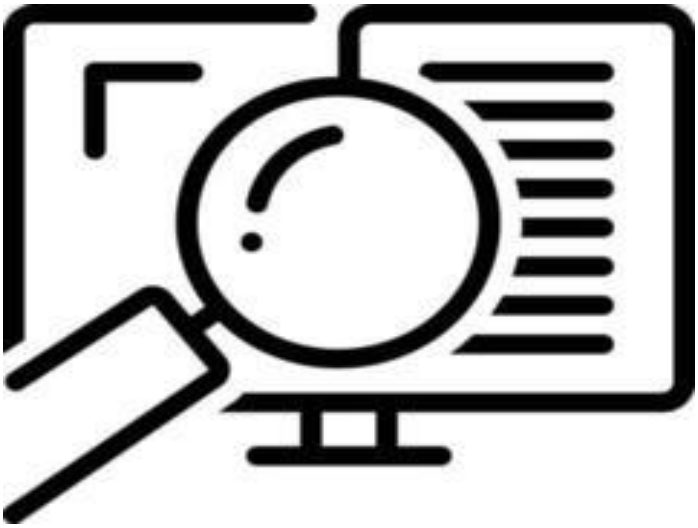
RAPORT PËRFUNDIMTAR AUDITIMI

MBI AUDITIMIN E SISTEMEVE TË TEKNOLOGJISË SË INFORMACIONIT, NË DREJTORINË RAJONALE TË ARSIMIT PARAUNIVERSITAR LEZHË



Tiranë, prill 2025

PËRMBAJTJA

LISTA E SHKURTIMEVE

Shkurtimi	Emërtimi i plotë
KLSH	Kontrolli i Lartë i Shtetit
DRAP	Drejtoria Rajonale e Arsimit Parauniversitar
RSH	Republika e Shqipërisë
BCP	Business Continuity Plan
IQ	Inspektoriati Qendror
BCC	Business Continuity Center
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 Drejtorinë Rajonale të Arsimit Parauniversitar Lezhë nga data 08.01.2025 deri më datë 19.02.2025.
Grupi i auditimit pasi mblodhi informacione të mjaftueshme, zhvilloi pyetësorë e intervista për caktimin e zonave me risk të lartë, 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.

I.1. Përshkrim i shkurtër i Projektit të Auditimit

Projekti i auditimit, për auditimin e Sistemeve të Teknologjisë së Informacionit, në Drejtorinë Rajonale të Arsimit Parauniversitar Lezhë, është pjesë e Planit Vjetor 2025 të auditimit të KLSH-së, miratuar nga Kryetari i KLSH. Drejtoria Rajonale e Arsimit Parauniversitar (DRAP) Lezhë është institucioni përgjegjës për mbikëqyrjen, menaxhimin dhe vlerësimin e institucioneve arsimore parauniversitare në rajonin e Lezhës. Ajo siguron zbatimin e ligjeve dhe standardeve arsimore, monitoron procesin mësimor dhe administrativ, si dhe mbështet zhvillimin profesional të mësuesve. Gjithashtu, DRAP garanton shpërndarjen e drejtë dhe efektive të burimeve njerëzore në arsim, dhe propozon zgjidhje për përmirësimin e cilësisë së shërbimeve arsimore në rajon.
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.Përzgjedhja e këtij subjekti 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 Drejtoria Rajonale e Arsimit Parauniversitar Lezhë 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. Pas marrjes së ambienteve të përshtatshme, 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.1461/1 me datë 06.01.2025.

I.2. Paraqitja e gjetjeve kryesore dhe rekomandimeve

Nga shqyrtimi i evidencave rezultoi se institucioni për periudhën nënauditim paraqet mangësi në drejtimin e Teknlogjisë së Informacionit. Grupi i auditimit ka konstatuar 10 gjetje dhe ka dhenë 10 rekomandime.

Paraqitja e gjetjeve kryesore:
-Nga auditimi i strukturës organizative të Drejtorisë Rajonale Arsimore Parauniversitare (DRAP) Lezhë u konstatua se, që prej krijimit të institucionit, nuk ka qenë i parashikuar një pozicion i dedikuar për një specialist të fushës së teknologjisë së informacionit (TI). Si rrjedhojë, funksionet që lidhen me menaxhimin e TI-së janë kryer nga përgjegjësi i sektorit të kurrikulës, i cili nuk zotëron kualifikimet e nevojshme për këtë fushë. Gjithashtu, u konstatua mbivendosje në përshkrimet e punës së stafit, ku në disa raste kualifikimet e punonjësve nuk

përputheshin me kërkesat përkatëse të pozicionit të tyre sipas kërkesave të ligjit nr.10296, datë 08.07.2010, "Për menaxhimin financiar dhe kontrollin". Me miratimin e strukturës së re më datë 23.01.2025, është rekrutuar një specialist TI në sektorin e statistikës për të mbuluar nevojat teknologjike të institucionit.
-Nga auditimi i kryer u konstatua se Drejtoria Rajonale Arsimore Parauniversitare (DRAP) Lezhë operon në fushën e teknologjisë së informacionit (TI) në mungesë të një baze të mirëfilltë rregullatore. Mungesa e stafit të specializuar ka ndikuar në mos hartimin e rregullave dhe procedurave të nevojshme për menaxhimin e proceseve të TI-së, sipas kërkesave të ligjit nr.10296, datë 08.07.2010, "Për menaxhimin financiar dhe kontrollin". Institucioni nuk disponon dokumentacion bazë si rregulloren për funksionimin e veprimtarisë së TI-së apo procedurat për menaxhimin e incidenteve kibernetike. Kjo situatë ka çuar në një funksionim të paorganizuar, duke rritur riskun ndaj situatave të paparashikuara, me përgjegjësi të paqarta dhe kohë reagimi të papërcaktuar në rast emergjencash.
-Nga auditimi u konstatua se nuk ka një firewall (mbrojtës të rrjetit) të instaluar dhe të konfiguruar, duke e lënë atë të ekspozuar ndaj kërcënimeve të jashtme, si sulmet kibernetike, skanimet e portave dhe përpjekjet për hyrje të paautorizuar. Mungesa e një firewall-i gjithashtu e bën të vështirë monitorimin dhe filtrimin e trafikut të rrjetit për të parandaluar aktivitetet keqdashëse.
-Nga auditimi u konstatua se kompjuterat, printerat dhe ruterët lihen të ekspozuara fizikisht, pa asnjë masë sigurie për të parandaluar aksesin e paautorizuar, pasi nuk ka kontrolle hyrjeje në ambientet ku ndodhen pajisjet, duke rritur rrezikun ndaj vjedhjes së të dhënave dhe aksesimit përmes pajisjeve të paautorizuara

