VENDIM
Nr. 279, datë 17.4.2026

PËR MIRATIMIN E MASAVE PËR SIGURIMIN E VAZHDUESHMËRISË SË OFRIMIT TË SHËRBIMEVE TË KOMUNIKIMEVE ELEKTRONIKE NË SITUATA TË JASHTËZAKONSHME

Në mbështetje të nenit 100 të Kushtetutës dhe të pikës 5, të nenit 174, të ligjit nr. 54/2024, "Për komunikimet elektronike në Republikën e Shqipërisë", me propozimin e ministrit për Infrastrukturën dhe Energjinë, Këshilli i Ministrave

VENDOSI:

1. Miratimin e masave për sigurimin e vazhdueshmërisë së ofrimit të shërbimeve të komunikimeve elektronike në situata të jashtëzakonshme, sipas tekstit që i bashkëlidhet këtij vendimi dhe është pjesë përbërëse e tij.
2. Ngarkohen Ministria e Infrastrukturës dhe Energjisë dhe Autoriteti i Komunikimeve Elektronike dhe Postare për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

ZËVENDËSKRYEMINISTËR
Albana Koçiu

MASAT
PËR SIGURIMIN E VAZHDUESHMËRISË SË OFRIMIT TË SHËRBIMEVE TË KOMUNIKIMEVE ELEKTRONIKE NË SITUATA TË JASHTËZAKONSHME

Neni 1
Objekti dhe qëllimi

1. Ky dokument përcakton masat për sigurimin e vazhdueshmërisë së ofrimit të shërbimeve të komunikimeve elektronike, me qëllim përballimin e situatave të jashtëzakonshme, duke:
a) minimizuar ndikimin e situatave të jashtëzakonshme në marrjen e shërbimeve të komunikimeve nga përdoruesit e rrjeteve të komunikimeve elektronike;
b) siguruar rikuperimin e shpejtë dhe të sigurt të funksioneve kritike të komunikimeve pas një ndërprerjeje të mundshme;
c) siguruar pajtueshmërinë me kërkesat ligjore për sigurinë dhe integritetin e rrjeteve të komunikimeve elektronike në situata të jashtëzakonshme.
2. Ky dokument ka për qëllim sigurimin e bashkërendimit të masave dhe të bashkëpunimit për përballimin e situatave të jashtëzakonshme në rrjetet e në shërbimet e komunikimeve elektronike në Republikën e Shqipërisë.

Neni 2
Fusha e zbatimit

Masat e përcaktuara në këtë dokument zbatohen për sipërmarrësit e komunikimeve elektronike të autorizuar nga Autoriteti i Komunikimeve Elektronike dhe Postare (AKEP) për ofrimin e rrjeteve dhe të shërbimeve të komunikimeve elektronike, bazuar në ligjin nr. 54/2024, "Për komunikimet elektronike në Republikën e Shqipërisë".

Neni 3
Përkufizime

Përveç përkufizimeve të dhëna në nenin 4, të ligjit nr. 54/2024, "Për komunikimet elektronike në Republikën e Shqipërisë", për qëllime të këtij dokumenti, termat e mëposhtëm kanë këto kuptime:

a) "Situatë e jashtëzakonshme", dëmtimet e rënda të rrjetit të komunikimeve elektronike, fatkeqësitë natyrore, gjendja e emergjencës civile ose gjendja e luftës;

b) "Komiteti Ndërministror i Emergjencave Civile (KNEC)", një organ i përkohshëm, që krijohet menjëherë pas shpalljes së gjendjes së fatkeqësisë natyrore, sipas përcaktimeve në ligjin për emergjencat civile;

c) "Agjencia Kombëtare e Mbrojtjes Civile (AKMC)", i njëjti kuptim sipas përcaktimeve në ligjin për emergjencat civile;

ç) "AKSK", Autoriteti Kombëtar për Sigurinë Kibernetike, organ publik përgjegjës për zbatimin dhe mbikëqyrjen e ligjit për sigurinë kibernetike.

