STRATEGJIA KOMBËTARE PËR SIGURINË KIBERNETIKE
2025 -2030

Përmbajtja

PJESA I: KONTEKSTI STRATEGJIK

1. Hyrje

Në një periudhë ku transformimi digjital po ndikon thellësisht në të gjitha aspektet e jetës shoqërore, ekonomike dhe institucionale, siguria kibernetike ka marrë një rëndësi të jashtëzakonshme kudo në botë. Shqipëria, si pjesë e pandashme e ekosistemit global të informacionit, është e angazhuar të përballet me sfidat dhe të përqafoj mundësitë që ofron hapësira kibernetike, për të siguruar një mjedis digjital të sigurt dhe të besueshëm për qytetarët, bizneset dhe institucionet e saj.

Strategjia Kombëtare për Sigurinë Kibernetike 2025-2030 është një dokument i rendesishem që pasqyron këtë angazhim dhe përcakton drejtimet strategjike për zhvillimin dhe forcimin e sigurisë kibernetike në Shqipëri.

Kjo strategji ka si qëllim kryesor forcimin e kapaciteteve kombëtare për të identifikuar, parandaluar dhe menaxhuar kërcënimet kibernetike, duke përfshirë mbrojtjen e infrastrukturave kritike dhe të rëndësishme të informacionit, mbrojtjen e të dhënave sensitive dhe garantimin e vazhdimësisë së shërbimeve digjitale. Ajo gjithashtu synon rritjen e kapaciteteve teknike dhe profesionale të nevojshme për t'u përballur me sfidat e vazhdueshme për mbrojtjen e hapësirës digjitale dhe promovimin e bashkëpunimit ndërkombëtar për të përmirësuar efikasitetin dhe reagimin ndaj incidenteve kibernetike.

Strategjia vendos një kornizë për të rritur gatishmërinë dhe qëndrueshmërinë e sistemeve dhe shërbimeve të informacionit në vend, duke siguruar që Shqipëria të përmbushë standardet dhe praktikat më të mira ndërkombëtare në këtë fushë. Ajo reflekton harmonizimin e politikave të sigurisë kibernetike me ato të Bashkimit Evropian dhe partnerëve ndërkombëtarë, për të mbështetur zhvillimin e qëndrueshëm të infrastrukturave të informacionit dhe ekonomisë digjitale të vendit.

Një aspekt i rëndësishëm i kësaj strategjie është angazhimi i të gjithë aktorëve si: institucionet shtetërore, sektori privat, shoqëria civile dhe akademia, për të krijuar një ekosistem të koordinuar dhe gjithëpërfshirës të sigurisë kibernetike. Kjo do të mundësojë ndarjen e informacionit dhe burimeve, zhvillimin e politikave të përbashkëta dhe rritjen e ndërgjegjësimit rreth rreziqeve dhe masave të sigurisë.

2. Vlerësimi i Situatës Aktuale në Shqipëri

Në një kohë kur Shqipëria po implementon çdo ditë e më shumë teknologjitë e informacionit dhe komunikimit në çdo fushë të jetës, edhe rreziqet e sigurisë kibernetike po evoluojnë me shpejtësi. Tendencat globale tregojnë një rritje të sulmeve kibernetike, të nxitura nga subjekte të sponsorizuara nga shtete, organizata kriminale dhe grupe keqbërëse. Shteti, ekonomia dhe qeveria shqiptare përballen me kërcënime të vazhdueshme kibernetike, që kërkojnë vëmendje të menjëhershme për të mbrojtur infrastrukturën kritike, rrjetet e sektorit publik dhe të dhënat e qytetarëve.

Në Shqipëri, janë bërë hapa të rëndësishëm për forcimin e sigurisë kibernetike. Krijimi i strategjisë kombëtare për sigurinë kibernetike vendosi një kornizë të qartë për mbrojtjen e infrastrukturave kritike dhe menaxhimin e rreziqeve kibernetike. Autoriteti Kombëtar për Sigurinë Kibernetike fuqizoi dhe përmirësoi ndjeshëm proceset e monitorimit, vlerësimit të rreziqeve dhe menaxhimit të kërcënimeve. Disa nga arritjet më të rëndësishme në nivel kombëtar janë rritja e nivelit të zbatimit të masave të sigurisë në infrastrukturat kritike si dhe rritja e kapaciteteve teknike të ekspertëve nëpërmjet trajnimeve dhe kontrolleve rigoroze.
Shqipëria ka intensifikuar ndjeshëm bashkëpunimin me organizata ndërkombëtare si NATO dhe Bashkimi Evropian, duke siguruar përputhshmëri me normat ndërkombëtare. Përveç kësaj, janë ndërmarrë hapa për rritjen e ndërgjegjësimit dhe edukimit të qytetarëve dhe bizneseve mbi sigurinë kibernetike. Shqipëria ka harmonizuar legjislacionin e saj me direktivat e Bashkimit Evropian, duke forcuar kështu mbrojtjen kibernetike në nivel kombëtar dhe ndërkombëtar.
Sulmet kibernetike të viteve të fundit kanë theksuar rëndësinë e përmirësimit të proceseve të standardizuara për reagimin ndaj incidenteve, përforcimin e kapaciteteve për monitorimin e rrjetit dhe zhvillimin e mekanizmave të qendërzuar për ndarjen efektive të informacionit mbi kërcënimet.
Për më tepër, në Indeksin Global të Sigurisë Kibernetike 2024, Shqipëria ka shënuar një progres të jashtëzakonshëm, duke u ngjitur me 23 vende në renditjen globale, nga vendi i 80-të në vendin e 57-të, dhe duke avancuar nga vendi i 40-të në atë 30-të në Evropë, ku renditet në grupin "Tier 2", që përfshin vendet me avancim të shpejtë në sigurinë digjitale.
Në këtë drejtim, Shqipëria është e angazhuar të ndërtojë një hapësirë digjitale të sigurt dhe të besueshme për qytetarët dhe bizneset, duke fuqizuar qëndrueshmërinë kibernetike të vendit, përshpejtuar procesin e integrimit në Bashkimin Evropian dhe duke u pozicionuar si një aktor i fuqishëm dhe i besueshëm në epokën digjitale globale.
Pavarësisht progresit të konsiderueshëm që Shqipëria ka arritur në fushën e sigurisë kibernetike, ende mbeten shumë detyra për t'u realizuar. Sfidat e sigurisë kibernetike bëhen edhe më të mëdha si pasojë e rritjes së vazhdueshme të numrit të sulmeve kibernetike, si dhe nga niveli i lartë dhe sofistikuar i këtyre sulmeve, të cilat shfrytëzojnë teknologjitë më të avancuara. Objektivat e këtyre sulmeve po bëhen gjithnjë e më të gjera, duke përfshirë jo vetëm sektorin publik, por edhe shërbime jetike, si shëndetësia, financat, transporti dhe energjia.
Përdorimi i internetit për përhapjen e ideologjive ekstremiste dhe rekrutimin e individëve për qëllime terroriste është një kërcënim në rritje, duke bërë që parandalimi i këtyre aktiviteteve të jetë gjithnjë e më i komplikuar. Në këtë kontekst, siguria kombëtare e Shqipërisë është e lidhur ngushtë me aftësinë për të identifikuar, parandaluar dhe reaguar ndaj kërcënimeve kibernetike dhe atyre fizike që lidhen me terrorizmin. Një aspekt kyç i kësaj strategjie është zhvillimi i strukturave të inteligjencës që janë të specializuara për të monitoruar dhe parandaluar aktivitete ekstremiste dhe terroriste në hapësirën kibernetike. Në kuadër të luftës kundër terrorizmit, një fokus i rëndësishëm është parandalimi i propagandës ekstremiste dhe rekrutimit online. Kjo përfshin përdorimin e teknologjive të avancuara për të identifikuar dhe mbyllur faqe dhe përmbajtje që promovojnë dhunën dhe radikalizimin, si dhe krijimin e mekanizmave të bashkëpunimit me aktorët ndërkombëtarë dhe platformat online.
Gjithashtu, faktorët socialë po ndikojnë gjithnjë e më shumë, përfshirë bullizmin online, shfrytëzimin e fëmijëve dhe grupeve vulnerabël të shoqërisë, si dhe sulmet ndaj organizatave