Paraqitja e rekomandimeve kryesore:
-Drejtoria Rajonale Arsimore Parauniversitare Lezhë, të marrë masa për përditësimin e rregullores së brendshme dhe përshkrimeve të punës, në përputhje me strukturën e re organizative, duke i përshtatur ato me detyrat funksionale dhe përgjegjësitë reale të çdo pozicioni.
-Drejtoria Rajonale Arsimore Parauniversitare Lezhë të marrë masa për të centralizuar monitorimin dhe administrimin e rrjetit në të gjitha zyrat, për të siguruar një menaxhim më efikas të infrastrukturës. Implementimi i një qendre të menaxhimit të rrjetit do të ndihmojë në aplikimin e politikave të sigurisë në mënyrë të njëtrajtshme dhe do të lehtësojë identifikimin dhe trajtimin e incidenteve të mundshme të sigurisë.
-Drejtoria Rajonale e Arsimit Parauniversitar Lezhë, të marrë masa për instalimin dhe konfigurimin e një firewall-i, që mund të monitorojë dhe filtrojë trafikun e rrjetit, duke parandaluar sulmet kibernetike dhe aksesin e paautorizuar. , me qëllim identifikimin dhe bllokimin e sulmeve, si dhe sigurimin e një kontroll më të mirë mbi trafikun e rrjetit.
-Drejtoria Rajonale e Arsimit Parauniversitar Lezhë, të marrë masa për të forcuar sigurinë fizike të pajisjeve kompjuterike, printerave dhe ruterëve, duke kufizuar hyrjen në ambientet ku ndodhen pajisjet. Gjithashtu, institucioni të marrë masa për të ndaluar lidhjen e pajisjeve të paautorizuara në rrjet, për të parandaluar shpërndarjen e mundshme të malware-ve ose qasjen e paautorizuar në sistemet e brendshme.

1.3 Konkluzioni i përgjithshëm dhe Opinioni i Auditimit:

Grupi i auditimit është mbështetur në Standardet Ndërkombëtare të Auditimit, përkatësisht ISSAI 100 - Parimet themelore të auditimet në sektorin publik, ISSAI 5300 - Udhëzime për auditimin e IT-së dhe ISSAI 5310 - Metodologjia e Rishikimit të Sigurisë së Sistemit të Informacionit, si dhe në nenet 3 dhe 14 të Ligjit nr. 154, datë 27.11.2014, "*Për Organizimin dhe Funksionimin e Kontrollit të Lartë të Shtetit*". Nga auditimi i kryer është evidentuar se infrastruktura IT e Drejtorisë Rajonale Arsimore Parauniversitar Lezhë përballet me problematika të rëndësishme që kërcënojnë sigurinë, si rrjedhojë e mungesës së një

infrastrukture rrjeti të qëndrueshme, për shkak të mos implementimit të një firewall-i dhe mungesës së mbrojtjes nga viruset, e cila kërcënon sigurinë dhe vazhdimësinë e shërbimeve të institucionit. Po ashtu, mungesa e politikave të qarta për menaxhimin e aksesit dhe ndarjen e llogarive ndërmjet përdoruesve paraqet një rrezik serioz për integritetin dhe konfidencialitetin e të dhënave. Pa një sistem autentifikimi dhe autorizimi të qartë, gjurmimi i përgjegjësisë për veprimet e kryera në sistem bëhet i pamundur. Përdorimi i fjalëkalimeve të dobëta dhe mungesa e një mekanizmi të menaxhimit të tyre e ekspozon institucionin ndaj sulmeve. Gjithashtu ekspozimi fizik i pajisjeve IT pa masa mbrojtëse dhe mungesa e një qendre të menaxhimit të rrjetit riskojnë sigurinë dhe administrimin e infrastrukturës teknologjike.

II. HYRJA

Mbështetur në Ligjin 154/2014, datë 27.11.2014 "*Për Organizimin dhe Funksionimin e KLSH*", në zbatim të Programit të Auditimit 1461/1 Prot, datë 06.01.2025, të miratuar nga Kryetari i KLSH, me afat auditimi 08.01.2025 deri në 21.02.2025, në Drejtorinë Rajonale të Arsimit Parauniversitar Lezhë, (më poshtë DRAP), ku periudha e audituar është 01.01.2023 deri në 31.12.2024, u krye auditimi me objekt "*Auditimi i Sistemeve të Teknologjisë së Informacionit*", nga audituesit:

1. R.A, përgjegjës grupi
2. 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 Drejtorinë Rajonale të Arsimit Parauniversitar Lezhë, 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.1461/1 Prot, datë 06.01.2025:

