DIGI- JA VÄESTÖTIETO-VIRASTO

Digiturvan hallinnollinen kokonaiskuva julkisessa hallinnossa vuonna 2026

Raportti ja keskeiset havainnot

28.5.2026

Puh. **0295 536 000** (vaihde) | Yhteystiedot, katso **www.dvv.fi**

Sisällysluettelo

Digiturvan kokonaiskuvapalvelu

Digi- ja väestötietoviraston (jäljempänä DVV) tehtävänä on edistää julkisen hallinnon organisaatioiden tietoturvallisuuden, sekä laajemmin digitaalisen turvallisuuden, kehittämistä. Osana tätä tehtävää se vastaa Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI), kolmen VAHTI-asiantuntijaryhmän sekä valtionhallinnon tietoturvavastaavien verkoston toiminnasta. Tässä toiminnassa on mukana lähes 700 johdon edustajaa ja alan asiantuntijaa.

VAHTI-johtoryhmä on koonnut tietoa valtionhallinnon tietoturvallisuudesta jo 2000-luvun alusta alkaen, ja vuodesta 2017 tietoa on kerätty laajemmin koko julkisen hallinnon tietoturvallisuudesta. Vuodesta 2019 lähtien on koottu ja tarkasteltu hallinnollisen digitaalisen turvallisuuden tilannetietoa. Kyselyiden avulla on voitu selvittää muun muassa, miten lainsäädäntö, kuten tietoturvallisuusasetus vuonna 2010, EU:n yleinen tietosuoja-asetus vuonna 2018 sekä tiedonhallintalaki vuonna 2020 ovat vaikuttaneet organisaatioiden digitaalisen turvallisuuden osa-alueiden kehittymiseen.

Kyselytuloksia on hyödynnetty Julkisen hallinnon digitaalisen turvallisuuden kehittämistoimenpiteiden, VAHTI-työryhmien toiminnan ja tehtävien suunnittelussa, Taistoharjoituksen suunnittelussa ja Digiturvan tietopankin kehittämisessä. Jatkossa digiturvan kokonaiskuvapalvelulla voidaan seurata myös 2025 voimaan tulleen kyberturvallisuuslain vaikutuksia julkisenhallinnon kyber- ja digiturvallisuuden kehittymiseen.

Digiturvan kokonaiskuvapalvelun tuloksia hyödynnetään myös kansallisen kyberturvallisuusstrategian ja sen toimeenpanosuunnitelman seurantaan julkisen hallinnon osalta.

Digiturvan kokonaiskuvapalvelu on toteutettu saman sisältöisenä vuosina 2021–2024. Vuonna 2022 otettiin käyttöön DVV:n kehittämä verkkopalvelu, jonka avulla julkisen hallinnon organisaatioille voidaan tarjota niiden omasta digiturvatilanteesta ajantasainen tilannekuva jatkuvaan käyttöön tarkoitetulla kokonaiskuvapalvelulla sekä vertailutietoa muuhun julkiseen hallintoon. Vuonna 2024 digiturvan kokonaiskuvapalvelua kehitettiin DVV:n toteuttamassa Loisto-hankkeessa. Loisto-hankkeessa kysymyksen asettelua ja kysymyksiä päivitettiin hieman sekä päivitettiin vastausvaihtoehtoja. Muutokset toteutettiin niin, että vuonna 2025 kerätty data on vertailukelpoista aiempien vuosien kanssa. 2025 näitä kehitystoimenpiteitä jatkettiin ja tuotettiin mm. tukimateriaalia kyber- ja digiturvan resurssien tunnistamiseen, raportointiin ja kehittämiseen.

Lisätietoja kokonaiskuvapalvelusta antaa:

Erityisasiantuntija Tapani Rinne, puh. 0295 537 266, tapani.rinne@dvv.fi

Vuoden 2026 Digiturvabarometrin tulosten yhteenveto

Digiturvan kokonaiskuvapalvelun ohella DVV on toteuttanut Henkilöstön ja kansalaisten Digiturvabarometria syyskuusta 2020 alkaen. Digiturvan kokonaiskuvapalvelun avulla seurataan, miten organisaatioiden hallinnollinen digiturvallisuus kehittyy. Digiturvabarometrin avulla kartoitetaan digitaaliseen toimintaympäristöön liittyvää henkilöstön osaamista, koulutustarpeita, toteutuneita uhkia sekä luottamusta digimaailman toimijoihin ja palveluihin. Digi- ja väestötietoviraston kyselyyn vastasi 1250 täysi-ikäistä suomalaista heinä-elokuussa 2025.