dhe individëve me qëllim dizinformimin dhe përfitimet financiare përmes shkatërrimit të reputacionit, si në nivelin personal ashtu edhe në atë profesional.

3. Vizioni dhe Misioni

3.1 Vizioni

Strategjia Kombëtare për Sigurinë Kibernetike 2025-2030 ka si vizion garantimin e një ekosistemi digjital të sigurt, të qëndrueshëm dhe gjithëpërfshirës që nxit besimin, inovacionin dhe përparimin ekonomik të vendit.

Duke përqafuar transformimin digjital përmes aplikimit të teknologjive të avancuara si inteligjenca artificiale, superkompjuterat, blockchain, strategjia synon forcimin e pozicionit të Shqipërisë si lider në sigurinë kibernetike në rajon dhe integrimin me politikat dhe kornizën ligjore e rregullatore të Bashkimit Evropian.

Përtej mbrojtjes teknike, ky vizion reflekton një angazhim më të gjerë për të mbështetur zhvillimin politik, social dhe ekonomik të vendit, që promovon bashkëpunimin midis institucioneve, sektorit privat dhe partnerëve ndërkombëtarë, duke krijuar një qasje të unifikuar për adresimin e kërcënimeve dhe mundësive të reja në epokën digjitale.
Nëpërmjet kësaj strategjie, Shqipëria synon jo vetëm të mbrojë hapësirën e saj digjitale, por edhe të krijojë një kulturë të përgjegjësisë dhe ndërgjegjësimit për sigurinë kibernetike. Ky angazhim gjithëpërfshirës do të përmirësojë qëndrueshmërinë e vendit ndaj sfidave të vazhdueshme, duke e bërë Shqipërinë një model për qasje të avancuara në sigurinë kibernetike në rajon dhe më gjerë.

3.2 Misioni

Misioni i Strategjisë Kombëtare të Sigurisë Kibernetike 2025-2030 është krijimi i një mburoje të fortë dhe gjithëpërfshirëse për të mbrojtur qytetarët, institucionet dhe infrastrukturat kritike të Shqipërisë nga kërcënimet e vazhdueshme dhe në zhvillim të hapësirës kibernetike. Kjo strategji synon të konsolidojë një kuadër të avancuar ligjor, teknik dhe organizativ, të përputhur me standardet evropiane dhe ndërkombëtare, për të garantuar siguri të qëndrueshme dhe zhvillim të ekosistemit digjital kombëtar.
Duke ndërtuar një mjedis të sigurt digjital, kjo strategji synon të fuqizojë qytetarët dhe të krijojë kushte për një shoqëri ku teknologjia shërben si katalizator i inovacionit dhe progresit. Përmes mbështetjes së një zhvillimi të qëndrueshëm ekonomik dhe shoqëror, strategjia jo vetëm që mbron interesat kombëtare, por gjithashtu promovon konkurrencën dhe aftësinë e Shqipërisë për të luajtur një rol të rëndësishëm në transformimin digjital të rajonit dhe më gjerë. Misioni thekson gjithashtu rëndësinë e bashkëpunimit ndërinstitucional dhe ndërkombëtar për adresimin e sfidave komplekse të sigurisë kibernetike. Ai bazohet në një angazhim për krijimin e një kulture të përgjegjshmërisë kibernetike, duke përfshirë rritjen e ndërgjegjësimit publik dhe ndërtimin e kapaciteteve teknike dhe burimeve njerëzore. Nëpërmjet kësaj strategjie, Shqipëria synon jo vetëm të përballojë kërcënimet kibernetike të së tashmes, por edhe të ndërtojë një themel të fortë për mbrojtjen dhe zhvillimin e sigurt të hapësirës digjitale të së ardhmes.

PJESA II QËLLIMI I POLITIKAVE DHE OBJEKTIVAT SPECIFIKE TË STRATEGJISË

Objektivat e Strategjisë Kombëtare të Sigurisë Kibernetike 2025–2030 fokusohen në forcimin e mbrojtjes së infrastrukturave kritike dhe të rëndësishme të vendit, duke krijuar një kuadër ligjor dhe teknik që siguron vazhdimësinë e shërbimeve dhe stabilitetin e sistemeve të informacionit.
Strategjia synon përmirësimin e bashkëpunimit ndërmjet sektorit publik, privat dhe aktorëve të tjerë për të rritur kapacitetet mbrojtëse dhe për të mundësuar shkëmbimin e informacionit të rëndësishëm në menaxhimin e incidenteve kibernetike.
Një tjetër objektiv kyç është zhvillimi i kapaciteteve teknike dhe profesionale për të përballuar kërcënimet kibernetike, duke investuar në zhvillimin e aftësive dhe në teknologji të avancuara. Për më tepër, strategjia promovon inovacionin dhe kërkimin shkencor për të përmirësuar aftësitë me qëllim parashikimin, menaxhimin dhe reagimin ndaj sulmeve kibernetike, si dhe rritjen e ndërgjegjësimit dhe edukimit të shoqërisë mbi sigurinë kibernetike.
Në këtë kuadër, strategjia ka për qëllim përputhshmërinë me normat dhe direktivat e Bashkimit Evropian dhe forcimin e bashkëpunimit me partnerët ndërkombëtarë për të adresuar kërcënimet e sofistikuara dhe ato hibride që mund të cënojnë sigurinë kombëtare dhe stabilitetin digjital të vendit.

