# RAPORT PËRFUNDIMTAR AUDITIMI

# MBI AUDITIMIN E "SISTEMEVE TË TEKNOLOGJISË SË INFORMACIONIT" NË SHËRBIMIN SOCIAL SHTETËROR"

**Tiranë, Qershor 2024**

## PËRMBAJTJA

## LISTA E SHKURTIMEVE

| Shkurtimi | Emërtimi i Plotë |
|---|---|
| **KLSH** | Kontrolli i Lartë i Shtetit |
| **RSH** | Republika e Shqipërisë |
| **SHSSH** | Shërbimi Social Shtetëror |
| **NE** | Sistemi i menaxhimit të Ndihmës Ekonomike |
| **PPAK** | Regjistri elektronik i personave me aftësi të kufizuar |
| **SHKSH** | Sistemi i Adminsitrimit të Integruar të Shërbimeve Sociale |
| **BCP** | Business Continuity Plan |
| **ALCIRT** | Agjencia Kombëtare për Sigurinë Kibernetike |
| **BCC** | Business Continuity Center |
| **MNSH** | Marrëveshjeve Nivel Shërbimi |
| **AK** | Autoriteti Kontraktues |
| **OE** | Operator Ekonomik |
| **TI(IT)** | Teknologjia e Informacionit |
| **TIK** | Teknologjia e Informacionit dhe Komunikimi |
| **VKM** | Vendim i Këshillit të Ministrave |
| **KM** | Këshilli i Ministrave |
| **COBIT** | Objektivat e Kontrollit për Informacionin dhe Teknologjinë përkatëse |
| **INTOSAI** | Organizata Ndërkombëtare e Institucioneve Supreme të Auditimit |
| **ISSAI** | Standardet Ndërkombëtare të Institucioneve Supreme të Auditimit |
| **BE** | Bashkimi Evropian |
| **SSL** | Secure Sockets Layer |
| **VPN** | Virtual Private Network |
| **LAN** | Local area network |
| **IP** | Internet Protocol |

## 1.PËRMBLEDHJE EKZEKUTIVE

Kontrolli i Lartë i Shtetit (KLSH) mbështetur në nenet 3 dhe 14 të ligjit 154 "Për Organizimin dhe Funksionimin e Kontrollit të Lartë të Shtetit", datë 27.11.2014, zhvilloi një Auditim të Teknologjisë së Informacionit në Shërbimin Social Shtetëror, nga data 22.01.2024 deri më datë 29.03.2024.
Grupi i auditimit mblodhi informacione, zhvilloi pyetësorë e intervista për caktimin e zonave me risk të lartë dhe mbështetur në to hartoi matricat e auditimit.
Kërkesat për informacion për fushat përkatëse u hartuan në përputhje me manualin e Auditimit të Teknologjisë së Informacionit.

### I.1. Përshkrim i shkurtër i Projektit të Auditimit

Projekti i auditimit, për auditimin e Sistemeve të Teknologjisë së Informacionit, në Shërbimin Social Shtetëror, është pjesë e Planit Vjetor 2024 të auditimit të KLSH-së, miratuar nga Kryetari i KLSH. Projektimi i këtij auditimi, është bërë bazuar në një analizë risku, si gjatë hartimit të planit vjetor, po ashtu edhe gjatë hartimit të Programit të Projektit të Auditimit, ku KLSH, ka vlerësuar si të rëndësishëm auditimin e sistemeve të teknologjisë që Shërbimi Social Shtetëror disponon, për të garantuar disponibilitet dhe integritet të të dhënave. Mbështetur në punën në terren, evidencat e marra kanë qenë të mjaftueshme dhe të besueshme për punën audituese. Rezultatet kryesore të punës audituese përfshihen në këtë përmbledhje të Raportit Përfundimtar. Auditimi i sistemeve të Informacionit është i rëndësishëm për institucionet, si pasojë e rritjes së kompleksitetit të kontrollit të aksesit dhe ruajtjes së konfidencialitetit, integritetit dhe gatishmërisë së të dhënave nga marrëdhëniet e rrjeteve publike me ato private dhe nga bashkë përdorimi i burimeve të informacionit. Siguria e Informacionit përcaktohet si mundësia e një sistemi për të mbrojtur informacionin dhe burimet e sistemeve në përputhje me termat e konfidencialitetit, integritetit dhe gatishmërisë. Sistemet e informacionit janë bashkime komplekse të teknologjisë, proceseve dhe njerëzve që funksionojnë së bashku për të rregulluar përpunimin, ruajtjen, dhe transferimin e informacionit për të mbështetur misionin e institucionit dhe funksionet e tij. Lidhur nga sa më sipër, çdo institucion shtetëror që ofron shërbime ndaj qytetarëve e ka si detyrim ndërtimin e programit të sigurisë së informacionit me elementët kyç të cilët janë: *"*Mjedisi i sigurisë së informacionit, Vlerësimi i riskut, Politikat e sigurisë, Organizimi i sigurisë së TIK, Menaxhimi i aseteve, Siguria e burimeve njerëzore, Siguria fizike dhe mjedisore, Kontrolli i aksesit, Menaxhimi i incidenteve të sigurisë së TIK, Menaxhimi i vazhdueshmërisë së biznesit, Përputhshmëria*".*

**I.2. Përshkrim i gjetjeve kryesore dhe rekomandimeve:**

**Paraqitja e gjetjeve kryesore:**

- *Nga auditimi u konstatua se struktura TI e SHSSH ende nuk ka kaluar si pjesë e strukturës së AKSHI-t sipas përcaktimeve dhe afateve të vendosura në VKM Nr. 673, datë 22.11.2017, "Për riorganizimin e Agjencisë Kombëtarë të Shoqërisë së Informacionit", i ndryshuar.*
- *Nga auditimi u konstatua se ndjekësit e kontratave të nivelit të shërbimit nuk mbajnë një procesverbal për të konfirmuar veprimet e kryera në sistem të cilat janë të pasqyruara në raportet mujore të sjella nga kontraktuesi të renditurara si më poshtë:*
  - *-Kontroll i Gjendjes së Failover Cluster;*
  - *-Kontroll i Gjendjes së Failover Cluster Sql Te Serverave;*
  - *-Raportim i Sistemit të Backup;*
  - *-Probleme të Verifikuara gjatë Kontrolleve Periodike të Shërbimeve Infrastrukturore.*
- Nga auditimi u konstatua se Shërbimi Social Shtetëror nuk disponon përdoruesin me të drejta të plota – Db Owner, megjithëse është përgjegjëse për të dhënat që popullojnë sistemet e Ndihmës Sociale bazuar në VKM Nr. 673, datë 22.11.2017 "Për riorganizimin e Agjencisë Kombëtarë të Shoqërisë së Informacionit", i ndryshuar
- *Nga auditimi i përdoruesve të sistemeve të SHSSH u konstatua se :*
- *Detyra e administratorit të sistemit në rolin e Administratorit të SHSSH nuk është e caktuar me anë të një shkrese zyrtare nga organet drejtuese të MSHMC dhe AKSHI në mënyrë që të përcaktohen qartë të drejtat dhe detyrat e administratorit të sistemit, Nuk disponohet një akt rregullativ i dokumentuar dhe i miratuar për administrimin/menaxhimin e përdoruesve, në të cilën të jenë të përcaktuara procedurat që do të ndiqen për krijimin, fshirjen, ndryshim.*
- *-Nga auditimi i përdoruesve të sistemeve (NE, PAK, SHKSH) u konstatua se ka përdorues aktiv me emër useri të pa Identifikuar.*
- *-Nga auditimi i përdoruesve të databasës u konstatua se ekzistojnë një numër përdoruesish por nuk është kryer një ndarje privilegjesh për çdo përdorues sipas niveleve në bazë të detyrave që ata kanë.*
- *Nga auditimi u konstatua se sistemet e Ndihmës Ekonomike nuk ndërveprojnë me Webservice me Agjencinë Shtetërore të Kadastrës. Mungesa e ndërveprimit ndërmjet sistemeve sjell rriskun e vlerësimit të gabuar të aplikantëve për Ndihmën Ekonomike Sistemi nuk mund të verifikoj nëse aplikanët kanë ose jo prona të regjistruara në ASHK.*

**Paraqitja e rekomandimeve kryesore:**

- *Organet drejtuese në Shërbimin Social Shtetëror të analizojnë dhe vlerësojnë situatën për marrjen e masave për kalimin e strukturave përgjegjëse TIK tek AKSHI në zbatim të dispozitave ligjore në fuqi.*
- Komisioni i marrjes në dorëzim në MSHMS të marrë masa që në të ardhmen të mbajë raporte periodike mbi zbatimin e kontratës, në përputhje me kushtet e veçanta të kontratës
- Shërbimi Social Shtetëror si institucioni përgjegjës i bazës së të dhënave të sistemeve e Ndihmës Sociale, të marrë masat për menaxhimin e bazës së të dhënave, që përmban të gjitha llojet e aksesit në sistemet që ka në përdorim.
- Shërbimi Social Shtetëror në bashkëpunim me AKSHI-n të marrin masa për administrimin e përdoruesve të brendshëm, ku të përcaktohen saktë lidhja e punonjës-user në sistem sipas detyrave të caktuara që ata kanë.
- *AKSHI dhe Shërbimi Social Shtetëror të marrin masa duke komunikuar me ASHK për gjetjen e problematikave të funksionimit të webservisit për të vendosur në funksionim të plotë ndërveprimin ndërmjet sistemeve që SHSSH dhe ASHK me qëllim rritjen e efikastitetit të vlerësimit të formularëve për aplikuesit e Ndihmës Elonomike.*

### 1.3 Konkluzioni i përgjithshëm dhe Opinioni i Auditimit:

Grupi i auditimit është mbështetur në Standardet ndërkombëtare të Auditimit përkatësisht në ISSAI 100, ISSAI 5300, ISSAI 5310 si dhe nenet 3 dhe 14 të ligjit 154 "Për Organizimin dhe Funksionimin e KLSH" datë 27.11.2014. Kemi audituar Sistemet e Teknologjisë së Informacionit për periudhën ushtrimore 01.01.2022-31.12.2023 në të cilat përfshihet Qeverisja IT, Siguria e Informacionit, Investimet në fushën TIK dhe sistemet e teknologjisë së informacionit që Shërbimi Social Shtetëror ka në përdorim dhe mbështet aktivitetin e saj. Kemi konstatuar se, mungesa e akteve rregullatorë në drejtim të sistemeve të teknologjisë së informacionit kanë ndikuar në një zhvillim të pa monitoruar të aktivitetit institucional dhe pa deleguar përgjegjësitë individuale për veprimet e kryera.
Nga analizimi i të dhënave, rezultoi se sistemi i Ndihmës Ekonomike ka mungesë në mekanizmat e nevojshme për kontrollin e inputit, duke rritur riskun e popullimit të sistemit me të dhëna të gabuara, e për pasojë nxjerrjen e rezultateve të pasakta.
Implementimi i protokolleve themelore të sigurisë ashtë i pamjaftueshëm. Ka mungesë trajnimit të punonjësve në praktikat më të mira të sigurisë kibernitike, . Kjo pakujdesi paraqet një rrezik për konfidencialitetin, integritetin dhe disponueshmërinë e informacionit dhe sistemeve. Siguria e Informacionit dhe perspektiva e SHSSH është e kompromentuar nga investimet e pakta në teknologjinë e Informacionit.
Në gjykimin tonë, identifikimi dhe administrimi i elementëve kritikë në ofrimin e shërbimeve kundrejt qytetareve dhe garantimin e sigurisë së të dhënave si dhe vazhdimësisë në ofrimin e shërbimit pa ndërprerje nëpërmjet teknologjisë së informacionit është i pamjaftueshëm.
SHSSH nuk ka marrë masa për kalimin e strukturave përgjegjëse TIK tek AKSHI sipas përcaktimeve dhe afateve të vendosur në VKM Nr. 673, datë 22.11.2017, "Për riorganizimin e Agjencisë Kombëtarë të Shoqërisë së Informacionit", i ndryshuar.

## II. HYRJA

Mbështetur në Ligjin 154/2014, datë 27.11.2014 "*Për Organizimin dhe Funksionimin e KLSH*", në zbatim të Programit të Auditimit 1138/2 Prot, datë 22.01.2024 të miratuar nga Kryetari i KLSH, me afat auditimi 22.01.2024 deri në 29.03.2024, në Shërbimin Social Shtetëror (më poshtë SHSSH), ku periudha e audituar është 01.01.2022 deri në 31.12.2023, u krye auditimi me objekt "*Auditimi i Sistemeve të Teknologjisë së Informacionit*", nga audituesit:

1. R.A, përgjegjës grupi
2. A.A, anëtar
3. M.P, anëtare

### *II.1. Objektivat dhe qëllimi auditimit*

*Objekti i Auditimit TIK* është përcaktimi nëse objektivat e subjektit arrihen në mënyrën e duhur duke përdorur burimet IT, duke përfshirë pajtueshmërinë me kërkesat ligjore dhe rregullative, konfidencialitetin, integritetin si dhe disponueshmërinë e sistemeve të informacionit dhe të dhënave që gjenden në të.
Qëllimi i Auditimit TIK ushtruar në Shërbimin Social Shtetëror, është dhënia e opinionit apo vlerësimit nëse ekzistojnë kontrollet dhe mekanizmat e duhur me qëllim krijimin, mirëmbajtjen e burimeve IT dhe funksioneve për të cilat këto burime shërbejnë. Për të arritur në dhënien e një opinioni, janë mbledhur informacione, të dhëna dhe prova, për të përcaktuar nëse nëpërmjet teknologjisë së informacionit mbrohen asetet, ruhet integriteti i të dhënave, si dhe synimet e

subjektit që auditohet arrihen në mënyrë efektive duke përdorur burimet në mënyrë efiçente. Kërkesat për informacion sipas drejtimeve të programit të auditimit, u hartuan në përputhje me Manualin e Auditimit të Teknologjisë së Informacionit.

