REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Nr. 1066 Prot

Tiranë më 27.06.2025

URDHËR

Nr. 181 datë. 27.06 2025

PËR

MIRATIMIN E RREGULLORES PËR FUNKSIONIMIN TEKNIK TË CSIRT-EVE SEKTORIALE DHE CSIRT-EVE PRANË OPERATORËVE TË INFRASTRUKTURAVE TË INFORMACIONIT

Në zbatim të pikës 4, të nenit 15 të ligjit nr.25/2024 "Për sigurinë kibernetike",

URDHËROJ

1. Miratimin e rregullores "Për funksionimin teknik të CSIRT-eve sektoriale dhe CSIRT-eve pranë operatorëve të infrastrukturave të informacionit" sipas tekstit që i bashkëlidhet këtij urdhri dhe është pjesë përbërëse e tij.
2. Për zbatimin e këtij urdhri ngarkohen CSIRT-et sektoriale dhe CSIRT-et pranë operatorëve të infrastrukturave të informacionit.
3. Ky urdhër hyn në fuqi menjëherë.

DREJTORI I PËRGJITHSHËM

IGLI TAFA

REPUBLIKA E SHQIPËRISË - AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE - KËSHILLI I MINISTRAVE

Adresa: Rruga "Papa Gjon Pali II" nr.3Tiranë;
Faqe web: www.aksk.gov.al E-mail: info@aksk.gov.al
Tel./Fax : 04 2221 039

REPUBLIKA E SHQIPËRISË

AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

RREGULLORE PËR FUNKSIONIMIN TEKNIK TË CSIRT-EVE SEKTORIALE DHE CSIRT-EVE PRANË OPERATORËVE TË INFRASTRUKTURAVE TË INFORMACIONIT

Përmbajtje

1. Hyrje

Rritja eksponenciale e numrit, kompleksitetit dhe impaktit të sulmeve kibernetike në dekadën e fundit ka vënë në pikëpyetje kapacitetet tradicionale të institucioneve për të menaxhuar rreziqet në hapësirën digjitale. Sulmet me bazë ransomware, sulmet ndaj infrastrukturave kritike dhe të rëndësishme të informacionit, manipulimi i të dhënave dhe fushatat e dezinformimit kërkojnë një qasje shumë më të organizuar, të standardizuar dhe të ndërveprueshme për menaxhimin e incidenteve të sigurisë kibernetike. Në këtë kontekst, nevoja për një strukturë të qëndrueshme, të pavarur dhe të integruar, me staf të trajnuar dhe mjete të avancuara, bëhet kritike për mbrojtjen e integritetit institucional dhe garantimin e shërbimeve digjitale për qytetarët dhe bizneset.

Për këtë qëllim, ligji nr. 25/2024 "Për sigurinë kibernetike", ka përcaktuar krijimin dhe funksionimin e ekipeve të përgjigjes ndaj incidenteve të sigurisë kibernetike (CSIRT-et), si struktura thelbësore për përballimin e sfidave kibernetike në nivel kombëtar, sektorial dhe pranë operatorit. Ky kuadër synon të forcojë kapacitetet institucionale për përballimin e sfidave kibernetike dhe të ndërtojë një mekanizëm të besueshëm për zbulimin, analizimin dhe trajtimin e incidenteve kibernetike në kohë reale.

Në këtë rregullore përcaktohen rregullat teknike të funksionimit të CSIRT-eve sektoriale dhe CSIRT-eve pranë operatorëve të infrastrukturave të informacionit, bazuar në modelin **SIM3** *(Security Incident Management Maturity Model)*, një model i njohur ndërkombëtarisht, i cili mundëson vlerësimin dhe zhvillimin e maturitetit funksional të ekipeve CSIRT në katër parametra kryesore: **Organizim** (*Organisation*), **Burime Njerëzore** (*Human*), **Mjete dhe Teknologji** *(Tools),* si dhe **Procese Operacionale** *(Processes).*

Zbatimi i modelit SIM3 mbështet gjithashtu harmonizimin e funksionimit të CSIRT-eve me kërkesat e Direktivës NIS2 të Bashkimit Evropian[1] dhe standardet e ENISA-s, duke e pozicionuar Shqipërinë në linjë me përpjekjet rajonale dhe evropiane për ndërtimin e një arkitekture të përbashkët dhe të qëndrueshme të sigurisë kibernetike.

Parimet mbi bazën e të cilave mbështetet funksionimi teknik i CSIRT-eve janë profesionalizmi, maturiteti operacional dhe përmirësimi i vazhdueshëm i kapaciteteve teknike dhe organizative të ekipeve përkatëse, të cilat sigurojnë një qasje të strukturuar, të besueshme dhe të qëndrueshme në përmbushjen e funksioneve të tyre në përballimin e kërcënimeve dhe incidenteve të sigurisë kibernetike.

2. Qëllimi

Kjo rregullore përcakton rregullat teknike për funksionimin e CSIRT-eve sektoriale dhe atyre pranë operatorëve të infrastrukturave të informacionit, me qëllim forcimin e qëndrueshmërisë ndaj rreziqeve dhe kërcënimeve kibernetike, si dhe krijimin e një qasjeje të unifikuar ndërmjet strukturave përgjegjëse për sigurinë kibernetike në nivel sektorial dhe operatori.

[1] Direktiva (BE) nr. 2022/2555, të Parlamentit dhe Këshillit, datë 14 dhjetor 2022, "Mbi masat për një nivel të lartë të përbashkët të sigurisë kibernetike në të gjithë Bashkimin Evropian, e cila ka ndryshuar rregulloren (BE) nr. 910/2014 dhe direktivën (BE) nr. 2018/1972, si dhe ka shfuqizuar direktivën (BE) nr. 2016/1148.

Rregullorja synon:

- **Standardizimin** e strukturës organizative dhe funksionimit teknik të ekipeve CSIRT sektoriale dhe atyre pranë operatorëve, në përputhje me praktikat më të mira ndërkombëtare;
- **Vendosjen e një kornize të qartë dhe të matshme të maturitetit operacional**, për të mundësuar vlerësimin dhe rritjen graduale të kapaciteteve të ekipeve CSIRT;
- **Sigurimin e zhvillimit të qëndrueshëm dhe përmirësimit të vazhdueshëm** të kapaciteteve teknologjike, procedurale dhe njerëzore të ekipeve CSIRT, për të garantuar një reagim efektiv dhe të koordinuar ndaj incidenteve të sigurisë kibernetike.
- **Harmonizimin** me praktikat më të mira ndërkombëtare dhe përputhshmërinë me Direktivën e BE-së, NIS 2.

