AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Monitorimi "Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025"

Tiranë, 2022

Tabela e Përmbajtjes

1. HYRJE

Një hapësirë e lirë kibernetike i shërben komunikimit midis vendeve, komuniteteve dhe qytetarëve në shkëmbimin e informacionit në mbarë botën. Zhvillimet e fundit të teknologjisë së informacionit dhe komunikimit, sjellin përfitime të mëdha për komunitetin dhe qytetarët pasi shpërndarja e informacionit në kohë reale konsiderohet shumë e rëndësishme. Të gjitha këto zhvillime së bashku me përfitimet sjellin dhe kërcënime në fusha të ndryshme. Në këtë këndvështrim mbrojtja dhe siguria kibernetike konsiderohen sfida e të ardhmes.

Ekzistojnë individë dhe grupe të ndryshme keqdashëse në hapësirën kibernetike, të cilët influencojnë në mbarëvajten dhe funksionimin e shteteve. Ndërhyrjet e privatësisë dhe vjedhjet e identitetit janë një shqetësim në rritje për shoqërinë. Shqipëria duke synuar rritjen e mirëqënies dhe përmirësimin e shërbimeve publike po investon në infrastrukturën digjitale. Kjo, bashkë me përfitimet sjell edhe problematika në sigurinë kibernetike. Kërcënimet kibernetike janë në rritje duke synuar sigurinë e sistemeve të informacionit. Sfidat aktuale konsistojnë në ndërtimin e një shoqërie të zhvilluar digjitale por njëkohësisht dhe të mbrojtur kibernetikisht. Krahas zhvillimeve në teknologjinë e informacionit është përmirësuar edhe kuadri ligjor për sigurinë kibernetike.

Strategjia Kombëtare për Sigurinë Kibernetike 2020-2025 u miratua me Vendimin nr. 1034 datë 24.12.2020, të Këshillit të Ministrave dhe përbën një instrument kyç për rritjen e sigurisë së rrjeteve dhe sistemeve të informacionit në nivel kombëtar dhe prioritet i 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 digjitale, 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:

- zbatimin e 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.

Ky është raporti i parë i monitorimit dhe është përgatitur bazuar në raportimet e realizuara nga institucionet zbatuese gjatë vitit të parë të implementimit të strategjisë. Raporti i monitorimit ka për qëllim të vlerësojë ecurinë e zbatimit të kësaj strategjie sipas 4 qëllimeve të politikave dhe objektivave respektive për periudhën Janar – Dhjetor 2021.

Plani i Veprimit i Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025 përfshin në total 125 aktivitete bazë për t'u implementuar përgjatë viteve të zbatimit të Strategjisë.. Nga këto 52% (65 aktivitete) janë realizuar plotësisht përgjatë vitit të parë 2021, ndersa 42% (52 aktivitete) pritet të fillojnë përgjatë vitit 2022 e më pas.

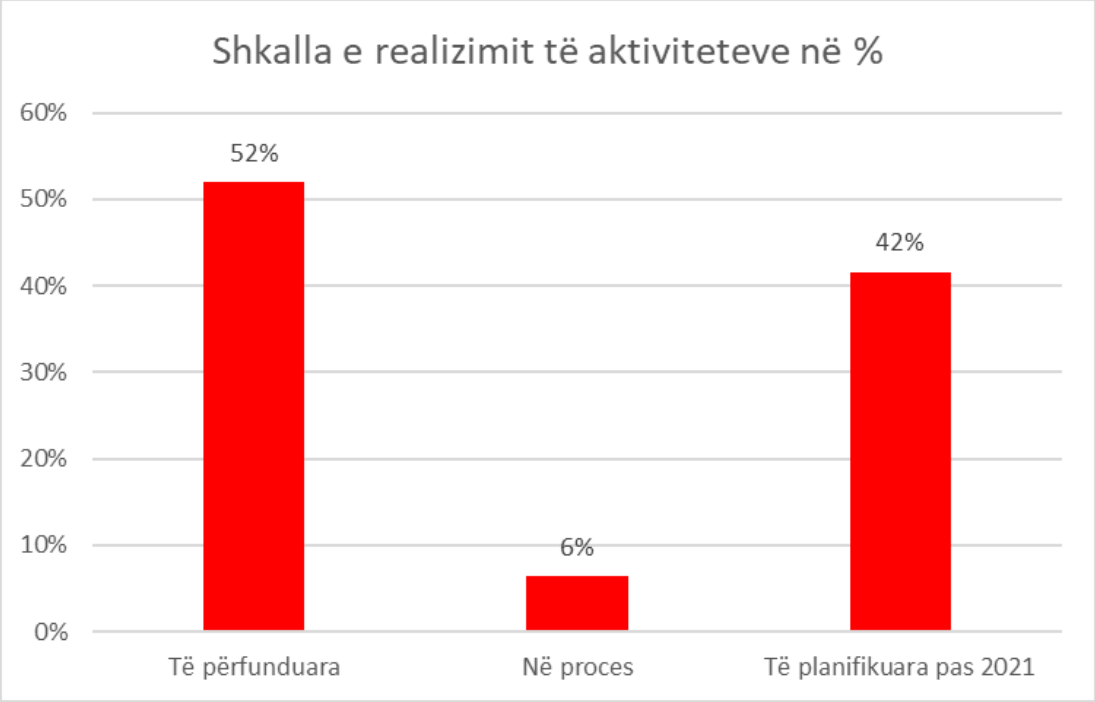
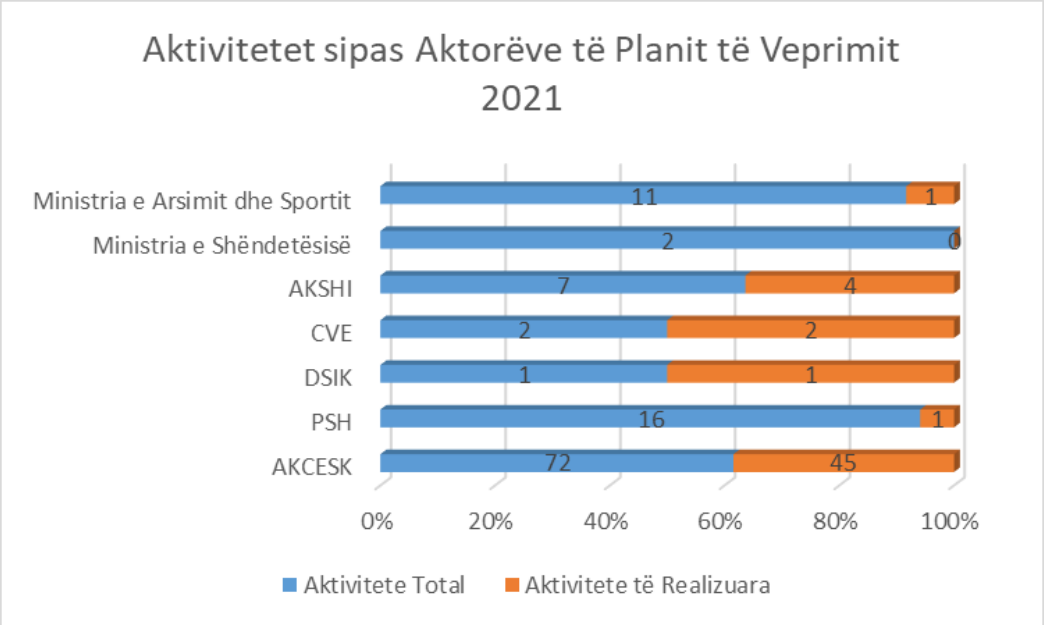


Figure 1 Shkalla e realizimit të aktiviteteve

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

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



Në veçanti ka progres në përmbushje të qëllimit të politikës së parë mbi "Garantimin e sigurisë kibernetike në nivel kombëtar, nëpërmjet mbrojtjes së infrastrukturave të informacionit, duke fuqizuar mjetet teknologjike dhe juridike." po të konsiderohen aktivitetet e realizuara dhe ato që janë në proçes.

