FLETORJA ZYRTARE
E REPUBLIKËS SË SHQIPËRISË

www.qbz.gov.al

Botim i Qendrës së Botimeve Zyrtare

Viti: 2026 – Numri: 2

Tiranë – E hënë, 5 janar 2026

PËRMBAJTJA

		Faqe
Vendim i Këshillit të Ministrave nr. 813, datë 30.12.2025	Për miratimin e skemës kombëtare të certifikimit të sigurisë kibernetike, si dhe të niveleve të sigurisë së skemës.....	219
Vendim i Këshillit të Ministrave nr. 814, datë 30.12.2025	Për miratimin e procedurave të identifikimit, klasifikimit, përshkallëzimit dhe menaxhimit të krizës kibernetike.....	251
Vendim i Këshillit të Ministrave nr. 822, datë 30.12.2025	Për disa shtesa në vendimin nr. 1128, datë 30.12.2020, të Këshillit të Ministrave, "Për zbatimin nga Republika e Shqipërisë të vendimeve të Këshillit të Bashkimit Evropian për vendosjen, ndryshimin dhe shfuqizimin e masave shtrënguese ndërkombëtare, të ndryshuara", të ndryshuar.....	262
Vendim i Këshillit të Ministrave nr. 831, datë 30.12.2025	Për miratimin e Kodit të Etikës në Shkencë dhe në Kërkim Shkencor	269
Vendim i Këshillit të Ministrave nr. 832, datë 30.12.2025	Për krijimin e bazës së të dhënave shtetërore të Sistemit të Menaxhimit të Informacionit të Arsimit të Lartë (SMIAL)	275
Vendim i Këshillit të Ministrave nr. 833, datë 30.12.2025	Për miratimin e standardeve e të kritereve që mundësojnë zbatimin e parimit të shkencës së hapur dhe janë në përputhje me politikat e zonës evropiane të kërkimit.....	277
Vendim i Këshillit të Ministrave nr. 840, datë 30.12.2025	Për një shtesë në vendimin nr. 893, datë 17.12.2014, të Këshillit të Ministrave, "Për miratimin e rregullave të organizimit dhe të funksionimit të kabineteve ndihmëse, të organizimit të brendshëm të institucioneve të administratës shtetërore, si dhe për procedurat e hollësishme për përgatitjen, propozimin, konsultimin dhe miratimin e organizimit të brendshëm", të ndryshuar	280

VENDIM
Nr. 813, datë 30.12.2025

PËR MIRATIMIN E SKEMËS KOMBËTARE TË CERTIFIKIMIT TË SIGURISË KIBERNETIKE, SI DHE TË NIVELEVE TË SIGURISË SË SKEMËS[1]

Në mbështetje të nenit 100 të Kushtetutës dhe të pikës 1, të nenit 42, të ligjit nr.25/2024, "Për sigurinë kibernetike", me propozimin e Kryeministrit, Këshilli i Ministrave

VENDOSI**:**

KREU I
DISPOZITA TË PËRGJITHSHME

Neni 1
Objekti dhe fusha e zbatimit

1. Objekti i këtij vendimi është miratimi i skemës së certifikimit të sigurisë kibernetike të bazuar në kriteret e përbashkëta evropiane, si dhe i niveleve të sigurisë së skemës.

2. Ky vendim zbatohet për të gjitha produktet e teknologjisë së informacionit dhe komunikimit (TIK), duke përfshirë dokumentacionin që dorëzohet për certifikim sipas skemës, si dhe të gjitha profilet e mbrojtjes, të cilat dorëzohen për certifikim si pjesë e procesit TIK deri në certifikimin e produkteve TIK.

Neni 2
Përkufizimet

Në kuptim të këtij vendimi, termat e mëposhtëm kanë këto kuptime:

1. "**Autoriteti i mbikëqyrjes së tregut**", struktura përgjegjëse për mbikëqyrjen e tregut, sipas parashikimeve të legjislacionit në fuqi dhe vendimit përkatës të Këshillit të Ministrave për krijimin, organizimin dhe funksionimin e inspektoratit shtetëror përgjegjës për mbikëqyrjen e tregut;

2. **"Certifikatë"**, një certifikatë sigurie kibernetike e lëshuar sipas skemës së certifikimit të sigurisë kibernetike për produktet TIK, ose për profilet e mbrojtjes që mund të përdoren ekskluzivisht në procesin e certifikimit TIK dhe të produkteve TIK;

3. **"Deklaratë konformiteti"**, një deklaratë e lëshuar nga prodhuesi ose ofruesi i një produkti, shërbimi apo procesi TIK, me të cilin ai deklaron nën përgjegjësinë e tij se ky produkt, shërbim apo proces përputhet me kërkesat dhe kriteret e sigurisë të përcaktuara në skemën e certifikimit të sigurisë kibernetike.

4. **"Dokument teknik më i fundit"**, një dokument që specifikon metodat, teknikat dhe mjetet e vlerësimit që zbatohen për certifikimin e produkteve TIK, ose kërkesat e sigurisë të një kategorie të përgjithshme produkti TIK, ose çdo kërkesë tjetër e nevojshme për certifikim, me qëllim harmonizimin e vlerësimit, në veçanti të fushave teknike apo profileve të mbrojtjes;

5. **"Fushë teknike"**, një kuadër i përbashkët teknik lidhur me një teknologji të caktuar për certifikimin e harmonizuar me një sërë kërkesash të sigurisë;

6. "**Kriteret e përbashkëta**", kriteret e përbashkëta për vlerësimin e sigurisë së teknologjisë së informacionit (TI), siç përcaktohen në standardet ISO/IEC 15408-1:2022, ISO/IEC 15408-2:2022, ISO/IEC 15408-3:2022, ISO/IEC 15408-4:2022 ose ISO/IEC 15408-5:2022, ose në kriteret e përbashkëta për vlerësimin e sigurisë së teknologjisë së informacionit (TI)[2], versioni i kritereve të përbashkëta 2022, pjesët 1 deri në 5, që janë adoptuar dhe publikuar në nivel kombëtar nga Drejtoria e Përgjithshme e Standardizimit;

7. **"Metodologjia e përbashkët e vlerësimit",** metodologjia e përbashkët për vlerësimin e sigurisë së teknologjisë së informacionit, siç përcaktohet në standardin ISO/IEC 18045:2022, që janë adoptuar

[1] Ky projektvendim është përafruar plotësisht me rregulloren zbatuese të Komisionit (BE) 2024/482, të datës 31 janar 2024, që përcakton rregullat për zbatimin e rregullores (BE) 2019/881 të Parlamentit Evropian dhe të Këshillit, në lidhje me miratimin e skemës së certifikimit të sigurisë kibernetike të bazuar në Kriteret e Përbashkëta Evropiane (EUCC), nr.CELEX: EUR-Lex-32024R0482, nr. natyral: 2024/482/BE, Fletore Zyrtare: seria L, datë 7.2.2024, faqe 6-45, e cila është ndryshuar me rregulloren zbatuese të Komisionit (BE) 2024/3144, të datës 18 dhjetor 2024, nr.CELEX: EUR-Lex-32024R3144, nr. natyral: 2024/3144 /BE, Fletore Zyrtare: seria L, datë 19.12.2024, faqe 3-7. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32024R0482

[2] Kriteret e përbashkëta për vlerësimin e sigurisë së teknologjisë së informacionit: https://commoncriteriaportal.org/files/ccfiles/CC2022PART1R1.pdf

dhe publikuar në nivel kombëtar nga Drejtoria e Përgjithshme e Standardizimit, ose metodologjia e përbashkët për vlerësimin e sigurisë së teknologjisë së informacionit[3], versioni "Metodologjia e përbashkët për vlerësimin 2022";

8. **"Niveli AVA_VAN"**, niveli i analizës së vulnerabiliteteve të sigurisë, që tregon shkallën e aktiviteteve të vlerësimit të sigurisë kibernetike të kryera për të përcaktuar nivelin e qëndrueshmërisë ndaj shfrytëzimit të mundshëm të defekteve ose të dobësive në objektivin e vlerësimit në mjedisin e tij operacional, siç përcaktohet në skemë;

9. **"Objekt i vlerësimit"**, një produkt TIK ose një pjesë e tij, ose një profil i mbrojtjes si pjesë e një procesi TIK, i cili i nënshtrohet vlerësimit të sigurisë kibernetike për të marrë certifikimin sipas skemës;

10. **"Objektiv sigurie"**, një përshkrim i kërkesave të sigurisë, që priten të përmbushen dhe varen nga zbatimi për një produkt TIK specifik;

11. **"Organ certifikues"**, një person juridik, kombëtar ose ndërkombëtar i akreditуar nga institucioni përgjegjës për akreditimin dhe i autorizuar nga autoriteti përgjegjës për sigurinë kibernetike, përgjegjës për kryerjen e aktiviteteve të vlerësimit të konformitetit, bazuar në raportet e vlerësimit të përgatitura nga ITSEF-i, duke përfshirë certifikim dhe inspektim;

12. **"Organe të vlerësimit të konformitetit"**, organe që kryejnë aktivitete të vlerësimit të konformitetit, duke përfshirë organe certifikuese dhe ITSEF, sipas përcaktimeve të kësaj skeme.

13. **"Organi kombëtar i certifikimit të sigurisë kibernetike",** Autoriteti Kombëtar për Sigurinë Kibernetike, përgjegjës për certifikimin e sigurisë kibernetike sipas këtij vendimi;

14. **"Organi i vlerësimit të sigurisë së teknologjisë së informacionit (ITSEF)"**, një person juridik, kombëtar ose ndërkombëtar, i akreditуar nga institucioni përgjegjës për akreditimin dhe i autorizuar nga autoriteti përgjegjës për sigurinë kibernetike për të kryer aktivitete të vlerësimit të konformitetit teknik, duke përfshirë kalibrim dhe testim.

15. **"Produkt i përbërë"**, një produkt TIK që vlerësohet së bashku me një produkt tjetër TIK, që ka marrë tashmë një certifikatë dhe mbi funksionalitetin e sigurisë së të cilit varet produkti i përbërë TIK;

16. **"Profili i mbrojtjes"**, një proces TIK, që përcakton kërkesat e sigurisë për një kategori specifike të produkteve TIK, duke adresuar nevojat e sigurisë të pavarura nga zbatimi, të cilat mund të përdoren për të vlerësuar produktet TIK, që i përkasin asaj kategorie specifike për certifikimin e tyre.

17. **"Raport teknik vlerësimi"**, një dokument i prodhuar nga një ITSEF, ku paraqiten gjetjet, vendimet dhe arsyetimet e marra gjatë vlerësimit të një produkti TIK ose një profili të mbrojtjes, në përputhje me rregullat dhe detyrimet e përcaktuara në këtë vendim.

Neni 3
Standardet e vlerësimit

1. Standardet që zbatohen për vlerësimet që kryhen sipas skemës janë:

a) kriteret e përbashkëta;

b) metodologjia e përbashkët e vlerësimit.

2. Një certifikatë që përmbush standardet e përmendura në pikën 1 të këtij neni mund të lëshohet, gjithashtu, sipas skemës, duke deklaruar konformitet me një profil të mbrojtjes, me kusht që përdorimi i një profili të tillë të mbrojtjes kërkohet sipas legjislacionit në fuqi për tahografët ose sipas legjislacionit në fuqi për identifikimin elektronik dhe shërbimet e besuara, i cili ka përmbushur njërin nga standardet e mëposhtme:

a) Kriteret e përbashkëta për vlerësimin e sigurisë së teknologjisë së informacionit, versioni 3.1, rishikimet 1 deri në 4;

b) Metodologjia e përbashkët për vlerësimin e sigurisë së teknologjisë së informacionit, versioni 3.1, rishikimet 1 deri në 4.

Neni 4
Nivelet e sigurisë për të cilat kërkohet certifikim

1. Organet e certifikimit lëshojnë certifikata sipas skemës në nivel sigurie "të konsiderueshme" ose "të lartë".

2. Certifikatat në nivelin e sigurisë "të konsiderueshme" korrespondojnë me certifikatat që mbulojnë nivelin AVA_VAN 1 ose 2.

[3] Metodologjia e përbashkët për vlerësimin e sigurisë së teknologjisë së informacionit: https://www.commoncriteriaportal.org/files/ccfiles/CEM2022R1.pdf

3. Certifikatat në nivelin e sigurisë "të lartë" korrespondojnë me certifikatat që mbulojnë nivelin AVA_VAN 3, 4 ose 5.

4. Niveli i sigurisë i konfirmuar në një certifikatë sipas skemës bën dallimin ndërmjet përdorimit konform dhe të shtuar të komponentëve të sigurisë, sipas përcaktimeve në kriteret e përbashkëta, në përputhje me aneksin VIII të këtij vendimi.

5. Organet e vlerësimit të konformitetit aplikojnë ata komponentë sigurie, nga të cilët varet niveli i përzgjedhur AVA_VAN, në përputhje me standardet e përmendura në nenin 3 të këtij vendimi.

Neni 5
Metodat për certifikimin e produkteve TIK

1. Certifikimi i një produkti TIK kryhet kundrejt objektivit të tij të sigurisë:

a) sipas përcaktimeve nga aplikanti;

b) duke përfshirë një profil të mbrojtjes të certifikuar si pjesë e procesit TIK, ku produkti TIK bën pjesë në kategorinë e produktit TIK, që mbulohet nga ai profil i mbrojtjes.

2. Profilet e mbrojtjes certifikohen për qëllimin e vetëm të certifikimit të produkteve TIK, që bëjnë pjesë në kategorinë specifike të produkteve TIK, që mbulohen nga profili i mbrojtjes.

Neni 6
Vetëvlerësimi i konformitetit

Një vetëvlerësim i konformitetit nuk lejohet nga ana e prodhuesit ose e ofruesit të produkteve, shërbimeve dhe proceseve TIK.

KREU II
CERTIFIKIMI I PRODUKTEVE TIK

SEKSIONI 1
STANDARDET DHE KËRKESAT SPECIFIKE PËR VLERËSIM

Neni 7
Kriteret dhe metodat e vlerësimit për produktet TIK

1. Një produkt TIK i paraqitur për certifikim vlerësohet minimalisht, në përputhje me sa më poshtë:

a) Elementet e zbatueshme të standardeve të përmendura në nenin 3 të këtij vendimi;

b) Klasat e kërkesat për garantimin e sigurisë për vlerësimin e vulnerabiliteteve dhe testimin e pavarur funksional, sipas përcaktimeve në standardet e vlerësimit të përmendura në nenin 3 të këtij vendimi;

c) Nivelin e rrezikut që lidhet me përdorimin e synuar të produkteve TIK, sipas përcaktimeve në nenin 8 të këtij vendimi dhe nenin 40 të ligjit nr.25/2024, "Për sigurinë kibernetike";

ç) Dokumentet teknike më të fundit të aplikimit sipas përcaktimeve në aneksin I të këtij vendimi;

d) Profilet e zbatueshme të mbrojtjes të certifikuara sipas përcaktimeve në aneksin II të këtij vendimi.

2. Në raste të jashtëzakonshme dhe të justifikuara, një organ i vlerësimit të konformitetit mund të kërkojë të tërhiqet nga zbatimi i dokumentit teknik më të fundit. Në raste të tilla, organi i vlerësimit të konformitetit informon organin kombëtar të certifikimit të sigurisë kibernetike me një justifikim për kërkesën e tij. Organi kombëtar i certifikimit të sigurisë kibernetike vlerëson justifikimin për një përjashtim kur është i arsyetuar dhe e miraton atë. Deri në vendimmarrjen e organit kombëtar të certifikimit të sigurisë kibernetike, organi i vlerësimit të konformitetit nuk lëshon asnjë certifikatë.

Me anëtarësimin e Republikës së Shqipërisë në Bashkimin Evropian (BE), organi kombëtar i certifikimit të sigurisë kibernetike njofton përjashtimin e miratuar pranë Grupit Evropian të Certifikimit të Sigurisë Kibernetike, i cili mund të dalë me një opinion. Opinioni i Grupit Evropian të Certifikimit të Sigurisë Kibernetike merret parasysh nga organi kombëtar i certifikimit të sigurisë kibernetike.

3. Certifikimi i produkteve TIK në nivelin 4 ose 5 AVA_VAN është i mundur vetëm për sa më poshtë:

a) Kur produkti TIK mbulohet nga një fushë teknike, sipas përcaktimeve në aneksin I të këtij vendimi, vlerësohet në përputhje me dokumentet teknike më të fundit të zbatueshme të fushave teknike;

b) Kur produkti TIK bën pjesë në një kategori produktesh TIK të mbuluara nga një profil i certifikuar i mbrojtjes, që përfshin nivelet AVA_VAN 4 ose 5 dhe është i renditur si një profil i mbrojtjes, sipas përcaktimeve në aneksin II të këtij

vendimi, vlerësohet në përputhje me metodologjinë e vlerësimit të specifikuar për atë profil të mbrojtjes;

c) Kur përcaktimet në shkronjat "a" dhe "b" të kësaj pike nuk janë të zbatueshme dhe kur përfshirja e një *domain*-i teknik, sipas përcaktimeve në aneksin I të këtij vendimi, ose e një profili të mbrojtjes të certifikuar, sipas përcaktimeve në aneksin II të këtij vendimi, nuk realizohet në të ardhmen e afërt, vetëm në raste të jashtëzakonshme e në raste të justifikuara në varësi të kushteve të përcaktuara në pikën 4 të këtij neni.

4. Kur një organ i vlerësimit të konformitetit e konsideron se ndodhet në një rast të jashtëzakonshëm e të justifikuar, të përmendur në shkronjën "c", të pikës 3, të këtij neni, njofton për certifikimin e synuar tek organi kombëtar i certifikimit të sigurisë kibernetike me një justifikim dhe një metodologji vlerësimi të propozuar. Organi kombëtar i certifikimit të sigurisë kibernetike vlerëson justifikimin për një përjashtim dhe, kur justifikohet, miraton ose amendon metodologjinë e vlerësimit, që zbatohet nga organi i vlerësimit të konformitetit. Deri në vendimmarrjen e organit kombëtar të certifikimit të sigurisë kibernetike, organi i vlerësimit të konformitetit nuk lëshon certifikata. Me anëtarësimin e Republikës së Shqipërisë në Bashkimin Evropian, organi kombëtar i certifikimit të sigurisë kibernetike ia raporton certifikimin e synuar Grupit Evropian të Certifikimit të Sigurisë Kibernetike, i cili mund të dalë me një opinion. Opinioni i Grupit Evropian të Certifikimit të Sigurisë Kibernetike merret në konsideratë nga organi kombëtar i certifikimit të sigurisë kibernetike.

5. Në rastin e një produkti TIK, që i nënshtrohet një vlerësimi të produktit të përbërë, në përputhje me dokumentet teknike më të fundit, ITSEF-i, që ka kryer vlerësimin e produktit TIK, ndan informacionin përkatës me ITSEF-in, që kryen vlerësimin e produktit të përbërë TIK.

Neni 8

Nivelet e sigurisë së skemës së certifikimit të sigurisë kibernetike

1. Skema e certifikimit të sigurisë kibernetike specifikon një ose më shumë nga nivelet e sigurisë për produktet, shërbimet dhe proceset TIK, "bazë", "i konsiderueshëm" ose "i lartë". Niveli i sigurisë është në proporcion me nivelin e rrezikut, që lidhet me përdorimin e synuar të produktit, shërbimit dhe procesit TIK, për sa i përket probabilitetit e ndikimit të një incidenti të sigurisë kibernetike.

2. Certifikata e sigurisë kibernetike i referohet çdo niveli sigurie të specifikuar në skemën e certifikimit të sigurisë kibernetike, sipas së cilës lëshohet certifikata e sigurisë kibernetike.

3. Kërkesat e sigurisë, që korrespondojnë me çdo nivel sigurie, përcaktohen në skemën e certifikimit të sigurisë kibernetike, duke përfshirë funksionet përkatëse të sigurisë, ashpërsinë dhe thellësinë përkatëse të vlerësimit që do t'i nënshtrohet produkti, shërbimi ose procesi TIK.

4. Certifikata u referohet specifikimeve teknike, standardeve dhe procedurave, që lidhen me to, duke përfshirë kontrollet teknike, qëllimi i të cilave është të ulin rrezikun ose të parandalojnë incidentet e sigurisë kibernetike.

5. Një certifikatë e sigurisë kibernetike ose deklaratë konformiteti, që i referohet nivelit të sigurisë "bazë", garanton siguri se produktet, shërbimet dhe proceset TIK, për të cilat është lëshuar certifikata ose deklarata e konformitetit, plotësojnë kërkesat përkatëse të sigurisë, duke përfshirë funksionet e sigurisë, si dhe vlerësimin e nivelit, që synon të minimizojë rreziqet e njohura bazë të incidenteve dhe të sulmeve kibernetike. Aktivitetet e vlerësimit, që ndërmerren, përfshijnë të paktën një rishikim të dokumentacionit teknik. Kur një rishikim i tillë nuk është i përshtatshëm, ndërmerren aktivitete vlerësimi zëvendësuese me efekt të njëjtë.

6. Një certifikatë e sigurisë kibernetike, që i referohet nivelit të sigurisë "të konsiderueshme", garanton siguri se produktet, shërbimet dhe proceset TIK, për të cilat është lëshuar certifikata, plotësojnë kërkesat përkatëse të sigurisë, duke përfshirë funksionet e sigurisë, si dhe vlerësimin e një niveli që synon të minimizojë rreziqet e njohura të sigurisë kibernetike dhe rrezikun e incidenteve dhe sulmeve kibernetike të kryera nga aktorë me aftësi dhe burime të kufizuara. Aktivitetet e vlerësimit, që ndërmerren, përfshijnë të paktën një rishikim për të demonstruar mungesën e dobësive të njohura publikisht dhe testim për të demonstruar se produktet, shërbimet ose proceset TIK zbatojnë saktë funksionalitetet e nevojshme të sigurisë dhe, kur aktiviteti i vlerësimit nuk është i përshtatshëm, ndërmerren aktivitete vlerësimi zëvendësuese me efekt të njëjtë.

7. Një certifikatë e sigurisë kibernetike, që i referohet nivelit të sigurisë "të lartë", garanton sigurinë se produktet, shërbimet dhe proceset TIK, për të cilat është lëshuar certifikata, plotësojnë kërkesat përkatëse të sigurisë, duke përfshirë funksionet e sigurisë, si dhe vlerësimin e një niveli, që synon të minimizojë rrezikun e sulmeve kibernetike moderne të kryera nga aktorë me aftësi dhe burime të konsiderueshme. Aktivitetet e vlerësimit që ndërmerren duhet të përfshijnë të paktën një rishikim për të demonstruar mungesën e dobësive të njohura publikisht, testim për të demonstruar se produktet e TIK, shërbimet ose proceset TIK zbatojnë saktë funksionalitetet e nevojshme të sigurisë në gjendjen e teknologjisë, si dhe një vlerësim të rezistencës së tyre ndaj sulmuesve, duke përdorur testimin e depërtimit dhe kur një aktivitet i tillë vlerësimi nuk është i përshtatshëm, ndërmerren aktivitete vlerësimi zëvendësuese me efekt të njëjtë.

8. Një skemë e certifikimit të sigurisë kibernetike mund të specifikojë disa nivele vlerësimi, në varësi të ashpërsisë dhe të thellësisë së metodologjisë së vlerësimit të përdorur. Secili prej niveleve të vlerësimit korrespondon me një nga nivelet e sigurisë dhe përcaktohet nga një kombinim i përshtatshëm i komponentëve të sigurisë.

Seksioni 2
Lëshimi, rinovimi dhe tërheqja e certifikatave

Neni 9

Informacion i nevojshëm për certifikim dhe vlerësim

1. Një aplikant për certifikim sipas skemës siguron ose vë në dispozicion të organit certifikues dhe ITSEF-it informacionin e nevojshëm për aktivitetet e certifikimit e të vlerësimit.

2. Informacioni i përmendur në pikën 1 të këtij neni përfshin të gjitha provat përkatëse, në përputhje me elementet e veprimit të zhvilluesit në formatin e duhur, sipas përcaktimeve te përmbajtja dhe prezantimi i elementit të provës të kritereve të përbashkëta dhe tek metodologjia e vlerësimit për nivelin e përzgjedhur të sigurisë dhe kërkesat e lidhura me garantimin e sigurisë. Prova përfshin, kur është e nevojshme, detaje mbi produktin TIK dhe kodin, burim të tij, sipas përcaktimeve të këtij vendimi, duke iu nënshtruar masave mbrojtëse kundër zbulimit të paautorizuar.

3. Aplikantët për certifikim mund t'u ofrojnë organeve të certifikimit dhe ITSEF-it rezultatet e duhura të vlerësimit nga certifikimi i mëparshëm në përputhje me:

a) përcaktimet e këtij vendimi;

b) një skemë evropiane të certifikimit të sigurisë kibernetike.

4. Kur rezultatet e vlerësimit janë të lidhura me detyrat e tij, ITSEF-i mund të ripërdorë rezultatet e vlerësimit, me kusht që këto rezultate të jenë në përputhje me kërkesat e zbatueshme dhe të konfirmohet vërtetësia e tyre.

5. Kur organi certifikues lejon që produkti t'i nënshtrohet një certifikimi të produktit të përbërë, aplikanti për certifikim i vendos në dispozicion organit certifikues dhe ITSEF-it të gjitha elementet e nevojshme, sipas rastit, në përputhje me dokumentet teknike më të fundit.

6. Aplikantët për certifikim, gjithashtu, i vendosin në dispozicion organit certifikues dhe ITSEF-it informacionin e mëposhtëm:

a) Lidhjen në faqen e tyre të internetit, që përmban informacionin shtesë të sigurisë kibernetike, sipas përcaktimeve në nenin 10 të këtij vendimi;

b) Një përshkrim të procedurave për menaxhimin e zbulimin e vulnerabiliteteve të aplikantit.

7. Dokumentacioni përkatës i përmendur në këtë nen ruhet nga organi certifikues, ITSEF-i dhe aplikanti për një periudhë 5-vjeçare pas skadimit të certifikatës.

Neni 10

Informacione plotësuese të sigurisë kibernetike për produktet, shërbimet dhe proceset TIK të certifikuara

1. Prodhuesi ose ofruesi i produkteve, i shërbimeve ose i proceseve TIK të certifikuara ose i produkteve, i shërbimeve dhe i proceseve TIK, për të cilat është lëshuar një deklaratë konformiteti, e bën të disponueshëm publikisht informacionin shtesë të sigurisë kibernetike, si më poshtë vijon:

a) Udhëzime dhe rekomandime për të ndihmuar përdoruesit fundorë me konfigurimin, instalimin, vendosjen, funksionimin dhe mirëmbajtjen e sigurt të produkteve ose të shërbimeve TIK;

b) Periudhën, gjatë së cilës mbështetja e sigurisë u ofrohet përdoruesve fundorë, veçanërisht në lidhje me disponueshmërinë e përditësimeve të lidhura me sigurinë kibernetike;

c) Informacionin e kontaktit të prodhuesit ose të ofruesit dhe metodat e pranuara për marrjen e informacionit për vulnerabilitetin nga përdoruesit fundorë dhe kërkuesit në fushën e sigurisë;

ç) Një referencë për listën e dobësive të publikuara *on-line*, në lidhje me produktin, shërbimin ose procesin TIK, si dhe çdo kështillë përkatëse për sigurinë kibernetike.

2. Informacioni i përmendur në pikën 1 të këtij neni duhet të jetë i disponueshëm në formë elektronike, si dhe të mbetet i disponueshëm dhe i përditësuar sipas nevojës, të paktën, deri në skadimin e certifikatës përkatëse të sigurisë kibernetike ose të deklaratës së konformitetit.

Neni 11
Kushtet për lëshimin e një certifikate

1. Organet certifikuese lëshojnë një certifikatë sipas skemës kur plotësohen të gjitha kushtet, si më poshtë vijon:

a) Kategoria e produktit TIK është brenda fushës së akreditimit dhe, aty ku është e zbatueshme, të autorizimit, të organit certifikues dhe ITSEF-it të përfshirë në certifikim;

b) Aplikanti për certifikim ka nënshkruar një deklaratë, që merr përsipër të gjitha angazhimet e renditura në pikën 2 të këtij neni;

c) ITSEF-i ka përfunduar vlerësimin pa kundërshtime, në përputhje me standardet, kriteret dhe metodat e vlerësimit të përmendura në nenet 3 dhe 7 të këtij vendimi;

ç) Organi certifikues ka përfunduar rishikimin e rezultateve të vlerësimit pa kundërshtime;

d) Organi certifikues ka verifikuar që raportet teknike të vlerësimit të ofruara nga ITSEF-i janë në përputhje me provat e ofruara dhe se standardet, kriteret e metodat e vlerësimit të përmendura në nenet 3 dhe 7 të këtij vendimi janë zbatuar saktë.

2. Aplikanti për certifikim merr përsipër:

a) t'i sigurojë organit certifikues dhe ITSEF-it të gjithë informacionin e nevojshëm, të plotë e të saktë, dhe të sigurojë informacion shtesë të nevojshëm, në qoftë se kërkohet;

b) të mos promovojë produktin TIK si të certifikuar sipas skemës përpara se të lëshohet certifikata;

c) të promovojë produktin TIK si të certifikuar vetëm në lidhje me qëllimin e përcaktuar në certifikatën e lëshuar;

ç) të ndërpresë menjëherë promovimin e produktit TIK si të certifikuar në rast të pezullimit, tërheqjes ose skadimit të certifikatës;

d) të sigurojë që produktet TIK të shitura, duke iu referuar certifikatës, janë rreptësisht identike me produktin TIK, që i nënshtrohet certifikimit;

dh) të respektojë rregullat e përdorimit të markës dhe etiketës të përcaktuara për certifikatën, në përputhje me nenin 13 të këtij vendimi.

3. Në rastin e një produkti TIK, që i nënshtrohet një certifikimi produkti të përbërë, në përputhje me dokumentet teknike më të fundit, organi certifikues që ka kryer certifikimin e produktit themelor TIK ndan informacionin përkatës me organin certifikues, që kryen certifikimin e produktit të përbërë TIK.

Neni 12
Përmbajtja dhe formati i një certifikate

1. Një certifikatë përfshin informacionin përkatës, sipas përcaktimeve në aneksin VII të këtij vendimi.

2. Objekti dhe kufijtë e produktit të certifikuar TIK specifikohen në certifikatën ose në raportin e certifikimit, duke treguar nëse i gjithë produkti TIK është certifikuar ose vetëm pjesë të tij.

3. Organi certifikues i siguron aplikantit certifikatën, të paktën, në formë elektronike.

4. Organi certifikues harton një raport certifikimi, sipas përcaktimeve në aneksin V të këtij vendimi për çdo certifikatë që lëshon. Raporti i certifikimit bazohet në raportin teknik të vlerësimit të lëshuar nga ITSEF-i. Raporti teknik i vlerësimit dhe raporti i certifikimit duhet të tregojnë kriteret dhe metodat specifike të vlerësimit të përmendura në nenin 7 të këtij vendimi të përdorura për vlerësimin.

5. Organi certifikues i siguron organit kombëtar të certifikimit të sigurisë kibernetike, si dhe me anëtarësimin e Republikës së Shqipërisë në Bashkimin Evropian, ENISA-s, çdo certifikatë dhe çdo raport certifikimi në formë elektronike.

Neni 13
Marka dhe etiketa

1. Zotëruesi i një certifikate mund të vendosë një markë dhe etiketë në një produkt të certifikuar TIK. Marka dhe etiketa tregojnë se produkti TIK është certifikuar në përputhje me këtë vendim. Marka dhe etiketa vendosen sipas përcaktimeve të këtij neni dhe aneksit IX të këtij vendimi.

2. Marka dhe etiketa vendosen në mënyrë të dukshme, të lexueshme dhe të pandryshueshme në produktin e certifikuar TIK ose në tabelën e të dhënave të tij. Kur nuk është e mundur ose nuk garantohet për shkak të natyrës së produktit, marka duhet të vendoset në paketim dhe në dokumentet shoqëruese. Kur produkti i certifikuar TIK dorëzohet në formën e *software*-it, marka dhe etiketa shfaqen në mënyrë të dukshme, të lexueshme dhe të pandryshueshme në dokumentacionin shoqërues ose dokumentacioni bëhet lehtësisht dhe drejtpërdrejt i aksesueshëm për përdoruesit në faqen e internetit.

3. Marka dhe etiketa vendosen sipas përcaktimeve në aneksin IX të këtij vendimi dhe përmbajnë:

a) nivelin e sigurisë dhe nivelin AVA_VAN të produktit të certifikuar TIK;

b) identifikimin unik të certifikatës, që përbëhet nga:

i. emri i skemës;

ii. emri dhe numri i referencës së akreditimit të organit certifikues, që ka lëshuar certifikatën;

iii. viti dhe muaji i lëshimit;

iv. numri i identifikimit të caktuar nga organi certifikues që ka lëshuar certifikatën.

4. Marka dhe etiketa shoqërohen nga një kod QR me një lidhje në një faqe interneti, që përmban të paktën:

a) informacion mbi vlefshmërinë e certifikatës;

b) informacionin e nevojshëm të certifikimit, sipas përcaktimeve në anekset V dhe VII të këtij vendimi;

c) informacionin që bëhet publikisht i disponueshëm nga zotëruesi i certifikatës, sipas përcaktimeve në nenin 10 të këtij vendimi;

ç) kur është e aplikueshme, informacionin historik në lidhje me certifikimin ose certifikimet specifike të produktit TIK, për të mundësuar gjurmueshmërinë.

