RREGULLORE MBI PËRMBAJTJEN DHE MËNYRËN E DOKUMENTIMIT TË MASAVE TË SIGURISË KIBERNETIKE

Versioni 2.0
(I ndryshuar)

Miratuar me Urdhër Nr. 10 datë 02/14/2022

(Ndryshuar me Urdhër Nr. 184, Datë 20.07.2023)

RRETH RREGULLORES DHE AKCESK

Kjo rregullore synon të përcaktojë objektivat dhe masat për garantimin dhe funksionimin e sistemeve të informacionit dhe rrjetet e komunikimit në Operatorët e Infrastrukturës Kritike të Informacioni (OIKI) dhe Operatorët e Infrastrukturës së Rëndësishme të Informacionit (OIRI).

Rregullorja përcakton gjithashtu detyrimet dhe masat bazë që OIKI dhe OIRI duhet të ndërmarrin për të minimizuar apo parandaluar incidentet e sigurisë në rrjetet e komunikimit dhe sistemet e informacionit, si dhe përcakton standardizimin në vlerësimin dhe raportimin e incidenteve dhe masave të sigurisë. Rregullorja liston 20 objektiva sigurie, duke u ndarë në Masa teknike dhe organizative, mbështetur mbi standardet ndërkombëtare.

Për secilin nga objektivat e sigurisë listohen masa më të detajuara të sigurisë, së bashku me mënyrën e dokumentimit të tyre. Masat e sigurisë dhe mënyra e dokumentimit përbëjnë listën e kërkesave minimale për OIKI dhe OIRI.

AKCESK

Autoriteti ka si objekt të veprimtarisë së tij mbikëqyrjen dhe zbatimin e legjislacionit në fuqi në fushën e sigurisë kibernetike, si dhe akteve nënligjore të nxjerra ne zbatim të tij.

Funksionet e AKCESK në lidhje me sigurinë kibernetike:

- përcakton masat e sigurisë kibernetike;
- vepron si pikë qendrore kontakti në nivel kombëtar për operatorët përgjegjës në fushën e sigurisë kibernetike dhe bashkërendon punën për zgjidhjen e incidenteve të sigurisë kibernetike;
- administron raportet e incidenteve në fushën e sigurisë kibernetike dhe siguron ruajtjen e regjistrimin e tyre;
- siguron ndihmë dhe mbështetje metodike për operatorët përgjegjës në fushën e sigurisë kibernetike;
- kryen analiza për dobësitë e konstatuara në fushën e sigurisë në internet; • kryen aktivitete ndërgjegjësimi dhe edukimi në fushën e sigurisë kibernetike;
- vepron në cilësinë e CSIRT-së kombëtare.
- koordinon veprimtaritë e tij me institucionet e sigurisë dhe të mbrojtjes dhe bashkëpunon me CSIRT-të sektoriale dhe autoritetet ndërkombëtare në fushën e sigurisë kibernetike, nëpërmjet marrëveshjeve të përbashkëta, në përputhje me legjislacionin në fuqi.

Autoriteti dhe legjislacioni, bazohen në modelet e ENISA e cila është agjencia e dedikuar për arritjen e një niveli të lartë të përbashkët të sigurisë kibernetike në BE.

RRETH ENISA

Agjencia e Bashkimit Evropian për Sigurinë Kibernetike, ENISA, është agjencia e dedikuar për arritjen e një niveli të lartë të përbashkët të sigurisë kibernetike në të gjithë Evropën. E themeluar në vitin 2004 dhe e forcuar nga Akti i BE-së për Sigurinë Kibernetike, Agjencia e Bashkimit Evropian për Sigurinë Kibernetike kontribuon në politikën kibernetike të BE-së, rrit besueshmërinë e produkteve TIK, shërbimeve dhe proceseve me skemat e certifikimit të sigurisë kibernetike, bashkëpunon me Shtetet Anëtare dhe organet e BE-së dhe ndihmon Evropën të përgatitet për sfidat kibernetike të së nesërmes. Nëpërmjet ndarjes së njohurive, ngritjen e kapaciteteve dhe rritjes së ndërgjegjësimit, Agjencia punon së bashku me aktorët kryesorë për të rritur besimin në ekonominë e përbashkët, për të rritur qëndrueshmërinë në infrastrukturën e Bashkimit Evropian dhe së fundmi për të mbajtur shoqërinë dhe qytetarët e Evropës të sigurt në hapësirën dixhitale. Më shumë informacion rreth ENISA dhe punës së tyre mund të gjenden në www.enisa.europa.eu

TABELA E PËRMBAJTJES

1. PËRKUFIZIMET DHE TERMINOLOGJIA

1.1 Përkufizime

Incidentet e sigurisë kibenetike

"Incident i sigurisë kibernetike" përcaktohet si një ngjarje e sigurisë kibernetike gjatë së cilës shkaktohet cënimi i sigurisë së shërbimeve ose sistemeve të informacionit dhe të rrjeteve të komunikimit dhe sjell një efekt real negativ.

Masat e sigurisë

“Masat e sigurisë" përfshijnë tërësinë e veprimeve për rritjen e sigurisë së informacionit në sistemet e informacionit dhe disponueshmërinë e besueshmërinë e shërbimeve e të rrjeteve të komunikimit në hapësirën kibernetike.

Infrastrukturë kritike e informacionit

“Infrastrukturë kritike e informacionit” është tërësia e rrjeteve dhe sistemeve të informacionit, cënimi apo shkatërrimi i të cilave do të kishte impakt serioz në shëndetin, sigurinë, dhe/ose mirëqenien ekonomike të qytetarëve dhe/ose funksionimin efektiv të ekonomisë në Republikën e Shqipërisë. Asetet kritike duhet (padyshim) të mbrohen me prioritet.

Personeli dhe personeli kryesor

Në këtë dokument termi "personel" u referohet të punësuarve, kontraktorëve dhe përdoruesve të palëve të treta. Ne përdorim termin "personel kryesor " për t'iu referuar roleve kryesore në organizatë që kanë lidhje me sigurinë e rrjeteve dhe sistemeve të informacionit. Operatorët nuk janë të gjithë të njëjtë dhe profilet e punës janë të ndryshme, por veçanërisht role si CEO, CIO, CISO, menaxher i vazhdimësisë së biznesit dhe administratorët e sistemeve kritike do të përfshiheshin këtu.

Operator i infrastrukturës kritike të informacionit (OIKI)

“OIKI” është një person juridik, publik ose privat, që administron infrastrukturën kritike të informacionit.

Operator i infrastrukturës së rëndësishme të informacionit (OIRI)

“OIRI” është një person juridik publik, që administron infrastrukturë të rëndësishme të informacionit.

2. HYRJE

Operatorët e infrastrukturave të rëndësishme të informacionit dhe operatorët e infrastrukturave kritike të informacionit duhet të njoftojnë pa vonesë Autoritetin Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (Autoritetin) për një incident të sigurisë kibernetike që ka pasur një impakt të rëndësishëm në rrjetet e komunikimit dhe sistemet e informacionit.

Me qëllim përcaktimin e rëndësisë së impaktit të një incidenti të sigurisë kibernetike, kur është e mundur, duhet të merren parasysh në veçanti parametrat e mëposhtëm:

a) numri i përdoruesve të prekur nga incidenti i sigurisë kibernetike;
b) kohëzgjatja e incidentit të sigurisë kibernetike;
c) shtrirjen gjeografike të zonës së prekur nga incidenti i sigurisë kibernetike;
d) shkallën në të cilën ndikohet funksionimi rrjeteve të komunikimit dhe sistemeve të informacionit;
e) shtrirjen e impaktit mbi aktivitetet ekonomike dhe sociale.

Aty kur është e përshtatshme, Autoriteti duhet të informojë autoritetet kompetente në Shtetet e tjera Anëtare të BE dhe ENISA. Autoriteti mund të informojë publikun ose të kërkojë nga operatorët ta bëjnë këtë, kur gjykojnë se zbulimi i incidentit të sigurisë kibernetike është në interesin e publikut.
Një herë në vit, Autoriteti harton një raport përmbledhës mbi njoftimet e marra dhe veprimet e ndërmarra në përputhje me këtë paragraf.

Autoriteti duhet të sigurohet se në rast kërcënimi të mundshëm të një incidenti të sigurisë kibernetike në operatorët e infrastrukturave të rëndësishme të informacionit dhe operatorët e infrastrukturave kritike të informacionit duhet të informojnë përdoruesit e tyre të prekur potencialisht nga një kërcënim i tillë, për masat ose mjetet e mundshme mbrojtëse që mund të merren nga përdoruesit. Aty ku është e mundur, operatorët do të informojnë gjithashtu përdoruesit e tyre për vetë kërcënimin.

Operatorët e infrastrukturave të rëndësishme të informacionit dhe operatorët e infrastrukturave kritike të informacionit i sigurojnë menjëherë Autoritetit:

a) Informacionin e nevojshëm për të vlerësuar sigurinë e rrjeteve të komunikimit dhe sistemeve të informacionit të tyre, duke përfshirë politikat e dokumentuara të sigurisë; nëse e disponojnë dhe,
b) Paraqitja e një raporti auditimi të sigurisë kibernetike të kryer nga një organ i pavarur i kualifikuar ose një autoritet kompetent dhe vënia në dispozicion të Autoritetit të këtyre rezultateve; kostoja e auditimit do të paguhet nga operatori.

Autoriteti ofron në çdo rast kur i kërkohet, ndihmën e një ekipi të reagimit ndaj incidenteve të sigurisë kompjuterike ("CSIRT") i caktuar në përputhje me Ligjin Nr. 2/2017 “Për Sigurinë Kibernetike” dhe nenin 9 të Direktivës (BE) 2016/1148 si në lidhje me çështjet që përfshihen në detyrat e CSIRT-ve në përputhje me pikën 2 të aneksit I të asaj direktive.

Autoriteti, përpara fillimit të procesit të kontrollit (onsite) pranë OIKI dhe OIRI për implementimin e masave të sigurisë, njofton zyrtarisht infrastrukturën që do të kontrollohet, për kryerjen e procesit të skanimeve të rrjeteve dhe sistemeve të informacionit që kanë akses publik, për vulnerabilite të mundshme, në kuadër të verifikimit të dobësive dhe implementimit të masave teknike të sigurisë kibernetike.

Autoriteti, me aprovimin paraprak të Operatorëve të Infrastrukturave Kritike dhe të Rëndësishme të Informacionit që do të kontrollohen, kryen testime, simulime dhe analiza kibernetike (penetration test), të rrjeteve dhe sistemeve të tyre të informacionit.

3. MASAT E SIGURISË KIBERNETIKE

3.1. STRUKTURA E MASAVE TË SIGURISË KIBERNETIKE

Ky dokument liston 20 masa sigurie të nxjerra nga një grup standardesh ndërkombëtare.

Për secilin nga objektivat e sigurisë listohen masa sigurie më të detajuara të cilat duhet të implementohen nga operatorët për të arritur objektivin e sigurisë kibernetike. Për secilin nga objektivat e sigurisë gjithashtu listojmë dokumentime (dëshmi) të detajuara që mund të tregojnë se masat janë në fuqi.

Masat e sigurisë kibernetike grupohen në **3 (tre)** nivele, si më poshtë:

NIVELI I SIGURISË	Përshkrimi i niveleve të sigurisë
1 dhe 2	Niveli 1 dhe 2 (Masat që janë të detyrueshme për OIRI dhe OIKI) Masa sigurie të nivelit të ulët dhe të mesëm duhen implementuar për të arritur objektivat e sigurisë. Dokumentimi që masat e sigurisë të nivelit të ulët dhe të mesëm janë implementuar. Masat e sigurisë të nivelit të ulët dhe të mesëm për të arritur objektivin dhe një rishikim ad-hoc të zbatimit, pas ndryshimeve apo incidenteve. Dokumentimi i masave të sigurisë së nivelit të ulët dhe të mesëm dhe dokumentimin e rishikimeve të zbatimit pas ndryshimeve ose incidenteve.
3	Niveli i tretë (Masat që janë të detyrueshme për OIKI) Masa sigurie në nivel të lartë dhe monitorimin e vazhdueshëm të zbatimit, rishikimin e zbatimit, duke marrë parasysh ndryshimet, incidentet, testet dhe ushtrimet, për të përmirësuar në mënyrë pro - aktive zbatimin e masave të sigurisë. Dokumentimi i zbatimit të avancuar të masave të sigurisë, dokumentimi i një procesi të shqyrtimit strukturor dhe dokumentimi i hapave pro - aktiv për të përmirësuar zbatimin e masave të sigurisë.

Shënim:

Niveli i parë dhe i dytë i masave të sigurisë duhet implementuar dhe dokumentuar nga Operatorët e Infrastrukturave të Rëndësishme të Informacionit, ndërsa niveli i tretë, përfshirë nivelin e parë dhe të dytë, duhet implementuar dhe dokumentuar nga Operatorët e Infrastrukturave Kritike të Informacionit.

3.2. MASAT E SGURISË KIBERNETIKE

Më poshtë listohen 20 masa sigurie të nivelit të ulët, të mesëm dhe të lartë, (MS1, MS2, etj.), të grupuara në 2 kategori (K1, K2).

Për secilën kategori të masave të sigurisë, listohen masat e sigurisë të detajuara, të cilat duhet të implementohen nga operatorët, po ashtu edhe llojin e dokumenteve që do të merren në konsideratë.

