RAPORT PËRFUNDIMTAR I AUDITIMIT

"PËR AUDITIMIN E SISTEMEVE TË TEKNOLOGJISË SË INFORMACIONIT"

Tiranë, më 31.05.2020

PËRMBAJTJA

I. 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 Institutin e Gjeoshkencave, Energjisë, Ujit dhe Mjedisit (IGJEUM), nga data 21.01.2020 deri në 31.03.2020.

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.a Përshkrimi i Auditimit:

Auditimi i Sistemeve të Teknologjisë së Informacionit, në Institutin e Gjeoshkencave, Energjisë, Ujit dhe Mjedisit (IGJEUM), është pjesë e Planit Vjetor të auditimit të KLSH-së, miratuar nga Kryetari i KLSH, si dhe Planit Mujor, janar 2020. 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 IGJEUM disponon, për të garantuar disponibilitet dhe integritet të të dhënave me të cilat bazon vendimmarrjen.
Siguria e Informacionit është bërë gjithnjë e më shumë e rëndësishme për institucionet, kjo si pasojë 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 mund të përcaktohet si mundësia e një sistemi për të mbrojtur informacionin dhe burimet e sistemeve në përputhje me termat e konfidencialitetit, integritetit dhe gatishmëria. 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 komunikimeve dhe operacioneve, 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.b Një përshkrim i përmbledhur i gjetjeve dhe rekomandimeve nga auditimi:

Gjetjet kryesore, të paraqitura në këtë Raport Auditimi në mënyrë të përmbledhur sipas drejtimeve të auditimit, rezultuan si më poshtë:

Gjetja Nr.	Përmbledhje e Gjetjes	Referenca me Raportin Përfundimtar	Rëndësia	Rekomandimi
1	Nga auditimi u konstatua se Instituti i Gjeoshkencave, Energjisë, Ujit dhe Mjedisit nuk ka në përbërje strukturë të teknologjisë së informacionit, madje asnjë pozicion specialisti IT, duke krijuar risk të lartë mbi identifikimin, trajtimin dhe zgjidhjen e problematikave të ndryshme të	faqe 8-15	e lartë	Strukturat drejtuese të IGJEUM dhe UPT të marrin masa për krijimin e një strukture të Teknologjisë së

	Teknologjisë së Informacionit në institucion. Si institucion nën varësinë e Universitetit Politeknik të Tiranës, IGJEUM duhet të ketë suportin e specialistëve IT të Universitetit Politeknik të Tiranës. UPT ka në strukturën e tij 7 Fakultete dhe IGJEUM, dhe për mbulimin e problematikave në fushën e IT, ka vetëm 2 specialistë të fushës të atashuar në zyrat e UPT. Në të tilla kushte, problemet që hasen në IGJEUM në fushën e Teknologjisë së Informacionit gjejnë zgjidhje pothuajse gjithnjë nëpërmjet vetë stafit të cilët kanë njohuri në këtë fushë.			Informacionit në IGJEUM, në nivel sektori apo drejtorie, me qëllim përmbushjen e nevojave institucionale mbi identifikimin, trajtimin dhe zgjidhjen e problematikave të ndryshme të Teknologjisë së Informacionit.
2	Nga auditimi mbi investimet e kryera në fushën e Teknologjisë së Informacionit, u konstatua se ato janë në përpjesëtim të zhdrejtë me rëndësinë kombëtare që ka monitorimi i aktivitetit sizmik, meteorologjik dhe hidrologjik. Pasojat e mungesës së investimeve të domosdoshme në drejtim të teknologjisë së informacionit dhe më gjerë, janë vënë re gjatë ngjarjeve të fundit në vend. Konkretisht, referuar regjistrimeve të vëna në dispozicion nga Departamenti i Sizmologjisë në IGJEUM në lidhje me tërmetin e datës 26.11.2019, i cili ka patur impakt në jetë njerëzish dhe dëme të shumta materiale, konstatohet se mungojnë të dhëna të plota nga stacioni i Durrësit, i cili është stacioni më i afërt me vatrën e tërmetit. Ky stacion ka regjistruar vetëm 15 sekondat e para të tërmetit, si pasojë e ndërprerjes së energjisë elektrike. Nisur nga fakti që gjatë një tërmeti të fortë ekziston një probabilitet i lartë për ndërprerjen e energjisë elektrike, është e domosdoshme pajisja e stacioneve sizmologjike me bateri (UPS) të cilat mundësojnë regjistrimin e të dhënave edhe nëse ndërpritet energjia elektrike. Theksojmë se funksionimi i rregullt i tre rrjeteve sizmike në vendin tonë është i rëndësishme për parashikimin dhe monitorimin e katastrofave natyrore në kohë reale, duke marrë masa në drejtim të mbrojtjes së jetës së njerëzve dhe reduktimin e dëmeve materiale.	faqe 8-15	e lartë	IGJEUM në bashkëpunim me UPT, duke marrë shkas edhe nga problematikat e shfaqura gjatë tërmetit të datës 26.11.2019, të marrin masat e nevojshme për analizimin e situatës dhe hartimin e një plan veprimi të ndarë në 3 faza, afat shkurtër, afat mesëm dhe afat gjatë, për kryerjen e ndërhyrjeve në sistemet IT si dhe në ambientet fizike ku këto sisteme janë, me qëllim krijimin e kushteve të përshtatshme për mbledhjen, përpunimin dhe ruajtjen e të dhënave që këto sisteme kanë, në përputhje me standardet dhe praktikat më të mira të fushës.
3	Nga auditimi u konstatua se IGJEUM nuk disponon një Plan Vazhdimësie (BCP) dhe Plan Rikuperimi (DRC) për garantimin e vazhdimësisë së ofrimit të shërbimit, duke krijuar risk për humbjen e të dhënave, veprim në kundërshtim me pikën 1 të VKM Nr. 710, datë 21.8.2013 "Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit", i ndryshuar.	faqe 15-20	e lartë	IGJEUM duke marrë në konsideratë kohën dhe burimet e nevojshme të marrë masa për ndërtimin dhe hartimin e Planit të Vazhdimësisë dhe Planit të Rikuperimit, duke përfshirë planet për backup dhe rimëkëmbjen nga katastrofat për sistemet, pajisjet kompjuterike dhe të dhënat, hartimin e planit të sigurisë së informacionit dhe implementimin e tij, duke përfshirë ndarjen e detyrave/përgjegjësive të sigurisë në TIK.
4	Nga auditimi u konstatua se IGJEUM nuk ka asnjë menaxhim dhe informacion se çfarë ndodh në rrjetin DATA në të gjitha pikat e saj, duke cënuar sigurinë e informacionit. Gjithashtu mungesa e aksesit dhe mos konfigurimi i saktë, ndikon në rritjen e mundësisë së hyrjes të paautorizuar në sistemet dhe databazat e IGJEUM.	faqe 21-24	e lartë	IGJEUM dhe UPT të marrin masat për planifikimin e ndërtimit të një sistemi monitorimi, i cili të monitorojë Infrastrukturat Network, OS, Sigurinë dhe trafikun në kohë reale.
5	Siguria mbi portat e aksesit në zyrën qendrore nga ku është	faqe 24-30	e lartë	IGJEUM të marrë masa

	konfiguruar edhe routeri ryesor me IP Publike nuk ka të konfiguruar mbrojtjen në portat e aksesit për jashtë. Nga një testim i bërë nga grupi i auditimit, rezulton se portat e aksesit nga jashtë [redacted], [redacted], [redacted] janë të hapura. Në këto kushte në rastin e një sulmi, IGJEUM është i ekspozuar ndaj hyrjeve të pa autorizuara në sistemet që ajo përdor.			për bllokimin e menjëhershëm të portave të aksesit për kategoritë Network dhe Sistemet e Operimit. Gjithashtu duhet të krijohet një script në routerin kryesor e cila duhet të monitorojë dhe bllokojë në kohe reale të gjitha IP-të që tentojnë hyrje të pa autorizuara.

I.c Konkluzioni dhe Opinioni i Auditimit:

Grupi i auditimit 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 konstaton se: Ushtrimi i aktivitetit të IGJEUM me 67.6 % të organikës, dhe përdorimi i Teknologjisë së Informacionit pa strukturë IT, mbart risk në plotësimin e detyrave institucionale si:

- Studimi dhe vlerësimi i fenomeneve gjeologjike e burimeve natyrore të vendit;
- Vlerësimi i riskut sizmik, meteorologjik dhe hidrik në shkallë lokale dhe kombëtare;
- Monitorimi 24/7 i aktivitetit sizmik, meteorologjik dhe hidrik të vendit, duke mundësuar shpërndarjen e të dhenave në kohë reale për vendimmarrësit dhe opinionin e gjerë.

Mungesa e akteve rregullatore, mos trajtimi dhe zgjidhja e problematikave të shfaqura, ka sjellë situatë me risk të lartë në drejtim të sigurisë së të dhënave. Mungesa e gjurmës së auditimit nuk jep siguri të arsyeshme mbi rregullshmërinë e përdorimit të sistemeve në IGJEUM.

Ekzistenca e IGJEUM nën varësinë e Universitetit Politeknik të Tiranës, i cili ka si qëllim kryesor përmirësimin e aktivitetit universitar, ka ndikuar në një mungesë të theksuar të vëmendjes për krijimin e kushteve të favorshme për zhvillimin pa ndërprerje të monitorimit të aktivitetit sizmik, meteorologjik dhe hidrologjik, objekt i cili në mungesë mund të ndikojë në jetë njerëzish dhe dëme materiale tejet të konsiderueshme. Mungesa e vëmendjes ndaj IGJEUM evidentohet dukshëm në gjendjen e stacioneve të shpërndara në të gjithë territorin e vendit, të cilat rrezikojnë të mos përmbushin plotësisht objektin e tyre, ose të dëmtohen në mënyrë të pariparueshme.

II. HYRJE

Mbështetur në Ligjin 154/2014, datë 27.11.2014 "*Për Organizimin dhe Funksionimin e KLSH*", në zbatim të Programit të Auditimit nr. 69/1, datë 11.02.2020 miratuar nga Kryetari i KLSH, me afat auditimi 21.01.2020 deri në 31.03.2020, në Institutin e Gjeoshkencave, Energjisë, Ujit dhe Mjedisit (IGJEUM), ku periudha e audituar është 01.01.2019 deri në 31.12.2019, u krye auditimi mbi "Auditimin e Sistemeve të Teknologjisë së Informacionit", me Grup Auditimi të përbërë nga:

[redacted]

II.a Titulli: Auditimi Sistemeve të Teknologjisë së Informacionit në Institutin e Gjeoshkencave, Energjisë, Ujit dhe Mjedisit (IGJEUM).

II.b Marrësi: Instituti i Gjeoshkencave, Energjisë, Ujit dhe Mjedisit (IGJEUM).

III.c Objektivat dhe qëllimi:
Objekti i Auditimit TIK ushtruar në IGJEUM, është përcaktimi nëse objektivat e subjektit arrihen në mënyrën e duhur duke përdorur burimet IT, duke përfshirë pajtueshmërinë me kërkesat ligjore dhe rregullatorë, konfidencialitetit, integritetin si dhe disponueshmërinë e sistemeve të informacionit dhe të dhënave që gjenden në të.
Qëllimi i Auditimit TIK ushtruar në IGJEUM, është dhënia e opinionit apo vlerësimi nëse ekzistojnë kontrollet dhe mekanizmat e duhur me qëllim krijimin/ mirëmbajtjen/ zhvillimin e burimeve IT dhe funksioneve për të cilat këto burime shërbejnë.
Objektivat e këtij projekt auditimi, u vendosën në koherencë me veprimtarinë, vizionin, qëllimin dhe objektivat në IGJEUM, duke marrë në konsideratë të gjithë kuadrin rregullator në bazë të të cilit institucioni zhvillon veprimtarinë e tij. Për të arritur në dhënien e një opinioni, është mbledhur informacion, të dhëna dhe prova, për të përcaktuar nëse nëpërmjet teknologjisë mbrohen asetet, ruhet integriteti i të dhënave, ndihmon realizimin e synimeve të subjektit që auditohet të arrihen në mënyrë efektive duke përdorur burimet në mënyrë efiçente.

II.d Identifikimi i çështjeve:
Pas marrjes së informacionit nga subjekti nëpërmjet pyetësorit të dërguar në mënyrë elektronike dhe përpunimit të tij nga grupi i auditimit, analizës së riskut nëpërmjet manualit aktiv të auditimit IT, si dhe vlerësimin e informacioneve nga burime të jashtme, kanë rezultuar si fusha me risk më të lartë:

1. Auditimi i funksionimit të Qeverisjes TIK
a. Verifikim i strategjisë, politikave dhe procedurave dhe vlerësimi i burimeve njerëzore në TIK.
b. Vlerësimi i menaxhimi i riskut nga strukturat drejtuese.
2. Operacionet IT
a. Procedurat e menaxhimit të problemeve dhe incidenteve të institucionit.
b. Menaxhimi i ndryshimit.
3. Auditimi i sigurisë së informacionit
a. Siguria e të dhënave dhe vazhdimësia në ofrimin e shërbimit.
b. Kontrollet e sigurisë së aplikacionit.
c. Të drejtat e përdoruesve dhe menaxhimi i tyre.
4. Auditim me zgjedhje i rrjetit të stacioneve sizmologjike dhe meteorologjike në Republikën e Shqipërisë.

II.e Përgjegjësitë e strukturave drejtuese:

Instituti i Gjeoshkencave, Energjisë, Ujit dhe Mjedisit është një njësi kombëtare kërkimore shkencore që vepron nën ombrellën e Universitetit Politeknik të Tiranës. Nga pikëpamja organizative është hartuar në 5 departamente kryesore, secila prej tyre përmban deri në tre njësi kërkimore.