Neni 4

Detyrimet e sipërmarrësve të komunikimeve elektronike

1. Në situatat e jashtëzakonshme, sipërmarrësit e komunikimeve elektronike bashkëpunojnë me ministrinë përgjegjëse për komunikimet elektronike dhe AKEP-in, me qëllim zbatimin e masave të emergjencës dhe koordinimin me:

a) Komitetin Ndërministror të Emergjencave Civile (KNEC);

b) Komitetin e Mbrojtjes Civile (KMC);

c) Agjencinë Kombëtare të Mbrojtjes Civile;

ç) autoritetet, strukturat e tjera përgjegjëse të ngritura në rastet e emergjencave kombëtare, në përputhje me ligjin nr. 45/2019, "Për mbrojtjen civile.".

2. Në rastin e incidenteve apo të sulmeve kibernetike, sipërmarrësit e komunikimeve elektronike bashkëpunojnë me AKEP-in dhe AKSK-në, sipas parashikimeve ligjore për sigurinë kibernetike dhe rregullat për sigurinë dhe integritetin e rrjeteve sipas ligjit për komunikimet elektronike.

Neni 5

Plani i masave për sigurimin e vazhdueshmërisë së shërbimeve

1. Për menaxhimin e vazhdimësisë së shërbimeve, sipërmarrësit e komunikimeve elektronike krijojnë e mbajnë plane emergjence dhe një strategji për të siguruar vazhdimësinë e rrjeteve të komunikimit dhe të sistemeve të informacionit.

2. Plani i masave për sigurimin e vazhdueshmërisë së ofrimit të shërbimeve dhe mirëfunksionimin e infrastrukturës së tyre në rastet e jashtëzakonshme, që hartohet nga sipërmarrësi i komunikimeve elektronike, përmban minimalisht parashikimet, si më poshtë:

a) Përcaktimin e qëllimit dhe të fushëveprimit të planit të masave;

b) Përcaktimin e objektivave të planit;

c) Përcaktimin e strukturave përgjegjëse organizative, si:

i. ekipin e menaxhimit të krizës;

ii. ekipin e vlerësimit të dëmtimeve dhe analizës së ndikimit në proces;

iii. ekipin e mbështetjes teknike, që zbaton procedurat teknike të rikuperimit;

iv. ekipin e komunikimit;

v. ekipin e sigurisë së informacionit;

ç) Përgjegjësitë e strukturave përkatëse për situatat e jashtëzakonshme;

d) Procesin e analizimit dhe identifikimit të sistemeve kritike;

dh) Strategjitë e kopjeve rezervë të të dhënave;

e) Infrastrukturën e rikuperimit;

ë) Procedurat e rikuperimit;

f) Planin e komunikimit dhe të koordinimit;

g) Testimin e mirëmbajtjen e planit;

gj) Aspektet ligjore, përputhshmërinë me standardet e sigurisë, reagimit në situata të emergjencave;

h) Trajnimin dhe ndërgjegjësimin e stafit;

i) Rishikimin periodik të planit.

3. Një model orientues për hartimin e planit të masave nga sipërmarrësit jepet në aneksin 1, që i bashkëlidhet këtij dokumenti.

Neni 6

Masat për sigurimin e vazhdueshmërisë së ofrimit të shërbimit

1. Masat për sigurimin e vazhdueshmërisë së ofrimit të shërbimeve të komunikimeve elektronike në situata të jashtëzakonshme përfshijnë masat:

a) parandaluese, përgatitore për situata të jashtëzakonshme;

b) gjatë situatës së jashtëzakonshme;

c) e rikuperimit pas situatës së jashtëzakonshme.

2. Masat për sigurimin e vazhdueshmërisë së ofrimit të shërbimeve përfshijnë, gjithashtu, masat parandaluese, të vazhdimësisë dhe të rikuperimit, në rastin e incidenteve apo të sulmeve kibernetike. Lista e masave dhe kërkesat për dokumentimin e tyre jepen në anekset 2 dhe 3, që i bashkëlidhen këtij dokumenti.

Neni 7

Masat parandaluese

1. Sipërmarrësit e komunikimeve elektronike hartojnë dhe mirëmbajnë:

a) planin e vazhdimësisë së biznesit (PVB);

b) planin e rikuperimit pas fatkeqësisë (PRF).

2. Sipërmarrësit e komunikimeve elektronike identifikojnë e raportojnë pranë AKEP-it asetet dhe burimet kritike të rrjetit, si dhe pajisjet e lëvizshme, që disponojnë për sigurimin e vazhdueshmërisë së ofrimit të shërbimit në raste të jashtëzakonshme, brenda 6 (gjashtë) muajve nga hyrja në fuqi e këtij vendimi.

