Monitorimi

i

Strategjisë Kombëtare

për Sigurinë Kibernetike

2020-2025

Tiranë, 2023

Tabela e Përmbajtjes

1. HYRJE

Siguria kibernetike është aktualisht më shumë se kurrë prioritet i qeverisë shqiptare. Sulmet kibernetike me të cilat u përball Shqipëria vitin e shkuar treguan rëndësinë e sigurisë kibernetike për të pasur një siguri kombëtare solide, si dhe vunë në dukje nevojën për forcimin e bashkëpunimit kombëtar dhe ndërkombëtar dhe rritjen e investimeve dhe kapaciteteve sa i përket mbrojtjes kibernetike. Ndonëse është bërë shumë për rritjen e nivelit të sigurisë kibernetike në vend, asnjë vend në botë nuk është imun ndaj sulmeve kibernetike, dhe sidomos vendet si Shqipëria, që kanë arritur një nivel të lartë të digjitalizimit të shërbimeve publike, duke u bërë kështu më të ekspozuar në këtë drejtim. Për të siguruar që Shqipëria të jetë e përgatitur për kërcënime të mundshme kibernetike, duke iu rezistuar dhe përgjigjur atyre në mënyrë të qëndrueshme, qeveria shqiptare po punon për të përmirësuar politikat aktuale si dhe për të vënë në jetë iniciativa dhe projekte të reja që kontribuojnë për krijimin e një ekosistemi të sigurt kibernetik.

Qëllimi kryesor i punës dhe nismave të qeverisë në këtë fushë ka qenë dhe është garantimi i sigurisë kibernetike në nivel kombëtar, nëpërmjet mbrojtjes së infrastrukturave të informacionit, duke fuqizuar mjetet teknologjike dhe juridike. Po ashtu, qeveria ka punuar edhe për edukimin dhe ndërgjegjësimin e shoqërisë, si dhe për ngritjen e kapaciteteve profesionale në fushën e sigurisë së informacionit, duke u angazhuar për të përgatitur një brez të ri të aftë për të përfituar nga përparësitë e teknologjisë së informacionit dhe për të përballuar sfidat e zhvillimit teknologjik. Një rëndësi e veçantë i është dhënë edhe adresimit të kërcënimeve kibernetike që shenjëstrojnë të rinjtë dhe fëmijët online, ku është punuar për krijimin e mekanizmave të nevojshëm për sigurinë e tyre në hapësirën kibernetike. Hapa të rëndësishëm janë ndërmarrë në kuadër të rritjes së bashkëpunimit kombëtar dhe ndërkombëtar në fushën e sigurisë dhe mbrojtjes kibernetike me partnerët strategjikë, ku janë nënshkruar një sërë marrëveshjesh bashkëpunimi, si dhe vijon puna për ta zgjeruar këtë bashkëpunim.

Strategjia Kombëtare për Sigurinë Kibernetike 2020-2025, miratuar me Vendimin nr. 1034 datë 24.12.2020, të Këshillit të Ministrave, përbën një instrument kyç për rritjen e sigurisë së rrjeteve dhe sistemeve të informacionit në nivel kombëtar, duke e konsideruar sigurinë kibernetike prioritet të qeverisë shqiptare.

Kjo strategji synon garantimin e sigurisë kibernetike në Republikën e Shqipërisë nëpërmjet, ngritjes dhe funksionimit të mekanizmave bashkëveprues institucionalë, instrumenteve ligjore dhe teknike, si element kritik i mbrojtjes në hapësirën kibernetike për infrastrukturat e informacionit, transaksionet dhe komunikimet elektronike; nëpërmjet ngritjes së kapaciteteve profesionale, rritjes së vetëdijes mbarëkombëtare, si dhe forcimit të bashkëpunimeve kombëtare dhe ndërkombëtare për një mjedis digjital të sigurt.

Strategjia mbështetet në parimet themelore të mëposhtme:

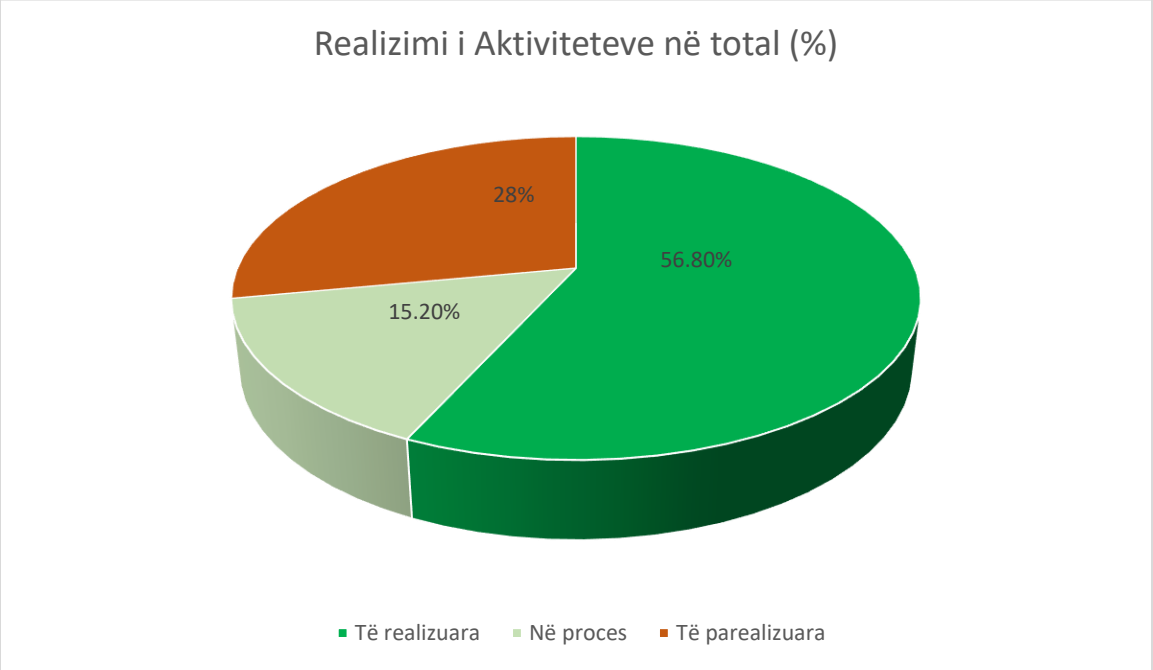
- zbatimi i vlerave të njëjta themelore në botën fizike dhe digjitale;
- mbrojtja e të drejtave themelore, liria e shprehjes, të dhënat personale dhe privatësia;
- qasja për të gjithë;
- qeverisje demokratike dhe efikase;
- përgjegjësi e përbashkët në garantimin e sigurisë kibernetike.

Aktorët e Planit të Veprimit të Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025 janë:

- Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike,
- Policia e Shtetit,
- Autoriteti Kombëtar për Sigurinë e Informacionit të Klasifikuar,
- Qendra për Koordinimin Kundër Ekstremizmit të Dhunshëm,
- Agjencia Kombëtare e Shoqërisë së Informacionit,
- Ministria e Shëndetësisë dhe Mbrojtjes Sociale,
- Ministria e Arsimit dhe Sportit.

Realizimi i aktiviteteve të Planit të Veprimit

Sa i përket zbatimit të Planit të Veprimit, rezulton se deri në vitin 2022, shkalla e realizimit të aktiviteteve në % është: aktivitete të realizuara 56.8% (71 aktivitete), aktivitete në process 15.2% (19 aktivitete) dhe aktivitete të parealizuara 28% (35 aktivitete). Bazuar tek këto të dhëna, arrihet në përfundimin se sa i përket rezultateve të arritura dhe aktiviteteve të zbatuara më shumë progres ka pasur në realizimin e Qëllimit të Politikës 1 dhe Qëllimit të Politikës 4.



2. METODOLOGJIA E MONITORIMIT

Vlerësimi i realizimit të objektivave të Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025, do të bëhet duke ndjekur në mënyrë periodike realizimin e planit të aktiviteve të parashikuara për periudhën si dhe ecurinë e indikatorëve kryesorë të monitorimit.

Analiza e këtij raporti është mbështetur kryesisht në monitorimin e realizimit të aktiviteteve të parashikuara në planin e veprimit që përfshin periudhën Janar – Dhjetor 2022.

Monitorimi i Strategjisë ka konsistuar në këto faza kryesore:

a) Raportimi i institucioneve mbi zbatimin e masave për arritjen e rezultateve për të cilat janë përgjegjëse, dhe

b) Monitorimi i indikatorëve të matshëm për Strategjinë Kombëtare të Sigurisë Kibernetike.

Me qëllim realizimin e sa më sipër, është kryer paraprakisht analiza e aktiviteteve të planit të veprimit sipas çdo prioriteti strategjik; janë identifikuar insitucionet përgjegjëse për zbatimin e tyre; është komunikuar me shkresë me çdo institucion dhe koordinuar në vazhdimësi me pikat e kontaktit për raportimin e statusit të realizimit sipas metodologjisë[1].

3. POLITIKAT E STRATEGJISË

Qëllimi i politikës 1. Garantimi i sigurisë kibernetike në nivel kombëtar, nëpërmjet mbrojtjes së infrastrukturave të informacionit, duke fuqizuar mjetet teknologjike dhe juridike.

Objektivat e prioritetit fokusohen në:

- Përmirësimi i kuadrit ligjor që normon dhe rregullon fushën e sigurisë kibernetike në vend, si dhe harmonizimi i i tij me direktivat dhe rregulloret e Bashkimit Europian.
- Ngritja dhe funksionimi i CSIRT-eve në të gjithë sektorët e industrisë në nivel kombëtar
- Fuqizimi dhe implementimi i masave të sigurisë në infrastrukturat kritike dhe të rëndësishme të informacionit
- Përmirësimi i infrastrukturave të informacionit për të luftuar krimin kibernetik, radikalizimin dhe ekstremizmin e dhunshëm

[1] *Shënim: Monitorimi i realizimit të aktiviteteve të Planit të Veprimit për vitin 2022 është mbyllur në datën 23 Mars 2023 dhe është vijuar me hartimin e raportit. Për aktivitetet që gjatë vitit 2022 kanë qenë në proces dhe janë realizuar në filllim të vitit 2023, përpara mbylljes së monitorimit, është dhënë informacioni për realizimin e tyre, por nuk janë llogaritur si aktivitete të realizuara në këtë raport.*

Për realizimin e objektivave të prioritetit të parë strategjik, institucionet e përfshira në realizimin e Planit të Veprimit, bazuar në raportimet e tyre, kanë arritur rezultatet si më poshtë vijon:

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK)

AKCESK ka punuar intensivisht për përafrimin e plotë të politikave dhe legjislacionit me politikat respektive të Bashkimit Evropian, në përputhje dhe me prioritetet dhe nevojat në nivel kombëtar. Gjithashtu, politikat e qeverisë shqiptare janë në një linjë me politikat e NATO-s sa i përket sigurisë kibernetike. Autoriteti, i cili vepron edhe në cilësinë e CSIRT-it Kombëtar, ka të hartuara dhe të miratuara procedurat për funksionimin dhe ushtrimin e veprimtarisë së tij. Ndonëse nuk është miratuar në vitin 2022, edhe pse e gjithë puna përgatitore është bërë në këtë vit kalendarik, vlen të përmendim që struktura e re e AKCESK, e cila parashikonte rritjen e punonjësve të institucionit nga 24 në 85, është miratuar me Urdhrin e Kryeministrit nr.32, datë 16.03.2023.

Është realizuar analiza e hendekut ligjor dhe institucional për Direktivat dhe Rregulloret e BE-së që normojnë fushën e sigurisë kibernetike.

Projektligji për transpozimin e Rregullores Evropiane eIDAS "Për identifikimin elektronik dhe shërbimet e besuara për transaksionet elektronike në tregun e brendshëm" është hartuar dhe ka përfunduar procesi i konsultimit publik (datë 07.12.2022 - 10.01.2023), është bërë reflektimi i komenteve dhe është dërguar i ripunuar në Kryeministri për të vijuar me procedurat e mëtejshme ligjore.

Gjithashtu, AKCESK ka përfunduar drafligjin "Për sigurinë kibernetike", duke transpozuar Direktivën NIS 2016/1148 të Parlamentit Evropian "Për masat e nivelit të lartë të sigurisë së rrjetit dhe sistemeve të informacionit në të gjithë Bashkimin Evropian" dhe duke përfshirë edhe disa elemente nga Direktiva NIS 2022/2555**.**

Në zbatim të Ligjit nr.2/2017 "Për Sigurinë Kibernetike" dhe bazuar në Direktivën Europiane të Rrjeteve dhe Sistemeve të Informacionit 2016/1148, të Parlamentit Evropian "Për masat e nivelit të lartë të sigurisë së rrjetit dhe sistemet e informacionit në të gjithë Bashkimin Evropian", është miratuar lista e përditësuar e infrastrukturave kritike dhe të rëndësishme të informacionit me Vendimin e Këshillit të Ministrave nr. 761, datë 12.12.2022 "Për miratimin e listës së infrastrukturave kritike te informacionit dhe listës së infrastrukturave të rëndësishme të informacionit".