Këto departamente janë:

1. Departamenti i Klimës dhe Mjedisit
2. Departamenti i Gjeologjisë
3. Departamenti i Sizmologjisë
4. Departamenti i Ekonomisë së Ujrave

Organet drejtuese të Institutit janë:

Këshilli i Institutit
Drejtori
Përgjegjësit e departamenteve

Misioni i Institutit të Gjeoshkencave Energjisë, Ujit dhe Mjedisit është përmirësimi i kërkimit shkencor në fushën e gjeoshkencave në Shqipëri nëpërmjet:

- kryerjes së kërkimeve shkencore dhe aplikative
- udhëheqjes në procesin arsimor të studentëve dhe studiuesve të rinj
- ndërmarrjen e shërbimeve me të tretë në fushat e sizmologjisë, burimeve natyrore, gjeoriskut, gjeologjisë, ujit dhe mjedisit.

Detyrat kryesore të këtij Instituti janë:

- Studimi i fenomeneve gjeologjike si fenomenet gjeofizike, gjeomekanike etj dhe krijimi mbi bazën e tyre i hartave gjeologjike dhe tematike
- Studimi dhe vlerësimi i burimeve natyrore të vendit për sa i përket burimeve nëntokësore mi nerale, energjetike dhe atyre ujore.
- Realizim i kërkimit shkencor në fushën e rreziqeve natyrore si dhe të atyre të krijuara nga aktiviteti i njeriut (rrëshqitje, erozion,përmbytje, ndotje e mjedisit etj).
- Studim i mikrozonimit në lidhje me vlerësimin e riskut sizmik në shkallë lokale dhe kombëtare.
- Adoptimi i standarteve europiane në studimet sizmike.
- Studimi dhe monitorimi i vazhdueshëm i aktivitetit sizmik të vendit dhe mundësimi i shpërndarjes së të dhenave në kohë reale për vendimmarrësit dhe opinionin e gjerë.
- Zhvillimi i gjeomodeleve të cilat mbështesin kërkimin shkencor në fushat e gjeofizikës, gjeologjisë, gjeomjedisit, sizmologjisë, energjisë termale etj të bazuar këto në teknologjinë bashkëkohore të gjeoinformacionit.

II.f Përgjegjësitë e audituesve:

Kontrolli i Lartë i Shtetit auditoi Institutin e Gjeoshkencave, Energjisë, Ujit dhe Mjedisit, mbi periudhën e veprimtarisë nga 01.01.2019 deri në 31.12.2019, 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. 69/1, datë 11.02.2020 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 IGJEUM. Gjithashtu, gjatë veprimtarisë

adituese, është siguruar një evidencë e përshtatshme, e mjaftueshme dhe e besueshme auditimi, në të cilën jemi mbështetur në dhënien e konkluzioneve dhe rekomandimeve.

II.g Kriteret e vlerësimit:

Kriteret e vlerësimit bazohen në ligjet, rregulloret në fuqi, standardet e përcaktuara nga AKSHI si dhe ato ndërkombëtare COBIT dhe ISSAI 5300 për auditimin e Teknologjisë së Informacionit, Manuali i Teknologjisë së Informacionit. Opinionet dhe konkluzionet e nxjerra nga auditimi janë mbështetur në Standardet Kombëtare dhe Ndërkombëtare të Auditimit, janë dokumentuar në aktet e mbajtura, observacionet mbi to gjenden të reflektuara në projekt raport, gjithashtu rekomandimet për përmirësimin e gjendjes.
Veprimtaria e MFE dhe AKSHI-t, mbështetet në bazën ligjore 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. 10296, datë 08.07.2010 "*Për Menaxhimin Financiar dhe Kontrollin*", i ndryshuar dhe aktet ligjore në zbatim të tij;
- Ligji nr. 9643, date 20.11.2006 "*Për Prokurimin Publik*", i ndryshuar;
- Ligji nr. 114/2015 "*Për Auditimin e Brendshëm në Sektorin Publik*";
- Legjislacioni mbi Krimin Kibernetik;
- Ligji Nr. 9918, datë 19.05.2008, "*Për Komunikimet Elektronike në Republikën e Shqipërisë*";
- Ligji Nr. 10325, datë 23.09.2010, "*Për Bazat e të Dhënave Shtetërore*";

Ligji nr. 9887, datë 10.03.2008, ndryshuar me ligjin nr. 48/2012 "*Për Mbrojtjen e të Dhënave Personale*".

- Ligji nr. 9741, datë 21.5.2007 "Për arsimin e lartë në Republikën e Shqipërisë", i ndryshuar.

II.h Standardet e auditimit:

Auditimi është kryer, në përputhje me Kodin Etik, Standardet, dhe teknika auditimi, 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.

III. GJETJET DHE REKOMANDIMET:

1. Auditimi i funksionimit të Qeverisjes TIK

a. Verifikim i strategjisë, politikave dhe procedurave dhe vlerësimi i burimeve njerëzore në TIK.

b. Vlerësimi i menaxhimi i riskut nga strukturat drejtuese.

Nga auditimi u konstatua se:

Struktura

IGJEUM e mbështet aktivitetin e saj në ligjin Nr. 85/2015 "Për Arsimin e Lartë dhe Kërkimin Shkencor në Republikën e Shqipërisë". Ky institucion është krijuar me Urdhrin e Ministrit të Arsimit dhe Shkencës Nr. 371 datë 28.07.2011 "Për Krijimin e Institutit të Gjeoshkenave dhe

Energjisë, Ujit dhe Mjedisit, si njësi kryesore pranë Universitetit Politeknik të Tiranës".
Struktura e IGJEUM është miratuar me Vendimin e Këshillit të Administrimit të UPT Nr. 2, datë 03.02.2017.
IGJEUM ka një numër total prej 71 punonjësish, si dhe 263 me kontratë. Aktualisht në administratën e IGJEUM janë të punësuar vetëm 48 punonjës, pra 23 më pak se organika e miratuar, ose 67.6%.
Gjithashtu, konstatohet se IGJEUM nuk ka në përbërje strukturë të Teknologjisë së Informacionit, si dhe asnjë pozicion specialisti IT.
Për sa i përket problematikave të ndryshme të dala gjatë punës rutinë në drejtim të Teknologjisë së Informacionit, IGJEUM duhet të ketë suportin e specialistëve IT të Universitetit Politeknik të Tiranës. Theksojmë se gjithë struktura e UPT, ku përfshihen 7 Fakultete dhe IGJEUM, ka vetëm 2 specialistë IT të atashuar në zyrat e UPT. Në të tilla kushte, problemet që hasen në IGJEUM në fushën e Teknologjisë së Informacionit gjejnë zgjidhje pothuajse gjithnjë nëpërmjet vetë stafit të cilët kanë njohuri në këtë fushë.
Që qeverisja e IT të sigurohet se investimet në IT gjenerojnë vlerë për institucionin, dhe se risqet e lidhura me IT janë të reduktuara, është e rëndësishme që të ekzistojnë struktura organizative me role të mirë-përcaktuara për përgjegjësinë e informacionit, proceseve të institucionit, aplikacioneve dhe infrastrukturës.
Aktualisht IGJEUM ka vetëm 1 (një) punonjës me profil IT, i cili është staf akademik pranë Departamentit te Simologjisë. Fakti që punonjësi ka profil të tillë, nuk përbën arsye legjitime që ky punonjës të ketë kompetencat e administruesit të të dhënave në IGJEUM. Kjo zgjidhje e gjetur në kushte të mungesës të një strukture IT, në opinion të grupit të auditimit është e papërshtatshme, madje në mungesë të një autorizimi nga ana e titullarit, përbën risk të lartë për sa i përket sigurisë së informacionit.
Mungesa e një strukture të posaçme të Teknologjisë së Informacionit, ndikon gjithashtu në mos identifikimin e nevojave të reja ose të përditësuara në këtë fushë, dhe më pas në ofrimin e zgjidhjeve të duhura IT për përdoruesit e institucionit.
Me gjithë kërkesat[1] e shumta të bëra nga departamentet e IGJEUM mbi nevojën e plotësimit të personelit, jo vetëm me profil IT por edhe të tjerë, institucioni është ende në kushtet e ekzistencës së lartë të vendeve vakante.
Për sa i përket punësimeve të stafit, vetë IGJEUM nuk ka kompetencë të tillë, pasi limitohet vetëm në kërkesën që i bën Universitetit Politeknik të Tiranës. Kjo e drejtë ushtrohet pikërisht nga UPT duke ndjekur politikat e përcaktuara në Ligjin Nr. 85/2015 "Për Arsimin e Lartë dhe Kërkimin Shkencor në Republikën e Shqipërisë", si dhe aktet e tjera ligjore e nënligjore në fuqi në Republikën e Shqipërisë.
Aktiviteti i IGJEUM bazohet në monitorimin e aktivitetit sizmik, meteorologjik dhe hidrologjik 24 orë pa ndërprerje, 7 ditë të javës, dhe mungesa e plotë e stafit rrit riskun e cënimit të monitorimit të plotë.

Investimet

Instituti i Gjeoshkencës, Energjisë, Ujit dhe Mjedisit nuk ka një regjistër parashikimesh dhe realizimesh për sa i përket shpenzimeve dhe investimeve, pasi këtë detyrë e ushtron Rektorati i Universitetit Politeknik të Tiranës, IGJEUM ka të drejtë të bëjë vetëm kërkesën për nevojat institucionale që ka, e më pas pret miratimin ose jo të tyre nga organet vendimmarrëse të UPT. Procedurat e prokurimit si dhe marrja në dorëzim e aktiveve, duke përfshirë këtu edhe pajisjet e sistemeve në fushën e teknologjisë së informacionit, bëhet nga

[1] Kërkesat janë bërë me email-e, verbalisht si edhe me kërkesë zyrtare drejt UPT.

grupet e punës të ngritura nga nënpunësi autorizues në Universitetin Politeknik Tiranë.
Kërkesat për shpenzime e investime evidentohen në njësitë bazë, pra Departamentet përkatëse. Këto kërkesa përcillen tek Drejtori i IGJEUM nëpërmjet Përgjegjësit të Departamentit. Pas miratimit nga ana e Drejtorit, i dërgohen Universitetit Politeknik të Tiranës, me qëllim përgatitjen e buxhetit për vitin ushtrimor.
Fondi për investime i miratuar nga UPT për katër vitet e fundit paraqitet në mënyrë të përmbledhur si më poshtë:

Në Lekë

Viti	2016	2017	2018	2019
Investimet	3,100,000	2,000,000	-	10,937,000
Investime IT	2,200,000	-	-	10,937,000

Burimi: IGJEUM

Nga sa shihet nga tabela e përmbledhur, konstatohet se investimet në IGJEUM dhe në fushën e IT në veçanti janë në një nivel të ulët, edhe pse monitorimi i aktivitetit sizmik dhe meteorologjik ka rëndësi kombëtare. Madje edhe vlera prej 10,937,000 lekë e akorduar në vitin 2019, është një paradhënie e UPT e cila do të rimbursohet nëpërmjet një financimi të huaj për rrjetin hidrologjik. Investimi konsiston në blerjen e 2 stacioneve të reja të monitorimit të nivelit të detit (njëri prej tyre mat edhe valën) dhe nuk janë pajisje të mirëfillta IT, por transmetimi i të dhënave nga këto stacione bëhet në kohë reale.
Investimet në lidhje me pajisjet e Teknologjisë së Informacionit për përmbushjen e nevojave institucionale janë kryer kryesisht nëpërmjet projekteve ndërkombëtare të NATO për pajisjet sizmologjike dhe Bankës Botërore për sistemin e monitorimit Hidro- meteorologjik. Ndërsa sistemi i monitorimit të Lumin Drin dhe Buna, është ngritur mbi bazën e një bashkëpunimi rajonal për ngritjen e një sistemi të përbashkët paralajmërimi, nëpërmjet projektit "Përshtatja ndaj ndryshimeve klimatike në Ballkanin Perëndimor" të financuar nga Qeveria Gjermane nëpërmjet GIZ.
Grupi i auditimit vlerëson se mungesa e një strukture IT në IGJEUM, rrit riskun e mos evidentimit të nevojave të përshtatshme në drejtim të Teknologjisë së Informacionit, duke ndikuar në funksionimin e duhur dhe koherent të sistemeve të përdorura nga Instituti i Gjeoshkencës, Energjisë, Ujit dhe Mjedisit.
Pasojat e mungesës së investimeve të domosdoshme në drejtim të teknologjisë së informacionit dhe më gjerë, për kryerjen normale të monitorimit të aktivitetit sizmik janë vënë re gjatë ngjarjeve të fundit në vend. Dhe më konkretisht:
Referuar të dhënave të regjistruara nga Departamenti i Sizmologjisë në IGJEUM në lidhje me tërmetin e datës 26.11.2019, i cili ka patur impakt në jetë njerëzish dhe dëme të shumta materiale, konstatohet se mungojnë të dhëna të plota nga stacioni i Durrësit, i cili është stacioni më i afërt me vatrën e tërmetit. Ky stacion ka regjistruar vetëm 15 sekondat e para të tërmetit, si pasojë e ndërprerjes së energjisë elektrike. Nisur nga fakti që gjatë një tërmeti të fortë, ekziston një probabilitet i lartë për ndërprerjen e energjisë elektrike, është e domosdoshme pajisja e stacioneve sizmologjike me bateri (UPS) të cilat mundësojnë matjen e lëkundjeve edhe nëse ndërpritet energjia elektrike.
Theksojmë se funksionimi i rregullt i tre rrjeteve sizmike në vendin tonë është i rëndësishme për parashikimin dhe monitorimin e katastrofave natyrore në kohë reale, duke marrë masa në drejtim të mbrojtjes së jetës së njerëzve dhe reduktimin e dëmeve materiale. Cënimi i monitorimit të aktivitetit sizmik, mund të sjellë pasoja në jetë njerëzish dhe dëme materiale më të larta nga vlera e investimit për mirëmbajtjen e tyre.
Nga verifikimi i dokumentacionit shkresor të vënë në dispozicion nga departamentet e IGJEUM mbi situatën e stacioneve të monitorimit, si dhe kërkesave të bëra nga IGJEUM në

UPT mbi nevojat institucionale, konstatohet se përcjellja e problematikave në UPT është e reduktuar, në krahasim me atë çka paraqesin departamentet, duke kërkuar vetëm ato investime të cilat kanë prioritet maksimal për vazhdimësinë e monitorimit sizmik dhe klimaterik. Por përsëri, miratimet e UPT për investime janë mjaft të ulta.

