include servicii de suport, direct de la producător, pentru o durată de minim 12 luni de la data Acceptanței finale a Sistemului.

Licențele pentru aplicațiile software trebuie să aibă drept de utilizare acordat life-time (pentru o perioadă nedeterminată de timp).

Furnizorul are obligația de a soluționa incidentele constatate de Beneficiar în perioada de garanție, chiar dacă soluționarea acestora va conduce la prelungirea garanției cu perioada de soluționare a problemelor/incidentelor constatate.

De asemenea, Furnizorul are obligația de a asigura garanția și suportul pentru produsele livrate, serviile prestate și lucrările executate inclusiv pe toată perioada de derulare a contractului, până la Acceptanță finală a Sistemului, fără a afecta perioada de **Garanție pentru întreg Sistemul informtic central.**

În plus, furnizorul va realiza un plan de mentenanță care vizează perioada post-garanție și va include cel puțin servicii de tip preventiv, corectiv, adaptiv/evolutiv cât și costurile aferente acestora.

Suport tehnic

În perioada de garanție, Furnizorul va oferi următoarele servicii de suport:

- Asistență și suport tehnic la darea în producție – specialiștii cheie din echipa de implementare vor asigura suport on-site la darea in producție (asistență in productie) pe o perioadă de minimum 30 zile. Lista acestor specialiști va fi stabilită de comun acord cu Beneficiarul.
- Suport tehnic
- Servicii de HelpDesk (cu administrarea priorităților de deranjament, rapoarte de deranjamente și corelarea erorilor)

Serviciile de suport furnizate după lansarea în producție a sistemului, pe perioada garanției, care vor cuprinde:

- Suport pentru produsele /modulele utilizate în dezvoltarea /configurarea sistemului informatic

- Suport pentru platforma hardware şi infrastructura software a sistemului implementat.

- Suport pentru echipa tehnică a Beneficiarului în investigarea problemelor apărute în funcţionarea soluţiei SIIEASC şi a interfeţelor acesteia cu sistemele externe

Suportul pentru componentele de sistem se va asigura de catre prestator prin personal certificat/autorizat de producator.

9. Descriere SLA

În cadrul SLA-ului, furnizorul va acorda următoarele servicii de suport:

- Servicii de Help Desk
- Fault Management
- Rapoarte de deranjamente şi remedierea problemelor

Pentru a permite o identificare proactivă a unor posibile soluţii, se va asigura acces la o bază de cunoştinţe tehnice şi/sau documentaţie tehnică, prin intermediul centrului de Help Desk.

Administratorul de Servicii al Furnizorului va:

- administra şi monitoriza incidentele;
- lua legatura cu persoana desemnată ca punct de contact din partea beneficiarului, pentru analiza stărilor incidentelor deschise;
- răspunde tuturor întrebărilor legate de incidente.
- înregistra incidentele raportate de catre utilizatorii Beneficiarului, precum si transmiterea confirmarii solutionarii incidentului semnalat, in urma rezolvarii acestuia.
- marca finalizarea cererii şi comunicarea modalităţii de soluţionare completă şi definitivă a cererii către Beneficiar

Problemele ridicate de beneficiar vor fi înregistrate de către specialişti ai Furnizorului, în cadrul aplicaţiei de tip HELPDESK furnizată în cadrul proiectului.

Suportul va fi asigurat conform SLA.

Furnizorul va asigura diagnosticarea unui incident pentru determinarea problemei de bază.

Furnizorul va efectua toate activităţile necesare pentru remedierea problemelor constate ca urmare a raportării de către Beneficiar a incidentelor, conform nivelelor SLA stabilite.

Furnizorul va monitoriza în permanenţă incidentul până la închiderea acestuia.

Beneficiarul va avea acces la aplicaţia de tip HELPDESK pentru a monitoriza incidentele.

Nivel acord servicii (SLA)

Aceste servicii presupun derularea următoarelor activităţi de către Furnizor:

- Preluare de cereri de suport tehnic prin telefon/fax/e-mail
- Soluţionarea cererii de suport tehnic;
- Escaladarea la nivelul superior de suport în cazul în care nu se poate rezolva cererea telefonic;
- Marcarea finalizării cererii şi comunicarea către Beneficiar;
- Suport tehnic legat de utilizarea componentelor SIIEASC.

Activităţile efectuate de către Furnizor în cadrul serviciilor de suport tehnic, presupun comunicarea către Beneficiar a posibilelor rezolvări ale erorilor, a defectelor care împietează asupra bunei funcţionări în parametrii optimi a sistemului şi, după caz, intervenţia nemijlocită, exclusiv la sediul Beneficiarului, a experţilor Furnizorului atunci când este evident faptul că disfuncţionalitatea apărută în sistem este ca urmare a unor erori de configurare sau de funcţionare ale componentelor SIIEASC.

Nivel acord servicii – cerinţe generale

Furnizorul va lua toate măsurile administrative şi logistice pentru asigurarea timpilor de intervenţie şi de soluţionare specificaţi în prezentul SLA şi va prezenta în cadrul ofertei tehnice modalităţile prin care va putea oferi serviciile la nivelul şi în intervalul de timp solicitate.

Neîncadrarea în parametrii de disponibilitate şi de continuitate a funcţionării serviciilor de mentenanţă şi suport tehnic, depăşirea timpilor de intervenţie şi de soluţionare a problemelor, neîndeplinirea cantitativă şi calitativă a serviciilor în perioadele de timp definite, lipsa de reacţie la solicitările de suport tehnic precum şi nesoluţionarea acestora atrage după sine aplicarea de penalităţi.