Politikat

Strategjia Kombëtare Për Sigurinë Kibernetike të Shqipërisë 2025-2030 është ndërtuar mbi pesë politika kryesore, ku ***Mbrojtja e Infrastrukturës Digjitale*** përbën politikën kryesore të gjithë strategjisë Zhvillimet e sigurisë kibernetike, të cilat janë të lidhura ngushtësisht me përparimet teknologjike, ekonomike dhe gjeopolitike, rritja e bashkëpunimeve ndërkombëtare, si dhe kërcënimet kibernetike të sofistikuara, kërkojnë një strategji kombëtare të sigurisë kibernetike dinamike dhe të aftë të përshtatet ndaj ndryshimeve të shpejta në mjedisin digjital.

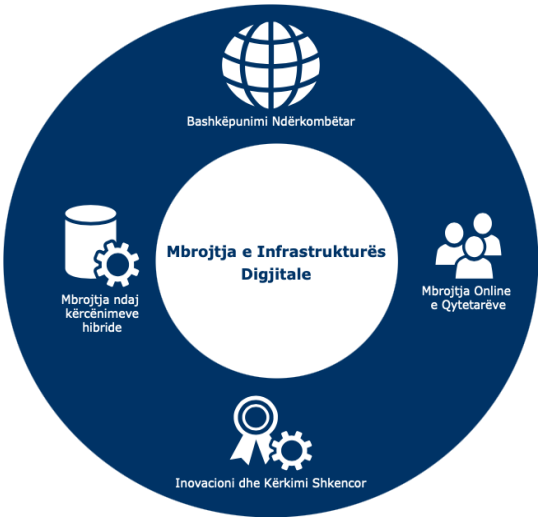

Figura 1. Politikat e Strategjisë

- Strategjia shoqërohet nga një plan veprimi që përcakton aktivitetet konkrete për implementimin e saj, duke synuar realizimin e objektivave të përcaktuara. Ky plan

veprimi specifikon hapa të qartë dhe afate kohore për secilën fazë të procesit. *Qëllimi i politikës 1*: **Mbrojtja e Infrastrukturës Digjitale**: Baza e Strategjisë Kombëtare të Sigurisë Kibernetike është mbrojtja e infrastrukturave kritike dhe të rëndësishme të vendit, që përfshin rrjetet, sistemet dhe shërbimet që mbështesin funksionimin e shtetit dhe jetën e përditshme të qytetarëve. Kjo politikë ka për qëllim sigurimin e vazhdimësisë së shërbimeve dhe mbrojtjen e sistemeve të informacionit që mbajnë në funksion energjinë, transportin, shëndetësinë, financat, administratën publike dhe sektorë të tjerë kyç. Pjesë e kësaj politike janë masat parandaluese dhe mbrojtëse për identifikimin dhe minimizimin e rreziqeve, si dhe zhvillimi i mekanizmave të reagimit të shpejtë në rastet e incidenteve kibernetike.

- *Qëllimi i politikës 2*: **Mbrojtja *online* e qytetareve dhe nxitja e kulturës kibernetike.** Krijimi dhe nxitja e një kulture ndërgjegjësimi për sigurinë kibernetike në të gjitha grupet e shoqërisë janë elemente thelbësore për këtë strategji. Ndërgjegjësimi promovon përgjegjësi të përbashkët. Një qytetar i ndërgjegjshëm kontribuon në një zinxhir më të sigurt në shoqëri, duke minimizuar dobësitë që mund të shfrytëzohen nga sulmuesit. Edukimi dhe ndërgjegjësimi i publikut është një proces i vazhdueshëm që synon të pajisë qytetarët me njohuri dhe mjete praktike për të adresuar sfidat aktuale dhe për të marrë vendime të informuara. Një shoqëri e informuar ka mundësi të kontribuojë në debatin publik dhe të nxisë për politika më të mira. Po ashtu, është e rëndësishme të promovohet etika kibernetike dhe respektimi i rregullave edukative në internet, si dhe parandalimi i radikalizmit online, duke promovuar përdorimin e një gjuhe të respektueshme dhe të përgjegjshme.
  Strategjia Kombëtare e Sigurisë Kibernetike 2025-2030 ka në fokus krijimin e mekanizmave të nevojshëm për mbrojtjen online të qytetarëve veçanërisht mbrojtjen e fëmijëve dhe të rinjve dhe grupeve të nënpërfaqësuara.
- *Qëllimi i politikës 3:* **Forcimi i Bashkëpunimit Ndërkombëtar**: Siguria kibernetike është një sfidë ndërkombëtare dhe një përpjekje e përbashkët për të adresuar sfidat që lidhen me kërcënimet dhe rreziqet në mjedisin digjital. Strategjia promovon forcimin e bashkëpunimit ndërmjet institucioneve dhe partnerëve ndërkombëtarë, duke nxitur shkëmbimin e informacionit, zhvillimin e kapaciteteve të përbashkëta dhe krijimin e standardeve të unifikuara, duke siguruar një mbrojtje kolektive dhe më efektive kundër kërcënimeve kibernetike. Në këtë kuadër, Shqipëria angazhohet për të kontribuar aktivisht në nismat dhe marrëveshjet ndërkombëtare për sigurinë kibernetike, duke forcuar kështu qëndrueshmërinë e mjedisit digjital global.
- *Qëllimi i politikës 4*: **Nxitja e inovacionit dhe kërkimit shkencor**: Strategjia Kombëtare për Sigurinë Kibernetike përqafon përdorimin e teknologjive më të avancuara, përfshirë inteligjencën artificiale, *blockchain* dhe llogaritjen kuantike, për të përforcuar mbrojtjen kibernetike dhe për të adresuar sfidat komplekse të një mjedisi digjital gjithnjë e më të ndërlikuar. Inovacioni është një shtyllë thelbësore që kontribuon në përmirësimin e protokolleve të përparuara të sigurisë, zbulimin e hershëm të kërcënimeve dhe garantimin e qëndrueshmërisë së ekosistemit digjital. Kërkimi shkencor dhe adoptimi i teknologjive të reja rrisin aftësinë strategjike të Shqipërisë për t'u përballur me kërcënimet kibernetike në mënyrë efikase, duke siguruar një mjedis digjital të besueshëm dhe të qëndrueshëm.

- *Qëllimi i politikës 5:* **Mbrojtja ndaj kërcënimeve hibride**: Për të frenuar kërcënimet hibride të natyrës komplekse, që shfrytëzojnë dobësitë në fushat kibernetike, Shqipëria po harton një strategji mbrojtëse proaktive, të qëndrueshme dhe të përshtatshme. Një nga politikat kyçe të kësaj strategjie është mbrojtja ndaj kërcënimeve hibride. Këto kërcënime përfshijnë aktivitete të dëmshme që kombinojnë sulme kibernetike me veprime të tjera si, manipulimi i informacionit , ndikimi ekonomik, manovrat politike, diplomacia shtrënguese dhe kërcënimet ushtarake. Objektivi i kësaj politike është të identifikohen dhe neutralizohen kërcënimet hibride përmes forcimit të kapaciteteve mbrojtëse, përmirësimit të bashkëpunimit ndërmjet institucioneve dhe partnerëve ndërkombëtarë, dhe zhvillimit të mekanizmave të shpejtë reagimi, për të ruajtur sigurinë kombëtare dhe integritetin e infrastrukturave kritike.

