RAPORT PËRFUNDIMTAR I AUDITIMIT

MBI KONTROLLET BAZË TË TEKNOLOGJISË SË INFORMACIONIT

NË

QENDRËN E STUDIMEVE DHE PUBLIKIMEVE PËR ARBËRESHËT

Tiranë, korrik 2025

I. PËRMBLEDHJE EKZEKUTIVE

KLSH mbështetur në Ligjin nr.154, datë 27.11.2014 "*Për Organizimin dhe Funksionimin e Kontrollit të Lartë të Shtetit*", zhvilloi auditimin mbi kontrollet bazë të Teknologjisë së Informacionit në Qendrën e Studimeve dhe Publikimeve për Arbëreshët, nga data 26.03.2025 deri në 28.04.2025 për periudhën audituese 01.01.2023-31.12.2024.
Grupi i auditimit pasi mblodhi informacione të mjaftueshme, zhvilloi pyetësorë e intervista dhe mbështetur në këto të dhëna hartoi drejtimet e auditimit.
Kërkesat për informacion për fushat përkatëse u hartuan në përputhje me manualin e Auditimit të Teknologjisë së Informacionit.

1. Përshkrim i shkurtër i Projektit të Auditimit

Auditimi me objekt "Mbi kontrollet bazë të teknologjisë së informacionit", në Qendrën e Studimeve dhe Publikimeve për Arbëreshët, është pjesë e Planit Vjetor 2025 të auditimit të KLSH-së, miratuar nga Kryetari i KLSH-së.
KLSH-ja, ka vlerësuar auditimin e sistemeve të teknologjisë së informacionit që zhvillon Qendra e Studimeve dhe Publikimeve për Arbëreshët, pasi ky institucion është përfitues shërbimit nga Agjencia Kombëtare e Shoqërisë së Informacionit.
Pas marrjes së ambienteve në QSPA, grupi auditues filloi fazën e studimit paraprak, ku u dërgua pyetësori i hartuar nga grupi i auditimit, bazuar në Manualin e Auditimit të Teknologjisë së Informacionit.
Programi i auditimit është miratuar nga Kryetari i Kontrollit të Lartë të Shtetit me Nr.274/1, datë 25.03.2025.

2. Përshkrimi i gjetjeve kryesore dhe rekomandimeve:

Paraqitja e gjetjeve kryesore:

- Referuar Standardit ISO/IEC 27001 dhe praktikave më të mira kombëtare e ndërkombëtare, në Rregulloren e Brendshme "Për Organizimin dhe Funksionimin e Punës së Qendrës së Studimeve dhe Publikimeve për Arbëreshët", e miratuar me Urdhrin nr.12, datë 11.12.2020, të ish-Ministrit të Shtetit për Diasporën, nuk janë përshkruar dhe pasqyruar disa rregulla dhe norma pune që lidhen me terma të veçanta të sigurisë së informacionit, përfshirë politikat, procedurat dhe teknologjitë që ndihmojnë dhe mbrojnë informacionin nga kërcënimet kibernetike dhe rreziqet e tjera.
- Për vitet 2023–2024, nuk është hartuar plan trajnimi vjetor apo periodik dhe nuk janë zhvilluar trajnime mbi, sigurinë kibernetike dhe teknologjinë e informacionit, as për burimet njerëzore në përgjithësi dhe as për punonjësin e IT-së në veçanti.
- Infrastruktura e rrjetit dhe shërbimeve të TI në QSPA është e kufizuar dhe nuk plotëson kërkesat bazë të menaxhimit dhe sigurisë.

Auditimi konstatoi se infrastruktura e rrjetit në Qendrën e Studimeve dhe Publikimeve për Arbëreshët (QSPA) mbështetet në pajisje të pakonsoliduara dhe të pamenaxhueshme. Switch-i në përdorim nuk ofron funksionalitete për menaxhimin dhe monitorimin e trafikut të rrjetit, duke

kufizuar ndjeshëm aftësinë për të zbuluar dhe adresuar anomalitë e mundshme. Gjithashtu, mungesa e një pajisjeje firewall ekspozon rrjetin ndaj rreziqeve të sulmeve të jashtme.
Për më tepër, shërbimi i internetit menaxhohet nga një subjekt i jashtëm dhe QSPA nuk disponon akses të plotë administrativ mbi pajisjet e rrjetit (modem/ruter), çka ndikon në kontrollin dhe sigurinë e përgjithshme të rrjetit.
Sipas standardit ISO/IEC 27001, organizatat duhet të përdorin pajisje të menaxhueshme dhe të qëndrueshme për të garantuar monitorimin, menaxhimin dhe mbrojtjen efektive të infrastrukturës së rrjetit.
- Qendra e Studimeve dhe Publikimeve për Arbëreshët (QSPA) ka në përdorim 12 pajisje kompjuterike për kryerjen e funksioneve të përditshme. Asnjë prej pajisjeve nuk është e pajisur me antivirus, duke i ekspozuar ndaj rreziqeve të sigurisë. Sistemet operative dhe paketat Microsoft Office të instaluara janë të palicencuara, duke krijuar mungesë përputhshmërie ligjore dhe rrezik për integritetin e të dhënave.

