VENDIM
Nr. 531, datë 25.9.2025

PËR PËRMBAJTJEN DHE MËNYRËN E DOKUMENTIMIT TË MASAVE ORGANIZATIVE, TEKNIKE DHE OPERACIONALE TË SIGURISË KIBERNETIKE DHE KATEGORIZIMIN E AFATEVE TË MASAVE KORRIGJUESE NË INFRASTRUKTURAT KRITIKE E TË RËNDËSISHME TË INFORMACIONIT

Në mbështetje të nenit 100 të Kushtetutës dhe të neneve 20, pika 5, e 43, pika 5, të ligjit nr. 25/2024, "Për sigurinë kibernetike", me propozimin e Kryeministrit, Këshilli i Ministrave

VENDOSI:

1. Miratimin e përmbajtjes dhe mënyrës së dokumentimit të masave organizative, teknike dhe operacionale të sigurisë kibernetike në infrastrukturat kritike e të rëndësishme të informacionit dhe të kategorizimit të afateve të masave korrigjuese, sipas tekstit që i bashkëlidhet këtij vendimi dhe është pjesë përbërëse e tij.
2. Ngarkohen operatorët e infrastrukturave kritike të informacionit dhe operatorët e infrastrukturave të rëndësishme të informacionit për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

KRYEMINISTËR
Edi Rama

PËRMBAJTJA DHE MËNYRA E DOKUMENTIMIT TË MASAVE ORGANIZATIVE, TEKNIKE DHE OPERACIONALE TË SIGURISË KIBERNETIKE DHE KATEGORIZIMI I AFATEVE TË MASAVE KORRIGJUESE NË INFRASTRUKTURAT KRITIKE E TË RËNDËSISHME TË INFORMACIONIT

KREU I
DISPOZITA TË PËRGJITHSHME

1. Ky vendim ka për qëllim përcaktimin e mënyrës së dokumentimit dhe verifikimit të implementimit të masave organizative, teknike dhe operacionale nga operatorët e infrastrukturave kritike të informacionit (OIKI) dhe operatorët e infrastrukturave të rëndësishme të informacionit (OIRI) dhe të kategorizimit të afateve të masave korrigjuese.
2. Dispozitat e këtij vendimi zbatohen nga të gjithë operatorët e infrastrukturave kritike të informacionit dhe operatorët e infrastrukturave të rëndësishme të informacionit.
3. Dispozitat e këtij vendimi zbatohen pa cenuar zbatimin e kërkesave të sigurisë së rrjeteve dhe shërbimeve të komunikimeve elektronike të përcaktuara në kreun VII "Siguria", të ligjit nr. 54/2024, "Për komunikimet elektronike në Republikën e Shqipërisë".
4. Përkufizimet në këtë vendim kanë të njëjtin kuptim sipas legjislacionit në fuqi për sigurinë kibernetike.

KREU II
KATEGORIZIMI DHE KLASIFIKIMI I MASAVE TË SIGURISË KIBERNETIKE

1. Masat e sigurisë kibernetike që zbatohen nga operatorët e infrastrukturave kritike të informacionit dhe operatorët e infrastrukturave të rëndësishme të informacionit ndahen në tri kategori kryesore: masa organizative, masa teknike dhe masa operacionale të sigurisë kibernetike.

2. Masat organizative të sigurisë kibernetike janë veprime administrative dhe procedurale, të ndërmarra nga operatorët e infrastrukturave kritike e të rëndësishme të informacionit, duke përfshirë, ndër të tjera, ndarjen e roleve dhe përgjegjësive për sigurinë, hartimin dhe miratimin e politikave dhe procedurave të sigurisë, menaxhimin e rrezikut kibernetik, ndërgjegjësimin dhe trajnimin e burimeve njerëzore, si dhe ndërtimin e një strukture organizative të dedikuar për sigurinë kibernetike.

3. Masat teknike të sigurisë kibernetike janë zgjidhje dhe mekanizma teknologjikë, që garantojnë mbrojtjen dhe integritetin e rrjeteve të komunikimit dhe sistemeve të informacionit të operatorëve të infrastrukturave të informacionit, duke përfshirë zbatimin e kontrollit të aksesit, autentifikimin dhe autorizimin, enkriptimin e të dhënave, monitorimin dhe regjistrimin e ngjarjeve të sigurisë, mbrojtjen nga sulmet kibernetike, si dhe zbatimin e teknologjive për zbulimin dhe parandalimin e incidenteve të sigurisë kibernetike.

4. Masat operacionale të sigurisë kibernetike janë proceset, praktikat dhe aktivitetet e përditshme të operatorëve të infrastrukturave të informacionit për garantimin e sigurisë së informacionit dhe funksionimin e qëndrueshëm të sistemeve kritike e të rëndësishme, duke përfshirë menaxhimin e incidenteve të sigurisë kibernetike, sigurimin e vazhdimësisë së shërbimeve dhe rikuperimin nga katastrofat, menaxhimin e ndryshimeve në infrastrukturë, si dhe aplikimin e procedurave për raportim dhe komunikim të ngjarjeve të sigurisë me autoritetet përgjegjëse.

5. Masat e sigurisë kibernetike të kategorizuara në masa organizative, masa teknike dhe masa operacionale klasifikohen në dy nivele:

a) niveli i parë (1): I detyrueshëm për t'u zbatuar nga operatorët e infrastrukturave të rëndësishme të informacionit (OIRI) dhe operatorët e infrastrukturave kritike të informacionit (OIKI);

b) niveli i dytë (2): I detyrueshëm për t'u zbatuar nga operatorët e infrastrukturave kritike të informacionit (OIKI).

6. Për çdo masë të sigurisë kibernetike (MS1, MS2 etj.), operatorët e infrastrukturave të informacionit duhet të dokumentojnë dhe duhet të mbajnë evidenca për zbatimin dhe implementimin e tyre, në përputhje me kërkesat e këtij vendimi.

7. Masat e sigurisë kibernetike dhe mënyra e dokumentimit të tyre përbëjnë listën e kërkesave minimale për implementim nga OIKI-ja dhe OIRI-ja.

KREU III
MASAT ORGANIZATIVE

1. Masat organizative përfshijnë:

1.1 MS1: Politika e sigurisë

Politika e sigurisë përfshin objektivat e sigurisë që lidhen me qeverisjen dhe menaxhimin e rreziqeve të sigurisë së rrjeteve të komunikimit dhe sistemeve të informacionit.

Niveli	Masa e sigurisë	Dokumentimi/verifikimi i implementimit
1	a. Vendosja e një politike sigurie të nivelit të lartë, e miratuar nga stafi i lartë menaxherial i infrastrukturës, që adreson sigurinë e rrjeteve të komunikimit dhe sistemeve kritike e të rëndësishme të informacionit dhe rishikimi në mënyrë periodike i saj. (Minimumi 1 (një) herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturën e OIKI-së/OIRI-së.)	i. Politika e sigurisë së informacionit - Dokument i miratuar nga stafi i lartë menaxherial, që përmban objektivat, fushën e zbatimit dhe parimet e sigurisë për rrjetet dhe sistemet e informacionit etj. - Versioni, data e miratimit etj. ii. Raportet e rishikimit periodik - Evidencat që tregojnë datat e rishikimit dhe detajet e ndryshimeve të bëra në politikën e sigurisë.

1.2 MS2: Menaxhimi i rrezikut kibernetik

Të krijohet e të zbatohet një kuadër i përshtatshëm i menaxhimit të rrezikut për të identifikuar

dhe për të trajtuar rreziqet kibernetike për rrjetet e komunikimit dhe sistemet e informacionit.