Në realizimin e objektivave të kësaj politike janë parashikuar 49 aktivitete (39%), 29 prej të cilave të realizuara plotësisht dhe 8 në proçes siç shihet në grafikun mëposhtë:

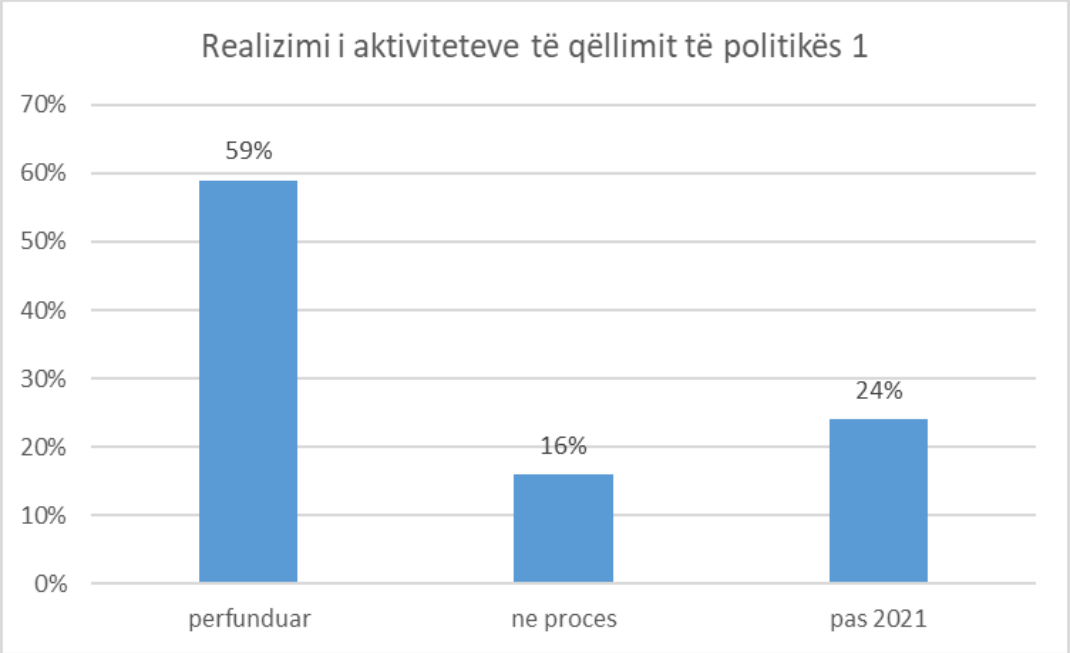


Figure 2 Realizimi i aktiviteteve të qëllimit të politikës 1

Në realizimin e objektivave të qëllimit të politikës së dytë janë parashikuar 19 aktivitete (15%), 8 prej të cilave të realizuara plotësisht dhe 11 të pafilluara akoma siç shihet në grafik.

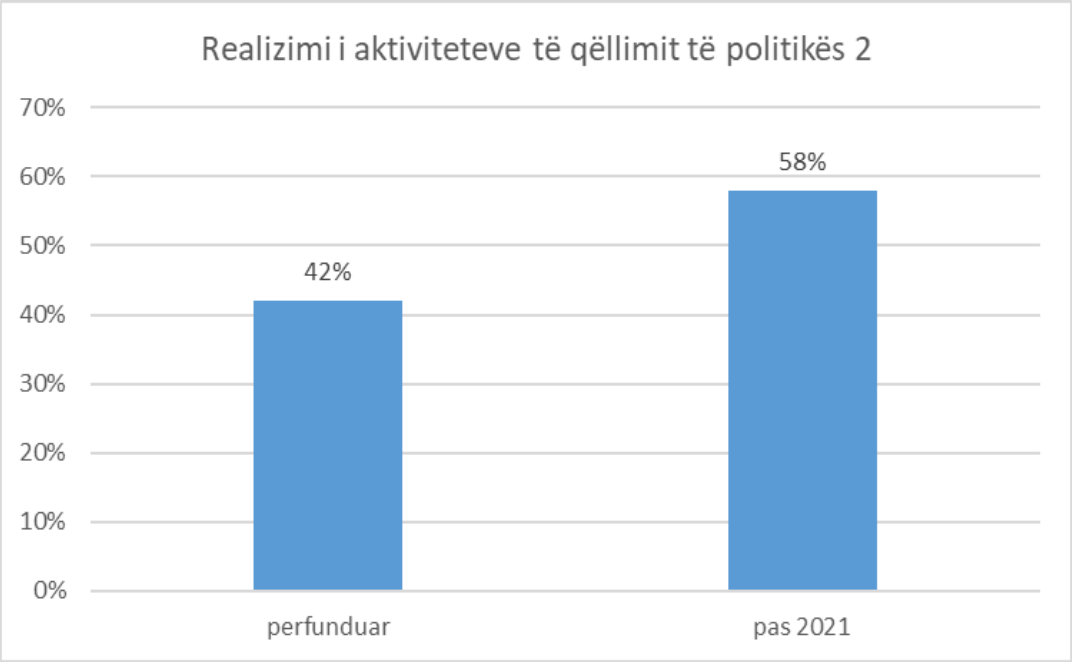


Figure 3 Realizimi i aktiviteteve të qëllimit të politikës 2

Në realizimin e objektivave të qëllimit të politikës së tretë janë parashikuar 42 aktivitete (34%), 17 prej të cilave të realizuara plotësisht dhe 25 të pafilluara akoma siç shihet në grafik.

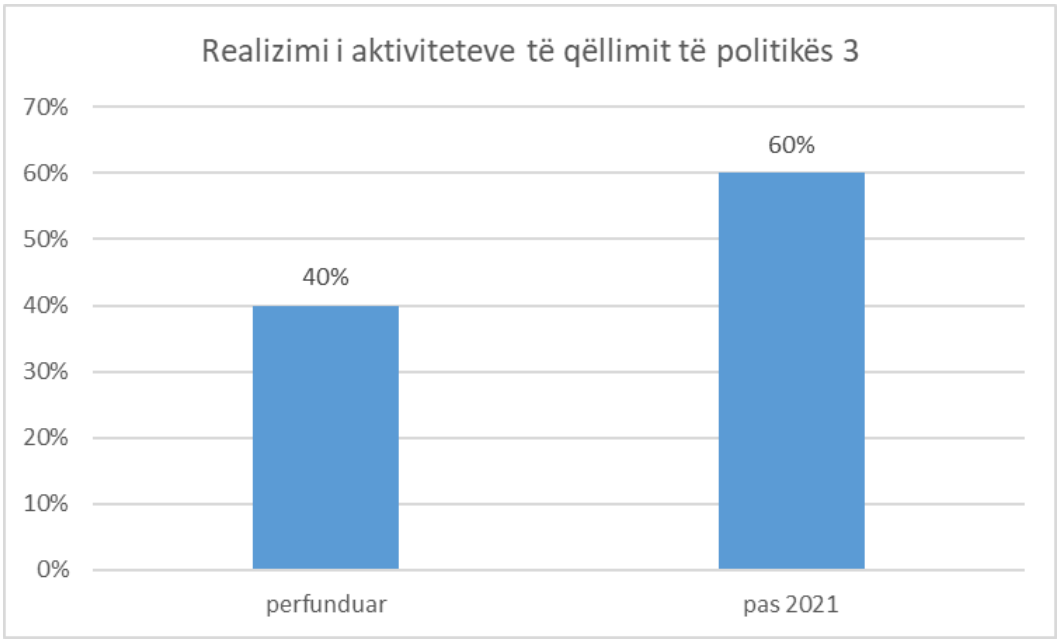


Figure 4 Realizimi i aktiviteteve të qëllimit të politikës 3

Në realizimin e objektivave të qëllimit të politikës së katërt janë parashikuar 15 aktivitete (12%), 11 prej të cilave të realizuara plotësisht dhe 4 të pafilluara akoma siç shihet në grafik.