Paraqitja e rekomandimeve kryesore:

Me qëllim përmirësimin e punës dhe eliminimin e problematikave të konstatuara, janë lënë disa rekomandime si vijon:
- Qendra e Studimeve dhe Publikimeve për Arbëreshët, në përputhje me Standardin ISO/IEC 27001, të marrë masa për përmirësimin e Rregullores së Brendshme "Për Organizimin dhe Funksionimin e Punës së Qendrës së Studimeve dhe Publikimeve për Arbëreshët", duke përshkruar termat e veçanta të sigurisë dhe mbrojtjes së informacionit nga kërcënimet kibernetike dhe rreziqet e tjera, dhe të dërgojë këto ndryshime për miratim nga Ministri për Evropën dhe Punët e Jashtme.
- Qendra e Studimeve dhe Publikimeve për Arbëreshët të marrë masa për hartimin e një plani vjetor trajnimesh dhe planeve periodike për trajnimin dhe kualifikimin e punonjësve në fushën e teknologjisë së informacionit. Si pjesë e këtij plani të merren në konsideratë trajnimet e ofruara nga Autoriteti Kombëtar për Sigurinë Kibernetike.

- Qendra e Studimeve dhe Publikimeve për Arbëreshët të ndërmarrë masa për përmirësimin e infrastrukturës kompjuterike, duke siguruar licencimin e përdorimit të sistemeve operative dhe paketës Office, si dhe duke instaluar një zgjidhje antivirus të përditësuar në të gjitha pajisjet.
- Qendra e Studimeve dhe Publikimeve për Arbëreshët (QSPA) duhet të ndërmarrë masa për përmirësimin e infrastrukturës kompjuterike, duke siguruar përdorimin e sistemeve operative dhe paketës Office të licencuara, si dhe duke instaluar një zgjidhje antivirus të përditësuar në të gjitha pajisjet. Këto masa do të minimizojnë rreziqet për dëmtim, kompromet apo humbje të të dhënave operacionale që lidhen me aktivitetin e institucionit, duke kontribuar njëkohësisht në përputhshmërinë me kërkesat e standardeve të sigurisë së informacionit.

3. Konkluzioni i përgjithshëm i auditimit

Mbështetur në Standardet Ndërkombëtare të Auditimit të Sektorit Publik (ISSAI 100, ISSAI 5300, ISSAI 5310) si dhe nenet 3 dhe 14 të Ligjit nr. 154/2014 "Për organizimin dhe funksionimin e KLSH", auditimi konstaton se Qendra e Studimeve dhe Publikimeve për Arbëreshët nuk disponon sisteme të mirëstrukturuara të Teknologjisë së Informacionit.

Infrastruktura aktuale mbështetet vetëm në një rrjet të kufizuar interneti, i cili nuk siguron funksionalitete për menaxhimin e sigurisë dhe performancës, duke mos përmbushur kërkesat minimale të standardeve ndërkombëtare për menaxhimin efektiv të TI-së.

Gjithashtu, Rregullorja e Brendshme e institucionit nuk përmban dispozita të qarta që rregullojnë sigurinë e informacionit dhe mbrojtjen e tij. Në përputhje me standardin ISO/IEC 27001 dhe praktikat më të mira, është e domosdoshme hartimi dhe zbatimi i politikave, procedurave dhe masave teknologjike për të garantuar mbrojtjen e informacionit dhe të aseteve të TI-së në institucion.

II. HYRJA

Mbështetur në ligjin 154/2014 "Për organizimin dhe funksionimin e Kontrollit të Lartë të Shtetit", në zbatim të programit nr. 274/1 prot., datë 25.03.2025, miratuar nga Kryetari i KLSH-së, nga data 26.03.2025 deri më datë 28.04.2025, në subjektin "Qendrën e Studimeve dhe Publikimeve për Arbëreshët", u krye auditimi me objekt *"Mbi kontrollet bazë të Teknologjisë së Informacionit"*, nga grupi i auditimit me përbërje:

1. A. A., përgjegjës grupi;
2. B. A., anëtar.

1. Objektivat dhe qëllimi i auditimit

Kontrolli i Lartë i Shtetit mbështetur në nenet 3 dhe 14 të ligjit 154 "*Për Organizimin dhe Funksionimin e Kontrollit të Lartë të Shtetit*", zhvilloi auditimin e teknologjisë së informacionit në Qendrën e Studimeve dhe Publikimeve për Arbëreshet, nga data 26.03.2025 deri më datë 28.04.2025. Kërkesat për informacion sipas drejtimeve të programit të auditimit, u hartuan në përputhje me Manualin e Auditimit të Teknologjisë së Informacionit.
Objekti i Auditimit TIK është përcaktimi mbi kontrollet bazë të Teknologjisë së Informacionit në Qendrën e Studimeve dhe Publikimeve për Arbëreshët, mbrojnë asetet e informacionit; ruajnë integritetin e të dhënave; sigurojnë disponueshmërinë dhe konfidencialitetin e informacionit dhe mbështeten në kontrolle të duhura.
Qëllimi i Auditimit TIK është vlerësimi nëse objektivat e subjektit arrihen në mënyrë efektive duke përdorur burimet e teknologjisë së informacionit, duke përfshirë pajtueshmërinë me kërkesat

ligjore dhe rregulluese, si dhe disponueshmërinë mbi kontrollet bazë të Teknologjisë së Informacionit dhe të dhënave që gjenden në të.

