REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Nr.2865 prot

Datë 03.11.2025

URDHËR

Nr. 316, datë 03.11.2025

PËR

"MIRATIMIN E METODOLOGJISË TË PËRCAKTIMIT TË MASËS SË DËNIMIT ADMINISTRATIV GJOBË"

Në zbatim të nenit 45, të pikës 2, të ligjit nr. 25/2024, "Për sigurinë kibernetike", si dhe ligjit nr. 10 279, datë 20.5.2010 "Për kundërvajtjet administrative",

URDHËROJ:

1. Miratimin e metodologjisë për përcaktimin e masës së dënimit administrativ gjobë sipas tekstit që i bashkëlidhet këtij urdhri dhe është pjesë përbërëse e tij.
2. Për zbatimin e këtij urdhri ngarkohet Autoriteti Kombëtar për Sigurinë Kibernetike.
3. Ky urdhër hyn në fuqi menjëherë.

DREJTOR I PËRGJITHSHËM
Igli T[illegible]

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

METODOLOGJIA PËR PËRCAKTIMIN E MASËS SË DËNIMIT ADMINISTRATIV GJOBË

Tabela e përmbajtjes

I. RREGULLA TË PËRGJITHSHME

1. Kjo metodologji përcakton rregullat e përgjithshme bazë për përcaktimin e masës së dënimit administrativ gjobë në zbatim të nenit 45, të pikës 2, të ligjit nr. 25/2024 "Për sigurinë kibernetike", ligjit nr.10279, datë 20.05.2010, "Për kundërvajtjet administrative", Vendimit të Këshillit të Ministrave nr.531, datë 25.09.2025 "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", si dhe rregullores "Për kategorizimin e incidenteve të sigurisë kibernetike" miratuar me urdhër nr. 299, datë 21.08.2024 të Drejtorit të Përgjithshëm të Autoritetit.
2. Objekti i kësaj metodologjie është përcaktimi i rregullave dhe procedurave për konstatimin, shqyrtimin dhe vendosjen e masës së dënimit administrativ ndaj operatorëve të infrastrukturave të informacionit, punonjësve të Autoritetit, në rastet e shkeljes së detyrimeve ligjore të parashikuara në ligjin nr.25/2024 "Për sigurinë kibernetike" si dhe akteve nënligjore të nxjerra në zbatim të tij.
3. Qëllimi i kësaj metodologjie është të sigurojë zbatim të njëtrajtshëm, proporcional dhe të drejtë të masës së gjobës, në funksion të forcimit të zbatueshmërisë së legjislacionit në fuqi për sigurinë kibernetike dhe parandalimit të shkeljeve të mëtejshme.
4. Kjo metodologji zbatohet nga Autoriteti Kombëtar për Sigurinë Kibernetike, në rastet kur gjatë procesit të ushtrimit të kontrollit në infrastrukturat e informacionit konstatohet nga grupi i kontrollit mos zbatimi i kërkesave ligjore të legjislacionit në fuqi për sigurinë kibernetike të cilat nuk përbëjnë kundërvajtje penale, si dhe për shkeljet e konstatuara për punonjësit e Autoritetit të cilët nuk zbatojnë detyrimet e përcaktuara në ligjin "Për sigurinë kibernetike" për sa i përket ruajtjes se konfidencialitetit gjatë trajtimit të një incidenti kibernetik.
5. Termat e përdorura në këtë metodologji kanë të njëjtin kuptim me termat e përcaktuara në ligjin nr.25/2024 "Për sigurinë kibernetike", ndërsa termat e mëposhtëm kanë këto kuptime:
   a) **"Dënim administrativ"** është masa e gjobës dhe çdo masë apo sanksion tjetër administrativ, të parashikuara në legjislacionin në fuqi për sigurinë kibernetike apo aktet e tjera nënligjore.
   b) "**Gjobë**" është dënimi administrativ kryesor në vlerë monetare, që sanksionon shkeljen e kërkesave ligjore nga operatorët e infrastrukturave të informacionit ku dëmi i shkaktuar është i rëndësishëm dhe që ka për qëllim kthimin e aktivitetit që kontrollohet në kushtet e zbatimit të kërkesave ligjore.
   c) **"Subjekt kontrolli**" i referohet operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, të cilët kanë detyrimin e përmbushjes së kërkesave të përcaktuara në legjislacionin në fuqi për sigurinë kibernetike.
   ç) **"Parimi i proporcionalitetit**" konsiderohet parimi sipas të cilit ushtrohet kontroll dhe merren masa administrative lidhur me veprimtarinë e subjektit që kontrollohet, duke siguruar që masa administrative e vendosur:
      - është e nevojshme për arritjen e qëllimit ligjor të garantimit të nivelit të duhur të sigurisë kibernetike;
      - është e përshtatshme dhe efektive për të parandaluar përsëritjen e shkeljeve dhe për të nxitur pajtueshmërinë me kërkesat ligjore; si dhe

- është në përpjesëtim të drejtë me natyrën, rrethanat, pasojat dhe nivelin e përgjegjësisë së subjektit që ka kryer shkeljen, duke shmangur çdo penalizim të tepruar apo të panevojshëm.

6. Në përcaktimin e masës së dënimit apo të masës administrative që duhet të marrë, grupi i kontrollit, në përputhje me rëndësinë e shkeljeve të konstatuara dhe pasojave të tyre, duke respektuar parimin e proporcionalitetit, vendos atë sanksion apo merr atë masë që është e domosdoshme dhe e përshtatshme për arritjen e qëllimit të dënimit apo masës, dhe që cenon më pak të drejtat apo interesat e ligjshme të subjektit të kontrolluar.

II. DËNIMET ADMINISTRATIVE

1. Llojet dhe vendosja e dënimit administrativ

1.1 Shkelja e kërkesave ligjore nga operatorët e infrastrukturave të informacionit, që konstatohen nga grupi i kontrollit, kur nuk përbën kundërvajtje penale, përbën kundërvajtje administrative.

1.2 Shkeljet e konstatuara të kërkesave ligjore të subjektit të kontrolluar klasifikohen si kundërvajtje administrative për të cilat parashikohen dënimet administrative, si vijon:

a) Dënim me gjobë;

b) Kërkesë institucionit kompetent për pezullim e ushtrimit të shërbimit, në rastet e shkeljeve të përsëritura për mos përmbushjen e masave të sigurisë, kur ndaj operatorit të infrastrukturës kritike janë marrë deri në 2 (dy) masa administrative të njëpasnjëshme.

1.3 Dënimi administrativ, kur është e nevojshme, shoqërohet edhe me urdhërimin e subjektit të kontrolluar për të korrigjuar shkeljet e konstatuara dhe për t'i eliminuar pasojat e tyre, duke përcaktuar dhe një afat të arsyeshëm kohor për këtë qëllim. Në përcaktimin e afatit, grupi i kontrollit merr në konsideratë nivelin e rrezikut të shkeljes, pasojat e saj dhe rrethanat konkrete që përcaktojnë kohën e nevojshme për kryerjen e veprimeve për këtë qëllim, me përpjekjet maksimale nga ana e subjektit të kontrolluar.

1.4 Për çdo shkelje të kërkesave ligjore do të zbatohet dënimi administrativ propocional, i cili duhet të jetë i mjaftueshëm për të siguruar zgjidhjen e shpejtë të shkeljes, parandalimin e përsëritjes së saj në të ardhmen, si dhe për të adresuar mungesën e bashkëpunimit nga ana e subjektit të kontrolluar.

III. KRITERET PËR CAKTIMIN E DËNIMIT ADMINISTRATIV GJOBË

1. Dënimi administrativ gjobë

1.1 Dënimi administrativ gjobë, është dënimi administrativ i cili i jepet operatorit të infrastrukturës kritike dhe të rëndësishme të informacionit, kur nuk plotëson kërkesat ligjore të përcaktuara në ligjin nr. 25/2024 "Për sigurinë kibernetike", si dhe akteve nënligjore të nxjerra në zbatim të tij.

1.2 Masa e gjobës është e shprehur me intervale sipas pikëve të grumbulluara, përqindjes (%) së përmbushjes së masave të sigurisë kibernetike, si dhe vlerësimit të nivelit të rrezikut sipas përcaktimeve të bëra në këtë metodologji.

1.3 Kriteret e përcaktimit të vlerës së gjobës bazohen në:

a) Përqindjen (%) e përmbushjes së masave teknike, organizative dhe operacionale të sigurisë kibernetike, të përcaktuara në ligjin nr.25/2024 "Për sigurinë kibernetike", si dhe në vendimin e Këshillit të Ministrave nr. 531, datë 25.09.2025 "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";

b) Nivelin e rrezikut të sigurisë në infrastrukturat kritike dhe të rëndësishme të informacionit;

c) Kategorinë e incidenteve kibernetike dhe impaktin e tyre;

ç) Nëse kundërvajtësi rezulton i dënuar administrativisht edhe më parë;

2. Rastet e dhënies së dënimit administrativ gjobë

2.1 Autoriteti, bazuar në përcaktimet e kësaj metodologjie përcakton vlerën e gjobës brenda kufirit minimal dhe maksimal të parashikuar në ligjin nr.25/2024 "Për sigurinë kibernetike".