Autoriteti ka të miratuara procedurat për zvogëlimin dhe menaxhimin e rreziqeve në hapësirën kibernetike duke përfshirë dhe rregulloren mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë, Versioni 2.0, të miratuar me urdhrin nr.10, datë 14.02.2022. Gjithashtu, procedurat, politikat dhe planet për mbrojtjen e hapësirës kibernetike nga incidentet kibernetike janë hartuar dhe miratuar dhe në këtë kuadër Plani i Veprimit i Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025 është në proces rishikimi që nga muaji tetor 2022.

Më datë 9.12.2022 , u miratua Akti Normativ nr.18, “Për disa ndryshime dhe shtesa në ligjin nr. 9880, datë 25.2.2008, “Për nënshkrimin elektronik”, i ndryshuar, i cili solli ndryshime të tilla për të bërë të mundur ndryshimet e nevojshme në strukturën e institucionit bazuar në veprimtarinë funksionale dhe plotësimin e nevojave për staf të kualifikuar në një kohë më të shkurtër.

AKCESK është institucioni koordinues në Republikën e Shqipërisë, i cili kryen organizimin dhe ndërveprimin me institucionet kombëtare të sigurisë dhe mbrojtjes në vend, për të marrë pjesë në ushtrimin kibernetik Cyber Coalition të NATO-s. Cyber Coalition është stërvitja kryesore vjetore e NATO-s për mbrojtjen kibernetike. Cyber Coalition, i cili mbahet çdo vit që nga viti 2008, bashkon një koalicion kibernetik të organeve të NATO-s, aleatëve dhe partnerëve të NATO-s për të forcuar aftësinë e Aleancës për të penguar dhe për t’u mbrojtur ndaj kërcënimeve në, dhe përmes hapësirës kibernetike në mbështetje të detyrave kryesore të NATO-s. Stërvitja e Cyber Coalition kryhet përmes Qendrës së Stërvitjes dhe Ushtrimeve të Sigurisë Kibernetike të Estonisë, ose 'CR14'. Pjesëmarrësit e trajnimit dhe trajnerët lokalë bëhen pjesë nga shtetet dhe subjektet e tyre përkatëse përmes rrjeteve virtuale dhe një grup pjesëmarrësish mblidhet në Estoni për të realizuar ushtrim të koordinuar.

AKCESK ka ngritur një Sistem Raportimi Incidentesh Kibernetike. Ky sistem shërben, jo vetëm për raportimin e ngjarjeve të incidenteve të sigurisë nga Operatorët e Infrastrukturave të Rëndësishme të Informacionit (OIRI) dhe në Operatorët e Infrastrukturave Kritike të Informacionit (OIKI), por edhe për raportim dhe informim nga AKCESK të vulnerabiliteteve apo sulmeve te mundshme, së bashku me rekomandimet përkatëse për parandalimin e tyre. Ky sistem është aktualisht në procesimi përmirësimi.

Aktualisht raportimi i incidenteve nga OIRI dhe OIKI ka pësuar rritje duke konsideruar rritjen e numrit të sulmeve kibernetike dhe të ndërgjegjësimit mbi nevojën e raportimit të incidenteve për një koordinim më të mirë në nivel kombëtar.

AKCESK ka bashkëpunuar me partnerë ndërkombëtarë si: EATM CERT, CISA, Qendra Lituaneze e Mbrojtjes Kibernetike, Shadowserver, Arctic-Hub, Bitsight, dhe janë prodhuar dhe publikuar rekomandime si dhe vulnerabilitete të evidentuara të sistemeve TIK.

Këto raporte përditësimi u janë dërguar OIKI dhe OIRI me anë të Sistemit të Monitorimit dhe Menaxhimit të Incidenteve dhe nëpërmjet e-mailit zyrtar të institucionit për ata operatorë të cilët kanë hasur problem në aksesimin e sistemit.

AKCESK, në cilësinë e insitucionit përgjegjës për implementimin e nën-objektivit mbi analizimin e infrastrukturave kritike dhe të rëndësishme të informacionit realizon vlerësimin e menaxhimin e riskut në to. Procedura që ndiqet për zvogëlimin dhe menaxhimin e risqeve është dërgimi tek të gjithë infrastrukturat kritike dhe të rëndësishme të informacionit, i një pyetësori i cili është i afishuar dhe në faqen zyrtare të Autoritetit.

Në kuadër të mbrojtjes së hapësirës kibernetike dhe rritjes së nivelit të sigurisë kibernetike në infrastrukturat kritike, AKCESK në zbatim të ligjit nr. 2/2017 “Për Sigurinë Kibernetike”, ka miratuar “Rregulloren mbi përmbajtjen dhe mënyrën e dokumentimit të masave të sigurisë”, të detyrueshme për t’u implementuar nga infrastrukturat kritike dhe të rëndësishme të informacionit në Republikën e Shqipërisë, me urdhrin nr. 10, datë 14.02.2022. Gjithashtu është miratuar edhe Metodologjia për Identifikimin dhe Klasifikimin e Infrastrukturave Kritike dhe Infrastrukturave të Rëndësishme të Informacionit”, miratuar me urdhër të Drejtorit të Përgjithshëm nr.9, datë 14.02.2022.

AKCESK kryen raporte për nivelin e maturimit të sigurisë kibernetike bazuar në deklarimet në pyetësorin e vetë-vlerësimit nga infrastrukturat kritike dhe të rëndësishme të informacionit. Në kuadër të vlerësimit të nivelit të sigurisë kibernetike në infrastukturat kritike dhe të rëndësishme të informacionit, AKCESK në përmbushje të detyrave funksionale kryen kontrolle të infrastrukturave kritike dhe të rëndësishme të informacionit në lidhje me implementimin e masave minimale të sigurisë së informacionit. Kontrollet e infrastrukturave kritike dhe të rëndësishme të informacionit kryhen nëpërmjet metodës së vetë-deklarimit dhe metodës në vend (onsite).

Për më tepër, Autoriteti ka organizuar aktivitete dhe trajnime me ekipet përgjegjëse pranë operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit në kuadër të veprimtarisë së Autoritetit për zhvillimin dhe rritjen e kapaciteteve vlerësuese dhe monitoruese të CSIRT-eve sektoriale.

AKCESK organizoi trajnimin e thelluar për "Menaxhimin e incidentit kibernetik", dy ditë rradhazi në datat 22-23 Dhjetor 2022, me të gjitha Infrastrukturat Kritike të Informacionit të ndara sipas sektorëve, në përmbushje të objektivave të Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025. Qëllimi i trajnimit ishte rritja e kapaciteteve profesionale të nevojshme për operatorët e infrastrukturave kritike në Shqipëri, si një ndër synimet kryesore të Autoritetit. Gjithashtu, u organizuan stërvitje kibernetike me skenarë të ndryshëm mbështetur në praktikat më të mira.

Në datën 21 Dhjetor 2022, Drejtori i Përgjithshëm i AKCESK, njëkohësisht Koordinatori Kombëtar për Sigurinë Kibernetike, zhvilloi takimin me temë “Siguria e informacionit financiar, prioritet aktual i AKCESK”, me pjesëmarrës drejtuesit më të lartë të sigurisë në sektorët bankar dhe financiar. Qëllimi i takimit ishte adresimi i nevojës së aplikimit të masave shtesë të sigurisë për mbrojtjen dhe sigurimin e informacionit financiar të qytetarëve, si fokus i qeverisë shqiptare dhe prioritet aktual i AKCESK.

Drejtori i përgjithshëm i AKCESK, në vijim të takimeve me qëllim rritjen e nivelit të sigurisë dhe bashkëpunimit, zhvilloi në datën 7 dhjetor 2022, një takim me “sektorin shëndetësor, mikrofinancat dhe kompanitë e sigurimeve”. Qëllimi i këtij takimi ishte analiza e situatës aktuale të sigurisë kibernetike si dhe krijimi i mundësive për forcimin e bashkëpunimit, për rritjen e sigurisë në infrastrukturat kritike, në kuadër të implementimit të strategjisë dhe vizionit të ri për sigurinë kibernetike.

Në kuadër të zhvillimeve aktuale në fushën e sigurisë kibernetike, AKCESK më datë 23 nëntor 2022, zhvilloi takimin me temë "Siguria kibernetike në sektorin bankar". Në këtë takim morën pjesë drejtuesit më të lartë të sigurisë në sektorin bankar.

Në datën 16 Nëntor 2022, u realizua **t**akimi me përfaqësues të lartë nga institucionet e mbrojtjes dhe sigurisë në vend. Qëllimi i këtij takimi ishte rritja e ndërveprimit institucional në funksion të rritjes së nivelit të sigurisë kibernetike në vend.

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike ka kryer ushtrime kibernetike në vazhdimësi në nivel kombëtar gjatë vitit 2022.

AKCESK në bashkëpunim me Geneva Centre for Security Governance (DCAF), OSBE, Regional Cooperation Council (RCC), Dhomën Amerikane të Tregtisë në Shqipëri, Shoqatën Shqiptare të Mikrofinancës, dhe One Telecommunications organizuan në datat 19-21 Prill 2022, workshop-in inovativ "Regional Cyber Camp Albania". Qëllimi i këtij workshop-i tre ditor, ishte zhvillimi i aftësive praktike për bashkëpunim dhe shkëmbim informacioni midis CSIRT-ve, Policisë së Shtetit dhe institucioneve të tjera rajonale përgjegjëse për sigurinë kibernetike, si dhe rritja e kapaciteteteve të të rinjve mbi sigurinë kibernetike. Përgjatë 3 ditëve të workshop-it, rreth 100 të rinj dhe 50 profesionistë nga Shqipëria, Kosova, Serbia, Bosnja dhe Hercegovina, Maqedonia e Veriut dhe Mali i Zi, thelluan njohuritë e tyre dhe shkëmbyen praktikat më të mira kombëtare në fushën e sigurisë kibernetike.

Gjithashtu, AKCESK ka marrë pjesë në workshop-in "CRDF Global Cross Cyber Drill" në datat 7-8 Korrik 2022", si dhe në aktivitetin online të NATO-s për rritjen e kapaciteteve mbi platformën MISP.

Autoriteti Kombëtar për Sigurinë e Informacionit të Klasifikuar (AKSIK)

Drejtoria e Sigurimit të Informacionit të Klasifikuar (DSIK), ka ndryshuar emërtimin bazuar në nenin 63 të Ligjit Nr.10/2023, datë 02.02.2023 "Për Informacionin e Klasifikuar", duke u emërtuar tashmë si Autoriteti Kombëtar për Sigurinë e Informacionit të Klasifikuar (AKSIK).

AKSIK, i quajtur DSIK përgjatë vitit 2022, për zhvillimin e mbrojtjes në fushën e krimit kibernetik pranë strukturës së tyre ka rekrutuar një punonjës të ri që në vitin 2021, i cili vazhdon të jetë i angazhuar në sistemet ku trajtohet informacioni i klasifikuar "sekret shtetëror" mbështetur në VKM nr.542 datë 25.07.2019 "Për miratimin e rregullores "Për sigurimin e informacionit të klasifikuar që trajtohet në sistemet e komunikimit dhe të informacionit (SKI)". Në kuadrin e plotësimit të strukturës së Mbrojtjes Kibernetike të ngritur në AKSIK, gjatë vitit 2022 procedura për plotësimin e vendeve vakante në këtë sektor është publikuar dy herë në faqen zyrtare të Departamentit të Administratës Publike dhe nuk ka pasur kandidatë të interesuar. AKSIK, me

qëllim tërheqjen e kandidatëve ekspert në këto pozicione, ka rritur pagat me një shtesë për natyrë të veçantë pune. Procedura është hedhur përsëri në dhjetor 2022.

AKSIK ka organizuar me homologët e saj të Spanjës dhe Italisë takime pune për marrjen e eksperiencave më të mira lidhur me procedurat e testimit, vlerësimit të sistemeve të klasifikuara "Sekret shtetëror" si dhe politikat e mbrojtjes kibernetike të zhvilluara nga këto vende. Personeli i AKSIK ka marrë pjesë në trajnimin e organizuar nga AKCESK, ofruar nga Cyber Diplomacy Academy.

Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI)

AKSHI në kuadër të Politikës 1 të Strategjisë Kombëtare për Sigurinë Kibernetike ka arritur rezultatet si më poshtë:

- Optimizimi dhe zgjerimi i infrastrukturave të sigurisë dhe procedurat për funksionimin e CSIRT qeveritar.

Përtej planizimit dhe angazhimeve të marra në Strategjinë Kombëtare të Sigurisë Kibernetike, sulmi kibernetik përshpejtoi tranzicionin e unifikimit drejt zgjidhjeve të sigurisë së Microsoft duke zgjeruar infrastrukturën e sigurisë. Këto zgjidhje iu shtuan atyre aktuale si Rapid7, Imperva, Bitsight etj.