Më poshtë po listojmë dy kategoritë e masave dhe 20 masat për referencë:

K1: MASAT ORGANIZATIVE

- MS1: Politika e sigurisë
  - 1.1 Politika e sigurisë së informacionit
- MS2: Menaxhimi i riskut
- MS3: Siguria organizative
- MS4: Kërkesat e sigurisë për palët e treta
- MS5: Siguria e burimeve njerëzore dhe aksesit të personave
  - 5.1 Kontrollet e Background-it
  - 5.2 Njohuritë dhe trajnimet
  - 5.3 Ndryshimet e personelit
  - 5.4 Trajtimi i shkeljeve
- MS6: Menaxhimi i Aseteve
  - 6.1 Menaxhimi i aseteve
  - 6.2 Procedurat operative
  - 6.3 Menaxhimi i ndryshimit
- MS7: Ngjarjet e sigurisë dhe menaxhimit të incidenteve të sigurisë kibernetike
  - 7.1 Procedurat e menaxhimit të incidentit
  - 7.2 Aftësia për zbulimin e incidentit
  - 7.3 Raportimi dhe komunikimi i incidentit
- MS8: Menaxhimi i vazhdimësisë së punës
  - 8.1 Strategjia e vazhdimësisë së shërbimit dhe planet e emergjencës
  - 8.2 Kapacitetet e rikuperimit nga katastrofa
  - 8.3 Përdorimi i planeve të emergjencës
- MS9: Menaxhimi i sigurisë së informacionit
- MS10: Kontrolli dhe auditi

K2 : MASAT TEKNIKE

- MS1: Siguria fizike
  - 1.1 Siguria fizike dhe mjedisore
  - 1.2 Siguria e furnizimeve
- MS2: Menaxhimi për autorizimin e aksesit
  - 2.1 Ndërgjegjësimi ndaj kërcënimit
  - 2.2 Informimi i përdoruesve rreth kërcënimeve
- MS3: Pajisjet kriptografike
  - 3.1 Mbrojtja e të dhënave kritike të sigurisë
- MS4: Zbulimi i ngjarjeve të sigurisë kibernetike
- MS5: Mjetet e gjurmimit dhe vlerësimit të ngjarjeve të sigurisë kibernetike
  - 5.1 Monitorimi dhe politikat e regjistrimit
- MS6: Mbrojtja e integritetit të rrjeteve të komunikimit
  - 6.1 Testimi i rrjetit dhe sistemeve të informacionit
  - 6.1 Vlerësimet e sigurisë
- MS7: Verifikimi i identitetit të përdoruesve
- MS8: Veprimtaria e administratorëve dhe përdoruesve
- MS9: Siguria e aplikacioneve
- MS10: Siguria e sistemeve industriale

4. MASAT ORGANIZATIVE

4.1. MS1: Politika e sigurisë

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

4.1.1. Politika e sigurisë së informacionit

Të krijohet dhe mbahet një politikë e përshtatshme e sigurisë së informacionit.

	Masat e sigurisë		Dokumentimi
1	a) Të vendoset një politikë sigurie e nivelit të lartë që adreson sigurinë e rrjeteve të komunikimit dhe sistemeve të informaconit.	i. ii.	Politika e dokumentuar e sigurisë, duke përfshirë rrjetet e komunikimit dhe sistemet e informacionit brenda fushës së veprimit, asetet kritike që i mbështesin ato dhe objektivat e sigurisë kibernetike.
	b) Të ndërgjegjësohet personeli kryesor rreth politikës së sigurisë.		Personeli kryesor është në dijeni të politikës së sigurisë dhe objektivave të saj. (intervistë)
2	c) Të përcaktohen politika të detajuara të sigurisë së informacionit për asetet kritike dhe proceset e punës.	iii.	Politikat e dokumentuara të sigurisë së informacionit, të miratuara nga stafi më i lartë menaxhues, duke përfshirë ligjin dhe rregulloret në fuqi, të aksesueshme për personelin.
	d) Të ndërgjegjësohet i gjithë personeli mbi politikën e sigurisë dhe çfarë nënkupton ajo për punën e tyre.	iv.	Personeli është në dijeni të politikës së sigurisë së informacionit dhe çfarë nënkupton ajo për punën e tyre (intervistë).
	e) Të rishikohet politika e sigurisë pas incidenteve.	v.	Rishikimi i komenteve ose ndryshimi i log-eve për politikën.
3	f) Të rishikohen në mënyrë periodike politikat e sigurisë së informacionit dhe të merren në konsideratë shkeljet, përjashtimet, incidentet e kaluara, testimet/ushtrimet e mëparshme dhe incidentet që prekin operatorët e tjerë (të ngjashëm) në këtë sektor.	vi.	Politikat e sigurisë së informacionit janë të përditësuara dhe të miratuara nga stafi më i lartë menaxhues.
		vii.	Dokumentim i përjashtimeve të politikës, të miratuara nga rolet përkatëse.
		viii.	Dokumentimi i procesit të rishikimit, duke marrë parasysh ndryshimet dhe incidentet e mëparshme.

4.2. MS2: Menaxhimi i rrezikut kibernetik

Të krijohet dhe ruhet një kuadër i përshtatshëm i menaxhimit të rrezikut për të identifikuar dhe trajtuar rreziqet kibernetike mbi rrjetet e komunikimit dhe sistemet e informacionit.

	Masat e sigurisë		Dokumentimi
1	a) Të bëhet një listë e rreziqeve kryesore për sigurinë e rrjeteve të komunikimit dhe sistemeve të informacionit, duke marrë në konsideratë kërcënimet kryesore për asetet kritike.	i. ii.	Listimi i rreziqeve kryesore të përshkruara në një nivel të lartë, duke përfshirë kërcënimin(et) themelor/e dhe impaktin e tyre potencial në sigurinë e rrjeteve të komunikimit dhe sistemeve të informacionit.
	b) Të ndërgjegjësohet personeli kryesor mbi rreziqet kryesore dhe mënyrën se si ato mund të minimizohen.		Personeli kryesor i njeh rreziqet kryesore kibernetike (intervistë).

2	c) Krijimi i një metodologjie dhe/ose mjete të menaxhimit të rrezikut të bazuar në standardet e industrisë. d) Të sigurohet që personeli kryesor të përdorë metodologjinë dhe/ose mjetet e menaxhimit të rrezikut. e) Rishikoni vlerësimet e rrezikut pas ndryshimeve ose incidenteve kibernetike. f) Sigurohuni që rreziqet e mbetura të pranohen nga stafi menaxhues. g) Sigurimi kibernetik "Cyber Insurance" Sigurimi i sistemeve dhe i rrjeteve kompjuterike (infrastrukturat e informacionit) me qëllim shmangien e dëmeve ose humbjes/vjedhjes së informacionit. -Të kryhet sigurimi nga rreziku kibernetik i infrastrukturës kritike të informacionit dhe i infrastrukturës së rëndësishme të informacionit.	iii. Metodologjia dhe/ose mjetet e dokumentuara të menaxhimit të rrezikut. iv. Udhëzime për personelin për vlerësimin e rreziqeve kibernetike. v. Një listë e rreziqeve kibernetike dhe dokumenteve të përditësimeve/rishikimeve. vi. Rishikimi i komenteve ose ndryshimi i log-eve për vlerësimet e rrezikut. vii. Miratimi i stafit menaxhues lidhur me rreziqet e pranuara. viii. Të dokumentohet sigurimi i infrastrukturës nëpërmjet një police sigurimi në një kompani sigurimi vendase apo të huaj (një prej vendeve të BE dhe/ose NATO).
3	h) Rishikim të metodologjisë dhe/ose mjeteve të menaxhimit të rrezikut, në mënyrë periodike, duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme.	ix. Dokumentimi i procesit të rishikimit dhe përditësimet e metodologjisë dhe/ose mjeteve të menaxhimit të rrezikut kibernetik

4.3. MS3 : Siguria organizative rijohet dhe mbahet një strukturë e përshtatshme e Të kroleve të sigurisë dhe përgjegjësive.

	Masat e sigurisë	Dokumentimi
1	a) Të caktohen rolet e sigurisë dhe përgjegjësitë për personelin. b) Sigurohuni që rolet e sigurisë të jenë të arritshme në rast incidentesh sigurie kibernetike.	i. Listë e roleve të sigurisë dhe informacione kontakti. ii. Plani i Sistemit te Menaxhimit të Sigurisë së Informacionit. iii. Objektivat e sigurisë së informacionit. iv. Kërkesat e burimeve njerëzore për marrjen në punë të personelit. v. Kërkesat e verifikimit të sigurisë së personelit. vi. Dokumenti i përfundimit të marrëdhënieve të punës. vii. Dokumenti i menaxhimit dhe aksesit të përdoruesve.
2	c) Personeli emërohet zyrtarisht në role sigurie. d) Ndërgjegjësoni personelin mbi rolet e sigurisë në organizatën tuaj dhe se kur duhet të kontaktohen.	viii. Dokumenti i sigurisë dhe përdorimit të pajisjeve teknologjike. ix. Dokumenti i sigurisë fizike. x. Listë e emërimeve dhe përshkrimi i përgjegjësive dhe detyrave për rolet e sigurisë. xi. Materiale ndërgjegjësimi dhe informimi për punonjësin duke shpjeguar rolet e sigurisë dhe si/ ku ata duhet të kontaktohen.

3	e) Struktura e roleve dhe përgjegjësive të sigurisë rishikohet dhe përmirësohet rregullisht, bazuar në ndryshimet dhe/ose incidentet e mëparshme.	xii. Dokumentim i përditësuar i strukturës së detyrave të roleve të sigurisë dhe përgjegjësive. xiii. Dokumentim i procesit të rishikimit, duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme.

4.4. MS4: Kërkesat e sigurisë kibernetike për palët e treta

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

	Masat e sigurisë	Dokumentimi
1	a) Të përfshihen kërkesat e sigurisë në kontratat me palët e treta, duke përfshirë konfidencialitetin dhe transferimin e sigurt të informacionit.	i. Kërkesa të qarta sigurie në kontratat me palët e treta që furnizojnë me produkte IT, shërbime IT, procese të kontraktuara biznesi, helpdesks, qendra thirrjesh, ndërlidhje, pajisjet e përbashkëta, etj.
2	b) Të vendoset një politikë sigurie për kontratat me palët e treta. c) Të sigurohet që të gjitha prokurimet e shërbimeve/produkteve nga palët e treta të ndjekin këtë politikë. d) Të rishikohet politika e sigurisë me palët e treta, pas incidenteve kibernetike apo ndryshimeve. e) Të kërkohen standarde specifike sigurie në proceset furnizuese të palëve të treta gjatë prokurimeve. f) Të zbuten/reduktohen rreziqet e mbetura që nuk adresohen nga palët e treta.	ii. Të dokumentohet politika e sigurisë për kontratat me palët e treta. iii. Lista e kontratave me palët e treta. iv. Kontratat e shërbimeve nga palët e treta përmbajnë kërkesa sigurie, në përputhje me manualet/procedurat e e prokurimit. v. Rishikimi i komenteve ose ndryshimi i log-eve në politikat. vi. Kontratat me furnizuesit e pajisjeve përmbajnë kërkesa duke ju përmbajtur praktikave më të mira të sigurisë dhe standardeve të industrisë. vii. Rreziqet e mbetura si pasojë e varësisë nga palët e treta, janë të listuara dhe të reduktuara.
3	g) Të mbahen gjurmët/rekordet e incidenteve të sigurisë kibernetike që lidhen ose janë të shkaktuara nga palët e treta. h) Të rishikohet dhe përditësohet periodikisht politika e sigurisë për palët e treta në intervale të rregullta, duke marrë në konsideratë incidentet e mëparshme, ndryshimet etj.	viii. Lista e incidenteve të sigurisë kibernetike që lidhen ose janë të shkaktuara nga angazhimi me palët e treta. ix. Dokumentimi i procesit të rishikimit të politikave.

4.5. MS5 : Siguria e burimeve njerëzore dhe aksesit të personave

Siguria e burimeve njerëzore dhe aksesit të personave mbulon objektivat e sigurisë në lidhje me personelin.

4.5.1. Kontrollet e background-it Të kryhen kontrollet e duhura të backgroundit të personelit për detyrat dhe përgjegjësitë e tyre.

	Masat e sigurisë	Dokumentimi
1	a) Të kontrollohen referencat profesionale të personelit kryesor (administratorët e sistemit, oficerët e sigurisë, rojet, etj.).	i. Dokumentim i kontrolleve të referencave profesionale të personelit kryesor.

2	b) Të kryhen kontrolle/ekzaminime të background-it për personelin kryesor, atëherë kur është e nevojshme dhe kur lejohet ligjërisht. c) Të vendoset një politikë dhe procedurë për kontrollet e background-it.	ii. iii.	Politika dhe procedura për kontrollet/shqyrtimet e background-it. Udhëzime për personelin se kur/si të kryejnë kontrolle/shqyrtime të background-it.
3	d) Të rishikohen dhe përditësohen politikat/procedurat për kontrollet e background-it dhe kontrollet e referencave në intervale të rregullta, duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme.	iv.	Rishikimi i komenteve ose ndryshimi i log-eve të politikës/procedurave.

4.5.2. Njohuri dhe trajnime mbi sigurinë kibernetike

Të sigurohet që personeli të ketë njohuri të mjaftueshme dhe trajnimet e duhura periodike për sigurinë kibernetike.

	Masat e sigurisë	Dokumentimi
1	a) Personelit kryesor t'i sigurohen trajnime dhe materialet e nevojshme për çështjet e sigurisë kibernetike.	i. Personeli kryesor ka ndjekur trajnime për sigurinë kibernetike dhe ka njohuri të mjaftueshme për sigurinë kibernetike (intervistë).
2	b) Të implementohet një program trajnimi, duke u siguruar që personeli kryesor të ketë njohuri të mjaftueshme dhe të përditësuara për sigurinë kibernetike. c) Të organizohen trajnime dhe sesione ndërgjegjësimi për personelin mbi temat e sigurisë kibernetike të cilat janë të rëndësishme për subjektin tuaj.	ii. Personeli ka marrë pjesë në sesione ndërgjegjësimi mbi temat e sigurisë kibernetike. iii. Program i dokumentuar për trajnime mbi aftësitë e personelit mbi sigurinë kibernetike, duke përfshirë objektivat për role të ndryshme dhe si t'i arrijmë ato (për shembull, trajnime, rritje ndërgjegjësimi, etj.).
3	d) Të rishikohet dhe përditësohet periodikisht programi i trajnimit, duke marrë parasysh ndryshimet dhe incidentet e mëparshme. e) Të testohen njohuritë e personelit mbi sigurinë kibernetike.	iv. Programi i përditësuar mbi ndërgjegjësimin dhe trajnimin për sigurinë kibernetike. v. Rezultatet e testeve të personelit mbi njohuritë për sigurinë kibernetike. vi. Të rishikohen komentet ose ndryshimet e log-eve

4.5.3. Ndryshimet e personelit

Të krijohet dhe mbahet një proces i përshtatshëm për menaxhimin e ndryshimeve në personel os ndryshimet në rolet dhe përgjegjësitë e tyre.

	Masat e sigurisë	Dokumentimi
1	a) Pas ndryshimeve në personel, revokoni të drejtat e aksesit, badge, pajisjet, etj., nëse nuk janë më të nevojshme ose të lejuara. b) Të informojë dhe trajnojë personelin e ri mbi politikat dhe procedurat në fuqi.	i. Një dokument se ndryshimet e personelit janë ndjekur nga revokimi i të drejtave të aksesit, badge, pajisjeve, etj. ii. Një dokument se personeli i ri është informuar dhe trajnuar rreth politikave dhe procedurave në fuqi.