2.2 Ndaj operatorëve të infrastrukturave kritike të informacionit dhe operatorëve të infrastrukturave të rëndësishme të informacionit jepet dënimi administrativ gjobë si vijon:

a) Mosraportimi pranë CSIRT-it Kombëtar dhe CSIRT-it sektorial i incidenteve të sigurisë kibernetike të ndodhur në infrastruktura, në zbatim të shkronjës "ë", pika 3, neni 17, dhe pika 3, neni 23 e ligjit nr.25/2024 "Për sigurinë kibernetike", përbën kundërvajtje administrative dhe sanksionohet me gjobë, në vlerë nga 1 000 000 lekë deri në 10 000 000 lekë;

b) Mosraportimi i saktë i infrastrukturave të informacionit gjatë procesit të identifikimit, sipas përcaktimeve të pikës 4, të nenit 12, të ligjit nr.25/2024 "Për sigurinë kibernetike" dhe akteve nënligjore në zbatim të tij, përbën, kundërvajtje administrative dhe sanksionohet me gjobë, në vlerë nga 200 000 lekë deri në 400 000 lekë;

c) Mosraportimi pranë Autoritetit të pikës së kontaktit apo i përditësimeve të tyre, sipas përcaktimeve në pikat 3 dhe 4, të nenit 18, të ligjit nr.25/2024 "Për sigurinë kibernetike", përbën, kundërvajtje administrative dhe sanksionohet me gjobë, në vlerë nga 200 000 lekë deri në 400 000 lekë;

ç) Mospërmbushja e detyrimeve nga ana e operatorëve sipas përcaktimeve në pikat 1, 3, 4, 5, 7, dhe 8 dhe 9 të nenit 31 të ligjit nr.25/2024 "Për sigurinë kibernetike", përbën, kundërvajtje administrative dhe sanksionohet me gjobë 1 000 000 lekë deri në 10 000 000 lekë;

d) Mospërmbushja nga ana e operatorëve e detyrimeve të përcaktuara në kuadër të marrjes së masave korrigjuese, në zbatim të pikave 1, 2, 4 të nenit 43, të ligjit nr.25/2024 "Për sigurinë kibernetike", përbën, kundërvajtje administrative dhe sanksionohet me gjobë 400 000 lekë deri në 1 000 000 lekë;

dh) Mospërmbushja nga ana e operatorëve e detyrimeve, të përcaktuara në pikat 5 dhe 6 të nenit 23 të ligjit nr.25/2024 "Për sigurinë kibernetike", përbën, kundërvajtje administrative dhe sanksionohet me gjobë në vlerë nga 200 000 lekë deri në 400 000 lekë;

e) Mospërmbushja nga ana operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit të administratës publik, e detyrimeve të përcaktuara në pikat 1 dhe 2 të nenit 32 të ligjit nr.25/2024 "Për sigurinë kibernetike" përbën, kundërvajtje administrative dhe sanksionohet me gjobë në vlerë nga 2 000 000 lekë deri në 5 000 000 lekë;

ë) Mospërmbushja e detyrimeve për nëpunësit e Autoritetit, sipas përcaktimeve në nenin 27 të ligjit nr.25/2024 "Për sigurinë kibernetike", përbën kundërvajtje administrative dhe sanksionohet me gjobë, në vlerë nga 200 000 lekë deri në 400 000 lekë.

IV. METODOLOGJIA E PËRCAKTIMI TË DËNIMIT ADMINISTRATIV GJOBË

1. Përcaktimi i dënimeve administrative për mospërmbushjen e detyrimeve të raportimit të incidenteve kibernetike nga operatorët e infrastrukturave të informacionit

1.1 Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit janë të detyruar të raportojnë të gjitha llojet e incidenteve të sigurisë kibernetike pranë CSIRT-it Kombëtar dhe CSIRT-it sektorial, brenda 4 orëve nga momenti i identifikimit të incidentit kibernetik. Në rastin e incidenteve të rëndësishme, operatorët e infrastrukturave kritike të informacionit dhe operatorët e infrastrukturave të rëndësishme të informacionit brenda 72 orëve nga momenti i identifikimit të incidentit kibernetik të rëndësishëm përditësojnë informacionin dhe bëjnë një vlerësim fillestar të incidentit kibernetik të rëndësishëm, duke përfshirë ashpërsinë dhe ndikimin, si dhe, aty ku ka, treguesit e kompromentimit.

1.2 Subjektet të cilët nuk raportojnë incidentet kibernetike sipas pikës 1.1 të kreut IV të kësaj metodologjie, do të sanksionohen me gjobë në bazë të:

a) Kategorisë së incidentit kibernetik, të përcaktuar në rregulloren "Për kategorizimin e incidenteve të sigurisë kibernetike" miratuar me urdhër nr. 299, datë 21.08.2024 të Drejtorit të Përgjithshëm të Autoritetit;
b) Në bazë të shërbimit kritik ose shërbimit të rëndësishëm;
c) Vlerësimit të nivelit të rrezikut;
ç) Kohës së përcaktuar të raportimit.

1.3 Mospërmbushja e detyrimit të raportimit të incidenteve kibernetike nga operatorët e infrastrukturave të informacionit sanksionohet me gjobë në vlerat e përcaktuara në tabelën si vijon:

Klasifikimi i incidenteve kibernetike sipas ndikimit	**Koha e raportimit**	**Masa e gjobës për operatorët e infrastrukturave kritike**	**Masa e gjobës për operatorët infrastrukturave të rëndësishme**
Incidentet kibernetike me ndikim **të lartë**	Brenda 4 orësh nga identifikimi	8 000 000 lekë	5 000 000 lekë
Incidentet kibernetike me ndikim **të mesëm**	Brenda 4 orësh nga identifikimi	5 000 000 lekë	3 000 000 lekë
Incidentet kibernetike me ndikim **të ulët**	Brenda 4 orësh nga identifikimi	2 000 000 lekë	1 000 000 lekë

Tabela nr.1

Shënim Kategoritë e incidenteve të sigurisë kibernetike janë përcaktuar në nenin 6, të rregullores "**Për kategorizimin e incidenteve të sigurisë kibernetike**", miratuar me urdhër nr. 299, datë 21.08.2024 të Drejtorit të Përgjithshëm të Autoritetit.*

1.4 Në rast të shkeljeve ligjore të përsëritura, pavarësisht nivelit të ndikimit të incidentit kibernetik, aplikohet masa e gjobës maksimale në vlerën 10 000 000 lekë, e përcaktuar në nenin 45, pika 1, shkronja "a" të ligjit nr. 25/2024 "Për sigurinë kibernetike".

2. Përcaktimi i dënimeve administrative në rast të mospërmbushjes së detyrimit për dorëzimin e raportit përfundimtar të incidentit pranë CSIRT-it Kombëtar, si dhe mosdorëzimi i raportit të progresit në rast incidenti kibernetik të vazhdueshëm

2.1 Bazuar në nenin 23, pikat 5 dhe 6 të ligjit nr. 25/2024 "Për sigurinë kibernetike", operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit kanë detyrimin që brenda 1 (një) muaji pas njoftimit të incidentit, të dorëzojnë pranë CSIRT-it Kombëtar një raport përfundimtar, i cili përmban:

a) një përshkrim të detajuar të incidentit, duke përfshirë rëndësinë dhe ndikimin e tij;
b) llojin e kërcënimit ose shkakun kryesor që mund ta ketë shkaktuar incidentin;
c) masat e zbatuara dhe masat e vazhdueshme për zvogëlimin e pasojave;
ç) aty ku është e aplikueshme, ndikimin ndërkufitar të incidentit.

2.2 Në rastet e një incidenti kibernetik të vazhdueshëm, operatori i infrastrukturës së informacionit i prekur nga ky incident, përveç detyrimit të dorëzimit të raportit përfundimtar, ka detyrimin të dorëzojë pranë CSIRT-it Kombëtar edhe një raport progresi në kohën e ndodhjes së incidentit kibernetik.