Pe tot parcursul tratării unei probleme, Furnizorul va asigura trasabilitatea acţiunilor întreprinse de către echipa de suport tehnic, inclusiv a momentelor de timp în care aceste

acţiuni au fost stabilite/desfăşurate. Pentru o corelare consistentă şi o mapare a incidentelor critice/majore şi repetitive se va păstra un istoric al tuturor problemelor semnalate, inclusiv al modalităţilor de soluţionare a acestora, la Administratorul de Servicii al Furnizorului, acestea putând fi consultate online de către Beneficiar.

Nivelul de severitate al unei probleme va fi stabilit de către Beneficiar şi va fi comunicat în solicitarea de suport tehnic.

Nivelurile de severitate sunt definite astfel:

Nivelul de severitate 1:

Impact critic / Sistem inaccesibil: Beneficiarul este în imposibilitatea de a utiliza cel puţin una din componentele principale ale sistemului, rezultând un impact critic asupra disponibilităţii, securităţii şi performanţei SIIEASC. Această stare necesită o soluţie imediată.

O problemă poate fi catalogată cu nivel de severitate 1, cel puţin în următoarele situaţii:

- Aplicaţia dezvoltată nu este funcţională, se blochează, este inaccesibilă ca urmare a funcţionării defectuoase a unei componente a sistemului,
- Un echipament sau o componentă a acestuia (inclusiv software-ul de bază aferent) din arhitectura mediului de producţie al SIIEASC nu este funcţional/ă sau funcţionează defectuos.

Nivelul de severitate 2

Impact semnificativ/major: Sistemul suferă o pierdere masivă a funcţionalităţii, funcţiile importante ale aplicaţiei SIIEASC nefiind accesibile sau cu timpi mari de răspuns. Funcţii importante ale aplicaţiei dezvoltate SIIEASC pot fi, fără a se limita la:

- Întocmirea de acte de stare civilă,
- Emiterea de certificate de stare civilă,
- Interogarea, respectiv afişarea de date relevante din sistem.

Nivelul de severitate 3

Sistemul suferă o uşoară pierdere a funcţionalităţii. Impactul asupra disponibilităţii, securităţii şi performanţei sistemului nu este major, dar este necesară o rezolvare a problemei apărute. Exemple de disfuncţionalităţi care nu sunt majore:

- Gestiune conturi utilizatori,

Prelucrări date, generare/export rapoarte şi statistici.

Nivelul de severitate 4

Impact minim: O componentă neesenţială este nefuncţională, cauzând un impact minim sau

se face o cerere de serviciu non-tehnic. Beneficiarul solicită o informaţie, o îmbunătăţire a funcţionalităţii produselor software comerciale sau documentaţie clarificatoare cu privire la acestea. Nu există un impact asupra funcţionării sistemului. Funcţiile sistemului nu sunt afectate. Această stare nu necesită o intervenţie imediată a Furnizorului în site-ul Beneficiarului pentru constatarea defecţiunii, ci se va furniza un răspuns pentru remedierea de către Beneficiar a problemei, iar în maximum **24 de ore** acesta se va deplasa la sediul Beneficiarului, dacă este cazul, pentru remedierea/verificarea remedierii problemei.

Niveluri de severitate (impact)		**Timpi de intervenţie pe niveluri de severitate***		
	Timp de răspuns	**Diagnosticare**	**Soluţie provizorie**	**Soluţie finală**
Nivelul de severitate 1	30 min	2 ore	8 ore	24 ore
Nivelul de severitate 2	30 min	3 ore	10 ore	24 ore
Nivelul de severitate 3	60 min	6 ore	24 ore	72 ore
Nivelul de severitate 4	60 min	24 ore	72 ore	120 ore

***Se vor corela timpii de intervenţie cu nivelul de disponibilitate asigurat de site-ul principal şi cel secundar.**

Timp de răspuns – intervalul de timp în care Furnizorul va transmite confirmarea primirii cererii de asistenţă tehnică şi înregistrarea solicitării Beneficiarului;

Diagnosticare – intervalul de timp necesar pentru identificarea cauzelor care au produs problemele de funcţionare ale sistemului, calculat din momentul notificării incidentului.

Soluţia provizorie - intervalul de timp necesar pentru a asigura funcţionalităţile sistemului informatic, calculat din momentul notificării incidentului şi până la închiderea acestuia.

Soluţia finală - intervalul de timp necesar pentru a aduce sistemul la parametrii normali de funcţionare şi disponibilitate, calculat din momentul notificării incidentului şi pana la închiderea acestuia.

Timpii de intervenţie se măsoară de la notificarea incidentului de către beneficiar.

Suportul tehnic va fi furnizat la sediul Beneficiarului sau telefonic/e-mail. Dacă soluţionarea problemei se realizează prin intervenţia experţilor Furnizorului la sediul

Beneficiarului, aceasta se va realiza în prezenţa Beneficiarului.

În cazul incidentelor cu nivel de severitate 1, 2 va fi asigurat suportul tehnic 24 de ore pe zi, 7 zile pe săptămână şi va fi disponibil permanent până când problema este rezolvată (închisă), în condiţiile respectării cerinţelor de disponibilitate şi securitate ale SIIEASC şi a SLA-ului corespunzător fiecărui nivel de severitate.

În cazul incidentelor cu nivel de severitate 1 şi 2, în cazul unor defecte hardware justificate temeinic de către Furnizor, soluţia provizorie va fi menţinută în stare de funcționare până la implementarea soluției finale, dar nu mai mult de 15 zile.