Qendra Operacionale e Sigurisë e AKSHI-it, tashmë e ngritur dhe funksionale, kryen monitorimin 24/7 të hapësirës kibernetike qeveritare dhe Sektori i Reagimit ndaj Incidenteve të Sigurisë trajton incidentet nëpërmjet mjeteve të Microsoft.

Tranzicioni ka përfunduar duke ofruar vizibilitet të plotë mbi infrastrukturën, monitorim dhe kontroll të të gjithë aktiviteteve të dyshimta ose keqdashëse dhe një panoramë të qartë mbi korrelimin e gjurmëve të aktorëve kërcënues që mund të jenë prezent ose tentojnë të fitojnë akses në hapësirën kibernetike qeveritare.

Disa nga mjetet që përdoren dhe kanë zgjeruar infrastrukturat e sigurisë janë:

- Microsoft Sentinel - zgjidhje SIEM, korrelon të gjithë aktivitetet që gjenerohen nga loget e integruara dhe i analizon nëpërmjet inteligjencës artificiale dhe machine learning.
- Microsoft Defender for Endpoint - zgjidhje EDR/XDR, detekton, parandalon dhe trajton të gjithë incidentet.
- Microsoft Defender for Identity - Zgjidhje e cila analizon sjelljen e përdoruesve duke evidentuar anomalitë që mund të paraqesin.

- Përmirësim i strukturave hardware dhe ngritja e sistemit të kontrollit të aksesit

Përmirësimi i strukturave hardware është realizuar duke zëvendësuar pajisjet firewall hardware ekzistuese me pajisje të gjeneratës së re dhe parametra teknik më të lartë, si dhe ngritja e sistemit të kontrollit falë implementimit të zgjidhjes për akses remote me MFA në GOV-NET.

- Realizimi i hulumtimeve për forcimin e prioriteve kombëtare si një bazë për zhvillimin e sigurisë kibernetike dhe analizimi i kapaciteteve aktuale të autoriteteve.

Niveli i sulmit kibernetik dhe i aktorëve kërcënues, të cilët tentuan fshirjen e sistemeve dhe infrastrukturave qeveritare e-GOV, tregoi qartë që tashmë, sfidat e hapësirës kibernetike shqiptare nuk janë vetëm në nivel rajonal, por edhe në atë global.

Analiza të kapaciteteve aktuale, identifikimi i boshllëqeve dhe realizimi i hulumtimeve për forcimin e prioriteteve kombëtare të sigurisë kibernetike u kryen nga partnerë të ndryshëm të cilët ndihmuan në hetimin dhe rikuperimin nga sulmi kibernetik.

Krijimi i një sistemi të mbrojtjes kibernetike përfshin: përgjigje ndaj kërcënimit dhe zvogëlim të dëmit (threat response and mitigation), qendrën e testimit për programet keqdashëse (test center of malicious programs), trajnim të stafit dhe monitorim të informacioneve sensitive.

Stafi i Drejtorisë së Monitorimit dhe Mbrojtjes Kibernetike për Sistemet dhe Infrastrukturat e-GOV ka qenë dhe janë në trajnim të vazhdueshëm nga ekipet e Microsoft. Suporti i tyre konsiston në analizimin e riskut, zvogëlimin e vulnerabiliteteve dhe reagimin ndaj kërcënimeve të identifikuara.

Sistemi “honeypot” për të tërhequr vëmendjen nga objektivi real i sulmeve të ndryshme është implementuar duke përdorur zgjidhjen Rapid7 dhe testimet për programet keqdashëse kryhen në konsolën e Microsoft Defender for Endpoint.

Monitorimi i informacioneve sensitive në Dark Web realizohet nga Sektori i Reagimint ndaj Incidenteve, të cilët nëpërmjet indikatorëve dhe gjurmëve të aktorëve kërcënues që evidentojnë, analizojnë nëse ka prezencë të tyre në rrjetin qeveritar.

Qendra për Koordinimin Kundër Ekstremizmit të Dhunshëm (QKEDH)

QKEDH është institucioni përgjegjës për implementimin e nën-objektivit mbi monitorimin dhe parandalimin e fenomeneve, që nxisin ekstremizmin e dhunshëm dhe radikalizimin në shtresat vulnerabël në hapësirën kibernetike.

Në kuadër të përmbushjes së objektivave të strategjisë, QKEDH ka organizuar fushata sensibilizuese në shkolla dhe me qasje në komunitet kundër radikalizimit dhe ekstremizmit të dhunshëm online. QKEDH ka koordinuar projektin “Mbështetja e QKEDH në përhapjen e komunikimit strategjik për parandalimin dhe kundërshtimin e ekstremizmit të dhunshëm nëpërmjet ngritjes së kapaciteteve dhe hulumtimit” në bashkëpunim me organizatën “Qendra për

Studimin e Demokracisë dhe Qeverisjes" (CSDG Albania) dhe me mbështetjen e Ambasadës së SHBA-ve në Shqipëri, ka zhvilluar tre trajnime. Në zbatim të këtij projekti në bashkëpunim me përfaqësues të Drejtorisë së Përgjithshme të Burgjeve, Ministrisë së Arsimit dhe Sportit (MAS) dhe Ministrisë së Shëndetësisë dhe Mbrojtjes Sociale (MSHMS), janë zhvilluar workshop-e për ngritjen e kapaciteteve të punonjësve të ministrive të cilët kanë në fushë veprmimi parandalimin e ekstremizmit të dhunshëm dhe komunikimin strategjik.

Po në kuadër të këtij projekti, QKEDH ka koordinuar punën me organizatën CSDG Albania për zhvillimin e trajnimit për personelin kyç të institucioneve që janë të përfshira në proceset e ri-integrimit të shtetasve të riatdhesuar nga vendet e konfliktit me fokus parandalimin e ekstremizmit të dhunshëm dhe komunikimin strategjik.

QKEDH dhe CSDG Albania bashkë-organizuan një workshop në kuadër të projektit "Forcimi i bashkëpunimit ndër-institucional dhe mekanizmave të komunikimit strategjik në funksion të parandalimit/luftës kundër ekstremizmit të dhunshëm". Në këtë workshop morën pjesë përfaqësues nga Ministria Brendshme dhe Ministria e Drejtësisë, si dhe mësues, psikologë dhe punonjës socialë. Nëpërmjet këtij workshopi, punonjësit e vijës së parë janë pajisur me njohuritë e duhura për identifikimin e shenjave të hershme të radikalizmit që çon në ekstremizëm të dhunshëm, duke rritur sensibilizimin për luftimin e këtij fenomeni.

Gjatë vitit 2022, Radio Televizioni Publik Shqiptar (RTSH), me koordinimin dhe bashkëpunimin e QKEDH, transmetoi Episodet 4, 5, 6, 7, 8 dhe 9 të ciklit të reportazheve që ka realizuar Qendra Media Aktive, mbi evidentimin e bashkëpunimit kundër fenomenit të ekstremizmit të dhunshëm ndërmjet institucioneve të shtetit shqiptar, shoqërisë civile dhe komuniteteve fetare.

Po gjatë vitit 2022, QKEDH koordinoi dhe realizoi dy intervista me individë të rikthyer nga zonat e konfliktit, të cilët po ndjekin programe rehabilituese/ri-integruese në komunitet, të mbështetura nga QKEDH-ja. QKEDH dha kontributin e saj nëpërmjet një intervistë në emisionin "Auditor Arsimi" në Radio Televizionin Shqiptar (RTSH), ku u përcoll informacioni mbi ndërhyrjet e realizuara përgjatë këtyre viteve nga QKEDH në bashkëpunim me Ministrinë e Arsimit dhe Sportit (MAS) në sistemin parauniversitar dhe universitar për identifikimin, parandalimin dhe kundërshtimin e ekstremizmit të dhunshëm si dhe lidhur me ri-integrimin e fëmijëve të rikthyer nga zonat e konfliktit në shkollë dhe komunitet.

Gjatë muajit tetor, QKEDH dha kontributin e saj nëpërmjet një interviste në emisionin "31 Minuta - Jeta pas ferrit në Al Haul" në televizionin A2CNN, gjatë së cilit u diskutua mbi planet e qeverisë për procesin e ri-integrimit të nënave dhe fëmijëve të rikthyer nga zonat e konfliktit në shkollë dhe komunitet.

QKEDH ka kontribuar në trajnimet e organizuara nga IDM gjatë vitit 2022 në shkolla të arsimit para universitar me tema si: Interneti i Sigurt, Bullizmi Kibernetik, Siguria në Internet, Ana Tjetër e Internetit, dhe Dita e Internetit të Sigurt. Lufta kundër ekstremizmit të dhunshëm dhe radikalizmit në hapësirën online dhe komunitet duke nxitur shkëmbimin e informacionit dhe bashkëpunimin ndërmjet institucioneve partnere mbetet fokusi kryesor i QKEDH-së.

Policia e Shtetit

Policia e Shtetit ka punuar për fuqizimin dhe implementimin e masave të sigurisë në infrastrukturat kritike dhe të rëndësishme të informacionit, si dhe forcimin e kapaciteteve për hetimin e krimit kibernetik, duke ndërmarrë disa iniciativa në kuadër të zbatimit të Strategjisë Kombëtare për Sigurinë Kibernetike.

Me qëllim forcimin e kapaciteteve, në funksion të rritjes së parametrave të sigurisë, DTI ka përcjellë pranë AKSHIT si autoriteti që do të negociojë marrëveshjen në nivel kombëtar me Microsoft disa kërkesa për implementimin e sistemeve si: Microsoft Intune dhe Microsoft Sentinel. Për vitin 2023 janë parashikuar investime nga buxheti i shtetit për projektet në kuadër të forcimit të kapaciteteve të sigurisë së rrjetit ku përmendim projektet:

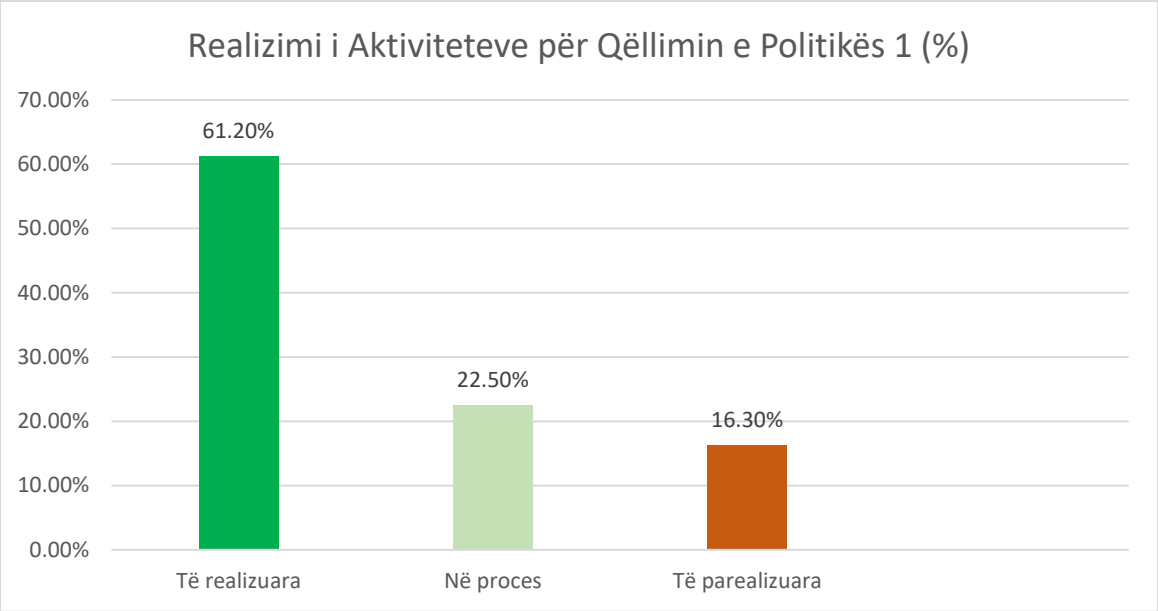
- Rritja e sigurisë kibernetike në infrastrukturën e Policisë dhe

- Auditimi i sistemeve informatike për sigurinë.

Po ashtu, është punuar për projektin “Ngritja e infrastrukturës DRC për sistemet e Policisë së Shtetit” me angazhim financiar 2 vjeçar, (2023- 2024).

Realizimi i Aktiviteteve për Qëllimin e Politikës 1

Për Qëllimin e Politikës 1, rezulton se deri në vitin 2022, shkalla e realizimit të aktiviteteve është: aktivitete të realizuara 61.2% (30 aktivitete), aktivitete në proces 22.5% (11 aktivitete) dhe aktivitete të parealizuara 16.3% (8 aktivitete).



Qëllimi i politikës 2. Ndërtimi i një mjedisi të sigurt kibernetik duke edukuar dhe ndërgjegjësuar shoqërinë në ngritjen e kapaciteteve profesionale në fushën e sigurisë së informacionit.