### *II.2 Identifikimi i çështjeve:*

Drejtimet e këtij auditimi janë bazuar në programin e auditimit të miratuar nga Kryetari i Kontrollit të Lartë të Shtetit të protokolluar me nr.1138/2 Prot, datë 22.01.2024:

1.**Auditimi i Qeverisjes TIK dhe blerjes për teknologjinë e informacionit.**
*a.Verifikim i politikave, standardeve dhe vlerësimi i burimeve njerëzore në TIK.*
*b.Investimet në teknologjinë e informacionit.*
**2.Auditimi i sigurisë së informacionit.**
*a.Siguria e të dhënave dhe vazhdimësia në ofrimin e shërbimit.*
*b.Përdoruesit e sistemeve, të drejtat dhe gjurmët e veprimeve në sistem*
**3. Auditimi i sistemeve mbi të dhënat Input / Output.**
**4. Të tjera**

### *II.3 Përgjegjësitë e strukturave drejtuese të subjektit të audituar*

Shërbimi Social Shtetëror organizohet në dy nivele: në nivel qendror dhe rajonal, për çdo qark të vendit. SHSSH drejtohet nga drejtori i Përgjithshëm. Shërbimi Social Shtetëror, sipas fushave të veprimtarisë, në nivel qendror, ka këto funksione: Vlerëson, përgatit dhe propozon nevojat e financimit afatmesëm dhe vjetor për ndihmën ekonomike;
b) Programon dhe detajon në fillim të vitit në bazë të treguesve të njësive të pushtetit vendor dhe në vijim, në bazë të realizimit faktik, çdo dy muaj, fondet për ndihmën ekonomike, në përputhje me vlerësimin e nevojave të familjeve dhe të individëve për çdo bashki, si dhe të burimeve të buxhetit të shtetit;
c) Kontrollon përdorimin e fondeve të buxhetit të shtetit për ndihmën ekonomike; ç) Kontrollon zbatimin e legjislacionit për ndihmën ekonomike, sipas përcaktimeve të legjislacionit në fuqi;
d) Merr vendimin për përfitimin e ndihmës ekonomike dhe të masës së përfitimit për çdo rast individual, sipas procedurave të parashikuara në legjislacionin në fuqi;
dh) Mbledh, përpunon dhe analizon të dhënat mbi shpërndarjen e ndihmës ekonomike nga njësitë e qeverisjes vendore dhe raporton, periodikisht, në ministrinë përgjegjëse për çështjet sociale;
e) Raporton në ministrinë përgjegjëse për çështjet sociale, çdo tre muaj, mbi ecurinë e skemës së ndihmës ekonomike dhe rezultatet e kontrolleve të ushtruara në njësitë vendore; ë) Propozon përmirësimin e programeve dhe të politikave në fushën e ndihmës ekonomike për vlerësim pranë ministrisë përgjegjëse për çështjet sociale;
f) Ushtron çdo kompetencë tjetër specifike sipas legjislacionit në fuqi për ndihmën ekonomike;
g) Asiston njësitë e qeverisjes vendore dhe trajnon nëpunësit e tyre në ofrimin dhe përmirësimin e shërbimeve për ndihmën ekonomike;
gj) Administron dhe mirëmban Regjistrin Elektronik Kombëtar të Ndihmës Ekonomike.

### *II.4 Përgjegjësitë e audituesve*

Kontrolli i Lartë i Shtetit auditoi Shërbimin Social Shtetëror, mbi periudhën e veprimtarisë nga 01.01.2022 deri në 31.12.2023, duke i kushtuar vëmendje çështjeve që lidhen me zbatimin e ligjshmërisë dhe rregullshmërisë si dhe standardeve ndërkombëtare të teknologjisë dhe auditimit TIK.
Nga grupi i auditimit, me përgjegjësi të plotë, janë analizuar të gjitha çështjet që përmban Programi i Auditimit nr. 1138/2 Prot, datë 22.01.2024 miratuar nga Kryetari i KLSH. Në

realizimin e këtij Projekt Auditimi, grupi i auditimit është mbështetur në bazën ligjore mbi të cilën funksionon KLSH, standardet e auditimit, legjislacionin e fushës në të cilën operon SHSSH. Gjithashtu, gjatë veprimtarisë audituese, është siguruar një evidencë e përshtatshme, e mjaftueshme dhe e besueshme auditimi, në të cilën jemi mbështetur në dhënien e konkluzioneve dhe rekomandimeve.

### *II.5 Kriteret e vlerësimit*

Kriteret e vlerësimit janë bazuar në ligjet, rregulloret në fuqi, standardet ndërkombëtare COBIT dhe ISSAI 5300 për auditimin e Teknologjisë së Informacionit si dhe Manualin e Teknologjisë së Informacionit. Opinioni i auditimit mbështetet në praktikat më të mira, Standardet Kombëtare dhe Ndërkombëtare të Auditimit. Në këtë Raport Përfundimtar Auditimit krahas gjetjeve që janë konstatuar, grupi i auditimit ka rekomanduar disa masa organizative, për përmirësimin e situatës.

*Aktet ligjore dhe rregullative mbi të cilat është mbështetur vlerësimi janë si më poshtë:*

- Standardet Ndërkombëtare të Auditimit (ISSA1) të INTOSAI-t.
- Udhëzues dhe Manuale të Auditimit të Teknologjisë së Informacionit si: ISSAI 5300, Manuali Aktiv i Auditimit IT si dhe Standardet e COBIT.
- Kushtetuta e Republikës së Shqipërisë (nenet 162-165);
- Ligji nr.154/2014 "Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit";
- Ligji Nr. 162 Date 23.12.2020 Për Prokurimin Publik.
- Konventa për të drejtat e fëmijës
- Ligj nr. 121/2016 “Për shërbimet e kujdesit shoqëror në Republikën e Shqipërisë".
- Ligj nr. 8153, date 31.10.1996 "Për statusin e jetimit- Ligj nr. 18/2017 "Për të drejtat dhe mbrojtjen e fëmijës".
- VKM nr. 135, datë 07.03.2018 "Për miratimin e statutit të Shërbimit Social Shtetëror".
- VKM nr. 111, datë 23.02.2018 "Për krijimin dhe funksionimin e fondit social".
- Ligji nr. 7961, datë 12.07.1995 “Kodi i punës i Republikës së Shqipërisë”, ndryshuar;
- Ligji nr. 10296, datë 08.07.2010 "Për menaxhimin financiar dhe kontrollin", i ndryshuar dhe aktet ligjore në zbatim të tij;
- Ligji nr. 114/2015 "Për auditimin e brendshëm në sektorin publik";
- Ligji nr. 9887, datë 10.03.2008, ndryshuar me Ligjin nr. 48/2012 "Për mbrojtjen e të dhënave personale";
- Ligji nr. 119/2014 "Për të drejtën e informimit";
- VKMnr.710,datë 21.08.2013"Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit", i ndryshuar.
- Standardet TIK;
- Udhëzimi nr. 30, datë 27.12.2011 "Për Menaxhimin e Aktiveve në Njësitë e Sektorit Publik", i ndryshuar;
- Udhëzimi nr. 1159, datë 17.03.2014 "për hartimin e Marrëveshjes të Nivelit të Shërbimit", i ndryshuar;
- Akte të tjera ligjore apo nënligjore që do të jenë të nevojshme gjatë auditimit.

### *II.6 Standardet e auditimit*

Auditimi është kryer, në përputhje me Kodin Etik, Standardet, dhe teknikat e auditimit të teknologjisë së informacionit, duke përfshirë pyetësorë, intervista, testime dhe procedura, të cilat u gjykuan se ishin të nevojshme, për të dhënë një vlerësim sa më objektiv, profesional e të pavarur, të saktë, të plotë e të qartë, duke u fokusuar veçanërisht në standardet e fushës së auditimit të TIK, si: COBIT 4.1, Manuali i Auditimit IT, ISSAI 5310, etj

### *II.7 Metodat e auditimit*

Metodat mbi auditimin e sistemeve të Teknologjisë së Informacionit që grupi i auditimit ka ndjekur në SHSSH, janë si më poshtë:

- Intervista zhvilluar në subjekt me personat përgjegjës;
- Verifikime të sistemit si auditues;
- Shqyrtimi i dokumentacionit rregullativ të institucionit;
- Analizimi i të dhënave të eksportuara nga sistemi;

***II.8 Dokumentimi i auditimit***

Dokumentimi i auditimit është bazuar në rregulloren e brendshme të KLSH si dhe në manualin aktiv të auditimit të Teknologjisë së Informacionit në të cilin janë përfshirë:

- Planifikimi, qëllimi dhe objektivat e auditimit;
- Programi i auditimit;
- Evidencat e grumbulluara në lidhje me të dhënat e sistemit, raporte të ndryshme me të dhëna nxjerrë nga sistemi;
- Letrat e punës mbajtur nga audituesit sipas detyrave të përcaktuara gjatë fazës së auditimit në terren.

## III.PËRSHKRIMI I AUDITIMIT

***1. Informacioni i përgjithshëm mbi subjektin nën auditim***

Shërbimi Social Shtetëror është institucion buxhetor në varësi të ministrit përgjegjës për çështjet e ndihmës dhe të shërbimeve shoqërore, më tej "ministri", me seli në Tiranë. Shërbimi Social Shtetëror lind si Administrata e Përgjithshme e Ndihmës dhe e Shërbimeve Sociale me një vendim të Këshillit të Ministrave nr.52, 08.01.1996 "Per krijimin dhe funksionimin e Këshillit të Përgjithshëm të Ndihmës dhe Shërbimeve Sociale,si dhe të Administratës së Përgjithshme të Ndihmës dhe Shërbimeve Sociale".

Shërbimi Social Shtetëror ka për mision zbatimin e politikave, legjislacionin e ndihmës ekonomike, pagesës për personat me aftësi të kufizuar dhe shërbimeve shoqërore në të gjithë vendin për :

- 29 Institucione të Përkujdesit Shoqëror,
- 12 Drejtori Rajonale,
- Administrata Qendrore e Shërbimit Social Shtetëror si edhe,
- 61 njësi të qeverisjes vendore.

Këtë mision e realizon nëpërmjet:

- Administrimit të Shërbimeve Shoqërore për individët në nivel kombëtar;
- Programimit dhe detajimit të fondeve te ndihmës ekonomike;
- Programimit dhe detajimit të fondeve te pagesës për personat me aftësi të kufizuar;
- Programimit dhe detajimit të fondeve per shërbimet shoqërore;
- Kontrollit te zbatimit të legjislacionit dhe përdorimit të fondeve buxhetore për ndihmën; ekonomike, pagesën e personave me aftësi të kufizuar dhe shërbimet e shoqërore;
- Administrimit të Regjistrit Elektronik Kombëtar për aplikantët dhe përfituesit e ndihmës ekonomike, të pagesës së aftësisë së kufizuar dhe të shërbimeve të përkujdesit shoqëror;
- Monitorimit të standardeve të shërbimeve sociale në nivel kombëtar.

**2. Përshkrimi i rezultateve të auditimit**

**2.1Auditimi i Funksionimit të Qeverisjes Tik**

- *Burimet njerëzore, aktet rregullative, identifikimi dhe menaxhimi i risqeve në teknologjinë e informacionit*

Shërbimi Social Shtetëror ushtron veprimtarinë e tij në bazë të Vendimit të Këshillit të Ministrave nr. 135, datë 07.03.2018, "Për miratimin e Statutit të Shërbimit Social Shtetëror". SHSSH funksionon sipas strukturës së miratuar me Urdhër të Kryeministrimit nr 135, datë

21.10.2019, “Për disa ndryshime në Urdhërin nr. 88, datë 25.10.2011 “Për miratimin e strukturës dhe të organikës së Shërbimit Social Shtetëror”, të ndryshuar.
Nga auditimi ka rezultuar se në strukturën e miratuar institucioni ka një numër total prej 53 punonjësish, nga të cilët është 1 pozicion vakante. Drejtoria e Përgjithshme e Shërbimit Social Shtetëror ka në strukturën e saj të miratuar 3 specialistë TI, nga të cilët 2 prej tyre janë të pozicionuar në Drejtorinë e Kontrollit të Pagesës së NE dhe PAK dhe 1 specialist në Drejtorinë e Shërbimeve Sociale sipas Urdhërit nr. 135, datë 21.10.2019, i ndryshuar dhe Urdhëri nr. 66, datë 13.04.2022 “Për miratimin e strukturës dhe të organikës së Shërbimit Social Shtetëror”. Drejtoritë Rajonale të Shërbimit Social Shtetëror kanë në total 12 specialistë TI, përkatësisht nga 1 specialist për çdo drejtori. Gjithashtu, janë 2 specialistë TI të ndihmës sociale në Drejtorinë e TI atashuar pranë Ministrisë së Shëndetësisë dhe Mbrojtjes Sociale.