2. Identifikimi i çështjes

Drejtimet e këtij auditimi janë bazuar në programin me nr. 1462/1Prot, datë 06.01.2025:

1. Auditimi i përdorimit të infrastrukturës në Teknologjinë e Informacionit

1.1 Verifikimi i strategjisë, politikave dhe procedurave dhe vlerësimi i burimeve njerëzore në TIK

2. Mbledhja dhe ruajtja e të dhënave.

2.1 *Siguria e të dhënave, verifikimi i sigurisë fizike dhe vazhdimësia e ofrimit të shërbimit.*

3. Përgjegjësitë e strukturave drejtuese të subjektit të audituar

Në zbatim të nenit 23/1, të Ligjit nr.16, datë 05.042018 "Për Diasporën" i ndryshuar, me propozim të Ministrit të Shtetit për Diasporën, Këshilli i Ministrave ka nxjerrë Vendimin nr. 601, datë 04.09.2019 "Për krijimin e Qendrës së Studimeve dhe Publikimeve për Arbëreshët (QSPA)".
QSPA është pjesë e strukturës shtetërore për diasporën shqiptare dhe funksionon si institucion publik buxhetor. Fillimisht me krijimin e saj, ka qenë në varësi të ish- Ministrisë së Shtetit për Diasporën dhe më pas me shkrirjen e kësaj Ministrie, me VKM nr. 81, datë 09.02.2022 "Për Përcaktimin e Fushës së Përgjegjësisë Shtetërore të Ministrisë për Evropën dhe Punët e Jashtme" ka kaluar në varësi të Ministrisë për Evropën dhe Punët e Jashtme.
QSPA ka për mision kryerjen e studimeve të thelluara për historinë, letërsinë dhe kulturën e komunitetit arbëresh. Qendra është institucioni kryesor për ruajtjen dhe promovimin e identitetit kombëtar dhe trashëgimisë kulturore e shpirtërore shqiptare, dhe fokusohet veçanërisht te komuniteti arbëresh dhe kontributi i tij në kulturën shqiptare.

4. Përgjegjësitë e audituesve

Kontrolli i Lartë i Shtetit auditoi Qendrën e Studimeve dhe Publikimeve për Arbëreshët për periudhën e veprimtarisë nga data 01.01.2023 deri në 31.12.2024, në drejtim të çështjeve dhe zgjidhjeve informatike që janë implementuar në sistemet informatike.
Nga grupi i auditimit, janë analizuar të gjitha çështjet që përmban programi i auditimit nr. 274/1 Prot., datë 25.03.2025 miratuar nga Kryetari i KLSH-së.
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 institucioni nën auditim si dhe legjislacionin për Teknologjinë e Informacionit në vendin tonë. 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.

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. Konkluzioni i auditimit mbështetet në praktikat më të mira, Standardet Kombëtare

dhe Ndërkombëtare të Auditimit. Në këtë projekt raport krahas gjetjeve që janë konstatuar, grupi i auditimit ka rekomanduar disa masa organizative, për përmirësimin e situatës.
Aktet ligjore dhe rregullave mbi të cilat është mbështetur vlerësimi janë si më poshtë:

- Kushtetuta e Republikës së Shqipërisë (nenet 162-165);
- Ligji nr. 154/2014 *"Për organizimin dhe funksionimit e Kontrollit të Lartë të Shtetit"*;
- Ligji nr. 2/2017, "*Për sigurinë kibernetike*";
- Ligji nr. 10325, datë 23.09.2010, "*Për Bazat e të Dhënave Shtetërore*";
- Ligji nr. 92/2020, për disa shtesa dhe ndryshime në ligjin nr. 16/2018, "*Për Diasporën*"
- Ligji nr. 119/2014, datë 18.09.2014, "*Për të drejtën e informimit*"
- Ligji nr. 60/2016 "*Për sinjalizimin dhe mbrojtjen e sinjalizuesve*", i ndryshuar.
- VKM nr. 673, datë 22.11.2017 "*Për riorganizimin e Agjencisë Kombëtare të Shoqërisë së Informacionit*", i ndryshuar;
- 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;
- VKM nr. 945, datë 02.11.2012 "*Për miratimin e rregullores administrimi i sistemit të bazave të dhënave shtetërore*";
- Rregulloret përkatëse të Qendrës së Studimeve dhe Publikimeve për Arbëreshët;
- Standardet TIK, etj.

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 Teknologjisë së Informacionit dhe Komunikimit si: COBIT 4.1, Manuali i Auditimit IT, ISSAI 5310, etj.

7. Metodat e auditimit

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

- Shqyrtimi i dokumentacionit rregullatorë të institucionit;
- Shqyrtimi i dokumenteve ligjorë, për sistemet informatike që institucioni disponon;
- Intervista zhvilluar me personat përgjegjës;
- Analizimi i të dhënave të eksportuara nga sistemi, etj.