6.10.2025 julkaistun Digi- ja väestötietoviraston Digiturvabarometrin mukaan suomalaisten luottamus digipalveluiden ja -laitteiden turvallisuuteen on heikentynyt edelleen. Erityisesti kyberhyökkäykset ja digihuijaukset koetaan merkittäviksi uhiksi. Tekoälyjen nopea kehitys ja niiden kyky käsitellä henkilötietoja herättävät huolta.

Suomalaisten luottamus viranomaisiin, finanssialan toimijoihin ja omaan työnantajaan on pysynyt korkeana

Tulosten mukaan 38 % vastaajista kokee luottamuksensa digiturvaan heikentyneen, kun taas yli puolella (51 %) luottamus on säilynyt ennallaan. Vain 11 % kertoo luottamuksen vahvistuneen.

Suomalaiset kokevat digimaailman edelleen melko turvalliseksi. 91 % kokee osaavansa käyttää digitaalisia laitteita ja -palveluja turvallisesti ja 82 % tuntee olonsa vähintään melko turvalliseksi.

Tekoälyn käyttö on yleistynyt nopeasti. Joka kymmenes suomalainen käyttää tekoälyä päivittäin. Samalla luottamus tekoälyn turvallisuuteen on hieman laskenut: vain 20 % uskoo sen käsittelevän henkilötietoja turvallisesti. Eniten tekoälyyn luottavat nuoret (26 %), vähiten yli 65-vuotiaat (14 %).

Vuoden 2025 Digiturvabarometrissa kysyttiin ensimmäistä kertaa suhtautumista kyberuhkiin. Kyberuhat huolettavat laajasti: 60 % suomalaisista on melko tai erittäin huolissaan yhteiskuntaan kohdistuvista kyberhyökkäyksistä ja digihuijauksista. Silti vastaajista 51 % uskoo, että Suomi on varautunut niiden torjuntaan hyvin. Kaksi kolmesta arvioi digiturvan olevan paremmalla tasolla Suomessa kuin muissa EU-maissa.

Vaikka tutkimuksessa nousi esille huolia, luottamus viranomaisiin, finanssialaan ja omaan työnantajaan on säilynyt korkeana. Viranomaisiin luottaa 87 %, työantajaan 82 %, oppilaitoksiin 71 % ja finanssialaan 87 %.

Luottamus on edelliseen, vuoden 2024 tutkimukseen, verrattuna kauttaaltaan pienessä laskussa. Poikkeuksena luottamus kotimaisiin verkkokauppoihin on noussut kaksi prosenttiyksikköä 75 prosenttiin. Ulkomaisiin verkkokauppoihin vastaajista luottaa vain 23 %.

Lisätietoja vuoden 2025 Digiturvabarometristä löydät täältä: Digiturvabarometri 2025. Vuoden 2026 digiturvabarometrin tulokset julkaistaan syyskuussa 2026.

1 Johdon tiivistelmä

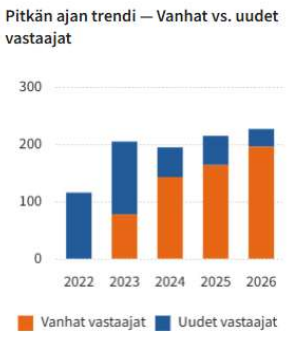
Digi- ja väestötietovirasto toteutti helmi-maaliskuussa 2026 Digiturvan kokonaiskuvapalvelun kampanjan, johon saatiin 209 vastausta julkisen hallinnon organisaatioilta. Saman sisältöinen kysely on tehty myös vuosina 2021, 2022, 2023, 2024 ja 2025; vastanneet organisaatiot tosin vaihtelevat vuosittain.