Objektivat e prioritetit fokusohen në:

- Rritja e kapaciteteve profesionale në fushën e sigurisë së informacionit nëpërmjet rishikimit të kurrikulave arsimore.
- Rritja e ndërgjegjësimit dhe aftësive profesionale të institucioneve publike dhe private për sigurinë kibernetike
- Rritje e ndërgjegjësimit të shoqërisë, për sigurinë kibernetike dhe për kërcënimet kibernetike.

Për realizimin e objektivave të Qëllimit të Politikës 2, institucionet e përfshira në realizimin e Planit të Veprimit raportojnë si më poshtë vijon:

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK)

Për të rritur ndërgjegjësimin në grupmosha të ndryshme të shoqërisë për përdorimin e internetit të sigurt dhe infrastrukturës digjitale, AKCESK ka kyer trajnime periodike për thellimin e njohurive në sigurinë kibernetike, bazuar në zhvilimet e reja të fushës, për stafin administrativ në nivel qendror dhe në nivel lokal.

AKCESK ka organizuar gjithashtu stërvitje kibernetike me qëllim rritjen e kapaciteteve të CSIRT-eve në nivel kombëtar dhe në nivel ekzekutiv të administratës publike të tilla si " Regional Cyber

Camp Albania" i mbajtur në Prill 2022. Ky aktivitet mundësoi zhvillimin e aftësive praktike të punonjësve të administratës publike që morën pjesë si, Policia e Shtetit, Ministria e Arsimit, Ministria e Mbrojtjes, Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale, AKEP etj. Ky aktivitet u organizua nga AKCESK në bashkëpunim me Qendrën e Gjenevës për Qeverisjen e Sektorit të Sigurisë (Geneva Centre for Security Sector Governance-DCAF), Organizatën për Siguri dhe Bashkëpunim në Evropë (OSBE), Këshillin e Bashkëpunimit Rajonal (Regional Cooperation Council-RCC), Dhomën Amerikane të Tregtisë në Shqipëri, Shoqatën Shqiptare të Mikrofinancës, dhe kompaninë One Telecommunications në datat 19-21 Prill 2022.

AKCESK në kuadër të rritjes së kapaciteteve ka organizuar trajnim dy ditor për thellimin e njohurive në sigurinë kibernetike në datat 22-23 Dhjetor 2022, me të gjitha infrastrukturat kritike të informacionit të ndara sipas sektorëve ku janë përfshirë edhe punonjës nga sektori publik në nivel qendror. Ky aktivitet përmbush disa objektiva të strategjisë në fushën e sigurisë kibernetike. Për të rritur kapacitetet e nivelit ekzekutiv të administratës publike dhe jo vetëm, gjatë këtij trajnimi u zhvilluan stërvitje kibernetike për pjesëmarrësit.

Autoriteti ka punuar për rritjen e ndërgjegjësimit të shoqërisë për sigurinë kibernetike, duke përdorur hapësirat e duhura për realizimin e tyre, përfshirë edhe mediat audiovizive dhe mediat sociale. Në këtë linjë, janë hartuar materiale ndërgjegjësuese dhe organizuar fushata ndërgjegjësimi.

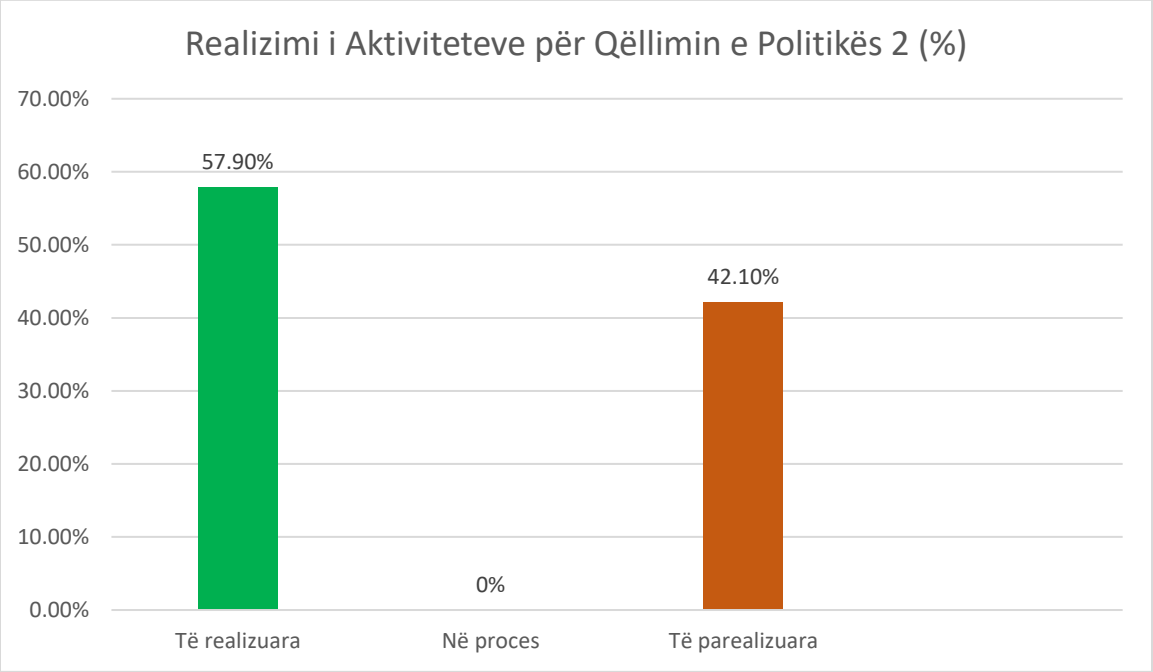
Në kuadër të implementimit të Planit të Veprimit të Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025, AKCESK ka vijuar organizimin e fushatave të ndërgjegjësimit online dhe fizikisht, me pjesëmarrës nga institucione publike e private, prindër, mësues, të rinj dhe fëmijë në qarqe të ndryshme të Shqipërisë. Gjithashtu, çdo muaj publikohet buletini i sigurisë kibernetike me lajme dhe eventet kryesore të organizuara ose zhvilluara nga Autoriteti.

Në Shtator të vitit 2021, AKCESK u angazhua për t'u bërë vendi i parë pilot në botë për Projektin Global ITU[2]. Projekti është planifikuar të zgjasë deri në Mars të vitit 2023. Në këtë kuadër, është krijuar edhe një platformë edukative online për sigurinë kibernetike, për të rritur ndërgjegjësimin në grupmosha të ndryshme të shoqërisë, për përdorimin e internetit të sigurt dhe të infrastrukturës digjitale. Në këtë faqe gjenden të publikuara iniciativat e përbashkëta në të gjithë sektorët përkatës për të garantuar sigurinë digjitale në mjedisin online për fëmijët dhe të rinjtë në Shqipëri, si dhe një sërë aktivitetesh të zhvilluara dhe të zbatuara në kuadër të Projektit Global, me synimin për të vepruar si një kornizë referimi për vendet e tjera të Rajonit të Evropës, të cilat do të ishin të interesuara për t'u bërë një vend përfitues për zbatimin e Mbrojtjes së Fëmijëve Online (COP) të financuar nga Projekti Global.

[2] https://cesk.gov.al/aktivitete/itu/ITU_Pilot_Project.html

Realizimi i Aktiviteteve për Qëllimin e Politikës 2

Për Qëllimin e Politikës 2, rezulton se deri në vitin 2022, shkalla e realizimit të aktiviteteve është: aktivitete të realizuara 57.9% (11 aktivitete), dhe aktiviteteve të parealizuara 42.1% (8 aktivitete).



Qëllimi i politikës 3. Krijimi i mekanizmave të nevojshëm për sigurinë e fëmijëve në hapësirën kibernetike, duke përgatitur njëkohësisht brezin e ri të aftë për të përfituar nga përparësitë e teknologjisë së informacionit dhe për të përballuar sfidat e zhvillimit

Objektivat e prioritetit fokusohen në:

- Forcimi i kuadrit ligjor për rritjen e sigurisë së fëmijëve në internet.
- Parandalimi i abuzimit seksual të fëmijëve në internet nëpërmjet rritjes së ndërgjëgjësimit dhe krijimit të hapësirave të sigurta për lundrimin në internet.
- Hetimi efektiv dhe sjellja para drejtësisë e autorëve të krimeve kibernetike ndaj fëmijëve, me fokus abuzimin dhe shfrytëzimin seksual.
- Rritja e ndërgjegjësimit dhe edukimi tek të gjitha segmentet e shoqërisë për përdorimin e sigurtë të internetit nga fëmijët
- Forcimi i bashkëpunimit ndërsektorial për mbrojtjen e fëmijëve në internet.

Për realizimin e objektivave të Qëllimit të Politikës 3, institucionet e përfshira në realizimin e Planit të Veprimit raportojnë si më poshtë vijon:

Ministria e Arsimit dhe Sportit (MAS)

Ministria e Arsimit dhe Sportit (MAS) ka punuar për forcimin e kuadrit ligjor për rritjen e sigurisë së fëmijëve në internet, sidomos përsa i përket bullizmit dhe abuzimit online, dhe mbrojtjes së fëmijëve nga përmbajtjet e dëmshme.

Me synim mbrojtjen e fëmijëve online, janë zhvilluar edhe pyetësorë nga ana e shërbimit psiko-social në lidhje me përceptimin e bullizmit dhe dhunës në shkollë nga nxënësit, si dhe janë shpërndarë materiale informuese te nxënësit për abuzimin online dhe bullizmin në shkolla.

Një rëndësi të veçantë ka njohja e nxënësve me temën e krimit kibernetik dhe pasojat e saj, si dhe mënyrat për identifikimin e rreziqeve kibernetike. Në kuadër të Ditës Ndërkombëtare të Sigurisë në internet janë zhvilluar video-mesazhe sensibilizuese nga senatet e shkollave të cilat janë shpërndarë në faqet zyrtare të tyre, si dhe aktivitete ndërgjegjësuese dhe ekspozita me piktura dhe postera sensibilizuese. MAS ka realizuar gjithashtu aktivitete në shkolla mbi temën "Përdorimi i internetit në mënyrë të sigurt" me qëllim njohjen me pasojat e dhënies së fjalëkalimeve të adresave të tyre personave të tretë, si dhe me format e ndryshme të dhunës emocionale, psikologjike, kibernetike dhe seksuale.

Përgjatë vitit 2022, ka vijuar trajnimi i drejtuesve të rrjetit TIK dhe anëtarëve të rrjetit. Gjatë kësaj periudhe është realizuar trajnimi i mësueseve të TIK-ut lidhur me tematika të ndryshme mbi punën dhe organizimin e rrjeteve profesionale, përfshirë këtu përdorimin e TIK-ut në zbatimin e kurrikulës dhe vlerësimin e nxënësit. Gjithashtu, kanë vijuar trajnimet të cilat synojnë zhvillimin profesional të mësuesve të TIK-ut për përdorimin platformave online në mënyrë të sigurt dhe eficente në procesin mësimor. Në kuadër të zbatimit të projektit të bashkëpunimit midis Agjencisë së Sigurimit të Cilësisë së Arsimit Parauniversitar dhe Institutit Shqiptar të Medias janë trajnuar rreth 250 mësues të ciklit të Arsimit të Mesëm të Ulët (AMU) dhe Arsimit të Mesëm të Lartë (AML), në lidhje me edukimin për median dhe informimin. Përveç njohurive të marra rreth botës së medias dhe informimit, janë diskutuar çështje të rëndësishme të cilat lidhen me sfidat dhe rreziqet në botën virtuale. Mësuesit janë njohur me kodet e sjelljes, rregullat e privatësisë dhe disa nga rreziqet kryesore që mund të hasen gjatë përdorimit të internetit. Janë inkurajuar mësuesit të përdorin metodat dhe mjetet bazë mësimore për të ndihmuar nxënësit të përdorin internetin në mënyrë të përgjegjshme dhe të sigurt, dhe t'i bëjnë ata të vetëdijshëm për sfidat dhe rreziqet që vijnë nga përdorimi i tij. Janë krijuar grupet e komunikimit në platforma të ndryshme ku minimalisht një herë në muaj organizohen takime të drejtpërdrejta ose online, ku mësuesit diskutojnë, ndajnë eksperincën dhe vlerësojnë nevojat.

Shërbimi psiko-social dhe drejtoritë e shkollave kanë realizuar seanca informuese për njohjen dhe publikimin e rubrikës "Raporto përmbajtje të paligjshme", e cila është e ndërlidhur me portalin

online të AKCESK[3], për mbylljen e aksesit të faqeve të intemetit me përmbajtje të paligjshme, që u vjen në ndihmë fëmijëve, personave që ushtrojnë përgjegjësinë prindërore dhe të rinjve për të raportuar përmbajtje të paligjshme të hasura gjatë lundrimit në internet.