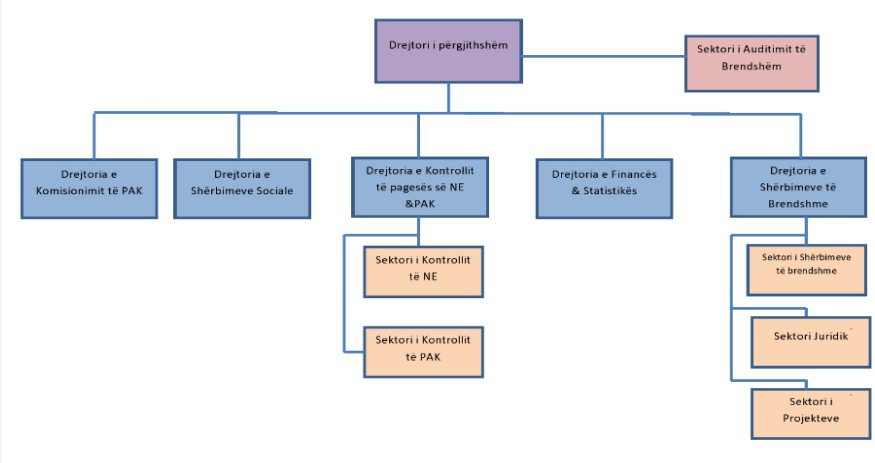



Figura nr.1: Struktura e SHSSH

Bazuar në VKM nr. 673, datë 22.11.2017, strukturat përgjegjëse TIK të institucioneve dhe organeve të administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave, bëhen pjesë e strukturës së AKSHI-t. Punonjësit aktualë të njësive të teknologjisë së informacionit në përbërje të strukturave të institucioneve dhe organeve të administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave, kalojnë tek AKSHI, Në kundërshtim me pikën 23 të VKM-së nr. 673, datë 22.11.2017, në të cilën citohet se: “Strukturat përgjegjëse TIK bëhen pjesë të strukturës së AKSHI-t. Punonjësit aktualë të njësive të teknologjisë së informacionit e të komunikimit (NJTIK), në përbërje të strukturave të institucioneve dhe organeve të administratës shtetërore nën përgjegjësinë e Këshillit të Ministrave, kalojnë tek AKSHI, brenda datës 31.12.2017 dhe do të trajtohen në bazë të përcaktimeve të legjislacionit në fuqi për nëpunësit civil, në rastin e mbylljes dhe ristrukturimit të institucionit, apo Kodit të Punës. AKSHI vendos në dispozicion të institucioneve të përmendura në shkronjën “i”, të pikës 6, personelin e mjaftueshëm dhe të certifikuar sipas legjislacionit në fuqi, për të mbajtur në funksion optimal sistemet të cilat nuk preken nga fusha e veprimit të këtij vendimi”.
*Nga auditimi u konstatua se struktura TI e SHSSH ende nuk ka kaluar si pjesë e strukturës së AKSHI-t sipas përcaktimeve dhe afateve të vendosura në VKM Nr. 673, datë 22.11.2017, “Për riorganizimin e Agjencisë Kombëtarë të Shoqërisë së Informacionit”, i ndryshuar.*

***Trajnimet***

Zhvillimi i trajnimeve ka një rëndësi të veçantë për menaxhimin e kapaciteteve njerëzore në institucion. Punonjësit të cilët kanë akses në sistemet e informacionit duhet të jenë të njohur me standardet e sigurisë dhe të gëzojnë aftësinë për zbatimin dhe implementimin e tyre gjatë aktivitetit që kryejnë. Është e nevojshme që të identifikohen nevojat e stafit për trajnime mbi teknologjinë e informacionit.
Nga dokumentacioni i vënë në dispozicion si dhe nga komunikimet verbale me subjektin deri më tani në Shërbimin Social Shtetëror është konstatuar se specialistët e TI nuk kanë zhvilluar trajnime për kualifikime profesionale brenda dhe jashtë vendit gjatë periudhës objekt auditimi.

Po ashtu, ka rezultuar se institucioni nuk ka një plan mbi trajnimin e stafit të TI në fusha specifike të cilat do të ndihmonin stafin në rritjen profesionale, certifikimin dhe kualifikimin e mëtejshëm të tyre. Mungesa e trajnimeve sipas fushave përkatëse për sektorin e teknologjisë së informacionit bën që për pasojë ata të mos mund të zbatojnë si duhet detyrat e përcaktuara në përshkrimet e punës sipas rregullores dhe statutit të SHSSH.
Nga auditimi rezultoi se nuk ka propozime konkrete nga niveli menaxherial i SHSSH për zhvillimin e trajnimeve dhe se nuk është i dokumentuar procesi i kërkesave, nevojave dhe analizimi i tyre për kualifikime profesionale, duke mos plotësuar kështu nevojat për trajnim mbi sistemet, sigurinë dhe teknologjinë e informacionit.
- Në Drejtoritë Rajonale të Shërbimit Social Shtetëror Shkodër dhe Vlorë u konstatua se specialistët e TI në këto drejtori nuk kanë kryer trajnime profesionale brenda dhe jashtë vendit të cilat do ti shërbenin stafit për kualifikime të mëtejshme për ti ndihmuar në kryerjen e detyrave funksionale të përcaktuara në përshkrimet e tyre të punës.

**Verifikim i politikave dhe procedurat në TIK**

Grupi i auditimit, me qëllim auditimin e nivelit të dokumentimit të politikave dhe procedurave në lidhje me teknologjinë e informacionit, verifikoi rregulloret e institucionit, si dhe udhëzime të tjera të brendshme. Auditimi për këtë çështje pati në konsideratë risqet që vijnë nga mungesa e politikave dhe procedurave të shkruara, si dhe nga praktikat me të cilat institucioni zhvillon aktivitetin e tij.
Nga auditimi u konstatua se Teknologjia e Informacionit në SHSSH zhvillohet në kushtet e mungesës së bazës rregullatore. SHSSH nuk ka marrë masa për hartimin e rregullave dhe procedurave të proceseve të teknologjisë se informacionit në përputhje me aktet ligjore, nënligjore dhe praktikat më të mira, duke mos konsideruar elementë të tillë si: rregulla mbi veprimtarinë e TI në institucion; rregulla mbi menaxhimin e incidenteve; procedura dhe indikatorë të matjes së performancës për gabimet/ incidentet e ndodhura dhe masat reaguese ndaj tyre; struktura kontrolli për verifikimin e efektivitetit të ndryshimeve të kryera; procedura për ndryshimet emergjente si dhe dokumentimin e të gjithë procesit të ndryshimeve. Mungesa e bazës së brendshme rregullatore për funksionimin e strukturave të teknologjisë së informacionit sjell operimin mbi baza ngjarjeje, duke rritur riskun e ekspozimit të institucionit ndaj situatave ku reagimi është i paidentifikuar, burimet njerëzore dhe përgjegjësitë të paalokuara, si dhe koha e përgjigjes e papërcaktuar.

**Identifikimi dhe menaxhimi i risqeve në TIK dhe në ofrimin e shërbimit**
Nga dokumentacioni i vendosur në dispozicion, ka rezultuar se Shërbimi Social Shtetëror nuk disponon regjistër risqesh lidhur me teknologjinë e informacionit. Në asnjë formë nuk rezulton të jenë dokumentuar risqe të identifikuara për periudhën objekt auditimi, por as përpara kësaj. Për veprimet ose mosveprimet që janë në kundërshtim me nenin 11 pika 2 *"Identifikimin dhe krijimin e regjistrit të riskut, vlerësimin, kontrollin e risqeve që vënë në rrezik arritjen e objektivave dhe realizimin me sukses të veprimtarive të strukturave që ata drejtojnë."*, 12 pika 3/d "*Identifikimin dhe krijimin e regjistrit të riskut, vlerësimin, kontrollin e risqeve që vënë në rrezikarritjen e objektivave dhe realizimin me sukses të veprimtarive të strukturave që ata drejtojnë"*, nenin 21 të ligjit nr. 10296, datë 08.07.2010, "Për menaxhimin financiar dhe kontrollin", i ndryshuar me ligjin nr. 110/2015, datë 23.10.2015, udhëzimin nr. 30, datë 27.12.2011 "Për menaxhimin e aktiveve në njësitë e sektorit publik", i ndryshuar, udhëzimi nr. 21, datë 25.10.2016 "Për nëpunësit zbatues të të gjitha niveleve", Udhëzimi i Ministrit të Financave nr. 16, datë 20.07.2016 "Për përgjegjësitë dhe detyrat e koordinatorit të menaxhimit financiar dhe kontrollit dhe koordinatorit të riskut në njësitë publike", Shërbimi Social Shtetëror duhet të kishte hartuar regjistrin e riskut ku të përfshihen edhe risqet që lidhen me teknologjinë e informacionit.

**Auditi i brendshëm**

Misioni i njësisë së auditimit të brendshëm, si pjesë e strukturës të SHSSH është orientimi i veprimtarisë, në mënyrë të pavarur dhe profesionale, duke dhënë garanci të arsyeshme, për efiçencën, efektivitetin, ekonomicitetin e menaxhimit të burimeve, përmirësimin e sistemit të kontrollit të brendshëm dhe menaxhimin e riskut. Ndjekjen e praktikave më të mira bashkëkohore dhe forcimin e kapaciteteve profesionale të auditimit. Auditi i brendshëm në Shërbimin Social Shtetëror është e organizuar në nivel Sektori e përbërë nga një përgjegjës sektori dhe dy specialistë.

Nga auditimi u konstatua se Sektori i Auditit të Brendshëm në SHSSH për periudhën 01.01.2021-31.12.2023 nuk ka kryer asnjë auditim mbi sistemet e teknologjisë së informacionit, në kundërshtim me nenet 14 dhe 8 të Ligjit nr. 114/2015 "Për Auditimin e Brendshëm në sektorin publik". "Të kryejë auditime IT sipas përcaktimeve të nenit 4, pika 6 dhe nenit 9 dhe në përputhje me Standardet ndërkombëtare për praktikën profesionale të auditimit të brendshëm. Veprimtaria e auditit të brendshëm në sektorin publik duhet të kryhet në përputhje me:

- Standardet ndërkombëtare të auditimit të brendshëm, të pranuara për t'u zbatuar në Republikën e Shqipërisë dhe të miratuara me urdhër të Ministrit të Financave;
- Këtë ligj dhe të gjitha aktet nënligjore bazuar në këtë ligj;
- Kartën e Auditimit, Kodin e Etikës për audituesit e brendshëm, manualin e auditimit të brendshëm, si dhe akte të tjera specifike për kryerjen e shërbimit të auditimit;
- Kryerjen e auditimeve TI sipas përcaktimeve te nenit 4, Pika 6, nenit 9 dhe në përputhje me Standardet ndërkombëtare për praktikën profesionale të auditimit të brendshëm.

**1.b.Investimet në teknologjinë e informacionit.**

Nga auditimi ka rezultuar se AKSHI në cilësinë e Autoritetit Kontraktor ka zhvilluar dy procedura prokurimi ku përfitues është Ministria e Shëndetësisë dhe Mbrojtjes Sociale.

- AKSHI dhe bashkimi i dy Operatorëve Ekonomik I.I dhe I.S kanë nënshkruar kontratën nr. 45, datë 04.04.2022 me objekt "Mirëmbajtja e sistemit të menaxhimit të informacionit për programin e pagesës së aftësisë së kufizuar dhe infrastrukturës hostuese – për Ministrinë e Shëndetësisë dhe Mbrojtjes Sociale". Nëpërmjet kësaj kontrate, Kontraktori ka marrë përsipër ofrimin e shërbimit me vlerë 36,672,000 lekë pa TVSH e cila ka nisur zbatimin e saj nga data e nënshkrimit dhe vazhdon për 24 muaj mirëmbajtje.
- AKSHI ka nxjerrë Urdhrin e Prokurimit nr. 9, datë 01.02.2023 me objekt "Mirëmbajtja e sistemit të ndihmës ekonomike dhe shërbimit social", për Ministrinë e Shëndetësisë dhe Mbrojtjes Sociale, me fond limit 189,984,000 lekë pa TVSH për një periudhë 24 mujore. AKSHI dhe bashkimi i dy Operatorëve Ekonomik I.I dhe I.S kanë nënshkruar kontratën nr. 46, datë 18.05.2023 me objekt "Mirëmbajtja e sistemit të ndihmës ekonomike dhe shërbimit social – për Ministrinë e Shëndetësisë dhe Mbrojtjes Sociale". Nëpërmjet kontratës, Kontraktori ka marrë përsipër ofrimin e shërbimit me vlerë 180,484,800 lekë pa TVSH e cila ka nisur zbatimin e saj nga data e nënshkrimit dhe vazhdon për 24 muaj mirëmbajtje.