1. Auditimi i funksionimit të Qeverisjes në TIK
a.Verifikim i politikave, standardeve dhe vlerësimi i burimeve njerëzore në TIK.
2. Auditimi i sigurisë së informacionit dhe sistemeve
a.Siguria e të dhënave dhe vazhdimësia në ofrimin e shërbimit.
b.Auditimi i sistemeve në TIK.
3.Të tjera

II.3 Përgjegjësitë e strukturave drejtuese të subjektit të audituar

Drejtoria Rajonale e Arsimit Parauniversitar Lezhë është institucion përgjegjës për funksionimin dhe mabrëvajtjen e institucioneve arsimore brenda juridiksionit të tyre duke siguruar cilësinë e shërbimit arsimor parauniversitar në nivel rajonal.
Përgjegjësitë e DRAP Lezhë janë renditur si më poshtë:

- Të menaxhojë, mbikqyrë, vlerësojë dhe inspektojë institucionet arsimore parauniversitare për pajtueshmërinë e veprumtarisë së tyre me aktet ligjore dhe nënligjore në fuqi;

- Të sigurojë zbatimin e kurrikulës, metodologjive dhe standardeve në institucionet arsimore në bashkëpunim me ZVAP-të e varësisë;
- Të mbikqyrë veprimtarinë e përditshme dhe funksionimin e institucioneve arsimore, përmbushjen e detyrave administrative dhe rregullsinë e procesit mësimor;
- Të vlerësojë nevojat dhe problematikat gjatë ofrimit të shërbimit arsimor në rajonin verior dhe të propozojë zgjidhjen e tyre;
- Të garantojë mirëadminstrimin e burimeve njerëzore për institucionet publike të arsimit parauniversitar në rajonin përkatës si dhe shpërndarjen e tyre në varësi të aftësive, kontributit të gjithsëcilit dhe parimeve të drejtësisë dhe meritokracisë;
- Të garantojë ngritjen e rrjeteve profesionale të mësuesve si dhe përhapjen e praktikave dhe përvojave të susksesshmë të mësuesve;
- Të organizojë dhe mbështesë shërbimin psikosocial në instuticionet arsimore parauniversitare publike;
- Të kërkojë nga njësitë e vetëqeverisjen vendore mirëmbajtjen e infrastruktuës së institucioneve arsimore;
- Të grumbullojë dhe përpunojë të dhëna statistikore nga institucionet arsimore nën juridiksionin e tyre;
- Të shqyrtojë dhe vlerësojë kërkesat e ministrisë përgjegjëse për arsimin për përmbushjen e kritereve infrastrukturore për hapjen e institucioneve arsimore dhe ushtrimin e veprimtarisë në fushën e arsimit paruniversitar;
- Të sigurojë se funksionet e lidhura më planfikimin, zbatimin, kontabilitetin dhe raportimin financiar për institucionet publike të arsimit parauniversitar të kryhen në përputhje me legjislacionin në fuqi.

II.4 Përgjegjësitë e audituesve

Kontrolli i Lartë i Shtetit auditoi Drejtorinë Rajonale të Arsimit Parauniversitar Lezhë, mbi periudhën e veprimtarisë nga 01.01.2023 deri në 31.12.2024, 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. 1461/1 Prot, datë 06.01.2025, 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 DRAP Lezhë. 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. Audituesit kanë përgjegjësi në identifikimin e çështjeve më të rëndësishme lidhur me auditimin e veprimtarisë së subjektit, në raport me kriteret e paracaktuara të auditimit, të nxjerra nga aktet ligjore, nënligjore, si dhe ato rregullative mbi të cilat subjekti i audituar mbështetet në ushtrimin e veprimtarisë së tij.

II.5 Kriteret e vlerësimit

Kriteret e vlerësimit janë bazuar në ligjet, rregulloret në fuqi, standardet ndërkombëtare 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 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. 69/2012 “Për Sistemin Arsimor Parauniversitar në Republikën e Shqipërisë”, i ndryshuar me nr. 56/2015 dhe nr. 48/2018;
- Ligji nr. 43/2023 “Për Qeverisjen Elektronike”;
- Ligji nr. 9918, datë 10.03.2008 “Për Komunikimet Elektronike në Republikën e Shqipërisë”;
- Ligji nr. 10325, datë 23.09.2010 “Për bazat e të dhënave shtetërore”;
- Ligji nr. 2/2017 “Për sigurinë kibernetike”;
- Ligji nr. 9887, datë 10.03.2008, ndryshuar me Ligjin nr. 48/2012 “Për mbrojtjen e të dhënave personale”;
- VKM nr. 621, datë 22.10.2021 “Për miratimin e Strategjisë Kombëtare të Zhvillimit të Arsimit Parauniversitar 2021-2026”
-
- 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.
- Standardet TIK;
- Udhëzimi nr. 30, datë 27.12.2011 “Për Menaxhimin e Aktiveve në Njësitë e Sektorit Publik”, i ndryshuar;
- Akte të tjera ligjore apo nënligjore që ishin 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 DRAP Lezhë, 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. PËRSHRIMI I AUDITIMIT

1. Informacioni i përgjithshëm mbi subjektin nën auditim

Drejtoria Rajonale e Arsimit Parauniversitar Lezhë është krijuar me VKM nr. 99, datë 27.2.2019 “*Për krijimin, mënyrën e organizimit e të funksionimit të Drejtorisë së Përgjithshme të Arsimit Parauniversitar*”.