- Vuonna 2021 kampanjaan vastasi 121 organisaatiota
- Vuonna 2022 kampanjaan vastasi 118 organisaatiota
- Vuonna 2023 kampanjaan vastasi 203 organisaatiota
- Vuonna 2024 kampanjaan vastasi 185 organisaatiota
- Vuonna 2025 kampanjaan vastasi 203 organisaatiota
- Vuonna 2026 kampanjaan vastasi 209 organisaatiota

Yhteensä palveluun on vastannut 400 eri organisaatiota. Vuoden 2023 hyvinvointialueiden uudistus ja eri vuosina tapahtuneet kuntayhdistymiset, Lupa- ja valvontaviraston perustaminen vuoden 2026 alusta ovat jonkin verran vaikuttaneet organisaatioiden määrään, jotka voivat vastata palveluun.

Vastanneiden määrää on viime vuosina vakiintunut n. 200 organisaatioon. Vastaajaorganisaatioissa tapahtuu kuitenkin jonkin verran vaihtelua. Esim. vuoden 2025 kampanjaan vastasi 40 uutta organisaatiota ja vuoden 2026 kampanjassa 31 uutta organisaatiota. Mahdollisia vastaajaorganisaatioita julkishallinnossa on n. 700.

Vastaajaorganisaatioiden trendit:



Vastaajaorganisaatioiden trendiluvuista on tunnistettavissa, että Digiturvan kokonaiskuvapalvelu ei ole kaikille organisaatiolle vakiintunut osaksi vuosikelloa.

Kerätyn tiedon luotettavuutta ja vertailtavuutta saadaan parannettua sitä mukaa kun uusien vastaajien määrä lisääntyy. Toivomme, että yhä useampi julkisen hallinnon organisaatio ottaisi nämä kokonaiskuvan raportointipalvelut omaan käyttöönsä ja kytkisi ne osaksi organisaation digiturvan hallintaa ja säännöllistä johdon raportointia.

1.1 Digitaalisen turvallisuuden osa-alueissa tapahtunut kehittyminen

Digiturvan kokonaiskuvapalvelu kattaa kaikki digitaalisen turvallisuuden osa-alueet;

- digiturvan johtamisen,
- riskienhallinnan,
- toiminnan jatkuvuuden ja varautumisen,
- tietoturvan,
- tietosuojan ja
- kyberturvallisuuden

Kaikkien osa-alueiden tasapainoista kehittämistä tarvitaan digitaalisen ja fyysisen toimintaympäristön suojaamiseksi.

Tulosten perusteella voidaan todeta, että organisaatioiden hallinnollinen turvallisuus on kokonaisuudessaan kehittynyt parempaan suuntaan vuosina 2021–2026. Sen sijaan yksittäisissä osa-alueissa ja tehtävissä on tapahtunut merkittävää vaihtelua. Erityisesti kyberturvallisuuden osa-alue on kehittynyt positiivisesti vuosien 2023 – 2026 vastausten perusteella.

Koska digitaalisen turvallisuuden kehittämiseen on rajallinen määrä henkilöresursseja ja rahaa, organisaatiot joutuvat priorisoimaan kehittämistoimiaan. Keskimäärin resurssien määrää pidettiin liian pienenä. Reaalimaailman ilmiöt kuten koronaviruspandemia, Venäjän hyökkäyssota ja globaalin maailmantilanteen kiristyminen ja konfliktit näkyvät kehittämistoimien priorisoinneissa.

Vuonna 2022 oli nähtävissä, että organisaatiot panostivat jonkin verran enemmän riskienhallintaan ja jatkuvuuden hallintaan, kun taas vuonna 2025 parantumista on nähtävissä kaikilla muilla osa-alueilla paitsi riskienhallinnassa. Resurssien puutteen vuoksi valitettavasti kaikkiin osa-alueisiin ei aina pystytä panostamaan. Resurssien puutteellisuuden vuoksi kehitys digiturvassa on maltillista. On kuitenkin syytä huomioida, että 0,01 parannus osa-alueen tulokseen on merkityksellinen. Tuloksen paraneminen muodostuu koko osa-alueen kysymyksistä ja yli 200 organisaation vastausten keskiarvosta. Yksittäisten lukuarvojen sijaan lukuarvojen trendi on siksi merkityksellisempi, kun arvioidaan kansallisesti julkisen hallinnon kyber- ja digiturvan kehittymistä.