3. Me qëllim sigurimin e vazhdimësisë së ofrimit të shërbimeve në situatë të jashtëzakonshme, sipërmarrësit e komunikimeve elektronike zbatojnë standardet e sigurisë, duke marrë masat, si më poshtë:

a) Instalojnë linja rezervë, servera pasivë, mjete komunikimi të bazuara në teknologjinë *cloud* dhe lidhje të pavarura për stacionet bazë e shërbimet kritike;

b) Pajisin qendrat e të dhënave, stacionet dhe antenat transmetuese me burime alternative të furnizimit me energji;

c) Sigurojnë funksionalitetin e shërbimeve të emergjencës dhe të numrit "112" edhe pa kartë SIM.

4. Sipërmarrësit duhet të marrin pjesë dhe të bashkëpunojnë me autoritetet përgjegjëse në ushtrimet kombëtare të simulimit të organizuara.

5. Operatorët duhet të caktojnë një person kontakti për 24 orë/7 ditë gjatë situatave të jashtëzakonshme, duke përditësuar të dhënat e kontaktit në AKEP.

Neni 8

Masat e reagimit gjatë situatës së jashtëzakonshme

1. Në rastin e situatave të jashtëzakonshme, sipërmarrësit e komunikimeve elektronike aktivizojnë menjëherë ekipet e brendshme të menaxhimit të krizës, të situatave të emergjencës dhe njoftojnë pa vonesë AKEP-in për çdo ndërprerje të shërbimeve.

2. Sipërmarrësit marrin masa për aktivizimin e kanaleve prioritare për komunikimin e institucioneve shtetërore për emergjencat dhe, sipas rastit, vendosin në operim pajisjet lëvizëse të rrjetit për mbulimin me shërbim, si dhe sigurojnë transmetimin e paralajmërimeve publike për emergjencat civile apo fatkeqësitë e mëdha në zhvillim ose të pritshme, drejt përdoruesve fundorë të prekur përkatësisht.

3. Aktivizojnë burimet alternative të energjisë për qendrat e të dhënave, stacionet dhe antenat transmetuese.

4. Përdorin rirrugëzimin automatik të lidhjeve përmes lidhjeve rezervë, përfshirë dhe ato ndërkombëtare.

5. Marrin masa për përdorimin e sistemeve satelitore për mbulimin me sisteme komunikimi për autoritetet.

6. Sigurojnë akses për përdoruesit në shërbimet bazë të emergjencës.

7. Gjatë situatës së jashtëzakonshme, raportojnë çdo 4 (katër) orë pranë ministrisë përgjegjëse dhe AKEP-it.

Neni 9

Masat e rikuperimit pas situatës së jashtëzakonshme

1. Sipërmarrësit e komunikimeve elektronike bëjnë vlerësimin dhe raportojnë në AKEP për dëmet brenda 48 orëve pas ngjarjes.

2. Sipërmarrësit e komunikimeve elektronike duhet të rikthejnë funksionalitetin e rrjetit, në përputhje me planin e rikuperimit, sipas nenit 7 të këtij dokumenti.

3. Sipërmarrësit e komunikimeve elektronike duhet të kryejnë një analizë pas ngjarjes me AKEP-in dhe institucionet e sigurisë.

4. Sipërmarrësit e komunikimeve elektronike duhet të përditësojnë planet PVB/PRF dhe të raportojnë tek AKEP-i.

5. Sipërmarrësit e komunikimeve elektronike ndërtojnë një manual praktik për përmirësim të kapaciteteve reaguese në të ardhmen.