Niveli	Masat e sigurisë	Dokumentimi/verifikimi i implementimit
1	a. Krijimi i një metodologjie për menaxhimin e rrezikut kibernetik. (Rishikimi minimumi 1 (një) herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturën e OIKI-së/OIRI-së).	i. Dokument i metodologjisë së menaxhimit të rrezikut kibernetik, duke përfshirë versionin, datat dhe miratimin nga stafi menaxherial. ii. Raportet e rishikimit periodik - Evidencat që tregojnë datat e rishikimit dhe detajet e ndryshimeve të bëra në metodologjinë për menaxhimin e rrezikut.
1	b. Hartimi i një liste të rreziqeve për sigurinë e rrjeteve të komunikimit dhe sistemeve të informacionit, duke marrë në konsideratë kërcënimet kryesore për asetet kritike. (Rishikimi minimumi 1 (një) herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturën e OIKI-së/OIRI-së.)	i. Lista e vlerësimit të rreziqeve të ardhura nga burime të ndryshme, duke përfshirë dhe rreziqet, të cilat vijnë nga palët e treta. ii. Njoftimi i stafit menaxherial për listën e rreziqeve, si dhe vendimi i marrë për trajtimin e tyre. iii. Rishikim i listës së rreziqeve.
1	c. Hartimi i një plani për trajtimin e rreziqeve të identifikuara.	i. Dokument i planit për trajtimin e rreziqeve. ii. Pasqyrimi i ndryshimeve të nivelit të rrezikut mbas zbatimit të planit të trajtimit të rreziqeve.

1.3 MS3: Siguria organizative

Të krijohet e të zbatohet një strukturë e përshtatshme e roleve të sigurisë dhe përgjegjësive për menaxhimin e sigurisë së informacionit.

Niveli	Masat e sigurisë	Dokumentimi/verifikimi i implementimit
1	a. Caktimi i roleve dhe përgjegjësive për menaxhimin e sigurisë së informacionit.	i. Lista e roleve të sigurisë dhe përshkrimi i detajuar i përgjegjësive e i detyrave për secilin rol p.sh. (*CISO, ISO, DPO, DBA, SYSADM, NETADM* etj.). ii. Organigrama që tregon hierarkinë dhe lidhjet midis roleve të sigurisë. iii. Lista e kontakteve për personat përgjegjës për sigurinë e informacionit (emër, pozicion, mënyra e kontaktit).

1.4 MS4: Kërkesat e sigurisë kibernetike për palët e treta

Të krijohet e të zbatohet një politikë me kërkesa sigurie për kontratat me palët e treta për të siguruar që marrëdhëniet me palët e treta të mos ndikojnë negativisht në sigurinë e rrjeteve të komunikimit e të sistemeve të informacionit.

Niveli	Masat e sigurisë	Dokumentimi/verifikimi i implementimit
1	a) Vendosja e një politike sigurie për furnizimet/ kontratat me palët e treta dhe rishikimi në mënyrë periodike i saj. (Minimumi 1 (një) herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturën e OIKI-së/OIRI-së.)	i. Politika e sigurisë për furnizimet/ kontratat me palët e treta (versioni, data e publikimit, miratimi). ii. Raporte të rishikimit periodik të politikës së sigurisë dhe ndryshimet e realizuara.
1	b) Përfshirja e kërkesave të sigurisë në kontratat me palët e treta, duke përfshirë konfidencialitetin dhe transferimin e sigurt të informacionit.	i. Kërkesa të qarta sigurie në kontratat me palët e treta. ii. Marrëveshje konfidencialiteti për ruajtjen e informacionit me palët e treta.
2	c) Mbajtja e gjurmëve/rekordeve të incidenteve të sigurisë kibernetike, që lidhen ose janë të shkaktuara nga palët e treta.	i. Regjistri i incidenteve kibernetike të lidhura me palët e treta (data, shkaku, ndikimi, veprimet).

1.5 MS5: Siguria e burimeve njerëzore dhe aksesit të personave

Të vendoset e të zbatohet një politikë për sigurinë dhe ndërgjegjësimin e burimeve njerëzore, si dhe të aksesit të personave, në bazë të objektivave të sigurisë në lidhje me personelin.

Niveli	Masat e sigurisë	Dokumentimi/verifikimi i implementimit
1	a) Vendosja e një politike sigurie për burimet njerëzore.	i. Politika e sigurisë për burimet njerëzore (përfshirë të gjitha fazat: para rekrutimit, gjatë punësimit, proceset disiplinore, në përfundim të marrëdhënies së punësimit). ii. Dokumenti i verifikimit të integritetit të personelit kryesor (vërtetim të verifikimit të gjendjes gjyqësore (dëshmi penaliteti), referenca të punëve të mëparshme, certifikime, CV etj.). iii. Procedura për mbrojtjen e të dhënave personale.
1	b) Implementimi i një programi trajnimi për sigurinë kibernetike. (Rishikim minimumi 1 (një) herë në vit.)	i. Programi i detajuar i trajnimit, i përshtatur sipas roleve dhe përgjegjësive të punonjësve. ii. Lista e pjesëmarrësve dhe datat e trajnimeve. iii. Dokument i realizimit të fushatave të ndërgjegjësimit/trajnimeve të punonjësve në lidhje me sigurinë kibernetike dhe sulmet e sigurisë kibernetike më të shpeshta si "*Phishing*", "*Malware*" etj.
1	c) Informimi dhe trajnimi i punonjësve të rinj për politikat e procedurat në fuqi për sigurinë kibernetike.	i. Evidenca për trajnimin për punonjësit e rinj. ii. Formularë të nënshkruar nga punonjësit për njohjen e politikave dhe procedurave. iii. Formularë të nënshkruar nga punonjësit për marrëveshjen e konfidencialitetit ("NDA" - *Non Disclosure Agreement).*
2	ç) Testimi i njohurive të punonjësve për sigurinë kibernetike. (Minimumi 1 (një) herë në vit për punonjësit, të cilët përdorin sistemet kritike të informacionit në infrastrukturë dhe/ose më shpesh në varësi të incidenteve kibernetike.)	i. Pyetësorë dhe rezultate testimi për ndërgjegjësimin e punonjësve në lidhje me sigurinë kibernetike.

1.6 MS6: Menaxhimi i aseteve

Të krijohen e të zbatohen procedurat e menaxhimit të aseteve dhe kontrollet e konfigurimit për të siguruar disponueshmërinë e aseteve kritike dhe konfigurimet e rrjeteve të komunikimit e të sistemeve të informacionit.

Niveli	Masat e sigurisë	Dokumentimi/verifikimi i implementimit
1	a. Marrja e masave për identifikimin dhe menaxhimin efektiv të aseteve. (Minimumi 1 (një) herë në vit dhe/ose apo pas çdo ndryshimi madhor në infrastrukturën e OIKI-së/OIRI-së).	i. Inventari i plotë i aseteve të teknologjisë së informacionit ("IT"- *Information Technology*) /teknologjisë operacionale ("OT"- *Operational Technology)*, duke përfshirë p.sh. modelin, kategorinë e aseteve, nr. serie, protokolli i internetit ("*IP*"- *Internet Protocol*), vendndodhjen, vjetërsinë, statusin e tyre etj. ii. Vendosja në inventar i ndikimit, sipas konfidencialitetit, integritetit dhe disponueshmërisë *(*"C/I/A"- *Confidentiality/ Integrity/ Availability)* së asetit.
1	b. Vendosja dhe zbatimi i politikave/ procedurave për menaxhimin e aseteve.	i. Politika/procedura të detajuara për menaxhimin e aseteve, duke përfshirë rolet dhe përgjegjësitë, asetet që janë objekt i kësaj politike/procedure, objektivat e menaxhimit të aseteve, si dhe shkatërrimin e aseteve. (Rishikim minimumi 1 (një) herë në vit dhe/ose pas çdo ndryshimi madhor në infrastrukturën e OIKI-së/OIRI-së.) ii. Topologji e detajuar e rrjetit dhe sistemeve të