Neni 14
Periudha e vlefshmërisë së një certifikate

1. Organi certifikues cakton një periudhë vlefshmërie për çdo certifikatë të lëshuar, duke marrë në konsideratë karakteristikat e produktit të certifikuar TIK.

2. Periudha e vlefshmërisë së certifikatës është jo më shumë se 5 (pesë) vjet.

3. Me përjashtim të pikës 2 të këtij neni, kjo periudhë mund t'i kalojë 5 vjet, me kusht që të miratohet paraprakisht nga organi kombëtar i certifikimit të sigurisë kibernetike. Me anëtarësimin e Republikës së Shqipërisë në Bashkimin Evropian, organi kombëtar i certifikimit të sigurisë kibernetike njofton menjëherë Grupin Evropian të Certifikimit të Sigurisë Kibernetike.

Neni 15
Rishikimi i një certifikate

1. Me kërkesë të zotëruesit të certifikatës ose për arsye të justifikuara, organi certifikues mund të vendosë të rishikojë certifikatën për një produkt TIK. Rishikimi kryhet sipas përcaktimeve në aneksin IV të këtij vendimi. Organi certifikues përcakton masën e rishikimit, si dhe, kur është e nevojshme për rishikimin, organi certifikues i kërkon ITSEF-it të kryejë një rivlerësim të produktit TIK të certifikuar.

2. Pas rezultateve të rishikimit dhe sipas rastit të rivlerësimit, organi certifikues duhet:

a) të konfirmojë certifikatën;

b) të tërheqë certifikatën, sipas përcaktimeve në nenin 16 të këtij vendimi;

c) të tërheqë certifikatën, sipas përcaktimeve në nenin 16 të këtij vendimi, si dhe të lëshojë një certifikatë të re me fushë identike dhe një periudhë vlefshmërie të zgjatur;

ç) të tërheqë certifikatën, sipas përcaktimeve në nenin 16 të këtij vendimi, dhe të lëshojë një certifikatë të re me një fushë të ndryshme.

3. Organi certifikues mund të vendosë të pezullojë menjëherë certifikatën, në përputhje me nenin 32 të këtij vendimi, deri në ndërmarrjen e veprimeve korrigjuese nga zotëruesi i certifikatës.

Neni 16
Tërheqja e një certifikate

1. Organi certifikues që ka lëshuar certifikatën e tërheq atë, kur certifikata nuk përputhet me kërkesat e përcaktuara në nenet 11, 12, 15 dhe 31, pika 3, të këtij vendimi.

2. Organi certifikues i përmendur në pikën 1 të këtij neni njofton organin kombëtar të certifikimit të sigurisë kibernetike për tërheqjen e certifikatës, si dhe, me anëtarësimin e Republikës së Shqipërisë në Bashkimin Evropian, njofton edhe ENISA-n. Organi kombëtar i certifikimit të sigurisë kibernetike njofton autoritetin e mbikëqyrjes së tregut.

3. Zotëruesi i një certifikate mund të kërkojë tërheqjen e certifikatës.

KREU III
CERTIFIKIMI I PROFILEVE TË MBROJTJES

SEKSIONI 1
STANDARDET DHE KËRKESAT SPECIFIKE PËR VLERËSIMIN

Neni 17
Kriteret dhe metodat e vlerësimit

1. Një profil i mbrojtjes vlerësohet, minimalisht, në përputhje me:

a) elementet e zbatueshme të standardeve të përmendura në nenin 3 të këtij vendimi;

b) nivelin e rrezikut, që lidhet me qëllimin e përdorimit të produkteve TIK, sipas përcaktimeve në nenin 8 të këtij vendimi dhe nenin 40 të ligjit nr.25/2024, "Për sigurinë kibernetike";

c) dokumentet teknike më të fundit, sipas përcaktimeve në aneksin I të këtij vendimi. Një profil i mbrojtjes i mbuluar nga një fushë teknike certifikohet kundrejt kërkesave të përcaktuara në atë fushë teknike.

2. Në raste veçanta e të justifikuara, një organ i vlerësimit të konformitetit mund të certifikojë një profil të mbrojtjes pa aplikuar dokumentet teknike më të fundit. Në raste të tilla, organi certifikues informon organin kombëtar të certifikimit të sigurisë kibernetike dhe paraqet një justifikim për certifikimin e synuar pa aplikimin e dokumenteve teknike më të fundit, si dhe metodologjinë e propozuar të vlerësimit. Organi kombëtar i certifikimit të sigurisë kibernetike vlerëson justifikimin dhe, kur pranohet, miraton moszbatimin e dokumenteve teknike më të fundit, si dhe miraton ose ndryshon, sipas rastit, metodologjinë e vlerësimit për t'u zbatuar nga organi i vlerësimit të konformitetit. Deri në zbardhjen e vendimit të organit kombëtar të certifikimit të sigurisë kibernetike, organi i vlerësimit të konformitetit nuk lëshon certifikatë për profilin e mbrojtjes. Me anëtarësimin e Republikës së Shqipërisë në Bashkimin Evropian, organi kombëtar i certifikimit të sigurisë kibernetike ia njofton menjëherë autorizimin për moszbatimin e dokumenteve teknike më të fundit Grupit Evropian të Certifikimit të Sigurisë Kibernetike, i cili mund të dalë me një opinion. Organi kombëtar i certifikimit të sigurisë kibernetike merr në konsideratë opinionin e Grupit Evropian të Certifikimit të Sigurisë Kibernetike.

SEKSIONI 2
LËSHIMI, RINOVIMI DHE TËRHEQJA E CERTIFIKATAVE PËR PROFILET E MBROJTJES

Neni 18
Informacion i nevojshëm për certifikimin dhe vlerësimin e profileve të mbrojtjes

Një aplikant, për certifikimin e një profili të mbrojtjes, siguron ose vendos në dispozicion të organit certifikues dhe ITSEF-it informacionin e nevojshëm për aktivitetet e certifikimit dhe vlerësimit. Pikat 2, 3, 4 e 7, të nenit 9, të këtij vendimi, zbatohen për aq sa është e mundur.

Neni 19
Lëshimi i certifikatave për profilet e mbrojtjes

1. Për lëshimin e certifikatave për profilet e mbrojtjes zbatohen, për aq sa është e mundur, përcaktimet në nenet 11 e 12 të këtij vendimi.

2. ITSEF-i vlerëson nëse një profil i mbrojtjes është i plotë, konsistent, teknikisht i saktë dhe efektiv për përdorimin e synuar dhe objektivat e sigurisë të kategorisë së produktit TIK të mbuluar nga ai profil i mbrojtjes.

3. Një profil i mbrojtjes certifikohet vetëm nga:

a) një autoritet kombëtar certifikues i sigurisë kibernetike;

b) një organ certifikues, pas miratimit paraprak nga organi kombëtar i certifikimit të sigurisë kibernetike për çdo profil të mbrojtjes individuale.

Neni 20

Periudha e vlefshmërisë së një certifikate për profilet e mbrojtjes

1. Organi certifikues cakton një periudhë vlefshmërie për çdo certifikatë.

2. Periudha e vlefshmërisë mund të jetë deri në jetëgjatësinë e profilit të mbrojtjes.

Neni 21

Rishikimi i një certifikate për profilet e mbrojtjes

1. Me kërkesë të zotëruesit të certifikatës ose kur është i justifikuar, organi certifikues mund të vendosë të rishikojë një certifikatë për një profil të mbrojtjes. Rishikimi kryhet duke zbatuar kushtet e përcaktuara në nenin 17 të këtij vendimi. Organi certifikues përcakton kohëzgjatjen e rishikimit dhe, kur është e nevojshme, për rishikimin, organi certifikues i kërkon ITSEF-it të kryejë një rivlerësim të profilit të mbrojtjes së certifikuar.

2. Pas rezultateve të rishikimit dhe sipas rastit të rivlerësimit, organi certifikues:

a) konfirmon certifikatën;

b) tërheq certifikatën, në përputhje me nenin 22 të këtij vendimi;

c) tërheq certifikatën, në përputhje me nenin 22 të këtij vendimi, dhe lëshon një certifikatë të re me një fushë identike dhe një periudhë vlefshmërie të zgjatur;

ç) tërheq certifikatën, në përputhje me nenin 22 të këtij vendimi, dhe lëshon një certifikatë të re me një fushë të ndryshme.

Neni 22

Tërheqja e një certifikate për një profil të mbrojtjes

1. Organi certifikues, që ka lëshuar certifikatën, e tërheq atë, kur certifikata nuk përputhet me dispozitat e këtij vendimi. Përcaktimet e nenit 16 të këtij vendimi zbatohen, për aq sa është e mundur, për tërheqjen e një certifikate për një profil të mbrojtjes.

2. Një certifikatë për një profil të mbrojtjes e lëshuar sipas përcaktimeve të shkronjës "b", të pikës 4, të nenit 19, të këtij vendimi, tërhiqet nga organi kombëtar i certifikimit të sigurisë kibernetike, që e ka miratuar atë certifikatë.

Neni 23

Specifikimi i kërkesave për akreditimin e organeve të vlerësimit të konformitetit

Akreditimi i organeve të vlerësimit të konformitetit merr në konsideratë specifikimin e kërkesave për akreditimin e organeve certifikuese dhe ITSEF-ve, siç përcaktohet në dokumentet teknike më të fundit përkatëse të listuara në pikën 2, të aneksit I, të këtij vendimi.

KREU IV

ORGANET E VLERËSIMIT TË KONFORMITETIT

Neni 24

Kërkesa shtesë ose specifike për një organ certifikues dhe njohja e vlerësimeve dhe e raporteve të tyre

1. Një organ certifikues autorizohet nga organi kombëtar i certifikimit të sigurisë kibernetike për të lëshuar certifikata në nivelin e sigurisë "të lartë", kur ky organ është i akredituar nga institucioni përgjegjës për akreditimin në Republikën e Shqipërisë, sipas legjislacionit në fuqi për akreditimin, dhe përmbush kërkesat, si më poshtë vijon:

a) Ka ekspertizën dhe kompetencat e duhura për nxjerrjen e vendimit të certifikimit në nivelin e sigurisë "të lartë";

b) Kryen aktivitetet e certifikimit në bashkëpunim me një ITSEF të autorizuar në përputhje me nenin 25 të këtij vendimi;

c) Ka kompetencat e nevojshme dhe vendos masat e duhura teknike dhe operacionale për të mbrojtur në mënyrë efektive informacionin konfidencial dhe sensitiv për nivelin e sigurisë "të lartë", përveç kërkesave të përcaktuara në nenin 44 të këtij vendimi.

2. Organi kombëtar i certifikimit të sigurisë kibernetike vlerëson nëse organi certifikues

përmbush të gjitha kërkesat e përcaktuara në pikën 1 të këtij neni. Vlerësimi përfshin të paktën intervista të strukturuara dhe një rishikim i të paktën një certifikimi pilot të kryer nga organi certifikues sipas përcaktimeve të këtij vendimi. Në vlerësim, organi kombëtar i certifikimit të sigurisë kibernetike mund të ripërdorë çdo dëshmi të përshtatshme nga autorizimi paraprak ose aktivitete të ngjashme sipas përcaktimeve në:

a) këtë vendim;

b) një skemë evropiane të certifikimit të sigurisë kibernetike.

3. Organi kombëtar i certifikimit të sigurisë kibernetike harton një raport autorizimi në përputhje me procedurat për monitorimin, autorizimin dhe mbikëqyrjen e veprimtarive të organeve të vlerësimit të konformitetit.

4. Organi kombëtar i certifikimit të sigurisë kibernetike specifikon kategoritë e produkteve TIK dhe profilet e mbrojtjes në të cilat shtrihet autorizimi. Autorizimi është i vlefshëm për një periudhë jo më të gjatë se vlefshmëria e akreditimit. Autorizimi mund të rinovohet me kërkesë me kusht që organi certifikues të plotësojë kërkesat sipas përcaktimeve të këtij neni. Për rinovimin e autorizimit nuk kërkohen vlerësime pilot.

5. Organi kombëtar i certifikimit të sigurisë kibernetike tërheq autorizimin e organit të certifikimit kur nuk i plotëson kushtet sipas përcaktimeve të këtij neni. Me tërheqjen e autorizimit, organi certifikues pushon menjëherë ushtrimin e veprimtarisë si një organ certifikues i autorizuar.

6. Vlerësimet e kryera, raportet e certifikimit dhe certifikatat e lëshuara nga organe certifikuese të akredituara dhe të autorizuara në një shtet të Bashkimit Evropian kanë të njëjtën vlefshmëri si vlerësimet e kryera, raportet e certifikimit dhe certifikatat e lëshuara nga organe certifikuese të akredituara dhe të autorizuara në Republikën e Shqipërisë.

Neni 25

Kërkesa shtesë ose specifike për një ITSEF dhe njohja e vlerësimeve dhe e raporteve të tyre

1. Një ITSEF autorizohet nga organi kombëtar i certifikimit të sigurisë kibernetike për të kryer vlerësimin e produkteve TIK, që i nënshtrohen certifikimit në nivelin e sigurisë "të lartë", ku ITSEF-i është organ i akredituar nga institucioni përgjegjës për akreditimin në Republikën e Shqipërisë, sipas legjislacionit në fuqi për akreditimin, i cili përmbush kërkesat, si më poshtë vijon:

a) Ka ekspertizën e nevojshme për kryerjen e aktiviteteve të vlerësimit për të përcaktuar rezistencën ndaj sulmeve kibernetike të sofistikuara të kryera nga aktorë me aftësi dhe burime të konsiderueshme;

b) Për fushat teknike dhe profilet e mbrojtjes, që janë pjesë e procesit TIK dhe për produktet TIK, ka:

i. ekspertizën për të kryer aktivitetet specifike të vlerësimit për të përcaktuar në mënyrë metodike një objektiv të rezistencës së vlerësimit kundër sulmuesve të aftë në mjedisin e tij operacional, duke supozuar një potencial sulmi "të moderuar" ose "të lartë", sipas përcaktimeve në standardet e përmendura në nenin 3 të këtij vendimi;

ii. kompetencat e duhura teknike, sipas specifikimeve në dokumentet teknike më të fundit, sipas përcaktimeve në aneksin I të këtij vendimi.

c) kompetencat e duhura dhe vendos masat e duhura teknike dhe operacionale për të mbrojtur në mënyrë efektive informacionin konfidencial e sensitiv për nivelin e sigurisë "të lartë", përveç kërkesave të përcaktuara në nenin 44 të këtij vendimi.

2. Organi kombëtar i certifikimit të sigurisë kibernetike vlerëson nëse një ITSEF përmbush të gjitha kërkesat e përcaktuara në pikën 1 të këtij neni. Ky vlerësim përfshin të paktën intervista të strukturuara dhe një rishikim të të paktën një vlerësimi pilot të kryer nga ITSEF-i, në përputhje me këtë vendim.

3. Në vlerësim, organi kombëtar i certifikimit të sigurisë kibernetike mund të ripërdorë çdo dëshmi të përshtatshme nga autorizimi paraprak ose aktivitete të ngjashme, sipas përcaktimeve në:

a) këtë vendim;

b) një skemë evropiane të certifikimit të sigurisë kibernetike.

4. Organi kombëtar i certifikimit të sigurisë kibernetike harton një raport autorizimi, në përputhje me procedurat për monitorimin,

autorizimin dhe mbikëqyrjen e veprimtarive të organeve të vlerësimit të konformitetit.

5. Organi kombëtar i certifikimit të sigurisë kibernetike specifikon kategoritë e produkteve TIK dhe profilet e mbrojtjes, në të cilat shtrihet autorizimi. Autorizimi është i vlefshëm për një periudhë jo më të gjatë se vlefshmëria e akreditimit. Autorizimi mund të rinovohet me kërkesë, me kusht që ITSEF-i të plotësojë kërkesat, sipas përcaktimeve të këtij neni. Për rinovimin e autorizimit nuk kërkohen vlerësime pilot.

6. Organi kombëtar i certifikimit të sigurisë kibernetike tërheq autorizimin e ITSEF-it, kur nuk plotëson kushtet sipas përcaktimeve të këtij neni. Pas tërheqjes së autorizimit, ITSEF-i pushon menjëherë së ushtruari veprimtarinë si një ITSEF i autorizuar.

7. Vlerësimet e kryera dhe raportet teknike të lëshuara nga ITSEF-e të akredituara dhe të autorizuara në një shtet të Bashkimit Evropian kanë të njëjtën vlefshmëri si vlerësimet e kryera dhe raportet teknike të lëshuara nga ITSEF-e të akredituara e të autorizuara në Republikën e Shqipërisë.

KREU V
MONITORIMI, MOSKONFORMITETI DHE MOSPAJTUESHMËRIA

SEKSIONI 1
MONITORIMI I PAJTUESHMËRISË

Neni 26
Organi kombëtar i certifikimit të sigurisë kibernetike

1. Në Republikën e Shqipërisë, Autoriteti Kombëtar për Sigurinë Kibernetike ushtron kompetencat e organit kombëtar të certifikimit të sigurisë kibernetike.

2. Organi kombëtar i certifikimit të sigurisë kibernetike është i pavarur nga subjektet që mbikëqyr, si nga organizimi, ana financiare, struktura ligjore dhe vendimmarrja.

3. Organi kombëtar i certifikimit të sigurisë kibernetike ka burime të mjaftueshme për të ushtruar kompetencat, si dhe për të kryer detyrat e tij në mënyrë efektive.

4. Organi kombëtar i certifikimit të sigurisë kibernetike ushtron kompetencat e mëposhtme:

a) Mbikëqyr dhe zbaton rregullat e përcaktuara në këtë vendim për monitorimin e pajtueshmërisë së produkteve, shërbimeve dhe proceseve TIK me kërkesat e certifikatave të sigurisë kibernetike që janë lëshuar;

b) Monitoron pajtueshmërinë dhe detyrimet e prodhuesve ose të ofruesve të produkteve, shërbimeve ose proceseve TIK;

c) Mbështet institucionin përgjegjës për akreditimin në monitorimin dhe mbikëqyrjen e aktiviteteve të organeve të vlerësimit të konformitetit, për qëllimet e këtij vendimi;

ç) Monitoron dhe mbikëqyr aktivitetet, sipas përcaktimeve të këtij neni, si dhe organet e vlerësimit të konformitetit të akreditura nga institucioni përgjegjës për akreditimin;

d) Kur është e zbatueshme, kufizon, pezullon ose tërheq autorizimin ekzistues kur organet e vlerësimit të konformitetit shkelin kërkesat e këtij vendimi;

dh) Trajton ankesat nga persona fizikë ose juridikë lidhur me certifikatat e sigurisë kibernetike të lëshuara nga organet e vlerësimit të konformitetit, si dhe trajton çështjen e ankesave të tilla dhe informon ankuesin për ecurinë dhe rezultatin e verifikimit brenda një periudhe të arsyeshme;

e) Siguron një raport përmbledhës vjetor për aktivitetet e kryera sipas këtij neni;

ë) Bashkëpunon me autoritete të tjera publike, duke përfshirë shkëmbimin e informacionit mbi mospërputhjen e mundshme të produkteve, shërbimeve dhe proceseve TIK me kërkesat e këtij vendimi;

f) Monitoron zhvillimet përkatëse në fushën e certifikimit të sigurisë kibernetike.

Neni 27
Monitorimi i aktiviteteve nga organi kombëtar i certifikimit të sigurisë kibernetike

1. Pa rënë ndesh me nenin 26 të këtij vendimi, organi kombëtar i certifikimit të sigurisë kibernetike monitoron pajtueshmërinë:

a) e organit certifikues dhe ITSEF -it me detyrimet sipas përcaktimeve të këtij vendimi;

b) e zotëruesit të një certifikate me detyrimet sipas përcaktimeve të këtij vendimi;

c) e produkteve të certifikuara TIK me

kërkesat e përcaktuara në këtë vendim;

ç) e sigurisë së shprehur në certifikatë, që trajton kërcënimet në zhvillim.

2. Organi kombëtar i certifikimit të sigurisë kibernetike kryen aktivitetet e tij të monitorimit, në veçanti, bazuar në:

a) informacionin që vjen nga organet e certifikimit, autoriteti përgjegjës për akreditimin dhe autoriteti përgjegjës për mbikëqyrjen e tregut;

b) informacionin që rezulton nga auditimet dhe verifikimet e tij ose të një autoriteti tjetër;

c) marrjen e kampioneve, në përputhje me përcaktimet e pikës 3 të këtij neni;

ç) ankesat e marra.

3. Organi kombëtar i certifikimit të sigurisë kibernetike, në bashkëpunim me autoritetin përgjegjës për mbikëqyrjen e tregut, merr kampionet për çdo vit, të paktën 4% të certifikatave, sipas përcaktimeve nga një vlerësim rreziku i kryer nga organi kombëtar i certifikimit të sigurisë kibernetike. Me kërkesë dhe duke bashkëpunuar me organin kombëtar të certifikimit të sigurisë kibernetike, organi certifikues dhe, nëse është e nevojshme, ITSEF-i, asistojnë autoritetin në monitorimin e pajtueshmërisë.

4. Organi kombëtar i certifikimit të sigurisë kibernetike zgjedh kampionin e produkteve të certifikuara të TIK-ut, që do të kontrollohen, bazuar në kriteret e mëposhtme:

a) Kategorinë e produktit;

b) Nivelet e garancisë së produkteve;

c) Zotëruesit e një certifikate;

ç) Organin certifikues dhe, sipas rastit, ITSEF-in e nënkontraktuar;

d) Merr në konsideratë çdo informacion tjetër.

5. Organi kombëtar i certifikimit të sigurisë kibernetike informon zotëruesit e certifikatës për produktet e përzgjedhura TIK, si dhe për kriteret e përzgjedhjes.

6. Organi certifikues, i cili ka certifikuar kampionin e produktit TIK, me kërkesë të organit kombëtar të certifikimit të sigurisë kibernetike dhe me ndihmën e ITSEF-it përkatës, kryen rishikime në përputhje me procedurën e përcaktuar në seksionin 2, të aneksit IV, të këtij vendimi, dhe informon për rezultatet organin kombëtar të certifikimit të sigurisë kibernetike.

7. Kur organi kombëtar i certifikimit të sigurisë kibernetike ka arsye të mjaftueshme për të besuar se një produkt i certifikuar TIK nuk është më në përputhje me këtë vendim, ai mund të kryejë verifikime ose të përdorë çdo kompetencë tjetër monitorimi të përcaktuar në nenin 26 të këtij vendimi.

8. Organi kombëtar i certifikimit të sigurisë kibernetike informon, në vijim, organin certifikues dhe ITSEF-in përkatës lidhur me verifikimet e me produktet e përzgjedhura TIK.

9. Kur organi kombëtar i certifikimit të sigurisë kibernetike identifikon se një verifikim në vazhdim lidhet me produkte TIK, që janë të certifikuara nga organet certifikuese të vendosura në shtetet anëtare të Bashkimit Evropian, ai informon autoritetet kombëtare të certifikimit të sigurisë kibernetike të atij shteti, në mënyrë që të bashkëpunojnë në verifikime, aty ku është e rëndësishme. Me anëtarësimin e Republikës së Shqipërisë në Bashkimin Evropian, organi kombëtar i certifikimit të sigurisë kibernetike njofton gjithashtu Grupin Evropian të Certifikimit të Sigurisë Kibernetike për hetimet ndërkufitare dhe rezultatet pasuese.

Neni 28

Monitorimi i aktiviteteve nga organi certifikues

1. Organi certifikues monitoron:

a) pajtueshmërinë e zotëruesit të një certifikate me detyrimet e tyre, sipas përcaktimeve të këtij vendimi, ndaj certifikatës që është lëshuar nga organi certifikues;

b) pajtueshmërinë e produkteve TIK, të cilat janë certifikuar me kërkesat e tyre përkatëse të sigurisë;

c) sigurinë e shprehur në profilet e certifikuara të mbrojtjes.

2. Organi certifikues ndërmerr aktivitete monitorimi në bazë të:

a) informacionit të dhënë, të angazhimeve të aplikantit për certifikim, të përmendur në pikën 2, të nenit 11, të këtij vendimi;

b) informacionit, që rezulton nga aktivitetet e autoritetit përgjegjës të mbikëqyrjes së tregut;

c) ankesave të marra;

ç) informacionit për vulnerabilitetet, që ndikon në produktet TIK, të cilat janë të certifikuara.

3. Organi kombëtar i certifikimit të sigurisë

kibernetike mund të hartojë protokoll komunikimi për shkëmbim informacioni ndërmjet organeve të certifikimit dhe zotëruesve të certifikatave për të verifikuar e raportuar për pajtueshmërinë me angazhimet e marra, në përputhje me pikën 2, të nenit 11, të këtij vendimi, pa anashkaluar aktivitetet që lidhen me autoritetin përgjegjës për mbikëqyrjen e tregut.

Neni 29
Monitorimi i aktiviteteve nga zotëruesi i certifikatës

1. Zotëruesi i një certifikate, për të monitoruar konformitetin e produktit të certifikuar TIK me kërkesat e tij të sigurisë, kryen këto detyra:

a) Monitoron informacionin e vulnerabiliteteve në lidhje me produktin e certifikuar TIK, me mjetet e veta, por edhe duke marrë në konsideratë:

i. një publikim ose një parashtrim në lidhje me informacionin e vulnerabiliteteve nga një përdorues ose kërkues në fushën e sigurisë të përmendur në pikën 1, të nenit 10, të këtij vendimi;

ii. një parashtrim nga çdo burim tjetër.

b) Monitoron sigurinë e shprehur në certifikatë.

2. Zotëruesi i një certifikate bashkëpunon me organin certifikues, ITSEF- in dhe, kur është e zbatueshme, me organin kombëtar të certifikimit të sigurisë kibernetike, për të mbështetur aktivitetet e tyre të monitorimit.

SEKSIONI 2
KONFORMITETI DHE PAJTUESHMËRIA

Neni 30
Pasojat e moskonformitetit të një produkti TIK të certifikuar ose të profilit të mbrojtjes

1. Kur një produkt i certifikuar TIK ose profil i mbrojtjes nuk përputhet me kërkesat e përcaktuara në këtë vendim, organi certifikues informon zotëruesin e certifikatës për moskonformitetin e identifikuar dhe kërkon veprime korrigjuese.

2. Kur një rast moskonformiteti me dispozitat e këtij vendimi mund të ndikojë në përputhshmërinë me legjislacionin e posaçëm në fuqi, i cili parashikon mundësinë për të demonstruar prezumimin e konformitetit me kërkesat e atij akti ligjor, duke përdorur certifikatën sipas skemës, organi certifikues duhet të informojë organin kombëtar të certifikimit të sigurisë kibernetike menjëherë. Autoriteti kombëtar i certifikimit të sigurisë kibernetike duhet të njoftojë menjëherë autoritetin përgjegjës për mbikëqyrjen e tregut për legjislacionin tjetër përkatës në lidhje me rastin e moskonformitetit të identifikuar.

3. Pas marrjes së informacionit të përmendur në pikën 1 të këtij neni, zotëruesi i certifikatës i propozon organit certifikues veprimet korrigjuese të nevojshme për të adresuar moskonformitetin brenda afatit kohor të vendosur nga organi certifikues, i cili nuk i kalon 30 (tridhjetë) ditë.

4. Në raste urgjente, organi certifikues mund të pezullojë menjëherë certifikatën, në përputhje me nenin 32 të këtij vendimi, ose kur zotëruesi i certifikatës nuk bashkëpunon si duhet me organin certifikues.

5. Organi certifikues kryen rishikime, në përputhje me nenet 15 e 21 të këtij vendimi, duke vlerësuar nëse veprimi korrigjues adreson moskonformitetin.

6. Kur zotëruesi i certifikatës nuk propozon veprime të duhura korrigjuese gjatë periudhës së përmendur në pikës 3 të këtij neni, certifikata pezullohet në përputhje me nenin 32 të këtij vendimi ose tërhiqet në përputhje me nenet 16 ose 22 të këtij vendimi.

7. Ky nen nuk zbatohet për rastet e vulnerabiliteteve, që prekin një produkt të certifikuar TIK, i cili trajtohet në përputhje me kapitullin VI të këtij vendimi.

Neni 31
Pasojat e mosrespektimit nga zotëruesi i certifikatës

1. Organi certifikues cakton një afat prej 30 (tridhjetë) ditësh për ndërmarrjen e veprimeve korrigjuese nga zotëruesi i certifikatës, kur konstaton se:

a) zotëruesi i certifikatës ose aplikanti për certifikim nuk është në përputhje me detyrimet, sipas përcaktimeve në nenet 11, pika 2, 19, pika 2, 29 dhe 43 të këtij vendimi;

b) zotëruesi i certifikatës nuk informon autoritetin ose organin certifikues për çdo dobësi

ose parregullsi të zbuluar në lidhje me sigurinë e produktit, shërbimit ose procesit TIK të certifikuar, që mund të ketë ndikim, në përputhje me kërkesat që lidhen me certifikimin.

2. Nëse zotëruesi i certifikatës nuk ndërmerr veprime korrigjuese gjatë periudhës kohore të përmendur në pikën 1 të këtij neni, certifikata pezullohet në përputhje me nenin 32 ose tërhiqet në përputhje me nenin 16 ose nenin 22 të këtij vendimi.

3. Shkeljet e vazhdueshme ose të përsëritura nga zotëruesi i certifikatës të detyrimeve të përmendura në pikën 1 të këtij neni shkaktojnë tërheqjen e certifikatës, në përputhje me nenin 16 ose nenin 22 të këtij vendimi.

4. Organi certifikues informon organin kombëtar të certifikimit të sigurisë kibernetike për gjetjet e përmendura në pikën 1 të këtij neni. Kur mospërmbushja bie në kundërshtim me përcaktimet ligjore në fuqi, organi kombëtar i certifikimit të sigurisë kibernetike njofton menjëherë autoritetin përgjegjës për mbikëqyrjen e tregut.

Neni 32
Pezullimi i certifikatës

1. Në rastin e pezullimit të një certifikate, sipas përcaktimeve të këtij vendimi, organi certifikues pezullon një certifikatë për një periudhë të përshtatshme për rrethanat që shkaktuan pezullimin, e cila nuk i kalon 42 (dyzet e dy) ditë. Periudha e pezullimit fillon të nesërmen e ditës së vendimit të organit certifikues dhe nuk ndikon në vlefshmërinë e certifikatës.

2. Organi certifikues njofton menjëherë zotëruesin e certifikatës dhe organin kombëtar të certifikimit të sigurisë kibernetike për pezullimin dhe jep arsyet e pezullimit, veprimet e duhura që duhen ndërmarrë, si dhe periudhën e pezullimit.

3. Zotëruesit e certifikatës njoftojnë blerësit e produkteve TIK për pezullimin dhe arsyet e dhëna nga organi certifikues për pezullimin, me përjashtim të atyre arsyeve, ku ndarja e të cilave përbën një rrezik sigurie ose përmban informacion të ndjeshëm. Ky informacion vihet, gjithashtu, në dispozicion të publikut nga zotëruesi i certifikatës.

4. Kur legjislacioni në fuqi parashikon një supozim konformiteti, bazuar në certifikatat e lëshuara sipas dispozitave të këtij vendimi, organi kombëtar i certifikimit të sigurisë kibernetike informon autoritetin përgjegjës për mbikëqyrjen e tregut për legjislacionin e posaçëm në fuqi në lidhje me pezullimin.

5. Në raste të justifikuara, organi kombëtar i certifikimit të sigurisë kibernetike mund të autorizojë një zgjatje të periudhës së pezullimit të një certifikate, ku periudha totale e pezullimit nuk mund të kalojë një vit.

Neni 33
Pasojat e mospajtueshmërisë nga organi i vlerësimit të konformitetit

1. Në rast të mospajtueshmërisë nga një organ certifikues me detyrimet e tij, ose në rast të identifikimit të mospajtueshmërisë nga një ITSEF-i, organi kombëtar i certifikimit të sigurisë kibernetike ndërmerr menjëherë veprimet, si më poshtë vijon:

a) Identifikon certifikatat potencialisht të prekura, me mbështetjen e ITSEF-it përkatës;

b) Kur është e nevojshme, kërkon që të kryhen aktivitete të vlerësimit në një ose më shumë produkte TIK ose profile të mbrojtjes nga ITSEF-i, që ka kryer vlerësimin, ose nga çdo ITSEF tjetër i akredituar dhe, sipas rastit, nga ITSEF-i, që ka aftësitë teknike për të suportuar identifikimin;

c) Analizon ndikimet e mospajtueshmërisë;

ç) Njofton zotëruesin e certifikatës të prekur nga mospajtueshmëria.

2. Bazuar në përcaktimet e pikës 1 të këtij neni, organi certifikues, në lidhje me çdo certifikatë të prekur, merr një nga vendimet, si më poshtë vijon:

a) Mban të pandryshuar certifikatën;

b) Tërheq certifikatën, në përputhje me nenin 16 ose nenin 22 të këtij vendimi, dhe, kur është e përshtatshme, lëshon një certifikatë të re.