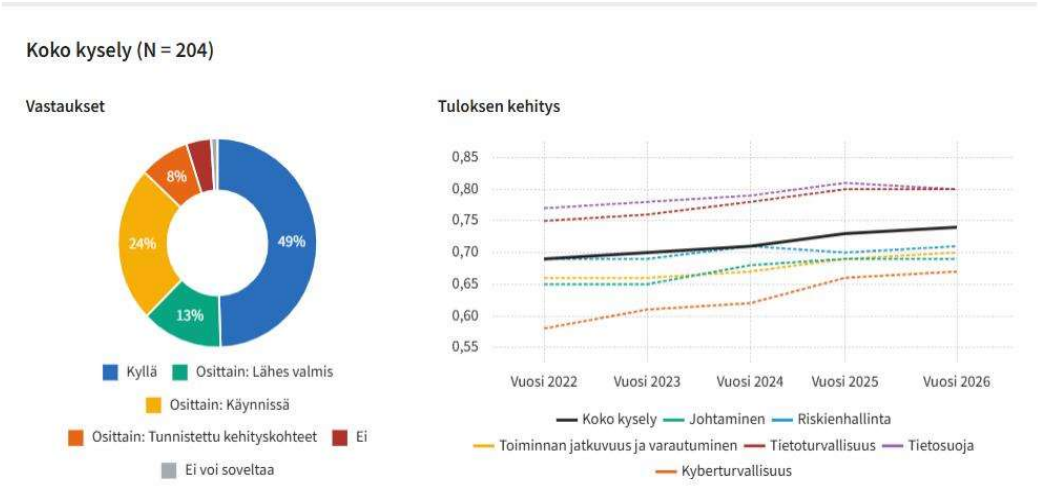
2026 tulosten perusteella maltillinen kehitys jatkui edelleen riskienhallinnan, toiminnan jatkuvuuden ja varautumisen sekä kyberturvallisuuden osa-alueilla. Laskua tapahtui tietosuojan osa-alueella. Johtamisen ja tietoturvallisuuden osa-alueilla tulos pysyi samalla tasolla kuin 2025 kyselyn tuloksissa.

Alla olevassa taulukossa ovat vuosien 2021–2026 vastausten keskiarvot osa-alueittain. Mitä lähempänä arvoa 1, sitä paremmin organisaatiot ovat arvioineet suoriutuneensa kyselyssä esitetyissä väittämissä.

	2026	2025	2024	2023	2022	2021
Koko kysely	0,74	0,73	0,71	0,70	0,69	0,71
Johtaminen	0,69	0,69	0,68	0,65	0,65	0,65
Riskienhallinta	0,71	0,70	0,71	0,68	0,70	0,68
Toiminnan jatkuvuus ja varautuminen	0,70	0,69	0,67	0,66	0,67	0,67
Tietoturvallisuus	0,80	0,80	0,78	0,75	0,75	0,78
Tietosuoja	0,80	0,81	0,79	0,78	0,77	0,81
Kyberturvallisuus	0,67	0,65	0,62	0,61	0,59	0,59

Taulukko 1. Digiturvakyselyn eri osioiden keskiarvot

Alla olevassa kuvassa sama tulos kuvattuna kaaviona sekä vastausten jakautuminen prosentteina. Lähes puolet kaikista annetuista vastauksista on Kyllä; Olemme toteuttaneet tarvittavat toimenpiteet riittävälle tasolle. Seuraavaksi eniten on vastauksia luokassa osittain: käynnissä. Lisätietoa vastausvaihtoehdoista löytyy luvusta 2.1. Osa-alueiden keskiarvot.



Kuva 1 kokonaiskuvapalvelun vastausten jakautuminen prosentteina sekä digitaalisen turvallisuuden kokonaiskuvapalvelun tuloksen kehitys, koko kysely ja digiturvan osa-alueet

1.2 Toimintaympäristön muutokset ja niiden vaikutus

Edellinen vastaavanlainen raportti Digiturvan kokonaiskuvapalvelusta tuotettiin keväällä 2025. Silloin tuloksista oli nähtävissä kyber- ja digiturvan kehityksen maltillinen kehittyminen parempaan. Kehitys on vuoden 2026 perusteella hieman hidastunut. Merkittävää on mm. tietosuojan lasku, joka on edellisen kerran tapahtunut 2022 vuoden tuloksissa. Tietosuojassa tulosten laskua selittää todennäköisesti globaalit geopoliittiset ilmiöt, jotka ovat aiheuttaneet epävakautta digitaalisessa maailmassa. Esim. henkilötietosiirtojen edellytyksissä kolmansiin maihin tulosten keskiarvoissa oli merkittävää laskua.