DRAP Lezhë ushtron veprimtarinë e tij në territorin që përmbledh dhjetë Zyra Vendore të Arsimit Parauniversitar, i cili organizohet në:
a) në nivel rajonal, nëpërmjet drejtorisë rajonale DRAP;
b) në nivel vendor, me njësitë e ofrimit direkt të shërbimeve të cilat përfshijnë zyrat vendore të arsimit parauniversitar ZVAP;
c) institucionet arsimore të sistemit parauniversitar public, shkollat –IA.
DRAP Lezhë ka mision ofrimin dhe sigurimin e shërbimit arsimor cilësor në të gjitha institucionet arsimore të sistemit parauniversitar në Zyrat Vendore në juridiksion, në përputhje me politikat, strategjitë kombëtare dhe kurrikulën e arsimit parauniversitar, me qëllim zhvillim dhe edukimin e plotë e të gjithanshëm të nxënësve, në mënyrë që të përballojë sfidat e së ardhmes.

2. Përshkrimi i rezultateve sipas drejtimeve të auditimit

2.1 Auditimi i funksionimit të Qeverisjes në TIK

1.a) "*Verifikimi i politikave, standardeve dhe vlerësimi i burimeve njerëzore në TIK*"

Në zbatim të pikës 1 "*Auditimi i funksionimit të Qeverisjes në TIK*" të Programit të Auditimit nr. 1461/1, datë 06.01.2025 u shqyrtua dokumentacioni si më poshtë:

- Akte ligjore / nënligjore, rregullore mbi të cilat institucioni kryen aktivitetin e tij;
- Urdhër nr. 144, datë 1.8.2024 "*Për Miratimin e Strukturës dhe të Organikës së Agjencisë Kombëtare dhe Drejtorive Rajonale të Arsimit Parauniversitar*" miratuar nga Kryeministri;
- Rregullore e Brendshme për organizimin dhe funksionimin e Drejtorisë Rajonale të Arsimit Parauniversitar;
- Regjistër risku për vitet 2023 - 2024;

Burimet njerëzore

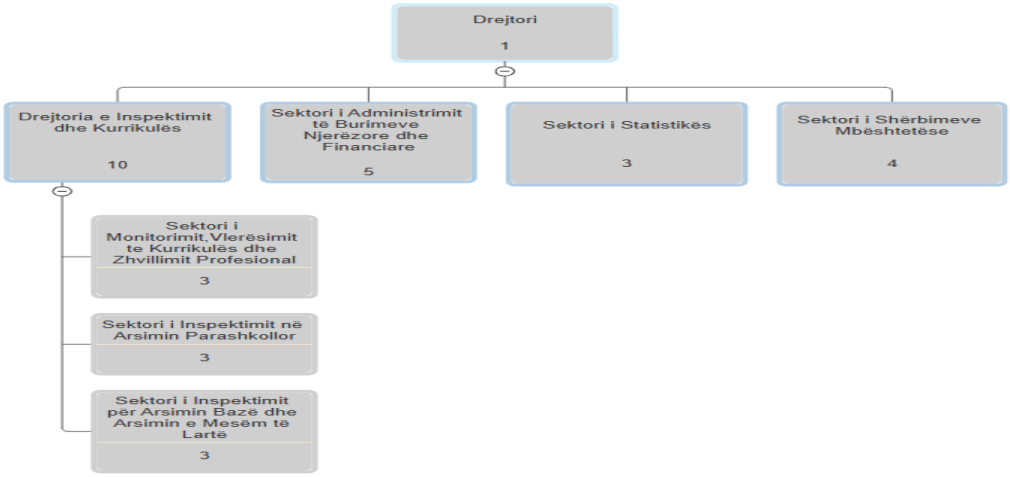
Drejtoria Rajonale e Arsimit Parauniversitar Lezhë është krijuar me VKM nr. 99, datë 27.2.2019 "*Për krijimin, mënyrën e organizimit e të funksionimit të Drejtorisë së Përgjithshme të Arsimit Parauniversitar*". Struktura e këtij institucioni është e përcaktuar me Urdhrin e Kryeministrit nr. 68, datë 05.04.2019 "*Për miratimin e strukturës dhe të organikës së Drejtorisë së Përgjithshme dhe Drejtorive Rajonale të Arsimit Parauniversitar*" të ndryshuar me Urdhrin nr. 144, datë 1.8.2024.
Nga auditimi u konstatua se në strukturën e miratuar institucioni ka një numër total prej 23 punonjësish, nga të cilët 2 janë pozicione vakante. Që nga krijimi i institucionit e deri më tani, DRAP Lezhë nuk ka pasur një punonjës TI por kjo fushë është mbuluar nga përgjegjësi i sektorit të kurrikulës, me profil mësuesi i cili ka kryer një sërë detyrash të parashikuara në përshkrimet e punës pa pasur kualifikimin e duhur në zbatim të tyre. Përshkrimet e punës të cilat i janë atashuar përgjegjësit të sektorit që kanë të bëjnë me teknologjinë e informacionit, janë si vijon:

- Merr informacion mujor nga shkollat mbi gjendjen e mjeteve elektronike të TIK-ut dhe të laboratorëve të kompjuterëve, verifikon gjendjen dhe raporton në DRAP dhe DPAP;
- Mbikëqyr instalimin e pjesëve hardware të kompjuterëve dhe pajisjeve të tjera teknologjike dhe software;
- Mirëmban rrjetin LAN në DRAP dhe ZVAP, mirëmban të gjitha pajisjet teknologjike të informacionit si dhe mirëmban shërbimin e internetit;
- Kontribuon që shërbimi i internetit dhe i laboratorëve në çdo shkollë të jetë në përputhje me parametrat e kontraktuara.

Nga auditimi u konstatua se përshkrimet e punës së punonjësve të DRAP Lezhë janë të mbivendosura dhe duhen rishikuar dhe përditësuar. Detyrat funksionale të punonjësve si dhe arsimimi i kërkuar për pozicionin e punës që ata mbulojnë jo në çdo rast është i duhuri për realizimin e objektivave të Drejtorisë dhe veprimtarisë institucionale.