3. Bazuar në përcaktimet e pikës 1 të këtij neni, organi kombëtar i certifikimit të sigurisë kibernetike, sipas rastit, ndërmerr veprimet, si më poshtë vijon:

a) Kur është e nevojshme, raporton mospajtueshmërinë e organit certifikues ose ITSEF-it përkatës tek autoriteti përgjegjës për akreditimin;

b) Kur është e aplikueshme, vlerëson ndikimin e mundshëm në autorizim.

KREU VI
MENAXHIMI I VULNERABILITETEVE DHE NXJERRJA E INFORMACIONIT

Neni 34
Qëllimi menaxhimit të vulnerabiliteteve

Ky kapitull zbatohet për produktet TIK, për të cilat është lëshuar një certifikatë.

SEKSIONI 1
MENAXHIMI I VULNERABILITETIT

Neni 35
Procedurat e menaxhimit të vulnerabilitetit

1. Zotëruesi i një certifikate krijon dhe mirëmban të gjitha procedurat e nevojshme të menaxhimit të vulnerabiliteteve, në përputhje me rregullat e përcaktuara në këtë seksion dhe, kur është e nevojshme, të plotësuara nga procedurat e përcaktuara në ISO/IEC 30111 për teknologjinë e informacionit, teknikat e sigurisë dhe proceset e trajtimit të vulnerabiliteteve.

2. Zotëruesi i një certifikate, bazuar në këtë vendim, mban e publikon metodat e duhura për marrjen e informacionit mbi vulnerabilitetet, që lidhen me produktet e tyre nga burime të jashtme, duke përfshirë përdoruesit, organet e certifikimit dhe kërkuesit në fushën e sigurisë.

3. Kur zotëruesi i një certifikate, sipas përcaktimeve të këtij vendimi, zbulon ose merr informacion në lidhje me një vulnerabilitet të mundshëm që prek një produkt të certifikuar TIK, duhet ta regjistrojë atë dhe të kryejë një analizë të ndikimit të vulnerabilitetit.

4. Kur një vulnerabilitet i mundshëm prek një produkt të përbërë, zotëruesi i certifikatës, bazuar në përcaktimet e këtij vendimi, informon zotëruesin e certifikatave të varura për vulnerabilitete të mundshme.

5. Në përgjigje të një kërkese të arsyeshme nga organi certifikues që ka lëshuar certifikatën, zotëruesi i një certifikate, bazuar në përcaktimet e këtij vendimi, transmeton informacionin përkatës në lidhje me vulnerabilitetet e mundshme tek ai organ certifikues.

Neni 36
Analiza e ndikimit të vulnerabiliteteve

1. Analiza e ndikimit të vulnerabiliteteve u referohet objektivit të vlerësimit dhe deklaratave të sigurisë të përfshira në certifikatë. Analiza e ndikimit të vulnerabiliteteve kryhet në një periudhë kohore të përshtatshme për shfrytëzimin dhe kritikalitetin e vulnerabilitetit të mundshëm të produktit TIK të certifikuar.

2. Kur është e aplikueshme, një përllogaritje e mundshme e sulmit kryhet në përputhje me metodologjinë përkatëse të përfshirë në standardet e përmendura në nenin 3 të këtij vendimi dhe dokumentet teknike më të fundit, sipas përcaktimeve në aneksin I të këtij vendimi, për të përcaktuar shfrytëzimin e vulnerabilitetit. Në konsideratë merret niveli AVA_VAN i certifikatës bazuar këtë vendim.

Neni 37
Raporti i analizës së ndikimit të vulnerabilitetit

1. Zotëruesi përgatit një raport të analizës së ndikimit të vulnerabilitetit, ku analiza e ndikimit tregon se vulnerabiliteti ka një ndikim të mundshëm të konformitetit të produktit TIK me certifikatën e tij.

2. Raporti i analizës së ndikimit të vulnerabilitetit përmban një vlerësim të elementeve, si më poshtë vijon:

a) Ndikimin e vulnerabilitetit në produktin TIK të certifikuar;

b) Rreziqet e mundshme, që lidhen me disponueshmërinë dhe/ose afërsinë e ndodhjes së një sulmi;

c) Nëse vulnerabiliteti mund të korrigjohet;

ç) Aty ku vulnerabiliteti mund të korrigjohet, zgjidhjet e mundshme të vulnerabilitetit.

3. Raporti i analizës së ndikimit të vulnerabilitetit, aty ku është e zbatueshme, përmban detaje rreth mjeteve të mundshme të shfrytëzimit të vulnerabilitetit. Informacioni rreth mjeteve të mundshme të shfrytëzimit të vulnerabilitetit trajtohet në përputhje me masat e duhura të sigurisë për të mbrojtur konfidencialitetin e tij dhe për të siguruar, kur është e nevojshme, shpërndarjen e kufizuar të tij.

4. Zotëruesi i një certifikate, bazuar në

përcaktimet e këtij vendimi, i transmeton menjëherë organit certifikues ose organit kombëtar të certifikimit të sigurisë kibernetike një raport të analizës së ndikimit të vulnerabilitetit.

5. Kur raporti i analizës së ndikimit të vulnerabilitetit përcakton se vulnerabiliteti nuk është i mbetur, sipas kuptimit të standardeve të përmendura në nenin 3 të këtij vendimi, dhe se mund të korrigjohet, zbatohet neni 38 i këtij vendimi.

6. Kur raporti i analizës së ndikimit të vulnerabilitetit përcakton se vulnerabiliteti nuk është i mbetur dhe se nuk mund të korrigjohet, certifikata bazuar në këtë vendim tërhiqet sipas përcaktimeve të nenit 16 të këtij vendimi.

7. Zotëruesi i certifikatës, bazuar në këtë vendim, monitoron çdo dobësi të mbetur për të siguruar që nuk mund të shfrytëzohet në rast të ndryshimeve në mjedisin operacional.

Neni 38
Korrigjimi i vulnerabilitetit

Zotëruesi i një certifikate, bazuar në përcaktimet e këtij vendimi, i paraqet një propozim organit certifikues për një veprim korrigjues. Organi certifikues rishikon certifikatën sipas përcaktimeve të nenit 15 të këtij vendimi. Qëllimi i rishikimit përcaktohet nga korrigjimi i vulnerabilitetit që është propozuar.

SEKSIONI 2
ZBULIMI I VULNERABILITETIT

Neni 39
Informacioni i ndarë me organin kombëtar të certifikimit të sigurisë kibernetike

1. Informacioni i dhënë nga organi certifikues tek organi kombëtar i certifikimit të sigurisë kibernetike përfshin të gjitha elementet e nevojshme, që organi kombëtar i certifikimit të sigurisë kibernetike të kuptojë ndikimin e vulnerabilitetit, ndryshimet që duhen bërë në produktin TIK dhe, kur është e disponueshme, çdo informacion nga organi certifikues mbi implikimet e vulnerabilitetit për produkte të tjera TIK të certifikuara.

2. Informacioni i dhënë sipas përcaktimeve të pikës 1 të këtij neni nuk përmban detaje të mjeteve të shfrytëzimit të vulnerabilitetit. Kjo dispozitë nuk cenon kompetencat verifikuese të organit kombëtar të certifikimit të sigurisë kibernetike.

Neni 40
Bashkëpunimi me autoritetet e tjera të certifikimit të sigurisë kibernetike

1. Organi kombëtar i certifikimit të sigurisë kibernetike ndan informacionin përkatës, të marrë sipas përcaktimeve të nenit 39 të këtij vendimi, me autoritetet e tjera të certifikimit të sigurisë kibernetike të shteteve anëtare të Bashkimit Evropian dhe me ENISA-n, me anëtarësimin e Republikës së Shqipërisë në Bashkimin Evropian.

2. Autoritetet e tjera të certifikimit të sigurisë kibernetike, me anëtarësimin e Republikës së Shqipërisë në Bashkimin Evropian, mund të vendosin të analizojnë më tej vulnerabilitetin ose, pasi të informojnë zotëruesin e certifikatës, bazuar në kriteret e përbashkëta evropiane, të kërkojnë nga organet certifikuese të vlerësojnë nëse vulnerabiliteti mund të prekë produkte të tjera TIK të certifikuara.

Neni 41
Publikimi i vulnerabilitetit

Pas tërheqjes së një certifikate, zotëruesi i certifikatës, bazuar në përcaktimet e këtij vendimi, zbulon dhe raporton çdo vulnerabilitet të njohur publikisht dhe të korrigjuar në produktin TIK, që në vijim regjistrohet në regjistrin e vulnerabiliteteteve, sipas përcaktimeve në legjislacionin në fuqi për sigurinë kibernetike, si dhe ndan informacion, sipas përcaktimeve të nenit 10 të këtij vendimi.

KREU VII
RUAJTJA, NXJERRJA DHE MBROJTJA E INFORMACIONIT

Neni 42
Ruajtja e të dhënave nga organi certifikues dhe ITSEF-i

1. ITSEF-i dhe organi certifikues mbajnë një sistem regjistrimi, i cili përmban të gjitha dokumentet e prodhuara në lidhje me çdo vlerësim e certifikim që kryejnë.

2. Organi certifikues dhe ITSEF-i ruajnë të dhënat në mënyrë të sigurt dhe i mbajnë regjistrimet për qëllimet e këtij vendimi, për të paktën 5 (pesë) vjet pas tërheqjes së certifikatës përkatëse, bazuar në përcaktimet e këtij vendimi. Kur organi certifikues ka lëshuar një certifikatë të re, sipas përcaktimeve në shkronjën "c", të pikës 2, të nenit 15, të këtij vendimi, organi ruan dokumentacionin e certifikatës së tërhequr së bashku dhe për aq kohë sa ruhet certifikata e re.

Neni 43
Informacioni i vënë në dispozicion nga zotëruesi i një certifikate

1. Informacioni i përmendur në nenin 10 të këtij vendimi është i disponueshëm në gjuhën shqipe dhe në një gjuhë tjetër të përshtatshme, që mund të jetë lehtësisht e aksesueshme për përdoruesit.

2. Zotëruesi i një certifikate ruan në mënyrë të sigurt për qëllimet e këtij vendimi për të paktën 5 (pesë) vjet pas tërheqjes së certifikatës, si më poshtë vijon:

a) Dokumentimin e informacionit të dhënë organit certifikues dhe ITSEF-it gjatë procesit të certifikimit;

b) Ekzemplarin e produktit TIK të certifikuar.

3. Kur organi certifikues ka lëshuar një certifikatë të re, sipas përcaktimeve në shkronjën "c", të pikës 2, të nenit 15, të këtij vendimi, zotëruesi mban dokumentacionin e certifikatës së tërhequr së bashku me të dhe për aq kohë sa mban certifikatën e re.

4. Me kërkesë të organit certifikues ose të organit kombëtar të certifikimit të sigurisë kibernetike, zotëruesi i një certifikate vendos në dispozicion të dhënat dhe kopjet e përmendura në pikën 2 të këtij neni.

Neni 44
Mbrojtja e informacionit

Organi kombëtar i certifikimit të sigurisë kibernetike, organet e vlerësimit të konformitetit dhe të gjitha palët e tjera garantojnë sigurinë e mbrojtjen e sekreteve të biznesit dhe të informacioneve të tjera konfidenciale, duke përfshirë sekretet tregtare, si dhe ruajtjen e të drejtave të pronësisë intelektuale dhe marrin masat e nevojshme e të duhura teknike dhe organizative.

KREU VIII
MARRËVESHJET E NJOHJES RECIPROKE

Neni 45
Kushtet

1. Republika e Shqipërisë, për të certifikuar produktet në përputhje me rregulloret e Bashkimit Evropian dhe që një certifikim i tillë të njihet brenda Bashkimit Evropian, lidh një marrëveshje njohjeje reciproke me Bashkimin Evropian.

2. Marrëveshja e njohjes reciproke mbulon nivelet e aplikueshme të sigurisë për produktet TIK të certifikuara dhe, sipas rastit, edhe profilet e mbrojtjes.

3. Republika e Shqipërisë, për lidhjen e marrëveshjes së njohjes reciproke me Bashkimin Evropian, sipas përcaktimeve në pikën 1 të këtij neni, duhet të plotësojë kushtet, si më poshtë vijon:

a) Të ketë një autoritet:

i. publik, të pavarur nga subjektet që mbikëqyr dhe monitoron për nga struktura organizative e ligjore, burimi financiar dhe vendimmarrja;

ii. me kompetencat e duhura monitoruese e mbikëqyrëse për të kryer verifikime dhe që është i autorizuar të marrë masat e duhura korrigjuese për të siguruar pajtueshmërinë;

iii. me sistem penaliteti efektiv, proporcional dhe bindës për të siguruar pajtueshmërinë;

iv. që dakordëson për të bashkëpunuar me Grupin Evropian të Certifikimit të Sigurisë Kibernetike dhe ENISA-n për të shkëmbyer praktikat më të mira dhe zhvillimet përkatëse në fushën e certifikimit të sigurisë kibernetike e për të punuar drejt një interpretimi uniform të kritereve dhe të metodave të vlerësimit aktualisht të zbatueshme, ndër të tjera, duke aplikuar dokumentacion të harmonizuar, që është ekuivalent me dokumentet teknike më të fundit, sipas përcaktimeve në aneksin I të këtij vendimi.

b) Të ketë një autoritet përgjegjës të pavarur për akreditimin që kryen akreditime, sipas rregulloreve të Bashkimit Evropian;

c) Të marrë angazhimin që proceset dhe procedurat e vlerësimit e të certifikimit të kryhen

në mënyrë profesionale, duke marrë në konsideratë pajtueshmërinë me standardet ndërkombëtare, sipas përcaktimeve në nenin 3 të këtij vendimi;

ç) Të ketë kapacitetin për të raportuar vulnerabilitete të pazbuluara më parë dhe një procedurë të vendosur, adekuate të menaxhimit e të zbulimit të vulnerabiliteteve;

d) Të ketë procedura që e mundësojnë paraqitjen dhe trajtimin efektiv të ankesave dhe ofrimin e mjeteve juridike efektive për ankuesin;

dh) Të krijojë një mekanizëm për bashkëpunimin me organet të Bashkimit Evropian dhe shteteve anëtare, që lidhen me certifikimin e sigurisë kibernetike, duke përfshirë ndarjen e informacionit në lidhje me mospajtueshmëritë e mundshme të certifikatave, monitorimin e zhvillimeve përkatëse në fushën e certifikimit, si dhe sigurimin e një qasjeje të përbashkët në mirëmbajtjen e rishikimin e certifikimit.

4. Republika e Shqipërisë, përveç kushteve sipas përcaktimeve të pikës 3 të këtij neni, për lidhjen e një marrëveshje njohjeje reciproke me Bashkimin Evropian, sipas përcaktimeve të pikës 1 të këtij neni, që mbulon nivelin e sigurisë "të lartë", duhet të plotësojë edhe kushtet, si më poshtë vijon:

a) Të ketë një autoritet të pavarur e publik të certifikimit të sigurisë kibernetike, që kryen ose delegon aktivitetet e vlerësimit për të lejuar certifikimin në nivelin e sigurisë "të lartë", që janë ekuivalente me kërkesat dhe procedurat e përcaktuara për autoritetet kombëtare të sigurisë kibernetike, sipas rregullores për skemën e certifikimit të sigurisë kibernetike bazuar në kriteret e përbashkëta, si dhe rregullores së sigurisë kibernetike të teknologjisë së informacionit dhe komunikimit të Bashkimit Evropian;

b) Marrëveshja e njohjes reciproke të krijojë një mekanizëm të përbashkët të ngjashëm me vlerësimin e oponencës për certifikimin e sigurisë kibernetike bazuar në kriteret e përbashkëta, për të përmirësuar shkëmbimin e praktikave dhe për të zgjidhur së bashku çështjet në fushën e vlerësimit e të certifikimit.

KREU IX
VLERËSIMI I OPONENCËS SË ORGANEVE CERTIFIKUESE

Neni 46
Procedura e vlerësimit të oponencës

1. Një organ certifikues që lëshon certifikata, bazuar në kriteret e përbashkëta evropiane në nivel sigurie "të lartë", i nënshtrohet një vlerësimi të oponencës në mënyrë të rregullt e periodike të paktën çdo 5 (pesë) vjet. Llojet e ndryshme të vlerësimit të oponencës janë të listuara në aneksin VI të këtij vendimi.

2. Grupi Evropian i Certifikimit të Sigurisë Kibernetike harton e mirëmban një plan vlerësimesh të oponencës, duke siguruar respektimin e këtij periodiciteti. Me përjashtim të rasteve të justifikuara, vlerësimet e oponencës kryhen në vend.

3. Vlerësimi i oponencës mund të mbështetet në provat e mbledhura gjatë vlerësimeve të mëparshme të oponencave ose të procedurave ekuivalente të oponencës të organit certifikues ose të organit kombëtar të certifikimit të sigurisë kibernetike, me kusht që:

a) rezultatet nuk janë më të vjetra se 5 (pesë) vjet;

b) rezultatet shoqërohen nga një përshkrim i procedurave të vlerësimit të oponencës të vendosura për atë skemë, të cilat lidhen me një vlerësim të oponencës të kryer, sipas një skeme tjetër certifikimi;

c) raporti i vlerësimit të oponencave, i përmendur në nenin 48 të këtij vendimi, të specifikojë se cilat rezultate janë ripërdorur me ose pa vlerësim të mëtejshëm.

4. Kur një vlerësim oponence mbulon një fushë teknike, vlerësohet gjithashtu edhe ITSEF-i përkatës.

5. Organi certifikues për vlerësimin e oponencës dhe, kur është e nevojshme, organi kombëtar i certifikimit të sigurisë kibernetike siguron që informacioni përkatës të vihet në dispozicion të ekipit të vlerësimit të oponencës.

6. Vlerësimi i oponencës kryhet nga një ekip vlerësimi oponence i ngritur sipas përcaktimeve në aneksin VI të këtij vendimi.

Neni 47
Fazat e vlerësimit të oponencës

1. Gjatë fazës përgatitore, anëtarët e ekipit të vlerësimit të oponencës shqyrtojnë dokumentacionin e organit certifikues, që mbulon politikat e procedurat e tij, duke përfshirë përdorimin e dokumenteve teknike më të fundit.

2. Gjatë fazës së vizitës në terren, ekipi i vlerësimit të oponencës vlerëson kompetencën teknike të organit certifikues dhe, kur është e zbatueshme, kompetencën e ITSEF-it që ka kryer të paktën një vlerësim të produktit TIK të mbuluar nga vlerësimi i oponencës.

3. Kohëzgjatja e fazës së vizitës në terren mund të zgjatet ose të zvogëlohet në varësi të faktorëve të tillë, si: mundësia e ripërdorimit të provave dhe të rezultateve ekzistuese të vlerësimit të oponencave, ose numri i ITSEF-ve dhe fushave teknike, për të cilat organi certifikues lëshon certifikata.

4. Nëse është e aplikueshme, ekipi i vlerësimit të oponencës përcakton kompetencën teknike të çdo ITSEF-i, duke vizituar laboratorin ose laboratorët e tij teknikë dhe duke intervistuar vlerësuesit e tij në lidhje me fushën teknike dhe metodat specifike të sulmit.

5. Në fazën e raportimit, ekipi i vlerësimit të oponencës dokumenton konkluzionet e tij në një raport vlerësimi oponence, duke përfshirë një vendim, dhe, ku është e zbatueshme, një listë të moskonformiteteve të konstatuara, secila e vlerësuar sipas një niveli kritikaliteti.

6. Raporti i vlerësimit të oponencës, së pari, diskutohet me organin certifikues të vlerësuar nga ekipi i vlerësimit të oponencës. Pas këtyre diskutimeve, organi certifikues i vlerësuar nga ekipi i vlerësimit të oponencës krijon një plan të masash që merren për të adresuar përfundimet.

Neni 48
Raporti i vlerësimit të oponencës

1. Ekipi i vlerësimit të oponencës i siguron organit certifikues një raport fillestar të vlerësimit të oponencës.

2. Organi certifikues i vlerësuar nga ekipi i vlerësimit të oponencës i paraqet grupit të vlerësimit të oponencës komentet lidhur me përfundimet dhe një listë angazhimesh për të adresuar mangësitë e identifikuara në raportin fillestar të vlerësimit të oponencës.

3. Ekipi i vlerësimit të oponencës i dorëzon Grupit Evropian të Certifikimit të Sigurisë Kibernetike një raport përfundimtar të vlerësimit të oponencës, i cili gjithashtu përfshin komentet dhe angazhimet e bëra nga organi certifikues i vlerësuar. Ekipi i vlerësimit të oponencës përfshin, gjithashtu, qëndrimin e tij mbi komentet, si dhe nëse ato angazhime janë të mjaftueshme për të adresuar mangësitë e identifikuara.

4. Kur konstatohen moskonformitete në raportin e vlerësimit të oponencës, Grupi Evropian i Certifikimit të Sigurisë Kibernetike mund të caktojë një afat kohor të përshtatshëm për organin certifikues të vlerësuar për të trajtuar moskonformitetet.

5. Grupi Evropian i Certifikimit të Sigurisë Kibernetike miraton një opinion mbi raportin e vlerësimit të oponencës, kur:

a) raporti i vlerësimit të oponencës nuk identifikon moskonformitetet ose kur moskonformitetet janë adresuar në mënyrën e duhur nga organi certifikues i vlerësuar, Grupi Evropian i Certifikimit të Sigurisë Kibernetike mund të dalë në një përfundim pozitiv dhe të gjitha dokumentet përkatëse publikohen në faqen e internetit të certifikimit të ENISA-s;

b) organi certifikues i vlerësuar nuk i trajton moskonformitetet në mënyrë të duhur, brenda afatit kohor të caktuar, Grupi Evropian i Certifikimit të Sigurisë Kibernetike mund të dalë në një përfundim negativ, i cili publikohet në faqen e internetit të certifikimit të ENISA, duke përfshirë raportin e vlerësimit të oponencës dhe të gjitha dokumentet përkatëse.

6. Përpara publikimit të përfundimit, nga dokumentet e publikuara hiqen të gjitha informacionet e ndjeshme, personale ose të pronësisë.

KREU X
DISPOZITA PËRFUNDIMTARE

Neni 49
Shfuqizime në datën e anëtarësimit të Republikës së Shqipërisë në Bashkimin Evropian

Në datën e anëtarësimit të Republikës së Shqipërisë në Bashkimin Evropian, të gjitha

dispozitat e këtij vendimi shfuqizohen, me përjashtim të nenit 26 të këtij vendimi.

Neni 50
Dispozita të fundit dhe kalimtare

1. Ngarkohen Autoriteti Kombëtar për Sigurinë Kibernetike, institucioni përgjegjës për mbikëqyrjen e tregut, institucioni përgjegjës për akreditimin dhe organet e vlerësimit të konformitetit për zbatimin e këtij vendimi.

2. Deri më 31 dhjetor 2027, një certifikatë mund të lëshohet sipas pikës 1, të nenit 3, të këtij vendimi, duke zbatuar një nga standardet e mëposhtme:

a) ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008 ose ISO/IEC 15408-3:2008;

b) Kriteret e përbashkëta për vlerësimin e sigurisë së teknologjisë së informacionit (TI), versioni 3.1, rishikimi 5;

c) ISO/IEC 18045:2008;

ç) Metodologjia e përbashkët për vlerësimin e sigurisë së teknologjisë së informacionit, rishikimi 5, versioni 3.1.

3. Deri më 31 dhjetor 2027, një certifikatë e lëshuar në përputhje me standardet e përmendura në pikën 1, të nenit 3, të këtij vendimi, mund të lëshohet sipas skemës, me prezumimin e konformitetit me një profil të mbrojtjes, që përmbush standardet e listuara në pikën 2 të këtij neni.

4. Nenet 46, 47 dhe 48 të këtij vendimi fillojnë të zbatohen me hyrjen në fuqi të marrëveshjes së nënshkruar për njohjen reciproke ndërmjet Republikës së Shqipërisë dhe Bashkimit Evropian, sipas përcaktimeve të nenit 45 të këtij vendimi ose me anëtarësimin e Republikës së Shqipërisë në Bashkimin Evropian.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

KRYEMINISTËR
Edi Rama

ANEKSI I: Fushat teknike dhe dokumentet teknike më të fundit

Dokumentet teknike më të fundit që mbështesin fushat teknike dhe dokumente të tjera teknike më të fundit.

1. Dokumente teknike më të fundit që mbështesin fushat teknike në nivelin AVA_VAN 4 ose 5:

a. Dokumentet që i referohen vlerësimit të harmonizuar të fushës teknike "karta inteligjente dhe pajisje të ngjashme" janë si më poshtë vijon:

i. Kërkesat minimale për ITSEF-et për vlerësimet e sigurisë të kartave inteligjente dhe pajisjeve të ngjashme, versioni 1.1;

ii. Kërkesat minimale për sigurinë e vendndodhjes, versioni 1.1;

iii. Zbatimi i Kritereve të Përbashkëta për qarqet e integruara, versioni 1.1;

iv. Kërkesat për arkitekturën e sigurisë (ADV_ARC) për kartat inteligjente dhe pajisjet e ngjashme, versioni 1.1;

v. Certifikimi i produkteve të kartave inteligjente "të hapura", versioni 1.1;

vi. Vlerësimi i produkteve të përbëra për kartat inteligjente dhe pajisjet e ngjashme, versioni 1.1;

vii. Aplikim i skenarit të mundshëm të sulmit në kartat inteligjente dhe pajisjet e ngjashme, versioni 1.2.

b. Dokumentet që i referohen vlerësimit të harmonizuar të fushës teknike "pajisje harduerike me kuti sigurie" janë si më poshtë vijon:

i. Kërkesat minimale për ITSEF-t për vlerësimet e sigurisë të pajisjeve harduerike me kuti sigurie, versioni 1.1;

ii. Kërkesat minimale për sigurinë e vendndodhjes, versioni 1.1;

iii. Aplikimi i skenarit të mundshëm të sulmit për pajisjet harduerike me kuti sigurie, versioni 1.2.

2. Dokumente teknike më fundit lidhur me akreditimin e harmonizuar të organeve të vlerësimit të konformitetit janë më poshtë vijon:

a. Akreditimi i ITSEF-ve sipas përcaktimeve të vendimit, versioni 1.1;

b. Akreditimi i ITSEF-ve sipas përcaktimeve të vendimit, versioni 1.6c;

c. Akreditimi i organeve certifikuese sipas përcaktimeve të vendimit, versioni 1.6b.

ANEKSI II: Profilet e mbrojtjes të certifikuara në nivelin AVA_VAN 4 ose 5

1. Për kategorinë e pajisjeve për krijimin e nënshkrimeve dhe vulave të kualifikuara në distancë:

a) EN 419241-2:2019 – Sisteme të besueshme

që mbështesin nënshkrimin e serverit - Pjesa 2: Profili i mbrojtjes për pajisje për krijimin e nënshkrimit të kualifikuar për nënshkrimin e serverit;

b) EN 419221-5:2018 – Profilet e mbrojtjes për modulet kriptografike të ofruesit të shërbimeve të besuara - Pjesa 5: Moduli kriptografik për shërbimet e besuara

2. Profilet e mbrojtjes të miratuara si dokumente teknike më të fundit.

ANEKSI III – Profilet e mbrojtjes të rekomanduara sipas përcaktimeve në aneksin I

1. Për kategorinë e dokumenteve e udhëtimit të lexueshme nga pajisjet të leximit të dokumenteve të udhëtimit:

a) Profil mbrojtje për dokumentet e udhëtimit të lexueshme nga pajisjet duke përdorur procedurën standarde të inspektimit me PACE (krijimi i lidhjes së autentifikuar me fjalëkalim), BSI-CC-PP-0068-V2-2011-MA-01;

b) Profil mbrojtje për dokumentet e udhëtimit të lexueshme nga pajisjet me aplikacionin "ICAO", kontrolli i aksesit të zgjeruar, BSI-CC-PP-0056-2009;

c) Profil mbrojtje për dokumentet e udhëtimit të lexueshme nga pajisjet me aplikacionin "ICAO" kontrolli i zgjeruar i aksesit me PACE (krijimi i lidhjes së autentifikuar me fjalëkalim), BSI-CC-PP-0056-V2-2012-MA-02;

ç) Profil mbrojtje për dokumentet e udhëtimit të lexueshme nga pajisjet me aplikacionin "ICAO", Kontrolli i aksesit bazë BSI-CC-PP-0055-2009.

2. Për kategorinë e pajisjeve të krijimit të nënshkrimit të sigurt:

a) EN 419211-1:2014 – Profilet e mbrojtjes për pajisjen e krijimit të nënshkrimit të sigurt - Pjesa 1: Vështrim i përgjithshëm;

b) EN 419211-2:2013 - Profilet e mbrojtjes për pajisjen e krijimit të nënshkrimit të sigurt - Pjesa 2: Pajisja me gjenerim çelësi;

c) EN 419211-3:2013 - Profilet e mbrojtjes për pajisjen e krijimit të nënshkrimit të sigurt - Pjesa 3: Pajisja me importim çelësi;

ç) EN 419211-4:2013 - Profilet e mbrojtjes për pajisjen e krijimit të nënshkrimit të sigurt –

Pjesa 4: Zgjerim për pajisjen me gjenerim çelësi dhe kanale të besuara në aplikacionin e gjenerimit të certifikatës;

d) EN 419211-5:2013 - Profilet e mbrojtjes për pajisjen e krijimit të nënshkrimit të sigurt - Pjesa 5: Zgjatim për pajisjen me gjenerim çelësi dhe kanalin e besuar për aplikacionin e krijimit të nënshkrimit;

dh) EN 419211-6:2014 - Profilet e mbrojtjes për pajisjen e krijimit të nënshkrimit të sigurt –

Pjesa 6: Zgjerim për pajisjen me importimin e çelësit dhe kanalin e besuar në aplikacionin e krijimit të nënshkrimit.

3. Për kategorinë e tahografit digjital:

a) Tahografi digjital - Karta e tahografit, sipas përcaktimeve në legjislacionin në fuqi;

b) Tahografi digjital - Njësia e automjeteve sipas përcaktimeve në legjislacionin në fuqi;

c) Tahografi digjital - Pajisja e jashtme e Sistemit Global i Navigimit Satelitor GNSS (EGF PP);

ç) Tahografi digjital - Sensori i lëvizjes (MS PP) sipas përcaktimeve në legjislacionin në fuqi.

4. Për kategorinë e qarqeve të integruara të sigurta, kartave inteligjente dhe pajisjeve përkatëse:

a) Profili i Mbrojtjes i Platformës së qarqeve të integruara të sigurisë IC për qarqet e integruara, BSI-CC-PP-0084-2014;

b) Sistemi i kartës Java - Konfigurimi i hapur, V3.0.5 BSI-CC-PP-0099-2017;

c) Sistemi i kartës Java - Konfigurimi i mbyllur, BSI-CC-PP-0101-2017;

ç) Profilet e mbrojtjes për një modul të platformës së besuar specifik të një kompjuteri personal (klienti PC), familja 2.0 niveli 0 rishikimi 1.16, ANSSI-CC-PP-2015/07;

d) Karta SIM universale, PU-2009-RT-79, ANSSI-CC-PP-2010/04;

dh) Karta e qarkut të integruar universal e integruar në pajisjet makinë-me-makinë, BSI-CC-PP-0089-2015.

5. Për kategorinë e pikave të ndërveprimit (të pagesës) dhe terminaleve të pagesës:

a) Pika e ndërveprimit vetëm me çip, ANSSI-CC-PP-2015/01;

b) Pika e ndërveprimit "vetëm me çip dhe Paketa e Protokollit të Hapur Open Protocol Package, ANSSI-CC-PP-2015/02;

c) Pika e ndërveprimit gjithëpërfshirëse, ANSSI-CC-PP- 2015/03;

ç) Pika e ndërveprimit gjithëpërfshirëse dhe paketa e protokollit të hapur, ANSSI-CC-PP-2015/04;

d) Pika e ndërveprimit vetëm me pajisje me vendosje PIN (Numër identifikimi personal) ", ANSSI-CC-PP-2015/05;

dh) Pika e ndërveprimit vetëm me pajisje me vendosje PIN (Numër identifikimi personal) dhe paketa e protokollit të hapur, ANSSI-CC-PP-2015/06.

6. Për kategorinë e pajisjeve harduerike me kuti sigurie (security boxes):

a) Moduli kriptografik për veprimet e nënshkrimit të ofruesit të shërbimit kriptografik me kopje rezervë (back up) – Profil mbrojtje CMCSOB, PP HSM CMCSOB 14167-2, ANSSI-CC-PP-2015/08;

b) Moduli kriptografik për shërbimet e gjenerimit të çelësave të ofruesit të shërbimit kriptografik – Profil mbrojtje CMCKG, PP HSM CMCKG 14167-3, ANSSI-CC-PP-2015/09;

c) Moduli kriptografik për veprimet e nënshkrimit të ofruesit të shërbimit kriptografik pa kopje rezervë (back up) - PP CMCSO, PP HSM CMCKG 14167-4, ANSSI-CC-PP-2015/10.

ANEKSI IV: Vazhdimësia e garantimit të sigurisë dhe rishikimi i certifikatës

IV.1 Vazhdimësia e garantimit të sigurisë: fusha e zbatimit

1. Kërkesat e mëposhtme për vazhdimësinë e garantimit të sigurisë zbatohen për aktivitetet e mirëmbajtjes që lidhen me si më poshtë:

a) një rivlerësim nëse një produkt TIK i pandryshuar i certifikuar i plotëson kërkesat e sigurisë;

b) një vlerësim të ndikimeve të ndryshimeve në një produkt TIK të certifikuar në certifikimin e tij;

c) nëse përfshihet në certifikim, aplikimi i korrigjimeve (*patches*) në përputhje me një proces të vlerësuar të menaxhimit të korrigjimeve (*patches*);

ç) nëse përfshihet, rishikimi i menaxhimit të ciklit jetësor ose proceseve të prodhimit të zotëruesit të certifikatës.