Neni 10

Masat për sigurinë në rastet e incidenteve apo të sulmeve kibernetike

1. Pa anashkaluar zbatimin e masave, sipas parashikimeve në nenin 20, të ligjit nr. 25/2024, “Për sigurinë kibernetike”, si dhe në nenet 54 e 157, të ligjit nr. 54/2024, “Për komunikimet elektronike në Republikën e Shqipërisë”, në kuadër të masave për të realizuar sigurinë e rrjeteve dhe të shërbimeve, me qëllim përballimin e situatave në rastet e sulmeve kibernetike, sipërmarrësit e komunikimeve elektronike marrin masat, si më poshtë:

a) të kryejnë vlerësime periodike të rrezikut kibernetik çdo 12 muaj;

b) të kenë në funksionim sisteme të monitorimit e të analizës (SIMNJ/QOS) për detektimin e anomalive;

c) të zbatojnë arkitekturën “Zero besim”, me akses të kufizuar sipas funksioneve;

ç) të mbajnë kopje rezervë *offline* të sistemeve dhe të konfigurimeve kritike;

d) të kryejnë testime dhe simulime për skenarë emergjencash kibernetike;

dh) të kenë një plan të shkruar të reagimit ndaj incidenteve (PRI), sipas kërkesave të AKSK-së.

2. Sipërmarrësit e komunikimeve elektronike aktivizojnë kanale të sigurta të komunikimit me autoritetet dhe duhet të realizojnë kriptimin e detyrueshëm të të gjitha lidhjeve të transmetimit.

3. Në rastin e incidenteve, sipërmarrësit e komunikimeve elektronike kryejnë izolimin e pjesëve të kompromentuara të rrjetit, respektojnë standardet e sigurisë për kontrollin e aksesit, si dhe kryejnë auditim dhe analizë të plotë teknike të incidentit.

4. Sipërmarrësit e komunikimeve elektronike hartojnë raportin e incidentit dhe e paraqesin në AKEP dhe AKSK jo më vonë se 72 orë.

5. Sipërmarrësit e komunikimeve elektronike rishikojnë periodikisht politikat e brendshme të sigurisë, planet e vazhdimësisë së biznesit dhe planet e reagimit ndaj incidenteve, si dhe kryejnë rregullisht trajnimin e stafit për sigurinë kibernetike.

Neni 11

Bashkëpunimi ndërkombëtar

Në rastet e jashtëzakonshme dhe sipas nevojës, bazuar në Konventën Tampere dhe në marrëveshjet e bashkëpunimit, ku Shqipëria është palë, ministria përgjegjëse për komunikimet elektronike dhe AKEP-i, në bashkëpunim me autoritetet përgjegjëse, mund të kërkojnë ndihmë nga partnerët ndërkombëtarë, vendet pjesëmarrëse në Konventën Tampere, për sigurimin e pajisjeve të komunikimit të lëvizshme, përfshirë mbulimin me komunikime satelitore, me qëllim sigurimin e shërbimeve të telekomunikacionit, sipas përcaktimeve në Konventën Tampere.

Neni 12

Autorizimet e përkohshme për rastet e situatave të jashtëzakonshme

Me qëllim përballimin e situatave të jashtëzakonshme, AKEP-i, sipas parashikimeve në ligjin për komunikimet elektronike dhe Planin Kombëtar të Frekuencave, ka të drejtë të japë autorizime të përkohshme për përdorimin e frekuencave rezervë për rastet e emergjencave, me qëllim sigurimin e komunikimeve elektronike.

Operatorët që veprojnë në fushën e ndihmës ndërkombëtare, në rastin e marrjes së ndihmës përmes Konventës Tampere, parashikuar në nenin 11 të saj, mund të pajisen me autorizim të përkohshëm për përdorimin e pajisjeve dhe të frekuencave, sipas një procedure të përshpejtuar.

Neni 13

Koordinimi operacional dhe pika kombëtare e kontaktit

1. Në rastin e situatave të jashtëzakonshme, me qëllim koordinimin e veprimeve për sigurimin e shërbimeve të komunikimeve elektronike, pranë ministrisë përgjegjëse krijohet njësia e koordinimit, si një strukturë *ad hoc*, që bashkëpunon me AKEP-in dhe autoritetet përgjegjëse për emergjencat, me qëllim koordinimin e veprimeve për sigurimin e vazhdueshmërisë së ofrimit të shërbimeve të komunikimit.

2. Ministria cakton një pikë kombëtare kontakti për të koordinuar me Bashkimin Ndërkombëtar të Telekomunikacionit (ITU), autoritetet përgjegjëse për emergjencat dhe partnerët ndërkombëtarë për të kërkuar ndihmë sipas nenit 11, në zbatim të Konventës Tampere.