8. Dokumentimi i auditimit

Dokumentimi i auditimit është bazuar në rregulloren e brendshme të KLSH, si dhe në manualin e 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, të dhëna dhe informacione të ndryshme të gjeneruara 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

Në zbatim të nenit 23/1 të Ligjit nr. 16, datë 05.04.2018 "Për Diasporën", i ndryshuar, dhe me propozim të Ministrit të Shtetit për Diasporën, Këshilli i Ministrave ka miratuar Vendimin nr. 601, datë 04.09.2019 "Për krijimin e Qendrës së Studimeve dhe Publikimeve për Arbëreshët (QSPA)". QSPA është pjesë e strukturës shtetërore për diasporën shqiptare dhe funksionon si një institucion publik buxhetor. Fillimisht, me krijimin e saj, ka qenë në varësi të ish-Ministrisë së Shtetit për Diasporën, dhe më pas, me shkrirjen e kësaj Ministrie, me Vendimin e Këshillit të Ministrave nr. 81, datë 09.02.2022 "Për Përcaktimin e Fushës së Përgjegjësisë Shtetërore të Ministrisë për Evropën dhe Punët e Jashtme", ka kaluar në varësi të Ministrisë për Evropën dhe Punët e Jashtme. QSPA ka për mision kryerjen e studimeve të thelluara për historinë, letërsinë dhe kulturën e komunitetit arbëresh. Qendra është institucioni kryesor për ruajtjen dhe promovimin e identitetit kombëtar dhe trashëgimisë kulturore e shpirtërore shqiptare, dhe fokusohet veçanërisht te komuniteti arbëresh dhe kontributi i tij në kulturën shqiptare.
Struktura e Qendrës së Studimeve dhe Publikimeve për Arbëreshët është miratuar me Urdhrin e Kryeministrit nr. 38, datë 18.02.2020 "Për miratimin e strukturës dhe të organikës së Qendrës së Studimeve dhe Publikimeve për Arbëreshët". QSPA është organizuar dhe funksionon në strukturë dhe organikë me: Titullarin e QSPA; Drejtorinë e Studimeve dhe Publikimeve me 7 punonjës në organikë, një nga të cilët është specialisti që mbulon informacionin, komunikimin dhe mirëmbajtjen elektronike të të dhënave; dhe Sektorin e Financës dhe Shërbimeve Mbështetëse me 4 punonjës në organikë.
QSPA-ja ushtron aktivitetin e saj në një apartament të marrë me qira nga Drejtoria e Shërbimit të Trupit Diplomatik në Tiranë, i vendosur në një pallat 6-katësh (kati 5). Ambienti është organizuar në 3 dhoma dhe një paradhomë, të gjitha të përshtatura si zyra pune, me një sipërfaqe totale prej 157.21 m² (përfshirë një verandë të madhe dhe ambientet e përbashkëta).
QSPA-ja financohet nga buxheti i shtetit përmes Ministrisë për Evropën dhe Punët e Jashtme. Për vitin 2023, buxheti total i QSPA-së ka qenë 26,883,216 lekë, ndërsa për vitin 2024 është parashikuar një buxhet prej 26,080,242 lekë.
Për funksionimin dhe zhvillimin e sistemeve të teknologjisë së informacionit, në vitin 2023 janë blerë vetëm 12 kompjuterë për stafin e Qendrës, me vlerë totale 885,600 lekë, përmes një procedure blerje në vlera të vogla nga zëri i investimeve (231). Ndërsa për vitin 2024, është blerë vetëm "Sistemi Access Control REGGIS" për menaxhimin e hyrjeve në institucion, me një vlerë prej 184,800 lekë.

2. Përshkrimi i auditimit sipas drejtimeve të auditimit

2.1 Auditimi i përdorimit të infrastrukturës në Teknologjinë e informacionit.

Verifikimi i infrastrukturës, politikave dhe procedurave dhe vlerësimi i burimeve njerëzore në TIK

Në zbatim të pikës 1. *"Verifikimi i infrastrukturës, politikave dhe procedurave dhe vlerësimi i burimeve njerëzore në TIK*", u shqyrtua dokumentacioni si më poshtë:
-Verifikim i infrastrukturës dhe networkut të institucionit;
-Burimet njerëzore;
-Aktet rregulluese, identifikimi dhe menaxhimi i risqeve në teknologjinë e informacionit;
-Zhvillimi i trajnimeve dhe menaxhimi i kapaciteteve njerëzore në institucion;
-Rregulloret për strukturën IT, përdorimin dhe sigurinë në teknologjinë e informacionit;
- Strategji të IT apo një përfshirje të teknologjisë në strategjinë institucionale;
- Skema e komunikimit të network-ut.

- ***Rregullorja e Brendshme***

Në zbatim të pikës 14 të VKM nr. 601, datë 04.09.2019 "Për krijimin e Qendrës së Studimeve dhe Publikimeve për Arbëreshët", ish-Ministri i Shtetit për Diasporën, me Urdhrin nr. 12, datë 11.12.2020, ka miratuar Rregulloren e Brendshme për Organizimin dhe Funksionimin e punës së Qendrës së Studimeve dhe Publikimeve për Arbëreshët.
Në nenin 27 të rregullores janë përcaktuar detyrat e specialistit të informacionit dhe komunikimit, si dhe mirëmbajtjes elektronike të të dhënave. Ndër detyrat e këtij specialisti përfshihen:

- Monitorimi dhe raportimi mbi pasqyrimin e iniciativave dhe sipërmarrjeve nga QSPA-ja në faqen e internetit.
- Përditësimi dhe publikimi i informacionit dhe lajmeve në kohë reale në faqen e internetit.
- Menaxhimi i procesit të informimit përmes internetit, në kohë, për të gjithë aktivitetet që organizon QSPA-ja.
- Propozimi dhe realizimi i ndryshimeve dhe përditësimeve të faqes së internetit të QSPA-së, pas miratimit nga eprorët, në funksion të rritjes së transparencës dhe mbarëvajtjes së misionit të institucionit, në bashkëpunim me Agjencinë Kombëtare të Shoqërisë së Informacionit.