3. Fusha e zbatimit

Kjo rregullore zbatohet nga subjektet përgjegjëse të sigurisë kibernetike dhe operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, pranë të cilëve ngrihet dhe funksionon struktura e CSIRT-it, në përputhje me përcaktimet e ligjit nr. 25/2024 "Për sigurinë kibernetike".

4. Përkufizime

Termat e përcaktuara në këtë rregullore kanë të njëjtin kuptim me termat e përcaktuara në ligjin nr.25/2024 "Për sigurinë kibernetike", ndërsa termat e mposhtëm kanë kuptimin si vijon:

1. **"Të dhëna personale**", sipas kësaj rregulloreje ka të njëjtin kuptim me përkufizimin e dhënë në legjislacionin në fuqi për mbrojtjen e të dhënave personale.
2. **"PIR"** *(Post-Incident Review),* është një proces analizues që realizohet pas ndodhjes së një incidenti kibernetik për të vlerësuar shkakun, ndikimin, efektivitetin e reagimit dhe për të nxjerrë mësime që ndihmojnë në parandalimin e incidenteve kibernetike të ngjashme në të ardhmen.
3. **"MTTR"** *(Mean Time to Repair),* është koha mesatare që nevojitet për të riparuar një pajisje ose sistem dhe për ta kthyer në funksion pas një dështimi teknik.
4. **"MTTR-R"** *(Mean Time to Repair – Recovery),* është koha mesatare e nevojshme për të riparuar dhe rikthyer plotësisht një sistem në funksion pas një ndërprerjeje.
5. **"SOAR"** (*Security Orchestration, Automation and Response*), është platforma për automatizim të reagimit dhe analizës operacionale të sigurisë.
6. **"SIM3" (***Security Incident Management Maturity Model***)**, është modeli ndërkombëtar i maturitet për CSIRT-et, që vlerëson dhe përmirëson katër parametra funksionale: Organizimi (O), Burimet Njerëzore (H), Mjetet Teknike (T), dhe Procese Operacionale (P).
7. **"Maturitet operacional"** *(Operational maturity),*është niveli i zhvillimit dhe formalizimit të kapaciteteve të një CSIRT-i për të reaguar ndaj incidenteve kibernetike, i matur sipas modelit SIM3.

8. **“RFC 2350”**, është një dokument standard ndërkombëtar i përdorur për përshkrimin zyrtar të një CSIRT-i (strukturë, shërbime, kontakte, juridiksion).
9. **“SIEM”** *(Security Information and Event Management)*, janë sisteme që mbledhin, analizojnë dhe korrelojnë evente sigurie për monitorim dhe alarmim të hershëm.
10. **“STIX”** *(Structured Threat Information Expression)*, është një format standard për përshkrimin dhe ndarjen e të dhënave mbi kërcënimet kibernetike.
11. **“TAXII”** *(Trusted Automated Exchange of Indicator Information),* është një protokoll për shkëmbimin automatik të informacionit mbi kërcënimet kibernetike.
12. **“Traffic Light Protocol”**, është një skemë klasifikimi për ndarjen e informacionit sensitiv, bazuar në nivelet: *TLP:RED, TLP:AMBER, TLP:GREEN, TLP:CLEAR*.
13. **“KPI”(** *Key Performance Indicators),* janë indikatorë kyç për matjen e performancës dhe reagimit të një CSIRT-i.
14. **“BCM”** (*Business Continuity Management),* është një qasje sistematike për të siguruar që CSIRT-i të mund të vazhdojë të ofrojë shërbimet e tij kritike edhe gjatë dhe pas një ndërprerjeje të paparashikuar, qoftë si rezultat i një incidenti kibernetik, katastrofe natyrore, mungese të infrastrukturës apo faktorësh njerëzorë.
15. **“IPS/IDS”** (Intrusion Prevention/Detection System), janë sisteme që zbulojnë dhe/ose parandalojnë ndërhyrje të paautorizuara në rrjet ose sisteme.
16. **“EDR/XDR”** (Endpoint/Extended Detection and Response), janë zgjidhje të avancuara për monitorimin, zbulimin dhe reagimin ndaj kërcënimeve kibernetike në pajisje fundore (EDR) dhe në mjedise më të gjera të rrjetit dhe cloud-it (XDR).
17. **“MISP”** *(Malware Information Sharing Platform)* është një platformë me burim të hapur për ndarjen, ruajtjen dhe korrelacionin e treguesve të kompromisit dhe inteligjencës së kërcënimeve kibernetike.
18. “**IDS”** *(Intrusion Detection System),* është një teknologji e sigurisë së rrjetit që monitoron trafikun dhe pajisjet për aktivitete të dyshimta ose që shkelin politikat e sigurisë.
19. **“NetFlow”,** është një protokoll që mbledh *metadata* mbi trafikun IP që kalon nëpër pajisjet e rrjetit, duke ndihmuar në analizimin e modeleve të trafikut dhe performancës së rrjetit.
20. **“OTRS”** *(Open source Ticket Request System*) është një sistem menaxhimi shërbimesh me burim të hapur që mund të përdoret nga çdo departament në një infrastrukturë informacioni për të reduktuar kostot operative dhe për të rritur performancën e shërbimeve.
21. **“TheHive”**, është platformë e hapur dhe e shkallëzueshme për menaxhimin e rasteve të sigurisë, e dizajnuar për të ndihmuar ekipet e SOC, CSIRT dhe CERT në trajtimin e incidenteve të sigurisë kibernetike.
22. **“OT”** (Teknologjia Operacionale/*Operational Technology),* i referohet harduerit dhe softuerit që monitorojnë dhe kontrollojnë pajisjet dhe procese fizike në industri të ndryshme, si prodhimi, energjia dhe transporti.
23. **“IT”** (Teknologjia e Informacionit*/Information Technology),* përfshin përdorimin e kompjuterëve, softuerëve dhe rrjeteve për të krijuar, përpunuar, ruajtur dhe transmetuar të dhëna dhe informacione.
24. **“DDoS”** (Distributed Denial of Service), është një lloj sulmi kibernetikë ku shumë pajisje të shpërndara (zakonisht të infektuara me malware) përdoren për të mbingarkuar një server, rrjet apo shërbim online, duke e bërë të paaksesueshëm për përdoruesit legjitimë.

5. Struktura e rrjetit të CSIRT-eve në Republikën e Shqipërisë

Rrjeti i ekipeve për reagim ndaj incidenteve të sigurisë kibernetike (CSIRT) në Republikën e Shqipërisë përbën një arkitekturë funksionale të ndërtuar mbi bazat e bashkëpunimit, ndërveprueshmërisë dhe ndarjes së informacionit në kohë reale. Kjo strukturë organizative është e përcaktuar në ligjin nr. 25/2024 "Për sigurinë kibernetike" dhe përbëhet nga nivele të ndryshme operacionale që mbulojnë gjithë spektrin institucional dhe sektorët e infrastrukturës kritike dhe të rëndësishme të informacionit.