2.3 Bazuar në nenin 44, shkronja "e", të ligjit nr. 25/2024 "Për sigurinë kibernetike", mosdorëzimi i raportit përfundimtar/ raport progresit, përbën, kundërvajtje administrative dhe sanksionohet me gjobë si me poshtë vijon:

Klasifikimi i incidenteve kibernetike sipas ndikimit	**Masa e gjobës në rast të mosdorëzimit të raportit përfundimtar/ raport progresit të incidenteve të ndodhura në operatorët e infrastrukturave kritike**	**Masa e gjobës në rast të mosdorëzimit të raportit përfundimtar/ raport progresit të incidenteve të ndodhura në operatorët e infrastrukturave të rëndësishme**
Incidentet kibernetike me ndikim **të lartë**	350 000 lekë	300 000 lekë
Incidentet kibernetike me ndikim **të mesëm**	300 000 lekë	250 000 lekë
Incidentet kibernetike me ndikim **të ulët**	250 000 lekë	200 000 lekë

Tabela nr.2

2.4 Në rast të shkeljeve ligjore të përsëritura, pavarësisht nivelit te ndikimit te incidentit kibernetik, aplikohet masa e gjobës maksimale në vlerën 400 000 lekë, e përcaktuar në nenin 45, pika 1, shkronja "b" të ligjit nr. 25/2024 "Për sigurinë kibernetike".

3. Përcaktimi i dënimeve administrative për mosraportim pranë Autoritetit i pikës së kontaktit apo përditësimi i tyre.

3.1 Bazuar në shkronjën "f", të nenit 16, si dhe në nenin 18 të ligjit nr. 25/2024 "Për sigurinë kibernetike", CSIRT-i sektorial cakton pikën e kontaktit dhe raporton të dhënat pranë CSIRT-it Kombëtar. Operatorët e infrastrukturës kritike dhe të rëndësishme të informacionit caktojnë pikat e kontaktit dhe raportojnë të dhënat tek CSIRT-it Kombëtar dhe CSIRT-it sektorial. Çdo ndryshim në të dhënat e pikave të kontaktit duhet t'i komunikohet CSIRT-it Kombëtar dhe CSIRT-it sektorial brenda 7 (shtatë) ditëve kalendarike.

3.2 Mosraportimi i pikës së kontaktit apo i përditësimeve të tyre, përbën, kundërvajtje administrative dhe sanksionohet me gjobë si më poshtë vijon:

a) mosraportimi i pikës së kontaktit nga operatorët e infrastrukturave kritike të informacionit (OIKI) apo i përditësimeve të tyre, dënohet me gjobe me vlerën me 300 000 lekë;

b) mosraportimi i pikës së kontaktit nga operatorët e infrastrukturave të rëndësishme të informacionit(OIRI) apo përditësimi i tyre dënohet me gjobë me vlerën me 200 000 lekë.

3.3 Në rast të shkeljeve ligjore të përsëritura, aplikohet masa e gjobës maksimale në vlerën 400 000 lekë, e përcaktuar në nenin 45, pika 1, shkronja "b" të ligjit nr. 25/2024 "Për sigurinë kibernetike".

4. Përcaktimi i dënimeve administrative për mospërmbushjen e masave korrigjuese

4.1 Bazuar në nenin 43, pika 1, të ligjit nr. 25/2024 "Për sigurinë kibernetike", kur Autoriteti konstaton mangësi në zbatimin e masave të sigurisë përcakton një afat të arsyeshëm brenda të cilit operatorët e infrastrukturës kritike dhe të rëndësishme të informacionit duhet të marrin masat korrigjuese përkatëse. Përcaktimi i këtij afati të arsyeshëm bëhet në përputhje me përcaktimet e vendimit të Këshillit të Ministrave nr.531, datë 25.09.2025 "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".

4.2 Bazuar në nenin 44, shkronja "dh", të ligjit nr. 25/2024 "Për sigurinë kibernetike" mospërmbushja e masave korrigjuese nga ana e operatorëve të infrastrukturave të informacionit do të sanksionohet me gjobë sipas kësaj metodologjie.

4.3 Për qëllime të vlerësimit të nivelit të mosrealizimit të masave të sigurisë kibernetike të përcaktuara në vendimin e Këshillit të Ministrave nr.531, datë 25.09.2025 "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", si dhe përcaktimit të masës përkatëse të dëmit administrativ (gjobë), kjo metodologji përcakton rregullat, kriteret dhe mënyrën e vlerësimit të mospërmbushjes së masave të sigurisë kibernetike bazuar në peshën specifike të secilës masë sigurie sipas Aneksit 1 të kësaj metodologjie, si dhe në përqindjen e realizimit të secilës masë të aplikuar.

4.4 Për secilën kategori të masave organizative, teknike dhe operacionale, paraqitet tabela e mëposhtme:

MASA ORGANIZATIVE, TEKNIKE DHE OPERACIONALE	**Pesha për masë (Aneksi nr 1)**	**Përqindja e realizimit të masës (përcaktohet nga Grupi Kontrollit 0-100%)**
MS – 1	-	-
MS – 2	-	-
:	-	-
:	-	-
MS – (N)	-	-

Tabela nr. 3

4.5 Në këtë strukturë:

- **Masa** : identifikon emërtimin e masës së sigurisë kibernetike;
- **Pikët e peshës** janë përcaktuar për secilën masë sigurie të vendimit të Këshillit të Ministrave nr.531, datë 25.09.2025 "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", nga Grupi i Kontrollit, bazuar në kategorizimin dhe rëndësinë e tyre sipas Aneksit nr. 1 të kësaj metodologjie.
- **Përqindja e realizimit të masës** vlerësohet gjatë procesit të kontrollit nga Grupi i Kontrollit për secilën masë. Të gjitha masat e sigurisë kibernetike pjesërisht të realizuara, apo të pa realizuara, i nënshtrohen vlerësimit sipas formulës në pikën 4.7, të kreut IV të kësaj metodologjie.

4.7 Formula e përllogaritjes së përqindjes totale të mosrealizimit të masave të sigurisë kibernetike është si vijon:

Përqindja e parealizuar = shuma [pesha për masë (pa realizuar, pjesërisht realizuar) * (100% - përqindja e realizimit të masës)] / totali i peshave për masat e aplikuara

Nivelet e vlerësimit të mosrealizimit të masave të sigurisë dhe gjobat përkatëse janë sipas tabelës si më poshtë vijon:

Niveli	**Totali i përqindjes së mosrealizit (%)**	**Gjoba (Lekë)**
Niveli 0	0% – 10%	0
Niveli 1	11% – 20%	400 000
Niveli 2	21% – 30%	500 000
Niveli 3	31% – 45%	600 000
Niveli 4	46% – 60%	700 000
Niveli 5	61% – 75%	800 000
Niveli 6	76% – 90%	900 000
Niveli 7	91% – 100%	1 000 000

Tabela nr. 4

4.8 Në rast të përsëritjes së shkeljeve të konstatuara nga Autoriteti Kombëtar i Sigurisë Kibernetike, nëse gjatë procesit të kontrollit konstatohet se subjekti ka përmbushur masat korrigjuese mbi nivelin e herës së parë, gjoba administrative vendoset sipas nivelit përkatës të përqindjes së mosrealizimit sipas tabelës nr.4 të kësaj metodologjie.

4.9 Në rast se niveli i përmbushjes së masave korrigjuese është i njëjtë me atë të herës së parë, pra nuk ka shënuar progres, aplikohet masa administrative maksimale në vlerën 1 000 000 lekë, në përputhje me nenin 45, pika 1, shkronja "c" të ligjit nr. 25/2024 "Për sigurinë kibernetike".

4.10 Autoriteti, kur konstaton shkelje të përsëritura lidhur me zbatimin e masave të sigurisë kibernetike të përcaktuara në ligjin nr.25/2024 "Për sigurinë kibernetike" nga operatori i infrastrukturës kritike të informacionit, ndaj të cilit rezulton se janë marrë deri në 2 (dy) masa

administrative të njëpasnjëshme, aplikon masat e tjera shtrënguese sipas parashikimeve të nenit 46 të ligjit nr.25/2024 "Për sigurinë kibernetike".

5. Përcaktimi i dënimit administrativ për mosraportimin nga operatorët e infrastrukturave të informacionit, të çdo infrastrukturë të re, të administruar prej tyre, që ndërvepron me infrastrukturat e kategorizuara kritike apo të rëndësishme

5.1 Bazuar në të nenin 31, pika 2, të ligjit nr.25/2024 "Për sigurinë kibernetike", operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit janë të detyruar të raportojnë pranë Autoritetit në vazhdimësi çdo infrastrukturë të re, të administruar prej tyre, që ndërvepron me infrastrukturat e kategorizuara si kritike apo të rëndësishme.

5.2 Bazuar në përcaktimet e pikës 2, të nenit 43 të ligjit nr.25/2024 "Për sigurinë kibernetike", kur Autoriteti konstaton se nga ana e operatorëve të infrastrukturave të informacionit nuk është zbatuar detyrimi i përcaktuar në pikën 2 të nenit 31 të ligjit nr.25/2024 "Për sigurinë kibernetike, i përcakton një afat prej 10 ditësh kalendarike brenda të cilit operatorët e infrastrukturës kritike dhe të rëndësishme të informacionit marrin masat për përmbushjen e detyrimit.