Grupi i auditimit vlerëson se misioni i Universitetit Politeknik Tiranë, i cili përcaktohet në nenin 3 të Statutit të këtij institucioni miratuar me Vendimin Nr. 15, datë 31.10.2018 të Senatit Akademik, dhe me Urdhrin e Ministrit të Arsimit Sportit dhe Rinisë Nr. 10, datë 11.01.2019, saktësisht:

"*Misioni i UPT është:*

a) të krijojë, të transmetojë, të zhvillojë e të mbrojë dijet me anën e mësimdhënies, kërkimit shkencor dhe shërbimeve, si edhe të formojë specialistë të lartë dhe të përgatitë shkencëtarë të rinj;

b) të ofrojë mundësi për të përfituar nga arsimi i lartë gjatë gjithë jetës në fushat e tij të ekspertizës;

c) të ndihmojë zhvillimin ekonomik në nivel kombëtar dhe rajonal;

ç) të kontribuojë në rritjen e standardeve të demokracisë e të qytetërimit të shoqërisë dhe në përgatitjen e të rinjve për një shoqëri të tillë";

ndikon në fokusin e munguar mbi rëndësinë kombëtare të mirëmbajtjes së rrjeteve të IGJEUM-it, duke bërë që për vitin 2019 i cili është objekt auditimi, investimet të jenë 0 lekë, nga 116,208,000 lekë të kërkuara nga IGJEUM. Ndërsa gjatë 4 viteve të fundit, investimet në fushën e teknologjisë së informacionit, kanë qenë vetëm 2,200,000 lekë.

Strategjia IT

Nga auditimi u konstatua se IGJEUM nuk ka një strategji për Teknologjinë e Informacionit, ku të evidentohen nevojat aktuale dhe merren në konsideratë ato të ardhshme të institucionit, kapacitetin aktual të TI për të ofruar shërbime dhe kërkesat e burimeve, duke marrë në konsideratë ekzistencën e infrastrukturës së IT, investimeve, modelin e ofrimit, burimet duke përfshirë stafin, si dhe paraqitjen e strategjisë që integron këto elementë në një qasje të përbashkët për të mbështetur objektivat e institucionit. Strategjia e IT duhet të përfaqësojë lidhjen e përbashkët midis objektivave të strategjisë së IT dhe atyre të strategjisë së institucionit. Strategjia e IT duhet të jetë pjesë e strategjisë institucionale, por nga auditimi u konstatua se IGJEUM nuk e ka një të tillë, në kundërshtim me nenin 13, pika 5, të Statutit të UPT.

Institucioni nuk ka një politikë të shkruar për sigurinë e informacionit, ku të vendosen kërkesat për mbrojtjen e aseteve të informacionit. Politikat duhet të jenë të disponueshme ndaj të gjithë punonjësve përgjegjës për sigurinë e informacionit, përfshirë përdoruesit e sistemeve të cilët kanë rol në mbrojtjen e informacionit. Gjithashtu, si pasojë edhe e mungesës së një strukture IT, institucioni nuk ka hartuar një rregullore për përdorimin e Teknologjisë së Informacionit. Madje IGJEUM nuk ka ende një rregullore të brendshme, ku të jetë përcaktuar funksionimi i këtij institucioni si dhe detyrat konkrete të pozicioneve të punës, veprim në kundërshtim me nenin 5/2 pika 3 dhe nenin 13, pika 5, të Statutit të UPT.

Nga auditimi u konstatua se IGJEUM nuk ka politika për dokumentimin dhe ruajtjen e dokumenteve në lidhje me teknologjinë e informacionit. Dokumentimi i sistemeve të informacionit, aplikacioneve, detyrat e punës, sistemet e raportimit dhe periodiciteti është një pikë referimi e rëndësishme për lidhjen e operacioneve të IT me objektivat institucionale. Politikat e sakta të ruajtjes së dokumenteve mundësojnë kapjen dhe menaxhimin e ndryshimeve të përsëritura të arkitekturës së informacionit në njësi.

Nga auditimi u konstatua se IGJEUM nuk ka Marrëveshje në Nivel Shërbimi (MNSH/SLA), për mirëmbajtjen e sistemeve, veprim në kundërshtim me pikën 2 të VKM Nr. 710, datë 21.8.2013 "Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit", i ndryshuar, pika 2, ku citohet: "*Çdo institucion, i cili ka ose do të zhvillojë një sistem në fushën e teknologjisë së informacionit, që ofron shërbime për qytetarët, për biznesin dhe për ndërveprim e shkëmbim informacioni për administratën publike nëpërmjet sistemeve elektronike, duhet të parashikojë dhe të hartojë marrëveshje kontraktuale mbi nivelin e shërbimit (Service Level Agreement - SLA)*". Mirëmbajtja e tyre kryhet nga vetë personeli në raste kur ndodhin probleme të ndryshme, por në asnjë rast nuk kemi një monitorim të dokumentuar.
Instituti i Gjeoshkencës, Energjisë, Ujit dhe Mjedisit nuk ka një regjistër risku për Teknologjinë e Informacionit ku të jenë evidentuar ato situata të mundshme apo ngjarje të cilat mund të kenë impakt negativ në mbarëvajtjen normale të punës së këtij institucioni. Në këtë mënyrë nuk kemi një plan masash për secilin nga risqet e evidentuara. Këto risqe institucioni i zgjidh rast pas rasti, sa herë që implementohet diçka e re merren parasysh dhe risqet e mundshme si edhe siguria e informacionit.
Nga auditimi u konstatua se IGJEUM nuk ka politika të aprovuara për menaxhimin e ndryshimeve, të cilat të përmbajnë kontrollet e përshtatshme përgjatë ciklit të ndryshimit. Gjithashtu nuk ka gjurmë të kontrolleve për ndryshimet emergjente për sa i përket përcaktimit, autorizimit, testimit dhe dokumentimit të tyre.
Madje, edhe për sa i përket backup-eve të të dhënave apo edhe faqes web, përsëri kryhen nga stafi i IGJEUM, edhe pse pozicioni i tyre nuk përputhet me këtë veprimtari. Në lidhje me këtë, u konstatua se nuk ka asnjë urdhër apo autorizim me shkrim nga titullari për kryerjen e punëve si: administrim i të dhënave të dy serverave, administrim i faqes web, kontroll të log-eve të web, etj. Kjo situatë, në opinion të grupit të auditimit, përbën një risk të lartë për sa i përket sigurisë së të dhënave të institucionit, pasi në rast të një dëmtimi, humbjeje apo kompromentimi të këtyre të dhënave, nuk ka asnjë person i cili mban përgjegjësi për to. Administrimi i këtyre atributeve individualisht dhe pa autorizim, nuk jep siguri të arsyeshme për kryerjen e tyre konform dispozitave ligjore si dhe praktikave më të mira.
Website i IGJEUM është ndërtuar nga stafi i Institutit i cili bëhet update dhe mirëmbahet në baza ditore. Tërmetet publikohen në realtime si edhe buletinet përmbledhëse çdo muaj.
Të dhënat e rrjeteve Hidro dhe Meterologjike përdoren vetëm në funksion të parashikimit, monitorimit dhe paralajmërimit në kohë reale të rreziqeve natyrore si moti ekstrem, përmbytjet apo rrëshqitjet.
IGJEUM publikon të dhëna të cilat janë deduksion i informacionit të ardhur, pasi të dhënat e ardhura fillimisht duhet ti nënshtrohen kontrollit, verifikimit, krahasimit, homogjenizimit dhe pasi të përpunohen më tej në përputhje me metodikat e OBM nxirren treguesit dhe produktet që janë të vlefshme dhe të dobishme për tu përdorur nga përdoruesit (klientët e ndryshëm, përfshi dhe median).
Çdo ditë jepen parashikime 24 orëshe online për publikun e gjerë si edhe çdo muaj publikohen buletine në formatin PDF.

1. Titulli i gjetjes: Mungesa e strukturës IT.
Situata: Nga auditimi u konstatua se Instituti i Gjeoshkencave, Energjisë, Ujit dhe Mjedisit nuk ka në përbërje strukturë të teknologjisë së informacionit, madje asnjë pozicion specialisti IT, duke krijuar risk të lartë mbi identifikimin, trajtimin dhe zgjidhjen e problematikave të

ndryshme të Teknologjisë së Informacionit në institucion. Si institucion nën varësinë e Universitetit Politeknik të Tiranës, IGJEUM duhet të ketë suportin e specialistëve IT të Universitetit Politeknik të Tiranës. UPT ka në strukturën e tij 7 Fakultete dhe IGJEUM, dhe për mbulimin e problematikave në fushën e IT, ka vetëm 2 specialistë të fushës të atashuar në zyrat e UPT. Në të tilla kushte, problemet që hasen në IGJEUM në fushën e Teknologjisë së Informacionit gjejnë zgjidhje pothuajse gjithnjë nëpërmjet vetë stafit të cilët kanë njohuri në këtë fushë.

Kriteri: Realizimi në kohë dhe cilësi i shërbimeve në fushën e Teknologjisë së Informacionit.

Ndikimi/efekti: Risk i lartë për mos identifikimin, trajtimin dhe zgjidhjen e problematikave të ndryshme të Teknologjisë së Informacionit

Shkaku: Mungesa e strukturës IT.

Rëndësia: E lartë

Rekomandimi: IGJEUM në bashkëpunim me UPT, të marrin masa për krijimin e një strukture të Teknologjisë së Informacionit në IGJEUM, në nivel sektori apo drejtorie, me qëllim përmbushjen e nevojave institucionale mbi identifikimin, trajtimin dhe zgjidhjen e problematikave të ndryshme të Teknologjisë së Informacionit.

2. Titulli i gjetjes: Akses dhe administrim i të dhënave pa autorizim.

Situata: Nga auditimi u konstatua se IGJEUM ka vetëm 1 (një) punonjës me profil shkenca kompjuterike, i cili në strukturë është staf akademik pranë Departamentit të Sizmologjisë. Duke qenë i vetmi punonjës me një profil të tillë, i janë dhënë *verbalisht* kompetenca si: administrim të sistemit sizmologjik, administrim të të dhënave të dy serverave, administrim të faqes web, kontroll të log-eve të web; etj. Grupi i auditimit vlerëson se fakti që një punonjës ka profil të tillë, nuk përbën arsye legjitime që ai të ketë këto kompetenca. Kjo zgjidhje e gjetur në kushte të mungesës të një strukture IT, është e papërshtatshme, madje në mungesë të një autorizimi me shkrim nga ana e titullarit, përbën risk të lartë për sa i përket sigurisë së informacionit dhe mbrojtjes së të dhënave të institucionit.

Kriteri: Dokumentimi i veprimeve autorizuese dhe në përputhje me strukturën.

Ndikimi/efekti: Risk i lartë në sigurinë e të dhënave të institucionit.

Shkaku: Mungesa e strukturës IT dhe mungesa e autorizimit me shkrim.

Rëndësia: E lartë

Rekomandimi: Strukturat drejtuese të IGJEUM në vijimësi të dokumentojnë çdo autorizim mbi përdorimin e sistemeve të Teknologjisë së Informacionit, si dhe të caktojnë detyrat administruese të të dhënave në përputhje me detyrat funksionale të punonjësve.

3. Titulli i gjetjes: Mungesë të burimeve njerëzore.

Situata: Nga auditimi u konstatua se IGJEUM ka një organikë të miratuar prej 71 punonjësish, ndërkohë janë të punësuar vetëm 48 punonjës, ose 67.6% e organikës së miratuar. Mungesat e burimeve njerëzore rrit riskun e cënimit të monitorimit të plotë të aktivitetit sizmik, meteorologjik dhe hidrologjik në Institutin e Gjeoshkencave, Energjisë, Ujit dhe Mjedisit, pasi ky monitorim kryhet 24 orë pa ndërprerje.

Kriteri: Përmbushja e detyrave institucionale.

Ndikimi/efekti: Cënim i monitorimit të plotë të aktivitetit sizmik, meteorologjik dhe hidrik.

Shkaku: Nuk janë marrë masat e nevojshme për plotësimin e vendeve vakante.

Rëndësia: E lartë

Rekomandimi: IGJEUM në bashkëpunim me UPT të marrin masat e nevojshme për plotësimin e vendeve vakante sipas strukturës së miratuar të IGJEUM, me qëllim përmbushjen e detyrimeve institucionale, në drejtim të monitorimit të aktivitetit sizmik, meteorologjik dhe hidrik pa ndërprerje.

4. Titulli i gjetjes: Mungesa e investimeve të domosdoshme.
Situata: Nga auditimi mbi investimet e kryera në fushën e Teknologjisë së Informacionit, u konstatua se ato janë në përpjesëtim të zhdrejtë me rëndësinë kombëtare që ka monitorimi i aktivitetit sizmik, meteorologjik dhe hidrologjik. Pasojat e mungesës së investimeve të domosdoshme në drejtim të teknologjisë së informacionit dhe më gjerë, janë vënë re gjatë ngjarjeve të fundit në vend. Konkretisht, referuar regjistrimeve të vëna në dispozicion nga Departamenti i Sizmologjisë në IGJEUM në lidhje me tërmetin e datës 26.11.2019, i cili ka patur impakt në jetë njerëzish dhe dëme të shumta materiale, konstatohet se mungojnë të dhëna të plota nga stacioni i Durrësit, i cili është stacioni më i afërt me vatrën e tërmetit. Ky stacion ka regjistruar vetëm 15 sekondat e para të tërmetit, si pasojë e ndërprerjes së energjisë elektrike. Nisur nga fakti që gjatë një tërmeti të fortë ekziston një probabilitet i lartë për ndërprerjen e energjisë elektrike, është e domosdoshme pajisja e stacioneve sizmologjike me bateri (UPS) të cilat mundësojnë regjistrimin e të dhënave edhe nëse ndërpritet energjia elektrike.
Theksojmë se funksionimi i rregullt i tre rrjeteve sizmike në vendin tonë është i rëndësishme për parashikimin dhe monitorimin e katastrofave natyrore në kohë reale, duke marrë masa në drejtim të mbrojtjes së jetës së njerëzve dhe reduktimin e dëmeve materiale.
Kriteri: Misioni i IGJEUM për përmbushjen e detyrimeve institucionale.
Ndikimi/efekti: Cënim i monitorimit të aktivitetit sizmik, meteorologjik dhe hidrik.
Shkaku: Nuk janë marrë masat paraprake për kryerjen e investimeve të domosdoshme.
Rëndësia: E lartë
Rekomandimi: IGJEUM në bashkëpunim me UPT, duke marrë shkas edhe nga problematikat e shfaqura gjatë tërmetit të datës 26.11.2019, të marrin masat e nevojshme për kryerjen e investimeve të domosdoshme në IGJEUM me qëllim krijimin e kushteve të përshtatshme për realizimin pa ndërprerje të procesit të monitorimit të aktivitetit sizmik, meteorologjik dhe hidrik.