5.1. CSIRT Kombëtar

I vendosur pranë Autoritetit Kombëtar për Sigurinë Kibernetike (AKSK), ky ekip ka funksionin drejtues dhe koordinues në nivel kombëtar për të gjitha aktivitetet e reagimit ndaj incidenteve të sigurisë kibernetike. CSIRT-i Kombëtar është përgjegjës për menaxhimin e incidenteve me ndikim kombëtar, bashkëpunimin ndërkombëtar dhe standardizimin e praktikave të reagimit ndaj incidenteve kibernetike.

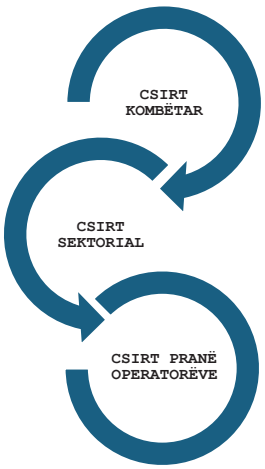
5.2 CSIRT Sektorial

CSIRT-i sektorial është ekipi i përgjigjes ndaj incidenteve të sigurisë kibernetike i ngritur nga subjektet përgjegjëse të sigurisë kibernetike për ofrimin e shërbimeve sipas sektorëve të përcaktuar në anekset e ligjit për sigurinë kibernetike.

5.3 CSIRT pranë operatorëve

CSIRT-et pranë operatorëve të infrastrukturës së informacionit janë ekipe të brendshme të ngritura nga operatorët e infrastrukturës kritike apo të rëndësishme të informacionit, të cilët janë përgjegjës për trajtimin e incidenteve kibernetike në nivel organizativ dhe për raportimin e tyre tek CSIRT sektorial dhe ai kombëtar.

5.4 Skema e CSIRT-eve



6. Rregullat teknike të funksionimit të CSIRT-it sektorial dhe CSIRT-it pranë operatorit të infrastrukturës së informacionit

Funksionimi teknik i CSIRT-eve bazohet në katër parametra kryesore: Organizimi (O), Burimet Njerëzore (H), Mjetet Teknike (T) dhe Proceset Operacionale (P).

6.1 Parametrat

Organizimi (O)

Ky parametër përcakton mënyrën se si është organizuar dhe funksionon një CSIRT, fushëveprimin, përshkrimin e shërbimeve që ofron, si dhe kuadrin organizativ dhe politik që e mbështet.

Burimet Njerëzore (H)

Kapacitetet njerëzore përbëjnë një ndër asetet më të rëndësishme për funksionimin e CSIRT-it. Në këtë kuptim, CSIRT-et duhet të kenë staf të kualifikuar, të trajnuar në mënyrë të vazhdueshme dhe të pajisur me kompetencat teknike dhe ndërpersonale të domosdoshme për menaxhimin efektiv të incidenteve të sigurisë kibernetike. Për këtë qëllim është e domosdoshme vendosja e mekanizmave të qarta për zhvillimin profesional dhe përmirësimin e vazhdueshëm të kapaciteteve teknike dhe menaxheriale të stafit, përmes programeve të trajnimit të rregullt, ndjekjes së standardeve më të mira dhe mbështetjes për zhvillimin e aftësive në përputhje me evolucionin e rreziqeve kibernetike.

Proceset Operacionale (P)

Një komponent thelbësor i funksionimit të CSIRT-it është përshkrimi i qartë dhe gjithëpërfshirës i proceseve kryesore operacionale si: menaxhimi, dhe monitorimi për parandalimin e incidenteve kibernetike, vlerësimi dhe analizimi i rrezikut kibernetik, dhe procese të tjera mbështetëse që lidhen me funksionimin efektiv të strukturave për sigurinë kibernetike.

Në veçanti, procesi i menaxhimit të incidenteve kibernetike duhet të përshkruhet në mënyrë të detajuar dhe përfshin të gjitha fazat sipas përcaktimeve në rregulloren në fuqi për procedurat e menaxhimit të incidenteve të sigurisë kibernetike, kundërmasat, playbooks dhe masat mbrojtëse të natyrës së përgjithshme: nga marrja dhe verifikimi i raportimeve, klasifikimi dhe ndërhyrja teknike, koordinimi me palët e përfshira, paralajmërimi i sektorëve të prekur, deri te zgjidhja e incidentit kibernetik dhe analiza retrospektive për të nxjerrë mësime për përmirësim të mëtejshëm.

Të gjitha këto procese duhet të jenë të dokumentuara në mënyrë të detajuar, të matshme përmes treguesve të performancës, të përsëritshme sipas procedurave standarde dhe të ndërtuara në mënyrë fleksibël për t'u përshtatur me ndryshimet teknologjike, rregullatore dhe organizative me qëllim garantimin e konsistencës, maturimit dhe përmirësimit të kapaciteteve.

Mjetet Teknike (T)

Përdorimi i mjeteve moderne teknologjike është një komponent tjetër i rëndësishëm për funksionimin e CSIRT-eve me qëllim fuqizimin e reagimit ndaj kërcënimeve/rreziqeve të sigurisë kibernetike. Këtu përfshihen përdorimi i mjeteve teknologjike si:

- Sistemet *SIEM* për monitorim dhe menaxhim të eventeve të sigurisë;
- Sisteme për ndërveprim dhe ndarje informacioni mbi kërcënimet nëpërmjet protokolleve të ndryshme si (*STIX, TAXII, TLP*);
- Sistemet për gjurmim dhe menaxhim të rasteve *(ticketing);*
  Sisteme për analizë forenzike dhe inteligjencë mbi kërcënimet *(threat intelligence sharing)*.

Përdorimi i këtyre mjeteve teknologjike mundëson dhe përmirëson ndjeshëm procedurën e menaxhimit të incidenteve të sigurisë kibernetike duke rritur efikasitetin operacional, duke reduktuar kohën e reagimit ndaj incidenteve të sigurisë kibernetike si dhe duke siguruar një analizë të thelluar dhe të strukturuar të çdo incidenti kibernetik.

6.2. Komunikimi dhe ndarja e informacionit

Komunikimi efektiv dhe ndarja e sigurt e informacionit përbëjnë një komponent të përbashkët që mbështesin të gjithë parametrat funksionalë të CSIRT-it pranë operatorit të infrastrukturës së informacionit dhe CSIRT-it sektorial të cilat janë thelbësorë për reagimin e koordinuar ndaj incidenteve të sigurisë kibernetike.