Qëllimi i politikës 1: Mbrojtja e Infrastrukturës Digjitale

Mbrojtja e Infrastrukturës Digjitale është politika kryesore e Strategjisë Kombëtare për Sigurinë Kibernetike të Shqipërisë 2025 - 2030. Sigurimi i sistemeve të informacionit, rrjeteve të komunikimit dhe aseteve të infrastrukturës kritike dhe të rëndësishme të informacionit është thelbësor për sigurinë kombëtare, publike dhe stabilitetin ekonomik.
Qëllimi i mbrojtjes së infrastrukturës digjitale synon të krijojë një model të qëndrueshëm dhe efektiv të mbrojtjes së përbashkët që shpërndan përgjegjësitë dhe menaxhon rrezikun duke ofruar një nivel të lartë sigurie dhe qëndrueshmërie për ekosistemin digjital.
Adresimi dhe trajtimi i kërcënimeve kibernetike do të jetë i suksesshëm vetëm nëse operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit kanë bashkëpunimin dhe ndërgjegjësimin e nevojshëm për rëndësinë e zbatimit të masave të sigurisë kibernetike.
Në mbështetje të objektivit kryesor të kësaj shtylle për sigurimin dhe mbrojtjen sistemeve te informacionit dhe rrjeteve të komunikimit përmes garantimit të disponueshmërisë, integritetit dhe konfidencialitetit të të dhënave, Shqipëria angazhohet të ndërmarrë nisma të plota dhe të koordinuara, që përfshijnë trajtimin e sfidave në:

- Procese
- Teknologji
- Kapacitete Njerëzore

1. Proceset

Proceset luajnë një rol kryesor në Strategjinë Kombëtare për Sigurinë Kibernetike.
Proceset përfshijnë një sërë hapash të ndërlidhura dhe të koordinuara që kanë për qëllim mbrojtjen e aseteve digjitale, sistemeve të informacionit dhe rrjeteve të komunikimit nga kërcënimet dhe sulmet kibernetike. Ato përcaktojnë se si një infrastrukturë digjitale ndërvepron me të gjitha aspektet e sigurisë kibernetike duke përfshirë praktika:

- të qarta dhe të mirë dokumentuara në përcaktimin e roleve dhe përgjegjësive;
- dinamika ndaj kërcënimeve hibride;
- të vazhdueshme dhe adoptuese drejt maturitetit të posturës së sigurisë kibernetike të infrastrukturës.

Objektivi specifik 1.1 : Hartimi dhe zbatimi i kuadrit ligjor për Sigurinë Kibernetike

Ky objektiv përfshin procesin e harmonizimit të standardeve dhe direktivave ndërkombëtare në hartimin e legjislacionit dhe kuadrit rregullator që përcaktojnë mënyrën e menaxhimit të sigurisë kibernetike në nivel kombëtar. Qëllimi i këtij objektivi është të sigurohet një mbrojtje efektive ndaj kërcënimeve dhe sulmeve kibernetike duke u përputhur me kërkesat e sigurisë dhe nevojat e zhvillimit të teknologjive të reja.

Objektivi specifik 1. 2: Përmirësimi i Kapaciteteve Monitoruese dhe Mbrojtjes së Sistemeve

Ky objektiv përfshin monitorimin e vazhdueshëm të sistemeve të informacionit dhe rrjeteve të komunikimit, gjurmimin e aktiviteteve të dyshimta, identifikimin e pikave të dobëta, zhvillimin e produkteve të sigurta softuer dhe harduer dhe sigurimin e një qasjeje të sigurtë për përdoruesit. Qëllimi i këtij objektivi është minimizimi i rreziqeve përmes implementimit të masave proaktive dhe sigurimit të mbrojtjes së qëndrueshme ndaj sulmeve dhe kërcënimeve kibernetike duke përfshirë zgjerimin e aktiviteteve të kontrollit dhe përputhshmërisë për teknologjitë e avancuara si blockchain, cloud computing, AI dhe teknologji të tjera në zhvillim (emerging technologies) për të siguruar mbrojtjen e sistemeve të reja dhe integrimin e tyre në ekosistemet ekzistuese të sigurisë.

Objektivi specifik 1. 3: Vlerësimi dhe Menaxhimi i Rreziqeve Kibernetike

Ky objektiv përfshin vlerësimin e vazhdueshëm të rreziqeve kibernetike duke përfshirë identifikimin, vlerësimin, analizimin dhe trajtimin e rreziqeve në nivel operatori, sektori dhe kombëtar. Qëllimi i këtij objektivi vë në fokus bashkëpunimin me partnerë kombëtarë dhe ndërkombëtarë për të adresuar rreziqet kibernetike, si dhe për të krijuar kanale komunikimi të shkëmbimit të informacionit.

Objektivi specifik 1.4: Zhvillimi i planeve të reagimit dhe menaxhimit të incidenteve kibernetike

Ky objektiv mbulon menaxhimin dhe shpërndarjen e informacionit lidhur me incidentet kibernetike, analizën e shkaqeve të incidenteve dhe raportimin për të përmirësuar masat mbrojtëse dhe reagimin në kohë. Qëllimi është krijimi i proceseve të qarta për trajtimin e incidenteve dhe reagimin e shpejtë për të parandaluar dhe kufizuar dëmet potenciale.

Objektivi specifik 1.5: Garantimi i transaksioneve elektronike përmes Shërbimeve të Besuara

Ky objektiv synon garantimin e transaksioneve të sigurta elektronike për bizneset dhe qytetaret nëpërmjet përdorimit të shërbimeve te besuara.

2. Kapacitetet Njerëzore

Përmbushja e vizionit dhe qëllimit të Strategjisë Kombëtare kërkon zhvillimin e aftësive, njohurive dhe kulturës së duhur në fushën e sigurisë kibernetike. Kapacitet Njerëzore luajnë një rol të rëndësishëm në rritjen e nivelit të sigurisë kibernetike, duke aplikuar ekspertizën e tyre në projektimin dhe implementimin e masave të sigurisë. Ky proces përfshin të gjithë aktorët si politikëbërësit, specialistët e sigurisë kibernetike, dhe përdoruesit e sistemeve digjitale, të cilët duhet të kuptojnë rolet dhe përgjegjësitë për të menaxhuar dhe zvogëluar rreziqet dhe kontribuar në rritjen e qëndrueshmërinë së sigurisë kibernetike. Programet e

edukimit, trajnimit dhe ndërgjegjësimit janë thelbësore për forcimin e kapaciteteve njerëzore, duke mundësuar krijimin e një mjedisi digjital të sigurt.