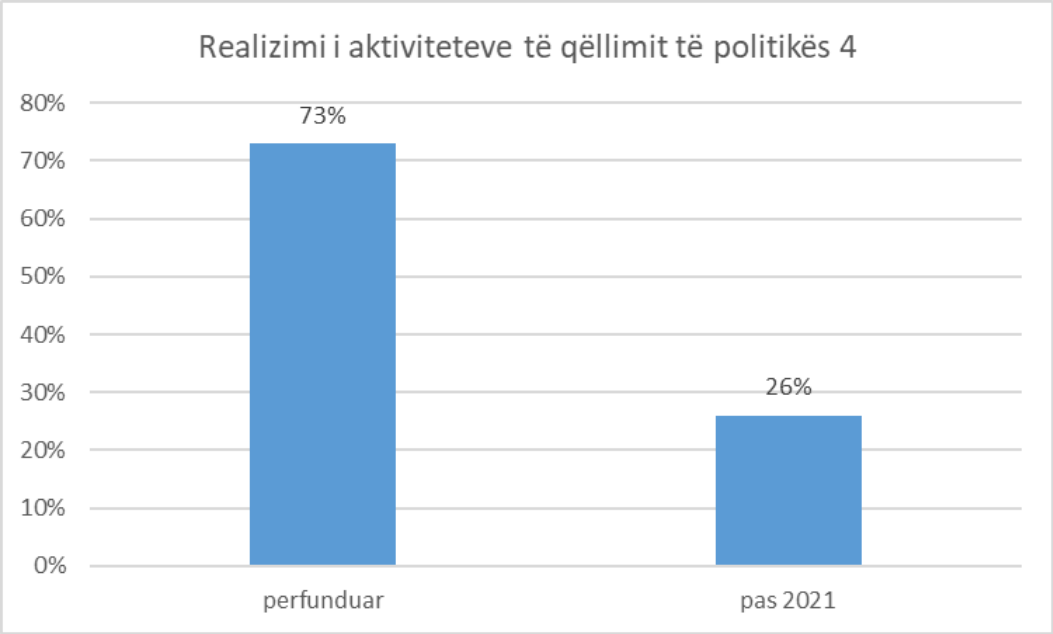


Figure 5 Realizimi i aktiviteteve të qëllimit të politikës 4

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 2021.

Monitorimi i Strategjisë ka konsistuar në këto faza kryesore:

a) Raportimi i institucioneve mbi zbatimin e Masave 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.

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.

Qëllimi i politikës 1 është 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

Për realizimin e objektivave të Prioritetit të Parë Strategjik, institucionet e përfshira në realizimin e PV raportojnë si më poshtë vijon:

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK)

AKCESK është në procesin e përafrimit të plotë të kuadrit ligjor rregullator të fushave të veprimtarisë së tij. Draftligji për transpozimin e Rregullores Evropiane eIDAS “Për identifikimin elektronik dhe shërbimet e besuara për transaksione elektronike në tregun e brendshëm” është në procesin final të draftimit dhe është gati për procesin e konsultimit publik. Gjithashtu, AKCESK është duke finalizuar drafligjin e transpozuar për sigurinë kibernetike bazuar në Direktivën NIS 2016/1148 të Parlamentit Evropian "Për masat e nivelit të lartë të sigurisë së rrjetit dhe sistemet e informacionit në të gjithë Bashkimin Evropian".

Në zbatim të Ligjit nr.2/2017 Për Sigurinë Kibernetike, është miratuar lista e përditësuar e infrastrukturave kritike dhe të rëndësishme të informacionit me Vendimin e Këshillit të Ministrave nr. 553 datë 15.07.2020 " Për miratimin e listës së infrastrukturave kritike te informacionit dhe listës së infrastrukturave të rëndësishme të informacionit". Aktualisht, është dërguar pranë Këshillit të Ministrave paketa e përditësuar për miratimin e listës së përditësuar së infrastrukturave kritike dhe të rëndësishme të informacionit, 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".

AKCESK është institucioni koordinues për 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 mbrojtur ndaj kërcënimeve në dhe përmes hapësirës kibernetike në mbështetje të detyrave kryesore të NATO-s.

Stërvitja e Cyber Coalition ekzekutohet përmes Qendrës së Stërvitjes dhe Ushtrimeve të Sigurisë Kibernetike të Estonisë, ose 'CR14'. Audienca e trajnimit dhe trajnerët lokalë marrin pjesë nga Kombet dhe entitetet e tyre përkatëse përmes rrjeteve virtuale dhe një grup pjesëmarrësish mblidhet në Estoni për të ekzekutuar ushtrimin.

AKCESK ka ngritur një Sistem Raportimi Incidentesh Kibernetike. Ky sistem shërben jo vetëm për raportimin e ngjarjeve të incidenteve të sigurisë në 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. Aktualisht raportimi i incidenteve nga OIRI dhe OIKI është i ulët, jo vetëm per faktin e nevojës për forcimin e besimit ndaj konfidencialitetit të të dhënave të raportuara, por edhe nga fakti që implementimi i shumë niveleve dhe shtresave të sigurisë ndaj Infrastrukturave Kritike dhe të Rëndësishme të informacionit i bën më imun ndaj incidenteve të mundshme.

AKCESK, në cilësinë e insitucionit përgjegjës për implementimin e nënobjektivit mbi analizimin e infrastrukturave kritike dhe të rëndesishme 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 i një Pyetësori i cili është i afishuar në faqen zyrtare të Autoritetit.

Në kuadër mbrojtjes së hapësirës kibernetike dhe rritjes së nivelit të sigurisë kibernetike në infrastukturat 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 tu implemetuar nga Infrstukturat Kritike dhe të Rëndësishme të Informacionit në Republikën e Shqipërisë.

AKCESK kryen raporte vetëvlerësimi nga Infrastrukturat Kritike dhe të Rëndësishme të informacionit për nivelin e maturimit te Sigurise Kibernetike. Në kuader të velerësimit të nivelit të sigurisë kibernetike në infrastukturat krititke dhe të rëndesishme të informacionit, AKCESK në përmbushje të detyrave funksionale kryen audimin e infrastukturave krtitike dhe të rendesishme të informacionit ne lidhje me implementimin e masave minimale të sigurise së informacionit.

Auditimet e infrastukturave kritike dhe të rendesishme kryhen nepermjet metodes se vetedeklarimit dhe metodës vajte në vend (onsite).

Autoriteti Kombëtar për Certifikimin Eletronik dhe Sigurinë Kibernetike me qëllim ngritjen e kapaciteteve të CSIRT-eve, nëpërmjet trajnimeve dhe stërvitjeve kibernetike, ka realizuar në bashkëpunim me RISI Albania, 4 broshura për të cilat janë kryer trajnime dhe ngritje kapacitetesh me grupet e interesit për secilën broshure.