2. Zotëruesi i një certifikate mund të kërkojë rishikimin e certifikatës në rastet si më poshtë vijon:

a) certifikata skadon brenda nëntë muajve;

b) ka një ndryshim ose në produktin TIK të certifikuar ose në një faktor tjetër që mund të ndikojë në funksionalitetin e sigurisë së tij;

c) zotëruesi i certifikatës kërkon që vlerësimi i vulnerabilitetit të kryhet përsëri në mënyrë që të rikonfirmohet siguria e certifikatës lidhur me rezistencën e produktit TIK ndaj sulmeve të kibernetike.

IV.2 Rivlerësimi

1. Kur është e nevojshme për të vlerësuar ndikimin e ndryshimeve në mjedisin e kërcënimit të një produkti TIK të certifikuar të pandryshuar, i paraqitet organit certifikues një kërkesë rivlerësimi.

2. Rivlerësimi kryhet nga i njëjti ITSEF që ishte përfshirë në vlerësimin e mëparshëm duke ripërdorur të gjitha rezultatet e tij që janë ende në zbatim. Vlerësimi përqendrohet në aktivitetet e garantimit të sigurisë të cilat mundësisht ndikohen nga mjedisi i ndryshuar i kërcënimit të produktit TIK të certifikuar, në veçanti AVA_VAN përkatëse përveç kësaj, te familja e ciklit të jetës së garantimit të sigurisë (ALC), ku mblidhen prova të mjaftueshme për mirëmbajtjen e mjedisit të zhvillimit.

3. ITSEF përshkruan ndryshimet dhe detajon rezultatet e rivlerësimit me një përditësim të raportit teknik të vlerësimit të mëparshëm.

4. Organi certifikues shqyrton raportin teknik të vlerësimit të përditësuar dhe krijon një raport rivlerësimi. Statusi i certifikatës fillestare modifikohet më pas në sipas përcaktimeve në nenin 15 të vendimit.

5. Raporti i rivlerësimit dhe certifikata e përditësuar i jepen organit kombëtar të certifikimit të sigurisë kibernetike dhe me anëtarësimin e Republikës së Shqipërisë në BE edhe ENISA-s për publikim në faqen e saj të internetit të certifikimit të sigurisë kibernetike.

IV.3 Ndryshimet në një produkt TIK të certifikuar

1. Kur një produkt TIK i certifikuar ka qenë subjekt i ndryshimeve, zotëruesi i certifikatës që dëshiron të mbajë certifikatën i siguron organit certifikues një raport të analizës së ndikimit.

2. Raporti i analizës së ndikimit siguron elementet e mëposhtëm:

a) një hyrje që përmban informacionin e nevojshëm për të identifikuar raportin e analizës

së ndikimit dhe objektin e vlerësimit që i nënshtrohet ndryshimeve;

b) një përshkrim të ndryshimeve në produkt;

c) identifikimin e provave të zhvilluesit të prekur;

ç) një përshkrim të modifikimeve të provave të zhvilluesit;

d) gjetjet dhe konkluzionet mbi ndikimin në garantimin e sigurisë për çdo ndryshim.

3. Organi certifikues shqyrton ndryshimet e përshkruara në raportin e analizës së ndikimit për të vërtetuar ndikimin e tyre mbi garantimin e sigurisë e objektit të vlerësuar të certifikuar, siç propozohet në konkluzionet e raportit të analizës së ndikimin.

4. Pas ekzaminimit, organi certifikues përcakton shkallën e një ndryshimi të vogël ose të madh që i korrespondon ndikimit të tij.

5. Kur ndryshimet konfirmohen nga organi certifikues si ndryshime të vogla, nuk lëshohet një certifikatë e re për produktin TIK të modifikuar, por krijohet një raport i mirëmbajtjes në raportin fillestar të certifikimit. Raporti i mirëmbajtjes përfshihet në raportin e analizës së ndikimit, dhe përmban seksionet e mëposhtme:

a) hyrje;

b) përshkrimi i ndryshimeve;

c) provat e zhvilluesit të prekur;

6. Kur ndryshimet e konfirmuara janë të mëdha, një rivlerësim kryhet në kontekstin e vlerësimit të mëparshëm dhe duke ripërdorur çdo rezultat nga vlerësimi i mëparshëm që është ende në zbatim.

7. Pas përfundimit të vlerësimit të objektit të ndryshuar të vlerësimit, ITSEF krijon një raport të ri teknik vlerësimi. Organi certifikues shqyrton raportin teknik të përditësuar të vlerësimit, aty ku është e zbatueshme, krijon një certifikatë të re me një raport të ri certifikimi.

IV.4 Menaxhimi i korrigjimeve (*patch*)

1. Një procedurë e menaxhimit të korrigjimeve (*patch*) siguron një proces të strukturuar të përditësimit të një produkti TIK të certifikuar. Procedura e menaxhimit të korrigjimeve (*patch*), duke përfshirë mekanizmin e zbatuar në produktin TIK nga aplikanti për certifikim, mund të përdoret pas certifikimit të produktit TIK nën përgjegjësinë e organit të vlerësimit të konformitetit.

2. Aplikanti për certifikim përfshin në certifikimin e produktit TIK një mekanizëm korrigjimesh (*patch*) si pjesë e një procedure menaxhimi të certifikuar të zbatuar në produktin TIK në një nga kushtet e mëposhtme:

a) funksionalitetet e prekura nga korrigjimi (*patch*) qëndrojnë jashtë objektit të vlerësimit të produktit TIK të certifikuar;

b) Korrigjimi (*patch*) lidhet me një ndryshim të vogël të paracaktuar në produktin TIK të certifikuar;

c) Korrigjimi (*patch*) lidhet me një vulnerabilitet të konfirmuar me efekte kritike në sigurinë e produktit TIK të certifikuar.

3. Nëse korrigjimi (*patch*) lidhet me një ndryshim të madh në objektin e vlerësimit të produktit TIK të certifikuar në lidhje me një vulnerabilitet të pazbuluar më parë që nuk ka efekte kritike për sigurinë e produktit TIK, zbatohen përcaktimet në nenin 15 të vendimit.

4. Procedura e menaxhimit të korrigjimit (*patch*) për një produkt TIK përbëhet nga elementët e mëposhtëm:

a) procesi për zhvillimin dhe nxjerrjen e korrigjimit (patch) për produktin TIK;

b) mekanizmin teknik dhe funksionet për instalimin e korrigjimit (*patch*) në produktin TIK;

c) një grup aktivitetesh vlerësimi që lidhen me efektivitetin dhe performancën e mekanizmit teknik.

5. Gjatë certifikimit të produktit TIK:

a) aplikanti për certifikimin e produktit TIK paraqet përshkrimin e procedurës së menaxhimit të korrigjimit (*patch*);

b) ITSEF verifikon elementët e mëposhtëm nëse:

i. zhvilluesi ka implementuar mekanizmat e korrigjimit (*patch*) në produktin TIK në përputhje me procedurën e menaxhimit të korrigjimeve (*patch*) të dorëzuar për certifikim;

ii. kufijtë e objektit të vlerësimit janë të ndara në një mënyrë që ndryshimet e bëra në proceset e ndara të mos ndikojnë në sigurinë e objektit të vlerësimit;

iii. mekanizmi teknik i korrigjimit funksionon në përputhje me dispozitat e ankesit VI.4. pretendimet e aplikantit;

c) organi certifikues përfshin në raportin e certifikimit rezultatin e procedurës së vlerësuar të menaxhimit të korrigjimit (*patch*).

6. Zotëruesi i certifikatës mund të aplikojë

korrigjimin e (*patch*) prodhuar në përputhje me procedurën e menaxhimit të korrigjimit (*patch*) të certifikuar për produktin TIK të certifikuar dhe ndërmerr hapat brenda 5 ditëve pune në rastet si më poshtë vijon:

a) në rastin e përmendur në shkronjën a) pikë 2 të aneksit IV.4, raporton korrigjimin (*patch*) tek organi certifikues që nuk e ndryshon certifikatën përkatëse;

b) në rastin e përmendur në shkronjën b) pika 2 të aneksit IV.4, paraqet korrigjimin (*patch*) tek ITSEF për shqyrtim. ITSEF informon organin certifikues pas marrjes së korrigjimit (*patch*) mbi të cilin organi certifikues ndërmerr veprimet e duhura për të lëshuar një version të ri të certifikatës përkatëse sipas skemës dhe përditësimin e raportit të certifikimit;

c) në rastin e përmendur në shkronjën c) pika 2 të aneksit IV.4, dorëzon korrigjimin (*patch*) tek ITSEF për rivlerësimin e nevojshëm, por mund ta instalojë paralelisht. ITSEF informon organin certifikues pas së cilës organi certifikues fillon aktivitetet e certifikimit përkatëse.

ANEKSI V: Përmbajtja e një raporti certifikimi

V.1 Raporti i certifikimit

1. Në bazë të vlerësimit të raporteve teknike të mundësuara nga ITSEF, organi certifikues krijon një raport certifikimi që publikohet së bashku me certifikatën korresponduese.

2. Raporti i certifikimit është burimi i informacionit të detajuar dhe praktik në lidhje me produktin TIK ose kategorinë e produkteve TIK dhe për instalimin e sigurt të produktit TIK dhe për këtë arsye përfshin informacionet e disponueshme publikisht dhe të ndara, me rëndësi për përdoruesit dhe palët e interesuara. Ky informacion mund të referohet nga raporti i certifikimit.

3. Raporti i certifikimit përmban të paktën pikat si më poshtë vijon:

a) përmbledhje ekzekutive;

b) identifikimin e produktit TIK ose kategorisë së produktit TIK për profilet e mbrojtjes;

c) shërbimet e sigurisë;

ç) supozimet dhe sqarimin e fushës së veprimit;

d) informacioni i arkitekturës;

dh) informacion shtesë për sigurinë kibernetike, nëse është e zbatueshme ;

e) testimi i produktit TIK, nëse është kryer;

ë) aty ku është e zbatueshme, një identifikim të proceseve të menaxhimit të ciklit jetësor të zotëruesit të certifikatës dhe objekteve të prodhimit;

f) rezultatet e vlerësimit dhe informacion në lidhje me certifikatën;

g) përmbledhjen e objektivit të sigurisë së produktit TIK të dorëzuar për certifikim;

gj) kur është e disponueshme, markën ose etiketën e lidhur me skemën;

h) bibliografinë.

4. Përmbledhja ekzekutive është një përmbledhje e shkurtër e të gjithë raportit të certifikimit. Përmbledhja ekzekutive siguron një pasqyrë të qartë dhe të përmbledhur të rezultateve të vlerësimit dhe përfshin informacionin si më poshtë vijon:

a) emrin e produktit TIK të vlerësuar, numërimin e përbërësve të produktit që është pjesë e vlerësimit dhe versionin e produktit TIK;

b) emrin e ITSEF i cili ka kryer vlerësimin dhe, sipas rastit, listën e nënkontraktorëve;

c) datën e përfundimit të vlerësimit;

ç) referencën në raportin teknik të vlerësimit të krijuar nga ITSEF;

d) përshkrimin e shkurtër të rezultateve të raportit të certifikimit, duke përfshirë:

i. versionin dhe nëse është e zbatueshme nxjerrjen e kritereve të përbashkëta të aplikuara në vlerësim;

ii. paketën e garantimit të kritereve të përbashkëta dhe komponentët e garantimit të sigurisë duke përfshirë nivelin AVA_VAN të aplikuar gjatë vlerësimit dhe nivelin përkatës të sigurisë sipas përcaktimeve në nenin 8 të vendimit të cilit i referohet certifikata;

iii. funksionalitetin e sigurisë së produktit TIK të vlerësuar;

iv. një përmbledhje të kërcënimeve dhe politikave të sigurisë organizative të adresuara nga produkti TIK i vlerësuar;

v. kërkesat e veçanta të konfigurimit;

vi. supozimet për mjedisin operativ;

vii ku është e zbatueshme, ekzistencën e një procedure të miratuar të menaxhimit të korrigjimit (*patch*) të miratuar në përputhje me aneksin IV.4;

viii.deklaratat e mohimit të përgjegjësisë.

5. Produkti TIK i vlerësuar të identifikohet qartë, duke përfshirë informacionin si më poshtë vijon:

a) emrin e produktit TIK të vlerësuar;

b) një numërim të përbërësve të produktit TIK që janë pjesë e vlerësimit;

c) numrin e versionit të përbërësve të produktit TIK;

ç) identifikimin e kërkesave shtesë për mjedisin operativ të produktit TIK të certifikuar;

d) emrin dhe informacionin e kontaktit të zotëruesit të certifikatës;

dh) ku është e zbatueshme, procedura e menaxhimit të korrigjimit (*patch*) të përfshirë në certifikatë;

e) lidhjen (*link*) në faqen e internetit të mbajtësit të certifikatës ku ofrohet informacion shtesë për sigurinë kibernetike për produktin TIK të certifikuar sipas përcaktimeve me nenin 10 të vendimit.

6. Informacioni i përfshirë në këtë seksion është i saktë për të siguruar një paraqitje të plotë dhe të saktë të produktit TIK që mund të ripërdoret në vlerësimet e ardhshme.

7. Seksioni i politikës së sigurisë përmban përshkrimin e politikës së sigurisë së produktit TIK dhe politikat ose rregullat që produkti TIK i vlerësuar zbaton. Në të përfshin një përshkrim të politikave si më poshtë vijon:

a) politikën e trajtimit të vulnerabiliteve të zotëruesit të certifikatës;

b) politikën e vazhdimësisë së garantimit të sigurisë së zotëruesit të certifikatës.

8. Kur është e zbatueshme, politika mund të përfshijë kushtet lidhur me përdorimin e një procedure të menaxhimit të korrigjimit (*patch)* gjatë vlefshmërisë së certifikatës.

9. Seksioni për supozimet dhe sqarimin e fushës së veprimit përmban informacion shterues në lidhje me rrethanat dhe objektivat që lidhen me përdorimin e synuar të produktit, sipas përcaktimeve në shkronjën c) të pikës 1, të nenit 7 të vendimit. Informacioni përfshin si më poshtë:

a) supozimet mbi përdorimin dhe vendosjen e produktit TIK në formën e kërkesave minimale, të tilla si instalimi dhe konfigurimi i duhur si dhe kërkesat e harduerit që plotësohen;

b) supozimet mbi mjedisin për funksionimin e përputhshëm të produktin TIK.

10. Informacioni i renditur në pikën 9 të aneksit V.1 është i kuptueshëm për t'i lejuar përdoruesit të produktit TIK të certifikuar të marrin vendime të informuara për rreziqet që lidhen me përdorimin e tij.

11. Seksioni i informacionit të arkitekturës përfshin një përshkrim të nivelit të lartë të produktit TIK dhe përbërësve kryesorë të tij në përputhje me projektimin e nënsistemeve ADV_TDS të kritereve të përbashkëta.

12. Një listë e plotë e informacionit për sigurinë kibernetike të produktit TIK sigurohet sipas përcaktimeve me nenin 10 të vendimit. Dokumentacioni përkatës shënohet me numrat e versionit.

13. Seksioni i testimit të produktit TIK përfshin informacionin si më poshtë vijon:

a) emrin dhe pikën e kontaktit të organit i cili ka lëshuar certifikatën, duke përfshirë autoritetin kombëtar të certifikimit të sigurisë kibernetike;

b) emrin e ITSEF-t i cili ka kryer vlerësimin, kur është i ndryshëm nga organi certifikues;

c) një identifikim të komponentëve të sigurisë të përdorura nga standardet e referuara në nenin 3 të vendimit;

ç) versionin e dokumentit Teknik të më të fundit dhe kriteret e vlerësimit të sigurisë të përdorura në vlerësim;

d) cilësimet dhe konfigurimi i plotë dhe i saktë i produktit TIK gjatë vlerësimit, duke përfshirë shënimet operacionale dhe vëzhgimet nëse janë të disponueshme;

dh) çdo profil i mbrojtjes i përdorur, duke përfshirë informacionin si më poshtë vijon:

i. Autorin e profilit të mbrojtjes;

ii. emrin dhe identifikuesin e profilit të mbrojtjes;

iii. identifikuesin e certifikatës së profilit të mbrojtjes;

iv. emrin dhe detajet e kontaktit të organit certifikues dhe ITSEF-it të përfshirë në vlerësimin e profilit të mbrojtjes;

v. paketat e garantimit të sigurisë të kërkuara për një produkt në përputhje me profilin e mbrojtjes.

14. Rezultatet e vlerësimit dhe informacioni në lidhje me seksionin e certifikatës përfshijnë informacionin si më poshtë vijon:

a) konfirmimin e nivelit të arritur të sigurisë sipas përcaktimeve në nenin 4 dhe 8 të vendimi;

b) kërkesat e sigurisë në standardet sipas

përcaktimeve në nenin 3 të vendimit që produkti ose profili i mbrojtjes i TIK përmbush, duke përfshirë nivelin AVA_VAN;

c) përshkrimin e detajuar të kërkesave të sigurisë, si dhe detajet si produkti i plotëson secilën prej tyre;

ç) datën e lëshimit dhe periudhën e vlefshmërisë së certifikatës;

d) identifikuesi unik i certifikatës.

15. Objektivi i sigurisë përfshihet në raportin e certifikimit ose referohet dhe përmblidhet në raportin e certifikimit dhe pajiset me raportin e certifikimit që lidhet me të për qëllime publikimi.

16. Objektivi i sigurisë mund të filtrohet në përputhje me aneksin VI.2.

17. Marka ose etiketa e lidhur me skemën mund të përfshihet në raportin e certifikimit në përputhje me rregullat dhe procedurat e përcaktuara në nenin 13 të vendimit.

18. Seksioni i bibliografisë përfshin referenca për dokumentet e përdorura në përpilimin e raportit të certifikimit. Ky informacion përfshin të paktën si më poshtë vijon:

a) kriteret e vlerësimit të sigurisë, dokumentet teknike më të fundit dhe specifikimet përkatëse të përdorura si dhe versioni i tyre;

b) raportin teknik të vlerësimit;

c) raportin teknik të vlerësimit për vlerësimin e përbërë, kur është e zbatueshme;

ç) dokumentacionin teknik të referencës;

d) dokumentacionin e zhvilluesit të përdorur në përpjekjet e vlerësimit.

19. Për të garantuar riprodhueshmërinë e vlerësimit, dokumentacioni i referuar duhet të identifikohet në mënyrë unike me datën e duhur të lëshimit dhe numrin e duhur të versionit.

V.2 Filtrimi i një objektivi sigurie për publikim

1. Objektivi i sigurisë të përfshihet në raportin e certifikimit, në përputhje me pikën 1 të aneksit VI.1, mund të filtrohet nga heqja ose përshkrimi i informacionit teknik të pronarit.

2. Objektivi sigurisë i filtruar i cili rezulton është një paraqitje reale e versionit të tij të plotë dhe origjinal. Objektivi i sigurisë i filtruar nuk heq informacionin i cili është i nevojshëm për të kuptuar veçoritë e sigurisë të objektit të vlerësimit dhe qëllimin e vlerësimit.

3. Përmbajtja e objektivit të sigurisë të filtruar është në përputhje me kërkesat minimale si më poshtë vijon:

a) prezantimi i tij nuk filtrohet pasi nuk përfshin informacion pronësor në përgjithësi;

b) objektivi i sigurisë i filtruar ka një identifikues unik që është i ndryshëm nga versioni i tij i plotë origjinal;

c) përshkrimi i objektit të vlerësimit mund të reduktohet pasi mund të përfshijë informacion pronësor dhe të detajuar në lidhje me projektimin e objektit të vlerësimit, i cili nuk publikohet;

ç) Përshkrimi i mjedisit të sigurisë të objektit të vlerësimit (supozimet, kërcënimet, politikat e sigurisë organizative) nuk reduktohen, për aq sa ky informacion është i nevojshëm për të kuptuar qëllimin e vlerësimit;

d) objektivat e sigurisë nuk reduktohen pasi i gjithë informacioni duhet të bëhet publik për të kuptuar synimin e objektivit të sigurisë dhe objektit të vlerësimit;

dh) të gjitha kërkesat e sigurisë bëhen publike. Shënimet e aplikacionit mund të japin informacion se si janë përdorur kërkesat funksionale të kritereve të përbashkëta të përmendura në nenin 3 të vendimit për të kuptuar objektivin e sigurisë;

e)specifikimi i përmbledhjes së objektit të vlerësimit përfshin të gjitha funksionet e sigurisë të objektit të vlerësimit, por informacioni pronësor shtesë mund të filtrohet;

ë) përfshihen referencat për profilet e mbrojtjes të zbatuara për objektin e vlerësimit;

f) arsyetimi mund të filtrohet për të hequr informacionin pronësor .

4. Edhe nëse objektivi i sigurisë i filtruar nuk vlerësohet zyrtarisht në përputhje me standardet e vlerësimit të përmendura në nenin 3 të vendimit, organi certifikues siguron që përputhet me objektivin e plotë dhe të vlerësuar të sigurinë, dhe i referohet objektivit të plotë dhe të filtruar të sigurisë, në raportin e certifikimit.

ANEKSI VI: Qëllimi dhe përbërja e ekipit për vlerësimet e oponencave

VI.1 Objektivi i vlerësimit të oponencave

1. Tipet e vlerësimeve të oponencës janë si më poshtë vijon:

a) Tipi 1: kur një organ certifikues kryen aktivitete certifikimi në nivelin AVA_VAN.3;

b) Tipi 2: kur një organ certifikues kryen

aktivitete certifikimi në lidhje me një fushë teknike të listuar si dokumente teknike më të fundit sipas përcaktimeve në aneksin I;

c) Lloji 3: kur një organ certifikues kryen aktivitete certifikimi mbi nivelin AVA_VAN.3 duke përdorur një profil të mbrojtjes të listuar si dokumente teknike më të fundit sipas përcaktimeve në aneksin II ose III.

2. Organi certifikues i vlerësuar nga ekipi i vlerësimit të oponencës paraqet listën e produkteve TIK të certifikuara të cilat mund të jenë kandidatë për rishikim nga ekipi i vlerësimit të oponencës, sipas përcaktimeve në rregullat e mëposhtme:

a) produktet kandidate mbulojnë fushën teknike të autorizimit të organit certifikues, nga të cilat të paktën dy vlerësime të produkteve të ndryshme në nivelin e sigurisë "të lartë" do të analizohen përmes vlerësimit të oponencës, dhe një profil të mbrojtjes nëse organi certifikues ka lëshuar certifikatën në nivelin e sigurisë "të lartë";

b) për një vlerësim të oponencës të tipit 2, organi certifikues dorëzon të paktën një produkt për fushë teknike dhe për ITSEF-in përkatës;

c) për një vlerësim të oponencës të tipit 3, të paktën një produkt kandidat vlerësohet në përputhje me profilet e mbrojtjes të zbatueshme dhe përkatëse.

VI.2 Ekipi i vlerësimit të oponencës

1. Ekipi i vlerësimit të oponencës përbëhet nga të paktën dy ekspertë, secili i përzgjedhur nga një organ i ndryshëm certifikimi nga shtete të ndryshme anëtare që lëshon certifikata në nivelin e sigurisë "të lartë". Ekspertët të demonstrojnë ekspertizën përkatëse në standardet e përmendura në nenin 3 të vendimit dhe dokumentet teknike më të fundit që janë në objektivin e vlerësimit të oponencës.

2. Për një vlerësim e oponencës të tipit 2, anëtarët e ekipit zgjidhen nga organet certifikuese të autorizuara për fushën teknike përkatëse.

3. Çdo anëtar i ekipit të vlerësimit të oponencës duhet të ketë të paktën dy vjet përvojë në kryerjen e aktiviteteve të certifikimit në një organ certifikues;

4. Për një vlerësim oponence të tipit 2 ose 3, çdo anëtar i ekipit të vlerësimit duhet të ketë të paktën dy vjet përvojë në kryerjen e aktiviteteve të certifikimit në atë fushë teknike ose profilin e mbrojtjes dhe ekspertizë të provuar si dhe pjesëmarrje në autorizimin e një ITSEF-i.

5. Autoriteti kombëtar i certifikimit të sigurisë kibernetike i cili monitoron dhe mbikëqyr organin certifikues të vlerësuar nga ekipi vlerësimit të oponencës dhe të paktën një autoritet kombëtar certifikues të sigurisë kibernetike, organi certifikues i të cilit nuk i nënshtrohet vlerësimit të oponencës marrin pjesë në vlerësimin e oponencës si vëzhgues. ENISA gjithashtu mund të marrë pjesë në vlerësimin e oponencës si vëzhgues.

6. Organit certifikues të vlerësuar nga ekipi i vlerësimit të oponencës i bëhet me dije përbërja e ekipit të vlerësimit të oponencës. Në raste të justifikuara, ai mund të kundërshtojë përbërjen e ekipit të vlerësimit te oponencës dhe të kërkojë rishikimin e tij.

ANEKSI VII: Përmbajtja e një certifikate sipas skemës

Një certifikatë përmban të paktën:

a) një identifikues unik i vendosur nga organi certifikues i cili lëshon certifikatën;

b) informacion në lidhje me produktin TIK të certifikuar ose profilin e mbrojtjes dhe zotëruesin e certifikatës, duke përfshirë:

i. emrin e produktit TIK ose të profilin e mbrojtjes dhe, kur është e zbatueshme, të objektit të vlerësimit;

ii. tipin e produktit TIK ose profilin e mbrojtjes dhe, kur është e zbatueshme, të objektit të vlerësimit;

iii. versionin e produktit TIK ose profilin e mbrojtjes;

iv. emrin, adresën dhe informacionin e kontaktit të zotëruesit të certifikatës;

v. lidhjen në faqen e internetit të zotëruesit të certifikatës që përmban informacionin shtesë të sigurisë kibernetike sipas përcaktimeve në nenin 10 të vendimit;

c) informacion në lidhje me vlerësimin dhe certifikimin e produktit TIK ose profilin e mbrojtjes, duke përfshirë:

i. emrin, adresën dhe informacionin e kontaktit të organit certifikues që ka lëshuar certifikatën;

ii. kur është i ndryshëm nga organi certifikues, emrin i ITSEF-it që ka kryer vlerësimin;

iii. emrin e autoritetit kombëtar përgjegjës për certifikimin e sigurisë kibernetike;

iv. një referencë për këtë vendim;

v. një referencë për raportin e certifikimit të lidhur me certifikatën e përmendur në aneksin V;

vi. nivelin e sigurisë të zbatueshëm sipas përcaktimeve në nenin 4 të vendimit;

vii. një referencë për versionin e standardeve të përdorura për vlerësimin, sipas përcaktimeve në nenin 3 të vendimit;

viii. identifikimin e nivelit të sigurisë ose paketës së specifikuar në standardet e përmendura në nenin 3 të vendimit dhe në përputhje me aneksin VIII, duke përfshirë komponentët e sigurisë të përdorura në nivelin që mbulon AVA_VAN;

ix. aty ku është e zbatueshme, referencë për një ose më shumë profile të mbrojtjes me të cilat përputhet produkti TIK ose profili i mbrojtjes;

x. data e lëshimit;

xi. periudha e vlefshmërisë së certifikatës.

d) markën dhe etiketën të lidhur me certifikatën sipas përcaktimeve në nenin 13.

ANEKSI VIII: Deklarata e paketës së garantimit të sigurisë

1. Ndryshe nga përkufizimet në Kriteret e Përbashkëta, një shtesë:

a) nuk shënohet shkurt me "+";

b) detajohet nga një listë e të gjithë komponentëve përkatës;

c) përshkruhet në detaje në raportin e certifikimit.

2. Niveli i sigurisë i konfirmuar në një certifikatë mund të plotësohet nga niveli i sigurisë së vlerësimit sipas përcaktimeve në nenin 3 të vendimit.

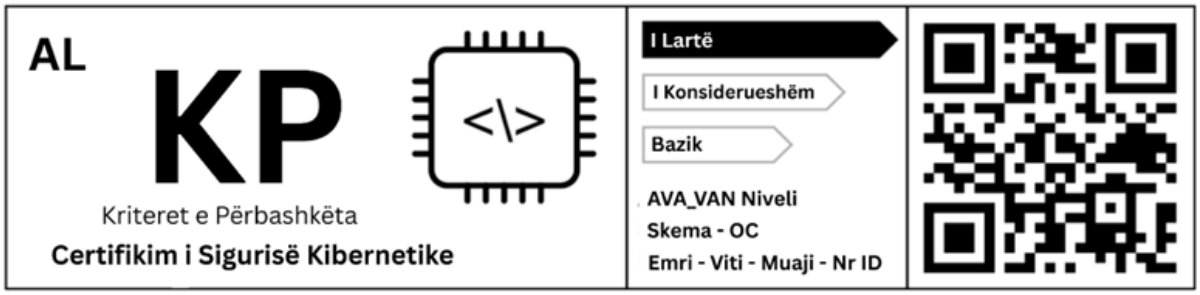
3. Nëse niveli i sigurisë i konfirmuar në një certifikatë nuk i referohet një shtese, certifikata tregon një nga paketat e mëposhtme:

a) "paketën specifike të garantimit të sigurisë;

b) "paketa e garantimit të sigurisë në përputhje me një profil të mbrojtjes" në rast se i referohet një profili të mbrojtjes pa një nivel sigurie të vlerësimit.

ANEKSI IX: Marka dhe etiketa

1. Forma e markës dhe etiketës:



2. Nëse marka dhe etiketa zvogëlohen ose zmadhohen, të respektohen përmasat e dhëna në figurën e mësipërme.

3. Kur janë të pranishme fizikisht, marka dhe etiketa duhet të kenë të gjerësi paktën 5 mm.

ANEKSI X: Kriteret, dokumentacioni dhe procedura për autorizimin e organeve të vlerësimit të konfomitetit si organi certifikues dhe ITSEF

1 Kriteret dhe dokumentacioni për autorizimin e organeve certifikuese

1.1. Subjekti që aplikon pranë organit kombëtar për certifikimin e sigurisë kibernetike me qëllim marrjen e autorizimit si organ certifikues duhet të plotësojë kriteret si më poshtë vijon:

1.1.1. Kriteret ligjore dhe financiare:

a) të jenë të regjistruar pranë Qendrës Kombëtare të Biznesit si person juridik me status aktiv;

b) të mos jenë në ndjekje penale;

c) të mos jenë në proces gjyqësor lidhur me ushtrimin e aktivitetit;

ç) të mos jenë i dënuar nga organet gjyqësore;

d) të mos kenë detyrime tatimore të pa paguara;

dh) të mos jenë në proces falimentimi apo likuidimi;

e) të jenë të pavarur nga ana ligjore, financiare dhe vendimarrja nga organizata ose produktet TIK, shërbimet e TIK ose proceset TIK që vlerësojnë.

ë) të mos jenë në proces ekzekutimi të detyrueshëm për detyrime pasurore të pashlyera në zyrën e përmbarimit gjyqsor;

1.1.2 Kriteret teknike dhe organizative:

a) të jetë i akreditуar nga autoriteti përgjegjës për akreditimin në Republikën e Shqipërisë apo një trupë akredituese nga një vend anëtar i Bashkimit Evropian dhe që ka marrëveshje të njohjes reciproke me Organizatën Evropiane të Akreditimit për këtë fushë akreditimi;

b) të paraqesë kategoritë e produkteve dhe profilet e mbrojtjes për të cilat kërkon autorizim;

c) të ketë strukturën me kapacitete, kualifikime, dhe kompetenca të duhura sipas kërkesave të përcaktuara në standardin ISO/IEC 19896, për kryerjen e aktiviteteve të certifikimit të sigurisë kibernetike sipas përcaktimeve të skemës.

Në strukturë duhet të ketë të paktën 10 (dhjetë) ekspertë me certifikime ndërkombëtare ose 20 (njëzet) vite eksperiencë në fushën e teknologjisë ose akademike, të lidhura me Internet of Things (IoT) dhe sigurinë kibernetike.