  Megjithatë, evidentohet se rregullorja nuk ka pasqyruar standardet ISO/IEC 27001, të cilat kërkojnë përfshirjen e disa rregullave dhe normave të punës që lidhen me sigurinë e informacionit, përfshirë politikat, procedurat dhe teknologjitë që ndihmojnë dhe mbrojnë informacionin nga kërcënimet kibernetike dhe rreziqet e tjera.

- ***Trajnimet***

Zhvillimi i trajnimeve ka një rëndësi të veçantë për menaxhimin e kapaciteteve njerëzore në institucion. Është thelbësore që të identifikohen nevojat e stafit për trajnime mbi teknologjinë e informacionit. Punonjësit që kanë akses në sistemet e informacionit duhet të jenë të njohur me standardet e sigurisë dhe të kenë aftësinë për t'i zbatuar dhe implementuar ato gjatë aktivitetit që kryejnë.
U konstatua se, për periudhën e auditimit vitet 2023-2024, QSPA-ja nuk ka pasur një plan trajnimi vjetor dhe plane periodike, as nuk ka zhvilluar trajnime mbi, sigurinë kibernetike dhe teknologjinë e informacionit për burimet njerëzore dhe specialistin e IT-së që ka në organikë. Trajnimet e përfituara nga punonjësi i TI-së, me temën "Graphic Design", janë të pa mjaftueshme dhe nuk plotësojnë nevojat për trajnimin mbi sigurinë dhe teknologjinë e informacionit.

- **Rrjeti kompjuterik**

Qendra e Studimeve dhe Publikimeve për Arbëreshët ka një staf prej 12 punonjësish. Rrjeti kompjuterik i kësaj Qendre përbëhet nga 12 kompjuterë, të cilët janë në përdorim nga secili punonjës përkatësisht:

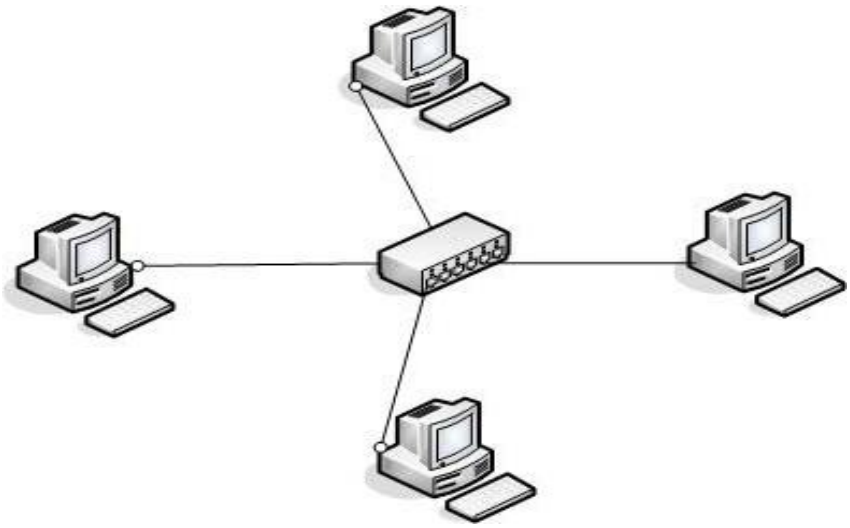
- Kompjuter All in One HP 24-cb1012në 2 copë
- Desktop 1 HP 290 G9 + Monitor HP V221 9 copë
- Desktop 2 HP 290 G9 + Monitor HP V221 1 copë

Rrjeti i internetit në Qendrën e Studimeve dhe Publikimeve për Arbëreshët është i ndërthurur me ethernet dhe USB wireless. Interneti sigurohet përmes një lidhjeje me fibra optike me shpejtësi 40 Mbps, një shpejtësi e mjaftueshme për të përmbushur nevojat e Qendrës.

Shpërndarja e rrjetit nëpër zyra realizohet me anë të switch-eve të thjeshtë. Tre prej kompjuterëve janë të lidhur me internetin përmes USB wireless, të diktuara nga infrastruktura e ambienteve të punës.

Përveç kompjuterëve, ka gjithashtu dhe 3 pajisje periferike printer:

- Lexmark cs417 në dispozicion të Drejtorit Ekzekutiv.
- Xerox Versalink B7035 i cili përdoret nga 2 punonjës
- Xerox Versalink C7125 i cili përdoret nga pjesa tjetër e stafit (9 punonjës).



Skema e shpërndarjes së internetit.

Nga auditimi u konstatua se:

- Pajisjet PC nuk kanë të instaluara software antivirus, duke rrezikuar sigurinë e informacionit dhe mbrojtjen nga viruset dhe malware.
- Sistemet e operimit dhe softuerët (si Office) që janë të instaluar në kompjuterët e QSPA-së janë të pa licencuara, duke cënuar sigurinë ligjore dhe funksionalitetin e plotë të këtyre sistemeve.
- Swtch-i është i pa menaxhueshëm. Pajisja e rrjetit nuk ofron mundësi menaxhimi dhe monitorimi të trafikut, ndërkohë që standardet si ISO/IEC 27001 kërkojnë që pajisjet që mbështesin monitorimin dhe menaxhimin e sigurisë dhe performancës të jenë të qëndrueshme.
- Internetin e menaxhon një kompani lokale dhe QSPA-ja nuk ka kontroll të plotë mbi pajisjet e rrjetit të internetit (modem/ruter). Sipas standardeve ISO/IEC 27001,

rekomandohet një kontroll të plotë mbi pajisjet e rrjetit për të siguruar mbrojtjen e plotë të sistemit.