1. Siguria Kibernetike në Sektorin e Energjisë
2. Siguria Kibernetike në Sektorin Financiar
3. Siguria Kibernetike në ndërmarrjet e vogla e të mesme
4. Siguria Kibernetike në shëndetësi

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike ka kryer ushtrime ne nivel kombëtar gjatë vitit 2021.

AKCESK në bashkëpunim me Ambasadën e SHBA-së në Tiranë, Tirana Bank, Union Bank, Albsig Sh.a., Iute Credit, DCAF, Silensec International Telecommunication Unit, Carnegie Mellon University, organizuan në datat 21-25 Qershor 2021, edicionin e pestë të Albanian Cyber Academy (ACA5). ACA5 synoi rritjen e kapaciteteve dhe thellimin e njohurive në fushën e sigurisë kibernetike për studentët e viteve të fundit të degëve TIK dhe operatorëve të infrastrukturave kritike të informacionit. Edicioni i pestë i Albanian Cyber Academy kishte të ftuar 10 folës ndërkombëtarë dhe 11 ekspertë kombëtarë: Dan Cimpean, Vilma Tomco, Ogerta Koruti, Almerindo Graziano, Volha Litvinets, JustinNovak, Stefan Tanase, Andrei Bozeanu, Dorin Nedelcu, Laura Thaqi, Eralda Caushaj, Paweł Srokosz, Naim Isufi, Hergis Jica, Lawrence Rogers, Fatjon Kadillari, Rexhion Qafa, Saimir Kapllani, Lorin Baxhaku, Ergis Gaxho, Klorenta Pashaj, të cilët ndanë ekspertizën e tyre me 300+ pjesëmarrës online dhe më shumë se 70 pjesëmarrës unik në ditë.

AKCESK organizoi aktivitetin 5-ditor "Cyber Health" me rreth 20 përfaqësues të sektorit publik dhe privattë shëndetësisë. Qëllimi i këtij aktiviteti është rritja e ndërgjegjësimit për ndërtimin e një shoqërie të zhvilluar digjitale, të mbrojtur kibernetikisht dhe të pajisur me njohuritë e nevojshme për të maksimizuar përfitimet dhe minimizuar rreziqet.

AKCESK , në përmbushje të detyrave funksionale dhe objektivave të "Strategjisë Kombëtare për Sigurinë Kibernetike", në bashkëpunim me Shoqatën Shqiptare të Bankave (AAB) Albanian Association of Banks (Shoqata Shqiptare e Bankave), organizuan aktivitetin 2-ditor, ne datat 17-18 Nëntor 2021, "Financial Cyber Drill", ku morën pjesë rreth 25 pjesëmarrës. Qëllimi i aktivitetit ishte ngritja e kapaciteteve të sektorit financiar, si një nga sektorët më sensitivë në nivel kombëtar

Drejtoria e Sigurimit të Informacionit të Klasifikuar (DSIK)

DSIK për zhvillimin e mbrojtjes në fushën e krimit kibernetik pranë strukturës së tyre kanë rekrutuar një punonjës të ri në vitin 2021, i cili është 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)”. Gjithashtu DSIK ka zhvilluar trajnime për ngritjen e kapaciteteve të punonjësve në strukturë.

Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI)

AKSHI në kuadër të Politikës 1 të Strategjisë Kombëtare për Sigurinë Kibernetike për optimizimin dhe zgjerimin e infrastrukturave të sigurisë ka realizuar Projektin "Përmirësimi me teknika të avancuara të sigurisë kibernetike në rrjetin qeveritar gov-net dhe qendrën e të dhënave qeveritare" me kosto totale 413,588,880 lek.

Qendra për Koordinimin Kundër Ekstremizmit të Dhunshëm (CVE)

CVE është insitucioni 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

Qendra për Koordinimin Kundër Ekstremizmit të Dhunshëm ka përfunduar projektin Moonshot CVE, që synon luftën ndaj Ekstremizmit të Dhunshëm në Shqipëri, i cili ka për qëllim individët në rrezik të EDH me shërbime të përshtatura që zvogëlojnë cenueshmërinë e tyre ndaj radikalizimit. Ky projekt u pilotua me një metodologji specifike për Shqipërinë, duke kombinuar qasjen e udhëhequr nga të dhënat e Moonshot CVE për angazhimin e individëve që cënohen në internet me ndërhyrje të qëndrueshme, që do të ofrohen nga ofruesit e shërbimeve lokale. Moonshot CVE ka përdorur metoda kërkimore sasiore dhe cilësore për të identifikuar narrativat kryesore ekstremiste të dhunshme që qarkullojnë në internet, shërbimet përkatëse lokale, rrugët e mundshme për shënjestrimin teknik dhe angazhimin, dhe mundësitë për sinergji me programimin ekzistues të CVE.

Qendra për Koordinimin Kundër Ekstremizmit të Dhunshëm ka organizuar fushata sensibilizuese në shkolla dhe me qasje ne komunitet "Kunder radikalizimit dhe ekstremizmit te dhunshem online" me target grupe te ndryshme sipas profilit dhe portofolit te Ministrive te Linjes, institucioneve te varesise si dhe pushtetit vendor.

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK) ka lidhur marrëveshje bashkëpunimi ndërmjet Qendrës CVE, dhe Autoritetit të Mediave Audiovizive (AMA).

ASP dhe QKEDH-në kanë organizuar aktivitet për “Prezantimin e portalit unik për sinjalizimin e faqeve të internetit me përmbajtje të paligjshme”.

IKTD në bashkëpunim dhe nën koordinimin e Qendrës CVE po zbaton projektin “Ndërtimi i komuniteteve të sigurta dhe të qëndrueshme ndaj fenomeneve të radikalizimit dhe ekstremizmit të dhunshëm ONLINE, në zonat periferike të Tiranës”. (Në proces)

Qendra CVE në bashkëpunim me Qendrën Media Aktive kanë realizuar një sërë intervistash me aktorët e vijës së parë të angazhuar në luftën kundër ekstremizmit të dhunshëm, në kuadër te ndërtimit të 5 reportazheve që kanë si qëllim evidentimin e bashkëpunimit mes institucioneve të

shtetit shqiptar, shoqërisë civile dhe komuniteteve fetare në përpjekjet për të luftuar ekstremizmin e dhunshëm në platformat online.

Pas një bashkëpunimi të frytshëm, më shumë sesa një vjeçar me Qendrën për Studimin e Demokracisë dhe Qeverisjes (CSDG), u finalizua studimi 'Eksplorimi i zhvillimit të një komunikimi strategjik në P/CVE në Shqipëri - Qasje e bazuar në kërkim".

Në përmbushje të qëllimit të politikës së parë mbi "Garantimin e sigurisë kibernetike në nivel kombëtar, nëpërmjet mbrojtjes së infrastrukturave të informacionit, duke fuqizuar mjetet teknologjike dhe juridike." konsiderohet dhe buxheti i realizuara dhe ai i parealizuar.

Në realizimin e objektivave të kësaj politike është parashikuar një buxhet prej 327,799,008 lekë ku 66,957,408 lekë (20%) është realizuar dhe 260,841,600 lekë (80%) i parealizuar ende siç shihet në grafikun mëposhtë:

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.