5. Titulli i gjetjes: IGJEUM nuk ka një Plan Strategjik të IT.
Situata: Nga auditimi u konstatua se IGJEUM nuk ka një Plan Strategjik për Teknologjinë e Informacionit, ku të adresohen qartë objektivat e institucionit, kapaciteti aktual i TI për të ofruar shërbime dhe kërkesat e burimeve, duke marrë në konsideratë ekzistencën e infrastrukturës së IT, investimeve, modelin e ofrimit, si dhe paraqitjen e strategjisë që integron këto elementë në një qasje të përbashkët për të mbështetur objektivat e institucionit.
Kriteri: Statuti i UPT.
Ndikimi/efekti: Teknologjia e Informacionit zhvillohet pa një Plan Strategjik.
Shkaku: Mos zbatimi i praktikave më të mira në zhvillimin dhe menaxhimin institucional.
Rëndësia: E lartë
Rekomandimi: IGJEUM dhe UPT, duke marrë në konsideratë kohën, burimet e nevojshme si dhe rëndësinë e të dhënave që institucioni zotëron dhe përpunon, të marrin masa për hartimin e një Plani Strategjik, ku të adresohen qartë objektivat e institucionit në drejtim të Teknologjisë së Informacionit.

6. Titulli i gjetjes: Mungesa e politikave mbi sigurinë e informacionit.
Situata: Nga auditimi u konstatua se IGJEUM nuk ka një procedura të miratuara për sigurinë e informacionit, apo plane për sigurinë e sistemeve IT, ku të vendosen kërkesat për mbrojtjen e aseteve të informacionit. Gjithashtu IGJEUM nuk ka hartuar një rregullore për përdorimin e Teknologjisë së Informacionit, duke ndikuar në akses të pakufizuar ndaj sistemeve që zotëron.
Kriteri: Siguria e informacionit në IGJEUM.
Ndikimi/efekti: Risk i lartë për mbrojtjen e informacionit.
Shkaku: Nuk janë marrë masat e nevojshme për hartimin e këtyre akteve.
Rëndësia: E mesme
Rekomandimi: IGJEUM në bashkëpunim me UPT, të marrin masat e nevojshme për hartimin e rregullave dhe procedurave mbi përdorimin e teknologjisë së informacionit në IGJEUM, duke dhënë siguri të arsyeshme mbi sigurinë e të dhënave të institucionit.

7. Titulli i gjetjes: Sistemet e IGJEUM janë pa MNSH.
Situata: Nga auditimi u konstatua se IGJEUM nuk ka Marrëveshje në Nivel Shërbimi (MNSH/SLA), për mirëmbajtjen e sistemeve, veprim në kundërshtim me pikën 2 të VKM Nr. 710, datë 21.8.2013 "*Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit*", i ndryshuar, pika 2, ku citohet: "*Çdo institucion, i cili ka ose do të zhvillojë një sistem në fushën e teknologjisë së informacionit, që ofron shërbime për qytetarët, për biznesin dhe për ndërveprim e shkëmbim informacioni për administratën publike nëpërmjet sistemeve elektronike, duhet të parashikojë dhe të hartojë marrëveshje kontraktuale mbi nivelin e shërbimit (Service Level Agreement - SLA)*". Mirëmbajtja e sistemeve kryhet nga vetë personeli në rastet kur ka probleme, por në asnjë rast nuk kemi një monitorim të dokumentuar.
Kriteri: VKM Nr. 710, datë 21.8.2013, i ndryshuar.
Ndikimi/efekti: Risk i lartë për mosfunksionimin e sistemeve IT.
Shkaku: Nuk janë marrë masat e nevojshme për lidhjen e një MNSH-je
Rëndësia: E mesme
Rekomandimi: IGJEUM në bashkëpunim me UPT të marrin masat e nevojshme për lidhjen e një marrëveshjeje në nivel shërbimi me qëllim garantimin e vazhdimësisë pa probleme të sistemeve që zotëron.

8. Titulli i gjetjes: Nuk është hartuar regjistri i riskut mbi Teknologjinë e Informacionit.
Situata: Nga auditimi u konstatua se Instituti i Gjeoshkencës, Energjisë, Ujit dhe Mjedisit nuk ka një regjistër risku për Teknologjinë e Informacionit ku të jenë evidentuar ato situata të mundshme apo ngjarje të cilat mund të kenë efekt negativ në mbarëvajtjen e punës së këtij institucioni, duke mos patur kështu një plan masash për zgjidhjen e problematikave të ndryshme që mund të ndodhin.
Kriteri: Ligji nr. 10296, datë 08.07.2010, "Për menaxhimin financiar dhe kontrollin", i ndryshuar.
Ndikimi/efekti: Mungesa e një plani masash për ngjarje të cilat nëse ndodhin do të kenë ndikim në arritjen e objektivave**.**
Shkaku: Nuk janë marrë masat për hartimin e regjistrit të riskut mbi Teknologjinë e Informacionit.
Rëndësia: E mesme.

Rekomandimi: IGJEUM të marrë masat për hartimin e një regjistri risku për teknologjinë e informacionit ku të jenë evidentuar ato ngjarje të mundshme të cilat mund të kenë efekt negativ në mbarëvajtjen e punës institucionale, me qëllim krijimin e një plani pune në rastet e shfaqjes së problematikave të ndryshme në fushën e teknologjisë së informacionit.

2. Operacionet IT

a. Procedurat e menaxhimit të problemeve dhe incidenteve të institucionit.
b. Menaxhimi i ndryshimit.

Nga auditimi u konstatua se:
-Menaxhimi i Vazhdimësisë së Shërbimit IT
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. Gjithashtu, po në këtë plan duhet të përshkruhet sesi një organizatë do të vazhdojë të funksionojë pas një situate që mund të ndodhi e cila mund të jetë si rezultat i një katastrofe.
Nga dokumentacioni i paraqitur, procesi i backup-it të të dhënave në IGJEUM kryhet manualisht në mënyre periodike (me anë të usb), ndërsa backup i webit është automatik në bazë javore. Këto backup-e të të dhënave apo faqes web kryhen nga stafi i IGJEUM për të cilët nuk ka asnjë autorizim me shkrim apo urdhër përkatës. Gjithashtu backup-i automatik si edhe manual ruhet në dy vende, por këto veprime nuk janë të dokumentuara si dhe nuk ka asnjë person përgjegjës të autorizuar nga titullari.
Për të ruajtur sigurinë e të dhënave, IGJEUM nuk ka ndërtuar procedura automatike në server me anë të të cilave të ruhen kopje backup të të dhënave të sistemeve të teknologjisë së informacionit.
Nga dokumentacioni i vendosur në dispozicion grupit të auditimit, u konstatua se IGJEUM nuk disponon plane dhe procedura të qëndrueshme për vazhdimësinë e institucionit, në kundërshtim me pikën 1 të VKM Nr. 710, datë 21.8.2013 *"Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit"* i ndryshuar, ku citohet: "*Çdo institucion, i cili ka ose do të zhvillojë një sistem në fushën e teknologjisë së informacionit, që ofron shërbime për qytetarët, për biznesin dhe për ndërveprim e*
shkëmbim informacioni 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".
Gjithashtu IGJEUM nuk disponon një plan të dokumentimit të rimëkëmbjes nga katastrofa e cila të jetë e gatshme për backup dhe rimëkëmbje. I vetmi plan që disponon IGJEUM është rimëkëmbja e website-it në rast problemesh duke rikthyer backup të vjetër. Mungesa e planit të vazhdueshmërisë dhe të rimëkëmbjes nga katastrofa përbën risk për humbjen e të dhënave, humbjen e kohës së vlefshme dhe kosto të tjera për shkak të rimëkëmbjes në rast katastrofe. IGJEUM nuk ka një server dytësor jashtë institucionit me qëllim që të ruhen të dhënat në rast të dëmtimit të serverit primar që IGJEUM disponon brënda institucionit.
Si përfundim IGJEUM:

- nuk disponon një plan vazhdimësie BPC (Business Continuity Plan) dhe plan rikuperimi DRC (Disaster Recovery Plan) për garantimin e vazhdimësisë së ofrimit të shërbimit.
- nuk ka caktuar personat përgjegjës për të siguruar vazhdimësinë e ofrimit të shërbimit, si dhe nuk janë identifikuar dhe ndarë sipas rëndësisë të dhënat kritike, sistemet, operacionet dhe burimet.
- kryen veprime manuale të pa dokumentuara dhe të paautorizuara në drejtim të ruajtjes së të dhënave
- nuk i ruan të dhënat (nuk ka një server dytësor) jashtë institucionit me qëllim rikuperimi në rast të dëmtimit të serverit primar

-Menaxhimi i Incidenteve dhe Problemeve

Rreziqet nga fatkeqësitë natyrore në Shqipëri mund të jenë: gjeologjike (tërmete, rrëshqitje dheu, shkëmbinjsh); hidrometeorologjike (përmbytje, shira të rrëmbyer, thatësira, stuhi bore, ortekë apo bllokim nga bora, stuhi ere); bio-fizike (zjarre në pyje, epidemi) ndërsa ato të shkaktuara nga njeriu konsistojnë në: shpërthim digash, përmbytje e fatkeqësi teknologjike.

Duke marre shkasë nga tërmetet që prekën Shqipërinë së fundmi u konstatua se shkaqet e ndërprerjes së regjistrimit në akselerometrin e qytetit të Durrësit në datën 26.11.2019, si dhe në disa stacione të tjera të Rrjetit Sizmologjik Shqiptar, lidhen me mungesën e pajisjeve të posaçme si UPS, Invertera, panele diellore, etj, që sigurojnë vazhdimësinë e punës në rastet e ndërprerjes së energjisë elektrike nga rrjeti.

Departamenti i Klimës dhe Mjedisit (DKM) ka një Sistem Kombëtar të Monitorimit Meteorologjik i cili përbëhet nga një sërë stacionesh manuale, ku pjesa e vrojtimeve manuale vjen në Institut nëpërmjet ditarëve mujore. Ekzistenca e stacioneve manuale, pra jo automatike përbën risk për humbjen e të dhënave, në rast se vëzhguesit e këtyre stacioneve ndërpresin punën e tyre duke mos dërguar ditarin mujor me vëzhgimet përkatëse që pajisjet kanë matur, gjë që sjell humbje në kohë dhe në burime përkatëse dhe mos realizimin e misionit të këtij departamenti.

- Nga dokumentacioni i vënë në dispozicion u konstatua se në IGJEUM, nuk janë hartuar rregulla mbi menaxhimin e incidenteve dhe problemeve, si dhe instituti nuk ka të dokumentuar një plan masash për trajtimin e problemeve dhe incidenteve që mund të ndodhin. Në mungesë të këtyre procedurave të miratuara, problemet dhe incidentet për periudhën nën auditim nga departamenti i sizmologjisë menaxhohen mbi bazë ngjarjesh dhe dërgimin e shkresave në formë informimi mbi gjendjen e rrjeteve sizmologjike, drejtuar drejtorit të IGJEUM. Gjithashtu problematikat e ndryshme që mund të shfaqin stacionet ose rrjetet meteorologjike, menaxhohen mbi baza ngjarjesh, dmth jepet suport, mbështetje teknike dhe logjike për operacionet TI nëpërmjet shkëmbimeve verbale me vëzhguesit përkatës të stacioneve.

Në këtë mënyrë, IGJEUM nuk ka politika të ruajtjes së dokumenteve në rast incidenti duke sjellë mos dokumentimin e këtyre rreziqeve të ndodhura, si dhe nuk disponon raporte të administrimit të incidenteve dhe problemeve, me qëllim gjetjen e zgjidhjeve për ti trajtuar ato dhe për të parandaluar ndodhjen e incidenteve të ngjashme në të ardhmen, në mënyrë që shërbimet e institutit të mos kompromentohen. Mungesa e masave dhe mungesa e rregullores për trajtimin e incidenteve dhe problemeve sjell:

-mos përcaktim të detyrave dhe përgjegjësive në rast të ndodhjes së një gabimi/ incidenti;
-mos dokumentim dhe mos lënie gjurmësh për trajtimin e gabimeve/incidenteve;
-akses të paautorizuar të përdoruesve edhe ndërhyrjet e paautorizuara;

-mungesë të koordinimit të menaxhimit të informacionit;
-mos efektivitet në sigurimin e informacionit teknik dhe shkencor në lidhje me kushtet dhe situatën hidrologjike, sizmike, meteorologjike dhe të mjedisit; etj
Si përfundim IGJEUM:

- nuk ka hartuar rregulla mbi menaxhimin e incidenteve dhe problemeve;
- nuk disponon raporte të administrimit të incidenteve dhe problemeve;
- nuk ka të dokumentuar një plan masash për trajtimin e gabimeve dhe incidenteve që mund të ndodhin.