-Nga auditimi u konstatua se marrjen në dorëzim të sistemeve të SHSSH e kryejnë specialistët e AKSHI-t atashuar pranë Ministrisë së Shëndetsisë dhe Mbrojtjes Sociale, të cilët nuk janë përdorues të këtyre sistemeve çfarë tregon për një monitorim formal të ndjekjes në zbatimin e kontratës.

-Nga auditimi u konstatua se ndjekësit e kontratave të nivelit të shërbimit nuk mbajnë një procesverbal për të konfirmuar veprimet e kryera në sistem të cilat janë të pasqyruara në raportet mujore të sjella nga kontraktuesi të renditura si më poshtë:

*-Kontroll i Gjendjes së Failover Cluster;*
*-Kontroll i Gjendjes së Failover Cluster Sql Te Serverave;*
*-Raportim i Sistemit të Backup;*
*-Probleme të Verifikuara gjatë Kontrolleve Periodike të Shërbimeve Infrastrukturore.*

**Për sa është trajtuar në këtë pikë të Projekt Raportit, janë paraqitur observacione me shkresën nr. 1502/4 prot., datë 21.05.2024 protokolluar në KLSH me nr. 1138/7, datë 24.05.2024.**

**Pretendimi i subjektit:**
Na lejoni t'ju bëjmë me dije se sikurse kemi paraqitur dhe në observacionin mbi akt konstatimin nr.2 datë 29.03.2024, komisioni i ngritur me urdhrin e Titullarit të Autoritetit Kontraktor për mbikëqyrjen e kontratës ka mbajtur procesverbale çdo muaj, pas kontrollit dhe verifikimit të shërbimeve të mirëmbajtjes mujore të paraqitura nga kontraktori nëpërmjet raporteve periodike mujore dhe është marrë në dorëzim shërbimi në përputhje me specifikimet teknike dhe kushtet e kontratës. Në vijim do merren masa për të përditësuar formatin e këtij procesverbali me elementet e përmendura me sipër.

**Qëndrimi i grupit të auditimit**
Sqarojmë se konstatimi i grupit të auditimit është për periudhën objekt auditimi, për të cilën ju rikujtojmë se ashtu sic kemi sqaruar nw projekt raport nga dokumentacionet e vëna në dispozicion dhe nga komunikimet verbale me përfaqësuesit ë AKSHI-t të atashuar në MSHMS, nuk ka pasur asnjë raport periodik mbi zbatimin e kontratës.

## 2.2 Auditimi i sigurisë së informacionit

Auditi i Sigurisë së Informacionit është një proces i vlerësimit të sigurisë së informacionit në Institucion për të identifikuar dhe adresuar rreziqet dhe incidentet e mundshme. Ky proces ndihmon Insitucionet të sigurojnë që të dhënat dhe informacioni të jenë të mbrojtur dhe të sigurtë, të përmbushin kërkesat e ligjeve dhe standardeve të sigurisë së informacionit, dhe të rrisin ndërgjegjësimin e punonjësve të Institucioneve rreth sigurisë së informacionit dhe rreziqeve të mundshme. Auditimi i sigurisë së informacionit identifikon sfidat dhe rreziqet e mundshme në nivelin e sigurisë së informacionit dhe ndihmon në zhvillimin e strategjive për t'i përballuar ato. Në të njëjtën kohë, ai identifikon politikat dhe procedurat e sigurisë së informacionit dhe vlerëson se a janë ato të përshtatshme dhe të ndjekura me përpikëri nga punonjësit e Institucionit. Çdo institucion publik shtetëror që ofron shërbime ndaj qytetarëve e ka si detyrim ndërtimin e programit të sigurisë së informacionit me elementët kyç të cilët janë: "Mjedisi i sigurisë së informacionit, Vlerësimi i riskut, Politikat e sigurisë, Organizimi i sigurisë së TI, Menaxhimi i komunikimeve dhe operacioneve, Menaxhimi i aseteve, Siguria e burimeve njerëzore, Siguria fizike dhe mjedisore, Kontrolli i aksesit, Menaxhimi i incidenteve të sigurisë së TI".

**Verifikimi në terren i Drejtorive rajonale të SHSSH**

Nga verifikimi në terren në Drejtorinë rajonale të SHSSH Shkodër dhe SHSSH Vlorë, grupi i auditimit konstatoi se:

*-Infrastruktura network e pajisjeve ndihmëse që nevojiten për shërbimet e komunikimit dhe ruajtjes së të dhënave është në kushtet jo optimale, ku shërbimet e ngritura mbi këto rrjete nuk janë të sigurta dhe nuk mbështesin vazhdimësinë e punës.*

*-Nuk ka një linjë back up interneti në rast të shkëputjes së linjës, duke sjellë kështu mosfunksionim të sistemit dhe ndërprerje të ofrimit të shërbimeve.*

*-Kompjuterat nuk janë të pajisur me antivirus për mbrojtje ndaj sulmeve.*

*-Nuk ka një server qendror të pajisur me Domain Controller për menaxhimin e përdoruesve dhe vendosjen e politikave të sigurisë.*

*–Nuk kanë një pajisje firewall për mbrojtjen e rrjetit nga sulmet e jashtme*.

**Siguria e të dhënave dhe vazhdimësia në ofrimin e shërbimit**

Procedurat e Backup që realizohen për të tre sistemet janë të kategorizuara në 3 nivele:
a. Backup në nivel baze të dhënash;
b. Backup në nivel aplikacioni;
c. Backup në nivel File-sh Serveri.
Secila procedurë backup-i është individuale dhe nuk afekton apo nuk afektohet nga të tjerat. Nisur nga kjo e fundit minimizohet risku i problematikave që mund të çojnë në dështim total të sistemit dhe njëkohësisht mbrohen të gjithë komponentët në varësi të nivelit të kritikalitetit të gjithsecilit. Për realizimin e procedurave të backup përdoren mjete automatike dhe më konkretisht mekanizmi System Center 2022 Data Protection Manager, i cili është i ngritur në një server fizik. Të gjithë procedurat e backup realizohen automatikisht sipas konfigurimeve dhe skedulimeve të përcaktuara të cilat janë implementuar në raport të drejtë me nivelin e kritikalitetit të komponentes përkatëse (aplikacion, bazë të dhënash, sistem operimi ).
*Nga audtimi u konstatua se kontraktuesit nuk i është caktuar niveli i aksesit nga Institucioni përfitues dhe shfrytëzues i sistemit për aksesimin e të dhënave. Hapat që ndiqen për kryerjen e backup-it kryhen sipas politikave të kontraktuesit.*

***Mbi verifikimin e dokumentimit të planeve për vazhdueshmërinë e biznesit dhe rimëkëmbjes nga katastrofat***
Auditimi mbi ofrimin e Vazhdimësisë së ofrimit të shërbimeve u bazua mbi VKM nr. 710, datë 21.08.2013 "Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit", i ndryshuar, risqeve të identifikuara dhe praktikave më të mira. Referuar kësaj VKM-je: "Çdo institucion i cili ka ose do të zhvillojë sisteme në fushën e teknologjisë së informacionit, që ofron shërbime për qytetarët, për biznesin dhe për ndërveprim e shkëmbimit të informacionit për administratën publike nëpërmjet sistemeve elektronike, duhet të parashikojë dhe të realizojë investime për krijimin e sistemit të vazhdueshmërisë së punës (Business Continuity) dhe sistemit të ruajtjes së informacionit (Backup), me qëllim mundësimin e ofrimit të shërbimit pa ndërprerje dhe parandalimin e humbjes ose të shkatërrimit aksidental të të dhënave". Në këtë VKM cilësohet gjithashtu edhe dokumentimi i politikave mbi planin e vazhdueshmërisë së punës dhe rikuperimit nga katastrofat, si dhe të bëhet i mundur evidentimi i sistemeve të cilat janë kritike për ofrimin e shërbimit 24/7. Qëllimi i menaxhimit të vazhdimësisë është të mirëmbahen kërkesat e vazhdimësisë së institucionit. Menaxhimi i vazhdimësisë përfshin rishikimin periodik dhe azhornimin e afatit të rimëkëmbjes për të siguruar që ato janë në përputhje me Planet e Vazhdimësisë së Biznesit. Vazhdueshmëria a biznesit (BCP) është procesi që një institucion ndjek për të planifikuar dhe testuar rimëkëmbjen e operimit të saj pas një ndërprerjeje.
*Nga auditimi u konstatua se AKSHI nuk ka ofruar një infrastrukturë BCC (Business Continuity Center) për SHSSH, në kundërshtim me VKM nr. 710, datë 21.08.2013 "Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit", pika 1 dhe VKM Nr. 673, datë 22.11.2017 "Për riorganizimin e Agjencisë Kombëtarë të Shoqërisë së Informacionit", i ndryshuar*
*-nuk ka bërë të mundur evidentimin e sistemeve kritike për ofrimin e shërbimit 24 orë në 7 ditë të javës.*

**Verifikimi i shkallës së sigurisë fizike dhe aksesit në rrjet.**

Verifikimi i shkallës së sigurisë së dhomës së serverave me qëllim parandalimin e humbjes ose të dëmtimit të pajisjeve kompjuterike, aksesit të paautorizuar, kopjimit ose shikimit të informacionit sensitiv. Auditimi mbi shkallën e sigurisë së dhomës së serverave u krye në bazë të manualit të auditimit IT, ISSAI 5310 dhe ISO 27001.
Shërbimi Social Shtetëror ka një ambient në të cilën ruhen pajisjet e rrjetit si modema me fibër optike dhe switch switch D-link layer 3 , i cili shërben dhe si router. *Nga auditimi u konstatua*

*se ambienti fizik i ruajtjes së pajisjeve të rrjetit nuk plotëson kushtet minimale të sigurisë, si ftohja ,lagështira e ajrit, sistemi elektrik, dera e aksesit në ambient.*
*Nga auditimi i nfrastrukturës network të SHSSH u konstatua se të gjithë përdoruesit mund të shohin listën e printerave dhe kompjuterave në lidhjen LAN, që tregon një mungesë të segmentimit të rrjetit ose kontrolleve të aksesit. Kjo ekspozon burimet e ndjeshme të rrjetit ndaj përdoruesve të paautorizuar dhe rrit rrezikun e aksesit të paautorizuar, shkeljeve të të dhënave dhe aktivitetit keqdashës.*

**Për sa është trajtuar në këtë pikë të Projekt Raportit, janë paraqitur observacione me shkresën nr. 1502/4 prot., datë 21.05.2024 protokolluar në KLSH me nr. 1138/7, datë 24.05.2024.**

**Pretendimi i subjektit:**
Na lejoni t'ju bëjmë me dije se ashtu siç kemi sqaruar edhe përgjigjet e dërguara mbi akt konstatimin nr.2 datë 29.03.2024, për sa i përket politikave të vazhdueshmërisë së punës dhe rikuperimit nga katastrofat, nga ana e AKSHI-t, në zbatim të percaktimeve ligjore të parashikuara në Ligjin nr. 43/2023 "Për Qeverisjen Elektronike", është miratuar Udhëzimi nr.1 datë 31.07.2023 "Për Zbatimin e Dokumentit të Përditesuar të Politikave të Vazhdimësisë së Punës dhe Planit për Ruajtjen e Informacionit", i përcjellë më parë drejt jush. Kërkojmë nga grupi i auditimit të mbahet në konsideratë egzistenca e këtij dokumenti të miratuar i cili është i publikuar edhe në faqen e AKSHI-t dhe se dokumentet të cilët grupi i ka cilësuar si të munguar, janë në proces rishikimi, në përputhje edhe me përcaktimet që bën Udhëzimi i sipërcituar.
Gjithashtu na lejoni të sjellim në vëmendjen e grupit të auditimit se vizioni i institucionit drejt qëndërzimit të infratrukturave dhe komponenteve të tjera ka rezultuar deri me tani efektiv dhe me perfitim në aspektin e kostove. Ky qëndërzim përfshin të gjithë komponentët ku një ndër të cilët është dhe vazhdimësia e punës. Në këto kushte vleresojmë se rekomandimi për të ngritur një qendër BCC vetëm për shërbimet e SHSSH do të ishte një rast përjashtimor dhe do të sillte një kosto të lartë për buxhetin. Duke vlerësuar objektivitetin dhe rëndësinë e rekomandimeve të lëna nga grupi do të kërkonim nëse është e mundur rishikimin e këtij rekomandimi për ta bërë atë më të zbatueshëm dhe me qëllimin përfundimtar reduktimin e kostove duke mbajtur një balancë kosto/përfitim
**Qëndrimi i grupit të auditimit**
Nga observacionet i dërguar nuk ka një dokument shoqërues , justifikues në të cilën instituiconi përfitues të ketë caktuar kërkesa në lidhje me backup-in e të dhënave. Ngritja e infrastrukturës kritike eshte detyrim ligjor sipas VKM Nr.710 datë 21.08.2013 "Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdiumësisë së punës dhe marrëveshjeve të nivelit të shërbimit", i ndryshuar". Për sa më sipër grupi mban ttë njëjtin qëndrim.