		informacionit.
1	c. Marrja e masave për zëvendësimin ose izolimin e sistemeve që iu ka përfunduar cikli i jetës ("EOL"- *End of Life*).	i. Dokument ose evidencë të identifikimit të sistemeve që iu ka përfunduar cikli i jetës (EOL) dhe planifikimi për zëvendësimin/izolimin e tyre. ii. Evidenca të zëvendësimit/izolimit të asetit, i cili ka arritur kohën e ciklit të jetës (EOL). iii. Verifikimi i sistemeve dhe evidencat.
1	ç. Kryerja e azhurnimeve ("*patch-imeve"*) automatike/manuale në sistemet fundore dhe në të gjithë infrastrukturën e teknologjisë së informacionit (IT) dhe teknologjisë operacionale (OT).	i. Procedurë për menaxhimin e zbatimit të azhurnimeve (*patch*-eve) për pajisjet dhe sistemet e teknologjisë së informacionit (IT) dhe teknologjisë operacionale (OT), përfshirë frekuencën, përgjegjësit, rekorde. ii. Verifikimi i sistemeve/ mjeteve ("*tools"*) dhe evidencat.
1	d. Përcaktimi dhe zbatimi i politikave e i kontrolleve të sigurisë për pajisjet personale të përdorura për akses në sistemet dhe të dhënat e infrastrukturës ("BYOD" – *Bring Your Own Device"*), duke siguruar mbrojtjen e informacionit dhe pajtueshmërinë me standardet e sigurisë.	i. Politikë/procedurë për përdorimin e pajisjeve personale (telefona, laptop, tableta etj.), si dhe një inventar të pajisjeve personale të autorizuara për t'u përdorur në rrjetet dhe sistemet e brendshme të infrastrukturës. ii. Evidenca të konfigurimeve minimale të sigurisë së pajisjeve personale sipas politikës.

1.7 MS7: Menaxhimi i incidenteve të sigurisë kibernetike

Të hartohen e të zbatohen plane e procedura për menaxhimin e incidenteve kibernetike, duke përfshirë zbulimin, reagimin, raportimin dhe komunikimin e tyre.

Niveli	Masat e sigurisë	Dokumentimi/verifikimi i implementimit
1	a) Hartimi i planeve dhe procedurave të detajuara për menaxhimin e incidenteve të sigurisë kibernetike. (Rishikim minimumi 1 (një) herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturën e OIKI-së/OIRI-së).	i. Dokumenti i planit për menaxhimin e incidenteve kibernetike (versioni, data, miratimi). ii. Procedura për identifikimin, klasifikimin dhe trajtimin e incidenteve (manual veprimi - "*Playbooks*"), lista e personave të ekipit për reagimin ndaj incidenteve kibernetike).
1	b) Mbajtja e rekordeve për të gjitha incidentet e sigurisë kibernetike.	i. Regjistri i incidenteve që përfshin: datën, shkakun, ndikimin dhe veprimet korrigjuese. ii. Raporte individuale të trajtimit të incidenteve dhe analizat e mësimeve të nxjerra.
1	c) Përcaktimi dhe zbatimi i komunikimeve dhe raportimeve të incidenteve kibernetike me autoritetet dhe njoftimi i palëve të treta dhe klientëve.	i. Formularë raportimi të incidenteve për autoritetet e përcaktuara në legjislacionin në fuqi për sigurinë kibernetike nga ana e infrastrukturës. ii. Inventari i komunikimeve dhe raportimeve.

1.8 MS8: Menaxhimi i ndryshimeve

Të përcaktohen e të zbatohen politikat dhe proceset për menaxhimin e ndryshimeve përmes planifikimit, vlerësimit, miratimit, komunikimit, implementimit dhe monitorimit të ndryshimeve në infrastrukturë.

Niveli	Masat e sigurisë	Dokumentimi/verifikimi i implementimit
1	a. Sigurimi se çdo ndryshim në sistemet dhe proceset e infrastrukturës së teknologjisë së informacionit (IT) brenda infrastrukturës kritike/të rëndësishme, menaxhohet në mënyrë të kontrolluar dhe të dokumentuar.	i. Politika e menaxhimit të ndryshimeve (përfshirë përshkrimin, datën, përgjegjësitë dhe impaktin e parashikuar, planin e zbatimit etj.). (Rishikim minimumi 1 (një) herë në vit.) ii. Procedura e menaxhimit të ndryshimeve (hapat nga propozimi deri tek miratimi dhe implementimi). iii. Formulari i kërkesës për ndryshim ("RFC" – *Request for Change*).

1.9 MS9: Menaxhimi i vazhdimësisë së punës

Të krijohen e të zbatohen plane emergjence dhe një strategji e qartë për të siguruar

vazhdimësinë e rrjeteve të komunikimit e të sistemeve të informacionit.

Niveli	Masat e sigurisë	Dokumentimi/verifikimi i implementimit
1	a. Krijimi dhe zbatimi i një plani të vazhdimësisë së biznesit ("BCP"- *Business Continuity Plan*) për të siguruar funksionimin e vazhdueshëm të proceseve kritike të infrastrukturës në rast të incidenteve kibernetike, fatkeqësive natyrore ose ndërprerjeve operacionale. (Rishikim minimumi 1 (një) herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturën e OIKI-së/OIRI-së).	i. Politika e strategjisë për vazhdimësinë e shërbimeve, duke përfshirë kushtet për aktivizimin e planit, kohën e rikuperimit, komunikimin në kohë krize, skenarët e incidenteve, planin e veprimit, rregullat e testimit etj. ii. Analiza e ndikimit në biznes ("BIA" - *Business Impact Analysis*), identifikimi i proceseve kritike dhe përcaktimi i objektivit të kohës/pikës së rikuperimit ("RTO" – *Recovery Time Objective* / "RPO" –*Recovery Time Objective*). iii. Lista e kontakteve emergjente – informacion për pikat e kontaktit në rast krize.
1	b. Shfrytëzimi i teknikave të pasqyrimit të të dhënave nëpërmjet konfigurimit redundant të disqeve të pavarur ("RAID" – *Redundant Array of Independent Disks*).	i. Verifikimi teknik i konfigurimit redundant të disqeve të pavarur ("RAID") (1/5/6/10) dhe evidencat përkatëse.
1	c. Realizimi i një politike/procedure për kryerjen e kopjeve rezervë (*backup*). (Rishikim minimumi 1 (një) herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturën e OIKI-së/OIRI-së).	i. Dokumenti i politikës/procedurës për kryerjen e kopjeve rezervë (*backup*-it) , duke përfshirë frekuencat, llojet, të dhënat dhe shërbimet. ii. Lista e kopjeve rezervë (*backup*-eve) të kryera dhe raportet e testimit të rikuperimit dhe integritetit të të dhënave.
2	ç. Realizimi i kopjeve rezervë (*backup*-it), duke përdorur teknika, si "*Backup Lock Retention*" ose "*Tape Worm*".	i. Evidenca të përdorimit të teknikave "*Backup Lock Retention*" ose "*Tape Worm*".
2	d. Shmangia e pikave të vetme të dështimit (*Single Point of Failure*) në shërbimet kritike dhe të rëndësishme të infrastrukturës.	i. Verifikimi teknik i pikave të vetme të dështimit. ii. Evidenca për redundancën e shërbimeve.
2	dh. Implementimi i infrastrukturës sipas skemave të shërbimit me disponueshmëri të lartë ("HA" – *High Availability*).	i. Dokument i skemave të infrastrukturës, sipas shërbimit me disponueshmëri të lartë (HA) në nivelet e mbështetjes teknike: L1, L2, L3 dhe perimetrit me mur mbrojtës digjital (*firewall*). ii. Verifikim dhe evidenca.
2	e. Implementimi i një ambienti të dytë për rikuperimin dhe vazhdueshmërinë e funksionimit të sistemeve të teknologjisë së informacionit (IT) pas një incidenti kibernetik ("DRS" – Vendi i rikuperimit nga katastrofa/*Disaster Recovery Site*).	i. Strategjia për DRS-në dhe konfigurimet e detajuara. (Rishikim minimumi 1 (një) herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturën e OIKI-së/OIRI-së). ii. Plani i rikuperimit nga fatkeqësitë (*DRS*), procedurat për rikuperimin e teknologjisë së informacionit (IT) dhe infrastrukturës (detyrat dhe përgjegjësitë, lista e sistemeve dhe aseteve kyçe), (rishikim minimumi 1 (një) herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturën e OIKI-së/OIRI-së). iii. Raporte të testimit të ambientit të dytë për rikuperimin dhe vazhdueshmërinë e funksionimit të sistemeve të teknologjisë së informacionit për rikuperim pas incidenteve/katastrofave (DRS). (Minimumi 1 herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturën e OIKI-së/OIRI-së). iv. Verifikim dhe evidenca.