-Menaxhimi i Sigurisë së Informacionit
IGJEUM në kuadër të punës së përditshme përdor faqen web për informimin e institucioneve të interesuar si edhe publikun e gjerë.
Menaxhimi i sigurisë së informacionit lidhet me menaxhimin e risqeve të lidhura me sigurinë, marrjen e masave të duhura dhe garancinë se informacioni që ky institut disponon, është i disponueshëm, i përdorshëm, i plotë dhe i pa kompromentueshëm, si dhe me sigurimin se vetëm përdoruesit e autorizuar kanë akses në sistemet e institucionit. Konstatohet se në IGJEUM nuk dokumentohet vlerësimi mbi risqe të mundshme lidhur me sigurinë e informacionit. Si një institucion që siguron informacion teknik dhe shkencor në lidhje me kushtet dhe situatën hidrologjike, sizmike, meteorologjike dhe të mjedisit, duhet të vlerësojë mbrojtjen e sigurisë së informacionit.
Në faqen web të Universitetit Politeknik të Tiranës (https://www.upt.al) në seksionin Politikat e privatësisë gjendet e cituar një paragraf në lidhje me politikat e sigurisë së informacionit.
"Politika e sigurisë së informacionit:
Universiteti Politeknik i Tiranës, si kontrollues i të dhënave personale, përpunon informacionin me qëllim kryerjen e detyrave të tij ligjore dhe statutore. Kjo mund të përfshijë informacionin sekret për studentët dhe stafin akademik, ndihmës akademik dhe administrativ. Universiteti i Politeknik i Tiranës përdor një qasje të bazuar në risk, gjatë vlerësimit dhe të kuptuarit të rreziqeve, si dhe përdor të gjitha mjetet fizike të personelit, teknike dhe procedurale për të arritur masat e duhura të sigurisë. Universiteti Politeknik i Tiranës, si kontrollues i të dhënave personale, merr parasysh zhvillimet në teknologji dhe kostot e zbatimit për të arritur një nivel sigurie të përshtatshëm për natyrën e informacionit dhe të dëmit që mund të rezultojë nga një shkelje e sigurisë. Stafi i Universitetit Politeknik të Tiranës i nënshtrohet detyrimit për të ruajtur konfidencialitetin e informacionit, i cili i jepet këtij të fundit për të ushtruar funksionet e tij në bazë ligjit, dhe mund t'ua përhapë atë vetëm autoriteteve të ligjshme. Universiteti Politeknik i Tiranës ofron udhëzime dhe trajnime stafit të tij për t'u mundësuar atyre të kuptojnë dhe të zbatojnë përgjegjësitë e tyre në respektimin e sigurisë. Universiteti Politeknik i Tiranës vlerëson integritetin e tyre përpara se ata të punësohen, si dhe monitoron pajtueshmërinë e tyre me detyrimet që kanë në lidhje me sigurinë".
Nga auditimi u konstatua që IGJEUM nuk disponon rregullore për Politikat e Sigurisë së Informacionit. Pasja dhe zbatimi i Politikave të Sigurisë së Informacionit ul riskun operacional dhe rrit mundësinë e mbrojtjes në mënyrë të arsyeshme të gjithë asetet e informacioneve kritike kundrejt humbjeve, dëmtimit dhe abuzimit.
Gjithashtu, nga dokumentacioni i vënë në dispozicion të grupit të auditimit, konstatohet se stafi i IGJEUM nuk ka kryer asnjë ditë trajnimi mbi sigurinë e informacionit. Referuar praktikave më të mira kombëtare dhe ndërkombëtare, duhet gjithnjë të promovohet

ndërgjegjësimi i sigurisë dhe trajnime gjatë punësimit të punonjësve dhe deri në shkëputjen e marrëdhënies së punës.
Gjithashtu IGJEUM nuk ka analizuar, identifikuar dhe planifikuar nevojat për trajnim të punonjësve për Sigurinë e Informacionit (përfshirë të kontraktuarit ose përdoruesit e të dhënave sensitive). Për periudhën nën auditim, nuk janë përfshirë trajnimet kritike të sigurisë së IT dhe kërkesat e ndërgjegjshmërisë, në përmbushje të nevojave të përgjithshme dhe specifike që ndihmojnë mbarëvajtjen dhe funksionimin e veprimeve dhe procedurave të këtij Instituti. Stafi duhet të jetë i trajnuar dhe i ndërgjegjshëm për përgjegjësitë e tyre referuar parandalimit, zvogëlimit, dhe reagimit ndaj situatave emergjente.
Si përfundim IGJEUM:

- nuk dokumenton identifikimin e risqeve dhe vlerësimin e tyre lidhur me sigurinë e informacionit;
- nuk disponon rregullore për Politikat e Sigurisë së Informacionit;
- nuk ka kryer asnjë ditë trajnimi mbi sigurinë e informacionit.

-Menaxhimi i Ndryshimit
Referuar procesit të menaxhimit të ndryshimit, i cili duhet të sigurojë që ndryshimet janë regjistruar, vlerësuar, autorizuar, prioritarizuar, planifikuar, testuar, implementuar, dokumentuar dhe rishikuar në përputhje me procedurat e dokumentuara dhe të aprovuara të menaxhimit të ndryshimit, grupit të auditimin nuk i është vënë në dispozicion asnjë dokumentacion. Fsite që IGJEUM disponon është ndërtuar nga stafi i Institutit i cili bëhet update dhe mirëmbahet në baza ditore, ku backup i të dhënave dhe faqes web përsëri kryhet nga stafi i IGJEUM pozicioni i të cilëve nuk përputhet me veprimtarinë përkatëse. Nisur nga kjo situatë ku përgjegjësitë dhe detyrat nuk janë alokuara në përputhje me praktikat më të mira, përbën risk të lartë në lidhje me sigurinë e të dhënave që institucioni disponon duke mos u mbajtur përgjegjësitë në raste të humbjeve apo dëmtimit të të dhënave.
Çështjet që përfshijnë nevojën për dixhitalizimin dhe rehabilitimin e mëtejshëm të rrjetit të stacioneve hidrometeorologjike dhe sizmike, mirëmbajtjen e rregullt të pajisjeve, lidhjet e sigurta e të vazhdueshme të internetit, nevojën për staf të ri dhe të kualifikuar, si hidrologë, meteorologë, sizmolog dhe sasi të konsiderueshme të të dhënave historike, të cilat ende nuk janë dixhitalizuar, duhet të trajtohen me qëllim përmirësimin për informimin e shpejtë të organizmave shtetërore në raste të fatkeqësive natyrore.
Të dhënat hidrologjike dhe meteorologjike të Rrjetit të observimit meteorologjik ende nuk shkëmbehen me sistemin GTS (Global Telecommunication System) të Organizatës Botërore të Meteorologjisë. Pjesa e stacioneve automatike është ende në proces kalibrimi e riparimi, për të qenë e vlefshme për përdorim dhe që të përmbushë standardet e WMO (World Meteorological Organization). Gjithashtu rrjeti hidrologjik e meteorologjik, referuar edhe verifikimit të grupit të auditimit në stacionet meteorologjike, ka nevojë të përmirësohet me teknologji bashkëkohore, pasi mungesa e modeleve dixhitale të parashikimit të kohës paraqet një pengesë për "paralajmërimin e hershëm". Në opinion të grupit të auditimit, hartimi i një plani afatgjatë për implementimin e teknologjive dhe metodologjive të reja për mbledhjen dhe përpunimin në kohë reale të informacionit, si dhe administrimin e shpërndarjes sa më të shpejtë të të dhënave të përftuara nga pajisjet dixhitale që departamentet përkatëse të IGJEUM-it disponojnë, do të ndikojë në një ofrim më të mirë të shërbimit.
Si përfundim IGJEUM:

- nuk disponon procedura të standardizuara për kontrollin e të gjitha ndryshimeve në sistemet që disponon.

- nuk disponon rregullore/udhëzime që përcakton detyra periodike apo të vazhdueshme, hapat që duhet të ndiqen, si dhe personat përgjegjës lidhur me veprimet, që përdorues të ndryshëm kryejnë në sistem, sipas pozicionit të punës dhe të drejtave të çdo punonjësi/përdoruesi.
- nuk ka procedura për kryerjen e ndryshimeve emergjente.

9. Titulli i Gjetjes: IGJEUM nuk disponon Plan Vazhdimësie (BCP) dhe Plan Rikuperimi (DRC).
Situata: Nga auditimi u konstatua se IGJEUM nuk disponon një Plan Vazhdimësie (BCP) dhe Plan Rikuperimi (DRC) për garantimin e vazhdimësisë së ofrimit të shërbimit, duke krijuar risk për humbjen e të dhënave, veprim në kundërshtim me pikën 1 të VKM Nr. 710, datë 21.8.2013 "*Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit",* i ndryshuar.
Kriteri: VKM Nr. 710, datë 21.8.2013, i ndryshuar.
Ndikimi/Efekti: Risk për humbjen e të dhënave.
Shkaku: Nuk janë marrë masat e nevojshme
Rëndësia: E Lartë
Rekomandim: IGJEUM duke marrë në konsideratë kohën dhe burimet e nevojshme të marrë masa për ndërtimin dhe hartimin e Planit të Vazhdimësisë dhe Planit të Rikuperimit, duke përfshirë planet për backup dhe rimëkëmbjen nga katastrofat për sistemet, pajisjet kompjuterike dhe të dhënat, hartimin e planit të sigurisë së informacionit dhe implementimin e tij, duke përfshirë ndarjen e detyrave/përgjegjësive të sigurisë në TIK.

10. Titulli i Gjetjes: IGJEUM nuk ka kryer trajnime të punonjësve mbi sigurinë e informacionit.
Situata: IGJEUM nuk ka analizuar, identifikuar dhe planifikuar nevojat për trajnim të punonjësve për Sigurinë e Informacionit, në përmbushje të nevojave të përgjithshme dhe specifike që ndihmojnë në mbarëvajtjen dhe funksionimin e veprimeve dhe procedurave të këtij instituti.
Kriteri: Përditësimi i njohurive të stafit me ndryshimet e TIK.
Ndikimi/Efekti: Risk për kompromet im të dhënash në mënyrë të pavullnetshme.
Shkaku: Mungesë trajnimi mbi sigurinë e informacionit.
Rëndësia: E Mesme
Rekomandim: Strukturat Drejtuese në IGJEUM të hartojnë plane për zhvillimin e trajnimeve në lidhje me sigurinë e informacionit në përmbushje të nevojave të përgjithshme dhe specifike që ndihmojnë në mbarëvajtjen dhe funksionimin e veprimeve dhe procedurave të këtij instituti.

11. Titulli i Gjetjes: Mungesa e procedurave të standardizuara për menaxhimin e ndryshimeve.
Situata: IGJEUM nuk ka politika të aprovuara për menaxhimin e ndryshimeve, të cilat të përmbajnë kontrollet e përshtatshme përgjatë ciklit të ndryshimit, si dhe nuk disponon procedurë për inicimin, rishikimin dhe aprovimin e ndryshimeve, klasifikimin e tyre sipas rëndësisë, ndarjen e detyrave dhe përgjegjësive për kryerjen e ndryshimeve.
Kriteri: Praktikat më të mira në kontrollin e ndryshimeve.
Ndikimi/Efekti: Një ndryshim i paaprovuar ose aksidental mund të ketë risqe të ndryshme dhe pasoja financiare për institucionin.
Shkaku: Mos zbatimi i praktikave më të mira në kontrollin e ndryshimeve.

Rëndësia: E mesme
Rekomandim: Strukturat Drejtuese në IGJEUM në të ardhmen të marrin masat e nevojshme për hartimin e procedurave mbi menaxhimin e ndryshimeve në fushën e Teknologjisë së Informacionit dhe dokumentimin e gjithë procesit të ndryshimeve.

3. Auditimi i sigurisë së informacionit

a. Siguria e të dhënave dhe vazhdimësia në ofrimin e shërbimit.
b. Kontrollet e sigurisë së aplikacionit.
c. Të drejtat e përdoruesve dhe menaxhimi i tyre.

Nga auditimi u konstatua se:
Përdoruesit e të dhënave janë institucionet shtetërore të cilat lidhen drejtpërdrejtë me dukuritë natyrore si dhe drejtoria e emergjencave civile, publiku i gjerë si dhe çdo institucion privat i interesuar për këto të dhëna. IGJEUM informon çdo institucion të interesuar si edhe publikun e gjerë nëpërmjet webit si edhe duke u përgjigjur rast pas rasti kërkesave specifike që vijnë në sekretarinë e IGJEUM.
IGJEUM publikon të dhëna të cilat janë deduksion i informacionit të ardhur, pasi të dhënat e ardhura fillimisht duhet ti nënshtrohen kontrollit, verifikimit, krahasimit, homogjenizimit dhe pasi të përpunohen më tej në përputhje me metodikat e OBM nxirren treguesit dhe produktet që janë të vlefshme dhe të dobishme për tu përdorur nga përdoruesit (klientët e ndryshëm, përfshi dhe median).

Në Sistemet e IGJEUM vetëm disa punonjës kanë të drejtë të hyjnë në sistem (vetëm punonjësit që kanë të bëjnë drejtpërdrejtë me monitorimin dhe parashikimin në kohë reale të rreziqeve natyrore). Nga auditimi u konstatua se nuk ka një rregull të brendshme në lidhje me aksesin dhe përdorimin e sistemeve që IGJEUM përdor.
Madje, edhe për sa i përket backup-eve të të dhënave apo edhe faqes web, përsëri kryhen nga stafi i IGJEUM, edhe pse pozicioni i tyre nuk përputhet me këtë veprimtari. Në lidhje me këtë, u konstatua se nuk ka asnjë urdhër apo autorizim me shkrim nga titullari për kryerjen e punëve si: administrim i të dhënave të dy serverave, administrim i faqes web, kontroll të log-eve të web, etj. Kjo situatë, në opinion të grupit të auditimit, përbën një risk të lartë për sa i përket sigurisë së të dhënave të institucionit, pasi në rast të një dëmtimi, humbjeje apo kompromentimi të këtyre të dhënave, nuk ka asnjë person i cili mban përgjegjësi për to. Administrimi i këtyre atributeve individualisht dhe pa autorizim, nuk jep siguri të arsyeshme për kryerjen e tyre konform dispozitave ligjore si dhe praktikave më të mira.