Objektivi specifik 2.1: Promovimi dhe zhvillimi i Kulturës Kibernetike

Forcimi i kulturës së sigurisë kibernetike është thelbësor për mbrojtjen e rrjeteve dhe sistemeve të informacionit, pasi përdoruesit shpesh janë hallka më e dobët e zinxhirit të mbrojtjes. Ky objektiv kërkon trajnime të vazhdueshme, fushata ndërgjegjësimi dhe partneritete me median dhe organizatat e komunitetit. Krijimi i mjediseve proaktive dhe përmirësimi i vazhdueshëm i praktikave janë të domosdoshme për të siguruar mbrojtje të qëndrueshme. Po ashtu, përfshirja e të gjithë grupeve të interesit dhe zbatimi i parimeve të sigurisë në të gjitha nivelet kontribuojnë në forcimin e mbrojtjes kibernetike.

Objektivi specifik 2.2: Rritja e Kapaciteteve Profesionale

Zhvillimi i kapaciteteve profesionale nëpërmjet integrimit të kurrikulave të përmirësuara në sektorin arsimor, trajnimeve të specializuara, certifikimeve profesionale, tërheqjes dhe angazhimit të talenteve, gjithëpërfshirjes dhe bashkëpunimit me organizatat ndërkombëtare për praktikat më të mira synon krijimin e një qasje efektive në adresimin e sfidave dhe përballimin e rreziqeve të sigurisë kibernetike.

3. Teknologjia

Teknologjia luan një rol të rëndësishëm në mbrojtjen e infrastrukturës digjitale, pasi ajo ofron mjetet dhe burimet e nevojshme për implementimin e masave të sigurisë kibernetike për parandalimin dhe menaxhimin e kërcënimeve kibernetike. Avancimi i teknologjisë, shton nevojën për një reagim të shpejtë ndaj sulmeve kibernetike, gjithmonë e me të sofistikuara. Ky proces përfshin një sërë sfidash të mëdha për të siguruar një mbrojtje të qëndrueshme dhe efikase kundër këtyre kërcënimeve komplekse.

Objektivi specifik 3.1: Përdorimi dhe integrimi i teknologjive të avancuara

Përdorimi dhe integrimi i teknologjive të avancuara, si Inteligjenca Artificiale (**AI**), kompjuterët kuantikë, kriptografia kuantike dhe teknologjitë e decentralizuara (**Blockchain**), do të përmirësojnë sigurinë kibernetike duke mundësuar identifikimin e avancuar të kërcënimeve dhe reagimeve të automatizuara.

Objektivi specifik 3.2: Monitorimi, zbulimi dhe mbrojtje kibernetike duke shfrytezuar Teknologjitë e avancuara

Shqipëria angazhohet të sigurojë një nivel të qëndrueshmërisë kibernetike proporcional me rrezikun, duke zgjeruar kapacitetet teknologjike të monitorimit për të identifikuar, parandaluar dhe trajtuar kërcënimet kibernetike në të gjitha infrastrukturat kritike dhe të rëndësishme të informacionit.

Objektivi specifik 3.3: Implementimi i kornizës 'secure by design' për infrastrukturat digjitale

Zbatimi i parimit *'secure by design'* për të integruar masat e sigurisë kibernetike në të gjitha fazat e ciklit të jetës së sistemeve dhe shërbimeve digjitale, blerje dhe çaktivizimi i sigurt. Kjo qasje do të sigurojë një proces të vazhdueshëm dhe interaktiv për menaxhimin e rrezikut, me përfshirjen e ekspertëve të sigurisë në çdo fazë të zhvillimit të shërbimeve digjitale.

Objektivi specifik 3.4: Menaxhimi efektiv i teknologjive të vjetruara

Kjo qasje do të sigurojë një menaxhim efektiv i teknologjive të vjetruara në nivel kombëtar përmes zhvillimit dhe zbatimit të politikave gjithëpërfshirëse që synojnë identifikimin, përditësimin, izolimin ose eliminimin e tyre, duke kontribuar në forcimin e mbrojtjes kibernetike, qëndrueshmërinë e shërbimeve dhe rritjen e besueshmërisë së infrastrukturave kritike dhe të rëndësishme të informacionit.

Objektivi specifik 3.5: Përdorimi i Teknologjive Alternative Kompensuese për Sigurinë Kibernetike

Shqipëria do të promovojë dhe implementoj teknologji alternative me burim të hapur (open-source) si një masë mbështetëse do të zbatohet në rastet kur teknologjitë me burim të mbyllur nuk janë të disponueshme ose të përballueshme për infrastrukturat kritike dhe të rëndësishme (OIKI/OIRI). Kjo qasje synon të garantojë vazhdimësinë e mbrojtjes kibernetike dhe ruajtjen e qëndrueshmërisë operacionale të këtyre infrastrukturave, veçanërisht në kushte të kufizuara teknologjike ose financiare.

Qëllimi i politikës 2: Mbrojtja *online e qytetareve* dhe nxitja e kulturës kibernetike

Kjo politikë synon të sigurojë një qasje gjithëpërfshirëse për mbrojtjen online dhe promovimin e një kulture të qëndrueshme kibernetike në Shqipëri. Ajo përqendrohet në përshtatshmërinë e kuadrit ligjor, duke siguruar se të gjithë qytetarët, përfshirë grupet e nënpërfaqësuara, janë të mbrojtur dhe kanë mundësi të barabarta për pjesëmarrje në hapësirën kibernetike. Për të arritur këtë qëllim, organizohen tavolina të rrumbullakëta, ku përfaqësues nga institucionet publike, sektori privat, organizatat jofitimprurëse (OJQ), media dhe shoqëria civile diskutojnë sfidat dhe zgjidhjet për sigurinë kibernetike. Këto platforma dialogu ndihmojnë në krijimin e politikave të bazuara në konsensus dhe adresimin e nevojave të ndryshme të komuniteteve. Gjithashtu, aktivitetet dhe trajnimet për rritjen e ndërgjegjësimit dhe aftësive kibernetike janë prioritet, ku përfshihen fushata ndërgjegjësimi për rreziqet online, programe edukative për të rinjtë dhe grupet e nënpërfaqësuara, si dhe trajnime specifike për profesionistët dhe publikun e gjerë. Bashkëpunimi ndërinstitucional dhe ndërsektorial luan një rol të rëndësishëm në zbatimin e kësaj politike. Institucionet publike, sektori privat, OJQ-të dhe media bashkërendojnë përpjekjet për të ndërtuar një ekosistem të fortë të sigurisë kibernetike, duke garantuar një qasje gjithëpërfshirëse dhe të qëndrueshme për mbrojtjen dhe nxitjen e qytetarëve.

Objektivi specifik 1: Hartimi dhe zhvillimi i Planit Kombëtar për Ndërgjegjësimin e Qytetarëve (PKNQ)

Ky objektiv synon hartimin dhe zbatimin e një plani gjithëpërfshirës për ndërgjegjësimin e qytetarëve lidhur me sfidat dhe rreziqet që lidhen me sigurinë kibernetike, si dhe përfitimet e të qenit pjesë e një mjedisi digjital të sigurt. PKNQ do të përfshijë fushata të organizuara në shkolla, institucione publike, dhe komunitete lokale, me qëllim rritjen e ndërgjegjësimit mbi praktikat më të mira për mbrojtjen *online*. Në këtë kuadër, do të zhvillohen programe edukative që synojnë të pajisin qytetarët me aftësi të domosdoshme për të identifikuar dhe shmangur kërcënimet kibernetike, duke përfshirë mbrojtjen nga mashtrimet *online*, menaxhimin e të

dhënave personale dhe sigurinë e llogarive të tyre, duke krijuar një zinxhir edukimi të vazhdueshëm për të gjithë.