Me miratimin e struktuës së re, DRAP Lezhë më 23.01.2025 ka rekrutuar një specialist TI, në sektorin e statistikës i cili do mbulojë çdo problematikë të hasur gjatë përdorimit të pajisjeve teknologjike apo me sistemet që institucioni ka në përdorim. Nga komunikimet e zhvilluara me grupin e auditimit ka rezultuar se specialisti nuk është trajnuar për përdorimin e sistemeve dhe ende nuk janë parashikuar përshkrimet e e tij të punës në rregulloren e brendshme sipas strukturës së re.

Figura nr.1 Organigrama e DRAP Lezhë



Burimi: *Drejtoria Rajonale e Arsimit Parauniversitar Lezhë. Punoi: Grupi i Auditimit*

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 shqyrtimi i dokumentacionit të vënë në dispozicion Drejtoria Rajonale e Arsimit Parauniversitar Lezhë sipas rregullores së brendshme miratuar me shkresën nr. 1237, datë 03.09.2019 "*Për organizimin dhe funksionimin e Drejtorisë Rajonale të Arsimit Parauniversitar Lezhë*", ka si mision kryesor ofrimin dhe sigurimin e shërbimit arsimor cilësor në të gjitha institucionet arsimore të sistemit paruniversitar në përputhje me politikat, strategjitë kombëtare dhe kurrikulën e arsimit parauniversitar, me qëllim zhvillimin dhe edukimin e nxënësve.

Nga auditimi u konstatua se Teknologjia e Informacionit në DRAP Lezhë zhvillohet në kushtet e mungesës së bazës rregullatore. Në DRAP Lezhë në mungesë të stafit në fushën e teknologjisë së informacionit nuk janë 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. 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.

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 Drejtorinë Rajonale të Arsimit Parauniversitar Lezhë është konstatuar se punonjësit 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 në fusha specifike të cilat do ti ndihmonin në rritjen profesionale, certifikimin dhe kualifikimin e mëtejshëm të tyre. Mungesa e trajnimeve sipas fushave përkatëse për punonjësit që kryejnë detyrat në fushën e teknologjisë së informacionit bën që për pasojë ata të mund mos të zbatojnë si duhet detyrat e përcaktuara në përshkrimet e punës sipas rregullores së DRAP.

III.2.2 Auditimi i sigurisë së informacionit dhe sistemeve

Në zbatim të pikës 2 "*Auditimi i sigurisë së informacionit dhe sistemeve*" të Programit të Auditimit nr. 1461/1, datë 06.01.2025, u shqyrtua dokumentacioni si më poshtë:

- Intervista të drejtpërdrejta me punonjës që kryenin apo administronin shërbime të caktuara;
- Indikatorë dhe statistika;
- Procedura e Menaxhimit të Aksesit.

DRAP Lezhë nuk ka sisteme ose aplikacione të teknologjisë së informacionit por është vetëm përdorues i sistemeve të krijuara nga AKSHI. Çdo sistem ka funksion dhe objektiva specifike, që synojnë përmirësimin e proceseve të ndryshme në realizimin e detyrave funksionale të institucionit të DRAP Lezhë.

Në vijim janë listuar sistemet tek të cilat DRAP Lezhë ka rol si përdorues:
1. **Platforma Checkpoint Harmony Connect** mbështet sektorin e arsimit në tre sisteme të veçanta:
- **Licensimi** i cili ka qëllim mundësimin e regjistrimit dhe certifikimit të mësuesve që kërkojnë të marrin licencë për të ushtruar mësimdhënie. Ky sistem përdoret si fillim nga specialistët e Zyrave Vendore të Arsimit Parauniversitar (ZVAP), të cilët bëjnë vlerësimin e dokumentacionit të ngarkuar nga ana e aplikantit, pastaj kalojnë për miratim në DRAP. Ky i fundit ka detyrim të bëjë rishikimin e dosjeve dhe miraton ose refuzon aplikimin në zbatim të legjislacionit në fuqi.
- **Portali "Mësues për Shqipërinë"** ka qëllim të shërbejë si platformë për mësuesit që dëshirojnë të punësohen, duke lehtësuar procesin e aplikimit dhe testimit. Nga auditimi ka rezultuar se nuk ka një manual përdorimi si dhe punonjësit nuk janë trajnuar për përdorimin e këtij sistemi por në rast se hasin problematika gjatë procesit të punës ata duhet ti drejtohen AKSHI-t.
- **Praktika Profesionale** e cila synon që kandidatët të cilët kanë përfunduar studimet për mësimdhënie, tu mundësohet praktika 3-mujore e detyrueshme. Nga auditimi ka rezultuar se nuk ka një manual përdorimi për këtë sistem dhe problematika që institucioni përballet më së shumti është që sistemi nuk lejon ngarkimin e të gjithë dokumenteve të parashikuara në Udhëzim dhe kandidatët janë të detyruar të ngarkojnë në një file dy deri në tre dokumente. Kjo problematikë është raportuar tek AKSHI por vijon të mbetet e pazgjidhur.
2. **HRMIS** është sistem i krijuar nga DAP dhe DRAP Lezhë është përdorues i Regjistrit Qendror të Personelit për të krijuar, administruar, përpunuar dhe reflektuar të dhëna që lidhen me dosjet e punonjësve në institucion si dhe është një burim planifikimi, informacioni dhe automatizimi për pagat. Aktualisht, ky sistem nuk është aktiv pasi DAP po kryen përditësimin e ndryshimeve ligjore.