3. Në rastet e jashtëzakonshme, Ministria dhe AKEP-i koordinojnë me sipërmarrësit dhe institucionet përgjegjëse për të siguruar vazhdimin e punës së sipërmarrësve të komunikimeve elektronike dhe të punonjësve të tyre, që operojnë në terren, në veçanti për pajisjen me lejet e nevojshme, për:

a) kryerjen e punimeve në terren për linjat apo infrastrukturat e telekomunikacioneve;

b) lëvizjen e kontrolluar sipas një liste personeli dhe targash të automjeteve, të cilat do të jenë në shërbim të operacioneve në rast emergjencash;

c) mundësimin e aksesimit të infrastrukturës publike apo private, që shërben për menaxhimin, vazhdueshmërinë dhe rikthimin në normalitet të shërbimeve të komunikimeve elektronike.

Neni 14

Regjistri i operatorëve dhe i shërbimeve të autorizuara

AKEP-i, mbi bazën e informacioneve të sipërmarrësve dhe në bashkëpunim me ministrinë përgjegjëse për komunikimet elektronike, krijon një regjistër të sipërmarrësve, që zotërojnë pajisje të lëvizshme telekomunikacioni, që mund të përdoren për rastet e situatave të jashtëzakonshme.

Neni 15
Testimet dhe auditimet

Sipërmarrësit e komunikimeve elektronike organizojnë, të paktën 1 (një) herë në vit, testime ose simulime të kapaciteteve të telekomunikacionit në raste të situatave të jashtëzakonshme. Testimet dhe auditimet duhet të jenë të dokumentuara. Testimet dhe auditimet kryhen dhe me kërkesë e prezencë të përfaqësuesve të AKEP-it dhe/ose të ministrisë/autoriteteve përgjegjëse mbi bazën e një plani të koordinuar e të dakordësuar paraprakisht.

ANEKS 1

MODEL ORIENTUES PËR SIPËRMARRËSIT PËR PLANIN E MASAVE

Plani i masave për vazhdueshmërinë e ofrimit të shërbimeve të komunikimeve elektronike në raste të jashtëzakonshme

Për: _____
Sektori: Telekomunikacion/komunikime elektronike

1. Qëllimi dhe fushëveprimi

Ky dokument përcakton politikat, procedurat dhe përgjegjësitë për rikuperimin e sistemeve kritike të rrjetit dhe të shërbimeve të komunikimeve të _____, në rast fatkeqësie ose ndërprerjeje të rëndë. Plani zbatohet për të gjitha sistemet, rrjetet dhe qendrat e të dhënave të operatorit, që ndikojnë në ofrimin e shërbimeve të komunikimit elektronik për klientët.

2. Objektivat e planit

- Sigurimi i rikuperimit të shpejtë dhe të sigurt të funksioneve kritike pas një ndërprerjeje.
- Minimizimi i ndikimit ndaj përdoruesve (individë, biznes, autoritete publike) dhe i infrastrukturës kombëtare të komunikimit.
- Pajtueshmëria me kërkesat ligjore për sigurinë dhe me kërkesat kombëtare për vazhdimësinë e shërbimit.

3. Struktura organizative dhe përgjegjësitë

Ekipet përgjegjëse për zbatimin e PRF-së përfshijnë:

- ekipin e menaxhimit të krizës – koordinon përgjigjen e përgjithshme ndaj incidentit;
- ekipin teknik, të operimit e të mirëmbajtjes së rrjetit – zbaton procedurat teknike të rikuperimit;
- ekipin e vlerësimit të dëmtimeve;
- ekipin e komunikimit – menaxhon njoftimet publike dhe komunikimin me autoritetet;
- ekipin e sigurisë së informacionit – monitoron aspektet e sigurisë kibernetike gjatë rikuperimit.

4. Analiza e sistemeve kritike

Operatori _____ identifikon sistemet dhe shërbimet kritike, që kanë ndikim të drejtpërdrejtë në funksionimin e rrjetit kombëtar të telekomunikacionit, duke përcaktuar për secilin objektivat, për:

- kohën maksimale të pranueshme për rikuperim;

- kufirin maksimal të humbjes së të dhënave të pranueshme.