**3.Auditimi i sistemeve mbi të dhënat Input / Output.**

Shërbimi Social Shtetëror është institucioni përdorues i tre sistemeve NE, PPAK dhe SHKSH. Te tre sistemet kanë një shtrirje gjeografike në të gjithë Shqipërinë, Operohet në të 12 Qarqet e Republikës së Shqipërisë, në të 61 Bashkitë e saj si dhe në 383 Njësitë Administrative. Në secilën prej këtyre drejtorive, është emëruar një IT, përgjegjës për mbarëvajtjen e punës së përdoruesve të sistemeve, të cilët sigurojnë që çdo Punonjës Social, Administrator Shoqërore, Vlerësues, Mjek, Vendimmarrës, sipas roleve të secilit në Sistem, të kryejë të gjithë aktivitetet regjistruese, vlerësuese dhe vendimmarrjeje për ekzekutimin e pagesave të ndihmës ekonomike, pagesave te aftësisë së kufizuar dhe Shërbimet Sociale përkatëse për të gjithë njerëzit në nevojë në të gjithë Shqipërinë.

**Sistemi i Ndihmës Ekonomike** përdoret në 383 njësi vendore në te gjithë Republikën e Shqipërisë dhe ka aktualisht 838 përdorues aktiv. Numri i institucioneve që e përdorin këtë sistem është 463, ku përfshihen (Njësitë Administrative, Bashki, Drejtori Rajonale, Drejtori e Përgjithshme e Shërbimit Social) Me të mund të kryhen të gjitha veprimet e lidhura me ndihmën ekonomike.

Sistemi i Ndihmës Ekonomike aksesohet nga dy tipe përdoruesish. Përdoruesi i parë është punonjës në njërin prej institucioneve të konfiguruara në sistem. Ai mund të aksesojë aplikacionin web të Ndihmës Ekonomike nëpërmjet një web browser-i. Përdoruesi i dytë është administrator i sistemit SharePoint, me të cilin vepron sistemi i Ndihmës Ekonomike.

Të gjithë përdoruesit e sistemit, e aksesojnë atë nëpërmjet shfletuesit të Internetit duke përdorur shërbimin VPN të ofruar nga AKSHI. Sistemi ofron një zgjidhje të qendërzuar që është e orientuar drejt punës dhe ofron një platformë të plotë për automatizimin e proceseve.

**Sistemi i SHKSH-se** përdoret në 61 Bashkitë në të gjithë Republikën e Shqipërisë dhe ka aktualisht 1037 përdorues aktive. Numri i institucioneve që e përdorin këtë sistem është 485, ku përfshihen (Njësite Administrative, Bashki, Drejtori Rajonale, Drejtori e Përgjithshme e Shërbimit Social, OJF dhe institucione të tjera publike dhe private që ofrojnë përkujdesje shoqërore për grupet vulnerabile, si të moshuarit, gratë e dhunuara dhe fëmijët e braktisur)

**Sistemi PPAK** ka aktualisht 1030 përdorues aktive. Numri i institucioneve qe e përdorin këtë sistem është 415, ku përfshihen (Njësitë Administrative, Bashki, Drejtori Rajonale, Drejtori e Përgjithshme e Shërbimit Social). Sistemi PPAK është i shpërndarë në te gjithë Republikën e Shqipërisë, Njësitë Vendore, në të 12 Drejtoritë Rajonale të Shërbimit Social Shtetëror dhe në Drejtorinë e Përgjithshme të Shërbimit Social Shtetëror.

**Sistemi NE**

Qëllimi bazë i MIS-NE ka qenë përmirësimi i efektivitetit të mbrojtjes sociale duke:

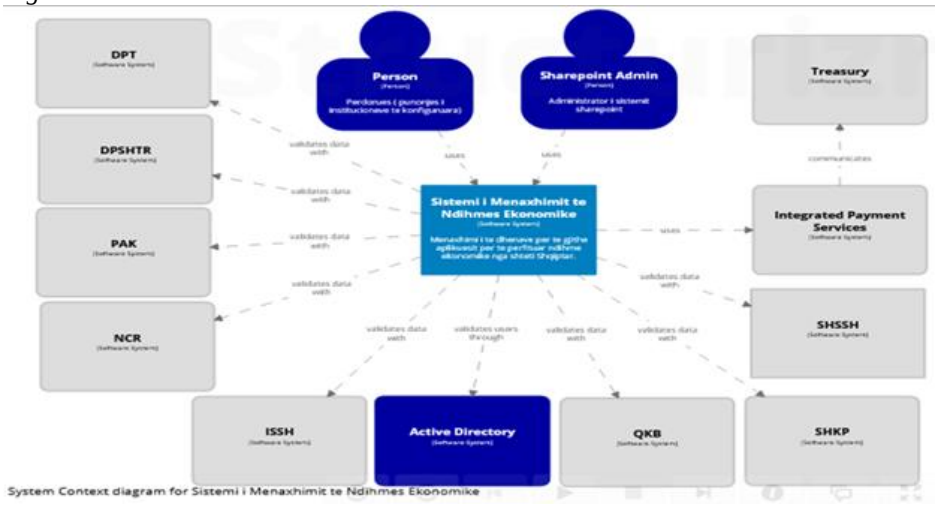
- Identifikuar në mënyrë sa më të saktë familjet/individët që kanë nevojë për ndihmë ekonomike.
- Përmirësuar kapacitetet për planifikimin, menaxhimin dhe dhënien e Ndihmës Ekonomike.
- Shkëmbyer në kohë reale informacion për verifikimin e të dhënave të aplikuesve për ndihmë ekonomike.
- Përmirësuar kapacitetet për monitorimin e Ndihmës Ekonomike dhe Administratës.
- Përjashtuar rastet abuzive nga skema e Ndihmës Ekonomike.
- Bashkërenduar cilësinë e proceseve përmes menaxhimit të çështjeve
- Mbështetur ndërveprimin e automatizuar të të dhënave nëpër Zyrat Rajonale dhe Lokale të Shërbimit Social dhe Agjencive/Institucioneve të tjera shtetërore.

Sistemi i menaxhimit të Ndihmës Ekonomike ka këto komponentë:

- Modulet për menaxhimin e Ndihmës Ekonomike (me procese të automatizuara për çdo rol)
- Modulin e raporteve
- Modulin e integrimeve dhe verifikimeve me sisteme te tjera nëpërmjet ESB
- Modulin e gjurmimit të auditimeve

- Modulin e administrimit të sistemit

Konteksti në të cilin vepron ky sistem paraqitet në figurën më poshtë:
*Fig nr.1*




Sistemi operativ është Microsoft WindoWs Server 2012 R2, etj sipas tabelës me poshtë. Baza e të dhënave e përdorur është SQL Server 2014 (Enterprise Edition). Aplikimi është ngritur mbi Sharepoint Server 2013, dhe ndërtuar mbi .NET 4.0. Për infrastrukturën Data Warehouse është përdorur SQL Server 2016 (Enterprise Edition) dhe SQL Server Integration Services.
Të gjithë komponentët kanë "role-based security" dhe administrim të përdoruesve që lejon krijimin e kategorive të ndryshme të përdoruesve dhe nivel të diferencuar aksesi tek të dhënat sipas grupeve dhe kredencialeve të dhëna nga administratori.

Sistemi i Ndihmës Ekonomike është dizenjuar dhe programuar bazuar në legjislacionin në fuqi dhe me konsulencën e Bankës Botërore.Sistemi është "web-based" dhe si i tillë nuk ka kufizime gjeografike. Nga ana organizative sistemi përfshin Njësitë Vendore të ndihmës ekonomike pranë bashkive dhe komunave, drejtoritë rajonale të Shërbimit Social Shtetëror, Drejtorinë e Përgjithshme të Shërbimit Social Shtetëror dhe Ministrinë e Shëndetësisë dhe Mbrojtjes Sociale. Nga ana funksionale, sistemi përfshin procedura specifike të procesit të ndihmës ekonomike duke filluar nga kriteret dhe dokumentet e nevojshme për aplikim, validimi dhe verifikimi i të dhënave me sistemet e tjera, llogaritja e masës së përfitimit në bazë të kushteve të caktuara, etj.
Në bashkësinë e brendshme "Internal" ndodhen modulet kryesore të tij. Diagrama e mëposhtme është një paraqitje vizuale e infrastrukturës logjike/arkitekturore të sistemit të Ndihmës Ekonomike. Kjo diagramë e arkitekturës së sistemit tregon ndarjen e moduleve kryesore të sistemit si dhe veçon pjesën e moduleve të brendshme nga nyjet e jashtme.
Sistemi Ndihmës Ekonomike është i bazuar në platformën Microsoft SharePoint Server. Në këtë platformë hostohet në formën e "SharePoint Site".
Të tre modulet bazë ndërveprojnë me modulin e data bazës për aksesimin e të dhënave. Shtresa e aplikimit komunikon me modulin "Active Directory" ose me modulin "Authentication Provider" si pjesë e sigurisë dhe autorizimit në sistem.
Sistemi ndërvepron me sisteme të tjera, si sistemet e DPSHTRR, QKB, ISSH, DPT, RKGJC, PPAK, AKPA (SHKP), SHKSH, Thesary nëpërmjet Platformës Qeveritare të Ndërveprimit (ESB GovNet).
Komponentet në SharePoint përbëjnë një pjesë të rëndësishme të sistemit. Ato janë si më poshtë:
- Aplikimet Web

Sistemi SharePoint aktualisht ka dy web aplikime:

-Central Admin Web App: për të menaxhuar sistemin sharepoint, e aksesueshme vetëm nga administratorët e sistemit sharepoint.
-NE Web App: për të hostuar aplikiacionin e NE, i aksesueshëm nga të gjithë institucionet e konfiguruar.

- Sherbimet

Shërbimet e mëposhtme janë aktive në sistemin sharepoint:
- Search service – Për kërkimin dhe indeksimin e dokumentave
- ASP.NET Session State Service – Për menaxhimin e sesionit te përdoruesve

- Sitet

Për ruajtjen e dokumentave ekzistojnë 2 site versione të veçanta:
*ERMS – për ruajtjen e dokumenteve zyrtare*
Dokumentet e regjistruara në ERMS janë vetëm dokumente zyrtare të cilat nuk mund të modifikohen nga përdoruesit. Çdo institucion ka nga një librari të veçantë në ERMS për ruajtën e dokumenteve në mënyre të ndarë për çdo institucion.
*EDMS – për ruajtjen e dokumenteve te përkohshme*
Dokumentet e regjistruara në EDMS janë dokumente të punës së përditshme të zyrave të ndryshme. Çdo zyrë ka librarinë e saj në EDMS ku mund të krijojë, modifikojë dhe fshijë dokumentet e krijuara prej zyrës. Përdoruesit kanë mundësinë që dokumentet e krijuara në EDMS pasi të kenë marre formën përfundimtare mund t'i arkivojnë ato ne ERMS për ruajte si dokumente zyrtare.
Sistemi i Ndihmës Ekonomike është i shoqëruar edhe me dataëarehouse për ruajtjen e të dhënave në mënyrë të përshtatshme për gjenerimin e raporteve analitike. Ky modul përfaqëson rëndësi të veçantë pasi do të ruajë të dhënat e historizuara të sistemit. Burimi i të dhënave për DataËarhouse është baza e të dhënave operacionale. Zgjidhja e implementuar përbëhet nga disa nënkomponentë:

- Nën-komponenti ETL (Extract, Load, Transform) është përgjegjës për çfarëdo agregimi, transformimi apo manipulimi tjetër të të dhënave që kërkohet.
- Paketa e popullimit inkremental të DataËarehouse është dizenjuar për të lexuar vetëm të dhënat e ndryshuara rishtazi në sistemin operacional.
  Popullimi i DataËarehouse realizohet në dy faza, për të minimizuar impaktin mbi performancën e sistemit. *Në fazën e parë* të dhënat lexohen nga sistemi operacional dhe vendosen në një zonë staging, ku struktura e të dhënave ka ndryshime jo-thelbësore krahasuar me databazën e NE. Në këtë zonë ruhen dhe të dhënat e historizuara të sistemit operacional, pasi ai i mbishkruan gjatë përditësimit të të dhënave. Popullimi i zonës staging është ndarë më vete dhe skedulohet të ekzekutohet me një frekuencë më të lartë se popullimi i vetë dataëarehouse. *Në fazën e dytë*, të dhënat lexohen nga zona staging, dhe aplikohen transformimet e shumëfishta për shndërrimin e të dhënave në formën e denormalizuar të përshtatshme për databazën OLAP të dataëarehouse.
  *Një tjetër komponent i zgjidhjes softuerë* te implementuar është edhe Sistemi i integruar i pagesave i cili është i integruar me sistemin e Thesarit (IPS -NE). Ky sistem është bazuar ne Microsoft Dynamics NAV 2017 dhe është përshtatur sipas standardeve të pagesave të Ndihmës Ekonomike (NE). Baza e zgjidhjes se implementuar është një sistem menaxhimi financiar, mbulon edhe administrimin e pagesave të ndihmës ekonomike për përfituesit e saj, si dhe merr informacion në kohë reale nga:
  Sistemit NE – nga i cili merr informacion për të gjithë përfituesit e Ndihmës ekonomike se bashku me informacion të detajuar për ta.
  Sistemi i Thesarit - nga i cili merr informacionin për pagesat e ekzekutuara.
  Ky sistem është i hostuar pranë Datacenterit Qeveritar dhe ne të janë të konfiguruara 61 Bashkitë si ndërmarrje të veçanta, të cilat administrojne të pavaruara buxhetet për përfituesit e ndihmës ekonomike qe i përkasin njësisë së tyre administrative.
  Për infrastrukturën mbështetëse detajet janë dhënë me poshtë në paragrafin 6.4
  Për secilin nga aktorët e listuar sistemi ofron komponentë të veçanta për të realizuar të gjithë funksionalitetet përkatëse.