ç) të provojë ekspertizën e duhur për certifikimin e sigurisë kibernetike të një produkti TIK ose profili të mbrojtjes, duke bashkëpunuar me një ITSEF dhe një subjekt të interesuar për pjesëmarrjen në një proces certifikimi pilot të sigurisë kibernetike;

d) të provojë kapacitetet dhe aftësitë e duhura për menaxhimin e vulnerabiliteteve dhe ndërmarrjen e korrigjimeve pas lëshimit të certifikatës, duke paraqitur të dhëna mbi çështjet e trajtuara;

dh) të demonstrojë vazhdimësinë e garantimit të sigurisë;

e) të ketë vendosur marrëdhënie bashkëpunimi me një ITSEF të autorizuar, të formalizuar në mënyrë të detajuar;

ë) të demonstrojë kompetencat e duhura për mbrojtjen e informacionit, përmes zbatimit të masave teknike dhe organizative, kryerjes së vlerësimit të rrezikut dhe analizës së kërcënimeve, si dhe ruajtjen e integritetit gjatë përpunimit të të dhënave konfidenciale dhe sensitive;

f) të ketë sistem të menaxhimit të cilësisë që garanton se politikat, procedurat dhe masat janë zbatuar dhe audituar rregullisht, si dhe i janë nënshtruar ciklit të përmirësimit të vazhdueshëm.

g) aftësi për mbrojtjen dhe shkëmbimin e informacionit;

1.2 Dokumentet që duhet të dorëzojë subjekti që aplikon pranë organit kombëtar të certifikimit të sigurisë kibernetike për autorizim si organ certifikues në përputhje me kriteret e pikës 1.1 të këtij Aneksi, janë si më poshtë vijon:

1.2.1 Dokumentet ligjore dhe financiare:

a) ekstraktin nga QKB-ja, ku të vërtetohet se shoqëria është me status aktiv;

b) vërtetim të lëshuar nga Prokuroria pranë Gjykatave të Juridiksionit përkatës se ndaj subjektit nuk është filluar çështje penale që ka lidhje me aktivitetin;

c) vërtetim të lëshuar nga Gjykata e Juridiksionit përkatës se nuk është në proces gjyqësor lidhur me aktivitetin;

ç) vërtetim të gjendjes gjyqësore që tregon se subjekti nuk është i dënuar;

d) vërtetim nga organet tatimore ku subjekti është i regjistruar, ku vërtetohet se nuk ka detyrime tatimore të pa paguara;

dh) statutin dhe aktin e themelimit të shoqërisë;

e) vërtetim nga zyra përmbarimore që subjekti nuk është në proces ekzekutimi të detyrueshëm pasuror;

ë) vërtetim që subjekti nuk është në procedura falimentimi;

1.2.2 Dokumentet teknike dhe organizative:

a) certifikatën e akreditimit të lëshuar nga autoriteti përgjegjës për akreditimin në Republikën e Shqipërisë ose sipas marrëveshjes së njohjes reciproke me Organizatën Evropiane të Akreditimit për këtë fushë akreditimi;

b) një dokument të nënshkruar ku përcaktohen kategoritë e produkteve të teknologjisë së informacionit dhe çdo profil të mbrojtjes për të cilat kërkohet autorizim;

c) strukturën organizative, me rolet, përgjegjësitë dhe kompetencat sipas standardit ISO/IEC 19896, me informacion të detajuar për çdo njësi organizative si më poshtë vijon:

i. përshkrimi i aktiviteteve të njësive organizative;

ii. përshkrimi i punës për punonjësit;

iii. aftësitë dhe kualifikimet profesionale të punonjësve;

iv. kompetencat e duhura të kërkuara të njësive organizative.

ç) përshkrim i detajuar i procesit të certifikimit pilot të sigurisë kibernetike për një produkt TIK ose profil të mbrojtjes, duke listuar hapat dhe aktivitetet e vlerësimit dhe certifikimit, planin e certifikimit, raportin e certifikimit duke përfshirë planin e vlerësimit dhe raportin e vlerësimit teknik të vënë në dispozicion nga ITSEF i autorizuar, si dhe një certifikatë pilot;

d) procedura e menaxhimit të vulnerabiliteteve si dhe regjistri i vulnerabiliteve të trajtuara me sukses për subjektet që kanë ushtruar më parë veprimtarinë brenda 2 (dy) viteve më të fundit;

dh) procedurën e vazhdimësisë së garantimit të sigurisë sipas skemës;

e) marrëveshjen e bashkëpunimit duke përfshirë kontratën e nënshkruar të detajuar me ITSEF-in e autorizuar;

ë) dokumentin me masat teknike dhe organizative sipas standardit ISO/IEC 27001;

f) raportin e fundit të auditit të brendshëm, bashkë me listën e veprimeve korrigjuese dhe parandaluese që dëshmon vlerësimin periodik dhe adresimin e gjetjeve;

g) procedurat për ruajtjen dhe administrimin e informacionit sipas ISO/IEC 27001.

2 Kriteret dhe dokumentacioni për autorizimin e ITSEF

2.1 Subjekti që aplikon pranë organit kombëtar për certifikimin e sigurisë kibernetike me qëllim marrjen e autorizimit si ITSEF duhet të plotësojë kriteret si më poshtë vijon:

2.1.1 Kriteret ligjore dhe financiare:

a) të jenë të regjistruar pranë Qendrës Kombëtare të Biznesit si person juridik me status aktiv;

b) të mos jenë në ndjekje penale;

c) të mos jenë në proces gjyqësor lidhur me ushtrimin e aktivitetit;

ç) të mos jenë i dënuar nga organet gjyqësore;

d) të mos kenë detyrime tatimore të pa paguara;

dh) të mos jenë në proces falimentimi apo likuidimi;

e) të jenë të pavarur nga ana ligjore, financiare dhe vendimmarrja nga organizata ose produktet TIK, shërbimet e TIK ose proceset TIK që vlerësojnë.

ë) të mos jenë në proces ekzekutimi të detyrueshëm për detyrime pasurore të pashlyera në zyrën e përmbarimit gjyqësor;

2.1.2 Kriteret teknike dhe organizative:

a) të jetë i akreditуar nga autoriteti përgjegjës për akreditimin në Republikën e Shqipërisë apo një trupë akredituese nga një vend anëtar i Bashkimit Evropian dhe që ka marrëveshje të njohjes reciproke me Organizatën Evropiane të Akreditimit për këtë fushë akreditimi;

b) të paraqesë kategoritë e produkteve dhe profilet e mbrojtjes për të cilat kërkon autorizim;

c) të ketë strukturën organizative me kapacitete, kualifikime, dhe kompetenca të duhura sipas kërkesave të përcaktuara në standardin ISO/IEC 19896, për kryerjen e aktiviteteve të vlerësimit teknik duke përfshirë kalibrim dhe testim sipas përcaktimeve të skemës.

Në strukturë duhet të ketë të paktën 5 (pesë) ekspertë me certifikime ndërkombëtare sipas kompetencave të nevojshme, si dhe me më shumë se 5 (pesë) vite eksperiencë në penetration testing, vlerësim risku, qeverisje dhe monitorim në standarde ndërkombëtare, analizë SOC, menaxhim incidenti ose analizë forensics.

ç) të provojë ekspertizën e duhur për vlerësimin e një produkti TIK ose profili të mbrojtjes, në bashkëpunim me një organ certifikues dhe një subjekt të interesuar për pjesëmarrjen në një proces vlerësimi pilot të sigurisë kibernetike

d) të ketë ambiente laboratorike me hapësirë të mjaftueshme, pajisje teknologjike të 5 (pesë) viteve të fundit, si dhe software nga kompani të mirënjohura kombëtare ose ndërkombëtare sipas vlerësimit të AKSK.

dh) të provojë se zotëron kompetencat e duhura teknike dhe i përditëson ato, në fushat si më poshtë vijon:

i. përdorimi i inteligjencës së kërcënimeve dhe kryerja e vlerësimeve të riskut;

ii. zbatimi i metodologjisë të vlerësimit në nivel sigurie "i lartë", me një qasje të bazuar në risk, për testimin e qëndrueshmërisë ndaj sulmeve kibernetike të sofistikuara;

iii. aftësia për të përshtatur sulmet kibernetike në metodologji konkrete vlerësimi dhe përmirësimi i saj;

iv. llogaritja e skenarit të sulmit sipas standardit ISO/IEC 18045 dhe dokumenteve teknike më të fundit sipas përcaktimeve në aneksin I të këtij vendimi;

v. ekspertizë për përdorimin e mjeteve të zhvillimit, analizës dhe sulmit si dhe sistemeve IT të nevojshme për aktivitetet e vlerësimit për nivelin e sigurisë "i lartë";

vi. përgatitja e përshkrimeve teknike për aktivitetet e vlerësimit;

vii. ekspertizë në algoritme kriptografike dhe protokolle si dhe vlerësimin e tyre;

viii. njohuri specifike për llojin e produktit të përfshirë në fushën e autorizimit, duke përfshirë proceset e zhvillimit, mjedisin operacional dhe dobësitë e njohura;

ix. aftësi për të përzgjedhur dhe aplikuar teknikat dhe mjetet e analizës së kodit burim dhe penetration testing (Black-box, Grey-box, Crystal Box ose White-box);

x. aftësi në përdorimin e mjeteve me burim të hapur dhe AI për testim, si dhe mjeteve harduerike për analizë;

xi. kryerja e një procesi reverse-engineering të avancuar;

xii. monitorimi i proceseve të vlerësimit për produktet TIK dhe profilet e mbrojtjes, dhe kur është e aplikueshme, për fushat teknike;

xiii. hartimi i raportit teknik të vlerësimit;

xiv. zhvillimi i procedurave për administrimin, mirëmbajtjen dhe ruajtjen e dokumentacionit;

xv. aftësi teknike për të mbështetur organin certifikues në trajtimin e vulnerabiliteteve;

xvi. aftësi për mbrojtjen dhe shkëmbimin e informacionit konfidencial dhe sensitiv;

e) të provojë se ka kompetencat e duhura për mbrojtjen e informacionit, përmes zbatimit të masave teknike dhe organizative, kryerjes së vlerësimit të rrezikut dhe analizës së kërcënimeve, si dhe ruajtjen e integritetit gjatë përpunimit të të dhënave konfidenciale;

ë) të ketë sistem të menaxhimit të cilësisë që garanton se politikat, procedurat dhe masat janë zbatuar dhe audituar rregullisht, si dhe i janë nënshtruar ciklit të përmirësimit të vazhdueshëm.

2.2 Dokumentet që duhet të dorëzojë subjekti që aplikon pranë organit kombëtar të certifikimit të sigurisë kibernetike për autorizim si ITSEF në përputhje me kriteret, janë si më poshtë vijon:

2.2.1 Dokumentet ligjore dhe financiare:

a) ekstraktin nga QKB-ja, ku të vërtetohet se shoqëria është me status aktiv;

b) vërtetim të lëshuar nga Prokuroria pranë Gjykatave të Juridiksionit përkatës se ndaj subjektit nuk është filluar çështje penale që ka lidhje me aktivitetin;

c) vërtetim të lëshuar nga Gjykata e Juridiksionit përkatës se nuk është në proces gjyqësor lidhur me aktivitetin;

ç) vërtetim të gjendjes gjyqësore që tregon se subjekti nuk është i dënuar;

d) vërtetim nga organet tatimore ku subjekti është i regjistruar, ku vërtetohet se nuk ka detyrime tatimore të pa paguara;

dh) stautin dhe aktin e themelimit të shoqërisë;

e) vërtetim nga zyra përmbarimore që subjekti nuk është në proces ekzekutimi të detyueshëm pasuror;

ë) vërtetim që subjekti nuk është në procedura falimentimi;

2.2.2 Dokumentet teknike dhe organizative:

a) certifikatën e akreditimit të lëshuar nga autoriteti përgjegjës për akreditimin në Republikën e Shqipërisë ose sipas marrëveshjes së njohjes reciproke me Organizatën Evropiane të Akreditimit për këtë fushe akreditimi;

b) një dokument i nënshkruar ku përcaktohen kategoritë e produkteve të teknologjisë së informacionit dhe çdo profil mbrojtjeje për të cilat kërkohet autorizim;

c) strukturën organizative, me rolet, përgjegjësitë dhe kompetencat sipas standardit ISO/IEC 19896, me informacion të detajuar për çdo njësi organizative si më poshtë vijon:

i. përshkrimi i aktiviteteve të njësisë organizative;

ii. përshkrimi i punës për punonjësit;

iii. aftësitë dhe kualifikimet profesionale të punonjësve;

iv. kompetencat e duhura të kërkuara të njësive organizative.

ç) përshkrim i detajuar i procesit të vlerësimit pilot për një produkt TIK ose profil të mbrojtjes, duke e detajuar raportin e vlerësimit pilot sipas Skemës.

d) planimetrinë e ambientit laboratorik, si dhe listën e pajisjeve teknologjike dhe software me dokumentacionin përkatës.

dh) përshkrimi i kompetencave që zotëron me dokumentacionin përkatës si më poshtë vijon:

i. raport vlerësimi të riskut dhe evidenca që përdoret inteligjenca e kërcënimeve kibernetike;

ii. dokument i miratuar mbi rezultatet e një rasti vlerësimi në nivel sigurie "i lartë", me një qasje të bazuar në risk, për testimin e qëdrueshmërisë ndaj sulmeve kibernetike;

iii. metodologji vlerësimi e përshtatur bazuar në sulme kibernetike;

iv. raporti i një skenari sulmi të llogaritur;

v. lista e mjeteve të zhvillimit, analizës dhe sulmit si dhe sistemeve IT të nevojshme për aktivitetet e vlerësimit si dhe evidenca mbi kualifikimin e punonjësve për t'i përdorur;

vi. përshkrimet teknike për aktivitetet e vlerësimit;

vii. një dokument vlerësimi mbi algoritmet kriptografike dhe protokollet e përdorura;

viii. certifikimet dhe trajnimet e stafit mbi produket e përfshira në fushën e autorizimit, proceset dhe mjedisin operacional;

ix. raportet mbi aplikimin e teknikave, mjeteve të analizës së kodit burim dhe penetration testing (*Black-box, Grey-box, Crystal Box* ose *White-box*);

x. lista e mjeteve me burim të hapur dhe AI për testim, si dhe mjeteve harduerike për analizën e përdorur, si dhe evidenca mbi kualifikimin e punonjësve për t'i përdorur;

xi. një raport për një rast kur është kryer *reverse-engineering*;

xii. raport monitorimi të proceseve të vlerësimit për produktet TIK dhe profilet e mbrojtjes, dhe kur është e aplikueshme, për fushat teknike;

xiii. raporti teknik i vlerësimit në gjuhën shqipe;

xiv. procedurë e miratuar për administrimin, mirëmbajtjen dhe ruajtjen e dokumentacionit;

xv. raport mbi procedurën e ndjekur dhe masat e marra në një rast konkret për trajtimin e vulnerabiliteteve në mbështetje të organit certifikues;

xvi. procedurat për ruajtjen dhe administrimin e informacionit sipas ISO/IEC 27001;

dh) masat teknike dhe organizative sipas standardit ISO/IEC 27001;

e) raportin e fundit të auditit të brendshëm, bashkë me listën e veprimeve korrigjuese dhe parandaluese që provon vlerësimin periodik dhe adresimin e gjetjeve.

3 Procedurat dhe afatet e shqyrtimit të dokumentacionit për marrjen e autorizimit nga organet e vlerësimit të konformitetit

3.1 Dorëzimi i dokumentacionit nga organet e vlerësimit të konformitetit (OVK) të përmendura në pikën 1.1 dhe 2.1 të këtij aneksi bëhet nëpërmjet postës zyrtare ose dorazi pranë organit përgjegjës për certifikimin e sigurisë kibernetike.

3.2 Dokumentet e përmendura në pikën 1.2 dhe 2.2 të këtij aneksi duhet të jenë origjinale ose kopje të njësuara me origjinalin dhe të jenë të lëshuara brenda afateve të vlefshmërisë.

3.3 Organi përgjegjës për certifikimin e sigurisë kibernetike shqyrton brenda 30 (tridhjetë) ditëve dokumentacionin e dorëzuar nga OVK-të, ku në rast pasaktësish apo mungese të dokumentacionit i njofton me shkrim OVK-në për pasaktësitë apo mangësitë si dhe afatin 15 (pesëmbëdhjetë) ditor për plotësimin e konstatimeve në dokumentacion.

3.4 Organi përgjegjës për certifikimin e sigurisë kibernetike për raste të arsyeshme zgjat afatin e shqyrtimit të dokumentacionit të dorëzuar nga OVK-të me 30 (tridhjetë) dite.

3.5 Në rastin kur konfirmohet se është dorëzuar gjithë dokumentacioni i nevojshëm, organi përgjegjës për certifikimin e sigurisë kibernetike i dërgon organit të vlerësimit të konformitetit një plan autorizimi. Plani i autorizimit përmban elementet si më poshtë vijon:

a) Vlerësimin e dokumentacionit për plotësinë dhe përmbajtjen;

b) Intervistat e strukturuara lidhur me aktivitetet e bashkëpunimit ndërmjet ITSEF-it dhe organit certifikues si dhe zbatimin e masave teknike dhe organizative;

c) Kur është e zbatueshme, çdo informacion tjetër të nevojshëm.

3.6 Në rastet kur për procedurën e autorizimit nevojiten dokumentacion ose sqarime shtesë, organi përgjegjës për certifikimin e sigurisë kibernetike i paraqet OVK-së kërkesën për vendosjen në

dispozicion të tyre si dhe planifikon takime nëse është e nevojshme.

3.7 Organi përgjegjës për certifikimin e sigurisë kibernetike harton raportin e autorizimit brenda një afati 15 (pesëmbëdhjetë) ditor nga përfundimi i shqyrtimit të dokumentacionit të dorëzuar nga OVK-ja.

3.8 Organi përgjegjës për certifikimin e sigurisë kibernetike kur konstaton plotësimin e kritereve sipas këtij aneksi, lëshon autorizimin për subjektin për ushtrimin e veprimtarisë si OVK, si dhe e njofton atë me shkrim duke i vendosur në dispozicion raportin e autorizimit brenda 7 (shtatë) ditësh.

3.9 Organi përgjegjës për certifikimin e sigurisë kibernetike kur konstaton pasaktësi apo mungesë të dokumentacionit të përmendur në këtë aneks edhe pas ezaurimit të afatit për përmbushjen e pasaktësive apo mangësive të konstatuara në dokumentacion apo vlerësim sipas këtij aneksi, vendos mosdhënien e autorizimit për OKV-në si dhe njofton këtë të fundit me shkrim duke i vendosur në dispozicion raportin e autorizimit.

3.10 OVK-ja pas marrjes së njoftimit për mosdhënien e autorizimit ka të drejtën e ankimit brenda 30 (tridhjetë) ditëve nga marrja dijeni për njoftim në gjykatën administrative.

3.11 Organi përgjegjës për certifikimin e sigurisë kibernetike pezullon autorizimin e dhënë OVK-së, në rastet si më poshtë vijon:

a) Në rast të konstatimit të mospërmbushjeve të kritereve nga OVK në bazë të të cilave i është dhënë autorizimi;

b) Në rast të tërheqjes, reduktimit ose pezullimit nga autoriteti përgjegjës për akreditimin te fushës së akreditimit për fushën të cilën ka marrë autorizimin;

c) Në rast të ndryshimeve të ndodhura në organin e vlerësimit të konformitetit që ndikojnë ndjeshëm në plotësimin e kërkesave për të cilat është autorizuar OVK dhe nevojitet një rivlerësim për rinovimin e autorizimit.

VENDIM
Nr. 814, datë 30.12.2025

PËR MIRATIMIN E PROCEDURAVE TË IDENTIFIKIMIT, KLASIFIKIMIT, PËRSHKALLËZIMIT DHE MENAXHIMIT TË KRIZËS KIBERNETIKE

Në mbështetje të nenit 100 të Kushtetutës dhe të pikës 9, të nenit 28, të ligjit nr. 25/2024, "Për sigurinë kibernetike", me propozimin e Kryeministrit, Këshilli i Ministrave

VENDOSI:

1. Miratimin e procedurave të identifikimit, klasifikimit, përshkallëzimit dhe menaxhimit të krizës kibernetike, sipas tekstit që i bashkëlidhet këtij vendimi dhe është pjesë përbërëse e tij.

2. Ngarkohen Autoriteti Kombëtar për Sigurinë Kibernetike, CSIRT-et sektoriale, CSIRT-et pranë operatorëve të infrastrukturave të informacionit dhe të gjitha strukturat e institucionet përgjegjëse, që kanë role dhe përgjegjësi specifike të përcaktuara në procedurën e identifikimit, klasifikimit, përshkallëzimit dhe menaxhimit të krizës kibernetike, për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

KRYEMINISTËR
Edi Rama

PROCEDURAT PËR IDENTIFIKIMIN, KLASIFIKIMIN, PËRSHKALLËZIMIN Dhe MENAXHIMIN E KRIZËS KIBERNETIKE

1. HYRJE

Rritja e përdorimit të teknologjive digjitale të informacionit e të komunikimit, si dhe e shërbimeve digjitale ka bërë që edhe kërcënimet ndaj sigurisë kibernetike të jenë gjithnjë e më të pranishme e të sofistikuara. Ky fenomen, tashmë global, nuk njeh kufij, duke e bërë menaxhimin e incidenteve dhe krizave kibernetike një sfidë të rëndësishme për të gjitha shtetet. Incidentet e sigurisë kibernetike mund të përfshijnë, që nga sulmet e thjeshta deri tek sulmet më të sofistikuara, me pasojë ndërprerjen e shërbimeve kritike, vjedhjen e informacionit sensitiv

apo shkatërrimin e infrastrukturave kritike dhe të rëndësishme të informacionit.

Pas një rritjeje të ndjeshme të sulmeve kibernetike, kuadri ligjor për menaxhimin dhe reagimin ndaj incidenteve kibernetike, në shkallë të gjerë me përshkallëzim në krizë kibernetike, është një instrument për të siguruar që Shqipëria të jetë e përgatitur për të përballuar çdo incident apo krizë të mundshme të sigurisë kibernetike, duke mbrojtur infrastrukturat kritike e të rëndësishme të informacionit dhe duke siguruar vazhdimësinë e shërbimeve kyçe. Për të siguruar një menaxhim të koordinuar dhe efikas të incidenteve në shkallë të gjerë dhe krizave kibernetike është e rëndësishme të përfshihen të gjithë aktorët relevantë, qeveria, institucione të pavarura, sektori privat dhe shoqëria civile. Nëpërmjet bashkëpunimit, koordinimit dhe trajnimit të vazhdueshëm në fushën e sigurisë kibernetike, do të bëhet e mundur që Shqipëria të përballet me sfidat e sigurisë kibernetike, si dhe të reagojë në mënyrë të shpejtë dhe efikase, me qëllim minimizimin e pasojave. Hartimi i kësaj procedure ka si qëllim krijimin e një kornize gjithëpërfshirëse e të strukturuar për identifikimin, klasifikimin, menaxhimin ndaj krizave të sigurisë kibernetike që mund të rrezikojnë funksionimin normal të shoqërisë dhe ekonomisë shqiptare.

Kapaciteti efektiv i menaxhimit të krizave kibernetike varet nga kapacitetet efektive në nivel strategjik politik, operacional dhe teknik, si dhe bashkëpunimit të ngushtë ndërmjet këtyre niveleve, ashtu siç theksohet në rekomandimin e Komisionit Evropian (BE) 2017/1584, datë 13 shtator 2017, mbi reagimin e koordinuar ndaj incidenteve në shkallë të gjerë dhe krizave kibernetike.

Menaxhimi i krizës kibernetike kombëtare përfshin shumë aktorë, si: ministri, autoritete rregullatore, institucione të pavarura, institucione ligjzbatuese etj., pasi ato udhëheqin përpjekjet mbrojtëse të shtetit për të përballuar sulmet dhe pasojat e tyre. Qëndrueshmëria kibernetike është aftësia për të ruajtur vazhdimësinë e shërbimeve kritike e të rëndësishme për vendin, pavarësisht ashpërsisë së goditjeve kibernetike drejt infrastrukturave të tyre të informacionit.

Në këtë kuadër, ky dokument synon:

- të përcaktojë proceduarat për identifikimin, klasifikimin, përshkallëzimin dhe menaxhimin e krizës kibernetike;

- të sigurojë koordinimin dhe bashkëpunimin ndërmjet institucioneve shtetërore, sektorit privat dhe organizatave ndërkombëtare për të krijuar një rrjet të sigurt dhe të besueshëm për përgjigjen dhe menaxhimin e krizave kibernetike, për të ndihmuar në minimizimin e pasojave, si dhe për të siguruar shkëmbimin e shpejtë dhe efikas të informacionit dhe të masave mbrojtëse midis aktorëve të përfshirë në fushën e sigurisë kibernetike, institucioneve dhe shteteve;

- të përgatitë institucionet dhe infrastrukturat kritike e të rëndësishme të informacionit për të reaguar ndaj krizave të sigurisë kibernetike, përfshirë masat për parandalimin e përshkallëzimit të incidenteve kibernetike në shkallë të gjerë dhe mësimet e nxjerra nga situatat e mëparshme;

- të rritë kapacitetet e reagimit e të ndërhyrjes për të menaxhuar me sukses situata të krizës së sigurisë kibernetike dhe për të garantuar vazhdimësinë e funksioneve dhe të shërbimeve kritike e të rëndësishme të infrastrukturave të informacionit.

2. PROCEDURAT PËR IDENTIFIKIMIN, KLASIFIKIMIN, PËRSHKALLËZIMIN DHE MENAXHIMIN EFEKTIV TË KRIZËS KIBERNETIKE

2.1 Kriza kibernetike

Krizë kibernetike është situata gjatë së cilës siguria e informacionit në sistemet e informacionit ose siguria e rrjeteve të komunikimeve elektronike është seriozisht e rrezikuar, duke vënë në rrezik interesin publik të Republikës së Shqipërisë.

Identifikimi, përshkallëzimi dhe menaxhimi i krizës kibernetike bazohen në dokumentin e ENISA-s "Për bashkëpunimin dhe menaxhimin e krizave kibernetike". Sipas ENISA-s, kriza kibernetike fillon kur një incident i zakonshëm kibernetik shndërrohet në një ngjarje të jashtëzakonshme, që do të thotë se ai ndryshon nga normalja dhe përfshin shqetësim serioz ose rrezik për bllokimin e funksioneve jetësore të shoqërisë.

Kriza kibernetike trajtohet duke u bazuar në këto dy elemente themelore, të vlerësuar në ndërveprim me rrethanat në hapësirën kibernetike dhe atë fizike:

1. Vlerësohet potenciali i një incidenti kibernetik për të shkaktuar dëme reale, për të ndërprerë ose për të kompromentuar vazhdimësinë funksionale të shërbimeve kritike e të rëndësishme të infrastrukturave të informacionit, si dhe për t'u përshkallëzuar në një gjendje të jashtëzakonshme kombëtare.

2. Në rastet e situatave emergjente të shkaktuara nga faktorë fizikë jokibernetikë, si konflikte të armatosura, akte terroriste apo fatkeqësi natyrore, merret në konsideratë rritja e nivelit të rrezikut për shpërthimin e një krize kibernetike dhe intensifikimi i aktivitetit keqdashës kibernetik.

2.2 Fazat e krizës kibernetike

Kriza kibernetike kalon në disa faza:

- Faza e alarmit në një krizë kibernetike;
- Faza e vlerësimit të situatës dhe identifikimit të krizës kibernetike;
- Faza e përgjigjes dhe menaxhimit të krizës kibernetike;
- Faza e rimëkëmbjes pas krizës kibernetike.

2.2.1 Faza e alarmit në një krizë kibernetike

Faza e alarmit në një krizë kibernetike është momenti kur incidenti kibernetik i identifikuar vlerësohet si kërcënim serioz, që mund të ndikojë në funksionimin normal të sistemit ose të infrastrukturës së informacionit, duke kërkuar aktivizimin e menjëhershëm të strukturave të reagimit. Në këtë fazë, konfirmohet karakteri kritik i ngjarjes, përcaktohet niveli i alarmit, sipas protokolleve të brendshme, dhe njoftohen aktorët kyç operativë dhe vendimmarrës, përfshirë ekipet teknike, menaxhimin e lartë, si dhe autoritetet kombëtare kompetente, me qëllim koordinimin e shpejtë e të strukturuar, që të parandalohet përhapja e dëmeve dhe të fillojë menaxhimi aktiv i situatës në kohë reale.

Gjendjet e alarmit kibernetik përcaktohen dhe përdoren si mekanizëm formal për vlerësimin e nivelit të vigjilencës e të gatishmërisë institucionale për përballimin e rreziqeve në hapësirën kibernetike e fizike. Autoriteti, në koordinim me infrastrukturën e informacionit të prekur, përcakton gjendjen e alarmit kibernetik mbi bazën e vlerësimit të situatës, i cili mbështetet në informacione të verifikuara, fakte e analiza të përbashkëta teknike dhe operacionale. Në përputhje me nivelin e incidentit kibernetik të konstatuar, autoriteti ngre gjendjen përkatëse të alarmit kibernetik dhe aktivizon procedurat përkatëse të reagimit, duke siguruar funksionimin e mekanizmave të koordinimit e të ndërhyrjes. Me shpalljen e gjendjes së alarmit kibernetik, subjektet përgjegjëse zbatojnë menjëherë masat dhe veprimet e përcaktuara për nivelin përkatës të alarmit, me qëllim kufizimin e ndikimit të incidentit dhe reduktimin e rrezikut të dëmtimit të infrastrukturës së informacionit.

Shpallja në kohë e gjendjes së alarmit kibernetik është e detyrueshme dhe synon parandalimin e përshkallëzimit të incidenteve kibernetike në krizë kibernetike, si dhe kufizimin e dëmeve, në rastet kur kriza kibernetike është identifikuar.

Mosshpallja ose vonesa në shpalljen e gjendjes së alarmit kibernetik rrit rrezikun e shkaktimit të dëmeve në shkallë të gjerë ndaj infrastrukturave të informacionit dhe të vazhdimësisë së shërbimeve kritike.

2.2.1.1 Skema e përshkallëzimit të gjendjes së alarmit kibernetik

Skema e përshkallëzimit të gjendjes së alarmit kibernetik përcaktohet sipas tabelës 1, të kësaj procedure, dhe zbatohet nga Autoriteti dhe nga subjektet përgjegjëse, në përputhje me nivelin e rrezikut dhe ndikimit të incidentit kibernetik.

Situatë e mbrojtjes rutinë – Në mungesë të shpalljes së një gjendjeje alarmi kibernetik, infrastruktura kritike e informacionit konsiderohet në gjendje të mbrojtjes rutinë dhe është e detyruar të zbatojë masat standarde të sigurisë kibernetike, të kryejë operacione rutinë dhe të përditësojë planet e mbrojtjes kibernetike, pa konstatuar ndërprerje të funksionimit normal të infrastrukturës së informacionit.

Situatë e përshkallëzimit të nivelit fillestar – Aktivizohet kur konstatohet një kërcënim i rëndësishëm ndaj një shërbimi kritik ose rrezik për ndërprerjen e funksionimit normal të infrastrukturës së informacionit, edhe nëse origjina kibernetike e kërcënimit nuk është ende e konfirmuar.

Situatë e përshkallëzimit të nivelit mesatar – Aktivizohet kur konstatohet dëmtim i infrastrukturave kritike të informacionit, që cenon në mënyrë të konsiderueshme vazhdimësinë e proceseve kryesore.

Situatë e përshkallëzimit të nivelit të lartë – Aktivizohet kur ndodh një dëmtim i zgjatur në kohë dhe në shkallë të gjerë ndaj infrastrukturave kritike të informacionit, duke shkaktuar dëme të mëdha në proceset bazë dhe në vazhdimësinë e funksionimit të shërbimeve të infrastrukturës së informacionit të prekur.

Faza	Përshkrimi
Mbrojtja rutinë	Niveli i mbrojtjes rutinë: nuk ka tregues të ndërprerjes së vazhdimësisë funksionale të shërbimeve kritike të infrastrukturës së informacionit.
Përshkallëzimi	Niveli fillestar: kërcënim thelbësor për një shërbim kritik të infrastrukturës së informacionit. Vazhdimësia funksionale e një shërbimi kritik të infrastrukturës së informacionit mund të rrezikohet.
	Niveli mesatar: dëmtimi i shërbimeve kritike të infrastrukturës së informacionit mund të shkaktojë mosfunksionim të konsiderueshëm në vazhdimësinë e proceseve kryesore.
	Niveli i lartë: dëmtimi i zgjatur në kohë dhe në shkallë të gjerë ndaj shërbimeve kritike të infrastrukturës së informacionit shkakton dëme të konsiderueshme në proceset kritike dhe në vazhdimësinë e funksionimit të shërbimeve.

Tabela 1: Skema e përshkallëzimit të alarmit kibernetik.

2.2.1.2 Treguesit për përcaktimin e gjendjes së alarmit kibernetik në hapësirë kibernetike dhe fizike

Gjendja e alarmit kibernetik përcaktohet mbi bazën e vlerësimit të rrezikut nëpërmjet treguesve të ashpërsisë së kërcënimit dhe mundësive të materializimit të tyre, duke analizuar veprimet që duhet të ndërmerren, si dhe burimet e mjetet që duhet të përdoren. Emergjencat e shkaktuara nga një faktor jokibernetik (si: lufta, fenomeni natyror, aktivitetet terroriste, keqfunksionimi, etj.) shpesh shërbejnë si mundësi për sulmuesit kibernetikë për të rritur përpjekjet e tyre, pikërisht, kur funksionimi normal i shërbimeve kritike të infrastrukturës së informacionit bëhet edhe më thelbësor, gjendja e alarmit kibernetik do të përcaktohet jo vetëm nga rrethanat në hapësirën kibernetike, por edhe nga rrethanat në hapësirën fizike.

Në lidhje me korrelacionin midis treguesve dhe gjendjeve të alarmit kibernetik, veprimet dhe vlerësimet kryhen sipas këtyre parimeve:

1. Përdorimi i treguesve: Një tregues i caktuar nuk përcakton automatikisht një nivel specifik të alarmit kibernetik. Treguesit shërbejnë si mjete për vlerësimin e situatës për të ndihmuar në përcaktimin e nivelit të alarmit.