Kyselykierros tehtiin myös kesällä 2024. Tuloksista ei kuitenkaan tuotettu laajaa raporttia, vaan tuloksia esiteltiin DVV:n tilaisuuksissa. Silloin tuloksissa oli nähtävissä muuttuneen maailmantilanteen vaikutus. Venäjän hyökkäyssodan seurauksena organisaatioissa alettiin kiinnittää enemmän huomiota riskitilanteen seurantaan, riskien arviointiin ja niiden raportointiin johdolle. Lisäksi varautuminen ja harjoittelu oli lisääntynyt ja tietoturvallisuuteen budjetoitu raha lisääntynyt jonkin verran.

Vuonna 2025 Venäjän hyökkäyssota jatkuu edelleen ja Suomessakin on havaittu lisääntyneitä verkkohyökkäyksiä ja kielteistä verkkovaikuttamista. Kyselyn tuloksista on havaittavissa, että kyberturvallisuuden osa-alueella on tapahtunut selvää parantumista. Sen tulokset ovat edelleen osa-alueista heikoimmalla tasolla, mutta globaalin tilanteen kehittyminen pakottanee kiinnittämään siihen lisää huomiota myös jatkossa.

Kansainvälisesti verkkorikollisuus ja kansalaisiin kohdistuvat digihuijaukset ovat jatkaneet kasvua, mutta se ei tämän kyselyn perusteella ainakaan merkittävästi näy organisaatioiden kokemien verkkohyökkäysten määrässä.

2026 tuloksissa näkyy maailman poliittisen tilanteen epävakauden jatkuminen. Näitä ovat mm. konfliktit ympäri maailmaa ja Euroopan sekä Yhdysvaltojen kiristyneet välit sekä luottamus kansainväliseen oikeuteen. Lisäksi tekoälyn hyödyntäminen verkkorikollisuudessa, toimitusketjujen hallinta ja kvanttivarautuminen huolestuttavat. 2027 kampanjaan mennessä kokonaiskuvapalveluun tullaan lisäämään uusi kokonaisuus, jonka avulla tullaan seuraamaan toimitusketjuihin liittyvää riskienhallintaa ja kvanttivarautumisen edistymistä.

1.3 Kyberturvallisuuslain ja tiedonhallintalain 4a luvun vaikutukset

NIS2 -direktiivin mukaiset velvoitteet tulivat voimaan 8.4.2025. Kyberturvallisuusdirektiivin tavoitteena on vahvistaa sekä EU:n yhteistä että jäsenvaltioiden kansallista kyberturvallisuuden tasoa useiden yhteiskunnan toiminnan kannalta kriittisten toimialojen osalta. NIS 2 -direktiivi korvaa aiemman EU:n verkko- ja tietoturvadirektiivin (NIS-direktiivi), jolla on säädetty tiettyihin toimialoihin kohdistuvista kyberturvallisuusvelvoitteista. NIS 2 direktiivin pohjalta säädettiin kansallinen kyberturvallisuuslaki (124/2025) sekä tehtiin muutoksia lakiin julkisen hallinnon tiedonhallinnasta (906/2019)

Kyberturvallisuuslaki ja tiedonhallintalain luku 4a asettavat tietyille organisaatioille uusia velvoitteita muun muassa kyberturvallisuutta koskevien riskien hallintaan ja poikkeamista raportointiin.

Koska digiturvan kokonaiskuvapalvelu tarkastelee myös riskienhallinnan, poikkeamien havainnoinnin ja kyberturvallisuuden osa-alueita, voidaan tulevien vuosien tarkastelussa seurata myös uuden lainsäädännön vaikutuksia lain soveltamisalan ja yleisemminkin vastaajaorganisaatioiden arvioihin vuosittaisten muutosten ja kehittymistrendien avulla.

NIS2 sääntelyn vaikutukset näyttävät painottuneen enemmän 2025 vuoden tuloksiin organisaatioiden valmistautuessa NIS2 ja tiedonhallintalain 4a luvun tuomiin vaatimuksiin. Tuloksia tarkasteltaessa on kuitenkin huomioitava, että alle puolet vastaajista ovat NIS2 ja tiedonhallintalain 4a luvun vaikutuksen piirissä.