5. Strategjitë e kopjeve rezervë të të dhënave dhe të ruajtjes së të dhënave

- Kopjet rezervë të të dhënave kryhen çdo ditë për sistemet kritike dhe ruhen në një lokacion të sigurt jashtë sistemeve primare;
- Kopjet e të dhënave ruhen në *cloud* të sigurt brenda vendit dhe në një qendër alternative të të dhënave (*hot site*);
- Integriteti i kopjeve rezervë të të dhënave testohet periodikisht për të garantuar rikthimin e plotë të të dhënave.

6. Infrastruktura e rikuperimit

Operatori _____ mban kapacitete alternative operative për rikuperimin e shërbimeve:

- Qendër rezervë me pajisje të gatshme për aktivizim të menjëhershëm;
- Kapacitete të përgatitura pjesërisht për aktivizim brenda 24 orëve;
- Ambient rezervë pa pajisje, për raste ekstreme.

7. Procedurat e rikuperimit

Në rast fatkeqësie, aktivizohen procedurat e mëposhtme:

1. Vlerësimi i incidentit dhe njoftimi i menjëhershëm i ekipit të menaxhimit të krizës;
2. Aktivizimi i qendrës rezervë dhe rikthimi i serverave kritikë;
3. Rikthimi i bazave të të dhënave dhe lidhjeve të rrjetit;
4. Testimi i funksionimit të plotë para rifillimit të shërbimeve për publikun.

8. Plani i komunikimit dhe koordinimi

Operatori _____ mban linja të dedikuara komunikimi për situata emergjente dhe një plan komunikimi të krizës, që përfshin:

- informimin e autoriteteve rregullatore (AKEP, AKSK);
- komunikimin me klientët dhe partnerët për ndërprerjet;
- përdorimin e kanaleve alternative të komunikimit, në rast dështimi të rrjeteve primare.

9. Testimi dhe mirëmbajtja e planit

Plani testohet të paktën një herë në vit përmes simulimeve dhe ushtrimeve praktike. Pas çdo testi ose incidenti real, plani përditësohet në bazë të mësimeve të nxjerra. Verifikimet përputhen me kërkesat e NIS2 dhe udhëzimet e ENISA-s për testimin e qëndrueshmërisë së rrjeteve.

10. Aspektet ligjore dhe përputhshmëria

Ky plan është në përputhje me përcaktimet e ligjit për komunikimet elektronike dhe të ligjit për emergjencat civile, të ligjit për sigurinë kibernetike dhe rregulloret përkatëse të AKEP-it. Operatorët janë të detyruar të raportojnë incidentet madhore të sigurisë brenda 24 orëve nga identifikimi i tyre dhe të bashkëpunojnë me autoritetet për rikuperim të plotë.

11. Trajnimi dhe ndërgjegjësimi

Të gjithë punonjësit e përfshirë në zbatimin e PRF-së trajnohen periodikisht mbi procedurat e reagimit, të sigurisë së informacionit dhe komunikimit në situata emergjente. Operatori _____ organizon ushtrime praktike dhe verifikon gatishmërinë e personelit në çdo nivel.

Ky plan hyn në fuqi në datën _____ dhe rishikohet çdo 12 muaj.

ANEKS 2

MASAT PËR SIGURIMIN E VAZHDUESHMËRISË SE SHËRBIMEVE PARA, GJATË DHE MBAS SITUATAVE TË JASHTËZAKONSHME DHE DOKUMENTIMI

Masat e sigurisë	**Dokumentacioni**
- Sipërmarrësi i rrjeteve publike të komunikimeve elektronike duhet të implementojë një strategji për vazhdimësinë e ofrimit të shërbimit për rrjetet e komunikimit dhe sistemet e informacionit.	Strategjia/plani i dokumentuar për vazhdimësinë e shërbimit, duke përfshirë kohën e rikuperimit për shërbimet dhe proceset kryesore. Dokumentim i "Planit të vazhdimësisë së biznesit" (PVB).
- Sipërmarrësi i rrjeteve publike të komunikimeve elektronike duhet të implementojë dhe të zbatojë planet e emergjencës për sektorët dhe	Planet e emergjencës për sistemet kritike, duke përfshirë hapa të qartë dhe procedurat për kërcënimet e njohura, shkaktuesit për aktivizimin, hapat dhe