Aksesi i përdoruesve gjithmonë limitohet me password (passwordet duhet të jenë të gjatë mbi 8 karaktere si edhe të përmbajnë karaktere të veçanta si !@$ etj). Passwordet që janë online enkriptohen me MD5.
Informacioni sensitiv arkivohet në server mbi baza mujore në disa raste edhe ditore, por për këtë nuk ka një dokumentacion të mbajtur nga një grup pune apo individ. Në opinion të grupit të auditimit, mungesa e gjurmës audituese në proceset e punë së institucionit në lidhje me përdorimin e teknologjisë së informacionit lidhet me mungesën e procedurave të miratuara për operacionet IT në IGJEUM.
Aktualisht IGJEUM përdor 4 IP reale. Njëra përdoret nga Qendra Kombëtare për Parashikimin dhe Monitorimin e Rreziqeve Natyrore. 2 IP të tjera reale përdoren nga Qendra Kombëtare e monitorimit të aktivitetit sizmik si edhe 1 IP përdoret për shërbimin e internetit

të stafit të IGJEUM. Rrjeti ka një sallë të veçantë në të cilën ndodhen Serverat, switchet të vendosura në Rack të ndryshëm.

Instituti i Gjeoshkencave, Energjisë, Ujit dhe Mjedisit shfrytëzon teknologjinë e informacionit për një sërë procesesh të cilat ndihmojnë në përmbushjen e objektivave institucionale.
IGJEUM ka të ndërtuar një rrjet të brendshëm në zyrat qendrore si dhe një rrjet privat për stacionet që ka në varësi në qytetet e Shqipërisë nga një operator ISP i cili ka konfiguruar rrjetin në VLAN (Virtual LAN).

Menaxhimi i routerave bëhet nga Operatori ISP, ndërsa stafi i IGJEUM nuk ka asnjë akses në routerat e vendosur në stacionet e IGJEUM. I gjithë trafiku mblidhet në një router në zyrën qendrore nga ku lidhet edhe me rrjetin e brendshëm

IGJEUM ka të instaluar software për monitorimin e aktivitetit sizmik i cili është i lidhur me sensorët e instaluar në terren. Ky software mbledh të dhëna në kohë reale duke shfrytëzuar rrjetin data. Këto të dhëna i shkruan në një database MySQL. Software është i hostuar në një PC të thjeshtë i cili funksionon si Server. Software ka gjithashtu mundësi komunikimi API si dhe akses Webi për konfigurime etj. Kompjuteri është konfiguruar me sistem operimi UBUNTU i cili ka arkitekture LINUX. Ka të instaluar 2 karta rrjeti ku njëra kartë ka të konfiguruar network-un për LAN të brendshëm i cili lidhet me LAN të zyrës qendrore si dhe komunikon me pajisjet e sensorëve të instaluar në terren, ndërsa karta e dytë ka të instaluar një IP publike e cila shërben që kompania që ka ndërtuar Software-in të futet remote.

Për të siguruar backup-et, IGJEUM ka një Storage dhe të dhënat e backup bëhen manualisht çdo fund muaji.

Referuar politikave të sigurisë dhe mbarëvajtjes së proceseve online, IGJEUM lejon ISP për monitorimet e shërbimeve online si dhe sigurisë.

Si përfundim:
- IGJEUM nuk ka asnjë menaxhim dhe informacion se çfarë ndodh në rrjetin DATA në të gjitha pikat e saj. Për këtë arsye, grupi i auditimit vlerëson se ka risk të lartë për cënimin e sigurisë së informacionit. Gjithashtu mungesa e aksesit dhe mos konfigurimi i saktë, ndikon në rritjen e mundësisë së hyrjes të paautorizuar në sistemet dhe databazat e IGJEUM.
- Siguria mbi portat e aksesit në zyrën qendrore nga ku është konfiguruar edhe routeri kryesor me IP Publike nuk ka të konfiguruar mbrojtjen në portat e aksesit për jashtë. Nga një testim i bërë nga grupi i auditimit, rezulton se porta e aksesit nga jashtë [redacted], [redacted], [redacted] janë të hapura.
- IGJEUM nuk përdor hardware të posaçëm Server për sistemin e monitorimit të aktivitetit sizmik, por ka të vendosur një PC me arkitekturë përdorimi nga disa persona.
- Mbrojtja për të dhënat personale, bllokimi i hyrjeve të pa autorizuara me firewall në sistemin e operimit është i fikur.
- Useri "root" i cili është Super Administrator i sistemit është i aktivizuar dhe nuk ka usera me të drejta të limituara për të hyrë në sistem.
- Infrastruktura e backup kryhet manualisht dhe nuk ka një sistem të mirëfilltë backup/replikim ditor çka përbën një risk serioz për humbjen dhe ndërhyrjen e të dhënave.

- IGJEUM nuk ka të ndërtuar një sistem LOG Managment si dhe një Sistem i cili analizon trafikun TCP/UDP në kohë reale.

12. Titulli i gjetjes: Nuk monitorohet infrastruktura IT
Situata: Nga auditimi u konstatua se IGJEUM nuk ka asnjë menaxhim dhe informacion se çfarë ndodh në rrjetin DATA në të gjitha pikat e saj, duke cënuar sigurinë e informacionit. Gjithashtu mungesa e aksesit dhe mos konfigurimi i saktë, ndikon në rritjen e mundësisë së hyrjes të paautorizuar në sistemet dhe databazat e IGJEUM.
Kriteri: Siguria e informacionit.
Ndikimi/efekti: Risk për thyerjen e sigurisë së informacionit.
Shkaku: IGJEUM nuk analizuar situatën mbi sigurinë e informacionit.
Rëndësia: E lartë
Rekomandim: IGJEUM dhe UPT të marrin masat për planifikimin e ndërtimit të një sistemi monitorimi, i cili të monitorojë Infrastrukturat Network, OS, Sigurinë dhe trafikun në kohë reale.

13. Titulli i gjetjes: Siguria në portat e aksesit.
Situata: Siguria mbi portat e aksesit në zyrën qendrore nga ku është konfiguruar edhe routeri kryesor me IP Publike nuk ka të konfiguruar mbrojtjen në portat e aksesit për jashtë. Nga një testim i bërë nga grupi i auditimit, rezulton se portat e aksesit nga jashtë [redacted], [redacted], [redacted] janë të hapura. Në këto kushte në rastin e një sulmi, IGJEUM është i ekspozuar ndaj hyrjeve të pa autorizuara në sistemet që ajo përdor.
Kriteri: Siguria e rrjetit të IGJEUM.
Ndikimi/efekti: Ekspozim ndaj hyrjeve të pa autorizuara në sisteme.
Shkaku: Portat e aksesit nga jashtë [redacted], [redacted], [redacted] janë të hapura.
Rëndësia: e Lartë
Rekomandim: IGJEUM të marrë masa për bllokimin e menjëhershëm të portave të aksesit për kategoritë Network dhe Sistemet e Operimit. Gjithashtu duhet të krijohet një script në routerin kryesor e cila duhet të monitorojë dhe bllokojë në kohe reale të gjitha IP-të që tentojnë hyrje të pa autorizuara.

14. Titulli i gjetjes: IGJEUM përdor për server një PC të thjeshtë dhe kryen backup manual
Situata: Nga auditimi u konstatua se IGJEUM nuk përdor hardware të posaçëm Server, por ka të vendosur një PC me arkitekturë përdorimi nga disa persona, situatë e cila mund të ndikojë në performancën software-it dhe bllokimin e shërbimit të software monitorues. Ndërkohë procesi i backup-it kryhet manualisht, pra nuk ka një sistem të mirëfilltë backup/replikim ditor çka përbën një risk serioz për humbjen e të dhënave.
Kriteri: Siguria e rrjetit të IGJEUM.
Ndikimi/efekti:
Shkaku: IGJEUM nuk ka kryer investimet e nevojshme për përmirësimin e rrjetit.
Rëndësia: E lartë
Rekomandim: IGJEUM të marrë masa për instalimin e software në një arkitekturë server, e cila të jetë projektuar për të qëndruar ndezur dhe të punojë me intensitet të lartë. Gjithashtu të krijohet një sistem automatik i cili kryen backup-e ditore dhe inkrementale për bazën e të dhënave.

15. Titulli i gjetjes: Firewall inaktiv dhe useri “root” aktiv.

Situata: Nga verifikimi i konfigurimit të firewall-it u konstatua se ai është i pa aktivizuar, çka lejon hyrje të pa autorizuara. Gjithashtu useri "root" i cili është me të drejta të plota, pra "Super Administratori" është aktiv, dhe në rastin e një ndërhyrjeje të pa autorizuar, mund të fshihen ose të merren të dhëna sensitive.
Kriteri: Siguria e të dhënave.
Ndikimi/efekti: Risk për humbje apo fshirje të dhënash.
Shkaku: Firewall i çaktivizuar.
Rëndësia: E lartë
Rekomandim: IGJEUM të marrë masat për aktivizimin e firewall-it të sistemit të operimit dhe bllokimin e portave të aksesit, duke krijuar një listë e cila lejon vetëm IP-të që IGJEUM bashkëpunon për shkëmbimin e të dhënave. Useri i aksesit "root" të bëhet disable dhe të krijohet një user tjetër me të drejta Administrative.

4. Auditim me zgjedhje i rrjetit të stacioneve sizmologjike dhe meteorologjike në Republikën e Shqipërisë.

Nga auditimi u konstatua se:
<u>Rrjeti sizmologjik</u>
Bazuar në misionin dhe detyrat kryesore të IGJEUM-it, stafit të punonjësve shkencorë dhe infrastrukturës që zotëron, DS ka për detyrë:
-Monitorimin, regjistrimin dhe analizimin e vazhdueshëm 24/7 të aktivitetit sizmik të vendit nëpërmjet rrjeteve kombëtare të monitorimit sizmologjik dhe gjeodinamik si dhe njoftimin në kohë reale të organizmave shtetërore përgjegjëse për emergjencat civile dhe të publikut për rreziqet nga tërmetet;
-Studime të thelluara në fushën e sizmologjisë dhe të sizmotektonikës për tërmetet që godasin vendin tonë;
-Formulimin e hartave te rrezikut sizmik të vendit.
DS ka në përdorim 3 rrjete sizmologjike
1. Rrjeti i Lëkundjeve të Dobëta i përbërë nga 8 stacione,
2. Rrjeti i Lëkundjeve të Forta i përbëra nga 17 stacione dhe
3. Rrjeti Gjeodinamik i përberë nga 9 stacione dhe aktualisht numri i stacioneve ka shkuar në 11, me dhurimin kohët e fundit nga Universiteti Savois Grenobel, France dhe 2 stacione te tjera. Gjithashtu duhet të theksohet se të gjitha pajisjet (sensorët) janë dixhital dhe grumbullimi i të dhënave nga stacionet periferike (të shpërndara në gjithë territorin e vendit) në Qendrën Kombëtare të Monitorimit të Aktivitetit Sizmik pranë IGJEUM-it bëhet në kohë reale.
Të tre rrjetet sizmologjike të DS ofrojnë kontrollin në distancë dhe transmetimin në kohë reale ndërmjet sistemit VSAT, radio linjave dhe rrjetit mobile 3G.

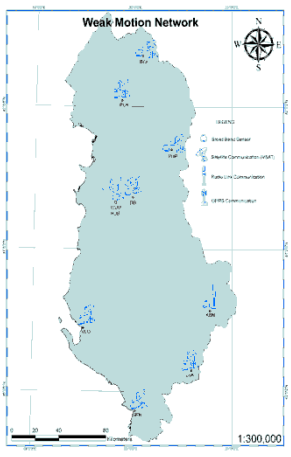


Figura 1 Figura 2 Figura 3

Figura 1. Stacionet e rrjetit sizmologjik të Shqipërisë
Figura 2. Rrjeti Shqiptar i Lëkundjeve të Forta
Figura 3. Rrjeti permanent i stacioneve GNSS të Shqipërisë

Grupi i auditimit e konsideroi të nevojshme verifikimin e gjendjes në të cilën ndodhen stacionet e RRS dhe pajisjet e tyre. Në fillimet e veta këto stacione janë konceptuar të vendosura në godina të përmasave të vogla me dy kate dhe me një dhomë të veçantë pranë godinës së stacionit të ndërtuar mbi shkëmbinj të fortë, ku ndërtohej një bazament betoni mbi të cilin vendoseshin sensorët sizmikë si, sizmometrat, akselerografët, sizmoskopët. Kati i parë i godinës 2-katëshe ka shërbyer si mjedis pune (zyra) për punonjësin e stacionit, kurse kati i dytë ishte konceptuar si ambient banimi për punonjësin e stacionit sizmologjik. Deri në fundin e viteve '90, RRS është bazuar tërësisht në regjistrimin analog të ngjarjeve sizmike, e në këto kushte ka qenë e domosdoshme prania e personelit i cili interpretonte sizmogramën e regjistruar dhe e dërgonte në Institut informacionin parametrik për ngjarjen sizmike nëpërmjet lidhjes telefonike. Punonjësi duke banuar në godinën e stacionit, e kalonte pjesën më të madhe të kohës pranë aparateve sizmologjike, të cilat sapo fillonte të regjistrohej një tërmet lëshonin një alarm zanor, duke tërhequr në këtë mënyrë vëmendjen e tij. Në fillimin e viteve '90, punonjësve të RRS ju mundësua privatizimi i katit të dytë të godinës ku ata banonin. Aktualisht, asnjë prej punonjësve që privatizuan katet e dyta të godinave të stacioneve sizmologjike nuk banon në to. Ato u janë shitur personave të tjerë, të cilët deri vonë, ish-Instituti i Sizmologjisë ka qënë i detyruar t'i punësonte për të siguruar vazhdimësinë e punës.
Me instalimin e teknologjisë dixhitale të regjistrimit dhe transmetimit të sinjalit sizmik, veçanërisht me vendosjen e sistemit sizmografik satelitor VSAT, roli i punonjësve të stacioneve të rrjetit është zvogëluar ndjeshëm. Ata tashmë kryejnë funksionin e rojës së aparaturave dhe vëzhguesin e funksionimit të tyre, si dhe ndonjë shërbim tjetër sekondar (tërheqje të faturave telefonike dhe të energjisë, njoftim për ndjeshmërinë e tërmeteve të zonës, etj.). Shërbimet për të cilat kanë nevojë pajisjet e stacioneve, kryhen nga punonjësit e DS në Tiranë.
Nga verifikimi në terren si dhe komunikimi me përfaqësues të IGJEUM, u konstatua se stacionet sizmike kanë mjaft problematika. Më poshtë trajtojmë disa prej tyre:
-Godina e stacionit të Beratit është zaptuar prej vitit 1997.
-Në stacionet e Korçës, Vlorës, Shkodrës, Bajram Currit, Sarandës, Kukësit dhe Pukës nuk janë bërë ndërhyrje prej kohës kur janë ndërtuar, para rreth 30-35 vjetësh, dhe gjendja e tyre paraqitet mjaft kritike, duke cënuar monitorimin pa ndërprerje të aktivitetit sizmik të vendit. Duhet të theksojmë se IGJEUM ka bërë kërkesa çdo vit për rregullimin e godinave, por për këtë nuk ka pasur miratim nga UPT.
-Në të gjithë stacionet e rrjetit mungojnë rrufepritëset, gjë që ka dëmtuar dhe përbën rrezik të vazhdueshëm për prishjen në vazhdimësi të pajisjeve.
-Dikur, stacionet sizmike janë ndërtuar në periferi dhe larg mjedisit urban si kusht për të qënë sa më larg zhurmave që dëmtonin sinjalin sizmik, tashmë shumë prej këtyre stacioneve janë pjesë e zonave të banuara, gjë që ka ulur cilësinë e regjistrimit. Këto stacione duhet të