MAS kryen monitorimin e aplikimit të metodologjisë së hartuar me veprimtari praktike me nxënësit e klasave V-IX dhe X-XII, për masat mbrojtëse dhe sigurinë kibernetike. Nëpër shkolla janë zhvilluar gjithashtu edhe veprimtari praktike me nxënësit për masat mbrojtëse dhe sigurinë kibernetike. Këto veprimtari përfshijnë diskutim përvojash me stafin dhe grupe nxënësish, krijimin e posterave dhe eseve nga vetë nxënësit për rreziqet kibernetike dhe sigurinë online, dhe implementimin e projekteve në këtë fushë në institucionet arsimore të AMU dhe AML, si dhe nga organizatat/shoqatat që kanë bashkëpunim me MAS.

Me qëllim identifikimin, mbështetjen dhe promovimin e talenteve për të krijuar zgjidhje teknike që ndihmojnë në mbrojtjen dhe sigurinë online, MAS ka zhvilluar konkurse, projekte me temë "Siguria në Internet", Olimpiadën Kombëtare në lëndën e TIK-ut me nxënësit e AML-së, dhe veprimtari të tjera ekstra për nxënësit që shfaqin prirje në TIK.

MAS në bashkëpunim me AKCESK kanë realizuar aplikimin e filtrave në shkollat publike dhe private për të parandaluar aksesin e fëmijëve në faqe të papërshtatshme dhe të paligjshme si dhe informimin në vijueshmëri të mësuesve të TIK për raportimin e incidenteve. Gjithashtu, është vendosur në funksion Rubrika “Raporto përmbajtje të paligjshme”, në faqen zyrtare të MAS, DPAP, DRAP-ve, ZVAP-eve dhe IAP-ve, e cila është ndërlidhur me portalin online www.cesk.gov.al të AKCESK, për mbylljen e aksesit të faqeve të internetit me përmbajtje të paligjshme, që u vjen në ndihmë fëmijëve, personave që ushtrojnë përgjegjësinë prindërore dhe të rinjve, për të raportuar përmbajtje të paligjshme të hasura gjatë lundrimit të tyre në internet.

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK)

AKCESK ka koordinuar dhe bashkërenduar punën për realizimin e aktiviteteve në kuadër të projektit të përbashkët me UNICEF Albania “Zhvillimi i mekanizmave të nevojshëm për sigurinë në internet të fëmijëve dhe të rinjve në Shqipëri” gjatë Shkurt – Shtator 2022.

Rezultatet e këtij projekti janë:

✓ Hartimi i 6 dokumentave në formën e protokollit ndërinstitucional, udhëzues, raport analizues
✓ Trajnuar 518 prindër dhe mësues në 12 njësi / qytete të Shqipërisë: Babrru, Vorë, Kavajë, Dibër, Klos, Kukës, Has, Laknas, Burrel, Bulqizë, Fushë Arrëz, Pukë, Vau Dejës, Shkodër, Tropojë, Kamëz dhe Paskuqan.

[3] www.cesk.gov.al

✓ Hartuar 1 manual ndërgjegjësimi për prindërit dhe mësuesit, me këshilla për mbrojtjen e fëmijëve në internet, me fokus trafikimin online.

Dokumentat e hartuar janë:

- Raport për analizimin dhe identifikimin e mekanizmave të raportimit të përmbajtjeve të paligjshme.
- Protokolli ndërinstitucional për bashkëpunimin midis agjencive ligjzbatuese, ofruesve të shërbimit të internetit dhe AKCESK.
- Raport për analizimin dhe identifikimin e hendekut ligjor të mbrojtjes së fëmijëve online nga abuzimi seksual, duke përfshirë rekomandimet e nevojshme.
- Raport për analizimin e funksionaliteteve teknike të Portalit për Bllokimin e Faqeve me Përmbajtje të Paligjshme, së bashku me rekomandimet për përmirësimin e funksionaliteteve me qëllim rritjen e eficiencës.
- Raport për analizimin e inciativave ekzistuese të Ofruesve të Shërbimit të Internetit për mbrojtjen e fëmijëve në internet.
- Udhëzim për integrimin e Internet Watch Foundation Hash List në shërbimet e Ofruesve të shërbimit të internetit.

Gjithashtu, AKCESK ka koordinuar dhe bashkërenduar punën për realizimin e aktiviteteve në kuadër të pilotimit të projektit global me Unionin Ndërkombëtar të Telekomunikacionit (ITU) "Krijimi i një mjedisi digjital të sigurt dhe fuqizues për fëmijët" për periudhën Janar-Dhjetor 2022.

Rezultatet e këtij projekti janë:

✓ Hartimi i 2 manualeve ndërgjegjësues:
  - Child-friendly manual – i dedikuar për mbrojtjen e fëmijëve në internet
  - Train of Trainers (ToT) Manual – i dedikuar për prindërit, për rritjen e sigurisë së fëmijëve në internet

✓ 37 trajnime për fëmijë e të rinj, prindër dhe mësues, përfaqësues të industrisë
  - 12 trajnime për fëmijë e të rinj
  - 15 trajnime për prindër dhe mësues
  - 10 trajnime për përfaqësues të industrisë

✓ 750 pjesëmarrës në trajnime
  - 190 fëmijë e të rinj
  - 460 prindër dhe mësues
  - 100 përfaqësues të industrisë

✓ 1 mesazh i unifikuar i publikuar në dyqanet fizike dhe mediat sociale të Ofruesve të Shërbimit të Internetit.

✓ 1 poster me këshilla nga Udhëzimet e ITU.

Në kuadër të implementimit të Planit të Veprimit të Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025, AKCESK ka vijuar organizimin e fushatave të ndërgjegjësimit online dhe fizikisht, me pjesëmarrës nga institucione publike e private, prindër, mësues dhe të rinj e fëmijë, në qarqe të ndryshme të Shqipërisë.

Trajnimet e realizuara kanë përfshirë edhe grupin e mëposhtëm:

- Njësitë e Mbrojtjes së Fëmijëve në qarkun e Tiranës, Dibrës, Shkodrës dhe Kukësit
- Ofruesit e Shërbimit të Internetit, të cilët operojnë në Republikën e Shqipërisë
- 4500 përdorues unik online në fushatën e ndërgjegjësimit online

Në kuadër të Muajit të Ndërgjegjësimit për Sigurinë Kibernetike, nga data 19 tetor deri më 2 nëntor 2022, AKCESK zhvilloi takime me fëmijë, prindër, mësues, psikologë dhe punonjës socialë në shkolla për të rritur ndërgjegjësimin e komunitetit për kërcënimet kibernetike. Sesionet informuese, të zhvilluara në Korçë, Pogradec, Shkodër Malësi e Madhe, Rrëshen dhe Lezhë synuan gjithashtu t'i ndihmonin të rinjtë të mbrohen online, ndërkohë që kërcënimet ndaj teknologjisë dhe të dhënave personale bëhen gjithnjë e më të zakonshme. AKCESK i organizoi këto sesione informuese në partneritet me Prezencën e OSBE-së në Shqipëri.

Gjatë vitit 2022, në zbatim të planit të komunikimit të sektorit, u krye realizimi dhe publikimi në rrjetet sociale të Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike i tre videove promovuese për ndërgjegjësimin e komunitetit për rritjen e nivelit të sigurisë kibernetike, të cilat kanë arritur më shumë se 6000 shikime në media sociale (videot e mëposhtme mund të aksesohen duke klikuar në linket përkatëse në youtube).

- Video "**Siguria e fëmijëve në internet"**
- Video "**Këshilla për prindërit dhe edukatorët për sigurinë e fëmijëve në internet"**
- Video "**Udhezime per industrine e mbrojtjes se femijeve ne Internet"**

Bazuar në analizën e situatës aktuale të TIK dhe sigurisë kibernetike janë publikuar periodikisht lajme dhe artikuj në kanalet zyrtare të komunikimit në media sociale të Autoritetit. Këtu mund të përmendim edhe publikimet "Buletini i Lajmeve të Sigurisë Kibernetike" nga muaji Janar 2022, çdo muaj, deri në muajin Dhjetor 2022.

Ministria e Shëndetësisë dhe Mbrojtjes Sociale (MSHMS)

MSHMS koordinon dhe monitoron Agjendën Kombëtare për të Drejtat e Fëmijëve 2021-2026 miratuar me VKM Nr. 659, datë 3.11.2021, dokument strategjik me natyrë ndërsektoriale që përfshin qëllime, objektiva dhe masa, të cilat kanë si qëllim angazhimin e të gjithë aktorëve publike dhe jopublikë për të ofruar në mënyrë efektive dhe të drejtë shërbime sa më cilësore për fëmijët. Njëkohësisht, kjo realizohet duke ndjekur parimet dhe standarde miqësore për ta, me qëllim

edukimin në funksion të mbrojtjes së fëmijëve online, duke garantuar kështu mirëqenien dhe një të ardhme më të mirë për fëmijët.

Në kuadër të mbrojtjes së fëmijëve nga të gjitha format e dhunës, si një nga shtyllat kryesore e kësaj Agjende, janë parashikuar objektiva që kanë të bëjnë me mekanizma dhe shërbime të specializuara dhe të integruara për adresimin e formave të rënda të dhunës, përfshirë abuzimin seksual dhe abuzimin dhe shfrytëzimin online. Një kapitull i veçantë është "Qëllimi strategjik për promovimin e të drejtave të fëmijëve në botën digjitale", që përfshin sigurimin e aksesit dhe përfshirjen e fëmijëve në mjedisin digjital në përputhje të plotë me objektivin 5 të Strategjisë së Bashkimit Evropian për të Drejtat e Fëmijëve. Nxënia dhe kreativiteti në mjedisin digjital nëpërmjet zhvillimit të kompetencave digjitale përmes TIK është parë si një qëllim prioritar dhe i rëndësishëm për fëmijët duke vlerësuar si të rëndësishme në këtë proces interesin më të lartë të fëmijës, nga të gjitha institucionet që kontribuojnë në mjedisin digjital.

Agjencia Shtetërore për të Drejtat dhe Mbrojtjen e Fëmijës (ASHDMF) monitoron dhe është në kontakt të përhershëm me strukturat e mbrojtjes së fëmijëve në të gjithë vendin, duke ofruar mbështetje teknike për menaxhimin e rasteve, duke koordinuar ndërhyrjet institucionale për marrjen në mbrojtje të çdo rasti të fëmijëve të dhunuar, të abuzuar apo neglizhuar, për të siguruar që fëmijët të marrin shërbimet e nevojshme dhe trajtim psikologjik të specializuar.

Pranë ASHDMF raportohen përmes Linjës së Këshillimit Alo116 111 dhe platformës isigurt.al raste të dhunës dhe abuzimit të fëmijëve në mediat sociale dhe faqeve web. Këto faqe raportohen më pas nga ASHDMF pranë portalit që administrohet nga Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK). Për vitin 2022 janë raportuar 6 faqe web me përmbajtje të papërshtatshme për fëmijën pranë portalit të AKCESK.

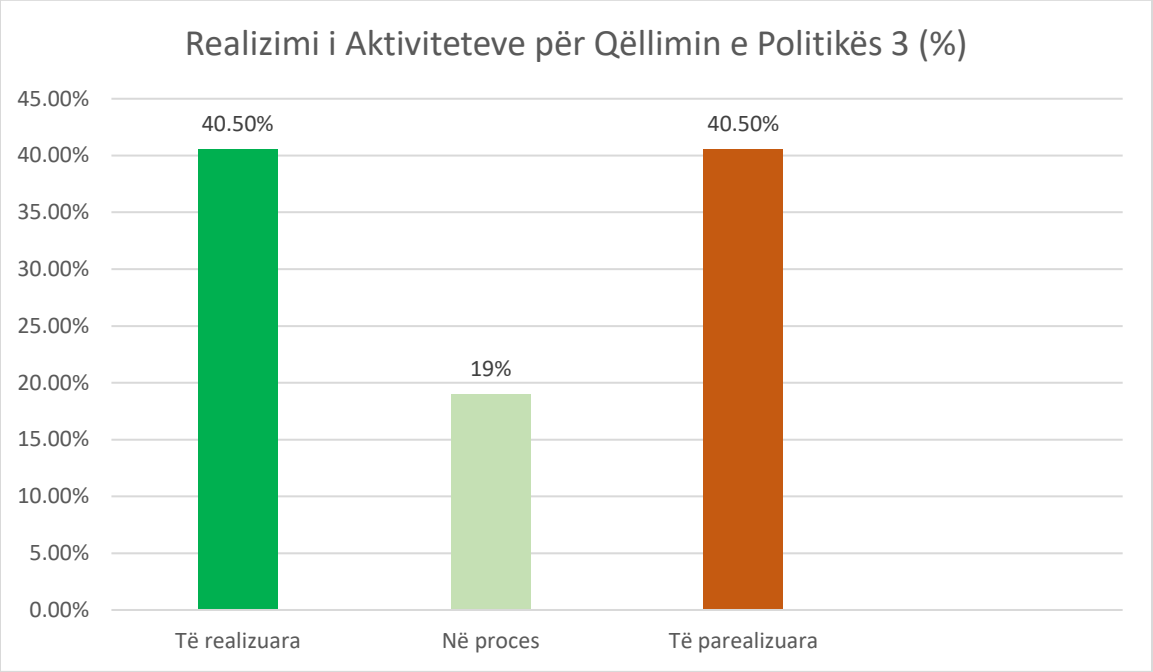
MSHMS mbështet Linjën Kombëtare të Këshillimit ALO 116 111, e cila ofron këshillim psikosocial për rastet e abuzimit apo bullizmit online, si dhe ka referuar raste pranë organeve përgjegjëse për trajtimin e tyre. Për rastet e trajtura në periudhën Janar-Dhjetor 2022, kemi një numër prej 28,812 telefonatash, ku përfshihen këtu raste të fëmijëve në nevojë për mbrojtje, ku nga këto, është dhënë këshillim për 1727 raste, si edhe janë referuar 439 raste pranë institucioneve publike për trajtim. Në lidhje me sigurinë online janë raportuar 50 raste.