2. Shpallja e alarmit para incidentit: Një alarm kibernetik mund të aktivizohet edhe pa konstatimin e një dëmtimi konkret të shërbimeve kritike. Aktivizimi mund të bazohet në sinjalizime të shërbimeve të inteligjencës mbi rreziqe të mundshme ose në rrethanat që rrisin rëndësinë e funksionimit normal të infrastrukturës së informacionit. Në këtë mënyrë, mund të përcaktohet një nivel alarmi (p.sh., A ose B), si rezultat i një incidenti me ndikim të ulët ose të konsiderueshëm, veçanërisht gjatë emergjencave të shkaktuara nga faktorë jokibernetikë, duke ruajtur në të njëjtën kohë masat e mbrojtjes rutinë.

2.2.1.3 Gjendjet e alarmit kibernetik dhe treguesit për përcaktimin e secilit nivel

Mbrojtja rutinë: Përfaqëson situatën e paracaktuar, kur rrethanat në hapësirën kibernetike dhe në hapësirën fizike nuk shfaqin tregues për një ndërprerje të funksionimit normal të infrastrukturës së informacionit ose ndonjë nevojë për të rritur nivelin e mbrojtjes. Në këto rrethana, nuk ka tregues për nivele të larta alarmi.

Treguesit në hapësirën kibernetike përcaktojnë nëse kanë ndodhur incidente të dukshme kibernetike, por pa ndërprerë funksionimin e infrastrukturës së informacionit ose nuk kanë ndodhur incidente të dukshme kibernetike.

Treguesit në hapësirën fizike përcaktojnë alarme të përgjithshme për mundësinë e ndodhjes së incidenteve kibernetike.

Niveli A i alarmit kibernetik: Niveli A i alarmit kibernetik (incident në nivel të ulët) përcaktohet pas vlerësimit të situatës, kur përmbushet të paktën një nga treguesit e mëposhtëm:

- *Treguesit në hapësirën kibernetike:*

- *Paralajmërim për një incident kibernetik:* Ka ndodhur një incident kibernetik i izoluar, i cili tregon për ndërprerje të mundshme të funksionimit normal të një shërbimi jokritik në një operator të infrastrukturës së informacionit, por nuk ka tregues që prekin të gjithë sektorin apo degë të operatorit të infrastrukturës së informacionit;

- *Marrja e një alarmi informativ:* Informacion lidhur me një kërcënim, dobësi në sistemet e informacionit, të cilat mund të prekin një ose disa shërbime jokritike të operatorit të infrastrukturës së informacionit;

- *Ngjarje botërore që prekin direkt ose indirekt Republikën e Shqipërisë:* Sulme kibernetike që ndodhin

jashtë territorit të Republikës së Shqipërisë, por që prekin direkt apo indirekt shtetin tonë, p.sh. sulme kibernetike ndaj kompanive që kanë filiale në vendin tonë ose sulme ndaj vendeve aleate.

- Treguesit në hapësirën fizike:

- Problem operacional ose teknik: Një mosfunksionim operacional ose teknik në një shërbim jokritik dhe/ose në vendin ku infrastruktura përkatëse e informacionit ndodhet;

-Ngjarje botërore që prekin indirekt Shqipërinë: Paralajmërimi i një ngjarjeje jonormale sigurie (si p.sh. një përshkallëzim i lëshimit të raketave drejt vendeve aleate).

Niveli B i alarmit kibernetik: Niveli B i alarmit kibernetik përcaktohet pas vlerësimit të situatës, kur përmbushet të paktën një nga treguesit e mëposhtëm:

- Treguesit në hapësirën kibernetike:

- Paralajmërim për një sulm kibernetik: CSIRT-i kombëtar informohet nga shërbimet e inteligjencës, CSIRT-et e shteteve aleate ose organizata ndërkombëtare për sulme të mundshme kibernetike drejt një shërbimi të një sektori kritik;

- Dëmtimi i shërbimeve kritike si pasojë e sulmit kibernetik: Rezultati konsiston në ndërprerjen e mundshme të vazhdimësisë së një shërbimi kritik të infrastrukturës së informacionit, por nuk ka të dhëna për përhapje në të gjithë sektorin.

- Treguesit në hapësirën fizike:

- Dëmtime fizike: Dëmtime fizike të shërbimeve që janë kritike (si: ndërprerja e energjisë elektrike, ndërprerja e shërbimeve shëndetësore), por që janë të lokalizuara vetëm në një operator të infrastrukturës së informacionit;

- Ngjarje botërore që prekin drejtpërdrejt Shqipërinë: Një sulm i ndodhur diku në një vend tjetër, por që i atribuohet Shqipërisë.

Niveli C i alarmit kibernetik: Niveli C i alarmit kibernetik është niveli i lartë i alarmit kibernetik, ku rrethanat që nxitën shpalljen e kësaj gjendjeje mund të përshkallëzohen deri në një gjendje emergjence kombëtare. Niveli C i alarmit kibernetik përcaktohet pas vlerësimit të situatës, kur përmbushet të paktën një nga treguesit e mëposhtëm:

- Treguesit në hapësirën kibernetike:

- Dëmtime të disa shërbimeve kritike, si pasojë e sulmeve kibernetike: Dëmtime ndaj disa shërbimeve kritike të operatorit të infrastrukturës së informacionit, të cilat çojnë në ndërprerje të disa proceseve bazë dhe në vazhdimësinë funksionale të ekonomisë (siç është dëmtimi ndërsektorial);

- Treguesit në hapësirën fizike:

- Dëmtime fizike të vazhdueshme: Dëmtime fizike të disa infrastrukturave, shërbimeve që janë të rëndësishme për ekonominë e vendit;

- Përgatitje për fillimin e një lufte: Përgatitje serioze për luftë ose një operacion ushtarak në shkallë të gjerë.

Niveli D i alarmit kibernetik: Niveli D është gjendja e emergjencës kombëtare, që është niveli më i lartë i alarmit kibernetik. Niveli D i alarmit kibernetik përcaktohet pas vlerësimit të situatës, kur përmbushet të paktën një nga treguesit e mëposhtëm:

- Treguesit në hapësirën kibernetike:

- Dëmtime në shkallë të gjerë të shërbimeve kritike si pasojë e sulmeve kibernetike: Dëmtime të mëdha dhe/ose të vazhdueshme ndaj shërbimeve kritike të operatorit të infrastrukturës kritike e të rëndësishme të informacionit, të cilat çojnë në ndërprerje të shumë shërbimeve bazë jetësore, si edhe të ekonomisë (siç është dëmtimi ndërsektorial).

- Indikatorët në hapësirën fizike:

- Dëmtime fizike të vazhdueshme: Dëmtime fizike të shumta dhe/ose të vazhdueshme ndaj infrastrukturave të informacionit që mundësojnë ofrimin e shërbimeve, që janë të rëndësishme për ekonominë e vendit;

- Situata e një lufte: Luftë ose një operacion ushtarak në shkallë të gjerë;

- Gjendja e jashtëzakonshme: Shpallja e një gjendjeje të jashtëzakonshme, e kushtëzuar me qëndrimin në shtëpi "/"ngjarje emergjence civile".

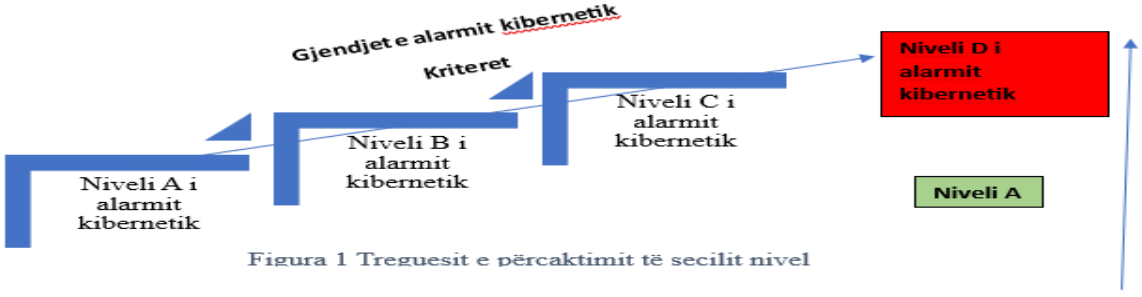


Figura 1 Treguesit e përcaktimit të secilit nivel

2.2.1.4 Përcaktimi i gjendjes së alarmit kibernetik përcaktohet nga Autoriteti pas koordinimit me infrastrukturën e prekur, bazuar në një raport të vlerësimit të situatës.

2.2.1.5 Parimet për ndryshimin e gjendjes së alarmit kibernetik

Gjatë çdo gjendjeje alarmi, çdo infrastrukturë informacioni kryen një vlerësim të situatës, shqyrton treguesit në hapësirën kibernetike dhe në hapësirën fizike e më pas konstaton nëse ka nevojë për të ndryshuar gjendjen e alarmit.

Rritja e nivelit të alarmit kibernetik:

Rritja e nivelit të alarmit kibernetik ndikohet nga përshkallëzimi i situatës në rrethana të caktuara dhe kërkon ndërmarrjen e veprimeve të mëtejshme ose intensifikimin e masave tashmë të zbatuara. Qëllimi i këtyre veprimeve është të parandalohet përkeqësimi i situatës ose të minimizohen dëmtimet e mundshme.

- Rritja graduale e alarmit: Niveli i alarmit duhet të përcaktohet dhe të rritet gradualisht, bazuar në treguesit e situatës, duke analizuar çdo ndryshim në rrezikun ose ndikimin e mundshëm në shërbimet kritike.

- Përjashtimet: Në situata ekstreme, mund të shpallet menjëherë niveli i emergjencës kibernetike, pa kaluar përmes niveleve të tjera të alarmit, për të garantuar ndërhyrje të menjëhershme dhe mbrojtje të vazhdueshme të infrastrukturës kritike.

Ulja e nivelit të alarmit kibernetik:

Niveli i alarmit kibernetik ulet nëse treguesit përkatës, që çuan në përcaktimin e nivelit të alarmit, nuk janë më të pranishëm. Niveli i alarmit ulet gradualisht, nga një kategori çdo herë, derisa të rikthehet mbrojtja kibernetike rutinë.

1.2.1 Faza e vlerësimit të situatës dhe identifikimit të krizës kibernetike

Faza e vlerësimit të situatës dhe identifikimit të krizës kibernetike zhvillohet si më poshtë:

Fillimi i vlerësimit: Vlerësimi i situatës nis sapo gjendja e alarmit kibernetik arrin nivelin C. Kjo përfshin analizën e shkaqeve, shtrirjes dhe ndikimit të mundshëm të incidenteve kibernetike në shkallë të gjerë për operatorët e infrastrukturave të informacionit.

Përshkallëzimi i alarmit: Nëse nga analiza rezulton se gjendja e alarmit është rritur nga niveli C në nivelin D (emergjencë kibernetike) dhe në të njëjtën kohë shërbimet kritike të operatorit janë ndërprerë, duke cenuar rëndë sigurinë e informacionit dhe nuk mund të rikthehen brenda një afati të përcaktuar, situata konsiderohet për identifikimin e krizës kibernetike.

Identifikimi i krizës kibernetike: Kriza kibernetike përcaktohet, sipas rastit, duke marrë parasysh:

a) Shkallën e ndikimit për shërbimet kritike;

b) Kohëzgjatjen e ndërprerjes së funksionimit normal;

c) Pamundësinë për rikthim të shpejtë të sigurisë dhe funksionalitetit të infrastrukturës.

Kriza kibernetike mund të identifikohet, sipas rastit:

Në nivel kombëtar – Kriza kibernetike identifikohet pas një kërcënimi ose rrethanash që mund të përshkallëzohen deri në një gjendje emergjence kombëtare/krize kibernetike, ku janë përfshirë disa sektorë kritikë ose të gjithë sektorët kritikë të ekonomisë, me shtrirje në nivel kombëtar.

Në nivel sektorial – Kriza kibernetike identifikohet pas një kërcënimi ose rrethanash që mund të përshkallëzohen deri në një gjendje emergjence kombëtare/krize kibernetike, edhe për një nga sektorët jetikë me shtrirje dhe ndikim kombëtar (p.sh. është përfshirë sektori i energjisë, i cili ka paralizuar gjithë sektorët e tjerë). Shpallja e gjendjes së krizës kibernetike në nivel sektorial bën të detyrueshëm që të gjitha strukturat, që janë pjesë e atij sektori, të kalojnë në gjendje alarmi. Shpallja e gjendjes së alarmit kibernetik në një sektor të caktuar nuk është detyruese për sektorët e tjerë, por tregon se ekzistojnë rrethana të caktuara në hapësirën kibernetike, të cilat duhet të adresohen edhe nga sektorët e tjerë.

2.2.2.1 Hapat për shpalljen e gjendjes së krizës kibernetike

1. Kur Autoriteti merr njoftim për një incident të rëndë të sigurisë kibernetike, që ka ndikim dhe shtrirje të gjerë në operatorët e infrastrukturave kritike të informacionit, Autoriteti fillon një vlerësim paraprak mbi incidentin për të përcaktuar ndikimin politik, ekonomik dhe të sigurisë.

2. Pas vlerësimit të situatës, Autoriteti harton një raport paraprak.

3. Kur nga raporti paraprak arrihet në përfundimin se situata konsiston në një krizë të mundshme kibernetike, Autoriteti njofton menjëherë subjektet e tjera përgjegjëse të sigurisë dhe mbrojtjes, sipas shkronjës "a", të nenit 11, të ligjit nr. 25/2024, "Për sigurinë kibernetike", duke

filluar një proces koordinues dhe konsultues për vlerësimin e situatës në nivel kombëtar.

4. Pas një vlerësimi të koordinuar me subjektet e tjera përgjegjëse të sigurisë dhe mbrojtjes, merret një vendim për propozimin ose jo të shpalljes së gjendjes së krizës kibernetike.

5. Në rastin kur vendoset të propozohet shpallja e gjendjes së krizës kibernetike, Autoriteti i dërgon Kryeministrit propozimin për shpalljen e krizës kibernetike dhe masat për zgjidhjen e situatës.

6. Kryeministri, me marrjen e propozimit nga Autoriteti, i propozon Këshillit të Ministrave shpalljen e gjendjes së krizës kibernetike.

7. Shpallja e gjendjes së krizës kibernetike bëhet me vendim të Këshillit të Ministrave.

8. Këshilli i Ministrave mund të vendosë zgjatjen e periudhës së gjendjes së krizës kibernetike, por jo më shumë se 30 ditë.

3. FAZA E PËRGJIGJES DHE MENAXHIMIT TË KRIZËS KIBERNETIKE

Faza e përgjigjes dhe menaxhimit të krizës kibernetike përfshin hapa të koordinuar dhe zbatimin e kundërmasave e playbooks-it për të minimizuar ndikimin, për të rikuperuar sistemet e prekura dhe për të siguruar vazhdimësinë e operacioneve kritike të infrastrukturës së informacionit, duke mundësuar kontrollin, kufizimin, neutralizimin, si dhe rikuperimin e pasojave të sulmit kibernetik të përshkallëzuar në krizë kibernetike, si dhe duke siguruar një koordinim institucional dhe komunikim të qartë. Faza e përgjigjes dhe menaxhimit të krizës kibernetike aktivizohet pas shpalljes zyrtare të gjendjes së krizës kibernetike me vendim të Këshillit të Ministrave.

3.1 Hapat për përgjigjen dhe menaxhimin ndaj krizës kibernetike

Hapat që ndiqen për përgjigjen dhe menaxhimin e krizës kibernetike janë, si më poshtë:

3.1.1 Aktivizimi i strukturave

3.1.1.1 Autoriteti Kombëtar për Sigurinë Kibernetike kërkon kalimin menjëherë në nivel gatishmërie të lartë të ekipit të përgjigjes ndaj incidenteve kibernetike pranë operatorit të sektorit/sektorëve të prekur nga incidenti kibernetik i përshkallëzuar në krizë kibernetike (CSIRT pranë operatorit), si dhe të kalojnë në gjendje emergjence kibernetike.

3.1.1.2 Autoriteti Kombëtar për Sigurinë Kibernetike kalon menjëherë në nivel gatishmërie të lartë Ekipin Kombëtar të Përgjigjes ndaj Incidenteve Kibernetike (CSIRT Kombëtar), si dhe kalon në gjendje emergjence kibernetike dhe nis procedurat e reagimit dhe koordinimit.

3.1.1.3 Autoriteti Kombëtar për Sigurinë Kibernetike ngre ekipin e përgjigjes ndaj emergjencave dhe krizës së sigurisë kibernetike (CERT), ku numri i ekspertëve dhe profilet e tyre vendoset mbi bazën e kompleksitetit të situatës, natyrës së sulmit, si dhe numrit të infrastrukturave të informacionit të prekura, sipas përcaktimeve të vendimit të Këshillit të Ministrave, për ngritjen, mënyrën e organizimit dhe funksionimit të ekipit të përgjigjes ndaj emergjencave dhe krizës së sigurisë kibernetike.

3.1.1.4 Në të gjitha rastet, komunikimi midis strukturave zhvillohet nëpërmjet kanaleve të sigurta të komunikimit, me qëllim shkëmbimin e informacionit teknik, njoftimin e aktorëve përgjegjës, si dhe koordinimin e masave urgjente.

3.1.2 Përditësimi i informacionit dhe vlerësimi i menjëhershëm i situatës

Autoriteti, në bashkëpunim me CERT-in mbledh dhe menaxhon të dhëna në kohë reale nga CSIRT-et pranë operatorëve si dhe nga CSIRT-et sektoriale, për sistemet dhe rrjetet e prekura, përmes të cilave realizohet analiza teknike e operacionale për shtrirjen e sulmit, ndikimin në shërbimet kritike, identifikimin e aktorëve të mundshëm, si dhe përcakton prioritetet për ndërhyrje. Autoriteti përditëson raportin e situatës çdo 24 (njëzet e katër) orë ose sipas nevojës.

3.1.3 Koordinimi ndërinstitucional dhe operacional

Autoriteti bashkërendon reagimin në nivel kombëtar dhe ndërkombëtar. Organizohen mbledhje të përditshme me:

a) CSIRT-et pranë operatorit dhe CSIRT-et sektoriale (p.sh. financa, energji, telekomunikacion, transport);

b) CERT-in;

c) Agjencitë e sigurisë (Policia e Shtetit, SHISH);

ç) Agjencitë partnere ndërkombëtare (p.sh. ENISA, EUROPOL EC3, NATO CCDCOE).

3.1.4 Përcaktimi, zbatimi dhe përditësimi i masave mbrojtëse e të kundërmasave kibernetike

Autoriteti përcakton e zbaton masat mbrojtëse të natyrës së përgjithshme dhe kundërmasat kibernetike për menaxhimin e krizës kibernetike, si dhe i përditëson ato sipas ecurisë së situatës.

3.1.5 Menaxhimi i komunikimit publik dhe transparenca

Autoriteti në koordinim me strukturën përgjegjëse për media dhe informim në varësi të Kryeministrit përgatit deklarata publike për të informuar qytetarët, duke shmangur panikun ose dezinformimin. Informacioni duhet të jetë i saktë dhe i bazuar mbi situatën aktuale, si dhe nuk duhet të përmbajë informacion të ndjeshëm teknik. Menaxhimi i medias në një rast të krizës kibernetike do të bëhet sipas aneksit I, të kësaj procedure.

3.2 Mbledhja e informacionit dhe menaxhimi i të dhënave

Autoriteti, në bashkëpunim me CERT-in, mbledh, analizon e ruan të dhënat dhe informacionin, që mund të ndihmojnë në identifikimin, zbutjen dhe rikuperimin e pasojave të incidenteve në shkallë të gjerë. Elementet kyçe për mbledhjen e informacionit dhe menaxhimin e të dhënave janë, si vijon:

3.2.1 Mbledhja e të dhënave në kohë reale

- Përdoren sisteme të monitorimit të sigurisë për të mbledhur informacionin në kohë reale. Këto sisteme mund të identifikojnë aktivitete të dyshimta në rrjet dhe mund të regjistrojnë të dhënat e lidhura me incidentet e mundshme, si adresat IP të dyshimta, kërkesat anormale dhe lëvizjet e paautorizuara të të dhënave.

- Regjistrohen aktivitetet në sisteme dhe servera për të krijuar një gjurmë të plotë të asaj që ka ndodhur. Kjo mund të përfshijë log-et e sistemeve, log-et e rrjetit dhe regjistrat e ngjarjeve të sigurisë.

3.2.2 Klasifikimi dhe filtrimi i të dhënave

- Klasifikohet informacioni për të dalluar informacionin e rëndësishëm nga ai që nuk është i nevojshëm. Ky klasifikim përfshin ndarjen e të dhënave në kategori, si: të dhëna të ndjeshme, informacion për kërcënime, aktivitete të dyshimta etj.

- Filtrohen të dhënat, pasi jo të gjitha të dhënat janë të nevojshme për analizë. Filtrimi i të dhënave për të identifikuar informacionin më të rëndësishëm ndihmon në hetimin e incidentit kibernetik dhe mund të ndihmojë në gjetjen e burimit të sulmit.

3.2.3 Ruajtja dhe sigurimi i të dhënave

- Ruhen të dhënat e mbledhura në mënyrë të sigurt, në mënyrë që të mund të analizohen në të ardhmen dhe të përdoren si prova, nëse është e nevojshme. Ruajtja mund të përfshijë përdorimin e serverëve të veçantë të siguruar, duke përdorur enkriptimin dhe kontrollet e aksesit për të mbajtur të dhënat të papërshkueshme.

- Kryhet ruajtja e të dhënave me integritet të plotë. Të dhënat nuk duhet të manipulohen ose të modifikohen nga palë të treta pa autorizim. Përdorimi i metodave të enkriptimit dhe të kontrolleve të integritetit mund të ndihmojë në sigurimin e këtyre të dhënave.

3.2.4 Analiza e të dhënave dhe identifikimi i kërcënimeve

- Analizohen të dhënat e mbledhura dhe të ruajtura për të kuptuar natyrën dhe shkallën e incidentit kibernetik, si dhe për të identifikuar karakteristikat e dyshimta, për të kuptuar se si janë kompromet uar sistemet dhe rrjetet e informacionit.

- Përdoret *threat intelligence*, një proces që përfshin mbledhjen e informacionit të jashtëm për kërcënimet aktuale dhe përdorimin e tij për të përmirësuar reagimin ndaj incidentit kibernetik.

3.3 Burimet dhe kapacitetet kombëtare për përgjigjen dhe menaxhimin e krizës kibernetike në Shqipëri

Përballimi i krizave kibernetike kërkon koordinim të mirëfilltë dhe shfrytëzimin e burimeve dhe të kapaciteteve kombëtare në të gjithë sektorët. Ministritë, institucionet shtetërore, strukturat operacionale dhe aktorët joqeveritarë kanë kapacitete specifike, të cilat duhet të integrohen në një qasje gjithëpërfshirëse për të siguruar një përgjigje efektive ndaj krizave kibernetike.

3.3.1 Subjektet përgjegjëse

1. Këshilli i Ministrave;
2. Kryeministri;
3. Autoriteti Kombëtar i Sigurisë Kibernetike/CSIRT-i Kombëtar;
4. CERT/Ekipi i Përgjigjes ndaj Emergjencave dhe Krizës së Sigurisë Kibernetike;
5. CSIRT-i sektorial;
6. CSIRT-i pranë operatorit;
7. Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale;
8. Policia e Shtetit.

3.3.2 Rolet dhe përgjegjësitë e subjekteve përgjegjëse për sigurinë kibernetike në fazën e përgjigjes

3.3.2.1 Këshilli i Ministrave, në cilësinë e organit kolegjial, me propozimin e Kryeministrit, merr vendim për:

a) shpalljen e gjendjes së krizës kibernetike për një periudhë 7-ditore.

b) zgjatjen e periudhës së gjendjes krizës kibernetike, por jo më shumë se 30 ditë.

3.3.2.2 Kryeministri i paraqet Këshillit të Ministrave propozimin për shpalljen e gjendjes së krizës kibernetike për një periudhë 7-ditore, si dhe zgjatjen e periudhës së gjendjes së krizës kibernetike, por jo më shumë se 30 ditë pas marrjes së propozimit për shpalljen e gjendjes së krizës kibernetike nga Autoriteti.

3.3.2.3 Autoriteti Kombëtar i Sigurisë Kibernetike/CSIRT-i Kombëtar është autoritet me kompetenca rregullatore, koordinuese, ekipi i përgjigjes ndaj incidenteve kibernetike dhe i krizës kibernetike dhe ushtron rolet e përgjegjësitë e mëposhtme:

a) I propozon Kryeministrit, në koordinim me institucionet e sigurisë dhe mbrojtjes, sikurse parashikohet në shkronjën "a", të nenit 11, të ligjit nr. 25/2024, "Për sigurinë kibernetike", shpalljen e gjendjes së krizës kibernetike dhe masat emergjente për zgjidhjen e situatës;

b) Thërret strukturën *ad-hoc* CERT;

c) Koordinon menaxhimin e krizës kibernetike;

ç) Nxjerr vendime me karakter të përgjithshëm ose merr masa mbrojtëse të natyrës së përgjithshme.

3.3.2.4 CERT – Ekipi i Përgjigjes ndaj Emergjencave dhe Krizës së Sigurisë Kibernetike është një strukturë *ad-hoc*, që vepron si linjë e parë e mbrojtjes për trajtimin e emergjencave dhe krizës së sigurisë kibernetike.

Detyrat kryesore:

a) Koordinimi dhe ndërhyrja e shpejtë për trajtimin e incidenteve kibernetike në shkallë të gjerë dhe krizave kibernetike;

b) Hartimi i planit të masave të emergjencës;

c) Menaxhimi dhe zgjidhja e emergjencës dhe krizës kibernetike;

ç) Ofrimi i asistencës në hartimin e rekomandimeve për të rikthyer në normalitet sistemet dhe rrjetet e informacionit në infrastrukturat e informacionit pas një incidenti në shkallë të gjerë dhe gjendjes së emergjencës dhe krizës kibernetike.

3.3.2.5 CSIRT-i sektorial, në cilësinë e ekipit të përgjigjes së incidenteve të sigurisë kibernetike të sektorit përkatës:

a) raporton pranë CSIRT-it kombëtar incidentin kibernetik të ndodhur në infrastrukturat e informacionit të sektorit përkatës;

b) koordinon me CSIRT-et pranë operatorëve për t'iu përgjigjur situatës.

3.3.2.6 CSIRT-i pranë operatorit, në cilësinë e ekipit të përgjigjes së incidenteve të sigurisë kibernetike të operatorit përkatës:

a) raporton incidentin e ndodhur në infrastrukturat e informacionit pranë operatorit të CSIRT-it kombëtar dhe CSIRT-it sektorial;

b) koordinon me CSIRT-in kombëtar dhe CSIRT-in sektorial për t'iu përgjigjur situatës.

3.3.2.7 Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale, në cilësinë e institucionit përgjegjës për hartimin e politikave për mbrojtjen e të dhënave personale të individëve, monitoron zbatimin e legjislacionit përkatës në rastin e incidenteve në shkallë të gjerë dhe krizës kibernetike:

- Trajton, kontrollon dhe monitoron zbatimin e legjislacionit në fuqi për mbrojtjen e të dhënave personale.

3.3.2.8 Policia e Shtetit, në cilësinë e institucionit përgjegjës për hetimin e krimit kibernetik, në zbatim të legjislacionit penal kryen këto veprime:

a) Ndjek veprimet e nevojshme operacionale/procedurale, në kuadër të zbatimit të legjislacionit penal;

b) Bashkëpunon me CSIRT-in kombëtar dhe atë pranë operatorit për analizën dhe hetimin e incidentit kibernetik;

c) Realizon veprimet procedurale, në kuadër të zbatimit të legjislacionit penal.

4. FAZA E RIMËKËMBJES

4.1 Rimëkëmbja e shërbimeve pas krizës kibernetike

Rimëkëmbja pas krizës kibernetike përbën një proces të koordinuar, me qëllim rikthimin e shërbimeve dhe funksioneve kritike të infrastrukturës së informacionit në një gjendje të qëndrueshme. Ky proces siguron vazhdimësinë e operacioneve dhe rikthimin e sigurisë, duke minimizuar ndikimet afatgjata të krizës e duke përmirësuar gatishmërinë për incidente të ardhshme. Veprimet përfshijnë vlerësimin e dëmeve, rivendosjen graduale të sistemeve e të shërbimeve, monitorimin e vazhdueshëm për stabilitet e siguri gjatë rimëkëmbjes, si dhe dokumentimin e përvojës për të përmirësuar procedurat dhe *playbook*-et për menaxhimin e incidenteve të ardhshme.

4.2 Vlerësimi pas krizës dhe përmirësimi i qëndrueshmërisë

4.1.1 Pas stabilizimit të situatës, Autoriteti kalon në fazën e analizës retrospektive (*post-incident review*), që përfshin veprimet e mëposhtme:

a) Dokumenton të gjitha ngjarjet, reagimet dhe mësimet e nxjerra;

b) Analizon nëse protokollet e sigurisë ishin të mjaftueshme;

c) Përgatit raportin final të krizës kibernetike, që përfshin:

i. përshkrimin teknik të ngjarjes;

ii. vlerësimin e dëmit dhe kostove;

iii. masat e marra;

iv. rekomandimet për përmirësim.

4.1.2 Ky raport i dërgohet Kryeministrit dhe, sipas rastit, Komisionit Parlamentar të Sigurisë Kombëtare.

4.1.3 Në bazë të raportit final të krizës kibernetike, Autoriteti harton ose përditëson:

a) Procedurat e reagimit ndaj incidenteve kibernetike;

b) Politikat kombëtare të sigurisë digjitale;

c) Planet e trajnimit dhe ndërgjegjësimit për personelin publik dhe operatorët e infrastrukturave kritike.

ANEKSI I
MENAXHIMI I MEDIAVE NË NJË SITUATË KRIZE KIBERNETIKE

1. Rëndësia e menaxhimit të medias në rastin e një ngjarjeje kibernetike

CSIRT-i kombëtar, së bashku me institucionet ligjzbatuese, rregullatorët përkatës, ministritë e linjës dhe mediat luajnë një rol vendimtar në menaxhimin e kanaleve mediatike, në rastin e një krize kibernetike. Qytetarët duhet të marrin informacion të besueshëm, të përditësuar e të verifikuar.

Këto institucione duhet të ofrojnë informacion efektiv, që mund të shpëtojë jetë, të zvogëlojë shtrirjen e dëmtimeve dhe të shtyjë popullatën të marrë masat e nevojshme mbrojtëse. Në këto raste, komunikimi i nisur ka rezultuar të jetë më efektiv në përcaktimin e kufijve të një ngjarjeje kur ndahet me publikun, për të mos përhapur panik dhe për të përcjellë besueshmëri në popullatë.

2. Gjatë koordinimit me median mbahen në konsideratë elementet e mëposhtme:

a) **Kritika publike** – Incidentet kibernetike, që kanë jehonë në media, ndonjëherë çojnë në kritika që mund të vijnë edhe nga profesionistë kibernetikë, të cilët nuk janë domosdoshmërish të përfshirë në detaje, dhe nga palët e interesuara që punojnë në mënyrë rutinore me subjektin që dëmtohet;

b) **Identiteti i sulmuesit** – sulmuesi, në veçanti një shtet apo aktivist, kërkon vëmendjen dhe dukshmërinë e medias ndaj sulmit, si dhe ndikimin e tij në publik. Shpesh, një nga qëllimet e një sulmi është të bëjë "zhurmë" në media. Ndonjëherë, sulmuesi do të përpiqet të imitojë dikë tjetër për të ngatërruar ose për të vështirësuar atribuimin. Identiteti i sulmuesit është tema më interesante për median, por është e rëndësishme të mbahet mend se identiteti i sulmuesit është zakonisht i paqartë dhe kërkon kohë gjatë një hetimi kibernetik për ta lidhur atë me një sulmues të caktuar;

c) **Dallimet ndërmjet infrastrukturave** – publiku nuk do të jetë gjithmonë në gjendje të bëjë dallimin ndërmjet infrastrukturës kritike dhe përgjegjësisë private kundrejt asaj kombëtare;

ç) **Siguria kibernetike është një gjuhë komplekse teknologjike**, që është shumë e pakuptueshme për publikun dhe ka boshllëqe në njohuri midis grupeve të ndryshme të popullsisë;

d) **Ngjarjet kibernetike kanë implikime politike** – deklarata të caktuara mund të ndikojnë në marrëdhëniet me vendet e tjera dhe veprimet pasuese;

dh) **Lloji dhe natyra e sulmit** zakonisht nuk ngjall interes mediatik, por më tepër pasojat e tij, megjithëse ka raste që krijojnë interes, kur ngjarja është veçanërisht e sofistikuar;

e) **Gjithçka është e lidhur** – Siguria kibernetike ndikon në të gjitha aspektet e jetës;

ë) **Sulmuesi kibernetik** mund të shkaktojë dëme fizike në terren (infrastruktura, shërbime, vazhdimësi operacionale, ndërprerje të transportit etj.) dhe dëmtim të ndërgjegjësimit (dëm ndaj qëndrueshmërisë kombëtare, pasiguri, dëmtim të aftësive parandaluese dhe dështim).