2	c) Të implementohen politika/procedura mbi ndryshimet e personelit, duke marrë në konsideratë revokimin në kohë të të drejtave të aksesit, badge dhe pajisjeve. d) Implementimi i politikave/procedurave për edukimin dhe trajnimin e personelit në role të reja.	iii. Dokumentimi i procesit për ndryshimet e personelit, duke përfshirë përgjegjësitë për menaxhimin e ndryshimeve, përshkrimin e të drejtave të aksesit dhe posedimit të aseteve sipas rolit, procedurat për informimin dhe trajnimin e personelit në rolet e reja. iv. Dokumentim se ndryshimet në personel janë kryer sipas procedurave dhe se të drejtat e aksesit janë përditësuar në kohë (p.sh. listat kontrolluese).
3	e) Kontrolloni periodikisht f) efektive. Rishikimi dhe vlerësimi i politikave/procedurave mbi ndryshimet e personelit, duke marrë në konsideratë ndryshimet ose incidentet e mëparshme.	v. Dokumentim të kontrolleve të të drejtave të aksesit etj. vi. vii. Politikat/procedurat e përditësuara për menaxhimin e ndryshimeve të personelit. Rishikoni komentet ose ndryshoni log-et.

4.5.4. Trajtimi i shkeljeve

Të krijohet dhe mbahet një proces disiplinor për personelin që shkel politikat e sigurisë dhe të ketë një proces më të gjerë që mbulon incidentet e sigurisë kibernetike të shkaktuara nga shkeljet e personelit.

	Masat e sigurisë	Dokumentimi
1	a) Personeli është përgjegjës për incidentet e sigurisë kibernetike të shkaktuara nga shkeljet e politikave, për shembull nëpërmjet kontratës së punës.	i. Rregullat për personelin, duke përfshirë përgjegjësitë, kodin e sjelljes, shkeljet e politikave, etj., mundësisht si pjesë e kontratave të punës.
2	b) Të vendosen procedurat për shkeljet e politikave nga personeli.	ii. Dokumentimi i procedurave, duke përfshirë llojet e shkeljeve që mund t'i nënshtrohen masave disiplinore dhe se cilat masa disiplinore duhet të ndërmerren.
3	c) Të rishikohet dhe përditësohet në mënyrë periodike procesi disiplinor, bazuar në ndryshimet dhe incidentet e mëparshme.	iii. Rishikoni komentet ose ndryshoni log-et.

4.6. MS6: : Menaxhimi i aseteve

Kjo masë sigurie mbulon menaxhimin e aseteve, procedurat operative dhe menaxhimin e ndryshimeve.

4.6.1. Menaxhimi i aseteve

Të krijohen dhe mbahen procedurat e menaxhimit të aseteve dhe kontrollet e konfigurimit në mënyrë që të menaxhohet disponueshmëria e aseteve kritike dhe konfigurimet e e rrjeteve të komunikimit dhe sistemeve të informacionit.

	Masat e sigurisë	Dokumentimi
1	a) Identifikimi i aseteve kritike dhe konfigurimet e sistemeve kritike.	i. Lista e aseteve kritike dhe sistemeve kritike. Lista duhet të përfshijë të gjitha asetet kritike dhe sistemet kritike të rrjeteve të komunikimit dhe sistemeve të informacionit, asetet operative dhe të sigurisë, duke përfshirë edhe asetet përkatëse të palëve të treta.

2	b) Zbatimi i politikës/procedurave për menaxhimin e aseteve dhe kontrollin e konfigurimit.	ii. Te dokumentohen politika/procedura për menaxhimin e aseteve, duke përfshirë rolet dhe përgjegjësitë, asetet dhe konfigurimet që janë objekt i politikës, objektivat e menaxhimit të aseteve. iii. Një inventar ose disa inventarë asetesh, që përmbajnë asete kritike dhe varësinë ndërmjet aseteve. iv. Një inventar ose disa inventarë kontrolli konfigurimi, që përmbajnë konfigurime të sistemeve kritike.
3	c) Rishikimi dhe përditësimi periodik i politikës së menaxhimit të aseteve, bazuar në ndryshimet dhe incidentet e mëparshme.	v. Politika/procedura të përditësuara të menaxhimit të aseteve, shqyrtimi komenteve dhe/ose ndryshim i loge-ve.

4.6.2. Procedurat operative

Të krijohen dhe mirëmbahen procedurat operacionale për funksionimin e rrjeteve kritike të komunikimit dhe sistemeve të informacionit nga personeli.

	Masat e sigurisë	Dokumentimi
1	a) Të vendosen procedurat operacionale dhe të caktohen përgjegjësitë për funksionimin e sistemeve kritike.	i. Dokumentimi i procedurave operacionale dhe përgjegjësive për rrjetet kyçe dhe sistemet e informacionit.
2	b) Të implementohet një politikë për funksionimin e sistemeve për të siguruar së të gjitha sistemet kritike operohen dhe menaxhohen në përputhje me procedurat e paracaktuara.	ii. Dokumentim i politikave për operimin e sistemeve kritike, duke përfshirë një topologji të rrjetit dhe sistemeve të informacionit brenda fushëveprimit.
3	c) Rishikim dhe përditësim të politikave/procedurave për funksionimin e sistemeve kritike, duke marrë në konsideratë incidentet dhe/ose ndryshimet.	iii. Përditësim i politikave/procedurave për sistemet kritike, rishikoni komentet dhe/ose ndryshimet i loge-ve e ndryshimeve.

4.6.3. Menaxhimi i ndryshimeve

Të vendosen procedurat e menaxhimit të ndryshimeve për rrjetet kritike dhe sistemet e informacionit në mënyrë që të minimizohet mundësia e incidenteve kibernetike që vijnë nga ndryshimet.

	Masat e sigurisë	Dokumentimi
1	a) Të ndiqen metodat ose procedurat e paracaktuara kur bëni ndryshime në sistemet kritike.	i. Dokumentacioni që përshkruan metodat ose procedurat e paracaktuara, të ndjekura kur bëhen ndryshime në sistemet kritike.

2	b) Të implementohen politika/procedura për menaxhimin e ndryshimeve, për të siguruar që ndryshimet e sistemeve kritike kryhen gjithmonë sipas një mënyre të paracaktuar. c) Të dokumentohen procedurat e menaxhimit të ndryshimeve dhe të regjistrohen hapat e procedurës së ndjekur për çdo ndryshim.	ii. Dokumentimi i politikave/procedurave të menaxhimit të ndryshimeve, duke përfshirë sistemet që i nënshtrohen politikës, objektivat, procedurave të rikthimit, etj. iii. Për çdo ndryshim, të mbahet një raport që përshkruan hapat dhe rezultatin e ndryshimit.
3	d) Të rishikohen dhe përditësohen rregullisht procedurat e menaxhimit të ndryshimeve, duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme.	iv. Të përditësohen procedurat e menaxhimit të ndryshimeve, të rishikohen komentet dhe/ose ndryshimet i loge-ve

4.7. MS7: Ngjarjet e sigurisë e të menaxhimit të incidenteve të sigurisë kibernetike

Ngjarjet e sigurisë e të menaxhimit të incidenteve të sigurisë kibernetike përfshijnë zbulimin, reagimin, raportimin dhe komunikimin për incidentin kibernetik.

4.7.1. Procedurat e menaxhimit të incidenteve të sigurisë kibernetike

Të krijohen dhe mbahen procedura për menaxhimin e incidenteve të sigurisë kibernetike dhe përcjelljen e tyre tek personeli përkatës (përzgjedhja).

	Masat e sigurisë	Dokumentimi
1	a) Të sigurohet që personeli është në gatishmëri dhe i përgatitur të menaxhojë dhe të trajtojë incidentet e sigurisë kibernetike. b) Të mbahen rekorde për të gjitha incidentet kryesore të sigurisë kibernetike.	i. Personeli është i njohur me mënyrën e trajtimit të incidenteve të sigurisë kibernetike dhe se kur duhet ta përshkallëzoj atë. ii. Inventari i incidenteve kibernetike kryesore dhe për secilin, ndikimi, shkaku, veprimet e marra dhe mësimet e nxjerra.
2	c) Zbatimi i politikës/procedurave për menaxhimin e incidenteve të sigurisë kibernetike.	iii. Politika/procedura për menaxhimin e incidentit kibernetik, duke përfshirë, llojet e incidenteve që mund të ndodhin, objektivat, rolet dhe përgjegjësitë, përshkrimin e detajuar, për llojin e incidentit, mënyrën e menaxhimit të incidentit, kur të përshkallëzohet tek stafi i lartë menaxherial (p.sh. CISO) etj.
3	d) Hetimi i incidenteve kibernetike kryesore dhe hartimi i raporteve përfundimtare të incidenteve, duke përfshirë veprimet e ndërmarra dhe rekomandimet për të zvogëluar mundësitë e ndodhjes në të ardhmen të këtij incidenti. e) Vlerësoni politikën/procedurat e menaxhimit të incidenteve kibernetike bazuar në incidentet e mëparshme .	iv. Raporte individuale për trajtimin e incidenteve kibernetike kryesore. v. Politika/procedura të përditësuara të menaxhimit të incidenteve kibernetike, shqyrtim i komenteve dhe/ose ndryshimi loge-ve .

4.7.2. Raportimi dhe komunikimi i incidentit kibernetik

Të krijohen dhe mbahen procedurat e duhura të raportimit dhe komunikimit të incidentit kibernetik, duke marrë parasysh legjislacionin kombëtar për raportimin e incidentit kibernetik tek autoritetet qeveritare.

Masat e sigurisë	Dokumentimi

1	a) T'u komunikohen dhe raportohen incidentet kibernetike aktuale ose të mëparshme palëve të treta, klientëve dhe/ose autoriteteve qeveritare, kur është e nevojshme.	i. Dokument i komunikimeve dhe raportimeve të mëparshme të incidentit kibernetik.
2	b) Të zbatohen politika dhe procedura për komunikimin dhe raportimin e incidenteve kibernetike.	ii. Dokumentimi i politikave dhe procedurave lidhur me komunikimin dhe raportimin e incidenteve kibernetike, përshkrimin e arsyeve/motiveve për komunikimin apo raportimin (motive biznesi, ligjore etje;) llojet e incidenteve brenda fushëveprimit, përmbajtjen e kërkuar të komunikimeve, njoftimet ose raportet, kanalet e komunikimit që do të përdoren, si dhe rolet përgjegjëse për komunikimin, njoftimin dhe raportimin. iii. Modele për raportimin dhe komunikimin e incidentit kibernetik.
3	c) Të vlerësohen komunikimet e mëparshme dhe raportet mbi incidentet kibernetike. d) Rishikimi dhe përditësimi i raportimit dhe planeve të komunikimit, bazuar në ndryshimet dhe incidentet e mëparshme.	iv. Lista e raportimeve të incidenteve dhe komunikimeve të mëparshme për incidentet. v. Politika e përditësuar e reagimit ndaj incidenteve dhe komunikimeve, shqyrtimi i komenteve dhe/ose ndryshim i loge-ve.

4.8. MS8: Menaxhimi i vazhdimësisë së punës

"Menaxhimi i vazhdimësisë së punës" mbulon strategjitë e vazhdimësisë dhe planet e emergjencës për të parandaluar dëmet e mëdha dhe katastrofat natyrore apo ato të shkaktuara nga njeriu.

4.8.1. Strategjia e vazhdimësisë së shërbimit dhe planet e emergjencës

Të krijohen dhe mbahen plane emergjence dhe një strategji për të siguruar vazhdimësinë e rrjeteve të komunikimit dhe sistemeve të informacionit.

	Masat e sigurisë	Dokumentimi
1	a) Të implementohet një strategji për vazhdimësinë e shërbimit për rrjetet e komunikimit dhe/ose sistemet e informacionit.	i. Strategjia e dokumentuar e vazhdimësisë së shërbimit, duke përfshirë kohën e rikuperimit për shërbimet dhe proceset kryesore.
2	b) Të implementohen planet e emergjencës/rezervë për sistemet kritike. c) Monitorimi i aktiviteteve dhe zbatimi i planeve të emergjencës, regjistrimi i tentativave të suksesshme të rikuperimit dhe dështimet. d) Të zbatohen planet e emergjencës për sektorët dhe shërbimet kritike të varura dhe të ndërvarura.	ii. Planet e emergjencës për sistemet kritike, duke përfshirë hapa të qarta dhe procedurat për kërcënimet e njohura, shkaktuesit për aktivizimin, hapat dhe kohën e rikuperimit. iii. Procesi i vendimmarrjes për aktivizimin e planeve të emergjencës. iv. Dokumentim i aktivizimit dhe zbatimit të planeve të emergjencës, duke përfshirë vendimet e marra, hapat e ndjekur, kohën e plotë të rikuperimit. v. Harta e sektorëve kritikë dhe shërbimeve thelbësore dhe/ose të varura nga vazhdimësia e funksionimit të rrjetit dhe shërbimeve dhe planet e emergjencës për të parandaluar ndikimin në sektorët dhe shërbimet e varura dhe të ndërvarura.
3	e) Rishikimi dhe kontrolli periodik i strategjisë për vazhdimësinë e shërbimit. f) Rishikimi dhe kontrolli i planeve të emergjencës, bazuar në ndryshimet dhe incidentet e mëparshme.	vi. Strategjia e përditësuar e vazhdimësisë dhe planet e emergjencës, shqyrtimi i komenteve dhe/ose ndryshimi i loge-ve.

4.8.2. Kapacitetet e rikuperimit nga katastrofat

Të krijohen dhe mbahen kapacitete të përshtatshme për kthimin në gjendjen normale të rrjeteve të komunikimit dhe sistemeve të informacionit në rastet e katastrofave natyrore ose të mëdha.