1.4 Keskeiset kehittämiskohteet

Tämä kyselyn tulokset painottuvat julkisen hallinnon organisaatioiden hallinnollisen digiturvan kokonaiskuvaan. Hallinnollisen turvallisuuden yhteinen kehittäminen on merkittävästi helpompaa kuin teknisen tietoturvallisuuden tai jatkuvuuden hallinnan kehittäminen. Hallinnollista digitaalista turvallisuutta voidaan kehittää esimerkiksi hankkeiden, työpajojen, tukimateriaalien sekä osaamisen kehittämisen tukivälineiden avulla. Sen sijaan teknisen tietoturvallisuuden ja jatkuvuuden hallinnan parantaminen vaativat organisaatiokohtaisia keinoja, johtuen käytössä olevista teknisistä järjestelmistä ja palveluista. Tästä huolimatta olemme nostaneet esille myös sellaisia tekniseen tietoturvallisuuteen ja jatkuvuuden hallintaan liittyviä toimenpiteitä, joita suosittelemme organisaatioiden tarkastavan ja ottavan käyttöön omassa ympäristössään.

Kaikki suositellut kehittämiskohteet on lueteltu kappaleissa 2.2.1–2.2.7.

2 Yhteenveto tuloksista

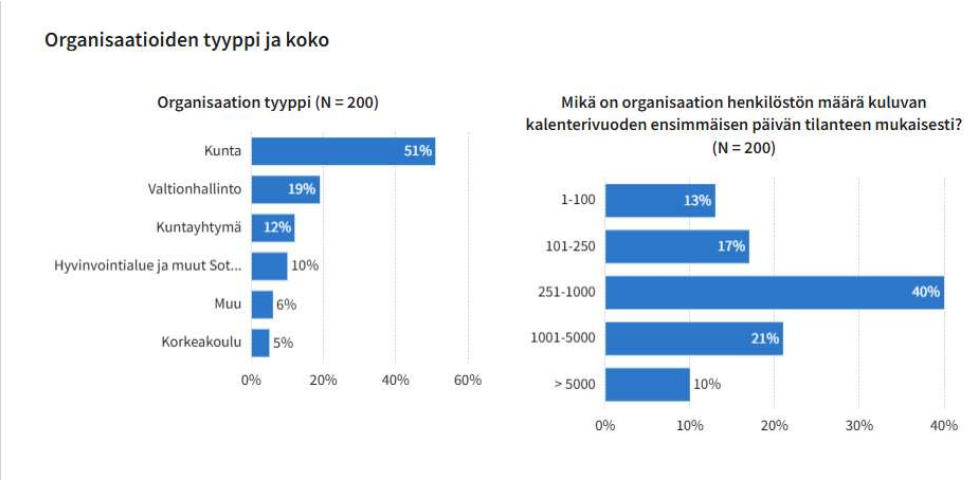
Tämä yhteenveto sisältää Digiturvan kokonaiskuvakyselyn eri osa-alueiden keskiarvotulokset, keskeiset toimiala- ja osa-aluekohtaiset havainnot sekä tulosten perusteella esille nostetut kehittämiskohteet.

Digiturvakyselyssä 2026 oli 24 taustakysymystä sekä 99 väittämää, joiden avulla kartoitettiin vastaajaorganisaatioiden digitaalisen turvallisuuden tilannekuvaa. Rakenteeltaan Digiturvakysely jakautui seuraaviin osa-alueisiin: taustatiedot, johtaminen, riskienhallinta, toiminnan jatkuvuus ja varautuminen, tietoturvallisuus, tietosuoja, kyberturvallisuus ja havainnointi. Alla oleviin kaavioihin ja taulukoihin on koottu osa-alue- ja väittämäkohtaiset keskiarvot.

Digiturvan kokonaiskuvapalvelusta ja sen tuloksista on hyvä huomioida, että kyseessä on organisaation itsearviotyökalu. Jokaisen organisaation vastaukset ovat organisaation itsensä tuottama arvio omasta tilanteesta ko. väittämän osalta. Organisaatioiden tulkinnat väittämistä ja arviot vastauksissa voivat vaihdella organisaatioiden välillä. Digiturvan kokonaiskuvapalvelua ei siis voida pitää absoluuttisena totuutena, auditointityökaluna eikä organisaation kypsyystason mittarina. Vastausten yhdenmukaisuutta on kehitetty tuottamalla VAHTI-hyvät käytännöt tukimateriaaleja, jotka löytyvät digiturvan tietopankista.