3. **Platforma e Bashkëqeverisjes "Shqipëria që duam"** ka si qëllim menaxhimin më efikas dhe të shpejtë në kohë të trajtimit dhe kthimit të përgjigjeve ndaj ankesave të qytetarëve. DRAP Lezhë deri më 05.11.2024, ka trajtuar ankesat e drejtuara nga Zyra e Bashkëqeverisjes,

nëpërmjet email zyrtar të institucionit. Deri në këtë datë institucioni nuk ka pasur akses në sistemin e Platformës, përgjigjja e ankesave bëhej me email dhe kjo e fundit më pas trajtohej nga Zyra e Bashkëqeverisjes. Ndërkohë që prej datës 5.11.2024, ankesat e platformës së Bashkëqeverisjes delegohen me email të gjeneruar automatikisht.

4. **Sistemi i Menaxhimit të Informacionit Parauniversitar (SMIP)** ka qëllim menaxhimin e të dhënave të institucioneve arsimore. DRAP nuk ka akses të bëjë ndërhyrje direkt, por mban kontakte me ZVA-të për plotësimin në kohë dhe me saktësi të kurrikulave të shkollave dhe krijimin e klasave duke përcaktuar listën emërore përfundimtare të nxënësve për klasë dhe punonjësve. DRAP koordinon punën me **suportsmip** për problematika teknike të sistemit, por DRAP-eve dhe as ZVAP-ve nuk u është lënë akses të shkarkojnë të dhëna. DRAP mban komunikim të vazhdueshëm me kordinatorët e ZVA-ve mbi regjistrimet e plotësimet e regjistrave elektronik të mësuesve.

Mungesa e stafit TI ka sjell vështirësi në adresimin e mangësive që kanë dalë gjatë procesit të punës.

Siguria e informacionit është e rëndësishme 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 bashkëpërdorimi i burimeve të informacionit. Siguria e Informacionit mund të përcaktohet si metoda e një sistemi për të mbrojtur informacionin dhe burimet e sistemeve në përputhje me kushtet e konfidencialitetit, integritetit dhe gatishmërisë. Lidhur nga sa më sipër, 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 i shkallës së sigurisë 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.

Nga auditimi i Infrastrukturës Network dhe pajisjeve ndihmëse që nevojiten për shërbimet e komunikimit dhe ruajtjes së të dhënave është në kushtet minimale dhe jo optimale, ku shërbimet e ngritura mbi këto rrjete nuk janë të sigurta dhe nuk mbështesin vazhdimësinë e punës.

-Nga auditimi u konstatua se nuk ka një firewall të instaluar dhe të konfiguruar, duke e lënë atë të ekspozuar ndaj kërcënimeve të jashtme si sulmet kibernetike, skanimet e portave dhe përpjekjet për hyrje të paautorizuar. Mungesa e një firewall-i gjithashtu e bën të vështirë monitorimin dhe filtrimin e trafikut të rrjetit për të parandaluar aktivitetet keqdashëse.

-Nga auditimi u konstatua se pajisjet kompjuterike të punës nuk kanë të instaluar një antivirus ose një zgjidhje për mbrojtjen e pikave fundore (endpoint protection), duke i bërë ato të cenueshme ndaj malware-ve, ransomware-ve dhe viruseve. Pa një sistem të mbrojtjes aktive, përdoruesit mund të hapin pa dijeni email-e phishing ose të shkarkojnë skedarë të infektuar, duke rritur rrezikun e kompromitimit të të dhënave dhe sulmeve të brendshme.

-Nga auditimi u konstatua se nuk ekzistojnë politika të qarta për menaxhimin e aksesit të përdoruesve. Punonjësit ndajnë të njëjtat llogari të përdoruesve për hyrje në sistemet dhe aplikacionet e brendshme, gjë që e bën të pamundur gjurmimin e aktiviteteve individuale. Për më tepër, mungesa e një sistemi të bazuar në role mund të çojë në ekspozimin e të dhënave të ndjeshme ndaj punonjësve që nuk kanë nevojë për to, duke krijuar rreziqe të brendshme.

-Nga auditimi u konstatua se përdoruesit nuk ndjekin një politikë për krijimin dhe ruajtjen e fjalëkalimeve. Nuk ka një sistem për të detyruar përdorimin e fjalëkalimeve të forta dhe

ndërrimin periodik të tyre, duke e bërë të lehtë për sulmuesit që të kryejnë sulme brute-force ose credential stuffing për të fituar akses të paautorizuar.
-Nga auditimi u konstatua se nuk ka një rregullore për backup-in e të dhënave të rëndësishme. Nuk kryhen kopje rezervë në mënyrë të rregullt dhe nuk ka një sistem për ruajtjen e kopjeve rezervë. Kjo e ekspozon institucionin ndaj humbjes së të dhënave në rast të një sulmi ransomware, dështimi të harduerit ose gabimeve njerëzore.
-Nga auditimi u konstatua se Kompjuterat e punës, printerat dhe ruterët lihen të ekspozuara fizikisht, pa asnjë masë sigurie për të parandaluar aksesin e paautorizuar. Nuk ka kontrolle hyrjeje në ambientet ku ndodhen pajisjet, duke rritur rrezikun e manipulimit të qëllimshëm ose vjedhjes së të dhënave përmes pajisjeve të paautorizuara.
-Nga auditimi u konstatua se DRAP Lezhë përdor ruterë të ndryshëm në çdo zyrë pa ndonjë sistem të centralizuar për monitorim dhe menaxhim. Kjo çon në mungesën e politikave të standardizuara të sigurisë dhe e bën të vështirë aplikimin e kontrolleve të rrjetit për të gjitha zyrat në mënyrë të njëtrajtshme. Mungesa e një qendre të menaxhimit të rrjetit e bën gjithashtu më të ndërlikuar identifikimin dhe zgjidhjen e problemeve të sigurisë ose sulmeve kibernetike.