- Nuk disponohet një server qendror i pajisur me Active Directory Domain Controller për menaxhimin e përdoruesve dhe vendosjen e politikave të sigurisë, duke kufizuar menaxhimin dhe mbrojtjen e përdoruesve dhe burimeve.
- Nuk ka një pajisje firewall për mbrojtjen e rrjetit nga sulmet e jashtme, duke lënë sistemet të pambrojtura ndaj kërcënimeve kibernetike.
- Nuk ka një rregullore për sigurinë dhe komunikimet elektronike, as dokumentacion mbi procedurat e ruajtjes së të dhënave "back-up" dhe procedurat e veprimeve të ndryshme, duke krijuar mangësi në menaxhimin e sigurisë dhe ruajtjen e të dhënave.

- **Sistemi i Kontrollit të Aksesit:**
  Sistemi i kontrollit të aksesit përdoret për të menaxhuar hyrjen dhe daljen e stafit në institucion. Mënyra e funksionimit të tij është me anë të kartave personale të secilit punonjës, të cilat skanohen në aparaturën e vendosur në pjesën e jashtme të ambienteve të zyrës. Ky sistem është i lidhur me një kompjuter kryesor ku është instaluar programi i kontrollit. Ruajtja e të dhënave bëhet në sistemin përkatës "Codeks". Kontrolli i të dhënave realizohet përmes raporteve mujore, të cilat mund të shkarkohen për të pasqyruar orët e punës të secilit punonjës ose për të gjithë stafin. Sistemi automatizon numërimin e orëve të punës për çdo punonjës.

  Megjithatë, u konstatua se sistemi i aksesit është i kufizuar vetëm për regjistrimin e prezencës së punonjësve dhe nuk është përdorur për menaxhimin e hyrjeve dhe daljeve fizike të personelit. Referuar standardit ISO 27001, rekomandohet që sistemet e aksesit të jenë gjithëpërfshirëse dhe të integrojnë kontrollet fizike, për të siguruar një menaxhim më të plotë dhe të sigurt të hyrjeve dhe daljeve të personelit, duke rritur nivelin e sigurisë fizike të institucionit.

2.2 Mbledhja dhe ruajtja e të dhënave.

2.Mbledhja e të dhënave dhe vazhdimësia e ofrimit të shërbimit

Në zbatim të pikës 2 *"Sistemet informatike , verifikimi i sigurisë fizike dhe siguria e të dhënave*", u shqyrtua dokumentacioni si më poshtë:

- Verifikime i infrastrukturës;
- Intervista të drejtpërdrejta me punonjës që kryenin apo administronin shërbime të caktuara;
- Vizita në terren;
- Indikatorë dhe statistika, etj.

- **Mbledhja dhe ruajtja e të dhënave:**

Llojet dhe ruajtja e të dhënave në QSPA bëhet në mënyrë manuale në një kompjuter, konkretisht atë të punonjësit të IT, si dhe një kopje rezervë në një hard-disk të jashtëm. Këto të dhëna janë të disponueshme për secilin studiues në çdo moment që lind nevoja.
Të dhënat e ruajtura përfshijnë të gjitha materialet që janë pjesë e aktiviteteve të QSPA-së, konkretisht:

- Posterat dhe banerat e dizajnuar nga IT
- Artikujt me kumtesat e pjesëmarrësve

- Materialet filikë (audio, video dhe fotografi) të cilat realizohen në bashkëpunim me kompanitë e kontraktuara
- Botimet janë një nga materialet më të rëndësishme, pasi ato përbëjnë një nga misionet kryesore të Qendrës. Për botimet ruhet kopja përfundimtare në formatin PDF, e cila më pas dërgohet për shtyp. Këto kopje shërbejnë gjithashtu për publikimin në faqen e internetit të QSPA-së, pasi konvertohen në formatin e-book për t'u shpërndarë dhe përdorur në mënyrë elektronike.

Nga auditimi u konstatua se:

-Të dhënat ruhen dhe janë në dispozicion të secilit studiues në çdo moment që lind nevoja. Megjithatë, nxjerrja e të dhënave nuk është e parashikuar në Rregulloren e Brendshme, për Organizimin dhe Funksionimin e punës së Qendrës së Studimeve dhe Publikimeve për Arbëreshët. Ky mangësi mund të shkaktojë paqartësi lidhur me procedurat e nxjerrjes dhe përdorimit të të dhënave për studiuesit dhe mund të ndikojë në efikasitetin e menaxhimit të informacionit.

-QSPA-ja nuk ka një plan formal për rikuperimin dhe vazhdimësinë pas katastrofave (Disaster Recovery Plan - DCP). Sipas standardeve ndërkombëtare, si ISO 22301, është e domosdoshme që organizatat të kenë një plan të mirë-dokumentuar për rikuperimin e të dhënave dhe vazhdimësinë e funksioneve kritike. Ky plan duhet të përfshijë procedura të detajuara për ruajtjen dhe rikuperimin e të dhënave dhe funksioneve kritike pas një fatkeqësie ose sulmi kibernetik.