MSHMS në bashkëpunim me AKCESK në kuadër të implementimit të aktiviteteve të Strategjisë Kombëtare të Sigurisë Kibernetike 2020-2025 dhe të Agjendës Kombëtare për të Drejtat e Fëmijëve 2021 -2026, ka realizuar trajnime lidhur me sigurinë e fëmijëve në mjedisin kibernetik. Aktualisht janë zhvilluar workshope me pjesëmarrjen e 31 punonjësve të mbrojtjes së fëmijëve dhe aktorëve të tjerë në nivel vendor në Bashkitë Tiranë, Kavajë, Kamëz, Vorë dhe Rrogozhinë.

Në muajin shkurt të çdo viti organizohen aktivitete sensibilizuese në kuadër të "Ditës së Internetit të Sigurt". Në këtë kuadër, në vitin 2022 u organizua një aktivitet sensibilizues me nxënës nga shkolla 9 vjeçare dhe të mesme, prindër dhe mësues, të ftuar tek Qendra COD në Kryeministri. Njëkohësisht, ASHDMF në bashkëpunim me punonjësit për mbrojtjen e fëmijëve ka organizuar takime sensibilizuese në kuadër të mbrojtjes së fëmijës në mjedisin digjital në shkolla të ndryshme në bashkitë Tiranë, Durrës, Bulqizë, Kukës, Fier dhe Burrel.

Realizimi i Aktiviteteve për Qëllimin e Politikës 3

Për Qëllimin e Politikës 3, rezulton se deri në vitin 2022, shkalla e realizimit të aktiviteteve është: aktivitete të realizuara 40.5% (17 aktivitete), aktivitete në process 19% (8 aktivitete) dhe aktivitete të parealizuara 40.5% (17 aktivitete).



Qëllimi i politikës 4. Rritja e bashkëpunimit kombëtar dhe ndërkombëtar në fushën e sigurisë kibernetike me partnerët strategjikë

Objektivat e prioritetit fokusohen në:

- Forcimi i bashkëpunimit institucional në nivel kombëtar
- Forcimi i bashkëpunimit ndërkombëtar në fushën e sigurisë dhe mbrojtjes kibernetike dhe luftës kundër ekstremizmit të dhunshëm dhe radikalizimit.

Për realizimin e objektivave të Qëllimit të Politikës 4, institucionet e përfshira në realizimin e Planit të Veprimit raportojnë si më poshtë vijon:

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK)

AKCESK në kuadër të rritjes, bashkëpunimit dhe koordinimit të punës së tij brenda dhe jashtë vendit me institucione kombëtare dhe ndërkombatare, për të garantuar një nivel sigurie më të lartë në nivel kombëtar në hapësirën kibernetike, ka hartuar dhe nënshkruar marrëveshje ndërinstitucionale, duke krijuar kështu një rrjet komunikimi dhe shkëmbimi informacioni me pikat e kontaktit. Marrëveshjet që mund të përmendim janë:

- Memorandum Mirëkuptimi me Autoritetin e Mediave Audiovizive
- Memorandum Mirëkuptimi me Institutin e Politikave në Siguri Kibernetike
- Memorandum Mirëkuptimi me 4iG (nënshkruar në janar 2023)
- Memorandum Mirëkuptimi me Raiffeisen Bank Albania
- Memorandum Mirëkuptimi me CERT-Rumani për t'u rinovuar (proces i filluar në 2022, për t'u firmosur në 2023)
- Memorandum Mirëkuptimi me Shoqatën e Bankave në Shqipëri (proces i filluar në 2022, firmosur në fillim 2023)
- Memorandum Mirëkuptimi me Drejtorinë Kombëtare Kibernetike të Izraelit (proces i filluar në 2022, firmosur në fillim 2023)
- Memorandum Mirëkuptimi me Këshillin e Sigurisë Kibernetike Emirateve Bashkuara Arabe (proces i filluar në 2022, për t'u firmosur në 2023)
- Memorandum Mirëkuptimi me CSIRT Itali (proces i filluar në 2022, për t'u firmosur në 2023)

Si ura komunikimi për bashkëpunimin dhe forcimin e besimit me infrastrukturat e informacionit publike dhe private dhe komunitetin akademik kanë shërbyer takimet dhe trajnimet në nivel kombëtar dhe rajonal. Ekspertët e fushës së sigurisë kibernetike kanë punuar për krijimin e bashkëpunimit dhe shkëmbimit të informacionit përmes pikave të kontaktit të dedikuara nga institucionet përkatëse, në rast të incidenteve të mundshme dhe kërcënimeve kibernetike.

Për kryer shkëmbimin e informacionit, njohurive dhe përvojës në sektorit publik, insitucioneve të mbrojtjes dhe sigurisë kibernetike dhe sektorit privat AKCESK ka ndërmmarë disa hapa në mënyrë që të sigurojë rrugë të sigurta komunikimi.

Një nga hapat që është ndërmarrë nga AKCESK është përmirësimi dhe zhvillimi i mëtejshëm i mekanizmave ekzistuese siç është ai i Sistemit të Menaxhimit të Raportimit të Incidenteve, sistem i ngritur në vitin 2019, që shërben për raportimin e incidenteve të ndodhura në infrastrukturat kritike dhe të rëndësishme të informacionit, komunikimin e vazhdueshëm mes CSIRT-it Kombëtar dhe infrastrukturave për raportet e sulmeve të ndodhura dhe analizën e tyre, të prodhuara këto nga ekipi përgjegjës i CSIRT Kombëtar. Gjithashtu, nëpërmjet këtij sistemi komunikohet me infrastrukturat lidhur me vulnerabilitetet dhe informacionet konfidenciale që mund të ndikojnë infrasatrukturat e informacionit në nivel kombëtar dhe ndërkombëtar. Sistemi i Menaxhimit të

Raportimit të Incidenteve është një sistem i klasifikuar që përmban elementët e duhur të sigurisë për shkëmbime informacioni.

Një tjetër hap i ndërmarrë është dhe ngritja e Platformës së Ndarjes së Informacioneve rreth Aktiviteteve Keqdashëse (MISP), e cila në nivel kombëtar, ka për qëllim ndarjen, ruajtjen dhe lidhjen e Indikatorëve të Kompromentimit (IOCs) të sulmeve të mundshme kibernetike dhe kërcënimeve, informacione të cilat lidhen me aktorët e kërcënimit kibernetik, vektorët e sulmeve etj. Aktualisht është ngritur platforma pranë CSIRT Kombëtar, e cila në vazhdim do të bëjë ndërveprimin direkt me infrastrukturat kritike të informacionit.

AKCESK, në kuadër të forcimit të bashkëpunimit ndërkombëtar në fushën e sigurisë dhe mbrojtjes kibernetike dhe luftës kundër ekstremizmit të dhunshëm dhe radikalizimit, ka pasur pjesëmarrje aktive në takimet e NATO-s për zbatimin e standardeve e rregulloreve ndërkombëtare në kuadër të sigurisë kibernetike.

Gjithashtu AKCESK ka rol të rëndësishëm në lidhje me forcimin e bashkëpunimit dhe shkëmbimin e informacionit me NATO, OSBE dhe organizata / forume të tjera ndërkombëtare.

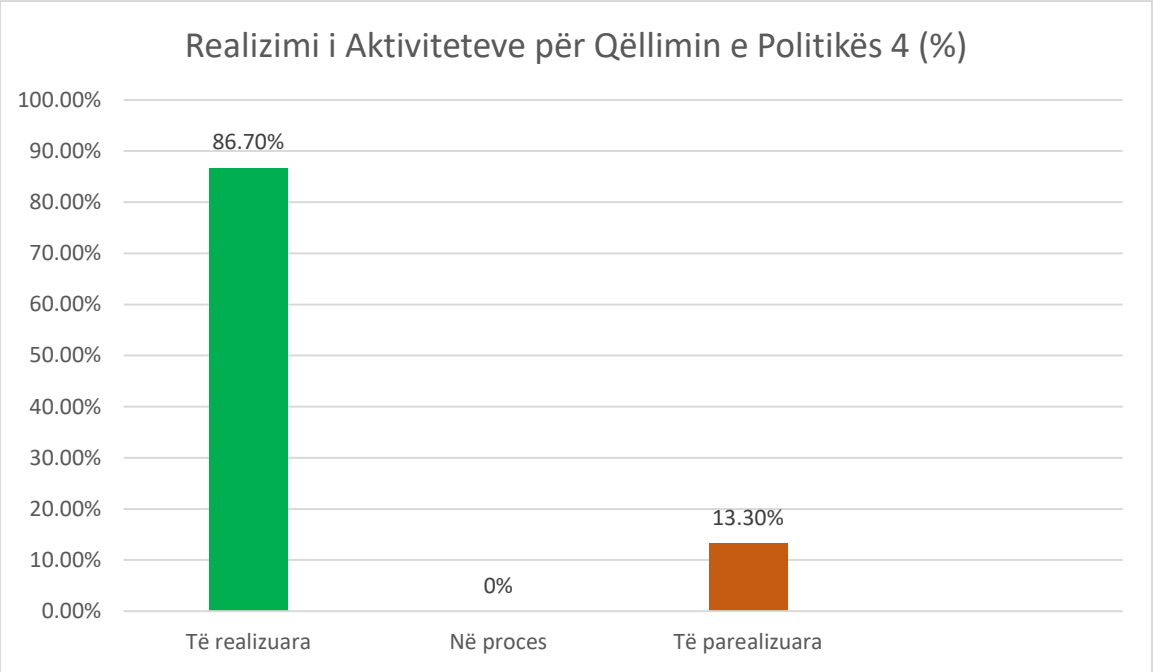
Në saj të ndërveprimit dhe bashkëpunimit me NATO-n, AKCESK ka arritur të jetë pjesë dhe të përdorë platformën NATO-MISP, vënë në dispozicion nga NATO për Shqipërinë, e cila kryen ndërveprim me organizatat ndërkombëtare për raportimin e incidenteve dhe Indikatorëve të Kompromentimit, të ndodhura në infrastrukturat e informacionit në nivel global. Kjo bën të mundur që AKCESK, në rolin CSIRT-it Kombëtar, të informojë dhe të ndërgjegjësojë në kohë reale infrastrukturat e informacioni rreth incidenteve të ndodhura dhe raportuara.

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike është anëtarësuar në aktivitete dhe iniciativa të ndryshme ndërkombëtare në fushën e sigurisë kibernetike (të tilla si First, Trust Introducer).

Gjithashtu, është realizuar bashkëpunimi i të gjithë aktorëve relevantë në procesin e zhvillimit dhe bashkimit të normave të sigurisë, standardizimin e bashkëpunimit, si dhe përcaktimin dhe vendosjen e nivelit të detyrueshëm të mbrojtjes së subjekteve që menaxhojnë incidentet kibernetike.

Realizimi i Aktiviteteve për Qëllimin e Politikës 4

Për Qëllimin e Politikës 4, rezulton se deri në vitin 2022, shkalla e aktiviteteve të realizuara është 86.7% (13 aktivitete), dhe aktiviteteve të parealizuara është 13.3% (2 aktivitete).



4. PASAPORTA E INDIKATORËVE

Qëllimi i Pasaportës së indikatorëve në vijim është që të sigurojë një përshkrim të hollësishëm metodologjik të matjes për të gjithë treguesit e nivelit të rezultatit që janë të përfshira në Strategjinë Kombëtare për Sigurinë Kibernetike 2020-2025.

Dokumenti mbulon vetëm të ashtuquajturit tregues të nivelit të rezultatit (ose performancës) që janë zhvilluar për matjen e progresit kundrejt objektivave të përcaktuara të Strategjisë.