IV. REKOMANDIME

A. MASA ORGANIZATIVE

1. Gjetje nga auditimi: Nga auditimi i strukturës organizative të Drejtorisë Rajonale Arsimore Parauniversitare (DRAP) Lezhë u konstatua se, që prej krijimit të institucionit, nuk ka qenë i parashikuar një pozicion i dedikuar për një specialist të fushës së teknologjisë së informacionit (TI). Si rrjedhojë, funksionet që lidhen me menaxhimin e TI-së janë kryer nga përgjegjësi i sektorit të kurrikulës, i cili nuk zotëron kualifikimet e nevojshme për këtë fushë. Gjithashtu, u konstatua mbivendosje në përshkrimet e punës së stafit, ku në disa raste kualifikimet e punonjësve nuk përputheshin me kërkesat përkatëse të pozicionit të tyre sipas kërkesave të ligjit nr.10296, datë 08.07.2010, "Për menaxhimin financiar dhe kontrollin". Me miratimin e strukturës së re më datë 23.01.2025, është rekrutuar një specialist TI në sektorin e statistikës për të mbuluar nevojat teknologjike të institucionit.
(Më hollësisht trajtuar në pikën 1, faqet 9-11, të Raportit Përfundimtar të Auditimit)
1.1 Rekomandimi: Drejtoria Rajonale Arsimore Parauniversitare Lezhë, të marrë masa për përditësimin e rregullores së brendshme dhe përshkrimeve të punës, në përputhje me strukturën e re organizative, duke i përshtatur ato me detyrat funksionale dhe përgjegjësitë reale të çdo pozicioni.

Menjëherë

2. Gjetje nga auditimi: Nga auditimi i kryer u konstatua se Drejtoria Rajonale Arsimore Parauniversitare (DRAP) Lezhë operon në fushën e teknologjisë së informacionit (TI) në mungesë të një baze të mirëfilltë rregullatore. Mungesa e stafit të specializuar ka ndikuar në mos hartimin e rregullave dhe procedurave të nevojshme për menaxhimin e proceseve të TI-së, sipas kërkesave të ligjit nr.10296, datë 08.07.2010, "Për menaxhimin financiar dhe kontrollin". Institucioni nuk disponon dokumentacion bazë si rregulloren për funksionimin e veprimtarisë së TI-së apo procedurat për menaxhimin e incidenteve kibernetike. Kjo situatë ka çuar në një funksionim të paorganizuar, duke rritur riskun ndaj situatave të paparashikuara, me përgjegjësi të paqarta dhe kohë reagimi të papërcaktuar në rast emergjencash.
(Më hollësisht trajtuar në pikën 1, faqet 9-11, të Raportit Përfundimtar të Auditimit)
2.1 Rekomandimi: DRAP Lezhë të marrë masa për hartimin e një Rregulloreje të Përgjithshme për Teknologjinë e Informacionit, duke garantuar vendosjen e kontrolleve të brendshme për menaxhimin e riskut dhe sigurimin e përputhshmërisë me procedurat e brendshme, rregullat ekzistuese dhe kuadrin ligjor në fushën e TI-së.

Menjëherë

3.Gjetje nga auditimi: Nga auditimi u konstatua se infrastruktura e rrjetit në DRAP Lezhë është e shpërndarë dhe jo në gjendje optimale, me përdorimin e ruterëve të ndryshëm në çdo zyrë dhe pa një sistem të centralizuar për menaxhim dhe monitorim. Kjo situatë sjell mungesë unifikimi në politikat e sigurisë, duke vështirësuar kontrollin e rrjetit dhe garantimin e vazhdimësisë së shërbimeve. Gjithashtu, mungesa e një qendre të menaxhimit të rrjetit pengon identifikimin dhe adresimin në kohë të problemeve, duke ekspozuar infrastrukturën ndaj rreziqeve kibernetike dhe dështimeve operacionale.
(Më hollësisht trajtuar në pikën 2, faqet 11-13, të Raportit Përfundimtar të Auditimit)
3.1 Rekomandimi: Drejtoria Rajonale Arsimore Parauniversitare Lezhë të marrë masa për të centralizuar monitorimin dhe administrimin e rrjetit në të gjitha zyrat, për të siguruar një menaxhim më efikas të infrastrukturës. Implementimi i një qendre të menaxhimit të rrjetit do të ndihmojë në aplikimin e politikave të sigurisë në mënyrë të njëtrajtshme dhe do të lehtësojë identifikimin dhe trajtimin e incidenteve të mundshme të sigurisë.

Menjëherë dhe në vijimësi

4.Gjetje nga auditimi: Nga auditimi u konstatua se nuk ka një firewall (mbrojtës të rrjetit) të instaluar dhe të konfiguruar, duke e lënë atë të ekspozuar ndaj kërcënimeve të jashtme, si sulmet kibernetike, skanimet e portave dhe përpjekjet për hyrje të paautorizuar. Mungesa e një firewall-i gjithashtu e bën të vështirë monitorimin dhe filtrimin e trafikut të rrjetit për të parandaluar aktivitetet keqdashëse.
(Më hollësisht trajtuar në pikën 1, faqet 11-13, të Raportit Përfundimtar të Auditimit)
4.1 Rekomandimi: Drejtoria Rajonale e Arsimit Parauniversitar Lezhë, të marrë masa për instalimin dhe konfigurimin e një firewall-i, që mund të monitorojë dhe filtrojë trafikun e rrjetit, duke parandaluar sulmet kibernetike dhe aksesin e paautorizuar, me qëllim identifikimin dhe bllokimin e sulmeve, si dhe sigurimin e një kontroll më të mirë mbi trafikun e rrjetit.