-Aktualisht, kopjimi i të dhënave bëhet dhe mbahet në një hard disk të jashtëm, por nuk ka testime periodike për të verifikuar funksionalitetin e kopjeve rezervë. Praktikat më të mira nga institucione si NIST (National Institute of Standards and Technology) rekomandojnë që kopjet rezervë duhet të testohen rregullisht për të siguruar integritetin dhe funksionalitetin e tyre. Ky proces është i domosdoshëm për të siguruar që, në rast nevoje, të dhënat mund të rikuperohen pa humbje ose dëmtim të informacionit.

-Kopjet rezervë aktualisht ruhen në të njëjtin vend me pajisjet kryesore (kompjuterët dhe sistemet), duke përfshirë hard disqet e jashtme. Kjo paraqet një rrezik të mundshëm, pasi një incident (p.sh. zjarri, përmbytja, etj.) mund të prekë të dyja: pajisjet kryesore dhe kopjet rezervë. Praktikat më të mira dhe standardet ndërkombëtare rekomandojnë ruajtjen e kopjeve rezervë në vendndodhje të ndryshme për të minimizuar rrezikun dhe për të siguruar një mbrojtje të plotë të të dhënave.

Me shkresën nr. 40/5 prot., datë 23.06.2025, hyr ne KLSH me nr.274/3 prot., datë 25.06.2025, subjekti i audituar ka përcjell Projekt Raportit e Auditimi . Nuk janë paraqitur komente apo observacione për Projekt Raportin e auditimit nga subjekti i audituar.

IV. REKOMANDIME

A. MASA ORGANIZATIVE

1. Gjetje nga auditimi: Nga auditimi u konstatua se në Rregulloren e Brendshme "Për Organizimin dhe Funksionimin e Punës së Qendrës së Studimeve dhe Publikimeve për Arbëreshët", e miratuar me Urdhrin nr.12, datë 11.12.2020, të ish-Ministrit të Shtetit për Diasporën, Referuar Standardit ISO/IEC 27001 dhe praktikave më të mira kombëtare e ndërkombëtare nuk janë përshkruar dhe pasqyruar disa rregulla dhe norma pune që lidhen me terma të veçanta të sigurisë së informacionit, përfshirë politikat, procedurat dhe teknologjitë që ndihmojnë dhe mbrojnë informacionin nga kërcënimet kibernetike dhe rreziqet e tjera.
(Më hollësisht trajtuar në pikën 2.1, faqet 8-10, të Raportit Përfundimtar të Auditimit).

1.1. Rekomandim: Qendra e Studimeve dhe Publikimeve për Arbëreshët, në përputhje me Standardin ISO/IEC 27001, të marrë masa për përmirësimin e Rregullores së Brendshme "Për Organizimin dhe Funksionimin e Punës së Qendrës së Studimeve dhe Publikimeve për Arbëreshët", duke përshkruar termat e veçanta të sigurisë dhe mbrojtjes së informacionit nga kërcënimet kibernetike dhe rreziqet e tjera, dhe të dërgojë këto ndryshime për miratim nga Ministri për Evropën dhe Punët e Jashtme.

Në vijimësi

2. Gjetje nga auditimi: Qendra e Studimeve dhe Publikimeve për Arbëreshët nuk ka hartuar dhe miratuar një rregullore të brendshme për sigurinë dhe komunikimet elektronike, si dhe për procedurat e veprimeve të ndryshme, në përputhje me standardet ndërkombëtare të sigurisë së informacionit, si ISO/IEC 27001.

(Më hollësisht trajtuar në pikën 2.1, faqet 8-10, të Raportit Përfundimtar të Auditimit).

2.1. Rekomandim: Qendra e Studimeve dhe Publikimeve për Arbëreshët të marrë masa për hartimin dhe miratimin e një rregulloreje të brendshme të veçantë për sigurinë dhe komunikimet elektronike, si dhe për menaxhimin e veprimeve të ndryshme operacionale.

Menjëherë

3. Gjetje nga auditimi: Gjatë periudhës objekt auditimi për vitet 2023 dhe 2024, QSPA nuk ka hartuar plane trajnimi periodike apo një plan trajnimi vjetor, dhe nuk ka zhvilluar trajnime për kualifikimin e burimeve njerëzore, në veçanti për specialistin e IT-së në fushën e sigurisë dhe teknologjisë së informacionit. Puna për zhvillimin e një plani trajnimi për të gjithë stafin lidhur me sigurinë e informacionit është e domosdoshme, për të siguruar që të gjithë punonjësit të kenë njohuri dhe aftësi të mjaftueshme për të zbatuar politikat e sigurisë dhe për të menaxhuar informacionin në mënyrë të sigurtë.

(Më hollësisht trajtuar në pikën 2.1, faqet 8-10, të Raportit Përfundimtar të Auditimit).

3.1 Rekomandim: Qendra e Studimeve dhe Publikimeve për Arbëreshët të marrë masa për hartimin e një plani vjetor trajnimesh dhe planeve periodike për trajnimin dhe kualifikimin e punonjësve në fushën e teknologjisë së informacionit. Si pjesë e këtij plani të merren në konsideratë trajnimet e ofruara nga Autoriteti Kombëtar për Sigurinë Kibernetike.