	Masat e sigurisë´	Dokumentimi
1	a) Të përgatiten për rikthimin në gjendje normale të sistemeve të informacionit në katastrofën potenciale të radhës.	i. Masat e ndërmarra për trajtimin e katastrofave, të tilla si "failover site" në rajonet e tjera, backup-et e të dhënave kritike në distancë (remote).
2	b) Të zbatohen politika/procedura për vendosjen e kapaciteteve për rikuperimin e katastrofave. c) Të zbatohen kapacitete standarde rikuperuese të industrisë, ose të bëhen të disponueshme nga palët e treta (siç janë rrjetet kombëtare të emergjencës).	ii. Procedura/ politika të dokumentuara për vendosjen e kapaciteteve për kthimin e situatës në gjendjen normale, duke përfshirë një listë të katastrofave natyrore dhe/ose madhore që mund të ndikojnë tek sistemet e informacionit, dhe një listë të kapaciteteve (ato nga palët e treta por edhe të brendshme). iii. Zbatimi i kapaciteteve standarde të industrisë në rastin e katastrofave, të tilla si pajisjet mobile, mobile site, failover site etj.
3	d) Të krijohen kapacitete rikuperuese për zvogëlimin e katastrofave natyrore dhe madhore. e) Të kontrollohen dhe përditësohen në mënyre të vazhdueshme kapacitetet, duke marrë parasysh ndryshimet që ndodhin, incidentet e mëparshme, rezultatet e testeve dhe ushtrimeve.	iv. Kapacitetet rikuperuese, të tilla si mekanizmat parandaluese dhe failover për të trajtuar katastrofat natyrore dhe /ose madhore. v. Dokumentacioni i përditësuar i kapaciteteve për kthimin në gjendjen normale të situatës, rishikimi i komenteve dhe / ose ndryshim i loge-ve.

4.8.3. Përdorimi i planeve të emergjencës

	Masat e sigurisë	Dokumentimi
1	a) Të monitorohet pajtueshmëria e standardeve me kërkesat ligjore.	i. Raportet që përshkruajnë rezultatet e monitorimit të pajtueshmërisë.

2	b) Të implementohen politika/procedurat për monitorimin e pajtueshmërisë dhe auditimit.	ii. Politika/procedura të dokumentuara për monitorimin e pajtueshmërisë dhe auditimin, përfshirë (asetet, proceset, infrastrukturën), frekuencën, udhëzime se kush do t'i kryejë auditimet (të brendshme apo të jashtme), politikat përkatëse të sigurisë që janë objekt i pajtueshmërisë së monitorimit dhe auditimit, objektivat dhe niveli i lartë i përafrimit të pajtueshmërisë së monitorimit dhe auditimit, modelet për raportet e auditit. iii. Planet e detajuara të monitorimit dhe auditimit, përfshirë planifikimin e objektivave afatgjata të një niveli të lartë.

Të përdoren dhe mbahen politika për testimin dhe ushtrimin e planeve rezervë (backup) dhe të emergjencës, në bashkëpunim me palët e treta, kur është e nevojshme.

Masat e sigurisë		Dokumentimi
1	a) Të përdoren dhe testohen planet rezervë (backup) dhe të emergjencës për të siguruar që sistemet dhe proceset funksionojnë dhe që personeli është i përgatitur në rastin e dëmtimeve të mëdha dhe emergjencave.	i. Raporte të ushtrimeve të mëparshme të planeve rezervë (backup) dhe të emergjencës.
2	b) Të implementohet një program për ushtrimin rregullisht të planeve rezervë dhe të emergjencës, duke përdorur skenarë realistë që mbulojnë një sërë skenarësh të ndryshëm me kalimin e kohës. c) Të sigurohet që problematikat dhe mësimet e nxjerra nga këto ushtrime janë adresuar nga personat përgjegjës dhe në përputhje me rrethanat të bëhet përditësimi i proceseve dhe sistemeve përkatëse.	ii. Përdorimi i programit për planet rezervë dhe të emergjencës, duke përfshirë llojet e emergjencave, frekuencën, rolet dhe përgjegjësitë, modele dhe procedura për kryerjen e ushtrimeve, modele për raportet e ushtrimeve. iii. Raporte lidhur me ushtrimet dhe stërvitjet (drills) që tregojnë zbatimin e planeve të emergjencës, duke përfshirë edhe mësimet e nxjerra nga këto ushtrime. iv. Adresimi nga personat përgjegjës i problematikave dhe mësimeve të nxjerra nga ushtrimet e mëparshme.
3	d) Rishikimi dhe përditësimi i planeve të ushtrimeve, duke marrë në konsideratë ndryshimet, incidentet e mëparshme dhe emergjencat që nuk kanë qenë të mbuluara nga programi i ushtrimit. e) Përfshirja në ushtrime e furnitorëve dhe palëve të tjera të treta, si për shembull ortakët e biznesit dhe klientët.	v. Përditësimi i planeve të ushtrimeve, rishikimi i komenteve, vi. dhe/ose ndryshimi i log-eve. Të dhëna nga furnitorët dhe palët e tjera të treta të përfshira për përmirësimin e skenareve të ushtrimeve.

4.9. MS9: Menaxhimi i sigurisë së informacionit

Të krijohet dhe mbahet një politikë për monitorimin e pajtueshmërisë së standardeve me kërkesat ligjore

3	c) Të vlerësohen politika/procedurat për pajtueshmërinë dhe auditimin. d) Të rishikohen dhe përditësohen politika/procedurat për pajtueshmërinë dhe auditimin, duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme.	iv. Lista e të gjithë raporteve të pajtueshmërisë dhe auditimeve. v. Politika/procedurat e përditësuara për pajtueshmërinë dhe auditimin, shqyrtimin e komenteve, dhe/ose ndryshimin e log-eve.

4.10. MS10: Kontrolli dhe auditi

	Masat e sigurisë	Dokumentimi
1	a) Të implementohet monitorimi i log-eve për sistemet e informacionit. b) Të implementohet politika e ngjarjeve dhe monitorimit të sistemeve. c) Të vendosen mjete për monitorimin e sistemeve të informacionit. d) Të vendosen mjetet për të mbledhur dhe ruajtur shkrimet e sistemeve të informacionit.	i. ii. Procedura e vlerësimit të performances. iii. Procedura e audit të brendshëm. iv. Rishikimi menaxherial i menaxhimit të sigurisë të sistemeve të informacionit. v. Raport i auditive të brendshëm. vi. Raport i rishikimeve menaxheriale. Log-et dhe raportet e monitorimit të rrjetit të komunikimit dhe të sistemeve te informacionit. vii. Politika të dokumentuara për monitorimin dhe ngjarjet, duke përfshirë kërkesat minimale për monitorimin dhe ngjarjet, periudhën e mbajtjes, dhe objektivat e përgjithshme të ruajtjes.
2	e) Të rishikohet dhe përditësohet monitorimi i politikave / procedurave, duke marrë parasysh ndryshimet dhe incidentet e mëparshme.	viii. Dokumentacioni i monitorimit dhe politikat e ngjarjeve / procedurat, të dokumentuara.

5. MASAT TEKNIKE

5.1 MS1: Siguria fizike Siguria fizike mbulon sigurinë fizike dhe logjike të rrjeteve/sistemeve të informacionit dhe pajisjeve.

5.1.1. Siguria fizike dhe mjedisore

Të krijohet dhe ruhet siguria e duhur fizike dhe mjedisore e rrjeteve/sistemeve të informacionit dhe pajisjeve.

	Masat e sigurisë	Dokumentimi
1	a) Të parandalohet aksesi fizik i paautorizuar në pajisje dhe infrastrukturë dhe të vendosen kontrolle të përshtatshme mjedisore, për të mbrojtur asetet kundër aksesit të paautorizuar, vjedhjes, zjarrit, përmbytjeve, etj.	i. Implementimi bazik i masave të sigurisë fizike dhe kontrolleve mjedisore, si bravat e dyerve dhe kabineteve, alarmi i aksesit të paautorizuar, alarmet e zjarrit, fikësit e zjarrit, etj.
2	b) Implementimi i një politike për masat e sigurisë fizike dhe kontrollet mjedisore. c) Implementimi i standardeve të industrisë të kontrolleve fizike dhe mjedisore. d) Aplikoni kontrolle të përforcuara për aksesin fizik tek asetet kritike.	ii. Politika e dokumentuar për masat e sigurisë fizike dhe kontrollet mjedisore, duke përfshirë përshkrimin e pajisjeve dhe sistemeve në fushëveprim. iii. Kontrollet fizike dhe mjedisore, si kontrolli elektronik i hyrjes dhe log-et e auditimit, segmentimi i hapësirave sipas niveleve të autorizuara, fikësit e automatizuar të zjarrit me gaze halokarbonike, etj. iv. Politika përfshin një listë të aseteve kritike dhe kontrolle fizike të përforcuara për të aksesuar këto asete.
3	e) Vlerësoni efektivitetin e kontrolleve fizike dhe mjedisore në mënyrë periodike. f) Rishikimi dhe përditësimi i politikës për masat e sigurisë fizike dhe kontrollet mjedisore duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme.	v. Politika e përditësuar për masat e sigurisë fizike dhe kontrollet mjedisore. vi. Dokumentim të vlerësimit të kontrollit mjedisor, komentet e rishikimit ose ndryshimit të logeve.

5.1.2. Siguria e furnizimeve (pajisjeve)

Vendosni dhe ruani sigurinë e duhur të furnizimeve kritike (psh:energjia elektrike,karburanti,ftohja etj)

	Masat e sigurisë	Dokumentimi
1	a) Të garantohet siguria e furnizimeve kritike.	i. Siguria e furnizimeve kritike është e mbrojtur në një mënyrë bazike, për shembull, UPS dhe/ose karburanti rezervë është i disponueshëm.
2	b) Implementimi i një politike për sigurinë e furnizimeve kritike. c) Të implementohen masa sigurie të standardit të industrisë për të mbrojtur furnizimet kritike dhe pajisjet mbështetëse (p.sh. ftohja pasive, rinisja automatike pas ndërprerjes së energjisë, energjia rezervë e baterisë, gjeneratorët me naftë, karburanti rezervë, etj).	ii. Politika e dokumentuar për mbrojtjen e furnizimeve kritike si energjia elektrike, karburanti, etj., duke përshkruar llojet e ndryshme të furnizimeve dhe masat e sigurisë që mbrojnë këto furnizime. iii. Dokumentim i masave standarde të industrisë për të mbrojtur sigurinë e furnizimeve kritike.
3	d) Implementimi i masave të avancuara të sigurisë për të mbrojtur furnizimet kritike (si ftohja aktive, UP, gjeneratorët e fuqisë të qëndrueshme, SLA me kompanitë e shpërndarjes së karburantit, ftohja e tepërt dhe sistemet rezervë të energjisë). e) Të rishikohen dhe përditësohen politikat dhe procedurat për të siguruar rregullisht furnizimet kritike, duke marrë parasysh ndryshimet dhe incidentet e mëparshme.	iv. Dokumentimin e masave të avancuara për të mbrojtur sigurinë e furnizimeve kritike. v. Politika e përditësuar për sigurimin e furnizimeve kritike dhe pajisjeve mbështetëse, rishikoni komentet dhe/ose regjistrat e ndryshimeve.

5.2. MS2: Menaxhimi për autorizimin e aksesit

Krijoni dhe mbani kontrolle aksesi të duhura (logjike) për të aksesuar rrjetet e komunikimit dhe sistemet e informacionit.

	Masat e sigurisë	Dokumentimi
1	a) Përdoruesit dhe sistemet kanë ID unike dhe autentifikohen përpara se të hyjnë në shërbime ose sisteme. b) Implementimi i mekanizmave të aksesit të kontrollit logjik për rrjetet dhe sistemet e informacionit për të lejuar vetëm përdorimin e autorizuar.	i. Log-et e aksesit tregojnë identifikues unikë për përdoruesit ii. dhe sistemet kur i jepet apo i mohohet aksesi. Një pasqyrë e përgjithshme e autentifikimit dhe metodave të kontrollit të aksesit për sistemet dhe përdoruesit.
2	c) Implementimi i politikave për mbrojtjen e aksesit në rrjetet dhe sistemet e informacionit, duke adresuar për shembull rolet, të drejtat, përgjegjësitë dhe procedurat për caktimin dhe revokimin e të drejtave të aksesit.	iii. Politika e kontrollit të aksesit e cila përfshin përshkrimin e roleve, grupeve, të drejtave të aksesit, procedurat për dhënien dhe revokimin e aksesit. iv. Lloje të ndryshme të mekanizmave të autentifikimit për lloje të ndryshme aksesi.

	d) Të zgjidhen mekanizmat e duhur të autentifikimit, në varësi të llojit të aksesit. e) Monitorimi i aksesit në rrjetet dhe sistemet e informacionit, të ketë një proces për miratimin e përjashtimeve dhe regjistrimin e shkeljeve të aksesit. b) Të përforcojë kontrollet për aksesin në distancë në asetet kritike të rrjeteve dhe sistemeve të informacionit nga palët e treta.	v. Regjistri i shkeljeve dhe përjashtimeve të politikave të vi. kontrollit të aksesit, të miratuar nga oficeri i sigurisë. vii. Parimet e më pak të privilegjuarit dhe ndarja e detyrave janë të dokumentuara dhe zbatohen aty ku është e mundur. Aksesi në distancë në asetet kritike nga palët e treta minimizohet dhe i nënshtrohet kontrolleve strikte të aksesit, duke përfshirë autentifikimin e avancuar, autorizimin dhe kontrollet e auditimit, veçanërisht për account-et e privilegjuara.
3	g) Vlerësimi i efektivitetit të politikave dhe procedurave të kontrollit të aksesit dhe implementimi i verifikimit të kontrolleve në mekanizmat e kontrollit të aksesit. e) Politika e kontrollit të aksesit dhe mekanizmat e kontrollit të aksesit rishikohen dhe kur nevojitet të korrigjohen.	viii. Raportet e testimeve (sigurisë) të mekanizmave të kontrollit të aksesit. ix. Mjete për zbulimin e përdorimit anormal të sistemeve apo sjelljen anormale të sistemeve (si sistemet e zbulimit të ndërhyrjeve dhe zbulimit të anomalive). x. Log-et e sistemeve të zbulimit të ndërhyrjeve dhe zbulimit të anomalive. xi. Përditësimet e politikës së kontrollit të aksesit, rishikoni komentet ose ndryshimet e regjistrave. xii. Analiza e rrezikut e dokumentuar mbi aplikimin e regjistrimit dhe ruajtjes. xiii. Procedurat për të siguruar që kontrollet e aksesit janë në fuqi gjatë gjithë kohës dhe se ato zhvillohen së bashku me rrjetin.

5.2.1. Ndërgjegjësimi ndaj kërcënimit kibernetik

"Ndërgjegjësimi për kërcënimin kibernetik" mbulon objektivat e sigurisë lidhur me "*threat intelligence*" dhe ndërgjegjësimin e përdoruesve fundorë me qëllim ndarjen e informacionit lidhur me kërcënimet madhore të sigurisë së rrjeteve të komunikimit dhe sistemeve të informacionit.