5.3 Bazuar në të nenin 44, shkronja "dh", të ligjit nr.25/2024 "Për sigurinë kibernetike", moszbatimi i këtij detyrimi përben kundërvajtje administrative dhe sanksionohet me gjobë si me poshtë vijon:

a) Operatorët e infrastrukturave kritike të informacionit sanksionohen me gjobë në vlerën 600 000 lekë;

b) Operatorët e infrastrukturave të rëndësishme të informacionit sanksionohen me gjobë në vlerën 400 000 lekë.

5.4 Në rast të shkeljeve ligjore të përsëritura, aplikohet masa e gjobës maksimale në vlerën 1 000 000 lekë, e përcaktuar në nenin 45, pika 1, shkronja "c" të ligjit nr. 25/2024 "Për sigurinë Kibernetike".

6. Përcaktimi i dënimit administrativ për mospërmbushjen e detyrimeve të përcaktuara në pikat 1, 3, 4, 5, 7, 8, 9 të nenit 31 të ligjit nr.25/2024 "Për sigurinë kibernetike"

6.1 Në nenin 31, pika 1, të ligjit nr. 25/2024 "Për sigurinë kibernetike" operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit kanë detyrimin të raportojnë të gjitha infrastrukturat e tyre kritike, të rëndësishme, si dhe të gjitha infrastrukturat e tjera që ndërveprojnë me to pranë Autoritetit.

6.1.1 Bazuar në nenin 44, shkronja "d", të ligjit nr.25/2024 "Për sigurinë kibernetike", mospërmbushja e këtij detyrimi përben kundërvajtje administrative dhe sanksionohet me gjobë si më poshtë vijon:

a) Operatorët e infrastrukturave kritike të informacionit sanksionohen me gjobë në vlerën 5 000 000 lekë;

b) Operatorët e infrastrukturave të rëndësishme të informacionit sanksionohen me gjobë në vlerën 1 000 000 lekë.

6.1.2 Në rast të shkeljeve ligjore të përsëritura, aplikohet masa e gjobës maksimale në vlerën 10 000 000 lekë, e përcaktuar në nenin 45, pika 1, shkronja "a" të ligjit nr. 25/2024 "Për sigurinë kibernetike".

6.2 Në pikën 3, të nenit 31 të ligjit nr. 25/2024 "Për sigurinë kibernetike" përcaktohet se operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit kanë detyrimin të

dokumentojnë çdo ndryshim dhe zhvillim të kryer në infrastrukturat e tyre kritike dhe të rëndësishme.

6.2.1 Bazuar në nenin 44, shkronja "d", të ligjit nr.25/2024 "Për sigurinë kibernetike", mospërmbushja e këtij detyrimi përben kundërvajtje administrative dhe sanksionohet me gjobë si më poshtë vijon:

a) Operatorët e infrastrukturave kritike të informacionit sanksionohen me gjobë në vlerën 5 000 000 lekë;

b) Operatorët e infrastrukturave të rëndësishme të informacionit sanksionohen me gjobë në vlerën 1 000 000 lekë.

6.2.2 Në rast të shkeljeve ligjore të përsëritura, aplikohet masa e gjobës maksimale në vlerën 10 000 000 lekë, e përcaktuar në nenin 45, pika 1, shkronja "a" të ligjit nr. 25/2024 "Për sigurinë kibernetike".

6.3 Në nenin 31, pika 4, të ligjit nr. 25/2024 "Për sigurinë kibernetike" përcaktohet se operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit kanë detyrimin të vendosin në dispozicion të Autoritetit çdo dokumentacion dhe evidencë që kërkohet nga Autoriteti në kuadër të procesit të kontrollit.

6.3.1 Bazuar në shkronjën "d", të nenit 44, të ligjit nr. 25/2024 "Për sigurinë kibernetike", mospërmbushja e këtij detyrimi përben kundërvajtje administrative dhe sanksionohet me gjobë si më poshtë vijon:

a) Operatorët e infrastrukturave kritike të informacionit sanksionohen me gjobë në vlerën 5 000 000 lekë;

b) Operatorët e infrastrukturave të rëndësishme të informacionit sanksionohen me gjobe në vlerën 1 000 000 lekë.

6.3.2 Në rast të shkeljeve ligjore të përsëritura, aplikohet masa e gjobës maksimale në vlerën 10 000 000 lekë, e përcaktuar në nenin 45, pika 1, shkronja "a" të ligjit nr. 25/2024 "Për sigurinë kibernetike".

6.4 Në pikën 5, të nenit 31, të ligjit nr. 25/2024 "Për sigurinë kibernetike" operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, në kuadër të aktivitetit mbikqyrës, i ofrojnë CSIRT-it kombëtar akses të drejtpërdrejtë në ambientet dhe sistemet e tyre të informacionit, në zbatim të procedurave të sigurisë të çdo operatori të këtyre infrastrukturave, të cilat janë të lidhura me shërbimet e ofruara prej tyre.

6.4.1 Bazuar në të nenin 44, shkronja "d", të ligjit nr. 25/2024 "Për sigurinë kibernetike", mospërmbushja e këtij detyrimi përben kundërvajtje administrative dhe sanksionohet me gjobë si më poshtë vijon:

a) Operatorët e infrastrukturave kritike të informacionit sanksionohen me gjobë në vlerën 5 000 000 lekë;

b) Operatorët e infrastrukturave të rëndësishme të informacionit sanksionohen me gjobe në vlerën 1 000 000 lekë.

6.4.2 Në rast të shkeljeve ligjore të përsëritura, aplikohet masa e gjobës maksimale në vlerën 10 000 000 lekë, e përcaktuar në nenin 45, pika 1, shkronja "a" të ligjit nr. 25/2024 "Për sigurinë kibernetike".

6.5 Në nenin 31, të pikës 7, të ligjit nr. 25/2024 "Për sigurinë kibernetike", përcaktohet se për impelementimin efektiv të masave të sigurisë kibernetike, operatorët paraqesin pranë Autoritetit raportin e vlerësimit të konformitetit, nga një Organ i Vlerësimit të Konformitetit, të paktën një herë në 2 vjet.

6.5.1 Bazuar në të nenin 44, shkronja "d", të ligjit nr. 25/2024 "Për sigurinë kibernetike", mospërmbushja e këtij detyrimi përben kundërvajtje administrative dhe sanksionohet me gjobë si më poshtë vijon:

a) Operatorët e infrastrukturave kritike të informacionit sanksionohen me gjobë në vlerën 5 000 000 lekë;

b) Operatorët e infrastrukturave të rëndësishme të informacionit sanksionohen me gjobe në vlerën 1 000 000 lekë.

6.5.2 Në rast të shkeljeve ligjore të përsëritura, aplikohet masa e gjobës maksimale në vlerën 10 000 000 lekë, e përcaktuar në nenin 45, pika 1, shkronja "a" të ligjit nr. 25/2024 "Për sigurinë kibernetike".

6.6 Në nenin 31, pika 9, ë ligjit nr. 25/2024 "Për sigurinë kibernetike", përcaktohet se operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, janë të detyruar të bashkëpunojnë me Autoritetin në kuadër të realizimit të funksioneve mbikëqyrëse të përcaktuara në ligj.

6.6.1 Bazuar në nenin 44, shkronja "d", të ligjit nr. 25/2024 "Për sigurinë kibernetike", mospërmbushja e këtij detyrimi përben kundërvajtje administrative dhe sanksionohet me gjobë si më poshtë vijon:

a) Operatorët e infrastrukturave kritike të informacionit sanksionohen me gjobë në vlerën 5 000 000 lekë;

b) Operatorët e infrastrukturave të rëndësishme të informacionit sanksionohen me gjobë në vlerën 1 000 000 lekë.

6.6.2 Në rast të shkeljeve ligjore të përsëritura, aplikohet masa e gjobës maksimale në vlerën 10 000 000 lekë, e përcaktuar në nenin 45, pika 1, shkronja "a" të ligjit nr. 25/2024 "Për sigurinë kibernetike".

7. Përcaktimi i dënimeve administrative për mospërmbushjen e detyrimeve të operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit të administratës publike

7.1 Bazuar në nenin 32, pika 1 dhe 2, të ligjit nr. 25/2024, mosmarrja e konfirmimit paraprak të operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit të administratës publik nga institucioni përgjegjës për qeverisjen elektronike lidhur me specifikimet teknike, përpara inicimit të implementimit të një sistemi, si dhe mosrespektimi nga ana e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit të administratës publik i detyrimit për hostimin e nyjës primare pranë Qendrës së të Dhënave Qeveritare dhe nyjes sekondare pranë Qendrës së Vazhdueshmërisë së Punës, përbëjnë kundërvajtje administrative dhe sanksionohen me gjobë si më poshtë:

a) 3 000 000 lekë për operatorët e infrastrukturës kritike të informacionit;

b) 2 000 000 lekë për operatorët e infrastrukturës së rëndësishme të informacionit.