Në vijimësi

4. Gjetje nga auditimi: Infrastruktura e rrjetit dhe shërbimeve të TI në QSPA është e kufizuar dhe nuk plotëson kërkesat bazë të menaxhimit dhe sigurisë.

Auditimi konstatoi se infrastruktura e rrjetit në Qendrën e Studimeve dhe Publikimeve për Arbëreshët (QSPA) mbështetet në pajisje të pakonsoliduara dhe të pamenaxhueshme. Switch-i në përdorim nuk ofron funksionalitete për menaxhimin dhe monitorimin e trafikut të rrjetit, duke kufizuar ndjeshëm aftësinë për të zbuluar dhe adresuar anomalitë e mundshme. Gjithashtu, mungesa e një pajisjeje firewall ekspozon rrjetin ndaj rreziqeve të sulmeve të jashtme.

Për më tepër, shërbimi i internetit menaxhohet nga një subjekt i jashtëm dhe QSPA nuk disponon akses të plotë administrativ mbi pajisjet e rrjetit (modem/ruter), mungesë që ndikon në kontrollin dhe sigurinë e përgjithshme të rrjetit.

Sipas standardit ISO/IEC 27001, organizatat duhet të përdorin pajisje të menaxhueshme dhe të qëndrueshme për të garantuar monitorimin, menaxhimin dhe mbrojtjen efektive të infrastrukturës së rrjetit.

(Më hollësisht trajtuar në pikën 2.1, faqet 8-10, të Raportit Përfundimtar të Auditimit).

4.1. Rekomandim: Qendra e Studimeve dhe Publikimeve për Arbëreshët të marrë masa për përmirësimin e infrastrukturës kompjuterike, duke siguruar licencimin e përdorimit të sistemeve

operative dhe paketës Office, si dhe duke instaluar një zgjidhje antivirus të përditësuar në të gjitha pajisjet.

Në vijimësi

5. Gjetje nga auditimi: Qendra e Studimeve dhe Publikimeve për Arbëreshët (QSPA) ka në përdorim 12 pajisje kompjuterike për kryerjen e funksioneve të përditshme. Asnjë prej pajisjeve nuk është e pajisur me antivirus bazuar në standardin ISO 27001:2022, duke i ekspozuar ndaj rreziqeve të sigurisë. Sistemet operative dhe paketat Microsoft Office të instaluara janë të palicencuara, duke krijuar mungesë përputhshmërie ligjore dhe rrezik për integritetin e të dhënave. *(Më hollësisht trajtuar në pikën 2.1, faqet 8-10, të Raportit Përfundimtar të Auditimit).*

5.1. Rekomandim: Qendra e Studimeve dhe Publikimeve për Arbëreshët (QSPA) duhet të marrë masa për përmirësimin e infrastrukturës kompjuterike, duke siguruar përdorimin e sistemeve operative dhe paketës Office të licencuara, si dhe duke instaluar një zgjidhje antivirus të përditësuar në të gjitha pajisjet. Këto masa do të minimizojnë rreziqet për dëmtim, kompromet apo humbje të të dhënave operacionale që lidhen me aktivitetin e institucionit, duke kontribuar njëkohësisht në përputhshmërinë me kërkesat e standardeve të sigurisë së informacionit.

Menjëherë dhe në vijimësi

6. Gjetje nga auditimi: QSPA ruan në mënyrë manuale një kopje rezervë për të dhënat në një hard-disk të jashtëm, për të cilat nuk janë kryer ndonjë herë testime periodike, nëse këto kopje janë të vlefshme**,** bazuar në standardin ISO 27001:2022, Institucion nuk ka hartuar një planifikim për të dhënat që nevojiten të krijohet një kopje e dytë në mënyrë që të sigurohet rikthimi i aktivitetit në rast të një ndërhyrje në rrjetin e brendshëm.

(Më hollësisht trajtuar në pikën 2.2, faqet 11-12, të Raportit Përfundimtar të Auditimit.)

6.1 Rekomandimi: Qendra e Studimeve dhe Publikimeve për Arbëreshët të marrë masa për krijimin e një procesi të strukturuar për testimin periodik të kopjeve rezervë, me qëllim sigurimin e funksionaliteteve, si dhe të implementojë një plan për ruajtjen e të dhënave jashtë godinës, në një lokacion fizikisht të sigurt.

Menjëherë dhe në vijimësi

7. Gjetje nga auditimi: Sistemi elektronik i hyrje-daljeve në institucion nuk është plotësisht funksional dhe i integruar për administrimin e hyrje - daljeve të punonjësve të institucionit, sikurse përcakton Standardi ISO 27001.

(Më hollësisht trajtuar në pikën 2.2, faqet 11-12, të Raportit Përfundimtar të Auditimit).

7.1. Rekomandim: Qendra e Studimeve dhe Publikimeve për Arbëreshët të marrë masa për të zgjeruar funksionalitetin e sistemit, me qëllim menaxhimin e hyrjeve dhe daljeve fizike, duke integruar mekanizma që mundësojnë kontrollin e lëvizjes së punonjësve.

Menjëherë dhe në vijimësi

Për sa më sipër paraqitet ky Raport Përfundimtar Auditimi.

KONTROLLI I LARTË I SHTETIT