5.2.1.1 Threat intelligence

Të krijohet dhe mbahet një mekanizëm për monitorimin dhe mbledhjen e informacionit në lidhje me kërcënimet përkatëse të sigurisë së rrjeteve të komunikimit dhe sistemeve të informacionit

	Masat e sigurisë	Dokumentimi

1	a) Informimi i përdoruesve fundorë të rrjeteve të komunikimit dhe sistemeve të informacionit rreth kërcënimeve të sigurisë kibernetike që mund t'i prekin ata.	i. ii. Buletini i sigurisë, një faqe interneti e dedikuar për informacion mbi kërcënimet kibernetike ose një mekanizëm tjetër i dokumentuar dhe i testuar për të kontaktuar me përdoruesit fundorë në rast kërcënimesh të rëndësishme. Lista të dokumentuara të praktikave më të mira dhe rekomandimet e sigurisë për përdoruesit fundorë për të minimizuar rreziqet tipike (p.sh. kriptimin, autentifikimin e sigurt, përditësimet, backup-et, ndërgjegjësimin e përdoruesve).

	Masat e sigurisë	Dokumentimi
1	a) Të kryhet monitorim i vazhdueshëm i kërcënimeve kibernetike	i. Monitorim i vazhdueshëm i burimeve të jashtme të " threat intelligence" (OSINT, risitë komerciale, hulumtimet e sigurisë) me një log të regjistruar të ngjarjeve të rëndësishme të kërcënimeve. ii. Ndarja përkatëse joformale dhe ad hoc e "threat intelligence" me organizatat përkatëse mbi baza dypalëshe.
2	b) Të zbatohet programi i "threat intelligence".	iii. Programi i dokumentuar dhe i implementuar i "threat intelligence" që përfshin rolet, përgjegjësitë, procedurat dhe mekanizmat për mbledhjen e informacionit lidhur me kërcënimet e rëndësishme dhe masat parandaluese përkatëse. iv. Programi pëfshin gjithashtu mekanizma për ndarjen sistematike të "threat intelligence" me organizatat përkatëse mbi baza dypalëshe dhe shumëpalëshe duke përdorur një platformë të dedikuar ndarjes së "threat intelligence" (p.sh MISP). v. Ekzistenca e një skeme të përshtatshme të shënimit të informacionit për lehtësimin e ndarjes së informacionit të ndjeshëm ndaj kërcënimit (psh. TLP).
3	c) Të rishikohet dhe përditësohet programi i "threat intelligence". d) Programi "threat intelligence" përdor sistemet më të fundit të "threat intelligence".	vi. vii. Përditësimi i programit të "threat intelligence", shqyrtimi i komenteve, dhe/ose ndryshimi I log-eve. Përdorimi i platformës "threat intelligence" (TIP) me funksionalitetin më të fundit (psh. konsolidimi i mekanizmave të "threat intelligence" nga burime të ndryshme, automatizimi, analizat e sigurisë dhe integrimi me mjetet e tjera të sigurisë etj.)

5.2.1.2. Informimi i përdoruesve rreth kërcënimeve të sigurisë kibernetike

Të informohen përdoruesit rreth kërcënimeve të sigurisë kibernetike të rrjeteve dhe sistemeve të informacionit që mund të prekin përdoruesit fundorë dhe për masat që mund të marrin për të mbrojtur sigurinë e sistemeve të tyre.

2	b) Zbatimi i politikës/procedurave për informimin e vazhdueshëm të përdoruesve fundorë lidhur me kërcënimet e sigurisë së rrjetit të komunikimit dhe sistemit të informacionit që mund t'i prekin ata.	iii. Politika e dokumentuar dhe e implementuar e kontaktit me përdoruesit fundorë me role dhe përgjegjësi të përcaktuara, mekanizmat dhe kriteret për identifikimin e kërcënimeve të rëndësishme dhe procedurat, mjetet dhe metodat për informimin në kohë dhe të duhur të përdoruesve fundorë. iv. Politika përfshin mekanizma për identifikimin dhe shpërndarjen e rekomandimeve dhe praktikave më të mira për përdoruesit fundorë për minimizimin e kërcënimeve specifike.
3	c) Rishikimi dhe përditësimi i politikave/procedurave për informimin e vazhdueshëm të përdoruesve fundorë mbi kërcënimet e sigurisë të rrjetit të komunikimit dhe sistemit që mund t'i prekin ata.	v. Politika e përditësuar e kontaktit, shqyrtimi i komenteve, dhe/ose ndryshimi i loge-ve.

5.3. MS3: Pajisjet kriptografike

Të sigurohet përdorimi adekuat i enkriptimit për të parandaluar dhe/ose minimizuar impaktin e incidenteve të sigurisë kibernetike tek përdoruesit, në rrjetet e komunikimit dhe sistemet e informacionit.

	Masat e sigurisë	Dokumentimi
1	a) Atëhere kur është e përshtatshme për të parandaluar dhe/ose minimizuar impaktin e incidenteve të sigurisë kibernetike mbi përdoruesit, në rrjete dhe shërbime të tjera, të enkriptohen të dhënat gjatë ruajtjes së tyre dhe/ose transmetimit nëpërmjet rrjeteve.	i. Përshkrimi i të dhënave kryesore të transferuara (data flow), si ii. dhe protokollet e enkriptimit dhe algoritmet e përdorura për secilin transferim. Përshkrimi i përjashtimeve dhe kufizimeve të justifikuara në implementimin e enkriptimit.
2	viii. Implementimi i politikës së enkriptimit. ix. Të përdoren algoritme të enkriptimit të standardit të industrisë, me gjatësitë përkatëse të rekomanduara të çelësave të enkriptimit.	iii. Dokumentim i politikave të enkriptimit duke përfshirë detaje rreth algoritmeve kriptografike dhe çelësave kriptografikë përkatës, sipas praktikave dhe standardeve më të mira ndërkombëtare. iv. Dokumentim i përjashtimeve të justifikuara të cilat ofrojnë arsyetim kur të dhënat nuk janë të enkriptuara, duke përfshirë vlerësimin e impaktit përkatës.
3	d) Rishikim dhe përditësim i politikave të enkriptimit. e) Të përdoren algoritme të avancuara të enkriptimit.	v. vi. Politika e enkriptimit e përditësuar, rishikimi i komenteve dhe/ose ndryshimi të log-eve. Politika e enkriptimit përfshin detaje mbi protokollet kriptografike të avancuara të përdorura.

5.3.1 Mbrojtja e sigurisë së të dhënave kritike

Të sigurohet që çelësi kriptografik dhe informacioni sekret i autentifikimit të jenë të mbrojtura në mënyrë adekuate.

	Masat e sigurisë	Dokumentimi
1	a) Sigurohuni që çelësi kriptografik dhe informacioni sekret i autentifikimit (përfshirë materialin e çelësit kriptografik të përdorur për autentifikim) të mos zbulohen ose të ngatërrohen. b) Aksesi në çelësat privat është i kontrolluar dhe i monitoruar në mënyrë rigoroze.	i. Çelësi kriptografik dhe informacioni sekret i autentifikimit janë ii. të mbrojtura duke përdorur praktikat më të mira të sigurisë dhe standardet për mekanizmat e mbrojtjes (si njohuritë e ndara *split knowledge* dhe kontrolli i dyfishtë, enkriptimi, hashimi, hardware i sigurt etj.). Përshkrimi i mekanizmave për kontrollin dhe monitorimin e aksesit për tek çelësat privatë.

2	c) d)	Implementim i politikës për menaxhimin e çelësave kriptografikë. Implementim i politikës për menaxhimin e fjalëkalimeve të përdoruesve.	iii. iv.	Politika për menaxhimin e çelësave duke përfshirë rolet, përgjegjësitë dhe kontrollet për përdorimin, mbrojtjen dhe jetëgjatësinë e çelësave kriptografikë gjatë gjithë ciklit jetësor të tyre, duke përfshirë kontrollet për akses si dhe *backup* dhe *recovery* të çelësave privatë. Politika për menaxhimin e fjalëkalimeve të përdoruesit duke përfshirë proceset, metodat dhe teknikat për një ruajtje më të sigurt të fjalëkalimeve të përdoruesve duke përdorur praktikat më të mira të industrisë
3	e) f)	Rishikim dhe përditësim i politikës të menaxhimit të çelesit. Rishikim dhe përditësim i politikave për menaxhimin e fjalëkalimeve të përdoruesve.	v. vi.	Politika e përditësuar e menaxhimit të çelësave, rishikoni komentet dhe/ose ndryshimet e log-eve. Politika e përditësuar e menaxhimit të fjalëkalimit të përdoruesit, rishikimi i komenteve dhe/ose ndryshimet e log-eve.

5.4. MS4: Zbulimi i ngjarjeve të sigurisë kibernetike

Të krijohen dhe mbahen kapacitete për zbulimin e incidenteve të sigurisë kibernetike që identifikojnë incidentet.

	Masat e sigurisë	Dokumentimi
1	a) Krijimi i proceseve ose sistemeve për zbulimin e incidentit kibernetik.	i. Shembuj të dokumentuar të incidenteve të mëparshme që janë zbuluar dhe janë dërguar në kohë tek personat përkatës.
2	b) Implementimi i sistemeve dhe procedurave te bazuara ne standartet e njohura ndërkombëtare për zbulimin e incidenteve kibernetike. c) Implementimi i sistemeve dhe procedurave për regjistrimin dhe dërgimin në kohë të incidenteve tek personat e duhur.	ii. Sistemet dhe procedurat e zbulimit të incidenteve, të tilla si mjetet e Incidentit të Sigurisë dhe Menaxhimit të Ngjarjeve (SIEM), asistenca për sigurinë e personelit, raportet dhe këshillimet nga Ekipet e Përgjigjes ndaj Emergjencave Kompjuterike (CERT), mjetet për të dalluar anomalitë, etj. iii. Qendrat Operative të Rrjeteve (NOC) dhe/ose Qendrat Operative të Sigurisë (SOC) për sigurimin e transparencës dhe monitorimit efektiv të rrjetit, për të zbuluar anomalitë, për të identifikuar dhe shmangur kërcënimet.
3	d) Rishikimi periodik i sistemeve dhe proceseve për zbulimin e incidenteve dhe përditësimi i tyre duke marrë parasysh ndryshimet dhe incidentet e mëparshme. e) Implementimi i sistemeve dhe procedurave të avancuara për zbulimin e incidenteve të sigurisë kibernetike.	iv. Dokumentacioni i përditësuar i sistemeve dhe proceseve të zbulimit të incidenteve të sigurisë kibernetike. v. Dokumentacioni i rishikimit të procesit të zbulimit të incidentit të sigurisë kibernetike, shqyrtim i komenteve dhe/ose ndryshim i loge-ve. vi. Përdorimi i zgjidhjeve NOC/SOC avancuara - p.sh. SOAR (Security Orchestration, Automation and Response-Harmonizimi i Sigurisë, Automatizimi dhe Përgjigjia), duke siguruar integrimin me kërcënimin dhe menaxhimin e mangësive, reagimin ndaj incidentit, automatizimin e operacioneve të sigurisë etj.

5.5. MS5: Mjetet e gjurmimit të vlerësimit të ngjarjeve të sigurisë kibernetike

Mjetet e gjurmimit të vlerësimit të ngjarjeve të sigurisë kibernetike përfshijnë monitorimin, testimin dhe auditimin e rrjetit dhe sistemeve të informacionit dhe pajisjeve.

5.5.1. Montorimi dhe politikat e regjistrimit

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

	Masat e sigurisë		Dokumentimi	
1	a)	Të implementohet monitorimi dhe regjistrimi i sistemeve kritike.	i.	Log-et dhe raportet e monitorimit të rrjetit kritik dhe të sistemeve te informacionit.
2	c)	Të implementohet politika për regjistrimin dhe monitorimin e sistemeve kritike.	ii. iii.	Politika të dokumentuara për monitorimin dhe regjistrimin, duke përfshirë kërkesat minimale për monitorimin dhe regjistrimin, periudhën e mbajtjes, objektivat e përgjithshme të ruajtjes, monitorimit të të dhënave dhe log-et.
	d)	Të vendosen mjete për monitorimin e sistemeve kritike.		Mjete për monitorimin e sistemeve dhe mbledhjen e log-eve.
	e)	Të vendosen mjete për të mbledhur dhe ruajtur log-et e sistemeve kritike.	iv.	Lista e të dhënave të monitoruara dhe skedarët e log- eve, në përputhje me politkën.
3	f)	Të vendosen mjete për grupimin e automatizuar dhe shqyrtimin e të dhënave dhe loge-ve të monitoruara.	v. vi.	Mjete për të lehtësuar regjistrimin dhe analizën strukturore të monitorimit dhe log-eve.
	g)	Rishikimi dhe përditësimi i regjistrave (logging) dhe politikave/ procedurave monitoruese, duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme.		Dokumentacioni i përditësuar i politikave/procedurave të monitorimit dhe regjistrimit (logging), rishikim i komenteve dhe/ose ndryshim i loge-ve.

5.6. MS6: Mbrojtja e integritetit të rrjeteve të komunikimit

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

	Masat e sigurisë		Dokumentimi	
1	a)	Të sigurohet që software-i i rrjetit dhe sistemeve të informacionit të mos jetë i manipuluar ose ndryshuar, për shembull duke përdorur kontrollet e hyrjes dhe firewall-et.	i. ii.	Software-i dhe të dhënat në rrjetet dhe sistemet e informacionit mbrohen duke përdorur kontrollet e hyrjes, firewall-et, enkriptimin dhe nënshkrimin.
	b)	Të kontrollohet për malware-t në rrjetin (e brendshëm) dhe sistemet e informacionit.		Të ekzistojnë sistemet e zbulimit te malware-ve dhe të jenë të përditësuara.
2	c)	Të implementohen masa të sigurisë të standardit të industrisë, duke siguruar mbrojtje të detajuar kundër ndërhyrjeve dhe ndryshimeve të sistemeve.	iii.	Dokumentim të mënyrës se si implementohet mbrojtja e software-t dhe të dhënave në rrjet dhe sistemin e informacionit.
	d)	Të aplikohet integritet i konsoliduar i software-it, të përditësohen dhe korrigjohen kontrollet e menaxhimit për asetet kritike në rrjetet e virtualizuara.	iv.	Mjetet për zbulimin e përdorimit anormal të sistemeve apo sjelljes anormale të sistemeve (si sistemet e zbulimit të ndërhyrjeve dhe zbulimit të anomalive).
			v. vi.	Log-et e sistemeve të zbulimit të ndërhyrjeve dhe zbulimit të anomalive.
				Mjete dhe procese adekuate për të siguruar integritetin e softuerit kur performohen përditësime të software-ve dhe kur aplikohen korrigjime (patch-e) të sigurisë për asetet kritike në rrjetet e virtualizuara.
3	e)	Të vendosen kontrolle të avancuara për të mbrojtur integritetin e sistemeve.	vii. viii.	Kontrollet e avancuara për të mbrojtur integritetin e sistemeve, të tilla si nënshkrimi, tripwire, etj.
	f)	Të vlerësohet dhe të rishikohet efikasiteti i masave për të mbrojtur integritetin të sistemeve.		Dokumentimi i procesit për kontrollin e log-eve të sistemeve të zbulimit të anomalive dhe ndërhyrjeve.