Në këtë kuadër CSIRT-i pranë operatorit dhe CSIRT-i sektorial duhet të krijojnë dhe përdorin kanale të sigurta komunikimi, duke garantuar konfidencialitetin, integritetin dhe gjurmueshmërinë e informacionit të ndarë me subjektet e tjera si dhe të marrin në konsideratë aplikimin e standardeve dhe protokolleve për shkëmbimin e sigurt të informacionit si STIX; TAXII, TLP etj.

7. Niveli i vlerësimit të maturitetit të CSIRT-eve

Rregullorja ofron një kornizë të qartë dhe të thjeshtuar për të matur nivelin e zhvillimit dhe funksionalitetit të çdo parametri të CSIRT-it, bazuar në katër parametrat themelore: Organizimi, Burimet Njerëzore, Proceset Operacionale dhe Mjetet Teknike.

Ky vlerësim i maturitetit i mundëson CSIRT-eve të identifikojnë pikat e forta dhe boshllëqet, të planifikojnë përmirësime strategjike dhe operacionale, të rrisin efektivitetin dhe qëndrueshmërinë, si dhe të harmonizohen me standardet ndërkombëtare dhe kërkesat e legjislacionit në fuqi për sigurinë kibernetike.

Vlerësimi do të jetë sipas një shkalle me pesë nivele, që lejon identifikimin objektiv të fazës aktuale të maturitetit për secilin parametër sipas tabelës së mëposhtme:

Niveli	**Përshkrimi**
Niveli 0 – (*I pa aplikueshëm / i pa përcaktuar / pa ndërgjegjësim)*	Ky nivel tregon mungesën e plotë të çdo njohurie apo praktike për parametrin e caktuar, referuar rasteve kur ekipet fillestare të reagimit ndaj incidenteve nuk kanë ndërmarrë masa për të funksionuar sipas parametrave të caktuar.
Niveli 1 – (*I nënkuptuar)*	Ky nivel tregon se parametri njihet brenda ekipit. Ekipi njeh procesin, por ky proces nuk është i dokumentuar si dhe nuk ka një ndarje të standardizuar midis anëtarëve të ekipit.
Niveli 2 – (*I dokumentuar, por jo i formalizuar)*	Ky nivel përfaqëson situatën kur informacioni dhe praktikat ekzistojnë në sisteme të brendshme joformale. Ato përfshijnë procese, mjete dhe

	politika të dokumentuara, por pa miratim zyrtar nga strukturat përgjegjëse të CSIRT-it. Edhe nëse ekziston konsensus brenda ekipit mbi përmbajtjen, mungesa e aprovimit formal e kufizon maturitetin në këtë nivel.
Niveli 3 - (*I formalizuar dhe i miratuar nga strukturat përgjegjëse)*	Ky nivel kërkon që përmbajtja e parametrave të jetë e dokumentuar dhe e miratuar zyrtarisht nga strukturat përgjegjëse të CSIRT-it. Këto dokumente duhet të jenë të integruara në funksionimin e përditshëm të ekipit dhe të rishikohen rregullisht.
Niveli 4 (*I kontrolluar dhe i mbikëqyrur nga strukturat e tyre përkatëse)*	**Niveli 4** kërkon që parametri, përveçse të jetë i dokumentuar dhe i miratuar (*si në nivelin 3*), të jetë objekt i një procesi të rregullt dhe aktiv kontrolli nga strukturat mbikëqyrëse. Ky proces duhet të përfshijë prova të qarta, ndjekje periodike dhe mekanizma *feedback-u* ndërmjet ekipit dhe strukturave mbikëqyrëse të tyre.

8. Mekanizmat e zhvillimit të parametrave

Këta mekanizma përfaqësojnë praktika të domosdoshme që duhet të zbatohen nga çdo CSIRT, me synim forcimin e rolit të tij institucional, përmirësimin e reagimit ndaj incidenteve kibernetike, dhe rritjen e aftësisë për të funksionuar në mënyrë të koordinuar, të dokumentuar dhe të përshtatur ndaj ndryshimeve teknologjike dhe rregullatore.

Mekanizmat e zhvillimit për parametrin O – Organizimi, përfshijnë:

- Hartimin dhe miratimin e politikave të qarta të komunikimit të brendshëm dhe të jashtëm;
- Hartimi dhe miratimi i politikave për klasifikimin, menaxhimin e incidenteve kibernetike në përputhje me kuadrin ligjor në fuqi për sigurinë kibernetike;
- Përdorimi i dokumentit referues RFC 2350 si standard i vazhdueshëm për përshkrimin e shërbimeve të CSIRT-it;
- Krijimi i mekanizmave për menaxhimin e marrëdhënieve me partnerët institucionalë dhe CSIRT-et partnere;
- Hartimi i një plan zhvillimi 3-vjeçar për CSIRT-in, me objektiva të matshëm dhe indikatorë monitorimi;
- Kontrolle vjetore nga AKSK për të verifikuar përputhshmërinë e strukturës organizative.

Mekanizmat e zhvillimit për parametrin H – Burimet Njerëzore, përfshijnë:

- Hartimi i një manuali funksional që përcakton rolet dhe përgjegjësitë e stafit të CSIRT-it;
- Zhvillimi i praktikave të qëndrueshme për shkëmbimin në mënyrë të vazhdueshme të njohurive midis anëtarëve të ekipit;
- Dokumentimi i proceseve të rekrutimit, trajnimit fillestar dhe zhvillimit profesional të vazhdueshëm;
- Zbatimi i një cikli të rregullt vlerësimi të performancës dhe përditësimit të kompetencave të stafit;
- Përdorimi i platformave për trajnime online dhe laboratorë virtualë për zhvillimin e aftësive teknike.

Mekanizmat e zhvillimit për parametrin T – Mjetet Teknike, përfshijnë:

- Përdorimin minimalisht të mjeteve me burim të hapur *(open-source tools)* për analizë dhe reagim ndaj incidenteve kibernetike *(p.sh. MISP, TheHive)*;
- Implementimi i mjeteve për zbulimin e kërcënimeve kibernetike si *IPS/IDS, EDR/XDR* etj;
- Automatizimi i procesit të zbulimit të kërcënimeve kibernetike dhe alarmimit nëpërmjet sistemeve *SIEM*, të cilat mbledhin, analizojnë dhe korelojnë në kohë reale të dhënat nga burime të ndryshme të sigurisë për të identifikuar incidente të mundshme kibernetike.
- Ruajtja në mënyrë të centralizuar dhe të pandryshueshme e të dhënave të ngjarjeve *(logs)* sipas përcaktimeve të rregullores në fuqi për mënyrat dhe afatet e ruajtjes së logeve të incidenteve kibernetike;
- Përdorimi i protokolleve që ofrojnë siguri për ndarjen e informacionit, si *STIX 2.1* dhe *TAXII 2.1*;
- Integrimi i platformave për monitorim të vazhdueshëm dhe reagim të automatizuar *SOAR* për efikasitet të lartë operacional.