Menjëherë dhe në vijimësi

5.Gjetje nga auditimi: Nga auditimi u konstatua se pajisjet kompjuterike të punës nuk kanë të instaluar një antivirus ose një zgjidhje për mbrojtjen fundore (endpoint protection), duke i bërë ato të cenueshme ndaj malware-ve, ransomware-ve dhe viruseve. Në mungesë të një sistemi të mbrojtjes aktive, përdoruesit janë të ekspozuar ndaj email-eve phishing dhe mund të shkarkojnë pa dijeni skedarë të infektuar, duke rritur rrezikun e kompromitimit të të dhënave dhe sulmeve të brendshme.
(Më hollësisht trajtuar në pikën 2, faqet 11-13, të Raportit Përfundimtar të Auditimit)
5.1 Rekomandimi: Drejtoria Rajonale e Arsimit Parauniversitar Lezhë, të marrë masa për të rritur sigurinë, duke instaluar antivirus dhe përditësimet e tij, të kryejë skanime të rregullta, si dhe të implementojë mbrojtje kundër email-eve phishing dhe faqeve të dyshimta.

Në vijimësi

6.Gjetje nga auditimi: Nga auditimi u konstatua se mungojnë politikat e qarta për menaxhimin e aksesit të përdoruesve. Punonjësit ndajnë llogari të përbashkëta për hyrjen në sistemet dhe aplikacionet e brendshme, duke e bërë të pamundur gjurmimin e aktiviteteve individuale. Gjithashtu, mungesa e një sistemi bazuar në role mund të ekspozojë të dhënat e ndjeshme ndaj punonjësve që nuk kanë nevojë për to, duke krijuar rreziqe të brendshme.
(Më hollësisht trajtuar në pikën 2, faqet 11-13, të Raportit Përfundimtar të Auditimit)
6.1 Rekomandimi: Drejtoria Rajonale e Arsimit Parauniversitar Lezhë, të marrë masa për përmirësimin e menaxhimit të aksesit të përdoruesve, duke implementuar një sistem bazuar në role, i cili kufizon qasjen në informacion vetëm për punonjësit që e kërkon pozicioni i tyre. Duhet të ndalohet përdorimi i përbashkët i llogarive të njëjta nga disa përdorues, ndërsa

monitorimi i vazhdueshëm i aksesit është i domosdoshëm për të identifikuar dhe përjashtuar përdoruesit e paautorizuar, duke garantuar kështu integritetin dhe sigurinë e të dhënave të institucionit.

Menjëherë

7.Gjetje nga auditimi: Nga auditimi u konstatua se përdoruesit nuk ndjekin një politikë të qartë, për përdorimin e fjalëkalimeve të forta dhe ndërrimin e tyre periodik, duke e lehtësuar për sulmuesit realizimin e sulmeve brute-force ose credential stuffing, për të fituar akses të paautorizuar.
(Më hollësisht trajtuar në pikën 2, faqet 11-13, të Raportit Përfundimtar të Auditimit)
7.1 Rekomandimi: Drejtoria Rajonale e Arsimit Parauniversitar Lezhë, të forcojë politikën e fjalëkalimeve, duke implementuar një sistem që detyron përdorimin e fjalëkalimeve të forta dhe ndërrimin e tyre periodik, si dhe të vendosë mekanizma për të kufizuar përpjekjet e shumta të dështuara për hyrje, me qëllim parandalimin e sulmeve brute-force dhe credential stuffing.

Menjëherë

8.Gjetje nga auditimi: Nga auditimi u konstatua se nuk ka një rregullore për backup-in e të dhënave të rëndësishme, si dhe nuk kryhen kopje rezervë të rregullta, duke ekspozuar institucionin ndaj humbjes së të dhënave në rast të sulmeve ransomware, dështimeve të pajisjeve fizike ose gabimeve njerëzore.
(Më hollësisht trajtuar në pikën 2, faqet 11-13, të Raportit Përfundimtar të Auditimit)
8.1 Rekomandimi: Drejtoria Rajonale e Arsimit Parauniversitar Lezhë, të marrë masa për krijimin e kopjeve rezervë në intervale të rregullta dhe ruajtjen e tyre në vende të sigurta, për të garantuar rikuperimin e shpejtë të informacionit në rast incidenti. Po ashtu, backup-et duhet të testohen periodikisht për të siguruar funksionimin e duhur të tyre.

Menjëherë dhe në vijimësi

9.Gjetje nga auditimi: Nga auditimi u konstatua se kompjuterat, printerat dhe ruterët lihen të ekspozuara fizikisht, pa asnjë masë sigurie për të parandaluar aksesin e paautorizuar, pasi nuk ka kontrolle hyrjeje në ambientet ku ndodhen pajisjet, duke rritur rrezikun ndaj vjedhjes së të dhënave dhe aksesimit përmes pajisjeve të paautorizuara.
(Më hollësisht trajtuar në pikën 2, faqet 11-13, të Raportit Përfundimtar të Auditimit)
9.1 Rekomandimi: Drejtoria Rajonale e Arsimit Parauniversitar Lezhë, të marrë masa për të forcuar sigurinë fizike të pajisjeve kompjuterike, printerave dhe ruterëve, duke kufizuar hyrjen në ambientet ku ndodhen pajisjet. Gjithashtu, institucioni të marrë masa për të ndaluar lidhjen e pajisjeve të paautorizuara në rrjet, për të parandaluar shpërndarjen e mundshme të malware-ve ose qasjen e paautorizuar në sistemet e brendshme.

Menjëherë

Për sa më sipër paraqitet ky Raport Përfundimtar Auditimi.

KONTROLLI I LARTË I SHTETIT