5.6.1. Testimi i rrjeteve dhe sistemeve të informacionit

Të vendosen dhe mbahen politika për testimin e rrjeteve dhe sistemeve të informacionit, veçanërisht kur lidheni me rrjete ose sisteme të reja.

	Masat e sigurisë	Dokumentimi
1	a) Të testohen rrjetet dhe sistemet e informacionit përpara përdorimit dhe lidhjes së tyre me sistemet ekzistuese.	i. Raportet e testimit të rrjetit dhe sistemeve të informacionit, duke përfshirë testimet pas ndryshimeve të mëdha ose përdorimit të sistemeve të reja.
2	b) Të implementohen politika/procedurat për testimin e rrjetit dhe sistemeve të informacionit. c) Të implementohen mjetet për testimin e automatizuar.	ii. Politika/procedurat për testimin e rrjeteve dhe sistemeve të informacionit, përfshirë se kur duhet të kryhen këto testime, planet e testimit, rastet e testimit, modelet për raportimin e testimit.
3	d) Të rishikohen dhe përditësohen politika/procedurat për testimin, duke marrë në konsideratë ndryshimet dhe incidentet e mëparshme.	iii. Lista e raporteve të testimit. iv. Politika/procedura të përditësuara të testimit të rrjetit dhe sistemeve të informacionit, shqyrtimi i komenteve, dhe/ose ndryshimi i log.

5.6.2. Vlerësimet e sigurisë

Të krijohet dhe mbahet një politikë e përshtatshme për vlerësimin e sigurisë së rrjetit dhe sistemeve të informacionit.

	Masat e sigurisë	Dokumentimi
1	a) Të sigurohet që sistemet kritike t'u nënshtrohen rregullisht skanimeve të sigurisë dhe testeve të sigurisë, veçanërisht kur kemi përdorimin e sistemeve të reja dhe ndryshime.	i. Raporte nga skanimet dhe testet e mëparshme të sigurisë.
2	b) Të implementohen politika/procedurat për vlerësimin dhe testimin e sigurisë.	ii. Politika/procedurat e dokumentuara për vlerësimet dhe testimet e sigurisë, përfshirë, cilat asete, në cfarë rrethanash, llojin e vlerësimit dhe testimit të sigurisë, frekuencën, palët e aprovuara (të brendshme ose të jashtme), nivelet e konfidencialitetit për vlerësimin, rezultatet e testimit dhe objektivat e vlerësimeve dhe testeve të sigurisë.
3	c) Të vlerësohet efektiviteti i politikave/procedurave për vlerësimet e sigurisë dhe testimin e sigurisë. d) Të rishikohet dhe përditësohet politika/procedurat për vlerësimet dhe testimet e sigurisë, duke marrë në konsideratë ndryshimet dhe incidentet e mëparshmne.	iii. Lista e raporteve mbi vlerësimet e sigurisë dhe testimet e sigurisë. iv. Raportet e veprimeve vijuese mbi vlerësimet dhe testimet e sigurisë. v. Politika/procedura të përditësuara për vlerësimet e sigurisë dhe testimet e sigurisë, shqyrtimi i komenteve, dhe/ose ndryshimi i log-eve.

5.7. MS7: Verifikimi i identitetit të përdoruesve

Masat e sigurisë	Dokumentimi

1 2	a) Të imlementohet monitorimi i të dhënave kritike. b) Të implementohet politika e ngjarjeve dhe monitorimi i sistemeve kritike. c) Të vendosen mjete për monitorimin e sistemeve kritike. d) Të vendosen mjetet për të mbledhur dhe ruajtur shkrimet e të dhënave kritike.	i. Raportet e monitorimit të rrjetit kritik dhe të sistemeve të informacionit. ii. Kërkesat për verifikimin e figurës së përdoruesve. iii. Dokumenti i kërkesave për akses. iv. Politika të dokumentuara për monitorimin dhe ngjarjet, duke përfshirë kërkesat minimale për monitorimin dhe ngjarjet, periudhën e mbajtjes, objektivat e përgjithshme të ruajtjes, monitorimin e të dhënave dhe log-et.

5.8. MS8: Veprimtaria e administratorëve dhe përdoruesve

	Masat e sigurisë	Dokumentimi
1	a) T'i caktohen personelit rolet e sigurisë dhe përgjegjësitë. b) Të sigurohet që rolet e sigurisë janë të arritshme në rast se ndodhin incidente të sigurisë kibernetike. c) Të emërohet personeli zyrtarisht në rolet e sigurisë. d) Të vendoset personeli në dijeni të roleve të sigurisë në organizatë dhe kur duhet të kontaktohen.	i. Listë e emërimeve (CISO, DPO,etj.) dhe përshkrimi i përgjegjësive dhe detyrave për rolet e sigurisë (CISO, DPO, etj. ii. Materiale ndërgjegjësimi dhe informimi për personelin duke shpjeguar rolet e sigurisë dhe kur / si ata duhet të kontaktohen. iii. Listë e pozicioneve të sigurisë (menaxher i vazhdimësisë së biznesit, etj.)
2	e) Të rishikohet rregullisht struktura e roleve të sigurisë dhe përgjegjësive, si pasojë e ndryshimeve dhe / ose incidenteve të mëparshme.	iv. Dokumentim i procesit të rishikimit, dı konsideratë ndryshimet dhe rincidentet e

5.9 MS9:Siguria e aplikacioneve

	Masat e sigurisë	Dokumentimi
1	a) Të kryhen vlerësimet e sigurisë e aplikimit web nga personeli i sigurimit të deleguara ose të punësuar ose të kontraktuar nga institucioni. Të gjitha gjetjet që janë konsideruar konfidenciale, duhet të shpërndahen personave me një "nevojë për njohje bazë". Shpërndarja e gjetjeve jashtë institucionit është rreptësishtë e ndaluar, përveç nëse miratohet nga eprori.	i. Dokumenti i vlerësimeve të sigurisë.
2	b) Çdo marrëdhënie brenda aplikacioneve do të përfshihen në vlerësimin nëse nuk kufizohet në mënyrë eksplicite.	ii. Dokumenti i vlerësimeve të sigurisë.

5.10 MS10 Siguria e sistemeve industriale

	Masat e sigurisë	Dokumentimi

1	a) Kontrolli i sistemeve industriale, duke përfshirë kontrollin mbikëqyrjes së të dhënave, kontrollin e sistemeve, dhe konfigurime të tjera të sistemit të kontrollit të tilla si kontrollin e programeve logjike. b) Trajtimin e performancës unike, besueshmërinë dhe sigurisë së kërkesave.	i. Përditësim të kontrollit të sistemeve industriale, kërcënimet dhe dobësitë. ii. Përditësim për menaxhimin e rrezikut në sistemet industriale, praktikat e rekomanduara dhe arkitektura. iii. Përditësim për aktivitetet aktuale në sigurinë e sistemeve industriale. iv. Përditësim për aftësitë e sigurisë dhe mjetet për sistemet industriale, shtrirjes shtesë me standardet e tjera të sigurisë dhe udhëzimet. v. Standarde dhe udhëzime të reja për sistemet industrial. vi. Zhvillimin e politikave të sigurisë, procedurat, trajnimin dhe materiale edukative që vlen në mënyrë specifike për SI. vii. Duke marrë parasysh politikat e sigurisë për sistemet industriale dhe procedurat bazuar në nivelin e kërcënimit. viii. Duke iu drejtuar sigurisë gjatë gjithë ciklit të jetës së sistemeve industriale nga dizajni i arkitekturës të prokurimit të instalimit tek mirëmbajtja e sistemit. ix. Zbatimi i një topologjie rrjeti për sistemet industriale që ka shtresa të shumëfishta, me komunikimet më kritike ndodhen në shtresën më të sigurtë dhe të besueshme. x. Projektimi sistemeve kritike për degradim (pjesë e tolerancës) për të parandaluar ngjarjet katastrofike. xi. Paaftësi portet dhe shërbime në pajisjet SHKB papërdorura pas testimit për të siguruar se kjo nuk do të ndikojë operacion ICS. xii. Kufizimi në akses fizik në rrjetin dhe pajisjet e sistemeve industriale xiii. Kufizimi i drejtave të përdoruesit vetëm ata që janë të nevojshëm për të kryer punën (d.m.th., duke vendosur kontrollin e aksesit të bazuar në konfigurimin për çdo rol kryesor) në sistemet industriale xiv. Përdorimi i mekanizmave të veçanta të autentifikimit dhe kredencialet për përdoruesit e rrjetit në sistemet industriale dhe rrjetit të korporatës (d.m.th., llogaritë e rrjetit sistemet industriale nuk i përdorin llogaritë e përdoruesve të rrjetit të korporatës).

ANEKS 1

Masat e shtuara teknike

		Afati i Implementimit		
Nr.	**Masat Minimale të Sigurisë**	**Metodologjia**	**Infrastruktura të Rëndësishme**	**Infrastruktura Kritike**
1	Të instalohen pajisje të perimetrit të rrjetit që bëjnë analizë të thellë të trafikut duke u mbështetur jo vetëm në rregullat e listave të aksesit por edhe në sjelljen e tij (Firewall-et).	Kjo masë i referohet përmirësimit të perimetrit të rrjetit. Perimetri i rrjetit i mbrojtur me anë të teknikave të analizës së rregullave të aksesit të konfigurara nga administratori i rrjetit është i pamjaftueshëm dhe kollaj i anashkalueshëm. Zhvillimet e fundit teknologjike kërkojnë ngritjen e teknikave të mbështetura në analizën e sjelljes së trafikut duke integruar firewall-et me shërbime IDS/IPS. Këto lloj firewall-esh janë quajtur Next Generation Firewall, duke bërë një analizë nga shtresa e 1-rë e arkitekturës OSI deri në atë të 5 të saj, duke eleminuar mundësinë e trafiqeve me sjellje jo të zakonshme.	6 muaj	3 muaj
2	Të merren parasysh skemat "High-Availability" në pajisjet "core-network" në nivel perimetri (firewall), në nivel rutimi (L3) dhe komutimi paketash (L2) dhe nivel linjash fizike (L1).	Skemat me disponueshmëri të lartë këtu i referohen piramidës së pajisjeve në nivelin e rrjetit, duke nisur nga niveli i perimetrit të jashtëm deri në brendësi të rrjetit lokal, të quajtur LAN. Më konkretisht: 1. Ofrimi i dy ose më shumë firewall-eve ose routerave në modelin Active-Pasive (Fail-Over) ose Active Active (Load Balancing) 2. Switch-et në modelin Active-Pasive dhe Active-Active 3. Ofrimi i internetit dhe data nga dy ose më shumë providera të ndryshëm	6 muaj	3 muaj
3	Të merren masa për shfrytëzimin e teknikave të pasqyrimit të të dhënave (RAID 1/5/6/10) për të shmangur humbjen e të dhënave sensitive.	Të gjitha të dhënat e shërbimeve të gjeneruara nga institucioni juaj në modelin data at rest, të ruajtura në pajisje storage të konfigurohen me teknikat e pasqyrimit të njohura si RAID – Redundant Array Independent Disk në njërin nga modelet e mëposhtme:	3 muaj	1 muaj

		1. RAID 1 - Kjo do të kërkonte dy-fishimin e burimeve 2. RAID 5 - Kjo do të kërkonte përdorimin e minimumit të tre disqeve fizikë të ndryshem për çdo konfigurim 3. RAID 6 - Si RAID 5 por kërkon edhe prezencën e një disku Rezervë të njohur si HOT Spare 4. RAID 1+0 - Si RAID 1 por rrit me dy-fish shpejtësinë e kërkimit të të dhënave në storage, krahasuar me teknikën RAID 1. Ky model duhet të kërkohet për të gjitha shërbimet: a. Të ofruara nga vetë institucioni b. Të hostuar nga palët e treta në institucionin tuaj.		
4	Të merren masa për shmangien e "Single Point of Failure" tek shërbimet tuaja kritike dhe të rëndësishme	Kjo pikë i referohet arkitekturës së shërbimeve. Shërbimet kritike dhe të rëndësishme duhet të jenë të vendosura në dy ose më shumë ambjente hostuese të cilat replikojnë të dhënat në kohë reale. Kjo arkitekturë quhet Active-Active. Ndërkohë kjo arkitekturë mbështetet në replikimin e të dhënave në kohë reale për: a. Shërbimet që janë të hostuara në një host janë të replikuara me downtime = 0 në një host tjetër b. Baza e të dhënave kritike dhe të rëndësishme duhet të replikohen nga një host në një host tjetër (Teknikat RAID 1,5,6,10 NUK mbulojnë këtë kërkesë).	6 muaj	3 muaj
5	Të aplikohen filtra të trafikut në rastin e aksesimit në distancë të hosteve (punonjësve/palë të treta/klientë).	Teknika e aksesimit në distancë ka si qëllim ofrimin e shërbimit drejt një vendodhjeje tjetër. Kjo teknikë duhet të realizohet në mënyrë të sigurtë përmes tuneleve të enkriptimit me anë të teknikave:	12 muaj	6 muaj