*Nga auditimi rezultoi se :*

- *Përdoruesit e Sistemeve të Shërbimit Social Shtetëror nuk mund të gjenerojnë dhe eksportojnë raporte.*
- *Sistemet kanë të aktivizuar Copy protection, përdoruesit nuk mund të kopjojnë dot tekstin që u nevojitet nga sistemi duke vonuar përpunimin e informacionit gjatë punës së tyre.*

*Detyra e administratorit të sistemit në rolin e Administratorit të SHSSH nuk është e caktuar me anë të një shkrese zyrtare nga organet drejtuese të MSHMC dhe AKSHI në mënyrë që të përcaktohen qartë të drejtat dhe detyrat e administratorit të sistemit, Nuk disponohet një akt rregullativ i dokumentuar dhe i miratuar për administrimin/menaxhimin e përdoruesve, në të cilën të jenë të përcaktuara procedurat që do të ndiqen për krijimin, fshirjen, ndryshim.*

**Sistemi SHKSH**

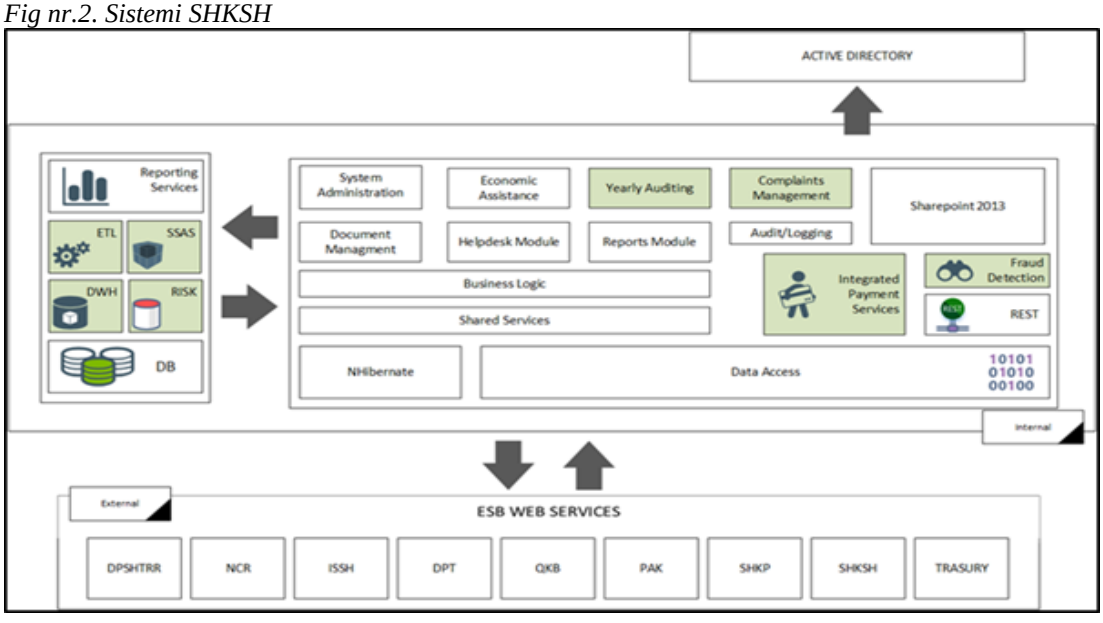
Sistemi i Adminsitrimit të Integruar të Shërbimeve Sociale është i përdorshëm nga 12 drejtori rajonale të Shërbimit Social Shtetëror, Drejtoria e Përgjithshme e Shërbimit Social Shtetëror dhe të gjitha Njësitë e Qeverisjes Vendore në Republikën e Shqipërisë. Qëllimi i sistemit është të mundësojë administrimin e të gjitha informacioneve të Shërbimeve Sociale si edhe të publikojë on/off-line të gjithë informacionin e nevojshëm për bashkëveprim me qytetarët dhe struktura të tjera të lidhura me të.

Sistemi i Administrimit të Integruar të Shërbimeve Sociale ka këto komponentë:

- Moduli i identifikimit dhe referimit te rasteve;
- Moduli i trajtimit të rasteve;
- Moduli i monitorimit dhe vlerësimit periodik;
- Moduli i administrimit të proceseve të punës;
- Moduli i Gjenerimit të Raporteve Statistikore, të Monitorimit dhe Performancës së Proceseve;
- Moduli i Ndërveprimit me sistemet e tjera dhe ndërveprimit të brendshëm;
- Moduli i Regjistrit të Legjislacionit (për Portalin Intranet);
- Moduli i Regjistri të institucioneve partnere të Shërbimeve Sociale (për Portalin Intranet)
- Moduli Web-GIS;

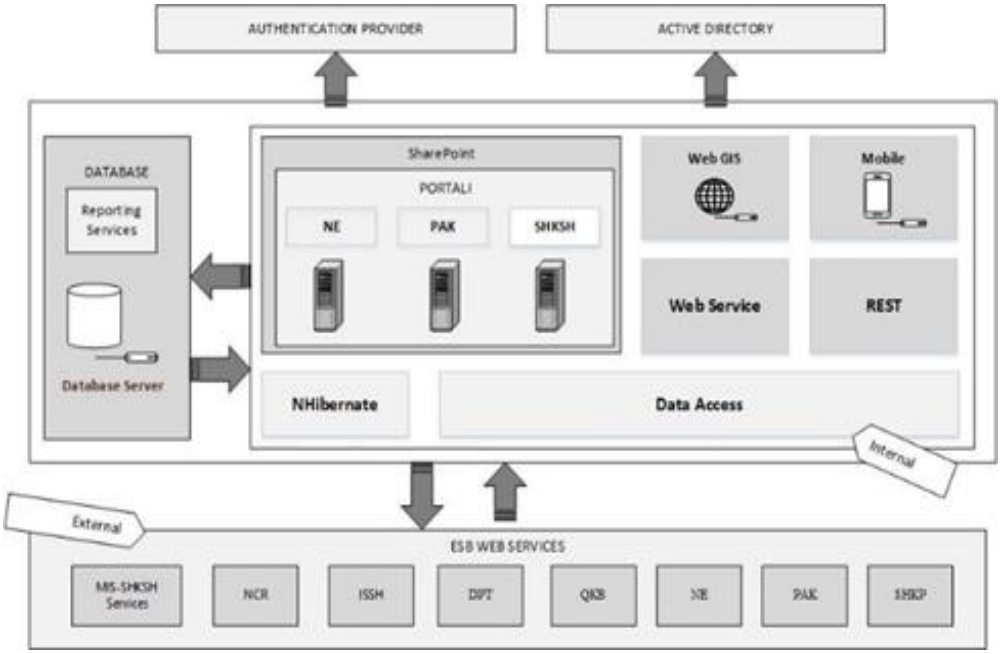
Ashtu si sistemi i Ndihmës Ekonomike aplikimi është ngritur mbi Sharepoint Server 2013, dhe ndërtuar mbi .NET 4.0. Baza e të dhënave e përdorur është SQL Server 2014 (Enterprise Edition). Për infrastrukturën Data Ëarehouse është përdorur SQL Server 2016 (Enterprise Edition) dhe SQL Server Integration Services.

*Fig nr.2. Sistemi SHKSH*



Sistemi i Administrimit të Integruar të Shërbimeve Sociale është konceptuar si një sistem web i aksesueshëm nga të gjithë përdoruesit pa patur nevoje për instalimin e ndonjë programi specifik ne kompjuterat e tyre. Ai është i ndërtuar me Microsoft Asp.Net Web Forms. Sistemi përdor Nhibernate si ORM.
Zgjidhja për portalin e integruar përdor Sharepoint 2013. Përdoruesi ka mundësi të aksesojë informacionin e portalit duke u loguar vetëm një herë në portal nëpërmjet kredencialeve përkatëse. Pra, me një logim përdoruesit pakësojnë dhe informacionin ne sistemet NE dhe PAK.
Moduli web GIS përdor si shtrese baze harta administrative/ortofoto, të cilat merren nga ASIG nëpërmjet shërbimeve ËMS të publikuar në portalin e tyre. Moduli Web shfaq informacion hapësinor në Web duke përdorur standardeve Web Map Service (ËMS), Web Feature Service (ËFS) dhe Web Coverage Service (ËCS).
Aplikacioni mobile perdor CodeName One. Komunikimi me shërbimet e ofruara nga sistemi backend kryhet me REST dhe formati i përdorur është JSON. Protokolli i përdorur ne komunikim është HTTPS, me certifikatë të vlefshme.
Pamje e komponentëve të përshkruar më lart paraqitet në figure

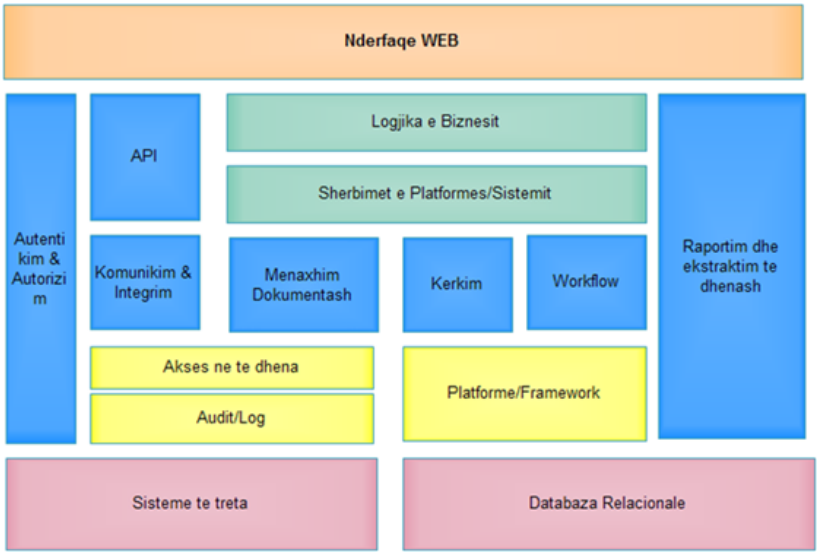
*Fig.nr 3.Komponentët*




**Sistemi PPAK**
Sistemi i menaxhimit të proceseve të PPAK është regjistri elektronik i personave me aftësi të kufizuar (PAK), të invalidëve të punës dhe kujdestarëve PAK. Ai ka dixhitalizuar historikun e praktikave ekzistuese nëpërmjet krijimit të një arkive elektronike.

Sistemi komunikon me Regjistrin e Gjendjes Civile, për të dhënat personale e familjare të personit dhe kujdestarit dhe me Sistemin e Sigurimeve Shoqërore, ku kontrollon nëse një aplikues i PAK ka paguar sigurime shoqërore. Sistemin e Drejtorisë së Përgjithshme të Tatimeve dhe sistemin e SHKP. Sistemi është i integruar edhe me *Active Directory (govnet)* për identifikimin dhe autentifikimin e përdorueseve.