Audienca e synuar	Qëllimet dhe objektivat e informacionit
Popullsia që preket drejtpërdrejt nga ngjarja – klientët, subjektet, banorët e një zone të caktuar etj.	▪Përshkruhet ngjarja dhe situata në mënyrë të besueshme; ▪Jepen udhëzime; ▪Sigurohet besimi tek entitetet e ndryshme dhe në aftësinë e tyre për të menaxhuar ngjarjen; ▪Shmangen dezinformatat; ▪Përcillen mesazhe uniforme nga të gjitha palët e përfshira; ▪Përshtaten mesazhet për popullatat e ndryshme të prekura nga ngjarja – niveli i ndërgjegjësimit, të kuptuarit teknologjik, gjuhët, dallimet kulturore, kanalet e ndryshme të komunikimit dhe ndikuesit.
Publiku i gjerë	▪Përforcohet besimi i publikut; ▪Sigurohet transparenca; ▪Shmangen dezinformatat; ▪Përcillen mesazhe uniforme nga të gjitha palët e përfshira.
Komunikimet nga ofrues të ndryshëm shërbimi	▪Përcillen mesazhe uniforme; ▪Sigurohet transparenca; ▪Të shmangen dezinformatat; Të përforcohet besimi në subjektin e ofruesit të shërbimit dhe në aftësinë për të menaxhuar ngjarjen.
Organet qeveritare	▪Të përcjellin mesazhe uniforme; ▪Të jenë transparent; ▪Të shmangen dezinformatat; ▪Të përforcohet besimi aftësia për të menaxhuar ngjarjen.
Arena rajonale (kundërshtarët dhe armiqtë)	▪Parandalim/pengim i arritjeve të kundërshtarëve
Arena ndërkombëtare	▪Konsolidimi i partneriteteve/koalicioneve kundër sulmuesit; ▪Delegjitimimi i sulmuesit dhe i sulmit.

Tabela 2: Përmbledhje e audiencës së synuar.

3. Sfidat për komunikimin e krizës

a) **Të ruhet raporti midis shpejtësisë dhe kujdesit në dhënien e informacionit** – ndërkohë që një raport i shpejtë, qoftë edhe i pjesshëm, drejton komunikimin, është e nevojshme t'i kushtohet vëmendje deklaratave që bëjnë pohime të forta, duke qenë se nuk janë të kolauduara e në vijimësi mund të rezultojnë të gabuara;

b) **Të mos zbulohet informacion kur nuk ka informacion** – në situata rreziku dhe krize, ajo që mund të shkaktojë panik është në fakt mungesa e informacionit;

c) **Të ruhet besimi i publikut tek autoritetet shtetërore dhe në hapësirën digjitale** – është e rëndësishme të sigurohet informacion gjithëpërfshirës dhe i besueshëm, të tregohet përkushtim dhe forcë në veprimet që ndërmerren për të menaxhuar ngjarjen e të demonstrohet se kriza mund të trajtohet. Gjithashtu, duhet të merren përgjegjësi, kur është e nevojshme, duke treguar udhëheqje dhe përmirësime apo mësime të nxjerra.

4. Rastet, në të cilat kryerja e një njoftimi, duhet të konsiderohet në mënyrë të favorshme:

a) Dëmtimi ose tentativa për dëmtim të infrastrukturave të informacionit që çojnë në dëmtimin e shërbimeve kritike për publikun, për shembull, transporti, furnizimi i mallrave, shërbimet shëndetësore, uji, energjia elektrike etj.;

b) Dëmtimi i një shërbimi që është me interes për publikun ose për një grup të caktuar individësh;

c) Dëmtimi i një infrastrukture të informacionit, që është e lidhur me infrastruktura të tjera dhe i rrezikon ato. Në këtë rast, është e nevojshme të paralajmërohen palët e interesit me infrastrukturën e informacionit të prekur;

ç) Përpjekje me efekt të gjerë në ekonomi, që nuk rezultojnë në dëmtime në terren dhe janë ndalur;

d) Rrjedhja e informacionit që është me interes dhe me rëndësi për publikun e gjerë ose për një grup të gjerë njerëzish;

dh) Ndërprerja e bazave të rëndësishme të të dhënave;

e) Një aktivitet që bën "zhurmë" ose që ka pasoja të gjera në publik;

ë) Dëmtimi i një shërbimi, një simboli qeveritar ose i një entiteti simbolik;

f) Financiar – një ngjarje e synuar ose e përhapur që i shkakton dëme të konsiderueshme një institucioni financiar, që mund të dëmtojë besimin e publikut në sistemin financiar shqiptar;

g) Shkaktimi i dëmeve të konsiderueshme ndaj infrastrukturave të informacionit që rezulton në një ndikim domethënës negativ në funksionimin e një

numri të madh të infrastrukturave të informacionit, duke prekur vazhdimësinë e shërbimeve ose proceseve të tyre thelbësore.

gj) Një ngjarje që ndikon në mendësinë e njerëzve dhe/ose dezinformim, që ndikon në besimin e publikut, si rezultat i ngjarjes kibernetike. Kjo përfshin dëmtimin (vandalizimin) e një *website*-i të madh qendror ose i një tabele buletini me informacion jetik;

h) Përpjekje, me qëllim për të dëmtuar sigurinë publike dhe shoqërinë ose një ngjarje, që në mënyrë indirekte ose direkte, ka rezultuar në dëmtim personal të individit.

5. Përballja me dezinformimin dhe lajmet e rreme

Lajmet e rreme dhe dezinformatat janë një problem global. Gjatë një ngjarjeje, rekomandohet të trajtohet fenomeni shpejt dhe në mënyrë efektive, duke përdorur mjetet e mëposhtme:

a) Monitorimi i informacioneve të rreme përmes sistemeve për monitorimin e diskutimit në internet dhe/ose përdorimit të një personi nga infrastruktura, që do të kërkojë në mënyrë aktive kanalet sociale. Është e mundur të krijohet një qendër komandimi për të monitoruar dhe dhënë përgjigje ose për të përdorur dhomat ekzistuese të operacioneve;

b) Marrja e një vendimi për llojin e përmbajtjes që do të trajtohet - çfarë dezinformimi është i rëndësishëm, sipas disa kritereve, çfarë e shkakton mosbesimin e publikut, çfarë është mashtruese dhe mund të shkaktojë dëm;

c) Përhapja e informacionit të besueshëm në mënyrë të vazhdueshme dhe të shpejtë për të parandaluar krijimin e një vakumi që do të mbushet me teori e gënjeshtra;

ç) Vendosja e autoritetit dhe besimit në informacionin dhe në kanalet e institucionit, duke përdorur ekspertë vendas ose të jashtëm, video, imazhe dhe tekste;

d) Dhënia e shembujve duke përdorur vetëmashtrimin – tregohet se çfarë është e gabuar dhe pse për të hedhur poshtë pretendimin; i bëhet thirrje publikut që të shpërndajë informacion të saktë. Për shembull, bëhet një foto e lajmeve të rreme dhe shtohet një etiketë që lexon "Mashtrim /Paralajmërim! Lajme të rreme!"). Shkruhet një artikull mbi këtë temë dhe shfaqet informacioni i rremë;

dh) Kur media përhap lajme të rreme ose dezinformata është e rëndësishme t'i thuhet atyre qartë se e kanë gabim;

e) Përdorimi i njerëzve të jashtëm që do të veprojnë dhe do t'u përgjigjen informacioneve të rreme;

ë) Evidentimi i rasteve specifike në media për të rritur ndërgjegjësimin e publikut për fenomenin, shpjegohet fenomeni, çfarë është informacioni i rremë dhe si të përgënjeshtrohet. Inkurajohet të menduarit kritik.

VENDIM
Nr. 822, datë 30.12.2025

PËR DISA SHTESA NË VENDIMIN NR. 1128, DATË 30.12.2020, TË KËSHILLIT TË MINISTRAVE, "PËR ZBATIMIN NGA REPUBLIKA E SHQIPËRISË TË VENDIMEVE TË KËSHILLIT TË BASHKIMIT EVROPIAN PËR VENDOSJEN, NDRYSHIMIN DHE SHFUQIZIMIN E MASAVE SHTRËNGUESE NDËRKOMBËTARE, TË NDRYSHUARA", TË NDRYSHUAR

Në mbështetje të nenit 100 të Kushtetutës, të neneve 3, pika 3, shkronja "c", e 6, pikat 2 e 5, të ligjit nr. 72/2019, "Për masat shtrënguese ndërkombëtare në Republikën e Shqipërisë", të ndryshuar, dhe të nenit 5, të ligjit nr. 157/2013, "Për masat kundër financimit të terrorizmit", të ndryshuar, me propozimin e ministrit për Evropën dhe Punët e Jashtme dhe të ministrit të Financave, Këshilli i Ministrave

VENDOSI:

I. Në vendimin nr. 1128, datë 30.12.2020, të Këshillit të Ministrave, të ndryshuar, bëhen këto shtesa:

1. Në pikën 3, të kreut I, pas fjalëve "... (CFSP) 2025/2072 ..." shtohen "... (CFSP) 2025/2398 ...".

2. Në aneksin 3, bashkëlidhur vendimit, shtohet vendimi (CFSP) 2025/2398, që i bashkëlidhet këtij vendimi.

II. Ngarkohen organet e parashikuara në pikën 1, të nenit 11, të ligjit nr. 72/2019, "Për masat shtrënguese ndërkombëtare në Republikën e Shqipërisë", të ndryshuar, dhe në pikën 1, të nenit 7,

të ligjit nr. 157/2013, "Për masat kundër financimit të terrorizmit", të ndryshuar, për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi menjëherë dhe botohet në Fletoren Zyrtare.

KRYEMINISTËR
Edi Rama

Gazeta Zyrtare e Bashkimit Evropian
AL Seria L
2025/2398
24.11.2025

VENDIMI I KËSHILLIT (CFSP) 2025/2398 i datës 24 nëntor 2025 që ndryshon Vendimin (CFSP) 2016/1693 mbi masat kufizuese kundër ISIL (Da'esh) dhe Al-Kaedës dhe personave, grupeve, ndërmarrjeve dhe subjekteve të lidhura me to

KËSHILLI I BASHKIMIT EVROPIAN,

Duke pasur parasysh Traktatin për Bashkimin Evropian, dhe në veçanti Nenin 29 të tij,

Duke pasur parasysh propozimin e Përfaqësueses së Lartë të Bashkimit për Punët e Jashtme dhe Politikën e

Sigurisë,

Ndërsa:

(1) Më 20 shtator 2016, Këshilli miratoi Vendimin (CFSP) 2016/1693 [1].

(2) Duke pasur parasysh kërcënimin e vazhdueshëm që paraqesin ISIL (Da'esh) dhe Al-Kaeda, si dhe personat, grupet, ndërmarrjet dhe subjektet e lidhura me to, një subjekt duhet të shtohet në listën e personave, grupeve, ndërmarrjeve dhe subjekteve të përcaktuara në Shtojcën e Vendimit (CFSP) 2016/1693.

(3) Duke pasur parasysh që subjekti që do të shtohet i nënshtrohet tashmë masave të përcaktuara në Vendimin e Këshillit 2010/788/CFSP [2], masat kufizuese përkatëse sipas Vendimit (CFSP) 2016/1693 duhet të pezullohen për atë subjekt për aq kohë sa masat e parashikuara në Vendimin 2010/788/CFSP zbatohen për të.

(4) Prandaj, Vendimi (CFSP) 2016/1693 duhet të ndryshohet në përputhje me rrethanat,

KA MIRATUAR KËTË VENDIM:

Neni 1

Vendimi (CFSP) 2016/1693 ndryshohet si më poshtë:

(1) në nenin 6, shtohet paragrafi i mëposhtëm:

'7. Masat e përmendura në nenin 3(3) dhe (4), për aq sa ato zbatohen për "Forcat Demokratike Aleate", do të pezullohen për aq kohë sa masat e përcaktuara në nenin 5(1) dhe (2) të Vendimit të Këshillit 2010/788/CFSP (*) zbatohen për atë entitet.

(*) Vendimi i Këshillit 2010/788/CFSP i 20 dhjetorit 2010 mbi masat kufizuese në lidhje me situatën në Republikën Demokratike të Kongos (OJ L 336, 21.12.2010, f. 30, ELI: http://data.europa.eu/eli/dec/2010/788/oj).';

(2) Shtojca e Vendimit (CFSP) 2016/1693 ndryshohet në përputhje me Shtojcën e këtij Vendimi.

(1) Vendimi i Këshillit (CFSP) 2016/1693 i datës 20 shtator 2016 mbi masat kufizuese kundër ISIL (Da'esh) dhe Al-Kaedës dhe personave, grupeve, ndërmarrjeve dhe subjekteve të lidhura me to dhe që shfuqizon Qëndrimin e Përbashkët 2002/402/CFSP (OJ L 255, 21.9.2016, f. 25, ELI: http://data.europa.eu/eli/dec/2016/1693/oj).

(2) Vendimi i Këshillit 2010/788/CFSP i 20 dhjetorit 2010 në lidhje me masat kufizuese në lidhje me situatën në Republikën Demokratike të Kongos (OJ L 336, 21.12.2010, f. 30, ELI: http://data.europa.eu/eli/dec/2010/788/oj).

Neni 2

Ky Vendim hyn në fuqi në datën e publikimit të tij në Gazetën Zyrtare të Bashkimit Evropian.

Bruksel, më 24 nëntor 2025.

Për Këshillin

President

L. LØKKE RASMUSSEN

SHTOJCË

Në Shtojcën e Vendimit (CFSP) 2016/1693, shtohet shënimi i mëposhtëm nën titullin "B. Grupet, ndërmarrjet dhe subjektet e përmendura në Nenin 3":

'8. Forcat Demokratike Aleate.'

Official Journal of the European Union
EN
L series

2025/2398
24.11.2025

COUNCIL DECISION (CFSP) 2025/2398

of 24 November 2025

amending Decision (CFSP) 2016/1693 concerning restrictive measures against ISIL (Da'esh) and Al-Qaeda and persons, groups, undertakings and entities associated with them

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Article 29 thereof,

Having regard to the proposal from the High Representative of the Union for Foreign Affairs and Security Policy,

Whereas:

(1) On 20 September 2016, the Council adopted Decision (CFSP) 2016/1693 [1].

(2) In view of the continued threat posed by ISIL (Da'esh) and Al-Qaeda and persons, groups, undertakings and entities associated with them, one entity should be added to the list of persons, groups, undertakings and entities set out in the Annex to Decision (CFSP) 2016/1693.

(3) Considering that the entity to be added is already subject to measures set out in Council Decision 2010/788/CFSP [2], the relevant restrictive measures under Decision (CFSP) 2016/1693 should be suspended for that entity for as long as the measures provided for in Decision 2010/788/CFSP apply to it.

(4) Decision (CFSP) 2016/1693 should therefore be amended accordingly,

HAS ADOPTED THIS DECISION:

Article 1

Decision (CFSP) 2016/1693 is amended as follows:

(1) in Article 6, the following paragraph is added:

'7. The measures referred to in Article 3(3) and (4), insofar as they apply to the "Allied Democratic Forces", shall be suspended for as long as the measures laid down in Article 5(1) and (2) of Council Decision 2010/788/CFSP (*) apply to that entity.

(*) Council Decision 2010/788/CFSP of 20 December 2010 concerning restrictive measures in view of the situation in the Democratic Republic of the Congo (OJ L 336, 21.12.2010, p. 30, ELI: http://data.europa.eu/eli/dec/2010/788/oj).';

(2) the Annex to Decision (CFSP) 2016/1693 is amended in accordance with the Annex to this Decision.

(1) Council Decision (CFSP) 2016/1693 of 20 September 2016 concerning restrictive measures against ISIL (Da'esh) and Al-Qaeda and persons, groups, undertakings and entities associated with them and repealing Common Position 2002/402/CFSP (OJ L 255, 21.9.2016, p. 25, ELI: http://data.europa.eu/eli/dec/2016/1693/oj).

(2) Council Decision 2010/788/CFSP of 20 December 2010 concerning restrictive measures in view of the situation in the Democratic Republic of the Congo (OJ L 336, 21.12.2010, p. 30, ELI: http://data.europa.eu/eli/dec/2010/788/oj).

Article 2

This Decision shall enter into force on the date of its publication in the *Official Journal of the European Union*.

Done at Brussels, 24 November 2025.

For the Council

The President

L. LØKKE RASMUSSEN

ANNEX

In the Annex to Decision (CFSP) 2016/1693, the following entry is added under heading 'B. Groups, undertakings and entities referred to in Article 3':

'8. Allied Democratic Forces.'.

VENDIM
Nr. 831, datë 30.12.2025

PËR MIRATIMIN E KODIT TË ETIKËS NË SHKENCË DHE NË KËRKIM SHKENCOR

Në mbështetje të nenit 100 të Kushtetutës dhe të pikës 1, të nenit 30, të ligjit nr. 109/2024, "Për shkencën dhe kërkimin shkencor në Republikën e Shqipërisë", me propozimin e ministrit të Arsimit, Këshilli i Ministrave

VENDOSI:

1. Miratimin e Kodit të Etikës në Shkencë dhe në Kërkim Shkencor, që zbatohet në zonën evropiane të kërkimit, në përputhje me Kodin Evropian të Sjelljes për Integritet në Kërkimin Shkencor, i cili rregullon normat e etikës në shkencë dhe në kërkim shkencor, që i bashkëlidhet këtij vendimi dhe është pjesë përbërëse e tij.

2. Ngarkohen ministria përgjegjëse për çështjet e shkencës dhe të kërkimit shkencor, subjektet publike dhe jopublike të kërkimit shkencor dhe punonjësit kërkimorë-shkencorë për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

KRYEMINISTËR
Edi Rama

KODI I ETIKËS NË SHKENCË DHE NË KËRKIM SHKENCOR

KREU I
DISPOZITA TË PËRGJITHSHME

Neni 1
Objekti

Objekti është përcaktimi i rregullave, normave, kritereve dhe procedurave të zbatimit të etikës në shkencë dhe në kërkim shkencor, bazuar në Kodin Evropian të Sjelljes për Integritet në Kërkimin Shkencor, që duhet të zbatohen nga institutet dhe njësitë e veçanta kërkimore-shkencore, institucionet e arsimit të lartë, institucionet kërkimore, punonjësit kërkimorë-shkencorë dhe financuesit e shkencës dhe të kërkimit shkencor.

Neni 2
Qëllimi

Ky kod ka për qëllim të përcaktojë integritetin shkencor, parimet themelore të etikës në shkencë dhe në kërkim shkencor, normat bazë të sjelljes, praktikat e mira të shkencës dhe të kërkimit shkencor, llojet e shkeljeve e të masave disiplinore, procedurat për dhënien e tyre, në rastin e shkeljeve të etikës në shkencë dhe në kërkim shkencor, risqet dhe sistemin e menaxhimit të tyre për institutet dhe njësitë e veçanta kërkimore-shkencore, institucionet e arsimit të lartë dhe institucionet e tjera kërkimore.

Neni 3
Fusha e zbatimit

Kodi zbatohet nga të gjitha institutet dhe njësitë e veçanta kërkimore-shkencore, institucionet e arsimit të lartë, institucionet kërkimore, punonjësit kërkimorë-shkencorë dhe financuesit e shkencës dhe të kërkimit shkencor, ku kryhet veprimtari kërkimore-shkencore, duke siguruar integritet dhe transparencë në kërkimin shkencor.

KREU II
PARIMET THEMELORE TË ETIKËS NË SHKENCË DHE NË KËRKIM SHKENCOR

Neni 4
Besueshmëria

Ky parim siguron që cilësia e veprimtarisë kërkimore-shkencore të pasqyrojë në mënyrë të besueshme sigurimin e cilësisë në shkencë dhe në kërkim shkencor, në projektim, në metodologjinë, analizën e në përdorueshmërinë e burimeve.

Neni 5
Ndershmëria

Ky parim ka qëllim garantimin e ndershmërisë në zhvillimin, realizimin, shqyrtimin, raportimin dhe komunikimin e kërkimit në një mënyrë transparente, të drejtë dhe të plotë.

Neni 6
Respekti

Çdo pjesëmarrës në veprimtarinë kërkimore-shkencore ka detyrimin të respektojë kolegët, subjektet e kërkimit, shoqërinë, ekosistemet, trashëgiminë kulturore dhe mjedisin.

Neni 7
Përgjegjshmëria

Parimi i përgjegjshmërisë për menaxhimin dhe organizimin e kërkimit shkencor pasqyrohet në formimin, mbikëqyrjen dhe mentorimin e kërkuesve.

Neni 8
Transparenca

Punonjësi kërkimor-shkencor siguron që të dhënat, metodat dhe rezultatet e kërkimit janë të disponueshme e të qarta për të gjithë, duke zbatuar katër parimet themelore të shkencës së hapur (të gjetshme, të aksesueshme, të ndërveprueshme, të ripërdorshme), në mënyrë të drejtë dhe transparente, duke njohur kontributet e çdo individi të përfshirë në procesin kërkimor-shkencor, në përputhje me legjislacionin në fuqi.

KREU III
PRAKTIKAT E MIRA TË SHKENCËS DHE TË KËRKIMIT SHKENCOR

Neni 9
Praktikat e mira kërkimore-shkencore

Praktikat e mira të shkencës dhe të kërkimit shkencor shërbejnë si model për institutet dhe njësitë e veçanta kërkimore-shkencore për të siguruar se rezultatet e kërkimit shkencor janë të sakta, të besueshme dhe në përputhje me standardet etike, në zbatim të kuadrit ligjor në fuqi.

Neni 10
Hartimi dhe procesi i projektit kërkimor-shkencor

Çdo projekt kërkimor-shkencor ndjek protokolle të qarta kërkimore, nga ku planifikohet, hartohet dhe strukturohet në mënyrë të qartë, me standarde të larta, transparence dhe dokumentimi, duke pasur parasysh objektivat, metodologjinë, marrjen e mostrës shkencore, si dhe metodat e mbledhjes e të analizës së të dhënave.

Neni 11
Mbrojtja e të dhënave

Të dhënat e mbledhura gjatë veprimtarisë kërkimore-shkencore ruhen në mënyrë të sigurt. Subjektet kërkimore-shkencore ndërmarrin masa teknike dhe organizative të përshtatshme për të mbrojtur të dhënat nga shkatërrime të paligjshme, humbje aksidentale, për të mbrojtur aksesin ose përhapjen nga persona të paautorizuar, veçanërisht kur përpunimi i të dhënave bëhet në rrjet, si dhe nga çdo formë tjetër e paligjshme përpunimi. Çdo veprim në sistem lidhur me aksesin, ndryshimin, korrigjimin, përhapjen e të dhënave etj., duhet të lërë gjurmë, me qëllim garantimin e sigurisë e të konfidencialitetit të të dhënave.

Neni 12
Publikimi dhe e drejta e autorit

Veprimtaria kërkimore-shkencore ndërtohet mbi bazën e publikimit të veprës, ndikimit dhe njohjes në një fushë të caktuar kërkimore e të subjekteve të tjera të përfshira. Njohja e kontributit të autorëve duhet të bëhet në mënyrë të drejtë, duke siguruar, që çdo individ që ka kontribuuar në projektin kërkimor, të përfitojë sipas legjislacionit në fuqi për mbrojtjen e të drejtave të autorit e të të drejtave të tjera të lidhur me të. Çdo subjekti i lind e drejta për rishikimin e punës së tij kërkimore, me qëllim e vlerësimin përfundimtar të saj.

Neni 13
Përputhshmëria me ligjin dhe etikën

Punonjësi kërkimor-shkencor siguron se çdo kërkim shkencor të kryhet në përputhje me kuadrin rregullator në fuqi, duke respektuar etikën në kërkimin shkencor, të drejtat e personave fizikë dhe juridikë të përfshirë në kërkimin shkencor.

Neni 14
Mjedisi i kërkimit shkencor

Institucionet kërkimore-shkencore dhe institucionet e arsimit të lartë janë mjediset që nxisin ndërgjegjësimin dhe ofrojnë burime të nevojshme për sigurimin e një kulture kërkimore-shkencore, duke garantuar mjedis të respektit të ndërsjellë të barazisë e të gjithëpërfshirjes.

Neni 15
Trajnimi, mbikëqyrja dhe udhëheqja

Institucionet kërkimore-shkencore dhe institucionet e arsimit të lartë sigurojnë që kërkuesit shkencorë të marrin një formim profesional në hartimin e projektit kërkimor-shkencor, metodologjinë, analizën, shpërndarjen dhe komunikimin shkencor, duke zhvilluar programe të përshtatshme dhe eficiente të trajnimeve për pajisjen me aftësitë e nevojshme. Trajnimi, mbikëqyrja dhe udhëheqja e kërkuesit realizohet mbi bazën e modeleve të praktikave të mira shkencore.

Neni 16
Menaxhimi dhe praktika e të dhënave

Institucionet kërkimore-shkencore dhe institucionet e arsimit të lartë sigurojnë menaxhimin, ruajtjen dhe mbrojtjen, sipas legjislacionit në fuqi, të të gjitha të dhënave kërkimore e të materialeve të tjera kërkimore. Menaxhimi dhe praktika e të dhënave realizohet në zbatim të parimeve të shkencës së hapur.

Neni 17
Bashkëpunimi

Të gjitha subjektet, që kryejnë veprimtari kërkimore-shkencore, bien dakord në mënyrë formale, që të ndërtojnë marrëdhënie mbi bazën e bashkëpunimit real, etik, profesional e frytdhënës, duke respektuar integritetin kërkimor dhe pronësinë intelektuale.

Neni 18
Integriteti i kërkimit shkencor në praktikë

1. Institutet apo njësitë e veçanta kërkimore-shkencore zbatojnë standarde kombëtare dhe evropiane të integritetit në çdo fazë të procesit të kërkimit. Kjo përfshin planifikimin, realizimin dhe raportimin e kërkimeve. Proceset kërkimore-shkencore duhet të jenë të hapura e të verifikueshme, duke siguruar transparencë e besueshmëri.

2. Publikimi është një komponent kyç i kërkimit shkencor. Punonjësit kërkimorë-shkencorë dhe institutet ose njësitë e veçanta kërkimore-shkencore sigurojnë që procesi i publikimit të ndjekë parime etike, duke përfshirë transparencën në lidhje me autorësinë, financimin e çdo konflikti interesi.

3. Institutet dhe njësitë e veçanta kërkimore-shkencore, për të siguruar cilësinë dhe saktësinë e veprimtarisë kërkimore-shkencore, zhvillojnë mekanizma të vlerësimit e të verifikimit të rezultateve, sipas legjislacionit në fuqi.

KREU IV
LLOJET E SHKELJEVE E TË MASAVE DISIPLINORE, SI DHE PROCEDURAT PËR DHËNIEN E TYRE NË RASTIN E SHKELJEVE TË ETIKËS NË SHKENCË DHE NË KËRKIM SHKENCOR

Neni 19
Shkeljet e etikës në shkencë dhe në kërkim shkencor

1. Nëse punonjësi kërkimor-shkencor, në ushtrimin e veprimtarisë së tij kërkimore-shkencore cenon integritetin dhe etikën e kërkimit shkencor, duke ndikuar në besueshmërinë e cilësinë e tij, ky cenim konsiderohet si shkelje e etikës në shkencë dhe në kërkim shkencor.

2. Për përcaktimin e masës këshilluese ose disiplinore të zbatueshme, Komiteti i Etikës bazohet në:

a) shkaqet, rrethanat e kryerjes së shkeljes, rëndësinë dhe pasojat e ardhura prej saj;

b) shkallën e fajësisë;

c) ekzistencën e masave të tjera disiplinore të mëparshme.

3. Masat këshilluese ose disiplinore jepen në raport të drejtë me shkeljen e kryer.

4. Shkeljet e etikës në veprimtarinë kërkimore-shkencore janë, si më poshtë vijon:

a) Fabrikimi, i cili është manipulimi i të dhënave ose i rezultateve dhe regjistrimi a publikimi i tyre, si të vërteta;

b) Falsifikimi është manipulimi i materialeve kërkimore, pajisjeve, imazheve ose proceseve apo ndryshimi, fshirja a retushimi i të dhënave ose rezultateve pa asnjë motiv;

c) Mosraportimi i konfliktit të interesit në veprimtarinë kërkimore-shkencore, i cili është mosdeklarimi i konfliktit të interesit apo të konfliktit të mundshëm të interesit, duke ndikuar në besueshmërinë dhe në objektivitetin e kërkimit shkencor;

ç) Plagjiatura është përdorimi i punës ose ideve të dikujt tjetër, pa dhënë asnjë meritë te burimi origjinal.

5. Parimet për trajtimin e shkeljeve dhe akuzave për sjellje të papranueshme janë, si më poshtë vijon:

a) Kushdo që akuzohet për shkelje të etikës në shkencë dhe në kërkim shkencor prezumohet i pafajshëm derisa të provohet e kundërta;

b) Palët e përfshira në hetim deklarojnë çdo konflikt interesi, që mund të lindë gjatë hetimit;

c) Hetimet kryhen në mënyrë konfidenciale, me qëllim mbrojtjen e palëve në proces;

ç) Procedurat e përgjithshme për trajtimin e shkeljeve të praktikës së mirë të kërkimit shkencor janë transparente dhe garantojnë uniformitetin e tyre;

d) Personave të akuzuar për shkelje të etikës në shkencë dhe në kërkim shkencor u garantohet një proces i drejtë administrativ gjatë procesit të hetimit.

Neni 20
Masat këshilluese

1. Masat këshilluese propozohen nga Komiteti i Etikës dhe jepen nga titullari i institutit apo njësisë së veçantë të kërkimit shkencor.

2. Masat këshilluese konsiderohen:

a) "Tërheqja e vëmendjes", në rastet kur punonjësi kërkimor-shkencor nuk respekton këshillat, rekomandimet ose procedurat e strukturave eprore;

b) "Tërheqje e vëmendjes dhe paralajmërim për dhënie mase disiplinore", kur nuk është zbatuar propozimi për ndryshimin e metodologjisë dhe të praktikave të aplikuara përgjatë veprimtarisë kërkimore-shkencore nga punonjësit kërkimorë-shkencorë;

c) "Paralajmërim për pezullim të veprimtarisë kërkimore-shkencore", në rastin kur duhet të realizohet rihartimi i projektit kërkimor-shkencor, në çdo fazë, nga punonjësi kërkimor-shkencor;

ç) "Vërejtje për shkelje të përsëritur dhe pezullim të veprimtarisë kërkimore-shkencore", njoftimi për rishikimin dhe ridimensionimin e projektit kërkimor-shkencor nga Komiteti i Etikës.

Neni 21
Shkeljet e etikës

1. Shkeljet e etikës në shkencë dhe në kërkim shkencor të masave këshilluese kategorizohen si:

a) shkelje të lehta, që konsiderohen:

i. mosrespektimi i këshillave ose i rekomandimeve të udhëheqësit shkencor;

ii. mosrespektimi i procedurave etike të vendosura nga strukturat eprore;

iii. mosrespektimi i metodologjive të kërkimit nga kërkuesit shkencorë;

iv. mosrespektimi i praktikave të mira të kërkimit nga kërkuesit shkencorë.

b) shkelje të rënda, që konsiderohen:

i. mosrespektimi i përsëritur i këshillave ose i rekomandimeve të udhëheqësit shkencor, duke mos rihartuar projektin në çdo fazë;

ii. mosrespektimi i përsëritur i korrigjimit të metodologjive ose praktikave të mira, të kërkimit shkencor, duke rishikuar dhe ridimensionuar projektin kërkimor-shkencor.

c) shkelje shumë të rënda, që konsiderohen:

i. mosrespektimi i çdo parimi dhe kriteri etik të këtij kodi;

ii. mosrespektimi i konfidencialitetit dhe i bërjes publike të materialeve konfidenciale të veprimtarisë kërkimore-shkencore.

Neni 22
Shkeljet disiplinore

1. Shkeljet në shkencë dhe në kërkim shkencor kategorizohen si:

a) shkelje të lehta, që konsiderohen:

i. manipulimi i produktit autorial, të paktën në një rast;

ii. mosdeklarimi i drejtpërdrejtë i faktit të një konflikti interesi të drejtpërdrejtë ose të mundshëm përgjatë procesit kërkimor-shkencor;

b) shkelje të rënda, që konsiderohen:

i. plagjiatura e konstatuar sipas kritereve në legjislacionin në fuqi;

ii. kompromentimi i etapave të ndryshme të veprimtarisë së kërkimit shkencor;

iii. manipulimi i tërthortë ose i plotë i rezultateve, dokumentacioneve, metodologjive, të dhënave, që mundësojnë rezultatin e dëshiruar nga punonjësi kërkimor-shkencor;

iv. mosrespektimi i 1 deri në 2 parimeve dhe i standardeve themelore, në zbatim të parimit të shkencës së hapur;

v. manipulimi i 1 deri në 2 të dhënave të veprimtarisë kërkimore-shkencore, në prezantimin e një rezultati të rremë;

vi. abuzimi me burimet financiare, kur shkaktohet dëm ekonomik, deri në masën 15% të buxhetit total të projektit;

c) shkelje shumë të rënda, që konsiderohen:

i. plagjiatura e përsëritur e evidentuar, sipas kritereve në legjislacioni në fuqi;

ii. mosrespektimi i çdo kriteri dhe standardi, që mundësojnë zbatimin e parimit të shkencës së hapur në Republikën e Shqipërisë;

iii. mosrespektimi i çdo parimi të Kodit të Etikës në Shkencë dhe në Kërkim Shkencor, sipas legjislacionit në fuqi;

iv. tjetërsimi i dokumentacionit, metodologjisë, të dhënave të kërkimit-shkencor në rezultatet përfundimtare, të veprimtarisë kërkimore-shkencore, duke prezantuar një rezultat të rremë.