		1- IPSEC ose SSL. 2- Tunelet IPSEC duhet të jenë të konfiguruara me anë të formatit IKEv2 dhe minimalisht enkriptimi simetrik të realizohet përmes algoritmave AES 256 dhe me çelsa asimetrik me gjatësi RSA 2048 bit. 3- Ndërkohë akseset nga distanca duhet të shoqërohen me: a. Analizë për fluktuacionin e trafikut b. Authentikimi me 2FA c. Implementimi i arkitekturës zero-trust.		
6	Të implementohen zgjidhje që kryen filtrimin, monitorimin dhe bllokimin e trafikut keqdashës ndërmjet aplikacioneve Web dhe internetit, Web Application Firewall (WAF).	Duke ditur që sulmet më të shpeshta përfundojnë drejt shtresës së Aplikacionit siç janë ato të quajtura OWASP, teknikat e mbrojtjes me Firewall Next Generation pavaresisht se bëjnë Depth-Analysis, nuk mund të filtrojnë dhe analizojnë trafikun në shtresën Sesion/Prezantim dhe Aplikacion. Në këtë rast, përfshirja e një shtrese shtesë do të sillte një filtrim më të mirë të trafikut për ato shërbime që janë të aksesueshme përmes Web, të quajtura Web-Service.	18 muaj	12 muaj
7	Të kryhen analiza të trafikut në nivel sjellje “behaviour” për pajisjet fundore.	Mbrojtja e sistemeve fundore me anë të sistemeve anti-malware tradicionale të mbështetura vetëm në “signature” është shumë kollaj i manipulueshëm. Kërkesa për të pasur këto sisteme duke analizuar sjelljen e trafikut do të ishte një vlerë e shtuar dhe do të rriste sigurinë në sistemet fundore si Servera apo stacionet fundore të punonjësve. Këtyre sistemeve i referohemi si EDR – Endpoint Detection and Response. Ky lloj sistemi kontrollon edhe skedarët që bëhen upload nga vetë sistemet e operatorit ekonomik drejt një sistemi tjetër kudo. Do të ishte e preferuar për të parë sjelljen në formë matricore të ishte e instaluar XDR, i cili mbledh të gjitha aktivitetet e EDR të instaluar në sistemet fundore.	3 muaj	1 muaj

		Të shikohet feature që të analizojë trafikun në nivel sjellje "behaviour" për pajisjet fundore.		
8	Të projektohet zgjidhja për menaxhimin e aksesit të përdoruesve "Identity Access Management" për të kontrolluar identitetin dhe privilegjet e përdoruesve në kohë reale sipas parimit "zero-trust".	Implementimi i kësaj mase është i ndarë në dy faza: 1- Ngritja e një sistemi qëndror per administrimin e të gjithë përdoruesve të konfiguruara me anë të teknikave LDAP sic janë Active Directory të Windows. Këto sisteme duhet të jenë versioni 2016 e sipër, pasi ofrojnë karakteristika shtesë sigurie si psh: SMB v3. 2- Instalimi i një Identity Access Management qëndror i cili verifikon nivelin e identitit të cdo përdoruesi dhe të drejtat e tij duke u mbështetur në arkitekturën 0-trust dhe 2 FA. IAM moderne kanë të integruar karakteristika të vecanta, si, PAM (Privilege Access Management). Do të ishte e rekomandueshme që të ishtë e ngritur teknika Single Sign ON jo vetëm për përdoruesit e privilegjuar por edhe për përdorues të thjeshtë. Kjo teknikë është parashikuar që të projektohet për 3 muaj për infrastruktura kritike dhe deri në 6 muaj për infrastrukturat e rëndësishme. Ndërkohë koha e implementimit të saj mund të variojë nga 6 muaj deri në 18 muaj në varësi të numrit të përdoruesve dhe të infrastrukturës nëse është kritike apo e rëndësishme. 1- Nëse numri i përdoruesve është <50 dhe numri i shërbimeve është <100 -> Koha mesatare e implementimit varion nga 6 muaj deri 12 muaj për infrastrukturat kritike dhe 12 muaj – 18 muaj për infrastrukturat e rëndësishme. 2- Nëse numri i përdoruesve është 51-150 dhe numri i shërbimeve të integruara është 101- 500 -> Koha mesatare e	Koha e projektimit 6 muaj Koha e Implementimit 12-18 muaj për <50 përdorues dhe numri i shërbimeve të integruara <100 Koha e Implementimit 15-24 muaj për 51-150 përdorues dhe numri i shërbimeve të integruara 101-500	Koha e projektimit 3 muaj Koha e Implementimit 6-12 muaj për <50 përdorues dhe numri i shërbimeve të integruara <100 Koha e Implementimit 12-15 muaj për 51-150 përdorues dhe numri i shërbimeve të integruara 101-500

		Implementimit varion nga 12 muaj deri 15 muaj për infrastrukturat kritike dhe 15-24 muaj për ato të rëndësishme. 3- Nëse numri i përdoruesve është >150 dhe numri i shërbimeve të integruara është > 500 -> Koha mesatare e implementimit varion nga 15 muaj deri 18 muaj për infrastrukturat kritike dhe 18-24 muaj për ato të rëndësishme.	Koha e Implementimit 18-24 muaj për >150 përdorues dhe numri i shërbimeve të integruara >500	Koha e Implementimit 15-18 muaj për >150 përdorues dhe numri i shërbimeve të integruara >500
9	Të implementohet sistem i automatizuar për menaxhimin dhe filtrimin e log-eve me qëllim identifikimin e alerteve në kohë reale.	Sistemi i automatizuar i log-eve sjell një avantazh në menaxhimin e tyre duke qenë se sasia e ofruar është shumë e lartë. Filtrimi i logeve dhe skedulimi i playbook-eve të krijuar nga specialistët e sektorit të Monitorimit, do t`a bënte më eficient rolin e këtyre platformave. Shpesh herë këto platforma janë të integruara me teknikat SOAR të cilat ofrojnë përgjigje automatike ndaj një incidenti të njohur me parë dhe jo vetëm (Një pjesë e tyre janë të pajisura me inteligjencë artificiale duke perdorur teknikën Learn by Doing). Në rastin kur sasia e logeve është mbi 50GB/Ditë bëhet e vështirë dhe jo efikase kontrolli i tyre në menyrë manuale. Instalimi i një sistemi automatik të shoqëruar me një sistem me Inteligjencë Artificiale SOAR të integruar do ta rriste efikasitetin e shërbimeve.	12 muaj	6 muaj
10	Nëse keni një departament zhvillimi, të realizohen testime të zhvillimeve të software-ve (stage-ing) në ambient të izoluar të ndarë nga ambienti i prodhimit(production).	Departamentet e zhvillimit për shkak të profilit të punes së tyre kanë të drejta të pakufizuara testimi dhe privilegjesh. Për këtë arsye duhet që këto ambjente të jenë të izoluara në mënyrë virtuale duke përdorur segmentimin e rrjetit me anë të teknikës VLAN ose në rastin më të mirë me ndarje fizike përmes teknikës Air GAP. Teknikat VLAN mund të ngrihen në switchet e shtresës së dytë/tretë ose duke përdorur Firewall dhe duke filtruar trafiqet përmes listave të aksesit.	6 muaj	3 muaj

		Kjo teknikë nuk shoqërohet me kosto shtesë. Vini re, në këtë metodologji nuk ka të bëjë analiza për ngritjen e ambjentit të testimit por vetëm segmentimi i rrjetit të ambjentit të testimit dhe izolimi i tij me ambjentin e biznesit. Segmentimi i tij mund të realizohet me anë të VLAN jo default për shkak të vulnerabilitetit të njohur si VLAN Hopping. Një ambjent testimi nëse nuk ekziston kërkon një analizë nga vetë operatori ekonomik dhe varion në bazë të volumit të testimeve që do të kryhen. Kosto e tyre është shumë e ndryshueshme pasi duhet të merren parasysh: a. Numri i serverave të cilët do te ngrihen në segmentin e testimit b. Numri i Sistemeve Operative të nevojshme c. Nëse do të duhej një ose disa Platforma virtualizimi d. Nëse do të mund të duhej një ose disa sisteme Baza të dhënash të integruara. e. Nëse do të mund të duhej një Network më vete me pajisje shtesë për testime si: I. Firewall-e II. Switche të menaxhueshëm III. Routera etj		
11	Të merren masa për implementim e një sistemi që kontrollon parametrat e sigurisë së një sistemi fundor, duke mos e lejuar këtë të fundit të jetë	Forcimi i sistemeve fundore duke përcaktuar në menyrë strikte një baseline të quajtur “hardening” do të bënte sistemet tuaja fundore më të sigurta në rrjetin e brendshëm.		

	pjesë e rrjetit tuaj nëse këto parametra janë nën nivelin “baseline” të dhënë më parë nga ju? (Sistem i cili kontrollon mungesën e patch-eve, update-t të Anti-Virusit etj).	Baseline mund të jetë si më poshtë vijon: a. Sistemi duhet të jetë me Patchimin e Fundit të Windows (Nëse është i familjes Microsoft). Në të kundërt duhet të njoftojë cdo një ore drejt përdoruesit dhe Administratorit të Rrjetit. Nëse ka dy patching të pa instaluara atëherë sistemi nuk mund të bëhet pjesë e rrjetit. b. Sistemi duhet të jetë me Patch-imin më të fundit të Office (Nëse është on-prem). Në të kundërt duhet të njoftojë cdo një orë drejt përdoruesit dhe Administratorit të Rrjetit. Nëse ka dy patching të pa instaluara atëherë sistemi nuk mund të bëhet pjesë e rrjetit. c. Sistemi duhet të jetë me Anti Malware family me të fundit të patchuar. Në të kundërt duhet të njoftojë cdo një orë drejt përdoruesit dhe Administratorit të Rrjetit. Nëse ka dy patching të pa instaluara atëherë sistemi nuk mund të bëhet pjesë e rrjetit. d. Sistemi duhet të ketë të konfiguruar sic duhet Firewall-in lokal (Nuk duhet të ketë rules permit any-any apo porta rdp të hapura (Remote Desktop)). e. Nuk duhet të ketë të instaluar Sistem Operativ dhe/ose Aplikacione End-Of Life. Ky sistem nuk bëhet pjesë e rrjetit. f. Nëse ka aplikacione të pa-patchuar duhet të njoftojë cdo një orë drejt përdoruesit dhe Administratorit të Rrjetit. Nëse ka dy patching të pa instaluara atëherë sistemi nuk mund të bëhet pjesë e rrjetit.	12 muaj	3 muaj

		g. Për sistemet e privilegjuara të kontrollohet Power Shelli. Nëse nuk është e nevojshme të c`aktivizohet pasi 70% e skripteve malinje përdorin karakteristikat e Power-Shell-it. h. Sistemi fundor duhet të ketë të bllokuara portat 25,110,135,137,138,139,444, si edhe rangen e portave 1024-49151 përveç rastit kur ndonjë portë në këtë range është e nevojshme pasi komunikon me shërbime të përcaktuara). Për sistemet operative Windows mund të përdoret teknika e update-t automatik të quajtur WSUS.		
12	Të izolohen logjikisht, (në VLAN-e të ndryshëm) Database dhe Web service-t (nëse janë të hostuara në ambientin tuaj).	Web Serveri është publik dhe ofron akses për këdo. Në rastin kur keni të hostuar Web Serverin në ambjentin lokal ajo duhet që: 1- Të jetë e ndarë në segmente të ndryshme me anë të teknikës VLAN 2- Të jetë në të njëjtin ambjent por me rregulla strikte duke përcaktuar a. Vetëm IP-në e Web Serverit për të komunikuar. b. Duke bërë reverse path forward drejt Web Serverit për të vërtetuar prezencën e tij. c. Filtrim të kërkesave që dërgon sipas protokollit (SOAP apo REST API) me anë të shtimit të një Filtri midis Web Serverit dhe Data Bases, e cila mund të kryhet me anë të EDR ose një filtër tjetër në Layer 7	3 muaj	1 muaj
13	Të merren masa për ngritjen e DNS_SEC për të shmangur DNS_Amplification attack dhe DNS_Poisoning attack.	Nëse DNS Serveri është vendosur lokalisht në ambjentin e brendshëm të Institucionit, atëherë rekursiviteti i cdo kërkese të nisur nga DNS-	3 muaj	1 muaj

		ja e konfiguruar në kompjuterin e përdoruesit drejt DNS Serverit mund të kishte dy efekte: 1- DNS Poisoning attack – Ku kërkesat e nisur nga përdoruesi shkojnë drejt një serveri C2 (Command & Control) i menaxhuar nga një keqdashës. 2- DNS Amplification attack – Gjenerohen kërkesa fallco drejt DNS Serverit i cili gjeneron përgjigje pafund drejt klientit duke cuar ne mohimin e shërbimit apo DoS Attack.		
14	Të implementohet dhe testohet Disaster Recovery Site për shërbimet më të rëndësishme dhe kritike.	Disaster Recovery është një mundësi për të pasur një pjesë ose të gjitha shërbimet e ofruara nga Site Primar edhe në një vend tjetër në një lokacion tjetër i cili duhet të ketë një distancë të konsiderueshme nga site primare. Komunikimi midis Primary Site dhe Secondary Site mund të jetë live ose në menyrë periodike, kjo në varësi të vetë institucionit Site i dytë mund të jetë: Tier 1/2 □ Ku ekziston një vendodhje me disa shërbime kritike të ruajtura në servera të fikur (Cold Space). Informacioni në to duhet të hidhet në mënyrë periodike sipas politikave të backup-eve: a. Daily Incremental Dump – Nuk konsumon kohë pasi kopjon të dhënat më të fundit drejt Site Sekondar b. Weekly Differential Dump – Ruan të dhënat në bazë javore c. Full Physical Dump – Kjo lloj ruajtje në bazë të sasisë duhet të bëhet të paktën një herë në 6 muaj	18 muaj	12 muaj

		Teknikat duhet të jenë me karakteristikën Backup Lock Retention ose me Tape në formatin WORM (Write Only Read Many) për të shmangur Ransomware. Tier ¾ □ Shërbimet, së bashku me Pozicionet e punonjësve janë të përcaktuara në siten sekondar (Hot Space) Ndërkohë është e këshillueshme që cdo 6 muaj të bëhen Integrity Check Data, ku të dhënat e kopjuara të verifikohen për integritetin e tyre duke përdorur modelin e marrjes së kampioneve. Teknika Cold Space ka kosto të mbështetur në: a. Ngritjen e Serverave të nevojshëm për ngritjen e shërbimeve b. Instalimin e Shërbimeve kritike c. Instalimin e Licensave për Shërbimet kritike d. Ngritjen e Dhomës së Serverave (Tapeti Teknologjik/Sensorët anti zjarr/anti theft, Sistemi i ftohjes) e. Facilitete të tjera shtesë Teknika Hot Space ka kosto disa herë më të larta se Cold Space, pasi kërkon shërbimet të jenë në statusin: UP & Running dhe numri i tyre arrin të jetë thuajse i njëjtë me ato në Siten Primare. Kostot rriten akoma më shumë kur ngrihet TIER 4 pasi site sekondar është një kopje e sitet primare duke përfshirë dhe pozicionimin e punonjësve. Analizat e kostove kërkojnë një projekt të detajuar në varësi të numrit të shërbimeve/serverave/përdoruesve etj		