Qëllimi i politikës 2 është 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 e 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 PV raportojnë si më poshtë vijon:

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK)

AKCESK për të rritur ndërgjegjësimin në grupmosha të ndryshme të shoqërisë, për përdorimin e internetit të sigurt dhe të infrastrukturës digjitale ka kyer trajnim

e periodike per thellimin e njohurive në sigurinë kibernetike, sipas dinamikës së fushës, për stafin administrativ në nivel qendror dhe në nivel lokal. Këto trajnime janë kryer bazuar ne broshurat e hartuara nga AKCESK ne lidhje me Sigurinë Kibernetike në Sektorin e Energjisë, Financiar, Ndërmarrjet e Vogla dhe të Mesme dhe në Shëndetësi.

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike me qëllim rritjen e kapaciteteve të CSIRT-eve në nivel kombëtar dhe nivelit ekzekutiv të administratës publike ka organizuar stërvitje kibernetike gjatë realizimeve te aktiviteteve si **Albanian Cyber Academy, "Cyber Health", "Financial Cyber Drill" dhe** "**Cyber Camp Albania**":

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike në bashkëpunim me Ambasadën e SHBA-së në Tiranë, Tirana Bank, Union Bank, Albsig Sh.a., Iute Credit, DCAF, Silensec International Telecommunication Unit, Carnegie Mellon University, organizuan në datat 21-25 Qershor 2021, edicionin e pestë të **Albanian Cyber Academy**. ACA5 synoi rritjen e kapaciteteve dhe thellimin e njohurive në fushën e sigurisë kibernetike për studentët e viteve të fundit të degëve TIK dhe operatorëve të infrastrukturave kritike të informacionit. Edicioni i pestë i Albanian Cyber Academy kishte të ftuar 10 folës ndërkombëtarë dhe 11 ekspertë kombëtarë, të cilët ndanë ekspertizën e tyre me 300+ pjesëmarrës online dhe më shumë se 70 pjesëmarrës unik në ditë.

AKCESK organizoi aktivitetin 5-ditor **"Cyber Health"** me rreth 20 përfaqësues të sektorit publik dhe privattë shëndetësisë. Qëllimi i këtij aktiviteti është rritja e ndërgjegjësimit për ndërtimin e një shoqërie të zhvilluar digjitale, të mbrojtur kibernetikisht dhe të pajisur me njohuritë e nevojshme për të maksimizuar përfitimet dhe minimizuar rreziqet.

AKCESK , në përmbushje të detyrave funksionale dhe objektivave të "Strategjisë Kombëtare për Sigurinë Kibernetike", në bashkëpunim me Shoqatën Shqiptare të Bankave (AAB) Albanian Association of Banks (Shoqata Shqiptare e Bankave), organizuan aktivitetin 2-ditor, ne datat 17-18 Nëntor 2021, **"Financial Cyber Drill",** ku morën pjesë rreth 25 pjesëmarrës. Qëllimi i aktivitetit ishte ngritja e kapaciteteve të sektorit financiar, si një nga sektorët më sensitivë në nivel kombëtar.

AKCESK në bashkëpunim me Këshillin e Europës, Raiffeisen Invest dhe Universiteti Katolik "Zoja e Këshillit të Mirë" organizojne ne datat 6-8 Dhjetor aktivitetin inovativ "**Cyber Camp**

Albania" prane Movenpick Hotel, Gjiri i Lalzit. Qëllimi i Cyber Camp është krijimi i një mjedisi te sigurt per femijet e te rinjte, nepermjet bashkepunimit te ngushte institucional, ndergjegjesimit dhe ngritjes se kapaciteteve profesionale dhe teknike.

AKCESK me qëllim rritjen e ndërgjegjësimit të shoqërisë për sigurinë kibernetike, duke përdorur hapësirat e duhura për realizimin e tyre, përfshirë edhe mediat audiovizive apo edhe ato sociale, ka hartuar materiale ndërgjegjësuese. Përgjatë vitit 2021 në zbatim të planit të komunikimit të Autoritetit u krye realizimi dhe publikimi i 4 videove promovuese për ndërgjegjësimin e komunitetit për rritjen e nivelit të sigurisë kibernetike nën moton **#ThinkCyber**:

a) Monitoro aksesin e fëmijës tend në internet

b) Aplikoni CYBER INSURANCE

c) Mbroni privatësinë tuaj online

d) Udhëzime për industrinë e mbrojtjes së fëmijëve në internet

Çdo muaj publikohet buletini i sigurisë kibernetike me lajme dhe eventet kryesore të zhvilluara ose organizuara nga Autoriteti.

AKCESK ka bashkëpunuar me partnerë ndërkombëtarë si: Qualys, EATM Cert, Shadowserver 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 si dhe nëpërmjet e-mailit zyrtar të institucionit për ata operatorë të cilët kanë hasur problem në aksesimin e sistemit.

Në realizimin e objektivave të kësaj politike është parashikuar një buxhet prej 5,256,000 lekë ku 4,183,200 lekë (80%) është realizuar dhe 1,072,800 lekë (20%) i parealizuar ende siç shihet në grafikun mëposhtë:

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

Qëllimi i politikës 3 është 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 Politikes 3, institucionet e përfshira në realizimin e PV raportojnë si më poshtë vijon:

Ministria e Arsimit, Sportit dhe Rinisë (MASR)

MASR në kuadër të qëllimit të politikës 1 dhe nënobjektivit 1 ka ndërmarrë hapa konkrete mbi hartimin 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.

Bazuar në dokumentin "Korniza Evropiane për kompetencën digjitale të mësuesve, DigComEdu1", në kornizën e kompetencës së TIK-ut për mësuesit (ICT CFT, version 3) nga UNESCO, ASCAP ka hartuar:

a) Modulet dhe materialet për trajnimin e mësuesve.
b) Qytetaria digjitale dhe siguria në internet në mjediset digjitale.

ASCAP ka hartuar dokumentin "Standardet profesionale të mësuesit për përdorimin e teknologjisë së informacionit dhe të komunikimit", ku në një pjesë të tij synohet kuptimi i parimeve themelore të sigurisë kibernetike, edukimit mediatik dhe informativ.

MASR në bashkëpunim me AKCESK kanë organizuar aktivite si "Siguria në internet" në shkollë, me qëllim sensibilizimin e komunitetit të shkollës mbi sigurinë në internet, të drejtat,

rreziqet dhe përgjegjësitë përmes performancës artistike, vizatime, ese, vjersha. Janë organizuar aktivitete në klasë, ku nxënësit bisedojnë me njëri-tjetrin, mësuesin dhe shërbimin psiko-social mbi përdorimin e internetit, bullizmin kibernetik (fletëpalosje) si dhe dhunën në shkollë. Gjatë ketyre aktiviteteve janë zhvilluar pyetësorë në lidhje me perceptimin e bullizmit, dhunës në shkollë nga nxënësit. Gjithashtu është bërë dhe shpërndarja e materialeve informuese tek prindërit dhe nxënësit për abuzimin dhe bullizmin online në shkolla.

Ministria e Arsimit, Sportit dhe Rinisë ka hartuar një rregullore shoqëruese në shkolla për mbledhjen e të dhënave të incidenteve të raportuara të dhunës, bullizmit dhe abuzimit online. Kjo rregullore e realizuar nga grupi i Mjedisit, Shëndetit dhe Sigurisë në bashkëpunim me Policimin në Komunitet mbi Strategjinë e Krimit Kibernetik, lehtëson identifikimin e rasteve të bullizmit në shkollë dhe online që në gjenezë, dhe parandalimi i tyre.