Mekanizmat e zhvillimit për parametrin P – Proceset Operacionale, përfshijnë:

- Hartimin dhe përditësimin e një Manuali Operacional të CSIRT-it që mbulon të gjitha proceset dhe udhëzimet për menaxhimin e incidenteve kibernetike;
- Dokumentimi i formateve standarde për regjistrimin dhe trajtimin e incidenteve kibernetike, sipas klasifikimeve të tipit, urgjencës dhe ndikimit të incidenteve kibernetike bazuar në rregulloren e miratuar me urdhër të drejtorit të përgjithshëm të Autoritetit "Për kategorizimin e incidenteve të sigurisë kibernetike";
- Ofrimi i trajnimeve të rregullta dhe zhvillimi i simulimeve për testimin e praktikave operacionale;
- Monitorimi i indikatorëve kyç të performancës si koha e përgjigjes, saktësia e klasifikimit dhe koha e rikuperimit nga incidenti kibernetikë;
- Realizimi i analizave retrospektive pas çdo incidenti kibernetikë, me qëllim dokumentimin e mësimeve të nxjerra dhe përmirësimin e vazhdueshëm të praktikave ekzistuese të sigurisë.

8.1. Parametrat

8.1.1 Parametri O – Organizimi

Organizimi është një nga parametrat kryesor dhe përfaqëson themelin institucional, juridik dhe funksional të një CSIRT-i. Ky parametër përcakton strukturën organizative, mandatin, rolet dhe përgjegjësitë, si dhe kuadrin e bashkëpunimit të brendshëm dhe të jashtëm, duke siguruar që CSIRT-i të funksionojë me efikasitet të plotë.

Elementët kyç të parametrit Organizimi:

Parametri	Përshkrim	Kërkesa minimale për CSIRT

O-1 Mandati	Mandati i CSIRT-it, përcakton ekzistencën dhe funksionin e tij sipas përcaktimeve ligjore në fuqi.	CSIRT-i duhet të ketë një mandat të qartë të dokumentuar, i nxjerrë nga një autoritet i lartë qeverisës ose drejtues, i bazuar në ligj.
O-2 Entitetet (*Grupi i mbuluar / përfituesit e shërbimit*)	Grupi i entiteteve ose përdoruesve për të cilët CSIRT-i ofron shërbime.	Të jetë i përcaktuar saktësisht cilët janë përdoruesit që mbulon CSIRT-i.
O-3 Autoriteti	Autoriteti që i jepet CSIRT-it për të vepruar ndaj klientëve të tij për të përmbushur mandatin.	Autoriteti i CSIRT-it duhet të jetë i përshkruar qartë dhe të vijë nga nivelet e larta të qeverisjes.
O-4 Përgjegjësitë	Detyrimet dhe përgjegjësitë që CSIRT-i pritet të përmbushë ndaj subjekteve që ofron shërbimet e tij.	CSIRT-i duhet të ketë të përcaktuara përgjegjësitë që burojnë nga mandati dhe autoriteti i tij.
O-5 Përshkrimi i shërbimeve	Përshkrimi i shërbimeve që ofron CSIRT-i dhe mënyra për të kontaktuar me të.	Duhet të përmbajë informacion kontakti, oraret e shërbimit, përshkrimin e shërbimeve dhe politikën për trajtimin e informacionit.
O-6 Politika për mediat publike	Politikat për ndërveprim me median publike dhe rrjetet sociale.	CSIRT-i duhet të ketë një politikë për menaxhimin e marrëdhënieve me median në raste incidentesh kibernetike, fushata informuese apo raste krizash të sigurisë kibernetike.
O-7 Përshkrimi i niveleve të shërbimit	Përshkrimi i niveleve të shërbimit që mund të priten nga CSIRT-i.	Reagim nga personeli i autorizuar ndaj çdo kërkese apo komunikimi të ardhur nga ekipet homologe, brenda një afati prej jo më shumë se 2 (dy) ditë pune nga momenti i marrjes së kërkesës.
O-8 Klasifikimi i incidenteve kibernetike	Përdorimi i një skeme klasifikimi të incidenteve kibernetike që përfshin llojin, rëndësinë dhe prioritetin.	CSIRT-i duhet të ketë një skemë klasifikimi të incidenteve kibernetike, përfshirë llojin dhe rëndësinë e tyre.
O-9 Pjesëmarrja në rrjetet e CSIRT-eve në nivel kombëtar dhe ndërkombëtar	Pjesëmarrja e CSIRT-it në rrjete bashkëpunimi kombëtare dhe ndërkombëtare.	CSIRT duhet të marrë pjesë në rrjete bashkëpunimi, direkt ose përmes një CSIRT-i të nivelit më të lartë.
O-10 Korniza organizative	Dokumenti ku përfshihen të gjitha parametrat *O-1* deri *O-9* në një kuadër të integruar.	Duhet të ekzistojë një dokument kuadër që përmbledh misionin dhe të gjithë parametrat *O-1* deri *O-9* të CSIRT-it.
O-11 Politika e sigurisë	Politikat e sigurisë dhe qëndrueshmërisë operative të CSIRT-it, përfshirë *BCM*.	Duhet të ketë një politikë sigurie që mbulon nevojat specifike të CSIRT-it dhe *BCM*, në përputhje me politikën e CSIRT-it.

8.1.2 Parametri H – Burime Njerëzore

Burimet Njerëzore është një parametër thelbësor për qëndrueshmërinë dhe profesionalizmin e një CSIRT-i. Ky parametër fokusohet në cilësinë, trajnimin, përbërjen dhe zhvillimin e vazhdueshëm të stafit teknik dhe menaxherial.