15	Të merren masa për zëvendësimin ose izolimin e sistemeve “End of Life” të instaluara në pajisjet tuaja.	Kjo masë ndahet në dy nën çështje: 1- Sistemet Operative EOL të instaluara në Servera 2- Sistemet Operative EOL të instaluara në përdoruesit fundorë Për secilën ekzistojnë dy zgjidhje të shkallëzuara: I. Të gjithë sistemet operative EOL duhet të izolohen në VLAN/VLAN-e të përcaktuara (Të ndryshëm nga ai Default). Pavarësisht se kur ato ndodhen ato duhet të jenë të izoluar me pjesën tjetër të rrjetit. Me izolim nënkuptohet segmentimi i rrjetit posacërisht që këto pajisje/sisteme EOL të mos impaktojnë edhe pjesën tjetër të infrastrukturës. a. Nëse identifikohen < 10 Sisteme = 1 javë b. Nëse identifikohen 11-50 Sisteme = 2 javë c. Nëse identifikohen 51-75 Sisteme = 3 javë d. Nëse identifikohen 76-100 Sisteme = 1 muaj e. Nëse identifikohen >100 Sisteme = 2 muaj Nëse operatori ka vetëm shërbime të rëndësishme, të gjitha pikat nga a-e kanë një interval kohe për tu përmbushur nga operatori ekonomik, 2 herë më të gjatë se ato kritike të pasqyruara në pikat a-e II. Të gjithë sistemet EOL duhet të zëvendësohen me sisteme të rinj. Në raste kur ato janë CORE Business, dhe përbën një sfidë të madhe zëvëndesimi i tyre, DUHET të fillojë menjëherë procesi i komunikimit/tenderimit/zhvillimit të këtyre sistemeve dhe duke vënë periodikisht (Çdo 1 muaj) në dijeni AKCESK për statusin e sistemit. Nëse i referohemi vetëm sistemeve operative të hosteve (jo serverave) EOL duhet qe:	2 javë – 4 muaj (Izolimi i sistemeve EOL të fundoreve në varësi të numrit të Sistemeve). 6-16 muaj (zëvendësimi i sistemeve EOL për Sisteme Core). 2-16 muaj (Upgrade i firmware-t) 2 vite (zëvendesimi i Firmware) Vini re: Sistemet presupozon një Sistem Operativ, apo aplikacione të instaluara.	1 javë – 2 muaj (Izolimi i sistemeve EOL të fundoreve në varësi të numrit të Sistemeve). 3-8 muaj (zëvendësimi i sistemeve EOL për Sisteme Core). 1-8 muaj (Upgrade i firmware-t) 1 vit (zëvëndesimi i Firmware) Vini re: Sistemet presupozon një Sistem Operativ, apo aplikacione të instaluara.

		a. Nëse identifikohen < 10 Sisteme = 3 muaj b. Nëse identifikohen 11-50 Sisteme = 4 muaj c. Nëse identifikohen 51-75 Sisteme = 5 muaj d. Nëse identifikohen 76-100 Sisteme = 6 muaj e. Nëse identifikohen > 101 Sisteme = 8 muaj Nëse operatori ka vetëm shërbime të rëndësishme, të gjitha pikat nga a-e kanë një interval kohe për t'u përmbushur nga operatori ekonomik, 2 herë me të gjatë se ato kritike të pasqyruara në pikat a-e Vini re që një tjetër element EOL janë pajisjet Hardware të cilat kanë firmware shumë të vjetër dhe me shumë vulnerabilitet. Këto lloj platformash janë ato që kanë kaluar më shumë se 5 vjet. Në këtë lloj platformash duhet: Të identifikohen dhe të upgradohet firmware-t e tyre a. Nëse identifikohen < 50 Hardware = 1 muaj b. Nëse identifikohen 51-100 Hardware = 2 muaj c. Nëse identifikohen 101-200 Hardware = 3 muaj d. Nëse identifikohen 201-400 Hardware = 4 muaj e. Nëse identifikohen 401-600 Hardware = 6 muaj f. Nëse identifikohen >600 Hardware = 8 muaj Nëse operatori ka vetëm shërbime të rëndësishme, të gjitha pikat nga a-e kanë një interval kohe për t'u përmbushur nga operatori ekonomik, 2 herë me të gjatë se ato kritike të pasqyruara në pikat a-e		

		Në rastin kur është e pamundur, të bëhet zëvendësimi i tyre me platforma (pajisje) të reja, për infrastrukturat kritike koha e nevojshme = 1vit Për infrastrukturat e rëndësishme kjo kohë është 2 here më e gjatë. Kostot për pikat 1 dhe 2 varen nga: a. Numri i sistemeve EOL të pajisjeve fundore të përdoruesve, të shoqëruara me aplikacionet që janë instaluar në të (Licensat janë pjesë e tyre). b. Numri i sistemeve EOL në serverat. Këtu situata është më e komplikuar pasi nëse serverat janë të lidhura me një Data Bazë, mund të kërkohet të llogaritet edhe zëvendësimi i Data Bazës nëse ajo nuk ndërvepron me një sistem të ri (Perfshihen edhe Licensat). c. Numri i Pajisjeve hardware Core apo Fundorë të cilat do të zëvendësoheshin në varësi edhe të brandit që ato do t'i përkisnin.		
16	Të merren masa për identifikimin dhe menaxhimin efektiv të aseteve dhe të realizohet vlerësimi i risqeve duke evidentuar: -Vjetërsisë -Afektimin e C/I/A (Konfidencialitetit/Integritetit/Disponueshmërisë -Vulnerabilitetet e identifikuara (CVE)	Me anë të kësaj mase kërkohet një menaxhim i aseteve të institucionit. Asetet duhet të klasifikohen në ato asete që kanë të bëjnë me të dhënat të ndara në tre kategori: 1- Data at Rest – Storage, HDD, SAN, NAS, SDD, USB, etj. 2- Data in Transit – Pajisjet Core Network si: Switche L2, L3, Routera, Firewall, Bridge 3- Data Use – Të gjitha Shërbimet dhe Sistemet e ngritura	6 muaj	3 muaj

		Formati i inventarit të aseteve mund të jetë në formën: Emri_Asetit/ Përshkrimi_Asetit/ Kë prek aseti (C,I apo A)/ Vjetërsia/Kodi_Unik/Risku Këto asete mund të ruhen në një format Excel/Word ose me anë të një programi specifik. Kjo e fundit do të jepte më shumë fleksibilitet dhe eficensë kohore, sidomos në momentin fillestar të ndërtimit të tabeles së aseteve. • Të gjitha asetet që prekin konfidencialitetin janë ato që si pasojë e korruptimit mund të shkelet konfidencialiteti i të dhënave në to si psh: Active Directory, IAM appliance, psh ISE, LDAP Server në Linux, RADIUS Server etj • Të gjitha asetet që prekin integritetin e të dhënave janë ato që si pasojë e rrezikut që mund të shfaqen mund të korruptojnë të dhënat e transmetuara si psh: Pajisjet që janë ngritur IPSEC VPN Site (Firewall-et) • Të gjitha asetet që ofrojnë shërbime vetëm në një pikë të vetme prekin Disponueshmërinë (Shiko kërkesën 2)		
17	Të hartohen plane dhe procedura të detajuara për menaxhimin e incidenteve kibernetike.	Incidentet Kibernetike në institucion duhet të shoqërohen: 1- Politika e Incidenteve e cila kontrollohet minimumi 1 herë në vit 2- Procedurat dhe Rekordet e Incidenteve të ndodhura Rekordi i incidentit duhet të jetë në formatin:	3 muaj	1 muaj

		Emri i Incidentit/ Aseti i prekur/Koha/Kohëzgjatja/Personi që e zbuloi/ Personat që u raportuan/Shkaku i incidentit/ Risku i prekur/ Kontrollet për përmirësimin e situatës/ Rivlerësimi i riskut pas zgjidhjes/Komentet Plani i incidenteve kibernetike është mbështetur në standartin ISO, Aneksi A16. AKCESK nga ana e tij po e ripërtërin planin e incidenteve kibernetike ekzistuese deri në krizën kibernetike, Për këtë arsye të gjitha infrastrukturat kritike do të vihen në dijeni së shpejti.		
18	Të merren masa për izolimin e rrjetit wireless nga pjesa tjetër e rrjetit.	Nëse keni një rrjet Wireless ai duhet që: 1- Të jetë i izoluar nga rrjeti i brendshëm i institucionit me Air GAP ose përmes segmentimit duke përdorur PrivateVLAN. 2- Authentikimi i tij të jetë përmes teknikes RADIUS/TACACS	12 muaj	3 muaj
19	Të realizohen fushata ndërgjegjësimi të punonjësve në lidhje me sigurinë kibernetike dhe sulmet më të shpeshta si Phishing etj.	Ndërgjegjësimi duhet të mbeshtetet rreth higjenës kibernetike. Punonjësit duhet të ndërgjegjësohen në grupe të vogla nga stafi i sigurisë së informacionit në menyrë periodike (të paktën mujore) Të mbahen shënime mbi performancën e cdo punonjësi dhe të vlerësohen. Disa nga temat mund të jenë si më poshtë: • Kujdesi nga Phishing/Smishing/Vishing/Whaling/Spear Phishing attack • Kujdesi nga Screen policy – Largimi duke kycur monitorin • Kujdesi nga perdorimi i pajisjeve USB • Klasifikimi i dokumentacioneve • Rrjedhja e njoftimit të një incidenti sipas planit të shkruar në pikën 17	6 muaj	3 muaj

		• Vendosja e passwordeve të gjatë dhe jo të lidhur me emra specifik • Kujdesi nga Social Engineering, etj.		
20	Të kryhen testime për vlerësimin e sigurisë së aplikacioneve dhe rrjeteve (penetration test) dhe të hartohet plani për trajtimin e problematikave të evidentuara.	Penetration testing për institucionin duhet të kryhet nga një palë e tretë në dy faza: 1- Black Box Penetration Testing – 1 herë në 6 muaj 2- Full White Box Penetration Testing – 1 herë në vit Ky lloj testimi duhet të bëhet për të gjitha shërbimet që ofron institucioni. Në rastin e shërbimeve të hostuara nga palë të treta, por që nuk ofrohen nga institucioni duhet të kryhet vetem testimi External Black Box, por më parë duke njoftuar institucionin që ka hostuar këtë shërbim. Nëse shrbimi i hostuar nga një palë e tretë komunikon me shërbime të tjera të vetë institucionit atëherë kjo palë e tretë është e detyruar të ndjekë pikat 1 dhe 2 dhe kostot sipas marrëveshjes mund të mbulohen nga: 1- Pala e tretë 2- Vetë Institucioni Kostot e penetration testing varen nga: 1- Fusha e Skanimit 2- Modeli i Penetration Testing: Black Box, Gray Box, White Box 3- Numri i shërbimeve që do të testohen 4- Lloji i sherbimit (Phishing/Exploit/Social Engineering, etj).	12 muaj	6 muaj

21	Të kryhen kontrolle/audite të brendshme ose nga palët e treta për sigurinë e informacionit në infrastrukturat tuaja.	Auditi ka të bëjë me verifikimin e procedurave metodike dhe teknike në institucionin tuaj. Kontrollet përcaktojnë sa është aktiviteti juaj në përputhje me standartet e sigurisë si ISO 27001, apo NIST. Auditi mund të kryhet: 1- Nga vetë brenda institucionit i quajtur Audit i Brendshëm (Forma e Thjeshtë). 2- Nga një palë e tretë e shoqëruar me një certifikatë (Forma e Avancuar)	12 muaj	6 muaj
22	Të kontrollohet nëse sistemi I Email-it nuk ka të konfiguruar featurat anti-spoofing: DMARC/SPF/DKIM	Për të shmangur mundesinë që të pranohen email-e phishing është e domosdoshme të jetë të konfiguruara në email të tre featurat.	6 muaj	3 muaj
23	Të kontrollohen nëse ka Web Service që operon në protokollin http	Nëse një faqe është me protokoll http ajo është shumë kollaj e përgjueshme pasi transmeton informacion tekst. E njëjta gjë është kur faqja është me certificatë të skaduar. Gjithashtu web servicet duhet të jenë të konfiguruara që të mos kenë mundësi për sulme OWASP-10 si psh: http_flag=1, sesioni I gjenerimit të faqeve të jetë dinamik, të ketë kufizim në numrin e karaktereve dhe llojin e tyre në format hyrëse etj.	3 muaj	1 muaj
24	Të kontrollohen nëse në firewall ka të ngritur White List të adresave të lejuara IP	Duke pasur të ngritur White List do të mundësohej që të lejoheshin vetëm ai grup IP-sh që I përket institucioneve/shteteve që priten dhe të eleminohet cdo kërkesë tjetër.	6 muaj	3 muaj
25	Të përdoret politika e passwordeve rastësore për userat/administratoret local (Psh si LAPS të Microsoft)	Politika e passwordeve në rastin e logimit si përdorues local duhet të gjenerohet random dhe të përdoret vetëm një herë Brenda një intervali të caktuar. Gjithashtu në rastin kur një faqe nuk përdoret për një kohë (idle time) të kalohet në password automatikisht – Screening Policy	3 muaj	1 muaj
26	Të përdoret platforma Data Leakage Prevention për parandalimin e rrjedhjes së informacionit.	Platforma DLP do të shmangte rrjedhjen e informacionit të klasifikuar drejt personave apo siteve të pa-autorizuar, pasi do të tag-ohesh cdo trafik dhe person që e përdor atë informacion	12 muaj	6 muaj

27	Të përdoret teknika e mbrojtjes nda DoS/DDoS attack	Kjo do të shmangë mundësinë e sulmeve DoS/DDoS drejt një institucioni pasi sapo të shikohej një gjë e tillë trafiku, do të analizohej dhe do të shmangej trafiku I gjeneruar random. Shfrytëzimi I AI do të ulte numrin e False-Positive	12 muaj	6 muaj
28	Të përdoret teknika e Port Security te Switch-et ku numri maksimal I MAC Adresave të jetë 1 për përdoruesit e thjeshtë dhe një numër I limituar për ekspertët e IT-së ose Sigurisë Kibernetike.	Kjo do të eleminonte mundesinë e sulmeve DoS nga Brenda institucionit ose dhe mundesinë e lidhjes së pa-autorizuar të një perdoruesi Brenda LAN-it të vetë operatorit ekonomik.	3 muaj	1 muaj