zhvendosen në pika të tjera, larg zhurmave urbane, me qëllim rritjen e cilësisë së regjistrimit të aktivitetit sizmik në vendin tonë.
-Rrjeti sizmologjik ekzistues i monitorimit nuk e mbulon plotësisht të gjithë territorin kombëtar, duke ndikuar në saktësinë dhe shpejtësinë e përcaktimit të epiqendrave të tërmeteve dhe ngjarjeve sizmike.
-Mjetet e komunikimit janë ende manuale dhe mungon një rrjedhë e vazhdueshme dhe e aktualizuar për mbledhjen, vlerësimin, analizën dhe përhapjen e informacionit sizmik. Përdoruesit potencialë të tij, qofshin këta studiues vendas apo partnerë të huaj, organizma publike ose firma private, veçanërisht Zyra Operacionale e Emergjencave Civile e kanë të vështirë që të sigurojnë në kohë reale (on line) informacionin që u nevojitet.
Grupi i auditimit verifikoi në terren stacionet e Tiranës, Vlorës, Shkodrës dhe Beratit, si më poshtë:

Tirana







Vlora





Shkodra







Berat




Nga sa shihet më sipër, konstatohet se stacionet sizmologjike janë amortizuar në një nivel i cili përbën risk të lartë për vazhdimësinë pa ndërprerje të monitorimit sizmik në vend.

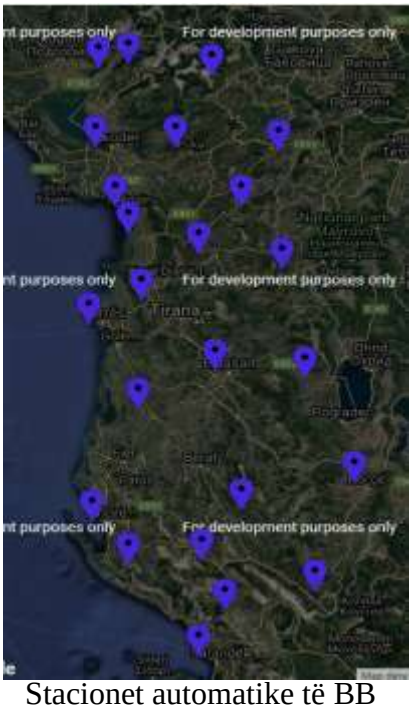
Rrjeti meteorologjik

IGJEUM ka një Sistem Kombëtar të Monitorimit Meteorologjik, i cili përbëhet nga 135 stacione manuale (natyra e vrojtimit), si dhe 20 stacione automatike të vendosura në kuadër të

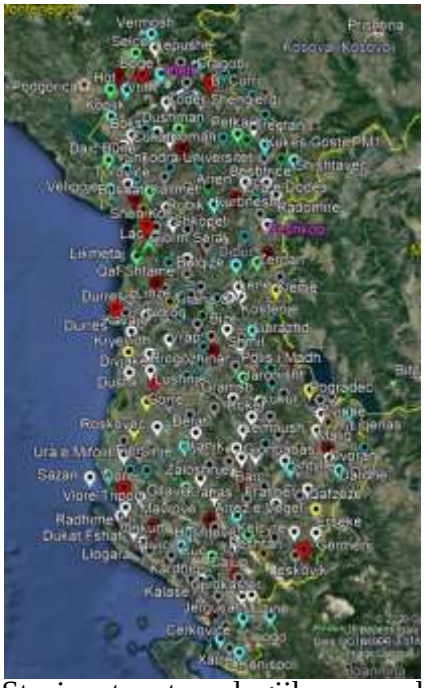
një projekti të BB. Gjithashtu dhe në kuadër të një projekti me GTZ janë instaluar dhe funksionojnë 4 stacione në zonën V të vendit.
Pjesa e vrojtimeve manuale vjen në Institut nëpërmjet ditarëve mujore, e cila më pas përpunohet pjesërisht sipas nevojave institucionale dhe arkivohet në përputhje me standardet e WMO.
Pjesa e stacioneve automatike është ende në proces kalibrimi e riparimi.

Rrjeti Hidrologjik

IGJEUM ka 104 stacione hidrologjike dhe detare, nga të cilat 20 janë automatike të vendosura nga projekti i BB (16 në hidro dhe 4 detare), 1 stacion automatik detar për matjen e valës i vendosur në Shëngjin në kuadër të projektit Hermes në vitin 2019 (me para financim nga buxheti i brendshëm i UPT-së) dhe 5 stacione të vendosura në basenin e Lumit Drin dhe Buna në kuadër të Projektit GIZ.
Më poshtë paraqitet harta e stacioneve meteorologjike dhe hidrologjike në vendin tonë:



Stacionet automatike të BB


Stacionet meteorologjike manuale

Grupi i auditimit verifikoi në terren stacionet meteorologjike në Fier dhe Shën Koll, nga ku u konstatua një amortizim deri në mosfunksionim të këtyre stacioneve.

Fier





Shën Koll





16. Titulli i gjetjes: Gjendja e stacioneve.
Situata: Nga auditimi me zgjedhje i ambienteve të stacioneve sizmologjike në Tiranë, Vlorë, Shkodër dhe Berat, u konstatuan problematika të tilla si:
- të gjitha ambientet/godinat ku ndodhen pajisjet për matjen e lëkundjeve sizmike janë mjaft të amortizuara dhe të ekspozuara ndaj lagështisë, duke pasur nevojë urgjente për riparime dhe izolime;
- instalimet elektrike janë mjaft të amortizuara;
- stacioni i Tiranës ruhet me roje private vetëm në 8 orë nga 24 (nga ora 00:00 deri 08:00), dhe në 16 orët e tjera është e pambrojtur;
- në stacionin e Shkodrës është e dëmtuar soleta, dhe izolimi ndaj reshjeve është bërë thjesht duke e mbuluar me plastmasë.
- në stacionin e Vlorës është e dëmtuar soleta dhe bazamenti i sensorëve;.

Gjendja e këtyre stacioneve është mjaft kritike, duke rritur riskun e dëmtimit të pajisjeve brenda tyre, vlera e të cilave është e konsiderueshme, e për pasojë të cënohet seriozisht aktiviteti i monitorimit sizmik në vend.
Nga auditimi me zgjedhje i ambienteve të stacioneve meteorologjike në Fier dhe Shën Koll, u konstatua se pajisjet janë mjaft të amortizuara dhe një pjesë e tyre jofunksionale, duke rritur riskun e marrjes së të dhënave jo të plota dhe të pasakta mbi monitorimin e aktivitetit meteorologjik në vend.
Kriteri: Zhvillimi i aktivitetit monitorues në kushte të përshtatshme.
Ndikimi/efekti: Risk për dëmtimit e pajisjeve brenda këtyre stacioneve marrjen e të dhënave jo të plota dhe të pasakta.
Shkaku: Nuk janë kryer investimet e nevojshme.
Rëndësia: E lartë
Rekomandimi: IGJEUM në bashkëpunim me UPT të marrin masa për riparimin dhe standardizimin e stacioneve sizmologjike, meteorologjike dhe hidrike në vend, me qëllim sigurimin e kushteve optimale për monitorimin e aktivitetit sizmik në vend.

IGJEUM ka dërguar Projektraportin e auditimit të nënshkruar nga Drejtori i IGJEUM, me shkresë përcjellëse nr. 152 prot, datë 15.05.2020, protokolluar në KLSH me nr. 69/4 prot, datë 18.05.2020.
Bashkëlidhur projektraportit nuk janë paraqitur observacione.

IV. KONKLUZIONE DHE REKOMANDIME

A. MASA ORGANIZATIVE:

1. Gjetje nga auditimi: Nga auditimi u konstatua se IGJEUM nuk ka një Plan Strategjik për Teknologjinë e Informacionit, ku të adresohen qartë objektivat e institucionit, kapaciteti aktual i TI për të ofruar shërbime dhe kërkesat e burimeve, duke marrë në konsideratë ekzistencën e infrastrukturës së IT, investimeve, modelin e ofrimit, si dhe paraqitjen e strategjisë që integron këto elementë në një qasje të përbashkët për të mbështetur objektivat e institucionit.
(në mënyrë të detajuar është pasqyruar në faqet 8-15 të Raportit të Auditimit)
1.1 Rekomandimi: IGJEUM në bashkëpunim me UPT, duke marrë në konsideratë kohën, burimet e nevojshme si dhe rëndësinë e të dhënave që institucioni zotëron dhe përpunon, të marrin masa për hartimin e një Plani Strategjik, ku të adresohen qartë objektivat e institucionit në drejtim të Teknologjisë së Informacionit.

Brenda vitit 2020

2. Gjetje nga auditimi: Nga auditimi u konstatua se Instituti i Gjeoshkencave, Energjisë, Ujit dhe Mjedisit nuk ka në përbërje strukturë të teknologjisë së informacionit, madje asnjë pozicion specialisti IT, duke krijuar risk të lartë mbi identifikimin, trajtimin dhe zgjidhjen e problematikave të ndryshme të Teknologjisë së Informacionit në institucion. Si institucion nën varësinë e Universitetit Politeknik të Tiranës, IGJEUM duhet të ketë suportin e specialistëve IT të Universitetit Politeknik të Tiranës. UPT ka në strukturën e tij 7 Fakultete dhe IGJEUM, dhe për mbulimin e problematikave në fushën e IT, ka vetëm 2 specialistë të fushës të atashuar në zyrat e UPT. Në të tilla kushte, problemet që hasen në IGJEUM në fushën e Teknologjisë së Informacionit gjejnë zgjidhje pothuajse gjithnjë nëpërmjet vetë stafit të cilët kanë njohuri në këtë fushë.
(në mënyrë të detajuar është pasqyruar në faqet 8-15 të Raportit të Auditimit)
2.1 Rekomandimi: IGJEUM në bashkëpunim me UPT të marrin masa për krijimin e një strukture të Teknologjisë së Informacionit në IGJEUM, në nivel sektori apo drejtorie, me qëllim përmbushjen e nevojave institucionale mbi identifikimin, trajtimin dhe zgjidhjen e problematikave të ndryshme të Teknologjisë së Informacionit.

Menjëherë

3. Gjetje nga auditimi: Nga auditimi u konstatua se IGJEUM ka vetëm 1 (një) punonjës me profil shkenca kompjuterike, i cili në strukturë është staf akademik pranë Departamentit të Sizmologjisë. Duke qenë i vetmi punonjës me një profil të tillë, i janë dhënë *verbalisht* kompetenca si: administrim të sistemit sizmologjik, administrim të të dhënave të dy serverave, administrim të faqes web, kontroll të log-eve të web; etj. Grupi i auditimit vlerëson se fakti që një punonjës ka profil të tillë, nuk përbën arsye legjitime që ai të ketë këto

kompetenca. Kjo zgjidhje e gjetur në kushte të mungesës të një strukture IT, është e papërshtatshme, madje në mungesë të një autorizimi me shkrim nga ana e titullarit, përbën risk të lartë për sa i përket sigurisë së informacionit dhe mbrojtjes së të dhënave të institucionit.
(në mënyrë të detajuar është pasqyruar në faqet 8-15 të Raportit të Auditimit)
3.1 Rekomandimi: Strukturat drejtuese të IGJEUM në vijimësi të dokumentojnë çdo autorizim mbi përdorimin e sistemeve të Teknologjisë së Informacionit, si dhe të caktojnë detyrat administruese të të dhënave në përputhje me detyrat funksionale të punonjësve.

Menjëherë dhe në vijimësi

4. Gjetje nga auditimi: Nga auditimi u konstatua se IGJEUM ka një organikë të miratuar prej 71 punonjësish, ndërkohë janë të punësuar vetëm 48 punonjës ose 67.6% e organikës së miratuar. Mungesat e burimeve njerëzore rrit riskun e cënimit të monitorimit të plotë të aktivitetit sizmik, meteorologjik dhe hidrologjik në Institutin e Gjeoshkencave, Energjisë, Ujit dhe Mjedisit, pasi ky monitorim kryhet 24 orë pa ndërprerje.
(në mënyrë të detajuar është pasqyruar në faqet 8-15 të Raportit të Auditimit)
4.1 Rekomandimi: IGJEUM dhe UPT të marrin masat e nevojshme për plotësimin e vendeve vakante sipas strukturës së miratuar të IGJEUM, me qëllim përmbushjen e detyrimeve institucionale, në drejtim të monitorimit të aktivitetit sizmik, meteorologjik dhe hidrik pa ndërprerje.

Menjëherë dhe në vijimësi

5. Gjetje nga auditimi: Nga auditimi u konstatua se IGJEUM nuk ka procedura të miratuara për sigurinë e informacionit, apo plane për sigurinë e sistemeve IT, ku të vendosen kërkesat për mbrojtjen e aseteve të informacionit. Gjithashtu IGJEUM nuk ka hartuar një rregullore për përdorimin e Teknologjisë së Informacionit, duke ndikuar në akses të pakufizuar ndaj sistemeve që zotëron.
(në mënyrë të detajuar është pasqyruar në faqet 8-15 të Raportit të Auditimit)
5.1 Rekomandimi: IGJEUM në bashkëpunim me UPT, të marrin masat e nevojshme për hartimin e rregullave dhe procedurave mbi përdorimin e teknologjisë së informacionit në IGJEUM, duke dhënë siguri të arsyeshme mbi sigurinë e të dhënave të institucionit.