Për secilin tregues përfshihen elementet e mëposhtme:

• Burimi i informacionit (të dhënave), që shërben si bazë për matjen e treguesit;

• Institucioni përgjegjës për grumbullimin e të dhënave për matjen e treguesit (dhe sigurimin e informacionit për qëllime të raportimit / monitorimit). Kjo përgjegjësi e caktuar përfshin gjithashtu përgjegjësinë për vlefshmërinë/cilësinë e të dhënave;

• Frekuenca e publikimit të të dhënave (dhe/ose grumbullimi i të dhënave);

• Një përshkrim metodologjik të metodës së matjes, duke lejuar për një kontroll të jashtëm dhe kuptuar më mirë se si janë zhvilluar disa vlera të caktuara të treguesve;

• Vlerat bazë dhe të synuara

Informacioni i përfshirë në Pasaportën e treguesve mëposhtë, i cili gjendet në Shtojcën 1, është zhvilluar në bashkëpunim të plotë me institucionet përgjegjëse bazuar në informacionin e dhënë nga institucionet përgjegjëse dhe formulimi i tyre mban pëlqimin e plotë të të gjitha institucioneve përgjegjëse.

Lista e indikatorëve:

1. Legjislacion i përafruar me Direktivat dhe Rregulloret e EU, që normojnë fushën e sigurisë kibernetike
2. Ngritja dhe funksionimi i CSIRT-eve në të gjithë sektorët e industrisë në nivel kombëtar
3. Ngritja e kapaciteteve të profesionistëve të fushës
4. Fushata ndërgjegjësimi për sigurinë kibernetike
5. Kuadër ligjor i plotësuar (për sigurine online të fëmijëve)
6. Fëmijë të trajnuar e ndërgjegjësuar në përdorimin e materialeve online
7. Forcimi i bashkëpunimit në nivel kombëtar për të garantuar sigurinë kibernetike në vend
8. Bashkëpunimi ndërkombëtar

5. REKOMANDIME

- ✓ Përmirësimi i kuadrit rregullator për sigurinë kibernetike i harmonizuar me acquis e BE-së, për t'i adresuar çështjet dhe zgjidhur ato duke përfshirë, por pa u kufizuar: Cloud computing, IoT, teknologjinë 5G, Inteligjencën Artificiale
- ✓ Hartimi dhe miratimi i rregullores për ofrimin e internetit të sigurt në hapësirat publike
- ✓ Përcaktimi i një procedure kombëtare për rastet e gjendjeve të jashtëzakonshme të krijuara nga krizat kibernetike, me qëllim marrjen e masave konkrete për zgjidhjen e situatës në kohë reale
- ✓ Hartimi dhe miratimi i metodologjisë për vlerësimin e rrezikut në nivel kombëtar
- ✓ Krijimi i kushteve optimale të punës për funksionimin e CSIRT-eve, për të lehtësuar përmbushjen e detyrave të tyrë me efektivitet, me qëllim garantimin e sigurisë kibernetike në infrastrukturat kritike e të rëndësishme të informacionit
- ✓ Zhvillimi dhe implementimi i programeve studimore në arsimin e lartë në fushën e sigurisë kibernetike, me qëllim krijimin e gjeneratës së re të ekspertëve të sigurisë kibernetike
- ✓ Ngritja e kapaciteteve të autoriteteve përgjegjëse kundër krimit kibernetik.
- ✓ Ngritja e qendrës kërkimore-shkencore në fushën e sigurisë kibernetike dhe pjesëmarrja në projektet dhe aktivitetet kërkimore kombëtare dhe ndërkombëtare të lidhura me sigurinë kibernetike.
- ✓ Rritja dhe mbështetja e kapaciteteve kërkimore dhe risive të biznesit nëpërmjet nxitjes së ngritjes së qendrave kërkimore shkencore në fushën e sigurisë kibernetike
- ✓ Hartimi i një udhëzimi të posaçëm dhe rregullores shoqëruese për mbledhjen e të dhënave të incidenteve të raportuara të dhunës, bullizimit dhe abuzimit online të fëmijëve në shkolla.

- ✓ Finalizimi i programeve të trajnimit për personelin e gjyqësorit, prokurorisë dhe policisë në lidhje me mbrojtjen e fëmijëvë në internet dhe sigurinë kibernetike, duke përfshirë ndihmën e ndërsjelltë juridike
- ✓ Ngritja e një sistemi kursesh pranë Shkollës së Magjistraturës dhe Akademisë së Sigurisë në lidhje me çështjet që kanë të bëjnë me krimet ndaj fëmijëve online dhe mënyrat e mbrojtjes së tyre në internet.
- ✓ Ngritja e një strukture fleksibël me ekspertët më të mirë të sigurisë kibernetike, me qëllim mbështetjen në raste krizash kibernetike, testimi dhe vlerësimi të nivelit të sigurisë kibernetike në nivel kombëtar
- ✓ Rishikimi i Planit të Veprimit të Strategjisë Kombëtare të Sigurisë Kibernetike, duke siguruar përfshirjen e vazhdueshme të palëve të interesuara
- ✓ Forcimi dhe promovimi i bashkëpunimit ndër-sektorial në sigurinë kibernetike për të siguruar zbatimin e plotë të programeve të sigurisë kibernetike
- ✓ Vijimi me organizimin e trajnimeve periodike për punonjësit e AKCESK dhe Infrastrukturave Kritike
- ✓ Përmirësimi i procedurës kombëtare të përshkallëzimit të reagimit ndaj incidenteve kibernetike duke detajuar koordinimin me Infrastrukturat Kritike dhe të Rëndësishme të Informacionit.
- ✓ Realizimi i Anketës së Vetëvlerësimit të Maturitetit të Infrastrukturave Kritike dhe të Rëndësishme të Informacionit të ENISA bazuar në modelin SIM3 për të fituar njohuri të mëtejshme mbi maturitetin dhe aftësitë e AKCESK.

SHTOJCA 1

Indikatori 1

Emërtimi I indikatorit	**Legjislacion i përafruar me Direktivat dhe Rregulloret e BE-së që normojnë fushën e sigurisë kibernetike**
Lloji i indikatorit	Tregues rezultati
Nr. Dt. Emertimi i Dokumentit	Strategjia Kombëtare për Sigurinë Kibernetike 2020-2025
Lidhja me SKZHI (Nr shtyllës)	Shtylla Nr.2 QEVERISJA E MIRË, DEMOKRACIA DHE SHTETI I SË DREJTËS
Qëllimi/Objektivi Strategjik në SKZHI	Qëllimi Strategjik SKZHI: "Konsolidimi i mbrojtjes shoqërore"
Qëllimi i politikës korresponduese	Garantimi i sigurisë kibernetike në nivel kombëtar, nëpërmjet mbrojtjes së infrastrukturave të informacionit, duke fuqizuar mjetet teknologjike dhe juridike
Objektivi Specifik me te cilin lidhet indikatori/treguesi	Përmirësimi i kuadrit rregullator për sigurinë kibernetike i harmonizuar me ligjet sektoriale, për të adresuar saktë çështjet dhe zgjidhur ato duke përfshirë, por pa u kufizuar: Cloud computing, IoT, teknologjinë 5G, Inteligjencën Artificiale
Përkatësia e Indikatorit	Kuadër Politikash
Lidhja me Acquis Communautaire	Direktiva NIS 2016
Burimi i të dhënave për monitorimin e treguesit të performancës	Akte të miratuara nga KM
Institucionet përgjegjëse për grumbullimin e të dhënave	AKCESK
	AKSHI/MB/etj
Përshkrimi i Metodologjisë	1) Kuadri strategjik rregullator i hartuar përkundrejt kuadrit rregullator të miratuar 2) Kuadri strategjik i zbatuar, niveli mesatar i raportit të zbatimit
Frekuenca e Matjes	Vjetore
	Vjetore
Natyra e Indikatorit/treguesit: Kumulativ/Rrites	Kumulativ
Input Direkt ose i Përbërë	I përbërë

Formula e llogaritjes	1) kuadër i planifikuar përkundrejt kuadrit strategjik të miratuar 2) raport mesatar i raporteve individuale të zbatimit të çdo dokumenti strategjikë, përmes monitorimit të planit përkatës të veprimit.	
Ndarja e të dhënave (për treguesit e përbërë)	Niveli i parë	
	Niveli i dytë	
	Niveli i tretë	
Theksoni drejtimin e ndryshimit / trendit (tendences) të ecurisë	Kumulaitv	
Vlerat Bazë	2019 1 Dokument politikash dhe 1 ligj	
Vlera e synuar/ Targeti	2020	1 VKM
	2021	1 ligj
	2022	2 projekt-ligje
	2023	
	2024	
	2025	Përafrim i plotë
Vlera e synuar/Targeti i rishikuar:	2025	100%
Vlera aktuale bazë:		
SDG - Titulli i Qellimit të Zhvillimit të Qëndrueshëm sipas OKB-së	N/A	N/A
Vlera e Synuar e treguesit të SDG	N/A	N/A

Indikatori 2

Emërtimi I indikatorit	**Ngritja dhe funksionimi i CSIRT-eve në të gjithë sektorët e industrisë në nivel kombëtar**
Lloji i indikatorit	Tregues rezultati
Nr Dt Emertimi i Dokumentit	Strategjia Kombëtare për Sigurinë Kibernetike 2020-2025
Lidhja me SKZHI (Nr. shtylles)	Shtylla Nr.2. QEVERISJA E MIRË, DEMOKRACIA DHE SHTETI I SË DREJTËS
Qëllimi/Objektivi Strategjik ne SKZHI	Qëllimi Strategjik SKZHI: “Konsolidimi i mbrojtjes shoqërore”
Qëllimi i politikës korresponduese	Garantimi i sigurisë kibernetike në nivel kombëtar, nëpërmjet mbrojtjes së infrastrukturave të informacionit, duke fuqizuar mjetet teknologjike dhe juridike

Objektivi Specifik me të cilin lidhet indikatori/treguesi	Ngritja dhe funksionimi i CSIRT-eve në të gjithë sektorët e industrisë në nivel kombëtar	
Përkatesia e Indikatorit	Masa zbatuese	
Lidhja me Acquis Communautaire	Direktiva NIS 2016	
Burimi i të dhënave për monitorimin e treguesit të performancës	Raporte vlerësimi vjetore	
Institucionet përgjegjëse për grumbullimin e të dhënave	AKCESK	
	CSIRT-et sektoriale	
Përshkrimi i Metodologjisë	Sipas rregullores së auditimit të AKCESK	
Frekuenca e Matjes	Vjetore	
	Vjetore	
Natyra e Indikatorit/treguesit: Kumulativ/Rritës	Rritës	
Input Direkt ose i Përbërë	Direkt	
Formula e llogaritjes		
Ndarja e të dhënave (për treguesit e përbërë)	Niveli i parë	
	Niveli i dytë	
	Niveli i tretë	
Theksoni drejtimin e ndryshimit / trendit (tendencës) të ecurisë	Rritës	
Vlerat Bazë		
	Mungojnë statistikat	
Vlera e synuar/ Targeti	2021-	1- CSIRT kombëtare operacional
	2022-	CSIRT sektoriale
	2023-	
	2024-	
	2025-	CSIRT-et e ngritura dhe funksionale
Vlera e synuar/Targeti i rishikuar:	2025	100%
Vlera aktuale bazë:		
SDG - Titulli i Qëllimit të Zhvillimit të Qëndrueshëm sipas OKB-së	N/A	N/A
Vlera e Synuar e treguesit të SDG	N/A	N/A

Indikatori 3

Emërtimi I indikatorit	**Ngritja e kapaciteteve të profesionistëve të fushës**	
Lloji i indikatorit	Tregues rezultati	
Nr Dt Emërtimi i Dokumentit	Strategjia Kombëtare për Sigurinë Kibernetike 2020-2025	
Lidhja me SKZHI (Nr shtyllës)	Shtylla Nr.5. INVESTIMI NË KAPITAL NJERËZOR DHE KOHEZION SOCIAL	
Qëllimi/Objektivi Strategjik në SKZHI	Qëllimi Strategjik SKZHI: "Konsolidimi i mbrojtjes shoqërore"	
Qëllimi i politikës korresponduese	Ndërtimi i një mjedisi të sigurt kibernetik duke edukuar dhe ndërgjegjësuar shoqërinë në ngritjen e kapaciteteve profesionale në fushën e sigurisë së informacionit	
Objektivi Specifik me të cilin lidhet indikatori/treguesi	Rritja e kapaciteteve profesionale në fushën e sigurisë së informacionit nëpërmjet rishikimit të kurrikulave arsimore	
Përkatësia e Indikatorit	Masa zbatuese	
Lidhja me acquis e BE-së	Direktiva NIS 2016/ ligj 2/2017	
Burimi i të dhënave për monitorimin e treguesit të performancës	Raporte vlerësimi vjetore	
Institucionet përgjegjëse për grumbullimin e të dhënave	AKCESK	
	CSIRT-et sektoriale/ Institucionet qeveritare	
Përshkrimi i Metodologjisë	Raportim bazuar në monitorimin vjetor	
Frekuenca e Matjes	Vjetore	
	Vjetore	
Natyra e Indikatorit/treguesit: Kumulativ/Rritës	Rritës	
Input Direkt ose i Përbërë	Direkt	
Formula e llogaritjes		
Ndarja e të dhënave (për treguesit e përbërë)	Nr kurrikulash	
	Nr Kursesh	
	Nr të trajnuarish	
Theksoni drejtimin e ndryshimit / trendit (tendencës) së ecurisë	Rritës	
Vlerat Bazë		
Vlera e synuar/ Targeti	2021-	25 profesionistë të trajnuar te sektorit financiar dhe 20 profesionistë të trajnuar të sektorit shëndetësor