Objektivi specifik 2: Hartimi i një kornize ligjore për qasjen gjithëpërfshirëse të qytetarëve

Ky objektiv synon krijimin dhe përshtatjen e një kuadri ligjor të avancuar, i cili garanton që të gjithë qytetarët të kenë akses të barabartë në hapësirën digjitale. Korniza ligjore do të përfshijë mekanizma që rregullojnë transparencën, barazinë në aksesin ndaj shërbimeve digjitale dhe mbrojtjen nga diskriminimi *online.* Për të arritur këtë, do të organizohen konsultime gjithëpërfshirëse me qytetarët, institucionet publike, sektorin privat dhe OJQ-të, për të siguruar që zëri i të gjithëve reflektohet në politikat dhe legjislacionin përkatës.

Objektivi specifik 3: Krijimi i mekanizmave të nevojshëm për mbrojtjen online të fëmijëve

Fëmijët përbëjnë një nga kategoritë më të cënueshme në ekosistemin digjital, ndaj ky objektiv synon krijimin dhe zbatimin e mekanizmave specifikë për garantimin e sigurisë së tyre *online.* Në këtë kuadër, do të zhvillohen platforma të dedikuara që ofrojnë përmbajtje edukative dhe argëtuese në një mjedis të sigurt dhe të monitoruar, ndërsa do të implementohen sisteme të avancuara monitorimi dhe plane të përbashkëta ndërinstitucionale për të mbështetur prindërit dhe kujdestarët në mbikëqyrjen efektive të aktiviteteve digjitale të fëmijëve. Si pjesë e këtij objektivi, do të realizohen gjithashtu fushata të strukturuara ndërgjegjësimi dheprograme trajnuese , duke i pajisur ata me aftësitë e nevojshme për të identifikuar dhe adresuar rreziqet kibernetike. Kjo qasje gjithëpërfshirëse synon krijimin e një mjedisi digjital të sigurt dhe edukativ që promovon mirëqenien dhe zhvillimin e fëmijëve.

Objektivi specifik 4: Nxitja e Barazisë Gjinore në Hapësirën Digjitale

Ky objektiv ka për qëllim krijimin e një mjedisi digjital gjithëpërfshirës dhe të sigurt për gratë dhe vajzat, duke u fokusuar në fuqizimin e tyre dhe luftimin e çdo forme diskriminimi ose dhune kibernetike. Përmes fushatave ndërgjegjësuese, do të promovohet pjesëmarrja aktive e grave dhe vajzave në sektorin e teknologjisë dhe sigurisë kibernetike. Aktivitetet do të përfshijnë trajnime për fuqizimin e tyre përmes aftësive digjitale, krijimin e platformave të sigurisë që adresojnë ngacmimet *online,* si dhe zhvillimin e rrjeteve mbështetëse për gratë profesioniste në fushën e teknologjisë. Ky objektiv do të synojë gjithashtu krijimin e politikave që inkurajojnë barazinë gjinore në çdo aspekt të hapësirës digjitale dhe promovojnë një kulturë mbështetëse për gratë dhe vajzat *online.*

Objektivi specifik 5: Krijimi i Mekanizmave të Nevojshëm për Mbrojtjen dhe Fuqizimin e Grupeve të Nënpërfaqësuara

Ky objektiv synon të mbrojë dhe fuqizojë grupet e nënpërfaqësuara, duke krijuar platforma gjithëpërfshirëse që adresojnë nevojat specifike të këtyre grupeve, për garantimin në një qasje të barabartë në mjetet dhe shërbimet digjitale. Përmes programeve edukative dhe trajnimeve, këto grupe do të fuqizohen për të qenë më aktive dhe të mbrojtura në hapësirën digjitale. Gjithashtu, do të implementohen politika dhe mekanizma që adresojnë diskriminimin *online* dhe sigurojnë një mjedis digjital të barabartë dhe gjithëpërfshirës për të gjithë. Ky objektiv do të realizohet përmes bashkëpunimit të ngushtë me organizatat që mbështesin këto grupe, institucionet publike dhe sektorin privat.

Qëllimi i politikës 3: Forcimi i Bashkëpunimit Ndërkombëtar

Siguria kibernetike është një sfidë ndërkombëtare dhe një përpjekje e përbashkët për të adresuar sfidat që lidhen me kërcënimet dhe rreziqet në mjedisin digjital. Strategjia promovon forcimin e bashkëpunimit ndërmjet institucioneve dhe partnerëve ndërkombëtarë, duke nxitur shkëmbimin e informacionit, zhvillimin e kapaciteteve të përbashkëta dhe krijimin e standardeve të unifikuara, duke siguruar një mbrojtje kolektive dhe më efektive kundër kërcënimeve kibernetike. Në këtë kuadër, Shqipëria angazhohet për të kontribuar aktivisht në nismat dhe marrëveshjet ndërkombëtare për sigurinë kibernetike, duke forcuar kështu qëndrueshmërinë e mjedisit digjital global.

Objektivi specifik 1: Harmonizimi i politikave dhe legjislacionit

Qëllimi i këtij objektivi është të sigurohet përputhshmëria e legjislacionit të sigurisë kibernetike të Shqipërisë me standardet dhe rregulloret ndërkombëtare, duke krijuar një kornizë ligjore të fortë dhe të qëndrueshme. Ky harmonizim do të mundësojë një reagim më efikas dhe të koordinuar ndaj kërcënimeve kibernetike, duke rritur mbrojtjen e hapësirës digjitale dhe kontributin e Shqipërisë në nivel global. Sulmet kibernetike janë më komplekse dhe nisur nga këto kushte mbrojtja, parandalimi apo rimëkëmbja pas tyre duhet të bazohet në pesë elementë shumë të rëndësishëm si ligjor, teknik, organizativ, kapacitet profesional dhe bashkëpunimi. Duke qënë se natyra e këtyre sulmeve ka treguar se nuk varen nga kufijtë mes shtetesh, situata ekonomike, politike apo sociale, legjislacioni apo standardet e unifikuara janë prioritet në luftën e përbashkët kundër sulmeve të vazhdueshme kibernetike.