7.2 Në rast të shkeljeve ligjore të përsëritura, aplikohet masa e gjobës maksimale në vlerën 5 000 000 lekë, e përcaktuar në nenin 45, pika 1, shkronja "ç", të ligjit nr. 25/2024 "Për sigurinë Kibernetike".

8. Përcaktimi i dënimeve administrative për mospërmbushjen e detyrimeve për nëpunësit e Autoritetit, për ruajtjen e konfidencialitetit

8.1 Bazuar në pikën 1, të nenit 27, të ligjit nr.25/2024 "Për sigurinë kibernetike", nëpunësit e Autoritetit, që marrin pjesë në zgjidhjen e incidentit të sigurisë kibernetike, janë të detyruar të ruajnë konfidencialitetin e plotë për të gjitha të dhënat e përpunuara gjatë procedurës së zgjidhjes së incidentit. Konfidencialiteti duhet të ruhet edhe pas ndërprerjes së marrëdhënieve të punës me Autoritetin, në përputhje me parashikimet ligjore në fuqi.

8.2 Nëpunësit e Autoritetit të cilët nuk përmbushin detyrimin e përcaktuar në pikën 8.1 të kësaj metodologjie, sanksionohen me gjobë me vlerën 200 000 lekë.

8.3 Në rast të shkeljeve ligjore të përsëritura, aplikohet masa e gjobës maksimale në vlerën maksimale 400 000 lekë**,** e përcaktuar në nenin 45, pika 1, shkronja "b", të ligjit nr. 25/2024 "Për sigurinë Kibernetike".

ANEKS 1: Pesha për secilën masë të VKM Nr.531, datë 25.09.2025 "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"

Niveli	Masa	Dokumentimi	Kategorizimi	Pesha
1	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 dhe të rëndësishme të informacionit, dhe rishikimi në mënyre 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/OIRI).	Politika e Sigurisë së Informacionit Raportet e Rishikimit Periodik	Organizative	**3**
1	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/OIRI).	Dokument i metodologjisë së menaxhimit të rrezikut kibernetikë duke përfshirë versionin, datat dhe miratimin nga stafi menaxherial. Raportet e Rishikimit Periodik	Organizative	**2**

1	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/OIRI).	Lista e vlerësimit të rreziqeve të ardhura nga burime të ndryshme duke përfshirë dhe rreziqet të cilat vijnë nga palët e treta.	Organizative	**4**
		Njoftimi i stafit menaxherial, për listën e rreziqeve si dhe vendimi i marrë për trajtimin e tyre.		
		Rishikim i listës së rreziqeve.		
1	Hartimi i një plani për trajtimin e rreziqeve të identifikuara.	Dokument i planit për trajtimin e rreziqeve.	Organizative	**2**
		Pasqyrimi i ndryshimeve të nivelit të rrezikut mbas zbatimit të planit të trajtimit të rreziqeve.		
1	Caktimi i roleve dhe përgjegjësive për menaxhimin e sigurisë së informacionit.	Lista e roleve të sigurisë dhe përshkrimi i detajuar i përgjegjësive dhe detyrave për secilin rol p.sh. (*CISO, ISO, DPO, DBA, SYSADM, NETADM* etj.).	Organizative	**2**

		Organigrama që tregon hierarkinë dhe lidhjet midis roleve të sigurisë.		
		Lista e kontakteve për personat përgjegjës për sigurinë e informacionit (emër, pozicion, mënyra e kontaktit).		
1	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/OIRI).	Politika e sigurisë për furnizimet/ kontratat me palët e treta (versioni, data e publikimit, miratimi).	Organizative	**2**
		Raporte të rishikimit periodik të politikës së sigurisë dhe ndryshimet e realizuara.		
1	Përfshirja e kërkesave të sigurisë në kontratat me palët e treta, duke përfshirë konfidencialitetin dhe transferimin e sigurt të informacionit.	Kërkesa të qarta sigurie në kontratat me palët e treta.	Organizative	**2**
		Marrëveshje konfidencialiteti për ruajtjen e informacionit me palët e treta.		
2	Mbajtja e gjurmëve/rekordeve të incidenteve të sigurisë kibernetike që lidhen ose janë të shkaktuara nga palët e treta.	Regjistri i incidenteve kibernetike të lidhura me palët e treta (data, shkaku, ndikimi, veprimet).	Organizative	**1**

1	Vendosja e një politike sigurie për burimet njerëzore.	Politika e sigurisë për burimet njerëzore (përfshirë të gjitha fazat: para rekrutimit, gjatë punësimit, proceset disiplinore, në përfundim të marrëdhënies së punësimit).	Organizative	**1**
		Dokumenti i verifikimit të integritetit të personelit kryesor (vërtetim të verifikimit të gjendjes gjyqësore (dëshmi penaliteti), referenca të punëve të mëparshme, certifikime, CV, etj...).		
		Procedura për mbrojtjen e të dhënave personale.		
1	Implementimi i një programi trajnimi për sigurinë kibernetike. (Rishikim minimumi 1 (një) herë në vit).	Programi i detajuar i trajnimit, i përshtatur sipas roleve dhe përgjegjësive të punonjësve.	Organizative	**2**
		Lista e pjesëmarrësve dhe datat e trajnimeve.		
		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	Informimi dhe trajnimi i punonjësve të rinj mbi politikat dhe procedurat në fuqi për sigurinë kibernetike.	Evidenca mbi trajnimin për punonjësit e rinj. Formularë të nënshkruar nga punonjësit për njohjen e politikave dhe procedurave. Formularë të nënshkruar nga punonjësit për Marrëveshjen e Konfidencialitetit ("NDA" - *Non Disclosure Agreement)*.	Organizative	**2**
2	Testimi i njohurive të punonjësve mbi 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.)	Pyetësorë dhe rezultate testimi për ndërgjegjësimin e punonjësve në lidhje me sigurinë kibernetike.	Organizative	**1**
1	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/OIRI).	Inventari i plotë i aseteve të Teknologjisë së Informacionit ("IT"- *Information Technology*) /Teknologjisë Operacionale ("OT"- *Operational Technology)*, duke përfshirë psh. modelin, kategorinë e aseteve, nr. serie, protokolli i internetit ("*IP"- Internet Protocol*), vendodhjen, vjetërsinë, statusin e tyre, etj.	Organizative	**5**

		Vendosja në inventar i ndikimit sipas Konfidencialitetit, Integritetit dhe Disponueshmërisë *("C/I/A"- Confidentiality/ Integrity/ Availability)* së asetit.		
1	Vendosja dhe zbatimi i politikave/procedurave për menaxhimin e aseteve.	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/OIRI).	Organizative	**2**
		Topologji e detajuar e rrjetit dhe sistemeve të informacionit.		
1	Marrja e masave për zëvendësimin ose izolimin e sistemeve që iu ka përfunduar cikli i jetës ("EOL"- *End of Life)*.	Dokument ose evidencë të identifikimit të sistemeve që iu ka përfunduar cikli i jetës (EOL) dhe planifikimi për zëvendësimin/izolimin e tyre.	Teknike dhe Operacionale	**5**
		Evidenca të zëvendësimit/izolimit të asetit i		

		cili ka arritur kohën e ciklit të jetës (EOL).		
		Verifikimi i sistemeve dhe evidencat.		
1	Kryerja e azhurnimeve (“*patch-imeve”*) automatike/manuale në sistemet fundore dhe në të gjithë infrastrukturën e teknologjisë së informacionit (IT) dhe teknologjisë operacionale (OT).	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.	Teknike dhe Operacionale	**4**
		Verifikimi i sistemeve/ mjeteve (“*tools”*) dhe evidencat.		
1	Përcaktimi dhe zbatimi i politikave dhe 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.	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.	Organizative	**1**

		Evidenca të konfigurimeve minimale të sigurisë së pajisjeve personale sipas politikës.		
1	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/OIRI).	Dokumenti i planit për menaxhimin e incidenteve kibernetike (versioni, data, miratimi).	Organizative	**4**
		Procedura për identifikimin, klasifikimin dhe trajtimin e incidenteve (Manual veprimi - "*Playbooks")*, lista e personave të ekipit për reagimin ndaj incidenteve kibernetike).		
1	Mbajtja e rekordeve për të gjitha incidentet e sigurisë kibernetike.	Regjistri i incidenteve që përfshin: datën, shkakun, ndikimin, dhe veprimet korrigjuese.	Organizative	**3**
		Raporte individuale të trajtimit të incidenteve dhe analizat e mësimeve të nxjerra.		