2	Opsionale: ë) Zbatimi i teknologjisë së rrjetit të përcaktuar nga *Software* ("SDN" – *Software Defined Networking*) që shërbimet dhe aplikacionet kritike të kenë mundësi rikuperimi sa më të shpejtë dhe me një ndërprerje minimale (ose pa ndërprerje) të shërbimeve në rast katastrofash ose incidentesh. f) Zbatimi i teknologjisë "*Blockchain*" për decentralizimin e menaxhimit të të dhënave duke siguruar mbrojtjen e të dhënave dhe paprekshmërinë e tyre gjatë rikuperimit.	i. Strategji për të siguruar që shërbimet dhe aplikacionet kritike (përfshirë ato që mbështeten në teknologjitë e rrjetit të përcaktuar nga *softwar*-i (SDN) dhe "*Blockchain*") të kenë mundësi rikuperimi sa më të shpejtë dhe me një ndërprerje minimale, në rast katastrofash apo incidentesh. ii. Testime periodike të konfigurimeve të teknologjisë së rrjetit të përcaktuar nga *softwar* (SDN) . iii. Verifikimi i zbatimit të teknikës "*Hashing*". iv. Politika e kopjeve rezervë (*backup*) për teknologjinë "*Blockchain*". v. Monitorimi i aktivitetit në "*Blockchain*".

1.10 MS10: Menaxhimi i pajtueshmërisë ligjore

Të krijohet e të zbatohet një politikë për monitorimin e pajtueshmërisë së standardeve me kërkesat ligjore.

Niveli	Masat e sigurisë	Dokumentimi/verifikimi i implementimit
1	a. Monitorimi i pajtueshmërisë së standardeve me kërkesat ligjore.	i. Politikë/procedurë për monitorimin e pajtueshmërisë me standardet dhe kërkesat ligjore. ii. Lista e standardeve dhe kërkesave ligjore të aplikueshme për infrastrukturën. iii. Rishikimi i politikave dhe procedurave për sistemin e menaxhimit të informacionit ("ISMS" – *Information Security Management System*), minimumi 1 (një) herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturën e OIKI-së/OIRI-së.

1.11 MS11: Kontrolli dhe auditimi

Të krijohen e të zbatohen politika e procedura për kryerjen e kontrolleve dhe auditimeve të brendshme e të jashtme, me qëllim monitorimin e pajtueshmërisë dhe përmirësimin e vazhdueshëm të sigurisë së informacionit në infrastrukturë.

Niveli	Masat e sigurisë	Dokumentimi/verifikimi i implementimit
1	a. Politikë/procedurë për kontrollin dhe auditimin e brendshëm për sigurinë e informacionit dhe rishikimi në mënyrë periodike. (Minimumi 1 herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturën e OIKI-së/OIRI-së.)	i. Dokument i politikës/procedurës për kontrolle dhe auditime (versioni, data, miratimi i politikës/procedurës nga stafi menaxherial).
1	b. Kryerja e kontrolleve/auditeve të brendshme ose nga palët e treta për sigurinë e informacionit dhe sistemeve kritike të infrastrukturës. (Minimumi 1(një) herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturën e OIKI-së/OIRI-së.)	i. Raporte të auditimeve të brendshme dhe plani i trajtimit të mangësive (data, metodologjia, rezultatet). ii. Raporte të auditimeve të realizuara nga palët e treta për sigurinë e informacionit. iii. Lista e veprimeve korrigjuese të ndërmarra pas auditimeve dhe evidenca e implementimit të tyre.

KREU IV
MASAT TEKNIKE DHE OPERACIONALE

2. Masat teknike dhe operacionale përfshijnë:

2.1 MS1: Siguria fizike

Të krijohet e të zbatohet siguria e duhur fizike dhe mjedisore e rrjeteve/sistemeve të

informacionit e pajisjeve.

Niveli	Masat e sigurisë	Dokumentimi/verifikimi i implementimit
1	a) Implementimi i masave të sigurisë fizike dhe kontrolleve mjedisore.	i. Evidenca të implementimit të masave të sigurisë fizike (brava, kabinete, kontroll elektronik i hyrjes). ii. Gjurmë të aktiviteteve (*logs*) të auditimit për aksesin në hapësira të autorizuara dhe alarme për hyrjet e paautorizuara. iii. Raporte të funksionimit dhe mirëmbajtjes së sistemeve të alarmit dhe fikësve të zjarrit. iv. Të sigurohet ndarja e hapësirave fizike në zona të segmentuara bazuar në nivelet e autorizimit, duke përfshirë hartimin e një topologjie të detajuar dhe një plani të qartë evakuimi për të garantuar sigurinë fizike dhe menaxhimin e aksesit.
1	b) Implementimi i një politike për masat e sigurisë fizike dhe kontrollet mjedisore.	i. Dokumenti i politikës për sigurinë fizike dhe kontrollet mjedisore (versioni, data, miratimi, rishikimi).

2.2 MS2: Menaxhimi për autorizimin e aksesit

Të krijohen e të mirëmbahen kontrollet e autorizimet e duhura të aksesit në rrjetet e komunikimit dhe sistemet e informacionit.

Niveli	Masat e sigurisë	Dokumentimi/verifikimi i implementimit
1	a) Implementimi i politikave për kontrollin dhe mbrojtjen e aksesit në rrjetet dhe sistemet e informacionit. (Rishikim minimumi 1 (një) herë në vit dhe/ose pas çdo ndryshimi madhor në infrastrukturën e OIKI-së/OIRI-së.)	i. Dokument i politikës për aksesin (role, grupe, të drejta, procedurat e dhënies dhe revokimit të aksesit). ii. Formular për dhënie të drejtash aksesi. iii. Formular për revokim të drejtash aksesi dhe dorëzimi asetesh. iv. Evidenca për fshirjen e llogarive gjenerike dhe raportet e kontrolleve periodike të aksesit.
1	b) Aplikimi i filtrave për trafikun në rastin e aksesimit në distancë të sistemeve, si dhe enkriptimi i trafikut me protokolle të sigurta.	i. Verifikimi teknik dhe evidencat për vendosjen e filtrave dhe enkriptimin e trafikut.
1	c) Kontrolli nëse në murin mbrojtës digjital (*firewall*) ka të konfiguruar lista të autorizuara/lista të bllokuara ("*Whitelist/Blacklist*") të adresave të protokollit të internetit (*IP*) të lejuara ose bllokuara.	i. Verifikim dhe evidenca për konfigurimet në murin mbrojtës digjital (*firewall*).
1	ç. Përdorimi i politikave për menaxhimin e fjalëkalimeve rastësore për përdoruesit dhe administratorët lokalë.	i. Dokumenti i politikës për menaxhimin e fjalëkalimeve dhe verifikim i implementimit të zgjidhjeve për menaxhimin e fjalëkalimeve rastësore për përdoruesit dhe administratorët lokalë ("LAPS"-*Local Administrator Password Solution*) ose teknologji të ngjashme.
2	d. Krijimi dhe implementimi i një zgjidhje teknologjike për menaxhimin e identiteteve dhe aksesit të përdoruesve ("IAM" – *Identity and Access Management)* për të garantuar sigurinë, autorizimin dhe auditimin e aktiviteteve të përdoruesve në sistemet kritike.	i. Verifikim teknik dhe evidenca.
2	dh. Implementimi i një zgjidhjeje teknologjike për menaxhimin e akseseve të privilegjuara ("PAM") – *Privileged Access Management*)	i. Verifikim teknik dhe evidenca.
2	e. Implementimi i shërbimit të sigurisë me akses në rrjet, sipas parimit me zero besim ("ZTNA" - *Zero Trust Network Access*")	i. Verifikim teknik dhe evidenca.