Objektivi specifik 2:Forcimi i bashkëpunimit rajonal (WB6) dhe ndërkombëtar

Për të ndërtuar një ekosistem digjital të sigurt dhe të qëndrueshëm, nuk mund të veprosh i vetëm, pasi sulmet kibernetike apo ato hibride kanë treguar se praktika më e mirë kundër tyre është bashkëpunimi. Aktorët keqdashës mund të kenë objektiv të tyre një shtet, por pasojat ndihen dhe ndikojnë si në nivelin rajonal ashtu edhe atë global, ndaj bashkëpunimi është i domosdoshëm për të shkatërruar ekosistemin e sulmeve kibernetike dhe për të suportuar izolimin e plotë të tyre duke ndaluar pasojat që mund të prekin hapësirën e përbashkët digjitale. Zhvillimi dhe forcimi i bashkëpunimit rajonal dhe ndërkombëtar për të përballuar kërcënimet kibernetike, mund të arrihet duke përmirësuar shkëmbimin e informacionit dhe koordinimin e përgjigjeve ndaj incidenteve kibernetike.

Objektivi specifik 3: Zhvillimi i diplomacisë kibernetike

Zhvillimi i diplomacisë kibernetike me qëllim krijimin e kornizave të qarta diplomatike në nivel kombëtar dhe ndërkombëtar për të adresuar efektivisht çështjet e sigurisë kibernetike, duke angazhuar shtetet, organizatat ndërkombëtare dhe aktorët e tjerë ne mbrojtjen e infrastrukturave digjitale dhe sistemeve te informacionit.

Qëllimi i politikës 4: Nxitja e Inovacionit dhe Kërkimit Shkencor

Shqipëria synon të zhvillojë një ekosistem të qëndrueshëm përmes inovacionit dhe kërkimit shkencor duke theksuar bashkëpunimin mes akademisë, sektorit privat dhe institucioneve publike në rritjen e kapaciteteve kombëtare në fushën e sigurisë kibernetike dhe krijimin e zgjidhjeve të reja teknologjike. Kjo qasje forcon aftësinë për t'u përballur me sfidat kibernetike, por edhe ndihmojnë në krijimin e një mjedisi inovativ dhe të sigurt digjital për Shqipërinë.

Objektivi specifik 1: Ngritja e Qendrës Kombëtare të Ekselencës për Sigurinë Kibernetike
Krijimi i Qendrës Kombëtare të Ekselencës për Sigurinë Kibernetike (QKESK) si një qendër inovative për kërkim dhe zhvillim teknologjik do të mundësojë bashkëpunimin e ngushtë mes akademisë, qendrave kërkimore kombëtare dhe ndërkombëtare dhe institucioneve publike e private. Ajo do të nxisë kërkimin shkencor, identifikimin e talenteve dhe trajnimin e tyre me teknologjitë më të avancuara. Në fokus do të jetë zhvillimi i zgjidhjeve inovatore, si inteligjenca artificiale, analiza e të dhënave dhe kriptografia, për parandalimin dhe zbulimin e sulmeve kibernetike në kohë reale, me synimin për të forcuar sigurinë dhe qëndrueshmërinë digjitale kombëtare.
Objektivi specifik 2: Mbështetja e Startup-eve në fushën e Sigurisë Kibernetike
Të mbështetet zhvillimi i startup-eve në fushën e sigurisë kibernetike përmes aksesit në burime kërkimore dhe trajnime profesionale, duke nxitur krijimin e zgjidhjeve teknologjike inovative për adresimin e kërcënimeve kibernetike dhe fuqizimin e ekosistemit kombëtar të sigurisë kibernetike.
Objektivi specifik 3: Zhvillimi i Programeve të Financimit për Kërkim dhe Inovacion në Sigurinë Kibernetike
Të zhvillohen programe financimi për kërkimin dhe inovacionin në sigurinë kibernetike. Këto programe do të përfshijnë krijimin e fondeve specifike, ofrimin e stimujve fiskalë për bizneset që investojnë në teknologji të sigurta dhe promovimit të partneriteteve publike-private për bashkëfinancimin e projekteve inovative.

Qëllimi i politikës 5: Mbrojtja ndaj kërcënimeve hibride
Kërcënimi hibrid përfshin përdorimin e një plani apo strategjie ku aktorë të ndryshëm kombinojnë kërcënime kibernetike me sulme në fusha të tjera, si ato fizike, ekonomike dhe informative, për të arritur qëllime specifike. Ky lloj kërcënimi shfrytëzohet shpesh nga shtete apo aktorë jo-shtetërorë, duke përfituar nga dobësitë në sistemet teknologjike, infrastrukturore, politike dhe sociale të objektivave apo qëllimeve të synuara.
Për t'u mbrojtur ndaj kërcënimeve hibride, nevojitet një qasje e integruar që përfshin forcimin e sigurisë së infrastrukturës kritike, përmirësimin e kapaciteteve për zbulimin dhe parandalimin e sulmeve kibernetike, si dhe një bashkëpunim të ngushtë ndërinstitucional dhe ndërkombëtar për të siguruar një reagim të koordinuar, të shpejtë dhe efektiv.

Objektivi specifik 1: Hartimi i Kuadrit Ligjor për Mbrojtjen ndaj Kërcënimeve Kibernetike Hibride
Hartimi i një kuadri ligjor të përshtatshëm për mbrojtjen ndaj kërcënimeve kibernetike hibride do të mundësojë parandalimin, identifikimin dhe menaxhimin e kërcënimeve. Ky kuadër ligjor do të sigurojë një bashkëpunim të ngushtë ndërinstitucional kombëtar dhe ndërkombëtar, duke forcuar mbrojtjen e infrastrukturave ndaj kërcënimeve hibride.
Objektivi specifik 2: Koordinimi Ndërinstitucional dhe Ndërkombëtar për mbrojtjen ndaj Kërcënimeve Hibride
Bashkëpunimi dhe koordinimi ndërinstitucional dhe ndërkombëtar do të adresojë kërcënimet hibride dhe do të optimizojë ndarjen e informacionit dhe burimeve. Koordinimi i ngushtë siguron një reagim të shpejtë dhe efikas për të parandaluar dhe menaxhuar pasojat e kërcënimeve hibride.

Objektivi specifik 3: Krijimi i mekanizmave të Mbrojtjes ndaj Kërcënimeve Hibride
Për zhvillimin e një strukture të integruar dhe efikase për parashikimin, identifikimin dhe reagimin ndaj kërcënimeve hibride, që përfshijnë sulme kibernetike dhe dezinformim, është i nevojshëm përdorimi i mjeteve dhe teknologjive moderne. Platformat për shkëmbimin e informacionit, si dhe rritja e ndërgjegjësimit në publik për të siguruar reagim të shpejtë dhe efektiv ndaj kërcënimeve, ruan stabilitetin dhe sigurinë kombëtare.
Objektivi specifik 4: Krijimi i mekanizmave për parandalimin dhe hetimin e Krimit Kibernetik
Parandalimi i krimit kibernetik kërkon një qasje proaktive dhe të bazuar në teknologji të avancuar që përfshin zbulimin e hershëm dhe reagimin e shpejtë ndaj kërcënimeve. Ky objektiv synon krijimin e një mjedisi të sigurt dhe të qëndrueshëm në hapësirën digjitale, duke parandaluar dhe menaxhuar efektet e mundshme të krimeve kibernetike.