Elementët kyç të parametrit të Burimeve Njerëzore:

Parametri	Përshkrim	Kërkesa minimale për CSIRT
H-1 Kodi i sjelljes / praktikës / etikës	Rregulla ose udhëzime për sjellje profesionale dhe etike për anëtarët e CSIRT-it që mund të shtrihen edhe jashtë vendit të punës.	CSIRT-i duhet të ketë një kod të sjelljes ose etike specifik për mënyrën e organizimit të punës së tij dhe për të dhënat sensitive, jo vetëm të mbështetur në rregullat e përgjithshme të CSIRT-it.
H-2 Qëndrueshmëria e Stafit	Sigurimi i vazhdimësisë së punës në raste mungesash të stafit për shkaqe: si pushime, sëmundje ose dorëheqje.	CSIRT-i sektorial duhet të ketë në strukturën e vet minimumi 4 anëtarë, ndërsa CSIRT-i pranë operatorit të infrastrukturës kritike së informacionit duhet të ketë jo më pak se 2 anëtarë në strukturën e vet, për të garantuar qëndrueshmërinë e stafit dhe aftësinë e ekipit për të përballuar situata të paparashikuara.
H-3 Përshkrimi i aftësive dhe detyrave	Përshkrimi i aftësive të kërkuara për çdo pozicion brenda CSIRT-it.	Të gjitha pozicionet në CSIRT duhet të kenë të përcaktuara aftësitë teknike dhe personale të nevojshme dhe detyrat përkatëse që do të kryej çdo anëtarë, pjesë e strukturës së CSIRT-it.
H-4 Zhvillimi profesional i stafit	Politika për zhvillimin profesional të stafit përmes trajnimeve profesionale të vazhdueshme.	CSIRT-i duhet të ketë një politikë zhvillimi të stafit që përfshin trajnimet për anëtarët e rinj dhe ekzistues.
H-5 Trajnimi teknik	Program trajnimesh për zhvillimin e aftësive teknike të stafit të CSIRT-it.	CSIRT-i duhet të ofrojë trajnim teknik për zhvillimin e njohurive dhe aftësive teknologjike të stafit në përputhje me rolet e tyre.
H-6 Trajnimi për aftësi personale *(soft skills)*	Program trajnimesh për zhvillimin e aftësive personale si komunikimi, menaxhimi i kohës dhe kryerja e punës në kushtet e presionit.	CSIRT-i duhet të sigurojë trajnim në aftësi personale për të gjithë anëtarët e ekipit, përfshirë komunikimin dhe prezantimin.
H-7 Ndërtimi dhe ruajtja e marrëdhënieve bashkëpunuese me aktorë të jashtëm	Pjesëmarrja e stafit në takime dhe aktivitete me ekipe të tjera CSIRT dhe organizata të sigurisë.	CSIRT-i duhet të ketë një politikë që inkurajon pjesëmarrjen e stafit në rrjete bashkëpunimi CSIRT në nivel kombëtar dhe ndërkombëtar.

8.1.3. Roli i stafit dhe profili profesional

Funksionimi efektiv i një CSIRT-i kërkon një strukturë të qartë rolesh dhe staf të kualifikuar me kompetenca të dokumentuara, të ndara sipas fushave teknike, menaxheriale dhe komunikimi. Në tabelën më poshtë paraqitet përshkrimi i roleve bazë të stafit në një CSIRT funksional, së bashku me përgjegjësitë kryesore dhe kualifikimet e rekomanduara.

Roli në CSIRT	Përgjegjësitë Kryesore	Kualifikimet e Rekomanduara
Menaxher CSIRT	- Drejton në nivel strategjik dhe operativ strukturën e CSIRT-it. - Përfaqëson dhe raporton pranë AKSK dhe institucioneve të tjera rregullatorë sipas sektorëve si dhe në nivele më të larta menaxheriale brenda strukturës. - Mbikëqyr planet e vazhdimësisë së biznesit (*BCM)* dhe të vetëvlerësimit.	-Rekomandohet që të ketë diplomë Master në Teknologji Informacioni dhe Komunikimi, Siguri Informacioni ose Siguri Kibernetike; -Përvojë në menaxhimin e sigurisë kibernetike (afërsisht 5+ vite); -Certifikime të tilla si *SIM3, CISM, CISSP* ose ekuivalente përbëjnë avantazh.
Analist Teknik	- Analizon incidentet kibernetike dhe zbaton parimin CIA; - Monitoron në kohë reale trafikun dhe alarmet - Kryen ekzaminim digjital (digital forensic) dhe analizë log-esh.	Diplomë Bachelor në Teknologji Informacioni dhe Komunikimi, Informatikë ose fusha të ngjashme; Përvojë me mjete të analizës së sigurisë *si SIEM, IDS/IPS*; Certifikime si *CEH, CompTIA Security+, ECIH* përbëjnë avantazh.
Inxhinier Sigurie (SOC/Infrastructure)	- Konfiguron dhe mirëmban mjetet teknike (*SIEM, SOAR, IDS/IPS*); - Kryen kontrolle teknike për parandalim dhe zbulim e incidenteve kibernetike; - Të njohë e topologjitë e rrjeteve dhe arkitekturat e mbrojtjes.	Diplomë në Teknologji Informacioni dhe Komunikimi, Inxhinieri ose fusha të ndërlidhura; Eksperiencë praktike me mjete të sigurisë teknike dhe sisteme automatizimi; Certifikime si *CompTIA CyberOps, GIAC, CCNA Security* janë avantazh
Koordinator Komunikimi/Person kontakti	- Raporton incidentet kibernetike sipas klasifikimit të tyre (*TLP*); - Ndan informacioni me partnerët institucionalë; - Komunikon me publikun dhe shtypin në raste incidentesh kibernetike.	Diplomë në Teknologji Informacioni dhe Komunikimi, Komunikim Teknik, Marrëdhënie Publike ose fusha të ngjashme; Aftësi të forta të shkrimit dhe komunikimit; Njohuri mbi protokollet dhe standardet bazë të sigurisë së informacionit përbëjnë avantazh.

8.1.4. Parametri T – Mjetet Teknike

Mjetet Teknike *(tools)* i referohet infrastrukturës teknologjike që mbështet funksionimin operativ të CSIRT-it. Mjetet teknike përfshijnë sisteme, aplikacione, platforma dhe protokolle komunikimi

që ndihmojnë në zbulimin, analizimin, trajtimin dhe raportimin e incidenteve të sigurisë kibernetike.

Elementët kyç të parametrit Mjeteve Teknike, janë si më poshtë vijojnë:

Parametri	Përshkrim	Kërkesa minimale për CSIRT
T-1 Asetet dhe konfigurimet IT	Përshkrimi i pajisjeve (*IT/OT*) dhe konfigurimeve në përdorim të përdoruesve të CSIRT-it.	CSIRT-i duhet të ketë akses në një listë të përditësuar dhe të detajuar të aseteve kritike të *IT/OT*, përfshirë konfigurimet teknike të tyre.
T-2 Lista e burimeve të informacionit	Lista e burimeve të informacionit për kërcënime, dobësi dhe monitorim të sigurisë apo skanime.	CSIRT-i duhet të ketë një listë të mirëmbajtur të burimeve të informacionit për të ndjekur zhvillimet në sigurinë kibernetike.
T-3 Sisteme të konsoliduara të komunikimit	Sisteme të konsoliduara komunikimi (email, aplikacione mesazhesh) me akses për të gjithë anëtarët e CSIRT-it.	CSIRT-i duhet të përdorë një sistem të besueshëm mesazhesh që mundëson ndarjen e informacionit mes anëtarëve të ekipit.
T-4 Sistemi për gjurmimin e incidenteve kibernetike	Sistem për regjistrimin dhe ndjekjen e incidenteve kibernetike (p.sh. *RT(IR), OTRS, TheHive*).	CSIRT-i duhet të përdorë një sistem të specializuar për ndjekjen e incidenteve kibernetike, përveç rasteve shumë të vogla kur një *spreadsheet* mund të jetë i mjaftueshëm.
T-5 Sisteme telefonike të qëndrueshme (*në kushte emergjence*)	Sistem telefonik ose zgjidhje komunikimi zanore me qëndrueshmëri dhe disponueshmëri të lartë.	CSIRT-i duhet të ketë një mekanizëm rezervë për rastet kur sistemi i thirrjeve zanore bie nga funksioni.
T-6 Mesazhe të qëndrueshme (komunikim emergjent)	Sistemet e mesazheve duhet të kenë qëndrueshmëri të lartë dhe të përmbushin kërkesat e nivelit të shërbimit.	CSIRT-i duhet të sigurojë që sistemet e mesazheve të jenë funksionale dhe me kopje rezervë për ruajtjen e të dhënave.
T-7 Akses i qëndrueshëm në internet	Akses në internet me disponueshmëri të lartë që përputhet me nevojat e shërbimit të CSIRT-it.	CSIRT-i duhet të ketë një linjë rezervë për qasje në internet ose një konfigurim të fortë *redundant*.
T-8 Paketë mjetesh për parandalimin e incidenteve kibernetike	Grup mjetesh *(tools)* për parandalimin e incidenteve kibernetike (*IPS*, antivirus, skanerë dobësish, etj.).	CSIRT-i duhet të përdorë ose të ketë akses në një grup të përcaktuar të qartë mjetesh *(tools)* për parandalimin e incidenteve kibernetike.

T-9 Paketë mjetesh për zbulimin e incidenteve kibernetike	Grup mjetesh *(tools)* për zbulimin e incidenteve kibernetike (*IDS, netflow, MISP*, etj.).	CSIRT-i duhet të përdorë ose të ketë akses në mjetet *(tools)* për zbulimin e incidenteve kibernetike dhe të ketë të përcaktuar rolin e tij për secilën.
T-10 Paketë mjetesh për zgjidhjen e incidenteve kibernetike	Grup mjetesh *(tools)* për zgjidhjen e incidenteve kibernetike pas ndodhjes së tyre (*forensic kits*, analizues *malware*, etj.).	CSIRT-i duhet të ketë një grup të qartë mjetesh *(tools)* për zgjidhjen e incidenteve dhe të jetë i përfshirë në përzgjedhjen dhe përdorimin e tyre.

8.1.5. Parametri P – Proceset Operacionale

Proceset Operacionale fokusohet në funksionimin real të një CSIRT-i në trajtimin e incidenteve kibernetike dhe menaxhimin e operacioneve të përditshme. Ky parametër mbulon të gjitha procedurat, rregullat dhe mekanizmat e punës, të cilat mundësojnë identifikimin, trajtimin dhe mbylljen efektive të incidenteve të sigurisë kibernetike, si dhe përfshin aktivitetet për parandalim, raportim dhe përmirësim të vazhdueshëm.

Elementët kyç të parametrit Proceset Operacionale, janë si vijon:

Parametri	**Përshkrim**	**Kërkesa minimale për CSIRT**
P-1 /Përshkallëzim i incidenteve kibernetike drejt niveleve drejtuese brenda infrastrukturës.	Procesi i përshkallëzimit të incidenteve kritike brenda strukturës së vet si dhe drejt autoriteteve të tjera.	CSIRT-i duhet të jetë në gjendje të përshkallëzojë incidente kritike në nivelet e duhura drejtuese në çdo kohë në bazë të një politike apo procedurë të miratuar.
P-2 Komunikimi me Median	Procesi i komunikimit me zyrën për media të strukturës mbështetëse të CSIRT-it	CSIRT-i duhet të ketë një mekanizëm për të informuar zyrën e shtypit në kohë dhe jashtë orarit zyrtar, në rast incidentesh kibernetike të cilat janë në interes të publikut.
P-3 Përshkallëzim i incidentit kibernetik drejt ekspertëve ligjorë	Procesi i njoftimit të zyrës ligjore për trajtimin e kërkesave nga ana ligjore.	CSIRT-i duhet të jetë në gjendje të kontaktojë me ekspertë ligjorë në kohë reale, sidomos në raste urgjente.
P-4 Procesi i parandalimit të incidenteve kibernetike	Procesi për parandalimin e incidenteve kibernetike përmes përdorimit të mjeteve teknike dhe shërbimeve proaktive si: paralajmërime për kërcënime, dobësi dhe përditësime sigurie.	CSIRT-i duhet të ketë një proces të strukturuar për parandalimin e incidenteve kibernetike , që përfshin njoftimet për kërcënime, monitorimin proaktiv dhe komunikimin e masave parandaluese tek strukturat përkatëse.
P-5 Procesi i zbulimit të	Procesi i zbulimit të incidenteve kibernetike, përfshirë gjenerimin	CSIRT duhet të ketë një proces të qartë për zbulimin dhe kategorizimin e