Neni 23
Masat disiplinore

1. Masat disiplinore propozohen nga Komiteti i Etikës dhe jepen nga titullari i institutit apo njësisë së veçantë të kërkimit shkencor.

2. Masat disiplinore jepen në varësi të llojeve të shkeljeve të Kodit të Etikës në Shkencë dhe në Kërkimin Shkencor dhe klasifikohen, si më poshtë vijon:

a) Shkelje të lehta janë, si vijon:

i. "Vërejtje me shkrim", jepet për nënndarjen "i", të shkronjës "a", të pikës 2, të nenit 22;

ii. "Vërejtje me shkrim dhe trajnim për zbatimin e kodit të etikës në kërkimin shkencor", jepet për nënndarjen "ii", të shkronjës "a", të pikës 2, të nenit 22;

iii. "Vërejtje me shkrim dhe reduktim i pagës me 30%", jepet për nënndarjen "ii", të shkronjës "a", të pikës 2, të nenit 22;

b) Shkelje të rënda janë, si vijon:

i. "Reduktim i pagës nga 30% deri në 70% përgjatë zhvillimit të projektit shkencor" jepet për nënndarjen "i", të shkronjës "b", të pikës 2, të nenit 22;

ii. "Vërejtje me shkrim për përjashtim nga projektet kërkimore-shkencore", jepet për nënndarjen "ii", të shkronjës "b", të pikës 2, të nenit 22;

iii. "Paralajmërim për ndërprerjen e kërkimit shkencor", jepet për nënndarjet "iii", "iv" "v" dhe "vi", të shkronjës "b", të pikës 2, të nenit 22;

c) Shkelje shumë të rënda janë, si vijon:

i. "Transferimi i kërkimit shkencor një kërkuesi tjetër shkencor", jepet për nënndarjen "i", të shkronjës "c", të pikës 2, të nenit 22;

ii. "Revokimi, shkurtimi ose ndërprerja, rimbursimi i fondeve të kërkimit shkencor", jepet për nënndarjen "ii", të shkronjës "c", të pikës 2, të nenit 22;

iii. "Përjashtimi përkohësisht për të marrë pjesë në aktivitete dhe kërkime shkencore", jepet për nënndarjen "iii", të shkronjës "c", të pikës 2, të nenit 22;

iv. "Shfuqizimi i kategorisë së punonjësit të kërkimit shkencor", jepet për nënndarjen "iv", të shkronjës "c", të pikës 2, të nenit 22.

3. Masat disiplinore parashkruhen sipas kalimit të këtyre afateve për:

a) shkelje të lehta, brenda 3 viteve;

b) shkelje të rënda, brenda 4 viteve;

c) shkelje shumë të rënda, brenda 5 viteve.

4. Masa disiplinore më e rëndë specifikohet në pikën 3, të nenit 32, të ligjit nr. 109/2024, ku përcaktohet se masa disiplinore më e rëndë është shfuqizimi i kategorisë së punonjësit të kërkimit shkencor, e cila jepet vetëm për shkelje të rënda të etikës së kërkimit shkencor.

5. Parimi i ligjshmërisë, proporcionalitetit dhe trajtimit të barabartë duhet të zbatohet gjatë përcaktimit të masës disiplinore, që propozohet nga Komiteti i Etikës.

6. Propozimi i dhënies së masës disiplinore përkatëse jepet në varësi të llojit, masës dhe dëmit të shkaktuar nga kryerja e shkeljes.

Neni 24
Procedurat për dhënien e masave disiplinore

1. Instituti apo njësia e veçantë kërkimore-shkencore përcakton në rregulloren e saj të brendshme rregullat dhe procedurën, që paraqiten në lidhje me ankimimin e masave disiplinore.

2. Forma procedurale e zhvillimit të procedurës për shqyrtimin e ankimit dhe dhënien e masës organizohet sipas legjislacionit në fuqi për organizimin dhe funksionimin e institutit apo njësisë së veçantë kërkimore-shkencore.

3. Regjistrimi, hetimi dhe trajtimi i ankesave për shkelje të mundshme të integritetit në shkencë dhe në kërkim shkencor realizohet nga Komiteti i Etikës, i cili ngrihet pranë çdo institucioni kërkimor-shkencor dhe institucionit të arsimit të lartë.

4. Gjatë shqyrtimit të ankesës ruhet konfidencialiteti i ankimimit.

5. Palët e përfshira në procesin e shqyrtimit të ankimit kanë të drejtë të dëgjohen, të përfaqësohen dhe të paraqesin prova.

6. Procedura fillestare e shqyrtimit të ankesës duhet të realizohet brenda 30 ditëve nga marrja e njoftimit për ankesën.

7. Dëgjesa e kërkuesit të akuzuar për shkelje të Kodit të Etikës realizohet sipas standardeve të përshtatshme të hetimit dhe kërkuesi, gjithashtu, ka të drejtën për të mos dëshmuar, nëse nuk dëshiron.

8. Procedura e shqyrtimit të ankesës duhet të realizohet sipas procedurave dhe afateve të përcaktuara në Kodin e Procedurave Administrative.

9. Në rast të parregullsive dhe të dyshimit lidhur me procedurën e ndjekur, organizata dhe/ose institucioni apo kërkuesi mund t'i drejtohen organit gjyqësor kompetent për shqyrtim të mëtejshëm.

Neni 25
Përgjegjësitë e instituteve apo njësive të veçanta të kërkimit shkencor

1. Instituti apo njësia e veçantë kërkimore-shkencore zhvillon dhe zbaton politikat dhe rregulloret, në lidhje me integritetin në kërkimin shkencor, etikën, autorësinë, menaxhimin e të dhënave dhe konfliktin e interesit. Politikat dhe rregulloret janë të disponueshme për publikun dhe janë në përputhje me standardet kombëtare dhe praktikat më të mira ndërkombëtare.

2. Instituti apo njësia e veçantë kërkimore-shkencore mbështet nismat e shkencës së hapur, përfshirë botimin me akses të hapur dhe ndarjen e të dhënave, në përputhje me politikat evropiane të kërkimit shkencor dhe zhvillimet digjitale të Shqipërisë dhe të BE-së.

3. Integriteti është pjesë e vlerësimit institucional, rekrutimit, promovimit dhe kritereve të financimit.

4. Institutet dhe njësitë e veçanta kërkimore-shkencore janë të detyruara:

a) të pranojnë dhe të regjistrojnë ankesa për shkelje të mundshme të integritetit në shkencë dhe në kërkim shkencor;

b) të hetojnë këto ankesa në mënyrë të shpejtë, të ndershme dhe në përputhje me procedurën e parashikuar në legjislacionin në fuqi;

c) të mbrojnë të drejtat e të gjitha palëve të përfshira në procedurën e hetimit administrativ;

ç) të zbatojnë masa këshilluese apo disiplinore proporcionale, kur konstatohen shkelje.

Neni 26
Zbatimi dhe përputhshmëria

1. Institutet dhe njësitë e veçanta kërkimore-shkencore kontribuojnë në veprimtarinë kërkimore-shkencore, duke zhvilluar sisteme për monitorimin e zbatimit të këtij kodi, duke vlerësuar përputhshmërinë e veprimtarisë së punonjësve kërkimorë-shkencorë, instituteve dhe njësive të veçanta kërkimore-shkencore me politikat e integritetit shkencor.

2. Në rastet kur shkeljet e integritetit shkencor konfirmohen, institutet ose njësitë e veçanta kërkimore-shkencore duhet të zbatojnë këtë kod dhe legjislacionin në fuqi.

3. Institutet apo njësitë e veçanta kërkimore-shkencore sigurojnë mbështetje për individët që kryejnë veprimtari kërkimore-shkencore, duke ofruar mundësi trajnimi e udhëzimi për përmirësimin e mëtejshëm të praktikave të tyre kërkimore-shkencore dhe etike.

Neni 27
Sanksionet

Shkeljet e rregullave të parashikuara në këtë kod, kur veprimet e tyre nuk përbëjnë vepër penale, ndiqen në rrugë administrative, sipas legjislacionit në fuqi.

KREU V
RISQET DHE SISTEMI I MENAXHIMIT TË TYRE NË SHKENCË DHE NË KËRKIM SHKENCOR

Neni 28
Risqet dhe sistemi i menaxhimit të tyre

1. Risqet në veprimtarinë kërkimore-shkencore konsiderohen elementet, të cilat ndikojnë në vërtetësinë dhe cilësinë e punës kërkimore-shkencore dhe produktin final të kërkimit shkencor.

2. Risqet që mund të paraqiten gjatë veprimtarisë kërkimore-shkencore janë, si më poshtë vijon:

a) paaftësia për realizimin e rekomandimeve ose plotësimin e kërkesave të Komisionit të Etikës, në mangësi të aftësive menaxheriale profesionale;

b) mospërditësimi dhe mosnjohja me aktet e ndryshme, që ndërlidhen me veprimtarinë kërkimore-shkencore nga kërkuesi shkencor;

c) shkelja e parimeve etike e të integritetit shkencor (plagjiatura, manipulimi i të dhënave, autorësi e pasaktë);

ç) konflikti i interesit dhe ndikimi i papërshtatshëm në rezultatet e kërkimit shkencor, cenimi i konfidencialitetit dhe i mbrojtjes së të dhënave, rreziqeve të sigurisë laboratorike dhe në terren, rreziqet e biosigurisë dhe rreziqet mjedisore;

d) rreziqet që cenojnë pronësinë intelektuale dhe rrjedhja e informacionit;

dh) rreziqet operacionale;

e) rreziqet financiare/procedurale;

ë) rreziqet reputacionale dhe komunikimi;

f) cenimi i sistemit të menaxhimit të risqeve, duke anashkaluar identifikimin, vlerësimin, masat paraprake dhe korrigjuese, procedurat e raportimit të incidenteve e të shkeljeve, trajnimin periodik, si dhe dokumentimin dhe rishikimin periodik të risqeve gjatë të gjithë ciklit të projektit.

3. Menaxhimi i risqeve dhe procedurave përkatëse, që mund të paraqiten gjatë veprimtarisë kërkimore-shkencore, parashikohen në aktet e brendshme rregullatore të instituteve e të njësive të veçanta kërkimore-shkencore, institucionet e arsimit të lartë dhe institucionet kërkimore, sipas fushës/ave kërkimore-shkencore që ato zhvillojnë.

VENDIM
Nr. 832, datë 30.12.2025

PËR KRIJIMIN E BAZËS SË TË DHËNAVE SHTETËRORE TË SISTEMIT TË MENAXHIMIT TË INFORMACIONIT TË ARSIMIT TË LARTË (SMIAL)

Në mbështetje të nenit 100 të Kushtetutës dhe të nenit 4, të ligjit nr. 10325, datë 23.9.2010, "Për bazat e të dhënave shtetërore", me propozimin e ministrit të Arsimit, Këshilli i Ministrave

VENDOSI:

1. Krijimin e bazës së të dhënave shtetërore të Sistemit të Menaxhimit të Informacionit të Arsimit të Lartë (në vijim SMIAL).

2. Institucioni administrues i bazës së të dhënave shtetërore SMIAL është Qendra e Shërbimeve Arsimore.

3. Të dhënat e bazës shtetërore ndahen në të dhëna parësore dhe dytësore, si më poshtë vijon:

a) Të dhënat parësore të SMIAL-it konsiderohen të dhënat e mbledhura nga Qendra e Shërbimeve Arsimore, që kanë të bëjnë me:

i. të dhënat e regjistrimit të studentëve në çdo program studimi;

ii. numrin e identifikimit të matrikullimit të studentit;

iii. informacionin për statusin për pajisjen me numër matrikullimi;

iv. mbështetjen financiare dhe kreditë studentore;

v. strukturën e institucioneve të arsimit të lartë;

vi. hapjen, riorganizimin dhe mbylljen e IAL-ve, degëve, njësive kryesore dhe bazë e të programeve të studimit;

vii. programet e studimit me profilet e tyre, si dhe kuotat e pranimit në to;

viii. certifikimin e kapaciteteve akademike dhe infrastrukturore për kuotat e pranimit në programet e studimit të ofruara nga IAL-të;

ix. udhëheqjet shkencore në programet e studimit për fitimin e gradës shkencore "Doktor";

x. projektstatutet dhe ndryshimet statutore të IAL-ve;

xi. informacione për aktet e hapjes/ riorganizimit dhe akreditimit të parë e periodik të IAL-ve e të programeve të studimit;

xii. regjistrimin e formave të diplomave dhe certifikatave, të cilat lëshohen nga institucionet e arsimit të lartë;

xiii. pajisjen e institucioneve të arsimit të lartë me regjistrat themeltarë, të arritjeve akademike e të lëshimit të diplomave dhe të certifikatave;

xiv. njohjen e njësimin e diplomave dhe të certifikatave të lëshuara nga institucionet e huaja të arsimit të lartë;

xv. njohjen e titujve akademikë të lëshuar nga institucionet e arsimit të lartë të huaj;

b) Të dhënat dytësore të SMIAL-it konsiderohen të dhënat që merren nga Regjistri Kombëtar i Gjendjes Civile, Regjistri Elektronik Kombëtar për të Huajt në Republikën e Shqipërisë, Regjistri Tregtar dhe nga Sistemi i Tatimit Elektronik, si më poshtë vijon:

i. emri, atësia, amësia, mbiemri;

ii. numri i identifikimit personal;

iii. datëlindja, gjinia, vendlindja;

iv. statusi civil;

v. adresa e vendbanimit;

vi. shtetësia;

vii. të dhënat personale të studentëve të huaj;

viii. të dhënat NUIS/NIPT të institucioneve publike dhe jopublike të arsimit të lartë.

4. Dhënës të informacionit për SMIAL-in janë institucionet e arsimit të lartë, Agjencia e Sigurimit të Cilësisë në Arsimin e Lartë, Agjencia Kombëtare e Financimit të Arsimit të Lartë dhe ministria përgjegjëse për arsimin.

5. Sistemi SMIAL ndërvepron me:

a) bazën e të dhënave shtetërore të Regjistrit Kombëtar të Gjendjes Civile;

b) Sistemin e Provimit të Shtetit dhe provimeve të tjera të digjitalizuara;

c) Regjistrin Elektronik Kombëtar për të Huajt në Republikën e Shqipërisë;

ç) Regjistrin Tregtar dhe Sistemin e Tatimit Elektronik.

6. Institucioni administrues siguron që përpunimi i të dhënave personale në SMIAL të kryhet në përputhje me parimet dhe kërkesat e legjislacionit për mbrojtjen e të dhënave personale, duke garantuar ligjshmërinë, drejtësinë, transparencën, minimizimin e të dhënave, saktësinë dhe ruajtjen e tyre, vetëm për periudhën e nevojshme për të përmbushur qëllimin e grumbullimit. Pas përfundimit të afatit të përcaktuar të ruajtjes, të dhënat personale fshihen ose anonimizohen, sipas procedurave të miratuara nga institucioni administrues, në përputhje me legjislacionin në fuqi.

7. Niveli i aksesimit në sistemin SMIAL bazohet në rolet e krijuara të përdoruesve:

a) Ministria përgjegjëse për arsimin për:

i. hapjen, riorganizimin dhe mbylljen e IAL-ve, degëve, njësive kryesore e të programeve të studimit, si lexues, konfirmues dhe përditësues;

ii. certifikimin e kapaciteteve akademike e infrastrukturore në sistem dhe kuotat e pranimit në programet e studimit të ofruara nga IAL-të, si lexues dhe konfirmues;

iii. udhëheqjet shkencore në programet e studimit për fitimin e gradës shkencore "Doktor", si lexues dhe konfirmues;

iv. projektstatutet dhe ndryshimet statutore të IAL-ve, si lexues e konfirmues;

b) Qendra e Shërbimeve Arsimore për:

i. hapjen, riorganizimin dhe mbylljen e IAL-ve, degëve, njësive kryesore dhe bazë e të programeve të studimit, si lexues;

ii. programet e studimit me profilet e tyre, si dhe kuotat e pranimit në to, si lexues;

iii. të dhënat e regjistrimit të studentëve në çdo program studimi, si lexues dhe konfirmues;

iv. gjenerimin, numrin e identifikimit të matrikullimit të studentit, si krijues;

v. certifikimin e kapaciteteve akademike dhe infrastrukturore për kuotat e pranimit në programet e studimit të ofruara nga IAL-të, si lexues;

vi. udhëheqjet shkencore në programet e studimit për fitimin e gradës shkencore "Doktor", si lexues;

vii. regjistrimin e formave të diplomave dhe të certifikatave, të cilat lëshohen nga institucionet e arsimit të lartë, si lexues e konfirmues;

viii. pajisjen e institucioneve të arsimit të lartë me regjistrat themeltarë, të arritjeve akademike e të lëshimit të diplomave dhe certifikatave, si lexues dhe konfirmues;

ix. njohjen e njësimin e diplomave e të certifikatave të lëshuara nga institucionet e huaja të arsimit të lartë, si lexues dhe konfirmues;

x. njohjen e titujve akademikë, të lëshuar nga institucionet e arsimit të lartë të huaj, si lexues dhe konfirmues;

c) Agjencia e Sigurimit të Cilësisë në Arsimin e Lartë për:

i. hapjen, riorganizimin dhe mbylljen e IAL-ve, degëve, njësive kryesore dhe bazë e të programeve të studimit, si lexues;

ii. të dhënat për akreditimin e parë të IAL-ve e të programeve të studimit, si lexues dhe përditësues;

iii. të dhënat për akreditimin periodik të IAL-ve e të programeve të studimit, si lexues dhe përditësues.

ç) Agjencia Kombëtare e Financimit të Arsimit të Lartë për:

i. të dhënat për mbështetjen financiare të studentëve, si lexues dhe konfirmues;

ii. të dhënat për kreditë studentore, si lexues dhe konfirmues;

d) Institucioni i arsimit të lartë për:

i. të dhënat për strukturën organizative të institucioneve të arsimit të lartë, njësitë, programet e studimit dhe profilet e tyre, si krijues;

ii. projektstatutet dhe ndryshimet statutore të IAL-ve, si krijues e përditësues;

iii. kuotat dhe rialokimet e tyre, në bazë të certifikimit të tyre nga ministria përgjegjëse për arsimin, për çdo program studimi dhe profil, si krijues;

iv. të dhënat për regjistrimin, transferimin, pezullimin, çregjistrimin e diplomimin e studentëve, si krijues dhe përditësues;

v. të dhënat e studentëve për pajisjen me numër matrikullimi, si krijues dhe përditësues;

vi. mbështetjen financiare dhe kredinë studentore, si krijues dhe përditësues;

vii. regjistrimin e formave të diplomave e të certifikatave, të cilat lëshohen nga institucionet e arsimit të lartë, si krijues dhe përditësues;

viii. pajisjen e institucioneve të arsimit të lartë me regjistrat themeltarë të arritjeve akademike dhe të lëshimit të diplomave e të certifikatave, si krijues dhe përditësues.

8. Organizimi e funksionimi i brendshëm i sistemit dhe i bazës së të dhënave të SMIAL-it përcaktohen e miratohen me rregullore të brendshme të institucionit administrues, në përputhje me parashikimet e ligjit nr. 10325, datë 23.9.2010, "Për bazën e të dhënave shtetërore".

9. Palët zbatojnë masat e duhura teknike dhe organizative për të siguruar një nivel sigurie të përshtatshëm ndaj rrezikut, për çdo veprim në regjistër lidhur me aksesin, ndryshimin, korrigjimin, përhapjen e të dhënave personale, me qëllim garantimin e gjurmueshmërisë, konfidencialitetit, integritetit, disponueshmërinë dhe qëndrueshmërinë e sistemeve e të shërbimeve të përpunimit.

10. Ngarkohen Ministria e Arsimit, Qendra e Shërbimeve Arsimore, Agjencia e Sigurimit të Cilësisë në Arsimin e Lartë, Agjencia Kombëtare e Financimit të Arsimit të Lartë dhe institucionet e arsimit të lartë për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

KRYEMINISTËR
Edi Rama

VENDIM
Nr. 833, datë 30.12.2025

PËR MIRATIMIN E STANDARDEVE E TË KRITEREVE QË MUNDËSOJNË ZBATIMIN E PARIMIT TË SHKENCËS SË HAPUR DHE JANË NË PËRPUTHJE ME POLITIKAT E ZONËS EVROPIANE TË KËRKIMIT

Në mbështetje të nenit 100 të Kushtetutës dhe të pikës 6, të nenit 5, të ligjit nr. 109/2024, "Për shkencën dhe kërkimin shkencor në Republikën e Shqipërisë", me propozimin e ministrit të Arsimit, Këshilli i Ministrave

VENDOSI:

I. TË PËRGJITHSHME

1. Zbatimi i parimit të shkencës së hapur nga institucionet që zhvillojnë kërkim shkencor në Republikën e Shqipërisë realizohet në përputhje me standardet dhe kriteret e parashikuara në këtë

vendim, të cilat janë në përputhje me ato të zonës evropiane të kërkimit.

2. Zbatimi i parimit të shkencës së hapur në të gjithë veprimtarinë e kërkimit shkencor synon rritjen e bashkëpunimit kërkimor-shkencor dhe shkëmbimin e informacionit në dobi të shkencës dhe shoqërisë, duke e bërë veprimtarinë e kërkimit shkencor të arritshme dhe transparente për të gjithë.

II. STANDARDET E SHKENCËS SË HAPUR

Qasja e hapur në veprimtarinë e kërkimit shkencor gjen zbatim në:

1. Publikimet shkencore, si më poshtë vijon:

a) Institucionet që zhvillojnë kërkim shkencor ofrojnë qasje të hapur në versionet digjitale të botimeve shkencore dhe rezultateve të kërkimit shkencor në rastin kur veprimtaritë e kërkimit shkencor financohen apo bashkëfinancohen me fonde publike.

b) Institucionet që zhvillojnë kërkim shkencor, menjëherë pas publikimit të një punimi shkencor, e bëjnë atë të disponueshëm me akses të hapur, së bashku me të dhënat përkatëse të kërkimit dhe rezultatet e tjera kërkimore. Publikimi bëhet me akses të lirë, të menjëhershëm dhe të pakushtëzuar, sipas fushës së kërkimit shkencor në të cilën kërkuesi kryen hulumtimin.

c) Qasja e hapur zbatohet duke mundësuar:

i. një format digjital, përmbajtja e të cilit mund të lexohet dhe të përpunohet lehtësisht nga kompjuterat ose dorëshkrimi i dorëzuar nga autori për botim, i depozituar në një arkiv digjital të sigurt për botimet shkencore;

ii. akses të menjëhershëm të hapur në botimin shkencor të ruajtur në arkivin digjital të cituar në nënndarjen "i", të kësaj shkronje;

iii. ngarkimin e publikimeve në një databazë shtetërore të të dhënave.

ç) Modalitetet e ruajtjes së arkivave digjitalë të sigurt për botime shkencore janë të njëjta me ato të Zonës Evropiane të Kërkimit si dhe ato ndërkombëtare.

d) Çdo publikim shkencor, fizik dhe digjital, i financuar nga fonde të buxhetit të shtetit, publikohet në gjuhën shqipe dhe në një prej gjuhëve zyrtare të Bashkimit Evropian.

2. Të dhënat e kërkimit dhe rezultatet e tjera të kërkimit në formatin digjital, si më poshtë vijon:

a) Në kushtet e financimit apo të bashkëfinancimit nga fonde publike dhe të aksesit të hapur në botimet shkencore, institucionet që zhvillojnë kërkim shkencor kanë detyrim:

i. të hartojnë dhe të përditësojnë periodikisht një plan për menaxhimin e të dhënave kërkimore (PMDK);

ii. të menaxhojnë të dhënat e kërkimit shkencor dhe rezultatet e tjera të kërkimit shkencor të krijuara në kuadër të një bashkëfinancimi publik, duke ofruar përdorueshmëri kohore afatgjatë në ruajtjen e të dhënave, në përputhje me parimet që bëjnë të dhënat e kërkimit dhe rezultatet e tjera kërkimore të gjetshme, të aksesueshme, të ndërveprueshme dhe të ripërdorshme;

iii. të mundësojnë një qasje të hapur në të dhënat e kërkimit shkencor dhe rezultatet e tjera të kërkimit shkencor, në përputhje me parimin "e hapur sa është e mundur dhe e mbyllur për aq sa është e nevojshme". Qasja plotësisht e hapur në të dhënat dhe rezultatet e veprimtarive kërkimore-shkencore kufizohet në rastet e cenimit të pronësisë intelektuale, mbrojtjes së të dhënave personale, të kufizimeve të vendosura në marrëveshjen e grantit apo kufizimeve të tjera të parashikuara nga kuadri ligjor në fuqi.

b) Në çdo rast të dhënat, si autorësia, data e publikimit, data e rishikimit, madhësia e skedarit, imazhet, videot dhe faqet e internetit duhet të jenë me qasje plotësisht të hapur.

c) Financuesit e veprimtarive të kërkimit shkencor dhe institucionet që zhvillojnë kërkim shkencor zbatojnë praktika që janë në përputhje me rekomandimet e Zonës Evropiane të Kërkimit lidhur me dokumentacionin ligjor të detyrueshëm dhe me ruajtjen e të dhënave shkencore në arkiva digjitalë të sigurt dhe të koduar.

3. Infrastrukturën e kërkimit shkencor, si më poshtë vijon:

a) Infrastruktura e kërkimit shkencor funksionon në përputhje me rekomandimet e Zonës Evropiane të Kërkimit, si dhe vendeve ku parimi i shkencës së hapur është i zbatueshëm.

b) Infrastruktura e hapur e kërkimit shkencor përbëhet nga:

i. qendra të dhënash specifike dhe të përgjithshme për *domain*-in me arkiva digjitalë të sigurt;

ii. arkiva digjitalë të sigurt të institucioneve që zhvillojnë kërkim shkencor për ruajtjen e aksesit të hapur në të dhënat dhe rezultatet e veprimtarive të kërkimit shkencor;

iii. platforma botuese shkencore me akses të hapur.

c) Institucionet e kërkimit shkencor, institutet dhe njësitë e veçanta të kërkimit shkencor që përfitojnë infrastrukturë kërkimore-shkencore të financuar apo të bashkëfinancuar me fonde publike, kanë detyrimin të mundësojnë qasjen dhe përdorimin e hapur të databazave kombëtare të kërkimit shkencor.

III. KRITERET E SHKENCËS SË HAPUR

1. Kriteret e përgjithshme që mundësojnë zbatimin e parimit të shkencës së hapur gjatë veprimtarisë kërkimore-shkencore nga institucionet janë, si më poshtë vijon:

a) Veprimtaria kërkimore-shkencore zhvillohet dhe publikohet në mënyrë transparente, duke mundësuar shqyrtim të hapur, kritikë shkencore dhe riprodhueshmëri të plotë, me qëllim garantimin e saktësisë dhe besueshmërisë së rezultateve të publikuara.

b) Veprimtaria kërkimore-shkencore zhvillohet duke garantuar barazi të plotë në qasje, pjesëmarrje, kontribute dhe përfitime për të gjithë kërkuesit dhe palët e interesuara, duke siguruar mundësi të barabarta dhe duke shmangur çdo formë diskriminimi.

c) Veprimtaria kërkimore-shkencore zhvillohet me përgjegjësi dhe llogaridhënie, duke siguruar që rezultatet e saj të jenë të matshme, të justifikueshme dhe të orientuara drejt ndikimit pozitiv në zhvillimin e shoqërisë.

ç) Veprimtaria kërkimore-shkencore zhvillohet duke siguruar reciprocitet dhe përfshirje të plotë, që garanton rritjen dhe zgjerimin e bashkëpunimit në të gjitha nivelet e veprimtarisë kërkimore-shkencore.

d) Veprimtaria kërkimore-shkencore zhvillohet duke garantuar fleksibilitet, duke nxitur diversitetin në zgjedhjen dhe ndjekjen e rrugëve të ndryshme për realizimin e parimit të shkencës së hapur.

dh) Veprimtaria kërkimore-shkencore zhvillohet duke garantuar qëndrueshmëri përmes sigurimit të praktikave, shërbimeve, infrastrukturave dhe modeleve afatgjata të financimit, të dokumentuara dhe të mbështetura nga politika institucionale dhe kombëtare.

2. Kritere të veçanta që mundësojnë zbatimin e parimit të shkencës së hapur gjatë veprimtarisë kërkimore-shkencore nga institucionet janë, si më poshtë vijon:

a) Qasja e hapur *(Open Access)* detyron aplikimin e parimeve "FAIR", ku të dhënat e veprimtarisë kërkimore-shkencore janë të gjetshme, të aksesueshme, të ndërveprueshme dhe të ripërdorshme.

b) Të dhënat e hapura *(Open Data)* detyrojnë publikimin e të dhënave mbi të cilat është realizuar veprimtaria kërkimore-shkencore.

c) Metodologjia e hapur *(Open Methodology)* detyron publikimin e metodave dhe teknikave që janë përdorur gjatë realizimit të veprimtarisë kërkimore-shkencore.

ç) Rekomandimi i kolegëve *(Open Peer Review)* detyron publikimin e rekomandimeve nga kërkues të tjerë kërkimorë-shkencorë.

d) Shkenca qytetare dhe bashkëpunimi *(Collaboration for Citizen Science)* detyron publikimin e subjekteve publike ose private, që kanë kontribut në veprimtarinë kërkimore-shkencore.

dh) Integriteti kërkimor *(Research Integrity)* detyron zbatimin e standardeve më të larta kërkimore-shkencore dhe etike në veprimtarinë kërkimore-shkencore.

e) Vlerësimi rigoroz *(Rigourous Evaluation)* cakton metodat e matjes etike, cilësore dhe sasiore të veprimtarisë kërkimore-shkencore, sipas udhëzuesit ndërkombëtar TOP Transparence *(Transparency and Openness Promotion – Guideline).*

IV. DISPOZITA PËRFUNDIMTARE

1. Zbatimi i përcaktimeve të këtij vendimi lidhur me kriteret e shkencës së hapur do të jetë në fuqi deri në aderimin në Bashkimin Evropian, ku në vijim zbatohen përcaktimet e bëra në rregulloren e BE 2021/695 të Parlamentit Evropian dhe të Këshillit, të datës 28 prill 2021, "Për themelimin e programit *Horizon Europe* – programi kornizë për kërkimin dhe inovacionin, përcaktimin e rregullave për pjesëmarrjen dhe përhapjen, si dhe shfuqizimin e rregulloreve (BE) nr. 1290/2013 dhe (BE) nr. 1291/2013".

2. Ngarkohen ministria përgjegjëse për kërkimin shkencor, Agjencia Kombëtare e Kërkimit Shkencor dhe Inovacionit dhe institucionet që zhvillojnë kërkim shkencor, të financuara apo të bashkëfinancuara me fonde publike, për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

KRYEMINISTËR
Edi Rama

VENDIM
Nr. 840, datë 30.12.2025

PËR NJË SHTESË NË VENDIMIN NR. 893, DATË 17.12.2014, TË KËSHILLIT TË MINISTRAVE, "PËR MIRATIMIN E RREGULLAVE TË ORGANIZIMIT DHE TË FUNKSIONIMIT TË KABINETEVE NDIHMËSE, TË ORGANIZIMIT TË BRENDSHËM TË INSTITUCIONEVE TË ADMINISTRATËS SHTETËRORE, SI DHE PËR PROCEDURAT E HOLLËSISHME PËR PËRGATITJEN, PROPOZIMIN, KONSULTIMIN DHE MIRATIMIN E ORGANIZIMIT TË BRENDSHËM", TË NDRYSHUAR

Në mbështetje të nenit 100 të Kushtetutës, të neneve 17, pika 2, 21, pika 5, dhe 29, pika 1, të ligjit nr. 90/2012, "Për organizimin dhe funksionimin e administratës shtetërore", me propozimin e ministrit të Shtetit për Administratën Publike dhe Antikorrupsionin, Këshilli i Ministrave

VENDOSI:

1. Pas pikës 7/5, të vendimit nr.893, datë 17.12.2014, të Këshillit të Ministrave, të ndryshuar, shtohet pika 7/6, me këtë përmbajtje:

"7/6. Përcaktimet në pikat 7/1, 7/2, 7/3, 7/4 dhe 7/5, të këtij vendimi, zbatohen me ndryshimet përkatëse edhe për institucionet me vetëfinancim në varësi të Kryeministrit.".

2. Efektet financiare të këtij vendimi përballohen nga të ardhurat e veta të institucioneve, pjesë e fushës së veprimit të tij, brenda planit financiar/buxhetit vjetor të miratuar të institucionit.

3. Ngarkohen institucionet me vetëfinancim në varësi të Kryeministrit për zbatimin e këtij vendimi.

Ky vendim hyn në fuqi pas botimit në Fletoren Zyrtare.

KRYEMINISTËR
Edi Rama

	Formati 61x86/8

Shtypshkronja e Qendrës së Botimeve Zyrtare
Tiranë, 2026

Adresa: Rr. "Nikolla Jorga", Tiranë
Tel./fax: +355 4 24 27 004 Tel.: +355 4 24 27 006

Çmimi 272 lekë