1	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.	Politika e menaxhimit të ndryshimeve (përfshirë përshkrimin, datën, përgjegjësitë dhe impaktin e parashikuar, planin e zbatimit etj.). (Rishikim minimumi 1(një) herë në vit.)	Organizative	**3**
		Procedura e menaxhimit të ndryshimeve (hapat nga propozimi deri te miratimi dhe implementimi).		
		Formulari i kërkesës për ndryshim ("RFC" – *Request for Change*).		
1	Krijimi dhe zbatimi i një Planit 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/OIRI).	Politika e strategjisë për vazhdimësinë e shërbimeve, duke përfshirë kushtet për aktivizimin e planit, kohën e rikuperimit, komunikimi në kohë krize, skenarët e incidenteve, plani i veprimit, rregullat e testimit, etj.	Organizative	**4**
		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)*.		

		Lista e kontakteve emergjente – informacion për pikat e kontaktit në rast krize.		
1	Shfrytëzimi i teknikave të pasqyrimit të të dhënave nëpërmjet konfigurimit redundant të disqeve të pavarur (*"*RAID*"* -*Redundant Array of Independent Disks*).	Verifikimi teknik i konfigurimit redundant të disqeve të pavarur ("RAID*"*) (**1/5/6/10**) dhe evidencat përkatëse.	Teknike dhe Operacionale	**3**
1	Realizimi i një politikë/procedurë 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/OIRI).	Dokumenti i politikës/procedurës për kryerjen e kopjeve rezervë (*backup-it)* , duke përfshirë frekuencat, llojet, të dhënat dhe shërbimet.	Organizative	**2**
		Lista e kopjeve rezervë (*backup-eve)* të kryera dhe raportet e testimit të rikuperimit dhe integritetit të të dhënave.		
2	Realizimi i kopjeve rezervë (*backup-it)* duke përdorur teknika si "*Backup Lock Retention*" ose "*Tape Worm*".	Evidenca të përdorimit të teknikave "*Backup Lock Retention"* ose "*Tape Worm*".	Teknike dhe Operacionale	**5**
2	Shmangia e pikave të vetme të dështimit (*Single Point of Failure*) në shërbimet kritike dhe të rëndësishme të infrastrukturës.	Verifikimi teknik i pikave të vetme të dështimit.	Teknike dhe Operacionale	**4**
		Evidenca për Redundancën e Shërbimeve.		

2	Implementimi i infrastrukturës sipas skemave të shërbimit me disponueshmëri të lartë ("HA" – *High Availability*).	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*). Verifikim dhe Evidenca.	Teknike dhe Operacionale	**4**
2	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*).	Strategjia për DRS 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/OIRI).	Teknike dhe Operacionale	**5**

		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/OIRI).		
		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/OIRI).		
		Verifikim dhe evidenca.		

2	Zbatimi i teknologjisë së Rrjetit të Përcaktuar nga Softueri ("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.	Strategji për të siguruar që shërbimet dhe aplikacionet kritike (përfshirë ato që mbështeten në teknologjitë e Rrjetit të Përcaktuar nga Softueri (SDN) dhe "*Blockchain*") të kenë mundësi rikuperimi sa më të shpejtë dhe me një ndërprerje minimale, në rast katastrofash apo incidentesh.	Teknike dhe Operacionale	**Nuk ka peshë (masë opsionale)**
		Testime periodike të konfigurimeve të Teknologjisë së Rrjetit të Përcaktuar nga Softueri (SDN) .		
		Verifikimi i zbatimit të teknikës "*Hashing*".		
2	Zbatimi i teknologjisë "*Blockchain*" për decentralizimin e menaxhimit të të dhënave duke siguruar mbrojtjen e të dhënave dhe paprekshmërinë e tyre gjatë rikuperimit.	Politika e kopjeve rezervë (*backup*) për teknologjinë "*Blockchain*".	Teknike dhe Operacionale	**Nuk ka peshë (masë opsionale)**
		Monitorimi i aktivitetit në "*Blockchain*".		
1	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/OIRI).	Dokument i politikës/procedurës për kontrolle dhe auditime (versioni, data, miratimi i politikës/procedurës nga stafi menaxherial).	Organizative	**1**

1	Monitorimi i pajtueshmërisë së standardeve me kërkesat ligjore.	Politikë/Procedurë për monitorimin e pajtueshmërisë me standardet dhe kërkesat ligjore. Lista e standardeve dhe kërkesave ligjore të aplikueshme për infrastrukturën. 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/OIRI.	Organizative	**1**
1	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/OIRI).	Dokument i politikës/procedurës për kontrolle dhe auditime (versioni, data, miratimi i politikës/procedurës nga stafi menaxherial).	Organizative	**1**

1	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/OIRI).	Raporte të auditimeve të brendshme dhe plani i trajtimit të mangësive (data, metodologjia, rezultatet).	Organizative	**2**
		Raporte të auditimeve të realizuara nga palët e treta për sigurinë e informacionit.		
		Lista e veprimeve korrigjuese të ndërmarra pas auditimeve dhe evidenca e implementimit të tyre.		
1	Implementimi i masave të sigurisë fizike dhe kontrolleve mjedisore.	Evidenca të implementimit të masave të sigurisë fizike (brava, kabinete, kontroll elektronik i hyrjes).	Teknike dhe Operacionale	**4**
		Gjurmë të aktiviteteve (logs) të auditimit për aksesin në hapësira të autorizuara dhe alarme për hyrjet e paautorizuara.		
		Raporte të funksionimit dhe mirëmbajtjes së sistemeve të alarmit dhe fikësve të zjarrit.		

		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	Implementimi i një politike për masat e sigurisë fizike dhe kontrollet mjedisore.	Dokumenti i politikës për sigurinë fizike dhe kontrollet mjedisore (versioni, data, miratimi, rishikimi).	Organizative	**1**
1	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/OIRI).	Dokument i politikës për aksesin (role, grupe, të drejta, procedurat e dhënies dhe revokimit të aksesit).	Organizative	**4**
		Formular për dhënie të drejtash aksesi.		
		Formular për revokim të drejtash aksesi dhe dorëzimi asetesh.		
		Evidenca për fshirjen e llogarive gjenerike dhe raportet e kontrolleve periodike të aksesit.		

1	Aplikimi i filtrave për trafikun në rastin e aksesimit në distancë të sistemeve, si dhe enkriptimi i trafikut me protokolle të sigurta.	Verifikimi teknik dhe evidencat për vendosjen e filtrave dhe enkriptimin e trafikut.	Teknike dhe Operacionale	**5**
1	Kontrolli nëse në murin mbrojtës digjital (*firewall)* ka të konfiguruar lista të autorizuara/lista të bllokuar ("*Whitelist/Blacklist*") të adresave të Protokollit të Internetit (*IP)* të lejuara ose bllokuara.	Verifikim dhe evidenca për konfigurimet në murin mbrojtës digjital (*firewall*).	Teknike dhe Operacionale	**5**
1	Përdorimi i politikave për menaxhimin e fjalëkalimeve rastësore për përdoruesit dhe administratorët lokal.	Dokumenti i politikës për menaxhimin e fjalëkalimeve dhe verifikim i implementimit të zgjidhjeve për menaxhimin e fjalëkalimeve rastësore për përdoruesit dhe administratorët lokal ("LAPS*"-Local Administrator Password Solution*) ose teknologji të ngjashme.	Teknike dhe Operacionale	**3**
2	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.	Verifikim teknik dhe evidenca.	Teknike dhe Operacionale	**5**

2	Implementimi i një zgjidhje teknologjike për Menaxhimin e Akseseve të Privilegjuara ("PAM*" – Privileged Access Management)*	Verifikim teknik dhe evidenca.	Teknike dhe Operacionale	**4**
2	Implementimi i shërbimit të sigurisë me Akses në rrjet sipas parimit me zero besim ("ZTNA*" - Zero Trust Network Access*")	Verifikim teknik dhe evidenca.	Teknike dhe Operacionale	**5**
1	Implementimi i politikave të enkriptimit duke përfshirë detaje rreth algoritmeve dhe çelësave kriptografikë.	Dokumenti i politikës së enkriptimit si p.sh., algoritmet: "*AES", "RSA", "ECC", "TLS", "IPSec", "SSH*", etj.. Lista e çelësave kriptografikë (p.sh., lloji, afati i vlefshmërisë, metoda e gjenerimit dhe ruajtjes).	Teknike dhe Operacionale	**2**
2	Kriptimi i të dhënave (në tranzit dhe në gjendje të qëndrueshme).	Lista e konfigurimeve të kriptimit për të dhënat dhe aplikacionet ("*on-prem*", "*hybrid*", "*cloud*"). Verifikimi teknik dhe evidenca.	Teknike dhe Operacionale	**4**
1	Implementimi i sistemit të automatizuar për zbulimin dhe menaxhimin e informacionit dhe të incidenteve/ngjarjeve të Sigurisë ("*SIEM" - Security Information and Event Management*).	Verifikim teknik dhe evidenca të konfigurimit të sistemit të automatizuar për zbulimin dhe menaxhimin e informacionit dhe të incidenteve/ngjarjeve të Sigurisë (SIEM) përfshirë rregullat e alarmimit dhe filtrimit të gjurmëve dhe aktiviteteve (*log-eve*) për zbulimin e incidenteve.	Teknike dhe Operacionale	**5**