MASR gjithashtu ka hartuar një metodologji për mbledhjen se rasteve te incidenteve ne shkolla duke i njohur nxënësit me temë e krimit kibernetike dhe pasojat e tij:

- Si identifikohet krimi kibernetik?
- Pse është e nevojshme kërkimi i ndihmës në rast se je i sulmuar?
- Rruga ligjore sipas Kodit Penal të Republikës së Shqipërisë?
- Video sensibilizuese mbi bullizmin dhe krimin kibernetik, është realizuar për t'i ardhur në ndihmë nxënëseve duke parandaluar çdo rast mes tyre, duke i krijuar siguri, qetësi edhe në kushte shtëpie.

MASR mbledh raportet e institucionet arsimore vendore, përgjegjëse për arsimin Parauniversitar dh krijon një raport final mbi situatën në shkolla dhe si mund të përmirësohet.

MASR në kuadër të parandalimit të abuzimit seksual të fëmijëve në internet nëpërmjet rritjes së ndërgjëgjësimit dhe krijimit të hapësirave të sigurta për lundrimin në internet ka hartuar procedura për integrimin e programit "Edukatorët bashkëmoshatarë për sigurinë online" në shkollat 9-vjeçare. Ky program përfshin:

- diskutime në klasat e 8-ta dhe 9-ta për temën "Përdorimi i internetit në mënyrë të sigurte" me qëllim njohjen me pasojat e dhënies së passwordeve të adresave të miqve, shokëve/shoqeve, format e ndryshme të dhunës emocionale, psikologjike deri në pasoja të dhunës seksuale dhe të dhunës kibernetike.
- aktivitet "Njohja e të drejtave dhe përgjegjësive të fëmijëve në internet", për t`i pajisur ata me vlerat, qëndrimet dhe sjelljet si qytetarë të vendit tonë në rrjetet sociale përmes performancës artistike, vizatimeve, eseve dhe krijimeve të ndryshme.

Ministria e Arsimit, Sportit dhe Rinisë ka mbështetur krijimin e rrjetit online të mësuesve të TIK për të promovuar çështjen e mbrojtjes së fëmijëve në Internet. Rrjeti i mësuesve TIK online ndikon në ngritjen dhe funksionimin e rrjeteve profesionale për vitin shkollor 2021-2022. Cdo muaj organizohen takime të rrjeteve profesionale TIK. Aktualisht janë 1200 mësues të TIK-ut në rrjete profesionale, të cilët janë trajnuar në mënyrë të vazhdueshme nga specialistët e ASCAP-it, për udhëzuesin e funksionimit të rrjeteve, për planifikimin e punës vjetore të rrjeteve, për mënyrën

e raportimit, si dhe për tema përmbajtjesore si: trajnimi për mësuesit e TIK-ut; ekstremizmi i dhunshëm.

Përgjatë kësaj periudhe ka vazhduar trajnimi i mësuesve 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 në 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 efiçente në procesin mësimor. Mësuesit e shkollave janë përgatitur për të rritur sigurinë e fëmijëve nëpërmjet:

a) hartimit të rregullave në shkollë për të rritur sigurinë e fëmijëve në ambientet shkollore;
b) krijimit të videove nga nxënësit e shkollave për ndërgjegjësimin e sigurisë kibernetike;
c) krijimit të rrjeteve të diskutimit për cyber-bulling;
d) krijimit të forumeve për t'u ardhur në ndihmë fëmijëve që mund të jenë pre e çdo lloj dhune.

Në kuadër të zbatimit të projektit të bashkëpunimit midis Agjencisë së Sigurimit të Cilësisë së Arsimit Parauniversitar dhe Institutit Shqiptar të Medias janë trajnuar 123 mësues lidhur mbi Edukimin për Median dhe Informimin. Në kuadër të këtij trajnimi 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 përgjatë 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 t'i bëjnë ata të vetëdijshëm për sfidat dhe rreziqet që vijnë nga përdorimi i tij.

MASR 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 informimi në vijueshmëri i mësuesve të TIK për raportimin e incidenteve. Gjithashtu është vëndosur 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 ju vjen në ndihmë fëmijëve, personave që ushtrojnë përgjegjësinë prindërore të tyre dhe të rinjve, për të raportuar përmbajtje të paligjshme të hasura gjatë lundrimit të tyre në internet.

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

MASR gjithashtu kryen monitorimin e aplikimit të metodologjisë së hartuar me veprimtari praktike me nx. Kl. V-IX dhe X-XII për masat mbrojtëse dhe sigurinë kibernetike. Diskutim përvojash me stafin dhe grupe nxënësish. Krijimi i posterave dhe ese nga vetë nxënësit për rreziqet e kibernetike dhe siguria online. Implementimi i projekteve, në institucionet arsimore të AMU dhe AML, nga organizatat/shoqatat që kanë bashkëpunim me MAS.

Ministria e Shëndetësisë (MSH)

Ministria e Shëndetësisë me qëllim forcimin e bashkëpunimit ndërsektorial për mbrojtjen e fëmijëve në Internet ka ngritur një Komitet Teknik Këshillues për Sigurinë e Fëmijëve në Internet, pranë Këshillit Kombëtar për të Drejtat dhe Mbrojtjen e Fëmijëve (Min Shendetesise)

VKM Nr 659, datë 3.11.2021 "Agjenda Kombëtare për të Drejtat e Fëmijëve, 2021-2026)". Ky document ka si synim:

- Të ndikojë në jetën e fëmijëve, duke përmirësuar cilësinë e shërbimeve në të gjitha nivelet.
- Të promovojë një kulturë të të drejtave të fëmijëve dhe të vendosë themelet për pjesemarrjen kuptimplotë të fëmijëve në Shqipëri.
- Te mundësojë mbrojtjen nga të gjitha format e dhunës.
- Të sigurojë të dhëna cilësore për të përmirësuar politikat dhe programet e hartuara për to.
- Të realizojë edukimin për të mbrojtur fëmijët online, duke garantuar keshtu mirëqënien dhe një të ardhme më të mire për fëmijët.

Në realizimin e objektivave të kësaj politike është parashikuar një buxhet prej 3,858,000 lekë ku 856,400 lekë (22%) është realizuar dhe 3,001,600 lekë (78%) i parealizuar ende siç shihet në grafikun mëposhtë:

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

Qëllimi i politikës 4 është 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 Politikes 4, institucionet e përfshira në realizimin e PV raportojnë si më poshtë vijon:

Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK)

AKCESK në kuadër të rritjes, bashkëpunimit dhe koordinimit ndërmjet institucioneve shtetërore për të garantuar sigurinë në nivel kombëtar në hapësirën kibernetike ka hartuar dhe nënshkruar marrëveshje ndërinstitucionale duke krijuar kështu një rrjet pikash kontakti. Marrëveshjet qe mund të përmendim janë :