shërbimet kritike. - Sipërmarrësi i rrjeteve publike të komunikimeve elektronike duhet të monitorojë aktivitetet dhe zbatimin e planeve të emergjencës, regjistrimin e tentativave të suksesshme të rikuperimit dhe dështimet. - Sipërmarrësi i rrjeteve publike të komunikimeve elektronike duhet të kryejë rishikimin dhe kontrollin periodik të strategjisë për vazhdimësinë e shërbimit. - Sipërmarrësi i rrjeteve publike të komunikimeve elektronike duhet të testojë planet rezervë (*backup*) dhe të emergjencës për të siguruar që sistemet dhe proceset funksionojnë, dhe që personeli është i përgatitur në rastin e dëmtimeve të mëdha dhe emergjencave. - Sipërmarrësi i rrjeteve publike të komunikimeve elektronike duhet të implementojë një program për ushtrimin rregullisht të planeve rezervë dhe të emergjencës, duke përdorur skenarë realistë, që mbulojnë një sërë skenarësh të ndryshëm me kalimin e kohës. - Përfshirja në ushtrime e furnitorëve dhe palëve të tjera të treta. - Sipërmarrësi i rrjeteve publike të komunikimeve elektronike duhet të rishikojë dhe të përditësojë planet, duke marrë në konsideratë ndryshimet, incidentet e mëparshme dhe emergjencat që nuk kanë qenë të mbuluara nga programi i ushtrimit. - Mësimet e nxjerra nga këto ushtrime të jenë adresuar nga personat përgjegjës dhe në përputhje me rrethanat të bëhet përditësimi i proceseve dhe sistemeve përkatëse.	kohën e rikuperimit. Dokumentim i planit të rikuperimit pas fatkeqësisë PRF.
	Dokumentimi që identifikon asetet dhe nyjat kritike të rrjetit.
	Dokumentimi që tregon se sipërmarrësi ka linja rezervë, servera pasivë, mjete komunikimi të bazuara në teknologjinë *cloud* dhe lidhje të pavarura për stacionet bazë dhe shërbimet kritike.
	Dokumentimi që tregon se sipërmarrësi ka pajisur qendrat e të dhënave, stacionet dhe antenat transmetuese me burime alternative të energjisë.
	Dokumentimi që garanton funksionalitetin e numrit unik evropian të emergjencave "112" edhe pa kartë SIM, si dhe çdo numër kombëtar të emergjencës, të përcaktuar sipas legjislacionit në fuqi.
	Dokumentimi që tregon se sipërmarrësi ka marrë pjesë në ushtrime kombëtare simulimi të organizuara nga AKEP-i dhe institucionet përgjegjëse.
	Dokumentimi që tregon se sipërmarrësi ka caktuar person kontakti në raste të jashtëzakonshme që komunikon me AKEP-in.
- Sipërmarrësi i rrjeteve publike të komunikimeve elektronike duhet të përgatitet për rikthimin në gjendjen normale të sistemeve të komunikimeve elektronike. - Sipërmarrësi i rrjeteve publike të komunikimeve elektronike duhet të implementojë politika/procedura për vendosjen e kapaciteteve për rikuperimin e infrastrukturave të komunikimit elektronike.	Dokumentimi i aktivizimit dhe i zbatimit të planeve të emergjencës, duke përfshirë vendimet e marra, hapat e ndjekur, kohën e plotë të rikuperimit. Dokumentacion që sipërmarrësi ka parashikuar ngritjen e qendrës së reagimit të emergjencave ose ekipit/eve të brendshëm/me të emergjencës.
	Dokumentacioni që sipërmarrësi ka përcaktuar sistem njoftimi për autoritetet përkatëse për çdo ndërprerje të shërbimeve.
	Dokumentacioni që sipërmarrësi ka siguruar mjete të lëvizshme të rrjetit telefonik celular për t'u vendosur në terren.
	Dokumentimi që tregon se sipërmarrësi ka pajisur qendrat e të dhënave, stacionet dhe antenat transmetuese me burime alternative energjie.
	Dokumentacioni që sipërmarrësi ka në përdorim rirutim automatik të lidhjeve përmes lidhjeve rezervë, përfshirë dhe ato ndërkombëtare. Përdorimi i sistemeve satelitore për mbulimin me sisteme komunikimi për autoritetet.
	Dokumentacioni që sipërmarrësi ka siguruar akses për përdoruesit në shërbimet bazë emergjente (telefoni, 112, SMS).
	Dokumentacioni që sipërmarrësi ka transportuar gjatë krizës drejt AKEP-it dhe strukturave të tjera gjatë situatës.
	Strategjia e përditësuar e vazhdimësisë dhe planet e emergjencës, shqyrtimi i komenteve dhe/ose