1	Monitorimi i vazhdueshëm i burimeve të jashtme të inteligjencës për kërcënimet kibernetike *"threat intelligence*"..	Raporte periodike nga mjetet e monitorimit të inteligjencës për kërcënimet kibernetike "*threat intelligence*". Lista e burimeve të përdorura për mbledhjen e informacionit mbi kërcënimet.	Teknike dhe Operacionale	**3**
2	Zbatimi i programit të inteligjencës për kërcënimet kibernetike "*threat intelligence*" në të cilin të përfshihen rolet, përgjegjësitë dhe procedurat.	Dokument i programit të inteligjencës për kërcënimet kibernetike "*threat intelligence*" (përfshirë strukturën e roleve dhe përgjegjësive).	Organizative	**1**
1	Implementimi i politikave për monitorimin dhe regjistrimin e ngjarjeve të sigurisë kibernetike.	Dokument i politikave për monitorimin dhe regjistrimin e gjurmëve dhe aktiviteteve (l*og-eve)* ku përfshihen (kërkesat minimale, periudha e mbajtjes, objektivat, miratimi, përditësimi).	Organizative	**2**
1	Vendosja e mjeteve për mbledhjen e gjurmeve dhe aktiviteteve (l*og-eve)* të sistemeve kritike.	Lista e mjeteve të implementuara për mbledhjen e gjurmëve dhe aktiviteteve/ logeve *të log servers* etj. Verifikim teknik dhe evidenca.	Teknike dhe Operacionale	**3**
1	Instalimi i pajisjeve për të monitoruar, kontrolluar dhe kufizuar trafikun hyrës dhe dalës të rrjetave kompjuterike me murin mbrojtës digjital i gjeneratës së re ("*Next Generation Firewall*").	Verifikim teknik për konfigurimin të murit mbrojtës digjital i gjeneratës së re.	Teknike dhe Operacionale	**5**

		Verifikimi teknik dhe evidencat.		
1	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.	Verifikim teknik dhe evidenca të analizave të trafikut.	Teknike dhe Operacionale	**5**
1	Ndarja e rrjetit në nën-rrjete në nivel mikrosegmentimi.	Verifikimi teknik dhe evidenca e topologjisë së rrjetit me ndarjen e dokumentuar në nën-rrjete.	Teknike dhe Operacionale	**5**
1	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 priviledge*").	Lista e rrjet lokal virtual (VLAN*)* dhe nënndarje të rrjetit të implementuara, përfshirë listat e kontrollit të aksesit. Verifikimi teknik dhe evidencat.	Teknike dhe Operacionale	**5**
1	Izolimi i rrjetit pa tela ("*wireless*") nga pjesa tjetër e rrjetit.	Verifikim teknik dhe evidencat e konfigurimit të izolimit të rrjetit pa tela (wireless).	Teknike dhe Operacionale	**3**
1	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.	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.	Teknike dhe Operacionale	**2**

1	Zbatimi i teknikave dhe standardeve mbi fortifikimin (“*hardening”*) e të gjitha pajisjeve në rrjet.	i. Manual për fortifikimin e pajisjeve (*PC, “server”, “router”, “firewall”,* etj.). Verifikimi teknik dhe evidencat.	Teknike dhe Operacionale	**4**
1	Izolimi logjikisht i bazës së të dhënave dhe shërbimet WEB (p.sh. në rrjet lokal virtual/*VLAN)* të ndryshëm).	i. Lista e rrjet lokal virtual (VLAN) dhe verifikimi teknik i konfigurimit për izolimin logjik të bazës së të dhënave dhe shërbimeve WEB.	Teknike dhe Operacionale	**4**
1	Implementimi i “*DNS_SEC*” për të shmangur “*DNS Amplification*” dhe “*DNS Poisoning*”.	Verifikimi teknik dhe evidencat.	Teknike dhe Operacionale	**4**
2	Zbatimi i mbrojtjes ndaj sulmeve DoS/DDoS.	Verifikim teknik i konfigurimit të mekanizmave të mbrojtjes nga DoS/DDoS (p.sh. “*rate limiting*”, “WAF*” - Web Application Firewall*, mjete (*tools*) për “*anti-DDoS*”).	Teknike dhe Operacionale	**5**
2	Implementimi i një zgjidhje/sistemi për kontrollin e parametrave të sigurisë së pajisjeve fundore (“NAC*” - Network Access Control).*	Procedurë për përcaktimin e parametrave të sigurisë minimale (*baseline*). Verifikimi teknik dhe evidencat	Teknike dhe Operacionale	**5**
1	Implementimi i politikave për menaxhimin e fjalëkalimeve të përdoruesve.	Dokument i politikës për menaxhimin e fjalëkalimeve (kompleksiteti, afati i skadimit, ndryshimet periodike).	Organizative	**1**

1	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).	Evidenca teknike të konfigurimeve dhe rregullave të zbatuara në sistem dhe verifikim.	Teknike dhe Operacionale	**5**
1	Menaxhimi i aksesit dhe privilegjeve të përdoruesve përmes shërbimit "AD".	Verifikim teknik dhe evidenca të implementimit të "AD" – në. (strukturat e grupeve, privilegjet, kufizimet).	Teknike dhe Operacionale	**4**
1	Sigurimi dhe mbrojtja e të dhënave dhe kufizimi i aksesit të paautorizuar në informacion.	Verifikim i zbatimit të politikës / procedurës "*Clean Desk*" dhe politikës / procedurës së kyçjes automatike të ekranit pas një kohe pasive ("*idle*").	Teknike dhe Operacionale	**2**
2	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.	Verifikimi dhe evidenca	Teknike dhe Operacionale	**4**
1	Implementimi i metodës së Autentifikimit me Shumë Faktorë (MFA), në nivel aplikacioni/web/ mail/ pajisje për administratorët.	Verifikimi dhe evidencat e implementimit të metodës së Autentifikimit me Shumë Faktorë (MFA).	Teknike dhe Operacionale	**5**
2	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.	Verifikimi i implementimit të metodës për Parandalimin e Humbjes së të Dhënave (DLP)	Teknike dhe Operacionale	**4**

		për rrjedhjen e të dhënave të ndjeshme.		
1	Kryerja e testimeve për vlerësimin e sigurisë së aplikacioneve dhe 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/OIRI.)	Raporti i vlerësimit të dobësive dhe plani i trajtimit.	Teknike dhe Operacionale	**5**
1	Kontrolli nëse shërbimet web ("*web services"*) operojnë duke zbatuar protokollin e sigurt "https".	Verifikimi teknik dhe evidencat (p.sh. evidenca vizuale të konfigurimeve përmes "*screenshot*", log-eve dhe dokumentimit të detajuar të parametrave teknikë).	Teknike dhe Operacionale	**5**
1	Konfigurimi i "*anti-spoofing*": DMARC/SPF/DKIM në sistemin e emailit.	Verifikimi teknik dhe evidencat (p.sh. evidenca e implementimit të anti-spoofing në sistemin e emailit).	Teknike dhe Operacionale	**5**
1	Realizimi i testimeve të zhvillimit të softuerëve ("*staging/testing"*) në ambient të dedikuar dhe të ndarë nga ambienti i prodhimit ("*production"*), nëse infrastruktura ka një departament zhvillimi.	Verifikimi i evidencave të ambientit të dedikuar për testime të softuerëve, të ndarë nga ambienti i prodhimit.	Teknike dhe Operacionale	**3**
2	Implementimi i një zgjidhje për filtrimin, monitorimin dhe bllokimin e trafikut keqdashës në internet, me mur mbrojtës digjital për Sigurinë e Aplikacioneve Web ("WAF*"- Web Application Firewall*.).	Verifikimi teknik dhe evidencat (p.sh. evidenca vizuale të konfigurimeve përmes *screenshot*, log-eve dhe dokumentimit të detajuar të parametrave teknikë.).	Teknike dhe Operacionale	**5**