2.3 MS3: Pajisjet kriptografike

Të sigurohet përdorimi i mjaftueshëm i enkriptimit për të parandaluar dhe/ose për të minimizuar ndikimin e incidenteve të sigurisë kibernetike te përdoruesit në rrjetet e komunikimit dhe në sistemet e informacionit.

Niveli	Masat e sigurisë	Dokumentimi/verifikimi i implementimit
1	a) Implementimi i politikave të enkriptimit, duke përfshirë detaje rreth algoritmeve dhe çelësave kriptografikë.	i. Dokumenti i politikës së enkriptimit si p.sh. algoritmet: "*AES*", "*RSA*", "*ECC*", "*TLS*", "*IPSec*", "*SSH*" etj. ii. Lista e çelësave kriptografikë (p.sh., lloji, afati i vlefshmërisë, metoda e gjenerimit dhe ruajtjes).
2	b) Kriptimi i të dhënave (në transit dhe në gjendje të qëndrueshme).	i. Lista e konfigurimeve të kriptimit për të dhënat dhe aplikacionet ("*on-prem*", "*hybrid*", "*cloud*"). ii. Verifikimi teknik dhe evidenca.

2.4 MS4: Zbulimi i incidenteve të sigurisë kibernetike

Të krijohen e të mirëmbahen kapacitete për zbulimin e incidenteve të sigurisë kibernetike.

Niveli	Masat e sigurisë	Dokumentimi/verifikimi i implementimit
1	a) Implementimi i sistemit të automatizuar për zbulimin dhe menaxhimin e informacionit e të incidenteve/ngjarjeve të sigurisë ("*SIEM*" - *Security Information and Event Management*).	i. Verifikim teknik dhe evidenca të konfigurimit të sistemit të automatizuar për zbulimin dhe menaxhimin e informacionit e të incidenteve/ngjarjeve të sigurisë (SIEM), përfshirë rregullat e alarmimit e të filtrimit të gjurmëve dhe aktiviteteve (*log*-eve) për zbulimin e incidenteve.

2.5 MS5: Mbledhja dhe përpunimi i informacionit për kërcënimet kibernetike

Të krijohet e të mirëmbahet një mekanizëm për monitorimin, mbledhjen dhe analizën e informacionit në lidhje me kërcënimet e sigurisë në rrjetet e komunikimit dhe në sistemet e informacionit.

Niveli	Masat e sigurisë	Dokumentimi/verifikimi i implementimit
1	a) Monitorimi i vazhdueshëm i burimeve të jashtme të inteligjencës për kërcënimet kibernetike "*threat intelligence*".	i. Raporte periodike nga mjetet e monitorimit të inteligjencës për kërcënimet kibernetike "*threat intelligence*". ii. Lista e burimeve të përdorura për mbledhjen e informacionit për kërcënimet.
2	b) Zbatimi i programit të inteligjencës për kërcënimet kibernetike "*threat intelligence*", në të cilin të përfshihen rolet, përgjegjësitë dhe procedurat.	i. Dokument i programit të inteligjencës për kërcënimet kibernetike "*threat intelligence*" (përfshirë strukturën e roleve dhe përgjegjësive). ii. Procedura për mbledhjen, përpunimin, analizën dhe shpërndarjen e informacionit për kërcënimet kibernetike.

2.6 MS6: Monitorimi dhe regjistrimi i ngjarjeve të sigurisë kibernetike

Të krijohen e të mirëmbahen sisteme dhe funksione për monitorimin dhe regjistrimin e ngjarjeve të sigurisë në rrjetet kritike e në sistemet e informacionit.

Niveli	Masat e sigurisë	Dokumentimi/verifikimi i implementimit
1	a) Implementimi i politikave për monitorimin dhe regjistrimin e ngjarjeve të sigurisë kibernetike.	i. Dokument i politikave për monitorimin dhe regjistrimin e gjurmëve e të aktiviteteve (*log*-eve), ku përfshihen kërkesat minimale, periudha e mbajtjes, objektivat, miratimi, përditësimi.
1	b) Vendosja e mjeteve për mbledhjen e gjurmëve dhe aktiviteteve (*log*-eve) të sistemeve kritike.	i. Lista e mjeteve të implementuara për mbledhjen e gjurmëve dhe aktiviteteve/ logeve të *log servers* etj. ii. Verifikim teknik dhe evidenca.

2.7 MS7: Mbrojtja e integritetit të rrjeteve të komunikimit

Të krijohet e të ruhet integriteti i rrjeteve dhe sistemeve të informacionit, si dhe të mbrohen nga viruset, injeksionet e kodeve dhe *malware*-ve të tjerë, që mund të ndryshojnë funksionalitetin e sistemeve.

Niveli	Masat e sigurisë	Dokumentimi/verifikimi i implementimit
1	a. Instalimi i pajisjeve për të monitoruar për të kontrolluar dhe për të kufizuar trafikun hyrës e dalës të rrjeteve kompjuterike me murin mbrojtës digjital të gjeneratës së re ("*Next Generation Firewall*").	i. Verifikim teknik për konfigurimin të murit mbrojtës digjital i gjeneratës së re. ii. Verifikimi teknik dhe evidencat.
1	b. Monitorimi, zbulimi dhe analiza e sjelljeve të dyshimta sjellje (*behaviour*) në pajisjet fundore (*endpoints*), si kompjuterët, laptopët dhe serverët. Ky sistem mbledh dhe analizon të dhëna nga pajisjet fundore për të zbuluar kërcënime të sofistikuara.	i. Verifikim teknik dhe evidenca të analizave të trafikut.
1	c. Ndarja e rrjetit në nënrrjete në nivel mikrosegmentimi.	i. Verifikimi teknik dhe evidenca e topologjisë së rrjetit me ndarjen e dokumentuar në nënrrjete.
1	ç. Vendosja në zona/ nënndarje të rrjetit/ rrjet lokal virtual (*zone/subnet/VLAN - Virtual Local Area Network*) të ndryshme e kompjuterëve dhe serverëve me lista të aksesit të kontrollit (*Access Control List*) sipas parimit të të drejtave minimale ("*least privilege*").	i. Lista e rrjet lokal virtual (VLAN*)* dhe nënndarje të rrjetit të implementuara, përfshirë listat e kontrollit të aksesit. ii. Verifikimi teknik dhe evidencat.
1	d. Izolimi i rrjetit pa tela ("*wireless*") nga pjesa tjetër e rrjetit.	i. Verifikim teknik dhe evidencat e konfigurimit të izolimit të rrjetit pa tela (*wireless*).
1	dh. Përdorimi i teknikave të sigurisë së portave të *switch*-it ("*switch port security*") "për të kufizuar numrin e adresave unike të identifikimit të pajisjes së lidhur në rrjet (MAC *Address*) në "1" për përdoruesit e thjeshtë dhe në një numër të kufizuar për ekspertët e teknologjisë të informacionit ose sigurisë kibernetike.	i. Verifikimi teknik i konfigurimit të *switch*-eve, duke zbatuar teknikën e sigurisë së portave "*Port Security*" për numrin unik të identifikimit të pajisjes së lidhur në rrjet (MAC *Address*) të lejuara.
1	e. Zbatimi i teknikave dhe standardeve për fortifikimin ("*hardening*") e të gjitha pajisjeve në rrjet.	i. Manual për fortifikimin e pajisjeve (*PC,* "*server*"*,* "*router*", "*firewall*" etj.). ii. Verifikimi teknik dhe evidencat.
1	ë. Izolimi logjikisht i bazës së të dhënave dhe shërbimet WEB (p.sh. në rrjet lokal virtual/*VLAN)* të ndryshëm).	i. Lista e rrjetit lokal virtual (VLAN) dhe verifikimi teknik i konfigurimit për izolimin logjik të bazës së të dhënave dhe shërbimeve WEB. ii. Verifikimi teknik dhe evidencat.
1	f. Implementimi i "*DNS_SEC*" për të shmangur "*DNS Amplification*" dhe "*DNS Poisoning*".	i. Verifikimi teknik dhe evidencat.
2	g. Zbatimi i mbrojtjes ndaj sulmeve DoS/DDoS.	i. Verifikim teknik i konfigurimit të mekanizmave të mbrojtjes nga DoS/DDoS (p.sh. "*rate limiting*", "WAF" - *Web Application Firewall*, mjete (*tools*) për "*anti-DDoS*").
2	gj. Implementimi i një zgjidhjeje/sistemi për kontrollin e parametrave të sigurisë së pajisjeve fundore ("NAC" - *Network Access Control).*	i. Procedurë për përcaktimin e parametrave të sigurisë minimale (*baseline*). ii. Verifikimi teknik dhe evidencat.