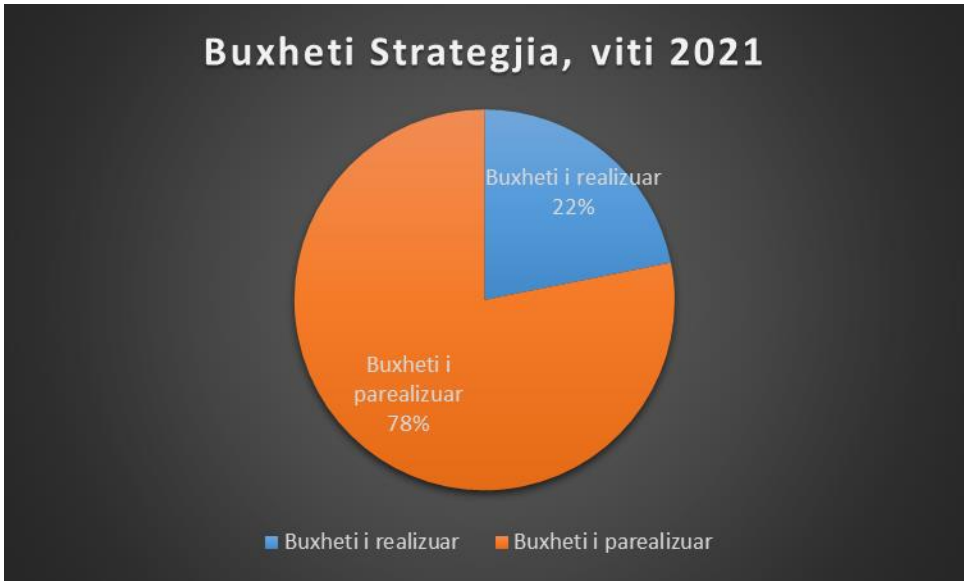
- Marrëveshje Bashkëpunimi me Autoritetin E Mediave Audiovzive Dhe Qendrën E Koordinimit Kundër Ekstremizmit Te Dhunshëm)
- Marrëveshje Bashkëpunimi me Maqedoninë (MKD-CIRT)
- Marrëveshje Bashkëpunimi me Kosovën (KOS-CERT)
- Marrëveshje Bashkëpunimi me Rumanine (CERT-RO)
- Marrëveshje Bashkëpunimi me AKEP

Si ura komunikimi për bashkëpunimin dhe forcimin e besimit me ekipet e tjera publike dhe private të CERT dhe CSIRT, dhe komunitetet akademike kanë shërbyer takimet dhe trajnimet në nivel vendas dhe rajonal. Ekspertët e fushës së sigurisë kibernetike kanë punuar për krijimin e një instrumenti për shkëmbimin e informacionit përmes pikave të kontaktit të dedikuara nga institucionet përkatëse, në raste të kërcënimeve kibernetike.

AKCESK në kuadër të forcimit të bashkëpunimit ndërkombëtar në fushën e sigurisë dhe mbrojtjes kibernetike dhe luftës kundër ekstremizmit të dhunshëm dhe radikalizimit ka patur pjesëmarrje aktive në takimet e NATO 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 tjerë ndërkombëtarë. Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike është anëtarësuar në aktivitete dhe iniciativa të ndryshme ndërkombëtare në fushën e sigurisë kibernetike (si psh. First, Trust Introducer).

Në realizimin e objektivave të kësaj politike është parashikuar një buxhet prej 2,408,400 lekë ku 2,190,000 lekë (91%) është realizuar dhe 218,400 lekë (9%) i parealizuar ende siç shihet në grafikun mëposhtë:

Në total, Plani i Veprimit të Strategjisë Kombëtare për Sigurinë Kibernetike 2020-2025, ka parashikuar një buxhet total për vitin 2021 prej rreth 339,321,408 lekë. Gjatë monitorimit të Strategjisë nga Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike, buxheti i realizuar gjatë vitit 2021 është 74,187,008 lekë (22%) si në grafikun mëposhtë:



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 treguesve e nivelit të Rezultatit që janë të përfshira në Strategjinë Kombëtare për Sigurinë Kibernetike 2020-2025.

Dokumenti mbulon vetëm e ashtuquajtura të tregues të nivelit të Rezultatit (ose Performancës), ato 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 tëjashtëm 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 ANEX 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 (per sigurine online te femijeve)
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

- ✓ Hartimi i metodologjisë për të realizuar vlerësimin kombëtar të rrezikut kibernetik.
- ✓ Hartimi i procedurës për menaxhimin e krizave kibernetike.
- ✓ Rishikimi i Strategjisë Kombëtare të Sigurisë Kibernetike, duke siguruar përfshirjen e vazhdueshme të palëve të interesuara.
- ✓ Ngritja e një forumi ekspertësh për sigurinë kibernetike në nivel kombëtar.
- ✓ Forcimi dhe promovimi i bashkëpunimit ndër-sektorial në sigurinë kibernetike për të siguruar zbatimin e plotë të programeve të sigurisë kibernetike.

- ✓ Organizimi i 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.

ANEX 1

Emërtimi I indikatorit	**Legjislacion i përafruar me Direktivat dhe Rregulloret e EU 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 shtylles)	Shtylla Nr.2. QEVERISJA E MIRË, DEMOKRACIA DHE SHTETI I SË DREJTËS	
Qëllimi/Objektivi Strategjik ne SKZHI	Qellimi 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 perfshire, por pa u kufizuar: Cloud computing, IoT, teknologjine 5G, Inteligjencen Artificiale	
Perkatesia e Indikatorit	Kuader Politikash	
Lidhja me Acquis Communautaire	NIS directive 2016	
Burimi i të dhënave për monitorimin e treguesit të performancës	Akte te miratuara nga KM	
Institucionet përgjegjëse për grumbullimin e të dhënave	AKCESK	
	AKSHI/MB/etj	
Përshkrimi I Metodologjisë	1) Kuadri strategjik rregullator i hartuar perkundrejt kuadrit rregullator te miratuar 2) Kuadri strategjik i zbatuar, niveli mesatar i raportit te zbatimit	
Frekuenca e Matjes	Vjetore	
	Vjetore	
Natyra e Indikatorit/treguesit: Kumulativ/Rrites	Kumulativ	
Input Direkt ose i Përbërë	I perbere	
Formula e llogaritjes	1) kuader i planifikuar perkundrejt kuadrit strategjik te miratuar	
Ndarja e të dhënave (per treguesit e perbere)	Niveli I pare	
	Niveli I dyte	
	Niveli I trete	
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 ligje
	2023	
	2024	
	2025	Perafrim i plote
Vlera e synuar/Targeti i rishikuar:	2025	100%
Vlera aktuale baze:		
SDG - Titulli i Qellimit të Zhvillimit të Qëndrueshëm sipas OKB-së	N/A	N/A
Vlera e Synuar e treguesit te SDG	N/A	N/A

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	Qellimi 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	Ngritja dhe funksionimi i CSIRT-eve në të gjithë sektorët e industrisë në nivel kombëtar	
Perkatesia e Indikatorit	Masa zbatuese	
Lidhja me Acquis Communautaire	NIS directive 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 se auditimit te AKCESK	
Frekuenca e Matjes	Vjetore	
	Vjetore	
Natyra e Indikatorit/treguesit: Kumulativ/Rrites	Rrites	
Input Direkt ose i Përbërë	Direkt	
Formula e llogaritjes		
Ndarja e të dhënave (per treguesit e perbere)	Niveli I pare	
	Niveli I dyte	
	Niveli I trete	
Theksoni drejtimin e ndryshimit / trendit (tendences) të ecurisë	Rrites	
Vlerat Bazë		
	Mungojne statistikat	
Vlera e synuar/ Targeti	2021-	1- CSIRT kombetare operacional
	2022-	CSIRT sektoriale
	2023-	
	2024-	
	2025-	CSIRT-e operacionale
Vlera e synuar/Targeti i rishikuar:	2025	100%
Vlera aktuale baze:		
SDG - Titulli i Qellimit të Zhvillimit të Qëndrueshëm sipas OKB-së	N/A	N/A
Vlera e Synuar e treguesit te SDG	N/A	N/A