	2022-	66 profesionistë nga operatorët e infrastrukturave kritike në Shqipëri dhe 50 profesionistë nga institucionet publike shqiptare dhe rajonale
	2023-	
	2024-	
	2025-	
Vlera e synuar/Targeti i rishikuar:		
Vlera aktuale bazë:		
SDG - Titulli i Qëllimit të Zhvillimit të Qëndrueshëm sipas OKB-së	N/A	N/A
Vlera e Synuar e treguesit te SDG	N/A	N/A

Indikatori 4

Emërtimi I indikatorit	**Fushata ndërgjegjësimi për sigurinë kibernetike**
Lloji i indikatorit	Tregues rezultati
Nr Dt Emërtimi i Dokumentit	Strategjia Kombëtare për Sigurinë Kibernetike 2020-2025
Lidhja me SKZHI (Nr shtyllës)	Shtylla Nr.2. QEVERISJA E MIRË, DEMOKRACIA DHE SHTETI I SË DREJTËS
Qëllimi/Objektivi Strategjik në SKZHI	Qëllimi Strategjik SKZHI: "Konsolidimi i mbrojtjes shoqërore"
Qëllimi i politikës korresponduese	Ndërtimi i një mjedisi të sigurt kibernetik duke edukuar dhe ndërgjegjësuar shoqërinë në ngritjen e kapaciteteve profesionale në fushën e sigurisë së informacionit
Objektivi Specifik me të cilin lidhet indikatori/treguesi	Rritje e ndërgjegjësimit të shoqërisë, për sigurinë kibernetike dhe kërcënimet kibernetike
Përkatësia e Indikatorit	Masa zbatuese
Lidhja me acquis së BE-së	Direktiva NIS 2016/ligj 2/2017
Burimi i të dhënave për monitorimin e treguesit të performancës	Raporte vlerësimi vjetore
Institucionet përgjegjëse për grumbullimin e të dhënave	AKCESK
Përshkrimi I Metodologjisë	Raportim bazuar ne monitorim vjetor
Frekuenca e Matjes	Vjetore
	Vjetore
Natyra e Indikatorit/treguesit: Kumulativ/Rritës	Kumulativ
Input Direkt ose i Përbërë	Direkt

Formula e llogaritjes		
Ndarja e të dhënave (për treguesit e përbëre)	Nr. kurrikulash	
	Nr. Kursesh	
	Nr. të trajnuarish	
Theksoni drejtimin e ndryshimit / trendit (tendencës) të ecurisë	Rritës	
Vlerat Bazë	Mungojnë statistikat	
Vlera e synuar/ Targeti	2020-	1
	2021-	1
	2022-	1
	2023-	1
	2024-	1
	2025-	1
Vlera e synuar/Targeti i rishikuar:		
Vlera aktuale bazë:		
SDG - Titulli i Qellimit të Zhvillimit të Qëndrueshëm sipas OKB-së	N/A	N/A
Vlera e Synuar e treguesit të SDG	N/A	N/A

Indikatori 5

Emërtimi i indikatorit	**Kuadër ligjor i plotësuar (për sigurinë online të fëmijëve)**
Lloji i indikatorit	Tregues rezultati
Nr Dt Emërtimi i Dokumentit	Strategjia Kombëtare për Sigurinë Kibernetike 2020-2025
Lidhja me SKZHI (Nr shtyllës)	Shtylla Nr.2. QEVERISJA E MIRË, DEMOKRACIA DHE SHTETI I SË DREJTËS
Qëllimi/Objektivi Strategjik në SKZHI	Qëllimi Strategjik SKZHI: “Konsolidimi i mbrojtjes shoqërore”
Qëllimi i politikës korresponduese	Krijimi i mekanizmave të nevojshëm për sigurinë e fëmijëve në hapësirën kibernetike, duke përgatitur njëkohësisht brezin e ri të aftë për të përfituar nga përparësitë e teknologjisë së informacionit dhe për të përballuar sfidat e zhvillimit
Objektivi Specifik me të cilin lidhet indikatori/treguesi	Forcimi i kuadrit ligjor për rritjen e sigurisë së fëmijëve në internet.
Përkatesia e Indikatorit	Kuadër politikash
Lidhja me acquis së BE-së	

Burimi i të dhënave për monitorimin e treguesit të performancës	Raporte vlerësimi vjetore	
Institucionet përgjegjëse për grumbullimin e të dhënave	UNICEF	
Përshkrimi i Metodologjisë	Raportim bazuar në monitorim vjetor	
Frekuenca e Matjes	Vjetore	
	Vjetore	
Natyra e Indikatorit/treguesit: Kumulativ/Rrites	Kumulativ	
Input Direkt ose i Përbërë	I përbërë	
Formula e llogaritjes		
Ndarja e të dhënave (për treguesit e përbërë)	Akte ligjore të rishikuara	
	Rregullore e miratuar	
	Metodologji	
Theksoni drejtimin e ndryshimit / trendit (tendencës) të ecurisë	Ritës	
Vlerat Bazë		
Vlera e synuar/ Targeti	2020-	10%
	2021-	
	2022-	50%
	2023-	
	2024-	
	2025-	100%
Vlera e synuar/Targeti i rishikuar:		
Vlera aktuale bazë:		
SDG - Titulli i Qellimit të Zhvillimit të Qëndrueshëm sipas OKB-së	N/A	N/A
Vlera e Synuar e treguesit të SDG	N/A	N/A

Indikatori 6

Emërtimi i indikatorit	**Fëmijë të trajnuar e ndërgjegjësuar në përdorimin e materialeve online**
Lloji i indikatorit	Tregues rezultati
Nr Dt Emërtimi i Dokumentit	Strategjia Kombëtare për Sigurinë Kibernetike 2020-2025

Lidhja me SKZHI (Nr shtyllës)	Shtylla Nr.5. INVESTIMI NË KAPITAL NJERËZOR DHE KOHEZION SOCIAL	
Qëllimi/Objektivi Strategjik në SKZHI	Qëllimi Strategjik SKZHI: "Konsolidimi i mbrojtjes shoqërore"	
Qëllimi i politikës korresponduese	Krijimi i mekanizmave të nevojshëm për sigurinë e fëmijëve në hapësirën kibernetike, duke përgatitur njëkohësisht brezin e ri të aftë për të përfituar nga përparësitë e teknologjisë së informacionit dhe për të përballuar sfidat e zhvillimit	
Objektivi Specifik me të cilin lidhet indikatori/treguesi	Rritja e ndërgjegjësimit dhe edukimi tek të gjitha segmentet e shoqërisë për përdorimin e sigurtë të internetit nga fëmijët	
Përkatësia e Indikatorit	Masa zbatuese	
Lidhja me acquis së BE-së		
Burimi i të dhënave për monitorimin e treguesit të performancës	Raporte vlerësimi vjetore	
Institucionet përgjegjëse për grumbullimin e të dhënave	UNICEF	
Përshkrimi I Metodologjisë	Raportim bazuar ne monitorim vjetor	
Frekuenca e Matjes	Vjetore	
	Vjetore	
Natyra e Indikatorit/treguesit: Kumulativ/Rritës	Kumulativ	
Input Direkt ose i Përbërë	Direkt	
Formula e llogaritjës		
Ndarja e të dhënave (për treguesit e përbërë)	Nxënës të trajnuar	
	Mësues të trajnuar	
	Magjistratë të trajnuar	
Theksoni drejtimin e ndryshimit / trendit (tendencës) të ecurisë	Rritës	
Vlerat Bazë	2019 13000 nxënës të trajnuar	
Vlera e synuar/ Targeti	2020-	1200
	2021-	1600
	2022-	2000
	2023-	2400
	2024-	2600
	2025-	3000
Vlera e synuar/Targeti i rishikuar:		
Vlera aktuale bazë:	2022	2000

SDG - Titulli i Qëllimit të Zhvillimit të Qëndrueshëm sipas OKB-së	N/A	N/A
Vlera e Synuar e treguesit të SDG	N/A	N/A

Indikatori 7

Emërtimi I indikatorit	**Forcimi I bashkëpunimit në nivel kombëtar për të garantuar sigurinë kibernetike në vend.**	
Lloji i indikatorit	Tregues rezultati	
Nr Dt Emërtimi i Dokumentit	Strategjia Kombëtare për Sigurinë Kibernetike 2020-2025	
Lidhja me SKZHI (Nr shtyllës)	Shtylla Nr.2. QEVERISJA E MIRË, DEMOKRACIA DHE SHTETI I SË DREJTËS	
Qëllimi/Objektivi Strategjik në SKZHI	Qëllimi Strategjik SKZHI: "Konsolidimi i mbrojtjes shoqërore"	
Qëllimi i politikës korresponduese	Rritja e bashkëpunimit kombëtar dhe ndërkombëtar në fushën e sigurisë kibernetike me partnerët strategjikë	
Objektivi Specifik me të cilin lidhet indikatori/treguesi	Forcimi i bashkëpunimit institucional në nivel kombëtar	
Përkatësia e Indikatorit	Masa zbatuese	
Lidhja me acquis së BE-së	Direktiva NIS	
Burimi i të dhënave për monitorimin e treguesit të performancës	Raporte vlerësimi vjetore	
Institucionet përgjegjëse për grumbullimin e të dhënave	AKCESK	
Përshkrimi i Metodologjisë	Raportim bazuar në monitorim vjetor	
Frekuenca e Matjes	Vjetore	
	Vjetore	
Natyra e Indikatorit/treguesit: Kumulativ/Rritës	Kumulativ	
Input Direkt ose i Përbërë	Direkt	
Formula e llogaritjes		
Ndarja e të dhënave (për treguesit e përbërë)		
Theksoni drejtimin e ndryshimit / trendit (tendences) të ecurisë	Kumulativ	
Vlerat Bazë	2019-	2

Vlera e synuar/ Targeti	2020-	1
	2021-	1
	2022-	1
	2023-	1
	2024-	1
	2025-	1
Vlera e synuar/Targeti i rishikuar:		
Vlera aktuale bazë:	2022	2
SDG - Titulli i Qëllimit të Zhvillimit të Qëndrueshëm sipas OKB-së	N/A	N/A
Vlera e Synuar e treguesit të SDG	N/A	N/A

Indikatori 8

Emërtimi i indikatorit	**Bashkëpunimi ndërkombëtar**
Lloji i indikatorit	Tregues rezultati
Nr Dt Emërtimi i Dokumentit	Strategjia Kombëtare për Sigurinë Kibernetike 2020-2025
Lidhja me SKZHI (Nr shtyllës)	Shtylla Nr.1. Anëtarsim në BE
Qëllimi/Objektivi Strategjik në SKZHI	Qëllimi Strategjik SKZHI: "Konsolidimi i mbrojtjes shoqërore"
Qëllimi i politikës korresponduese	Rritja e bashkëpunimit kombëtar dhe ndërkombëtar në fushën e sigurisë kibernetike me partnerët strategjikë
Objektivi Specifik me të cilin lidhet indikatori/treguesi	Forcimi i bashkëpunimit ndërkombëtar në fushën e sigurisë dhe mbrojtjes kibernetike dhe luftës kundër ekstremizmit të dhunshëm dhe radikalizimit.
Përkatësia e Indikatorit	Masa zbatuese
Lidhja me acquis së BE-së	Direktiva NIS
Burimi i të dhënave për monitorimin e treguesit të performancës	Raporte vlerësimi vjetore
Institucionet përgjegjëse për grumbullimin e të dhënave	AKCESK
Përshkrimi i Metodologjisë	Raportim bazuar në monitorim vjetor
Frekuenca e Matjes	Vjetore
	Vjetore

Natyra e Indikatorit/treguesit: Kumulativ/Rritës	Kumulativ	
Input Direkt ose i Përbërë	Direkt	
Formula e llogaritjes		
Ndarja e të dhënave (për treguesit e përbërë)		
Theksoni drejtimin e ndryshimit / trendit (tendences) të ecurisë	Kumulativ	
Vlerat Bazë	2019-	2
Vlera e synuar/ Targeti	2020-	4
	2021-	5
	2022-	6
	2023-	7
	2024-	8
	2025-	9
Vlera e synuar/Targeti i rishikuar:		
Vlera aktuale bazë:	2022	1
SDG - Titulli i Qëllimit të Zhvillimit të Qëndrueshëm sipas OKB-së	N/A	N/A
Vlera e Synuar e treguesit të SDG	N/A	N/A