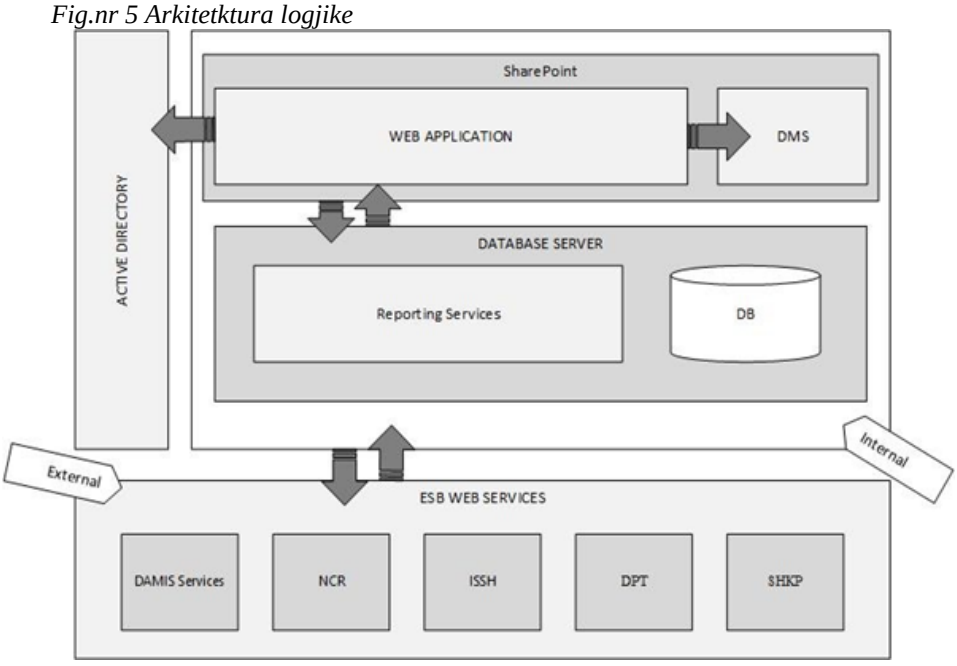
*Fig.nr 4. Sistemi PPAK*




Në nivel prezantimi ndërfaqja web e përdoruesve përmban PPAK web application që përfaqëson faqen e aksesueshëm nga të gjithë përdoruesit të institucioneve të konfiguruara. Ai ka ndërfaqe të veçantë për administratorin.

Arkitektura logjike e sistemit është:

*Fig.nr 5 Arkitetktura logjike*




Në bazën e të dhënave të këtyre tre sistemeve ruhen gjurmët e auditimit (audit trail) për veprimet e kryera nga përdoruesit, por nuk ekzistojnë procedura për analizimin e këtyre gjurmëve Teknologjitë në të cilat bazohet sistemi i PPAK janë ASP.NET, SharePoint 2013, Microsoft SQL Server.

*Nga auditimi mbi sistemet rezultoi se :*

- *Të gjithë sistemet janë të lidhura me active direktorinë e AKSHI-t, përdoruesit përdorin në sisteme të njëjtin password që përdorin në email., kjo sjellë risk pasi nëse një sistem është i kompromentuar, të gjithë sistemet komprometohen.*

- *Sistemet e Ndihmës Sociale nuk kanë komunikim me webservice me ASHK, duke sjell rrisk në vlerësimin e gabuar të kërkesave për ndihmë ekonomike.*
- *Manualet e përdorimit të moduleve të sistemeve nuk janë të përditësuara.*
- *Nga auditimi u konstatua se Shërbimi Social Shtetëror nuk disponon përdoruesin me të drejta të plota – db Owner, megjithëse është përgjegjëse për të dhënat që hidhen në sistemet informatike.*
- *Nga auditimi i përdoruesve të sistemeve (NE, PAK, SHKSH) u konstatua se ka përdorues aktiv me emër useri të pa Identifikuar.*
- *Nga auditimi i përdoruesve të databasës u konstatua se ekzistojnë një numër përdoruesish por nuk është kryer një ndarje privilegjesh për çdo përdorues sipas niveleve në bazë të detyrave që ata kanë.*

  *Nga auditimi u konstatua se Shërbimi Social Shtetëror nuk ndjek një politikë të përcaktuar për analizimin e gjurmëve të auditimit për veprimet që kryejnë përdoruesit në Sistemin e NE, PAK, SHKSH.*

**Për sa është trajtuar në këtë pikë të Projekt Raportit, janë paraqitur observacione me shkresën nr. 1502/4 prot., datë 21.05.2024 protokolluar në KLSH me nr. 1138/7, datë 24.05.2024.**

**Pretendimi i subjektit:**

Na lejoni t'ju bëjmë me dije se kontratat që lidhen për mirëmbajtjen e sistemeve kanë të përcaktuara të gjithë detyrimet dhe përgjegjësitë e palëve që lidhin kontratën. Në këtë kuptim, veprimtaria dhe detyrat që duhet të kryejë secila prej palëve të kontratës është parashikuar me nënshkrimin e saj, pjesë integrale e të cilës janë dhe termat e referencës që paraqesin detajet teknike të procedurës. Në këto kushte, niveli i aksesit për çdo kontratë apo sistem, atribuohet në përputhje me detyrimet kontraktuale.

Në lidhje me rekomandimin nr. 2 na lejoni t'ju bëjmë me dije se lidhur me këtë rekomandim të grupit të auditimit, përgjegjësitë dhe të drejtat e përdoruesve janë tëparashikuara në Rregulloren e Sigurisë së Informacionit nr. 2, datë 06.11.2023 "Për sigurinë e Informacionit", ku paraqiten qartë elementet e ndarjes së privilegjeve dhe detyrave të përdoruesve. Në këto kushte, në vleresimin tonë, përcaktimi i këtyrë përgjegjësive dhe detyrimeve në një rregullore gjithëpërfshirëse është me efektive sesa përcaktimi i tyre rast pas rasti, duke marrë parasysh që punonjësit e institucioneve janë në lëvizje të vazhdueshme dhe një praktike e tillë do të bënte të vështirë ndjekjen në vijimesi dhe përditesimin e akteve, ndërkohë që një rregullore është me robuste dhe me gjithëpërfshirëse.

Në lidhje me rekomandimin nr. 4.1 Na lejoni t'ju saktësojmë se është aktualisht i implementuar teknikisht webservice përkatës me Sistemin elektonik të ASHK i ngritur për marrjen e të dhënave por në mungesë të digjitalizimit të plotë të të gjithë të dhënave të Agjencisë Shtetërore të Kadastrës, për të patur një informacion të saktë, Shërbimi Social Shtetëror mund të komunikojë më vetë institucionin e ASHK për të patur akses në Modulin që ky institucion ka vendosur në dispozicion pikërisht për institucionet shtetërore.

Theksojmë se përgjegjës për të dhënat dhe administrator i tyre është institucioni i ASHK-së dhe sa konstatuar në këtë rekomandim është përtej AKSHI dhe çfarë mund të beje ai në këtë proces. Kjo duhet adresuar nga institucioni ofrues i shërbimit të Ndihmës Ekonomike.

Lutemi që ky sqarim i bërë nga ana jonë të merret në konsideratë nga grupi i auditimit përpara hartimit të raportit përfundimtar të auditimit.

**Qëndrimi i grupit të auditimit**

-Nga observacion i dërguar nuk ka një dokument shoqërues , justifikues në të cilën instituiconi përfitues të ketë caktuar kërkesa në lidhje me backup-in e të dhënave.

Për sa më sipër grupi i auditimit mban të njëjtin qëndrim..

-Në lidhje me rekomandimin nr. 2 grupi i auditmit eshhtë në dijeni të Rregullores së Sigurisë së Informacionit nr. 2, datë 06.11.2023 "Për sigurinë e Informacionit, por nga situata e sqaruar në Projekt Raport arrijmë në konkluzionin që ajo nuk është zbatuar.
- Në lidhje me rekomandimin nr. 4.1 jemi adresuar Akshit dhe SHSSH për zbatimin e Këtij rekomandimi pasi Akshi është Institucioni që merr në dorëzim mirëmbajtjet e sistemeve dhe SHSSH është Institucioni që zotërron këto Sisteme.

**IV. REKOMANDIME**

**B. MASA ORGANIZATIVE**

**1. Gjetje nga auditimi:** Nga auditimi u konstatua se struktura TI e SHSSH ende nuk ka kaluar si pjesë e strukturës së AKSHI-t sipas përcaktimeve dhe afateve të vendosura në VKM Nr. 673, datë 22.11.2017, "*Për riorganizimin e Agjencisë Kombëtarë të Shoqërisë së Informacionit*", i ndryshuar.
*(Më hollësisht trajtuar në pikën 2.1 faqet 9-13 të Raportit Përfundimtar të Auditimit*
**1.1.Rekomandimi:** Organet drejtuese të Shërbimit Social Shtetëror të analizojnë dhe vlerësojnë situatën për marrjen e masave për kalimin e strukturave përgjegjëse TIK tek AKSHI në zbatim të dispozitave ligjore në fuqi.

*Menjëherë dhe në vijimësi*

**2.Gjetje nga auditimi:** Nga auditimi rezultoi se nuk ka propozime konkrete nga niveli menaxherial i SHSSH për zhvillimin e trajnimeve dhe se nuk është i dokumentuar procesi i kërkesave, nevojave dhe analizimi i tyre për kualifikime profesionale, duke mos plotësuar kështu nevojat për trajnim mbi sistemet, sigurinë dhe teknologjinë e informacionit.
- Në Drejtoritë Rajonale të Shërbimit Social Shtetëror Shkodër dhe Vlorë u konstatua se specialistët e TI në këto drejtori nuk kanë kryer trajnime profesionale brenda dhe jashtë vendit të cilat do ti shërbenin stafit për kualifikime të mëtejshme për ti ndihmuar në kryerjen e detyrave funksionale të përcaktuara në përshkrimet e tyre të punës.
*(Më hollësisht trajtuar në pikën 2.1 faqet 9-13 të Raportit Përfundimtar të Auditimit*
**2.1.Rekomandimi:** Shërbimi Social Shtetëror të marrë masa për identifikimin e nevojave për trajnime profesionale teknike të punonjësve të Teknologjisë së Informacionit, si një mënyrë që nxit dhe përmirëson kryerjen e detyrave me nivel të lartë profesional.

*Menjëherë dhe në vijimësi*

**3. Gjetje nga auditimi:** Nga auditimi u konstatua se Teknologjia e Informacionit në SHSSH zhvillohet në kushtet e mungesës së bazës rregullatore. SHSSH nuk ka marrë masa për hartimin e rregullave dhe procedurave të proceseve të teknologjisë se informacionit në përputhje me aktet ligjore, nënligjore dhe praktikat më të mira, duke mos konsideruar elementë të tillë si: rregulla mbi veprimtarinë e TI në institucion; rregulla mbi menaxhimin e incidenteve; procedura dhe indikatorë të matjes së performancës për gabimet/ incidentet e ndodhura dhe masat reaguese ndaj tyre; struktura kontrolli për verifikimin e efektivitetit të ndryshimeve të kryera; procedura për ndryshimet emergjente si dhe dokumentimin e të gjithë procesit të ndryshimeve. Mungesa e bazës së brendshme rregullatore për funksionimin e strukturave të teknologjisë së informacionit sjell operimin mbi baza ngjarjeje dhe jo sipas procedurave të përcaktuara, duke rritur riskun e ekspozimit të institucionit ndaj situatave ku reagimi është i paidentifikuar, burimet njerëzore dhe përgjegjësitë të paalokuara, si dhe koha e përgjigjes e papërcaktuar.
*(Më hollësisht trajtuar në pikën 2.1 faqet 9-13 të Raportit Përfundimtar të Auditimit*
**3.1.Rekomandimi:** Shërbimi Social Shtetëror të marrë masa për hartimin e një Rregulloreje të

Përgjithshme mbi Teknologjinë e Informacionit duke marrë në konsideratë vendosjen e kontrolleve të brendshme lidhur me menaxhimin e riskut, përputhshmërinë me procedurat dhe rregullat e brendshme aktuale të shoqërisë si dhe me legjislacionin e Teknologjisë së Informacionit dhe Komunikimit në Shqipëri.

*Në vijimësi*

**4. Gjetje nga auditimi:** Nga auditimi u konstatua se Shërbimi Social Shtetëror nuk ka hartuar regjistër risku lidhur me teknologjinë e informacionit dhe se nuk janë dokumentuar risqet e identifikuara për periudhën objekt auditimi, si rreziku i biznesit që lidhet me përdorimin, pronësinë, operimin, përfshirjen, ndikimin dhe adoptimin e TI në SHSSH.
*(Më hollësisht trajtuar në pikën 2.1 faqet 9-13 të Raportit Përfundimtar të Auditimit*
**4.1.Rekomandimi:** Shërbimi Social Shtetëror të marrë masa për identifikimin dhe analizimin e risqeve për Teknologjinë e Informacionit me qëllim analizimin dhe vlerësimin e risqeve dhe përmbushjen e objektivave të institucionit.

*Menjëherë*

**5. Gjetje nga auditimi:** Nga auditimi u konstatua se Sektori i Auditit të Brendshëm në SHSSH për periudhën 01.01.2021-31.12.2023 nuk ka kryer asnjë auditim mbi sistemet e teknologjisë së informacionit, në kundërshtim Ligjin nr. 114/2015 "*Për Auditimin e Brendshëm në sektorin publik*" nenit 4, pika 6, nenit 9 dhe Standardeve ndërkombëtare për praktikën profesionale të auditimit të brendshëm, standardet ndërkombëtare të auditimit të brendshëm, të pranuara për t'u zbatuar në Republikën e Shqipërisë.
*(Më hollësisht trajtuar në pikën 2.1 faqet 9-13 të Raportit Përfundimtar të Auditimit*
**5.1.Rekomandimi:** Sektori i Auditit të Brendshëm të marrë masa mbi planifikimin dhe kryerjen e auditimeve mbi teknologjinë e informacionit, me qëllim vlerësimin e kontrolleve të menaxhimit në infrastrukturën e TI, në lidhje me ruajtjen e aseteve, integritetin e të dhënave dhe operimin në mënyrë efektive mbi arritjen e objektivave të institucionit.