Emërtimi I indikatorit	**Ngritja e kapaciteteve të profesionistëve të fushës**	
Lloji I indikatorit	Tregues rezultati	
Nr Dt Emertimi I Dokumentit	"Strategjia Kombëtare për Sigurinë Kibernetike 2020-2025"	
Lidhja me SKZHI (Nr shtylles)	Shtylla Nr.5. INVESTIMI NË KAPITAL NJERËZOR DHE KOHEZION SOCIAL	
Qëllimi/Objektivi Strategjik ne SKZHI	Qellimi 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 te cilin lidhet indikatori/treguesi	Rritja e kapaciteteve profesionale në fushën e sigurisë së informacionit nëpërmjet rishikimit të kurrikulave arsimore	
Perkatesia e Indikatorit	Masa zbatuese	
Lidhja me Acquis Communautaire	NIS directive 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 ne monitorim vjetor	
Frekuenca e Matjes	Vjetore	
	Vjetore	
Natyra e Indikatorit/treguesit: Kumulativ/Rrites	Rrites	
Input Direkt ose i Përbërë	Direkt	
Formula e llogaritjes		
Ndarja e të dhënave (per treguesit e perbere)	Nr kurrikulash	
	Nr Kursesh	
	Nr te trajnuarish	
Theksoni drejtimin e ndryshimit / trendit (tendences) të ecurisë	Rrites	
Vlerat Bazë		
Vlera e synuar/ Targeti	2021-	25 profesioniste te trajnuar te sektorit financiar dhe 20 profesioniste te sektorit shendetesor
	2022-	
	2023-	
	2024-	
	2025-	
Vlera e synuar/Targeti i rishikuar:		
Vlera aktuale baze:		
SDG - Titulli i Qellimit të Zhvillimit të Qëndrueshëm sipas OKB-së	N/A	N/A
Vlera e Synuar e treguesit te SDG	N/A	N/A

Emërtimi I indikatorit	**Fushata ndërgjegjësimi për sigurinë kibernetike**	
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	Qellimi 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 te cilin lidhet indikatori/treguesi	Rritje e ndërgjegjësimit të shoqërisë, për sigurinë kibernetike dhe kërcënimet kibernetike.	
Perkatesia e Indikatorit	Masa zbatuese	
Lidhja me Acquis Communautaire	NIS directive 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/Rrites	Kumulativ	
Input Direkt ose i Përbërë	Direkt	
Formula e llogaritjes		
Ndarja e të dhënave (per treguesit e perbere)	Nr kurrikulash	
	Nr Kursesh	
	Nr te trajnuarish	
Theksoni drejtimin e ndryshimit / trendit (tendences) të ecurisë	Rrites	
Vlerat Bazë	Mungojne 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 baze:		
SDG - Titulli i Qellimit të Zhvillimit të Qëndrueshëm sipas OKB-së	N/A	N/A
Vlera e Synuar e treguesit te SDG	N/A	N/A

Emërtimi I indikatorit	**Kuadër ligjor I plotësuar (per sigurine online te femijeve)**	
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	Qellimi 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 te cilin lidhet indikatori/treguesi	Forcimi i kuadrit ligjor për rritjen e sigurisë së fëmijëve në Internet.	
Perkatesia e Indikatorit	Kuader politikash	
Lidhja me Acquis Communautaire		
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/Rrites	Kumulativ	
Input Direkt ose i Përbërë	I përbërë	
Formula e llogaritjes		
Ndarja e të dhënave (per treguesit e perbere)	Akte ligjore te rishikuara	
	Rregullore e miratuar	
	Metodologji	
Theksoni drejtimin e ndryshimit / trendit (tendences) të ecurisë	Rrites	
Vlerat Bazë		
Vlera e synuar/ Targeti	2020-	10%
	2021-	
	2022-	50%
	2023-	
	2024-	
	2025-	100%
Vlera e synuar/Targeti i rishikuar:		
Vlera aktuale baze:		
SDG - Titulli i Qellimit të Zhvillimit të Qëndrueshëm sipas OKB-së	N/A	N/A
Vlera e Synuar e treguesit te SDG	N/A	N/A

Emërtimi I indikatorit	**Fëmijë të trajnuar e ndërgjegjësuar në përdorimin e materialeve online**	
Lloji I indikatorit	Tregues rezultati	
Nr Dt Emertimi I Dokumentit	"Strategjia Kombëtare për Sigurinë Kibernetike 2020-2025"	
Lidhja me SKZHI (Nr shtylles)	Shtylla Nr.5. INVESTIMI NË KAPITAL NJERËZOR DHE KOHEZION SOCIAL	
Qëllimi/Objektivi Strategjik ne SKZHI	Qellimi 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 te cilin lidhet indikatori/treguesi	Rritja e ndërgjegjësimit dhe edukimi tek të gjitha segmentet e shoqërisë për përdorimin e sigurtë të Internetit nga fëmijët	
Perkatesia e Indikatorit	Masa zbatuese	
Lidhja me Acquis Communautaire		
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/Rrites	Kumulativ	
Input Direkt ose i Përbërë	Direkt	
Formula e llogaritjes		
Ndarja e të dhënave (per treguesit e perbere)	Nxënës të trajnuar	
	Mësues të trajnuar	
	Magjistratë të trajnuar	
Theksoni drejtimin e ndryshimit / trendit (tendences) të ecurisë	Rrites	
Vlerat Bazë	2019	
	13000 nxenes te 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 baze:	2021	1600
SDG - Titulli i Qellimit të Zhvillimit të Qëndrueshëm sipas OKB-së	N/A	N/A
Vlera e Synuar e treguesit te SDG	N/A	N/A

Emërtimi I indikatorit	**Forcimi I bashkëpunimit në nivel kombëtar për të garantuar sigurinë kibernetike në vend.**	
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	Qellimi 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 te cilin lidhet indikatori/treguesi	Forcimi i bashkëpunimit institucional në nivel kombëtar	
Perkatesia e Indikatorit	Masa zbatuese	
Lidhja me Acquis Communautaire	NIS directive	
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/Rrites	Kumulativ	
Input Direkt ose i Përbërë	Direkt	
Formula e llogaritjes		
Ndarja e të dhënave (per treguesit e perbere)		
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 baze:		
SDG - Titulli i Qellimit të Zhvillimit të Qëndrueshëm sipas OKB-së	N/A	N/A
Vlera e Synuar e treguesit te SDG	N/A	N/A

Emërtimi I indikatorit	**Bashkëpunimi ndërkombëtar**	
Lloji I indikatorit	Tregues rezultati	
Nr Dt Emertimi I Dokumentit	"Strategjia Kombëtare për Sigurinë Kibernetike 2020-2025"	
Lidhja me SKZHI (Nr shtylles)	Shtylla Nr.1 - Anëtarsim në BE	
Qëllimi/Objektivi Strategjik ne SKZHI	Qellimi 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 te cilin lidhet indikatori/treguesi	Forcimi i bashkëpunimit ndërkombëtar në fushën e sigurisë dhe mbrojtjes kibernetike dhe luftës kundër ekstremizmit të dhunshëm dhe radikalizimit.	
Perkatesia e Indikatorit	Masa zbatuese	
Lidhja me Acquis Communautaire	NIS directive	
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/Rrites	Kumulativ	
Input Direkt ose i Përbërë	Direkt	
Formula e llogaritjes		
Ndarja e të dhënave (per treguesit e perbere)		
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 baze:	2021	2
SDG - Titulli i Qellimit të Zhvillimit të Qëndrueshëm sipas OKB-së	N/A	N/A
Vlera e Synuar e treguesit te SDG	N/A	N/A