Zbatimi, Përgjegjësia e Institucioneve, Llogaridhënia

Hartimi i Strategjisë Kombëtare të Sigurisë Kibernetike 2025–2030 mbështetet në VKM Nr. 783, datë 18.12.2024, "Për organizimin dhe funksionimin e Autoritetit Kombëtar për Sigurinë Kibernetike", si dhe në angazhimet dhe standardet e BE-së dhe organizmave të tjerë ndërkombëtarë.

- Angazhimi i institucioneve publike dhe private i jep kësaj Strategjie mundësinë për të qenë objektive dhe e realizueshme. Grupi ndërinstitucional i punës, si dhe të gjithë aktorët e përfshirë në konsultime dhanë komente të vlefshme, duke e rishikuar disa herë draftin e përgatitur me qëllim miratimin e një strategjie gjithëpërfshirëse, ku secili të gjejë veten e të japë kontributin e tij në garantimin e sigurisë kibernetike të vendit.

- Kjo Strategji nuk është një strategji vetëm për institucionet, por është një strategji që nxit dhe mbështet mbrojtjen kibernetike edhe të individit, qytetarëve dhe, veçanërisht, fëmijëve si e ardhmja e këtij vendi. Në të evidentohen edhe masa për të luftuar jo vetëm krimin kibernetik, por edhe nxitjen e terrorizmit dhe ekstremizmit të dhunshëm nëpërmjet hapësirës kibernetike.

Plani i Veprimit që shoqëron Strategjinë Kombëtare të Sigurisë Kibernetike, 2025–2027 u përgatit, bazuar në:

a) Strategjinë Kombëtare për Sigurinë Kibernetike 2025-2030 dhe Politikat përbërëse të saj;

b) në planet buxhetore të institucioneve publike.

Sikurse paraqitet edhe në objektivat specifikë dhe aktivitetet kryesore të propozuara në këtë Strategji dhe Planin e Veprimit, rolin koordinues duhet ta kryejë Autoriteti Kombëtar për Sigurinë Kibernetike. Gjithashtu, në këtë dokument janë marrë parasysh detyrimet që lindin

nga procesi i integrimit evropian dhe përshtatja me direktivat NIS2, EIDAS2, si dhe angazhimet si vend anëtar i NATO.

Të gjitha masat/aktivitetet e propozuara, pasi u vlerësuan dhe plotësuan edhe nga grupi ndërinstitucional i punës, përgjegjës për hartimin e Strategjisë, u detajuan më tej gjatë vlerësimit të efekteve financiare për zbatimin e kësaj Strategjie Kombëtare dhe Planit të saj të Veprimit 2025– 2027, me nevojën për rishikim periodik bazuar në dinamikën e zhvillimit në fushën e sigurisë kibernetike.

Secili institucion përgjegjës për aktivitetet duhet të planifikojë realizimin e tyre duke garantuar buxhetet e planifikuara, burimet njerëzore dhe kapacitetet teknike me qëllim realizimin e tyre. Çdo vit do të bëhet vlerësimi i zbatimit të aktiviteteve dhe arritjes së objektivave të identifikuar nëpërmjet realizimit të indikatorëve. Institucionet përgjegjëse për realizimin e aktiviteteve dhe arritjes së rezultateve kanë detyrimin e raportimit sipas standardeve raportuese. Koordinatori i Strategjisë duhet të përgatitë raportin vjetor dhe ta publikojë atë.

Plani i Veprimit dhe Burimet Financiare për Zbatim

Metodologjia e kostimit të aktiviteteve

Shpenzimet e nevojshme për zbatimin e PKVsë janë nxjerrë duke kostuar secilin nga aktivitetet e këtij plani veprimi. Metodologjia e zbatuar për llogaritjen e kostove paraqet një kombinim të metodave që mund të përdoren në rastet e strategjive me shumë aktorë. Metodologjia kryesore e përdorur është kostimi i bazuar në aktivitete (Activity Based Costing-ABC), ku për çdo aktivitet evidentohet institucioni përgjegjës si dhe burimi i mbulimit të kostove dhe alokon burimet për të gjitha produktet dhe shërbimet në bazë të konsumit aktual për secilin aktivitet.

Buxheti u hartua mbështetur në koston e secilit aktivitet të pasqyruar në planin e veprimit, kohështrirjen dhe frekuencën e zbatimit të tij, si dhe numrin e përfituesve për aktivitete të caktuara. Për llogaritjen e shpenzimeve për aktivitetet kryesore është vepruar si më poshtë:

- Llogaritja e shpenzimeve për burime njerëzore bazohet në kohën e parashikuar për realizimin e veprimtarisë dhe një page mesatare ditore të një kategorie të caktuar.
- Llogaritja e shpenzimeve për shërbime. Për këto aktivitete janë mbajtur parasysh kostot e shërbimeve të institucioneve përkatëse, bazuar në standardet e miratuara.
- Llogaritja e shpenzimeve për aktiviteteve që lidhen me hartimin dhe rishikimin e legjislacionit, monitorimin dhe funksionimin e strukturave të përhershme, etj. Për këto aktivitete gjatë llogaritjeve janë mbajtur parasysh shpenzimet e vazhdueshme që do të ndodhin, për shembull për pagat, kontributet e sigurimeve shoqërore, ekspertizë të huaj (kur është parashikuar në plan) dhe mjete konsumi.
- Llogaritja e shpenzimeve për aktiviteteve që lidhen me studime, fushata ndërgjegjësuese programe trajnimi ekspertiza të huaja, etj. Llogaritja e kostove është bërë sipas iniciativave specifike të ngjashme, si dhe sipas natyrës së aktiviteteve dhe kostove që ofron tregu për shërbime të tilla.

- - Në llogaritjen e shpenzimeve për trajnime është mbajtur në konsideratë kosto e trajnimit për një person. Si kosto për njësi janë përdorur kostot e aplikuara për trajnime të ngjashme në të shkuarën.
- Për atë pjesë të aktiviteteve ku informacioni nuk është i plotë (si në rastin e projekteve apo studimeve) është ndjekur metoda e vlerësimit për analogji ose duke marrë në konsideratë shpenzimet e bëra për aktivitete të ngjashme që kanë qenë përfshirë në planet buxhetore të mëparshme.

Buxheti dhe burimet financiare për zbatimin e planit të veprimit

Strategjia Kombëtare e Sigurisë Kibernetike do të zbatohet në periudhën 2025-2030. Për të mundësuar zbatimin e saj janë llogaritur shpenzimet e nevojshme për zbatimin e secilit aktivitet, objektiv specifik dhe qëllimit të politikave. Buxheti i përgjithshëm për zbatimin e Strategjisë është reflektuar në disa forma:

- Buxheti i përgjithshëm sipas viteve për secilin aktivitet, objektiv specifik, qëllim strategjik dhe burimeve të financimit;

- Buxheti i detajuar sipas aktiviteteve, burimeve të financimit dhe institucioneve përgjegjëse.