2.8 MS8: Menaxhimi i aksesit të përdoruesve

Të implementohen politikat për menaxhimin e fjalëkalimeve dhe dhënien e aksesit sipas modeleve kontroll diskrecional i aksesit ("DAC"- *Discretionary Access Control*"), kontroll i

detyrueshëm i aksesit ("MAC" -*Mandatory Access Control*") dhe kontroll i aksesit bazuar në role ("RBAC*"* – *Role Based Access Control*). Të përdoret shërbimi *Active Directory* (*AD*) për menaxhimin e privilegjeve dhe kufizimin e aksesit të paautorizuar në pajisje.

Niveli	Masat e sigurisë	Dokumentimi/verifikimi i implementimit
1	a. Implementimi i politikave për menaxhimin e fjalëkalimeve të përdoruesve.	i. Dokument i politikës për menaxhimin e fjalëkalimeve (kompleksiteti, afati i skadimit, ndryshimet periodike).
1	b. Modelet për dhënien e aksesit të përdoruesve (kontroll diskrecional i aksesit (DAC), kontroll i detyrueshëm i aksesit (MAC) dhe kontroll i aksesit bazuar në role (RBAC).	i. Evidenca teknike të konfigurimeve e të rregullave të zbatuara në sistem dhe verifikim.
1	c. Menaxhimi i aksesit dhe privilegjeve të përdoruesve përmes shërbimit "AD".	i. Verifikim teknik dhe evidenca të implementimit të "AD" – në (strukturat e grupeve, privilegjet, kufizimet).
1	ç. Sigurimi dhe mbrojtja e të dhënave dhe kufizimi i aksesit të paautorizuar në informacion.	i. Verifikim i zbatimit të politikës / procedurës "*Clean Desk*" dhe politikës / procedurës së kyçjes automatike të ekranit pas një kohe pasive ("*idle*").
2	d. Implementimi i sistemeve me 2 (dy) faktorë autentifikimi ("2FA" -*Two-Factor Authentication*) në nivel aplikacioni /*web/ mail/* pajisje për të gjithë përdoruesit e sistemit kritik.	i. Verifikimi dhe evidenca

2.9 MS9: Veprimtaria dhe autentifikimi i administratorëve

Të sigurohet aksesi i administratorëve, duke zbatuar autentifikimin me shumë faktorë ("MFA"-*Multi-Factor Authentication*) në aplikacione, *web, email* dhe pajisje. Të përdoren platforma për parandalimin e humbjes së të dhënave ("DLP" - *Data Loss Prevention*) për parandalimin e rrjedhjes së paautorizuar të informacionit.

Niveli	Masat e sigurisë	Dokumentimi/verifikimi i implementimit
1	a. Implementimi i metodës së autentifikimit me shumë faktorë (MFA), në nivel aplikacion/*web/ mail/* pajisje për administratorët.	i. Verifikimi dhe evidencat e implementimit të metodës së autentifikimit me shumë faktorë (MFA).
2	b. Përdorimi i metodës për parandalimin e humbjes së të dhënave (DLP) për identifikimin dhe parandalimin e rrjedhjes së paautorizuar të të dhënave të ndjeshme jashtë infrastrukturës.	i. Verifikimi i implementimit të metodës për parandalimin e humbjes së të dhënave (DLP) për rrjedhjen e të dhënave të ndjeshme.

2.10 MS10: Siguria e aplikacioneve

Të sigurohet mbrojtja e aplikacioneve, duke kryer testime të sigurisë për vlerësimin e dobësive ("VA"-*Vulnerability Assessment*) dhe testimi i penetrimit ("*Penetration Test*") e duke trajtuar problematikat e evidentuara.

Niveli	Masat e sigurisë	Dokumentimi/verifikimi i implementimit
1	a. Kryerja e testimeve për vlerësimin e sigurisë së aplikacioneve e rrjeteve të teknologjisë së informacionit për vlerësimin e dobësive (VA) dhe hartimi i planit për trajtimin e problematikave të evidentuara. (Minimumi 1 (një) herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturën e OIKI-së/OIRI-së).	i. Raporti i vlerësimit të dobësive dhe plani i trajtimit.

1	b. Kontrolli nëse shërbimet *web* ("*web services*") operojnë duke zbatuar protokollin e sigurt "*https*".	i. Verifikimi teknik dhe evidencat (p.sh. evidenca vizuale të konfigurimeve përmes "*screenshot*", *log*-eve dhe dokumentimit të detajuar të parametrave teknikë).
1	c. Konfigurimi i "*anti-spoofing*": DMARC /SPF/DKIM në sistemin e *e-mail*-it.	i. Verifikimi teknik dhe evidencat (p.sh. evidenca e implementimit të *anti-spoofing* në sistemin e *e-mail*-it).
1	ç. Realizimi i testimeve të zhvillimit të *software*-ve ("*staging/testing*") në ambient të dedikuar dhe të ndarë nga ambienti i prodhimit ("*production*"), nëse infrastruktura ka një departament zhvillimi.	i. Verifikimi i evidencave të ambientit të dedikuar për testime të *software*-ve, të ndarë nga ambienti i prodhimit.
2	d. Implementimi i një zgjidhjeje për filtrimin, monitorimin dhe bllokimin e trafikut keqdashës në internet, me mur mbrojtës digjital për sigurinë e aplikacioneve *Web* ("WAF*"- Web Application Firewall*).	i. Verifikimi teknik dhe evidencat (p.sh. evidenca vizuale të konfigurimeve përmes *screenshot*, *log*-eve dhe dokumentimit të detajuar të parametrave teknikë).
2	dh. Implementimi i "*Reverse Proxy*" në një server që qëndron midis klientëve dhe serverëve të brendshëm "*backend servers*" dhe vepron si ndërmjetës për të përpunuar kërkesat nga klientët dhe për t'i përcjellë ato te serverët e brendshëm.	i. Verifikimi i implementimit të "*Reverse Proxy*" në serverat *web* (p.sh. evidenca vizuale të konfigurimeve përmes *screenshot*, *log*-eve dhe dokumentimit të detajuar të parametrave teknikë).
2	e. Kryerja e testimeve për vlerësimin e sigurisë së aplikacioneve dhe rrjeteve (*Penetration Test – Black, Gray, White*) dhe hartimi i një plani për trajtimin e problematikave të evidentuara. (Minimumi 1 (një) herë në vit dhe/ose mbas çdo incidenti të sigurisë kibernetike apo pas çdo ndryshimi madhor në infrastrukturën e OIKI-së/OIRI-së).	i. Raporti i testimeve të llojeve: "*black*", "*grey*", "*white*" për vlerësimin e sigurisë së aplikacioneve dhe rrjeteve (*penetration test*) dhe plani i trajtimit.