incidenteve kibernetike	e alarmeve dhe përdorimin e mjeteve për zbulim.	incidenteve kibernetike, përfshirë gjenerimin e alarmeve.
P-6 Procesi i zgjidhjes së incidenteve kibernetike	Procesi për analizën dhe zgjidhjen e incidenteve kibernetike nga momenti i zbulimit deri në zgjidhjen dhe mësimet e nxjerra.	CSIRT duhet të ketë një proces të detajuar për zgjidhjen e incidenteve kibernetike sipas praktikave të standardizuara.
P-7 Procese të veçanta për incidente kibernetike specifike	Proceset për trajtimin e llojeve specifike të incidenteve kibernetike (p.sh. *phishing*, *DDoS*).	CSIRT duhet të ketë të përcaktuara proceset për trajtimin e incidenteve kibernetike të zakonshme ose specifike që kërkojnë qasje të veçantë.
P-8 Procesi i kontrollit dhe mekanizmit të *feedback*-ut	Procesi i kontrollit dhe kthimit të informacionit te ekipi për përmirësim të vazhdueshëm.	CSIRT-i duhet të ketë një proces kontrolli që përfshin vlerësim të jashtëm dhe reagim nga organet drejtuese/struktura e larte drejtuese.
P-9 Procesi për komunikime emergjente	Procesi që përcakton njoftimin e e CSIRT-it në raste emergjente jashtë orarit zyrtar.	CSIRT duhet të ketë kontakt emergjent dhe proces për trajtimin e rasteve emergjente nga personeli i autorizuar
P-10 Procesi i identifikimit të praktikave më të mira në internet	Procesi për menaxhimin e adresave të postës elektronike për çështje sigurie, faqes në internet dhe pranisë në rrjetet sociale.	CSIRT duhet të ketë mekanizma për monitorimin e adresave të postës elektronike, si dhe të ketë një politikë të qartë për përdorimin e rrjeteve sociale.
P-11 Procesi për trajtimin e sigurt të informacionit	Procesi për trajtimin e informacionit konfidencial, duke përfshirë përdorimin e *TLP* dhe përputhjen me kërkesat ligjore në fuqi (p.sh. *mbrojtja e të dhënave personale*).	CSIRT-i duhet të trajtojë të dhënat me ndjeshmëri të lartë duke respektuar protokollin *TLP*, konfidencialitetin e informacionit dhe kërkesat ligjore në fuqi.
P-12 Procesi për përdorimin e burimeve të informacionit	Procesi për identifikimin, monitorimin dhe vlerësimin e burimeve të informacionit për sigurinë.	CSIRT-i duhet të ketë një proces të formalizuar për administrimin e burimeve të informacionit si listat, bazat e dobësive, etj, përfshirë mekanizma për heqjen e burimeve të papërdorshme.
P-13 Procesi i ndërgjegjësimit dhe komunikimit të jashtëm	Procesi për ndërveprim me përdoruesit për promovim dhe ndërgjegjësim, përfshirë një kanal të dyanshëm komunikimi.	CSIRT-i duhet të ketë një proces të formalizuar për ndërveprim të vazhdueshëm me përdoruesit përmes informimit dhe mbledhjes së komenteve.
P-14 Procesi i raportimit sipas nivelit hierarkik brenda infrastrukturës	Procesi i raportimit ndaj niveleve të larta drejtuese, përfshirë statistika dhe analizë incidentesh kibernetike.	CSIRT-i duhet të ketë një proces të formalizuar për raportim të rregullt dhe të strukturuar tek nivelet e larta drejtuese.
P-15 Procesi i raportimit	Procesi i raportimit drejt autoriteteve përgjegjëse ose publikut kur është e nevojshme, p.sh. raportime mujore/vjetore.	CSIRT-i duhet të ketë një proces të qartë për raportim të incidenteve kibernetike drejt autoriteteve përgjegjëse , që përfshin statistika dhe informacione të dobishme për sigurinë, bazuar në klasifikimin e incidenteve kibernetike.

P-16 Procesi i mbajtjes së takimeve	Procesi i organizimit të takimeve të brendshme të ekipit, fizike apo online.	CSIRT-i duhet të sigurojë një minimum takimesh në mënyrë të rregullt, dokumentimin e pikave të veprimit, me ndarje detyrash dhe diskutime për mësime të nxjerra.
P-17 Procesi i bashkëpunimit me CSIRT-e partnere	Procesi për bashkëpunim me ekipe homologe (CSIRTs, SOCs, etj.).	Duhet të jenë të përcaktuar partnerët homologë dhe mënyrat e bashkëpunimit të ndërsjellë.

9. Kontrolli dhe përmirësimi i vazhdueshëm i CSIRT-eve

Me qëllim forcimin e performancës së CSIRT-ve, rritjen e qëndrueshmërisë operacionale, kjo rregullore përcakton një proces të strukturuar për kontroll dhe përmirësim të vazhdueshëm.

Ky proces do të fokusohet në këto mekanizma:

- Vetëvlerësim të parametrave (O- Organizim, H- Burime Njerëzore, P- Procese Operacionale, T - Mjete Teknike);
- Vlerësim të jashtëm, përmes intervistave, vizitave në terren dhe analizës së dokumentacionit zyrtar;
- Simulime teknike dhe testime me skenarë realë për të vlerësuar reagimin ndaj incidenteve;
- Matje të performancës bazuar në indikatorë kyç (*KPI*), si koha e reagimit, rikuperimi, numri i incidenteve të mbyllura, raportet pas incidenteve dhe pjesëmarrja në trajnime.

9.1. Indikatorë kyç të performancës (KPI) për CSIRT-et

Për vlerësim objektiv dhe të krahasueshëm të efikasitetit të CSIRT-ve, rregullorja parashikon përdorimin e një grupi indikatorësh kyç të performancës (*KPI*). Këta indikatorë shërbejnë për të matur aftësinë operacionale të ekipit, për të analizuar trendet dhe për të orientuar përmirësimet.

KPI	**Përshkrimi**
Koha mesatare e reagimit *(MTTR)*	Koha nga njoftimi deri në ndërhyrje nw rast incidenti kibernetik
Koha për rikuperim *(MTTR-R)*	Koha deri në rikthimin në gjendje funksionale tw infrastrukturws
Numri i incidenteve të trajtuara	Raportim mujor për incidente të mbyllura
Raportet pas incidentit *(PIR)*	Raporte të dokumentuara për analiza dhe mësime
Angazhimi në trajnime	Numri i sesioneve dhe pjesëmarrësve në vit

9.2 Roli i AKSK për mbështetjen e CSIRT-eve

AKSK do të ofroj mbështetje të vazhdueshme për CSIRT-et në drejtim të zhvillimit të kapaciteteve dhe zbatimit të rekomandimeve të vlerësimit, përmes:

- Ofrimit të modeleve standarde për planet e përmirësimit;
- Trajnimeve dhe asistencës teknike për CSIRT-et që kërkojnë ndihmë specifike;
- Organizimit të workshop-eve vjetore për shkëmbim përvojash dhe praktika të mira;

10. Vetëvlerësimi dhe kontrolli

Në kuadër të garantimit të cilësisë dhe përmirësimit të vazhdueshëm të funksionimit të CSIRT-eve, dhe në përputhje me përcaktimet e kësaj rregulloreje çdo CSIRT ka detyrimin të kryejë një vetëvlerësim një herë në vit, me qëllim vlerësimin objektiv të kapaciteteve dhe funksioneve të tij, si dhe identifikimin e fushave me nevojë për përmirësim. Ky vetëvlerësim do të kryhet për çdo parametër (O- Organizim, H- Burime Njerëzore, P- Procese Operacionale, T - Mjete Teknike);

Vetëvlerësimi ka për qëllim të identifikojë boshllëqet, të vlerësojë progresin e arritur dhe të krijojë bazën për hartimin e një plani konkret për përmirësim të mëtejshëm.

Rezultatet e vetëvlerësimit duhet të dokumentohen dhe të gjitha gjetjet i dërgohen CSIRT-it Kombëtar, në funksion të transparencës, analizës së të dhënave dhe përmirësimin e vazhdueshëm të kapaciteteve të CSIRT-it sektorial dhe atij pranë operatorit të infrastrukturave të informacionit.