2	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.	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.).	Teknike dhe Operacionale	**3**
2	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/OIRI).	Raporti i testimeve të llojeve: "*black*", "*grey*", "*white*", për vlerësimin e sigurisë së aplikacioneve dhe rrjeteve (*penetration test*) dhe plani i trajtimit.	Teknike dhe Operacionale	**5**
1	Implementimi i një procedure sigurie për projektimin dhe zhvillimin e softuerë-ve. (Rishikim minimumi 1(një) herë në vit.).	Dokumentim i procedurës së sigurisë për projektimin dhe/ose zhvillimin e softuerëve. Procedura duhet të miratohet nga stafi i lartë menaxherial dhe të rishikohet në mënyrë periodike.	Organizative	**1**
1	Kontrolli dhe monitorimi i aksesit të zhvilluesve dhe përdoruesve të softuerëve.	Të përfshihen në procedurë specifika si mënyra e autentifikimit, autorizimit,	Teknike dhe Operacionale	**3**

		enkriptimit për zhvilluesit e softuerëve. Të përcaktohen qartë të drejtat dhe akseset për përdoruesit e softuerëve.		
1	Ruajtja e historikut të ndryshimeve/ konfigurimeve/ aprovimit të zhvillimit të kodit burim (*source code*) të softuerit.	Verifikimi teknik dhe evidencat (p.sh. evidenca vizuale të konfigurimeve përmes "*screenshot*", log-eve dhe dokumentimit të detajuar të parametrave teknikë).	Teknike dhe Operacionale	**3**
1	Analiza e rrezikut dhe sigurisë të softuerit para se të dalë në prodhim (*production*).	Raporte të analizës së rrezikut dhe sigurisë së softuerit para se të dalë në prodhim duke përfshirë dhe varësinë nga libraritë e palëve të treta (*third party libraries*).	Teknike dhe Operacionale	**5**
1	Trajtimi dhe dokumentimi i incidenteve të sigurisë kibernetike për zhvillimin e softuerëve.	Raportet e auditit dhe log-et e incidenteve të zhvillimit te softuerëve.	Teknike dhe Operacionale	**5**
1	Monitorimi i vendit të ruajtjes (*repository*) së kodit burim të softuerit.	Raporte monitorimi të vendit të ruajtjes (*repository*) së kodit burim të softuerit.	Teknike dhe Operacionale	**3**

1	Enkriptimit të kodit burim ("*source code*") në ruajtje dhe në transmetim.	Verifikimi teknik dhe evidencat (p.sh. evidenca e kodit të enkriptuar në ruajtje dhe transmetim).	Teknike dhe Operacionale	**3**
1	Realizimi i lidhjes së enkriptuar të aplikacionit me bazën e të dhënave (*"connection string").*	Verifikimi teknik dhe evidencat (p.sh. evidenca e enkriptimit të lidhjes së aplikacionit me bazën e të dhënave).	Teknike dhe Operacionale	**5**
1	Realizimi i backup të kodit burim dhe testimi i integritetit të backup.	Verifikimi teknik dhe evidencat (p.sh. evidenca e pranisë së kopjes së kodit burim dhe testeve për rikuperimin e kodit përmes kopjes së ruajtur).	Teknike dhe Operacionale	**5**
2	Automatizimi nëpërmjet "*pipeline*" *("*CI/CD*" – Continuous Integration / Continuous Delivery /Deployment*) integrimit të vazhdueshëm / zhvillim/implementim i vazhdueshëm të procesit të zhvillimit, testimit dhe publikimit të softuerëve.	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).	Teknike dhe Operacionale	**5**
2	Implementimi i masave të sigurisë për mikroshërbimet ("*microservices*"), duke përfshirë izolimin e burimeve, monitorimin e vazhdueshëm dhe aplikimin e kontrolleve të aksesit.	Verifikimi teknik dhe evidencat (p.sh. evidenca vizuale të konfigurimeve përmes "*screenshot*", log-eve dhe dokumentimit të detajuar të parametrave teknikë).	Teknike dhe Operacionale	**5**

1	Zbatimi i parimit të privilegjeve të aksesit minimalë "*Least privileges*" duke vendosur Kontroll i Aksesit i 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)	Verifikimi teknik dhe evidencat.	Teknike dhe Operacionale	**5**
1	Implementimi i TLS/SSL, VPN për protokollet (MODBUS, IEC 104/105, DNP3, OPC UA, MQTT).	Verifikimi teknik dhe evidencat.	Teknike dhe Operacionale	**5**
1	Implementimi i teknikave "Hot" dhe "Cold" *backups,* për ruajtjen e të dhënave.	Verifikimi teknik dhe evidencat.	Teknike dhe Operacionale	**5**
1	Implementimi i një zgjidhje për menaxhimin e aksesit në distancë sipas parimit me zero besim (ZTNA).	Verifikimi teknik dhe evidencat.	Teknike dhe Operacionale	**5**
1	Menaxhimi i kontrolluar i *patch-eve* dhe konfigurimeve duke e testuar më parë në ambiente testi.	Verifikimi teknik dhe evidencat.	Teknike dhe Operacionale	**5**
1	Implementimi i një zgjidhje 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.	Verifikimi teknik dhe evidencat.	Teknike dhe Operacionale	**4**
1	Implementimi i mbrojtjes së pikave fundore, duke përfshirë mekanizmat e detektimit, reagimit apo izolimit të sulmit në nivel "*signature*" dhe sjelljeje "*behaviour*".	Verifikimi teknik dhe evidencat.	Teknike dhe Operacionale	**5**
1	Zbatimi i teknikës "*Hardening*" i pajisjeve të Teknologjisë Operacionale *si* (PLC, RTU, HMI, SCADA, BMS etj.)	Verifikimi teknik dhe evidencat.	Teknike dhe Operacionale	**4**
1	Ndarja e infrastrukturës të 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.	Verifikimi teknik dhe evidencat.	Teknike dhe Operacionale	**5**
2	Implementimi i monitorimt në kohë reale i veprimeve operacionale në sistemet e Teknologjisë Operacionale si dhe regjistrimi, analiza	Verifikimi teknik dhe evidencat.	Teknike dhe Operacionale	**5**

	dhe njoftimi i ngjarjeve bazuar në funksionet dhe rëndësinë e tyre për operacionet kritike.			
1	Hartimi, miratimi, zbatimi dhe rishikimi në mënyre periodike i procedurave për sigurinë e pajisjeve dhe sistemeve "*IoT*".	Procedura për sigurinë e pajisjeve dhe sistemeve "*IoT*".	Organizative	**1**
1	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).	Verifikimi teknik dhe evidencat (p.sh. evidenca vizuale të konfigurimeve përmes "*screenshot*", log-eve dhe dokumentimit të detajuar të parametrave teknikë).	Teknike dhe Operacionale	**5**
2	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	Verifikimi teknik dhe evidencat (p.sh. evidenca vizuale të konfigurimeve përmes "*screenshot*", log-eve dhe dokumentimit të detajuar të parametrave teknikë).	Teknike dhe Operacionale	**5**

	"IoT Central"). • Realizimi i monitorimit të sigurisë së zgjidhjeve "IoT".			
1	Vendosja e një politike/procedure të qeverisjes për shërbimet në "*Cloud*".	Politika/procedura mbi sigurinë në "*Cloud*".	Organizative	**1**
1	Përfshirja e kërkesave teknike, organizative dhe të sigurisë në marrëveshjet e nivelit të shërbimit (SLA) me ofruesit e shërbimeve "*Cloud*".	Dokumenti i Marrëveshjes për Nivelin e Shërbimit (SLA) që përfshin indikatorët kryesore të performancës, metrikat e monitorimit, sigurisë dhe rikuperimit.	Organizative	**1**
1	Implementimi i autentifikimit të fuqishëm, si autentifikimi me shumë faktorë (MFA) për aksesin e platformës së administrimit dhe shërbimeve në "*Cloud*".	Verifikimi dhe evidencat për implementimin e autentifikimit në "*Cloud*".	Teknike dhe Operacionale	**5**
1	Implementimi i një mekanizmi enkriptimi për të dhënat në ruajtje dhe në transit.	Verifikim teknik dhe evidenca.	Teknike dhe Operacionale	**4**
1	Realizimi i kopjes rezervë (*backup*) të rregullt të shërbimeve kritike dhe të rëndësishme në "*Cloud*".	Verifikim teknik dhe evidenca.	Teknike dhe Operacionale	**5**
1	Realizimi i aktivizimit të log-eve dhe monitorimi i aktiviteteve të infrastrukturës në "*Cloud*".	Verifikim teknik dhe evidenca.	Teknike dhe Operacionale	**5**
2	Implementimi i një arkitekturë 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).*	Verifikim teknik i zgjidhjes të Shërbimit të Sigurt për Aksesin në Skaj të Rrjetit (SASE). Verifikimi dhe evidenca e përdorimit të Shërbimit të Sigurt për Aksesin në Skaj të Rrjetit (SASE) nga përdoruesit.	Teknike dhe Operacionale	**3**