2.11 MS11: Siguria e prodhimit të *software*-ve

Siguria e prodhimit të *software*-ve për infrastrukturat kritike apo të rëndësishme përfshin praktikat dhe masat që mundësojnë projektimin, zhvillimin, testimin, dhe implementimin e *software*-ve me siguri të lartë për të mbrojtur infrastrukturat nga sulmet kibernetike.

Niveli	Masat e sigurisë	Dokumentimi/verifikimi i implementimit
1	a. Implementimi i një procedure sigurie për projektimin dhe zhvillimin e *oftware*-ve. (Rishikim minimumi 1 (një) herë në vit).	i. Dokumentim i procedurës së sigurisë për projektimin dhe/ose zhvillimin e *software*-ve. ii. Procedura duhet të miratohet nga stafi i lartë menaxherial dhe të rishikohet në mënyrë periodike.
1	b. Kontrolli dhe monitorimi i aksesit të zhvilluesve dhe përdoruesve të *software*-ve.	i. Të përfshihen në procedurë specifika, si mënyra e autentifikimit, autorizimit, enkriptimit për zhvilluesit e *software*-ve. ii. Të përcaktohen qartë të drejtat dhe akseset për përdoruesit e *software*-ve.
1	c. Ruajtja e historikut të ndryshimeve/ konfigurimeve/ aprovimit të zhvillimit të kodit burim (*source code*) të *software*-it.	i. Verifikimi teknik dhe evidencat (p.sh. evidenca vizuale të konfigurimeve përmes "*screenshot*", *log*-eve dhe dokumentimit të detajuar të parametrave teknikë).
1	ç. Analiza e rrezikut dhe sigurisë të *software*-it para se të dalë në prodhim (*production*).	i. Raporte të analizës së rrezikut dhe sigurisë së *software*-it para se të dalë në prodhim, duke përfshirë dhe varësinë nga libraritë e palëve të treta (*third party libraries*).
1	d. Trajtimi dhe dokumentimi i incidenteve të sigurisë kibernetike për zhvillimin e *software*-ve.	i. Raportet e auditit dhe *log*-et e incidenteve të zhvillimit te *software*-ve.

1	dh. Monitorimi i vendit të ruajtjes (*repository*) së kodit burim të *software*-it.	i. Raporte monitorimi të vendit të ruajtjes (*repository*) së kodit burim të *software*-it.
1	e. Enkriptimit të kodit burim ("*source code*") në ruajtje dhe në transmetim.	i. Verifikimi teknik dhe evidencat (p.sh. evidenca e kodit të enkriptuar në ruajtje dhe transmetim).
1	ë. Realizimi i lidhjes së enkriptuar të aplikacionit me bazën e të dhënave (*"connection string").*	i. Verifikimi teknik dhe evidencat (p.sh. evidenca e enkriptimit të lidhjes së aplikacionit me bazën e të dhënave).
1	f. Realizimi i *backup*-it të kodit burim dhe testimi i integritetit të *backup*-it.	i. Verifikimi teknik dhe evidencat (p.sh. evidenca e pranisë së kopjes së kodit burim dhe testeve për rikuperimin e kodit përmes kopjes së ruajtur).
2	g. Automatizimi nëpërmjet "*pipeline*" ("CI/CD" – *Continuous Integration / Continuous Delivery /Deployment*) integrimit të vazhdueshëm / zhvillim/ implementimit i vazhdueshëm të procesit të zhvillimit, testimit dhe publikimit të *software*-ve.	i. Verifikimi teknik dhe evidencat (p.sh. evidenca vizuale të konfigurimeve dhe funksionimit të CI/CD përmes "*screenshot*", *log*-eve dhe dokumentimit të detajuar të parametrave teknikë).
2	gj. Implementimi i masave të sigurisë për mikroshërbimet ("*microservices*"), duke përfshirë izolimin e burimeve, monitorimin e vazhdueshëm dhe aplikimin e kontrolleve të aksesit.	i. Verifikimi teknik dhe evidencat (p.sh. evidenca vizuale të konfigurimeve përmes "*screenshot*", *log*-eve dhe dokumentimit të detajuar të parametrave teknikë).

2.12 MS12: Siguria e sistemeve të teknologjisë operacionale (OT)

Të sigurohet mbrojtja e sistemeve të teknologjisë operacionale, duke zbatuar parimin e aksesit minimal, segmentimin e rrjeteve dhe enkriptimin e protokolleve kritike. Të implementohen masa për kontrollin e aksesit, monitorimin në kohë reale dhe mbrojtjen e pajisjeve nga sulmet kibernetike dhe "*malware*".

Niveli	Masat e sigurisë	Dokumentimi/verifikimi i implementimit
1	a. Zbatimi i parimit të privilegjeve të aksesit minimal "*Least privileges*", duke vendosur kontroll të aksesit të bazuar në role (RBAC) për përdoruesit, Lista e Kontrollit të aksesit ("ACL" - *Access Control List*") për filtrimin e trafikut, si dhe mbylljen e shërbimeve të panevojshme në sistemet kritike të teknologjisë operacionale (OT)	i. Verifikimi teknik dhe evidencat.
1	b. Implementimi i TLS/SSL, VPN për protokollet (MODBUS, IEC 104/105, DNP3, OPC UA, MQTT).	i. Verifikimi teknik dhe evidenca.
1	c. Implementimi i teknikave "Hot" dhe "*Cold*" *backups*, për ruajtjen e të dhënave.	i. Verifikimi teknik dhe evidenca.
1	ç. Implementimi i një zgjidhjeje për menaxhimin e aksesit në distancë, sipas parimit me zero besim (ZTNA).	i. Verifikimi teknik dhe evidenca.
1	d. Menaxhimi i kontrolluar i *patch*-eve dhe konfigurimeve, duke e testuar më parë në ambiente testi.	i. Verifikimi teknik dhe evidenca.
1	dh. Implementimi i një zgjidhjeje për kontrollin e *software*-it në zonën e "*production*", duke përdorur teknika si "*Application Whitelisting*", në mënyrë manuale apo automatike për të lejuar vetëm aplikacionet e autorizuara të ekzekutohen.	i. Verifikimi teknik dhe evidenca.
1	e. Implementimi i mbrojtjes së pikave fundore, duke përfshirë mekanizmat e detektimit, reagimit apo izolimit të sulmit në nivel "*signature*" dhe sjelljeje "*behaviour*".	i. Verifikimi teknik dhe evidenca.