*Në vijimësi*

**6. Gjetje nga auditimi:** Nga auditimi u konstatua se ndjekësit e kontratave të nivelit të shërbimit nuk mbajnë një procesverbal për të konfirmuar veprimet e kryera në sistem të cilat janë të pasqyruara në raportet mujore të sjella nga kontraktuesi të renditurara si më poshtë:
*-Kontroll i Gjendjes së Failover Cluster;*
*-Kontroll i Gjendjes së Failover Cluster Sql Te Serverave;*
*-Raportim i Sistemit të Backup;*
*-Probleme të Verifikuara gjatë Kontrolleve Periodike të Shërbimeve Infrastrukturore.*
*(Më hollësisht trajtuar në pikën 2.1 faqet 9-13 të Raportit Përfundimtar të Auditimit*
**6.1.Rekomandimi:** Komisioni i marrjes në dorëzim në MSHMS të marrë masa që në të ardhmen të mbajë raporte periodike mbi zbatimin e kontratës, në përputhje me kushtet e veçanta të kontratës si dhe me dispozitat ligjore dhe nënligjore në fuqi.

*Menjëherë*

**7.Gjetje nga auditimi:** Nga auditimi i Infrastrukturës TIK dhe Sigurisë së Informacionit në Drejtorinë qendrore dhe Rajonale të SHSSH Vlorë, Shkodër u konstatua se:
- Në Drejtorinë rajonale të SHSSH (Vlorë, Shkodër) Infrastruktura Network e pajisjeve ndihmëse që nevojiten për shërbimet e komunikimit dhe ruajtjes së të dhënave është në kushtet jo optimale, ku shërbimet e ngritura mbi këto rrjete nuk janë të sigurta dhe nuk mbështesin vazhdimësinë e punës.
- Në Drejtoritë Rajonale (Vlorë, Shkodër) nuk ka një linjë back up interneti në rast të shkëputjes së linjës, duke sjellë kështu mosfunksionim të sistemit dhe ndërprerje të ofrimit të shërbimeve.

Kompjuterat nuk janë të pajisur me antivirus për mbrojtje ndaj sulmeve. Nuk ka një server qendror të pajisur me Domain Controller për menaxhimin e përdoruesve dhe vendosjen e politikave të sigurisë. Nuk kanë një pajisje firewall për mbrojtjen e rrjetit nga sulmet e jashtme
- Drejtoria e Përgjithshme e Shërbimit Social Shtetëror ka një ambient në të cilën ruhen pajisjet e rrjetit si modema me fibër optike dhe switch layer 3 por ambienti fizik i ruajtjes së pajisjeve të rrjetit nuk plotëson kushtet minimale të sigurisë, si ftohja ,lagështira e ajrit, sistemi elektrik, dera e aksesit në ambient.
- Në Infrastrukturën network të SHSSH të gjithë përdoruesit mund të shohin listën e printerave dhe kompjuterëve në lidhjen LAN, që tregon një mungesë të segmentimit të rrjetit ose kontrolleve të aksesit. Kjo ekspozon burimet e ndjeshme të rrjetit ndaj përdoruesve të paautorizuar dhe rrit rrezikun e aksesit të paautorizuar, shkeljeve të të dhënave dhe aktivitetit keqdashës.

*(Më hollësisht trajtuar në pikën 2.2 faqet 13-15 të Raportit Përfundimtar të Auditimit)*

**7.1 Rekomandimi:** SHSSH të marrë masa për pajisjen dhe standardizimin e infrastrukturës IT në Drejtoritë e saj si dhe të marrë masa për hartimin dhe miratimin e një procedure standarde për komunikimin dhe zgjidhjen e problematikave që lindin me Drejtoritë Vendore në lidhje me sigurinë e IT, me qëllim sigurimin e kushteve optimale për ofrimin e shërbimit dhe mbarëvajtjen e punës pa ndërprerje.

*Në vijimësi*

**8.Gjetje nga auditimi**: Nga audtimi u konstatua se kontraktuesit nuk i është caktuar niveli i aksesit nga Institucioni përfitues dhe shfrytëzues i sistemit për aksesimin e të dhënave. Hapat që ndiqen për kryerjen e backup-it kryhen sipas politikave të kontraktuesit në kundërshtim me Udhëzimin nr.1 dt.31.07.2023 "*Për zbatimin e dokumentit të përditësuar të politikave të vazhdimësisë së punës dhe planit për ruajtjen e informacionit*" të AKSHI-t.

*(Më hollësisht trajtuar në pikën 2.2 faqet 13-15 të Raportit Përfundimtar të Auditimit)*

**8.1.Rekomandimi:** SHSSH si Institucion zotërues i të dhënave të sistemeve NE, PAK, SHKSH në bashkëpunim me AKSHIN në kontratat ardhshme të mirëmbajtjes së sistemeve duhet të përcaktojë nivelet e aksesit të Kontraktuesit në sisteme.

*Menjëherë dhe në vijimësi*

**9. Gjetje nga auditimi:** Nga auditimi u konstatua se AKSHI nuk ka ofruar një infrastrukturë BCC (Business Continuity Center) për SHSSH, në kundërshtim VKM Nr. 673, datë 22.11.2017 "*Për riorganizimin e Agjencisë Kombëtarë të Shoqërisë së Informacionit*", i ndryshuar.

*(Më hollësisht trajtuar në pikën 2.2 faqet 13-15 të Raportit Përfundimtar të Auditimit)*

**9.1 Rekomandimi**: Shërbimi Social Shtetëror, në bashkëpunim me AKSHI-n, bazuar në rëndësinë që ka ofrimi i shërbimit pas një fatkeqësie, të ndërmarrin hapat e nevojshëm për ndërtimin e një qendre *Business Continuity.*

*Në vijimësi*

**10..Gjetje nga auditimit:** Nga auditimi u konstatua se Shërbimi Social Shtetëror nuk disponon përdoruesin me të drejta të plota – Db Owner, megjithëse është përgjegjëse për të dhënat që popullojnë sistemet e Ndihmës Sociale. Ky user ka kontroll të plotë mbi një bazë të dhënash, që do të thotë ka aftësinë për të krijuar, modifikuar dhe fshirë objekte brenda bazës së të dhënave.

*(Më hollësisht trajtuar në pikën 2.3 faqet 13-15 të Raportit Përfundimtar të Auditimit)*

**10.1 Rekomandimi:** Shërbimi Social Shtetëror si institucioni përgjegjës i bazës së të dhënave të sistemeve e Ndihmës Sociale, të marrë masat për menaxhimin e bazës së të dhënave, që përmban të gjitha llojet e aksesit në sistemet që ka në përdorim.

*Menjëherë dhe në vijimësi*

**11. Gjetje nga auditimi :** Nga auditimi i përdoruesve të sistemeve të SHSSH u konstatua se
- Detyra e administratorit të sistemit në rolin e Administratorit të SHSSH nuk është e caktuar me anë të një shkrese zyrtare nga organet drejtuese të MSHMC dhe AKSHI në mënyrë që të

përcaktohen qartë të drejtat dhe detyrat e administratorit të sistemit, Nuk disponohet një akt rregullativ i dokumentuar dhe i miratuar për administrimin/menaxhimin e përdoruesve, në të cilën të jenë të përcaktuara procedurat që do të ndiqen për krijimin, fshirjen, ndryshim.
-Nga auditimi i përdoruesve të sistemeve (NE, PAK, SHKSH) u konstatua se ka përdorues aktiv me emër useri të pa Identifikuar.
-Nga auditimi i përdoruesve të databasës u konstatua se ekzistojnë një numër përdoruesish por nuk është kryer një ndarje privilegjesh për çdo përdorues sipas niveleve në bazë të detyrave që ata kanë.
*(Më hollësisht trajtuar në pikën 2.3 faqet 16-23 të Raportit Përfundimtar të Auditimit)*
**11.1 Rekomandimi**: Shërbimi Social Shtetëror në bashkëpunim me AKSHI-n të marrin masa për administrimin e përdoruesve të brendshëm, ku të përcaktohen saktë lidhja e punonjës-user në sistem sipas detyrave të caktuara që ata kanë.

*Menjëherë dhe në vijimësi*

**12.Gjetje nga auditimi** Nga auditimi u konstatua se SHSSH nuk ka hartuar akte rregullatore për menaxhimin e log-eve digjitale ku specifikohen kërkesat për ruajtjen e log-eve përkatëse për çdo sistem/pajisje të institucionit, procedurat e administrimit dhe përgjegjësitë, në kundërshtim me pikën 4 shkronja a) të "*Rregullores për menaxhimin e log-eve digjitale në Administratën Publike*", miratuar me urdhrin nr. 109 datë 10.06.2016 të Drejtorit të Agjencisë Kombëtare për Sigurinë Kompjuterike (ALCIRT).
*(Më hollësisht trajtuar në pikën 2.3 faqet 16-23 të Raportit Përfundimtar të Auditimit)*
**12.1.Rekomandimi:** Shërbimi Social Shtetëror, në bashkëpunim me Agjencinë Kombëtare të Shoqërisë së Informacionit, të marrin masa për rritjen e sigurisë dhe mbrojtjes së të dhënave duke hartuar një procedure apo rregullore për menaxhimin e gjurmës elektronike të auditimit, me qëllim uljen e riskut mbi sigurinë e të dhënave me pasojë humbjen dhe tjetërsimin e tyre. Gjithashtu, në këtë dokument duhet të specifikohet qartë vendi ku ruhen gjurmët, për cilat veprime të përdoruesit ruhen këto gjurmë, koha, struktura përgjegjëse për monitorimin dhe analizimin e tyre, detyrat dhe përgjegjësitë, e çdo element tjetër që i shërben sigurisë së të dhënave dhe parandalimit në tjetërsimin e tyre.

*Menjëherë dhe në vijimësi*

**13..Gjetje nga auditimit** : Nga auditimi u konstatua se sistemet e Ndihmës Ekonomike nuk ndërveprojnë me Webservice me Agjencinë Shtetërore të Kadastrës. Mungesa e ndërveprimit ndërmjet sistemeve sjell rriskun e vlerësimit të gabuar të aplikantëve për Ndihmën Ekonomike Sistemi nuk mund të verifikoj nëse aplikantët kanë ose jo prona të regjistruara në ASHK.
*(Më hollësisht trajtuar në pikën 2.3 faqet 16-23 të Raportit Përfundimtar të Auditimit)*
**13.1 Rekomandimi:** AKSHI dhe Shërbimi Social Shtetëror të marrin masa duke komunikuar me ASHK për gjetjen e problematikave të funksionimit të webservisit për të vendosur në funksionim të plotë ndërveprimin ndërmjet sistemeve që SHSSH dhe ASHK me qëllim rritjen e efikasitetit të vlerësimit të formularëve për aplikuesit e Ndihmës Ekonomike.

*Menjëherë*

**14..Gjetje nga auditimit:** Nga auditimi i përdorimit të funksionaliteteve të Sistemeve të SHSSH u konstatua se:
- Përdoruesit e Sistemeve të Shërbimit Social Shtetëror nuk mund të gjenerojnë dhe eksportojnë raporte.
- Sistemet kanë të aktivizuar Copy protection, përdoruesit nuk mund të kopjojnë dot tekstin që u nevojitet nga sistemi duke vonuar përpunimin e informacionit gjatë punës së tyre.
*(Më hollësisht trajtuar në pikën 2.3 faqet 16-23 të Raportit Përfundimtar të Auditimit)*

**14.1 Rekomandimi:** AKSHI në bashkëpunim me Shërbimin Social shtetëror të analizojnë kërkesat e përdoruesve të sistemeve dhe të kryejnë ndryshimet e nevojshme për lehtësimin e punës në sistem pa cënuar sigurinë e sistemeve.

*Në vijimësi*

**15. Gjetje nga auditimi:** Nga auditimi mbi aktet rregullatore të manualeve të përdorimit të sistem u konstatua se Manualet e përdorimit të sistemeve të ndihmës Sociale nuk janë të përditësuara me ndryshimet e ndodhura në sisteme. Këto manuale shërbejnë si udhëzues për të gjithë përdoruesit që kanë të drejtë të aksesojnë sistemin.
*(Më hollësisht trajtuar në pikën 2.3 faqet 16-23 të Raportit Përfundimtar të Auditimit)*
**15.1 Rekomandimi:** AKSHI në bashkëpunim me OE që ofron shërbimin e mirëmbajtjes për këtë sistem, të hartojë, përditësojë dhe miratojë, manualet e përdorimit të sistemeve të Ndihmës Sociale duke reflektuar ndryshimet ndërfaqësore, funksionalitet e sistemit që janë shtuar, rolet dhe përgjegjësitë që kanë pësuar ndryshime, mënyra e aksesimit dhe çdo ndryshim tjetër të ndodhur ndër vite në sistem.

*Menjëherë dhe në vijimësi*

*Për sa më sipër paraqitet ky Raport Auditimi.*

**KONTROLLI I LARTË I SHTETIT**