	ndryshimi i *log*-eve. Dokumentacioni që sipërmarrësi ka bërë vlerësim e raportim për dëmet brenda 48 orëve pas ngjarjes.
	Dokumentacioni që sipërmarrësi ka rikthyer funksionalitetin e rrjetit dhe të shërbimeve sipas planit të rikuperimit.
	Dokumentacioni që sipërmarrësi ka kryer një analizë pas ngjarjes dhe ka raportuar me AKEP-in dhe institucionet e përcaktuara me ligj.
	Dokumentacioni që sipërmarrësi ka përditësuar planet PVB/PRF dhe ka raportuar tek AKEP-i.
	Dokumentacioni që sipërmarrësi ka ndërtuar një manual praktik për përmirësim të kapaciteteve reaguese në të ardhmen.

ANEKS 3

MASAT PËR VAZHDUESHMËRINË E OFRIMIT TË SHËRBIMEVE NË RASTIN E SULMEVE KIBERNETIKE

Masat	**Dokumentacioni**
- Sipërmarrësi i rrjeteve publike të komunikimeve elektronike ose të shërbimeve të komunikimeve elektronike merr masat e duhura teknike, organizative dhe proporcionale për të menaxhuar në mënyrë të përshtatshme rreziqet që vijnë për sigurinë e rrjeteve dhe shërbimeve. Implementimi i monitorimit të *log*-eve për sistemet e informacionit. - Sipërmarrësi i rrjeteve publike të komunikimeve elektronike duhet të kryejë rishikime menaxheriale të menaxhimit të sigurisë së sistemeve, *log*-eve dhe raporteve të monitorimit të rrjeteve të komunikimit dhe të sistemeve të informacionit. - Implementimi i politikave të ngjarjeve dhe monitorimit të sistemeve. - Sipërmarrësi i rrjeteve publike të komunikimeve elektronike duhet të rishikojë dhe të përditësojë politikat e procedurat, duke marrë parasysh ndryshimet dhe incidentet e mëparshme.	Dokumentimi që tregon se sipërmarrësi ka kryer vlerësime të rrezikut kibernetik çdo 12 muaj.
	Dokumentimi që tregon se sipërmarrësi ka në funksionim sisteme të monitorimit dhe të analizës (SIMNJ/QOS) për detektimin e anomalive.
	Dokumentimi që tregon se sipërmarrësi ka zbatuar arkitekturën "Zero besim", me akses të kufizuar sipas funksioneve.
	Dokumentimi që tregon se sipërmarrësi ka kopje rezervë *offline* të sistemeve dhe të konfigurimeve kritike.
	Dokumentimi që tregon se sipërmarrësi ka kryer testime dhe simulime për skenarë emergjencash kibernetike.
	Dokumentimi që tregon se sipërmarrësi ka një plan të shkruar të reagimit ndaj incidenteve (PRI), të certifikuar nga AKSK-ja.
	Dokumentimi që tregon se sipërmarrësi ka sisteme njoftimi për institucionet e AKSK-së dhe AKEP-it, në rast incidenti.
	Dokumentimi që tregon se sipërmarrësi ka aktivizuar kanale të sigurta të komunikimit me autoritetet.
	Dokumentimi që tregon se sipërmarrësi ka kryer izolimin e pjesëve të kompromentuara të rrjetit dhe kontrollin e aksesit.
	Dokumentimi që tregon se sipërmarrësi ka kryer auditim forensik dhe analizë të plotë teknike të incidenteve.
	Dokumentimi që tregon se sipërmarrësi ka hartuar raportin e incidentit dhe e ka dorëzuar tek AKEP-i dhe AKSK-ja.

	Dokumentimi që tregon se sipërmarrësi ka rishikuar politikat e brendshme të sigurisë dhe trajnimit të stafit.
	Dokumentimi që tregon se sipërmarrësi ka përditësuar planet e vazhdimësisë së biznesit (PVB) dhe planet e reagimit ndaj incidenteve (PRI).