1	ë. Zbatimi i teknikës "*Hardening*" i pajisjeve të teknologjisë operacionale, si (PLC, RTU, HMI, SCADA, BMS etj).	i. Verifikimi teknik dhe evidenca.
1	f. Ndarja e infrastrukturës së teknologjisë së informacionit nga teknologjia operacionale (duke siguruar shërbime të veçanta për çdo infrastrukturë, si "*Active Directory*", "Antivirus", mur mbrojtës i gjeneratës së re ("*NextGen Firewall*") dhe SIEM, që janë të dedikuara për teknologjinë operacionale.	i. Verifikimi teknik dhe evidenca.
2	g. Implementimi i monitorimit në kohë reale i veprimeve operacionale në sistemet e teknologjisë operacionale, si dhe regjistrimi, analiza dhe njoftimi i ngjarjeve bazuar në funksionet e rëndësinë e tyre për operacionet kritike.	i. Verifikimi teknik dhe evidenca.

2.13 MS13: Siguria e sistemeve "*IoT – Internet of Things*"

Të hartohen e të zbatohen procedura për sigurinë e pajisjeve "*IoT*", duke përfshirë përdorimin e mekanizmave që garantojnë integritetin dhe konfidencialitetin e sistemeve. Të implementohen azhurnime të sigurta dhe të sigurohet mbrojtja e çelësave të autentifikimit në pajisjet "*IoT*".

Niveli	**Masat e sigurisë**	**Dokumentimi/verifikimi i implementimit**
1	a) Hartimi, miratimi, zbatimi dhe rishikimi në mënyrë periodike i procedurave për sigurinë e pajisjeve dhe sistemeve "*IoT*".	i. Procedura për sigurinë e pajisjeve dhe sistemeve "*IoT*".
1	b) Siguria e pajisjeve "*IoT*" – - Përcaktimi i kërkesave minimale për pajisjet "*hardware*". - Përdorimi i mekanizmave që garantojnë integritet ("*tamper proof*") dhe konfidencialitet (*Trusted Platform Module*). - Aplikimi i azhurnimeve/përditësimeve të sigurta të sistemeve të operimit dhe "*firmware*". - Garantimi i sigurisë së çelësave të autentifikimit. - Kryerja e analizave të trafikut në nivel sjellje (kur aplikohet).	i. Verifikimi teknik dhe evidencat (p.sh. evidenca vizuale të konfigurimeve përmes "*screenshot*", *log*-eve dhe dokumentimit të detajuar të parametrave teknikë).
2	c) Garantimi i integritetit dhe konfidencialitetit të të dhënave të transmetuara ndërmjet pajisjeve "*IoT*". - Përdorimi i certifikatave autentifikimi që ofrojnë siguri (pajisjet me Hub ose *Central* "*IoT*"). - Garantimi i komunikimit të sigurt (TLS 1.2 e lart). - Sigurimi i të dhënave të "*IoT*" kur transmetohen dhe ruhen. - Përcaktimi i qartë i kontrolleve të aksesit ("*IoT hub*" dhe aplikimit "*IoT Central*"). - Realizimi i monitorimit të sigurisë së zgjidhjeve "*IoT*".	i. Verifikimi teknik dhe evidencat (p.sh. evidenca vizuale të konfigurimeve përmes "*screenshot*", *log*-eve dhe dokumentimit të detajuar të parametrave teknikë).

2.14 MS14: Siguria në shërbimet *Cloud*

Siguria në shërbimet "*Cloud*" përfshin masat dhe politikat që sigurojnë mbrojtjen e të dhënave e të shërbimeve të infrastrukturës, duke përfshirë autentifikimin e fuqishëm, enkriptimin e të dhënave dhe monitorimin e aktiviteteve. Këto masa synojnë të garantojnë integritetin, disponueshmërinë dhe konfidencialitetin e sistemeve të përdorura në "*Cloud*", si dhe përputhshmërinë me kërkesat teknike dhe marrëveshje për nivelin e shërbimit ("SLA"- *Service Level*

Agreement) e dakorduara me ofruesit e shërbimeve.

Niveli	Masat e sigurisë	Dokumentimi/verifikimi i implementimit
1	a) Vendosja e një politike/procedure të qeverisjes për shërbimet në "*Cloud*".	i. Politika/procedura për sigurinë në "*Cloud*".
1	b) Përfshirja e kërkesave teknike, organizative dhe të sigurisë në marrëveshjet e nivelit të shërbimit (SLA) me ofruesit e shërbimeve "*Cloud*".	i. Dokumenti i marrëveshjes për nivelin e shërbimit (SLA), që përfshin indikatorët kryesorë të performancës, metrikat e monitorimit, sigurisë dhe rikuperimit.
1	c) Implementimi i autentifikimit të fuqishëm, si autentifikimi me shumë faktorë (MFA) për aksesin e platformës së administrimit dhe shërbimeve në "*Cloud*".	i. Verifikimi dhe evidencat për implementimin e autentifikimit në "*Cloud*".
1	ç) Implementimi i një mekanizmi enkriptimi për të dhënat në ruajtje dhe në transit.	i. Verifikim teknik dhe evidenca.
1	d) Realizimi i kopjes rezervë (*backup*) të rregullt të shërbimeve kritike dhe të rëndësishme në "*Cloud*".	i. Verifikim teknik dhe evidenca.
1	dh) Realizimi i aktivizimit të *log*-eve dhe monitorimi i aktiviteteve të infrastrukturës në "*Cloud*".	i. Verifikim teknik dhe evidenca.
2	e) Implementimi i një arkitekture të sigurisë së rrjetit që kombinon funksionet e rrjetit dhe sigurisë së teknologjisë së informacionit në një platformë të unifikuar, të bazuar në "*Cloud*". Përdorimi i shërbimit të sigurt për aksesin në skaj të rrjetit ("SASE" – *Secure Access Service Edge*).	i. Verifikim teknik i zgjidhjes të shërbimit të sigurt për aksesin në skaj të rrjetit (SASE). ii. Verifikimi dhe evidenca e përdorimit të shërbimit të sigurt për aksesin në skaj të rrjetit (SASE) nga përdoruesit.

KREU V
KATEGORIZIMI I AFATEVE TË MASAVE KORRIGJUESE

1. Bazuar në nenin 43, të ligjit nr. 25/2024, "Për sigurinë kibernetike", në rastet kur AKSK-ja konstaton mangësi në zbatimin e masave të sigurisë, përcakton një afat të arsyeshëm, brenda të cilit operatorët e infrastrukturës kritike e të rëndësishme të informacionit marrin masat korrigjuese përkatëse.

2. Afatet për përmbushjen e mangësive të konstatuara në lidhje me masat e sigurisë përcaktohen, bazuar në nivelin e rrezikut për çdo mangësi apo gjetje.

3. Nivelet e vlerësimit të rrezikut dhe afatet për implementimin e masave korrigjuese janë, si më poshtë vijon:

Vlera e rrezikut	Niveli i rrezikut	Koha e trajtimit
[1-3]	Shumë i ulët	Nuk ka nevojë për trajtim
[4-6]	I ulët	Nuk ka nevojë për trajtim
[7-11]	Mesatar	Ka nevojë për trajtim brenda afatit kohor prej 12-muajsh
[12-19]	I lartë	Ka nevojë për trajtim brenda afatit kohor prej 6-muajsh
[20-25]	Shumë i lartë	Ka nevojë për trajtim brenda afatit kohor prej 3-muajsh

4. Autoriteti Kombëtar për Sigurinë Kibernetike (AKSK) mund të vendosë shtyrjen e afateve për përmbushjen e masave korrigjuese nga operatorët e infrastrukturave kritike të informacionit (OIKI) dhe operatorët e infrastrukturave të rëndësishme të informacionit (OIRI). Ky vendim merret vetëm në raste të veçanta, bazuar në një vlerësim të dokumentuar të rrethanave specifike, me kërkesë të argumentuar nga infrastruktura përkatëse ose me nismë të vetë AKSK-së.

5. Operatorët janë të detyruar të njoftojnë AKSK-në për marrjen e masave korrigjuese, brenda

afatit të përcaktuar, si dhe të paraqesin dokumentacionin mbështetës për këto masa.