Menjëherë

6. Gjetje nga auditimi: Nga auditimi u konstatua se Instituti i Gjeoshkencës, Energjisë, Ujit dhe Mjedisit nuk ka një regjistër risku për Teknologjinë e Informacionit ku të jenë evidentuar ato situata të mundshme apo ngjarje të cilat mund të kenë efekt negativ në mbarëvajtjen e punës së këtij institucioni, duke mos patur kështu një plan masash për zgjidhjen e problematikave të ndryshme që mund të ndodhin.
(në mënyrë të detajuar është pasqyruar në faqet 8-15 të Raportit të Auditimit)
6.1 Rekomandimi: IGJEUM të marrë masat për hartimin e një regjistri risku për teknologjinë e informacionit ku të jenë evidentuar ato ngjarje të mundshme të cilat mund të kenë efekt negativ në mbarëvajtjen e punës institucionale, me qëllim krijimin e një plani pune në rastet e shfaqjes së problematikave të ndryshme në fushën e teknologjisë së informacionit.

Menjëherë dhe në vijimësi

7. Gjetje nga auditimi: Nga auditimi u konstatua se IGJEUM nuk disponon një Plan Vazhdimësie (BCP) dhe Plan Rikuperimi (DRC) për garantimin e vazhdimësisë së ofrimit të shërbimit, duke krijuar risk për humbjen e të dhënave, veprim në kundërshtim me pikën 1 të VKM Nr. 710, datë 21.8.2013 "*Për krijimin dhe funksionimin e sistemeve të ruajtjes së*

informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit", i ndryshuar.
(në mënyrë të detajuar është pasqyruar në faqet 15-20 të Raportit të Auditimit)
7.1 Rekomandim: IGJEUM duke marrë në konsideratë kohën dhe burimet e nevojshme të marrë masa për ndërtimin dhe hartimin e Planit të Vazhdimësisë dhe Planit të Rikuperimit, duke përfshirë planet për backup dhe rimëkëmbjen nga katastrofat për sistemet, pajisjet kompjuterike dhe të dhënat, hartimin e planit të sigurisë së informacionit dhe implementimin e tij, duke përfshirë ndarjen e detyrave/përgjegjësive të sigurisë në TIK.

Brenda vitit 2020 dhe në vijimësi

8. Gjetje nga auditimi: IGJEUM nuk ka analizuar, identifikuar dhe planifikuar nevojat për trajnim të punonjësve për Sigurinë e Informacionit, në përmbushje të nevojave të përgjithshme dhe specifike që ndihmojnë në mbarëvajtjen dhe funksionimin e veprimeve dhe procedurave të këtij instituti.
(në mënyrë të detajuar është pasqyruar në faqet 15-20 të Raportit të Auditimit)
8.1 Rekomandim: Strukturat Drejtuese në IGJEUM të hartojnë plane për zhvillimin e trajnimeve në lidhje me sigurinë e informacionit në përmbushje të nevojave të përgjithshme dhe specifike që ndihmojnë në mbarëvajtjen dhe funksionimin e veprimeve dhe procedurave të këtij instituti.

Brenda vitit 2020

9. Gjetje nga auditimi: IGJEUM nuk ka politika të aprovuara për menaxhimin e ndryshimeve, e cilat të përmbajnë kontrollet e përshtatshme përgjatë ciklit të ndryshimit, si dhe nuk disponon procedurë për inicimin, rishikimin dhe aprovimin e ndryshimeve, klasifikimin e tyre sipas rëndësisë, ndarjen e detyrave dhe përgjegjësive për kryerjen e ndryshimeve.
(në mënyrë të detajuar është pasqyruar në faqet 15-20 të Raportit të Auditimit)
9.1 Rekomandim: Strukturat Drejtuese në IGJEUM në të ardhmen të marrin masat e nevojshme për hartimin e procedurave mbi menaxhimin e ndryshimeve në fushën e Teknologjisë së Informacionit dhe dokumentimin e gjithë procesit të ndryshimeve.

Brenda vitit 2020

10. Gjetje nga auditimi: Nga auditimi mbi investimet e kryera në fushën e Teknologjisë së Informacionit, u konstatua se ato janë në përpjesëtim të zhdrejtë me rëndësinë kombëtare që ka monitorimi i aktivitetit sizmik, meteorologjik dhe hidrologjik. Pasojat e mungesës së investimeve të domosdoshme në drejtim të teknologjisë së informacionit dhe më gjerë, janë vënë re gjatë ngjarjeve të fundit në vend. Konkretisht, referuar regjistrimeve të vëna në dispozicion nga Departamenti i Sizmologjisë në IGJEUM në lidhje me tërmetin e datës 26.11.2019, i cili ka patur impakt në jetë njerëzish dhe dëme të shumta materiale, konstatohet se mungojnë të dhëna të plota nga stacioni i Durrësit, i cili është stacioni më i afërt me vatrën e tërmetit. Ky stacion ka regjistruar vetëm 15 sekondat e para të tërmetit, si pasojë e ndërprerjes së energjisë elektrike. Nisur nga fakti që gjatë një tërmeti të fortë ekziston një probabilitet i lartë për ndërprerjen e energjisë elektrike, është e domosdoshme pajisja e stacioneve sizmologjike me bateri (UPS) të cilat mundësojnë regjistrimin e të dhënave edhe nëse ndërpritet energjia elektrike.
Theksojmë se funksionimi i rregullt i tre rrjeteve sizmike në vendin tonë është i rëndësishme për parashikimin dhe monitorimin e katastrofave natyrore në kohë reale, duke marrë masa në drejtim të mbrojtjes së jetës së njerëzve dhe reduktimin e dëmeve materiale.
(në mënyrë të detajuar është pasqyruar në faqet 8-15 të Raportit të Auditimit)

10.1 Rekomandimi: IGJEUM në bashkëpunim me UPT, duke marrë shkas edhe nga problematikat e shfaqura gjatë tërmetit të datës 26.11.2019, të marrin masat e nevojshme për analizimin e situatës dhe hartimin e një plan veprimi të ndarë në 3 faza, afat shkurtër, afat mesëm dhe afat gjatë, për kryerjen e ndërhyrjeve në sistemet IT si dhe në ambientet fizike ku këto sisteme janë, me qëllim krijimin e kushteve të përshtatshme për mbledhjen, përpunimin dhe ruajtjen e të dhënave që këto sisteme kanë, në përputhje me standardet dhe praktikat më të mira të fushës.

Menjëherë

11. Gjetje nga auditimi: Nga auditimi u konstatua se IGJEUM nuk ka Marrëveshje në Nivel Shërbimi (MNSH/SLA), për mirëmbajtjen e sistemeve, veprim në kundërshtim me pikën 2 të VKM Nr. 710, datë 21.8.2013 "*Për krijimin dhe funksionimin e sistemeve të ruajtjes së informacionit, vazhdueshmërisë së punës dhe marrëveshjeve të nivelit të shërbimit*", i ndryshuar, pika 2, ku citohet: "*Çdo institucion, i cili ka ose do të zhvillojë një sistem në fushën e teknologjisë së informacionit, që ofron shërbime për qytetarët, për biznesin dhe për ndërveprim e shkëmbim informacioni për administratën publike nëpërmjet sistemeve elektronike, duhet të parashikojë dhe të hartojë marrëveshje kontraktuale mbi nivelin e shërbimit (Service Level Agreement - SLA)*". Mirëmbajtja e sistemeve kryhet nga vetë personeli në rastet kur ka probleme, por në asnjë rast nuk kemi një monitorim të dokumentuar.
(në mënyrë të detajuar është pasqyruar në faqet 8-15 të Raportit të Auditimit)
11.1 Rekomandimi: IGJEUM në bashkëpunim me UPT të marrin masat e nevojshme për lidhjen e një marrëveshjeje në nivel shërbimi me qëllim garantimin e vazhdimësisë pa probleme të sistemeve që zotëron.

Menjëherë dhe në vijimësi

12. Gjetje nga auditimi: Nga auditimi me zgjedhje i ambienteve të stacioneve sizmologjike në Tiranë, Vlorë, Shkodër dhe Berat, u konstatuan problematika të tilla si:
- të gjitha ambientet/godinat ku ndodhen pajisjet për matjen e lëkundjeve sizmike janë mjaft të amortizuara dhe të ekspozuara ndaj lagështisë, duke pasur nevojë urgjente për riparime dhe izolime;
- instalimet elektrike janë mjaft të amortizuara;
- stacioni i Tiranës ruhet me roje private vetëm në 8 orë nga 24 (nga ora 00:00 deri 08:00), dhe në 16 orët e tjera është e pambrojtur;
- në stacionin e Shkodrës është e dëmtuar soleta, dhe izolimi ndaj reshjeve është bërë thjesht duke e mbuluar me plastmasë.
- në stacionin e Vlorës është e dëmtuar soleta dhe bazamenti i sensorëve;.

Gjendja e këtyre stacioneve është mjaft kritike, duke rritur riskun e dëmtimit të pajisjeve brenda tyre, vlera e të cilave është e konsiderueshme, e për pasojë të cënohet seriozisht aktiviteti i monitorimit sizmik në vend.
Nga auditimi me zgjedhje i ambienteve të stacioneve meteorologjike në Fier dhe Shën Koll, u konstatua se pajisjet janë mjaft të amortizuara dhe një pjesë e tyre jofunksionale, duke rritur riskun e marrjes së të dhënave jo të plota dhe të pasakta mbi monitorimin e aktivitetit meteorologjik në vend.
(në mënyrë të detajuar është pasqyruar në faqet 24-30 të Raportit të Auditimit)
12.1 Rekomandimi: IGJEUM në bashkëpunim me UPT të marrin masa për riparimin dhe standardizimin e stacioneve sizmologjike, meteorologjike dhe hidrike në vend, me qëllim sigurimin e kushteve optimale për monitorimin e aktivitetit sizmik në vend.

Menjëherë

13. Gjetje nga auditimi: Nga auditimi u konstatua se IGJEUM nuk ka asnjë menaxhim dhe informacion se çfarë ndodh në rrjetin DATA në të gjitha pikat e saj, duke cënuar sigurinë e informacionit. Gjithashtu mungesa e aksesit dhe mos konfigurimi i saktë, ndikon në rritjen e mundësisë së hyrjes të paautorizuar në sistemet dhe databazat e IGJEUM.
(në mënyrë të detajuar është pasqyruar në faqet 21-24 të Raportit të Auditimit)
13.1 Rekomandim: IGJEUM dhe UPT të marrin masat për planifikimin e ndërtimit të një sistemi monitorimi, i cili të monitorojë Infrastrukturat Network, OS, Sigurinë dhe trafikun në kohë reale.

Menjëherë dhe në vijimësi

14. Gjetje nga auditimi: Siguria mbi portat e aksesit në zyrën qendrore nga ku është konfiguruar edhe routeri kryesor me IP Publike nuk ka të konfiguruar mbrojtjen në portat e aksesit për jashtë. Nga një testim i bërë nga grupi i auditimit, rezulton se portat e aksesit nga jashtë [redacted], [redacted], [redacted] janë të hapura. Në këto kushte në rastin e një sulmi, IGJEUM është i ekspozuar ndaj hyrjeve të pa autorizuara në sistemet që ajo përdor.
(në mënyrë të detajuar është pasqyruar në faqet 21-24 të Raportit të Auditimit)
14.1 Rekomandim: IGJEUM të marrë masa për bllokimin e menjëhershëm të portave të aksesit për kategoritë Network dhe Sistemet e Operimit. Gjithashtu duhet të krijohet një script në routerin kryesor e cila duhet të monitorojë dhe bllokojë në kohe reale të gjitha IP-të që tentojnë hyrje të pa autorizuara.

Menjëherë

15. Gjetje nga auditimi: Nga auditimi u konstatua se IGJEUM nuk përdor hardware të posaçëm Server, por ka të vendosur një PC me arkitekturë përdorimi nga disa persona, situatë e cili mund të ndikojë në performancën software-it dhe bllokimin e shërbimit të software monitorues. Ndërkohë procesi i backup-it kryhet manualisht, pra nuk ka një sistem të mirëfilltë backup/replikim ditor çka përbën një risk serioz për humbjen e të dhënave.
(në mënyrë të detajuar është pasqyruar në faqet 21-24 të Raportit të Auditimit)
15.1 Rekomandim: IGJEUM të marrë masa për instalimin e software në një arkitekturë server, e cila të jetë projektuar për të qëndruar ndezur dhe të punojë me intensitet të lartë. Gjithashtu të krijohet një sistem automatik i cili kryen backup-e ditore dhe inkrementale për bazën e të dhënave.

Menjëherë dhe në vijimësi

16. Gjetje nga auditimi: Nga verifikimi i konfigurimit të firewall-it u konstatua se ai është i pa aktivizuar, çka lejon hyrje të pa autorizuara. Gjithashtu useri "root" i cili është me të drejta të plota, pra "Super Administratori" është aktiv, dhe në rastin e një ndërhyrjeje të pa autorizuar, mund të fshihen ose të merren të dhëna sensitive.
(në mënyrë të detajuar është pasqyruar në faqet 21-24 të Raportit të Auditimit)
16.1 Rekomandim: IGJEUM të marrë masat për aktivizimin e firewall-it të sistemit të operimit dhe bllokimin e portave të aksesit, duke krijuar një listë e cila lejon vetëm IP-të që IGJEUM bashkëpunon për shkëmbimin e të dhënave. Useri i aksesit "root" të bëhet disable dhe të krijohet një user tjetër me të drejta Administrative.

Menjëherë

Me ndjekjen e zbatimit të detyrave dhe masave të përcaktuara në këtë vendim ngarkohet Departamenti i Auditimit të Teknologjisë së Informacionit.

Për sa më sipër paraqitet ky Raport Përfundimtar Auditimi

KONTROLLI I LARTË I SHTETIT