Alla olevassa kuvassa on nähtävissä vastaajaorganisaatioiden tyyppi ja koko. Noin puolet vastaajista on kuntia. Seuraavaksi eniten vastaajia on valtiohallinnosta. 100 – 1000 henkilön organisaatiot kattavat kaksi kolmasosaa vastaajista.

Kuva 2 vastaajaorganisaatioiden tyyppi ja koko



Tulosten vertailtavuutta häiritsee osaltaan vastaajaorganisaatioiden muutos. Näyttää siltä, että merkittävä osa vastaajaorganisaatioista eivät vastaa vuosittain kampanjan aikana, kun Digi- ja väestötietovirasto pyytää organisaatioita päivittämään tiedot. Alla olevassa kuvassa tuodaan esille tämä haaste. 85 organisaatiota ovat aikaisemmin vastanneet, mutta eivät ole viimeisen kahden vuoden aikana päivittänyt tietojaan.

Jonkin verran tätä tilastoa selittää muutoksen julkishallinnon organisoinnissa, kuten hyvinvointialueiden perustaminen, Lupa- ja valvontaviraston perustaminen yms.

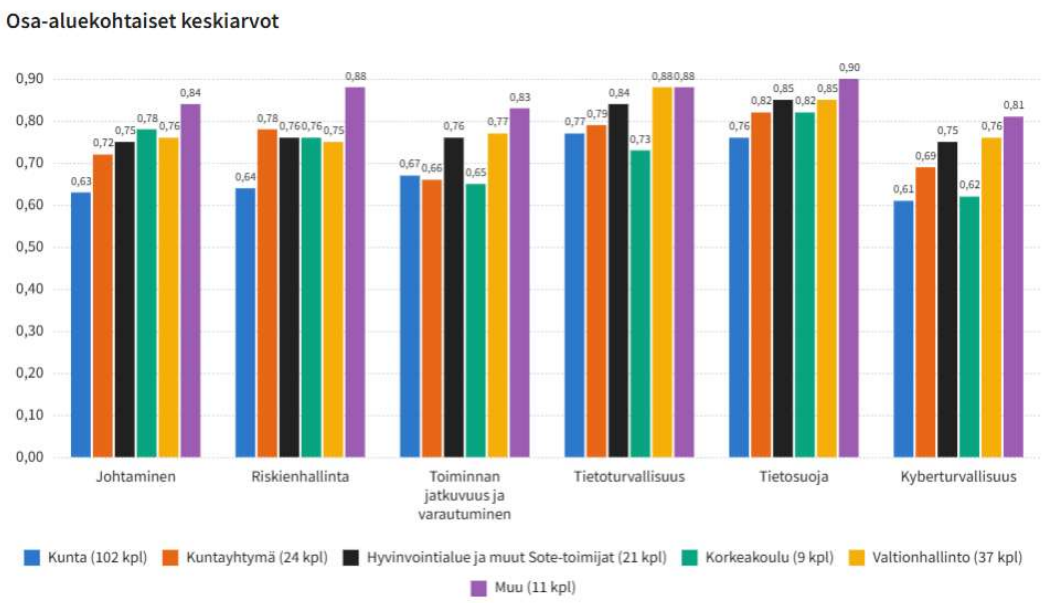
Uusia vastaajaorganisaatioita palveluun saadaan kuitenkin säännöllisesti. Vuonna 2025 uusia vastaajia oli peräti 51 organisaatiota ja vuoden 2026 kampanjassa 31 uutta organisaatiota. Raportin kirjoittamisen aikaan usealla organisaatiolla vastauksen lähettäminen oli vielä kesken.

Kuva 3 Pitkän ajan trendit vastaajaorganisaatioissa

2.1 Osa-alueiden keskiarvot

Kuvassa 1 esitetään Digiturvakyselyn eri osioiden (johtaminen, riskienhallinta, toiminnan jatkuvuus ja varautuminen, tietoturvallisuus, tietosuoja ja kyberturvallisuus) vastausten keskiarvot asteikolla 0–1. Organisaatiot vastasivat annettuihin väittämiin kuusiportaisella asteikolla ja vastaukset on pisteytetty seuraavasti:

- **Kyllä**; Olemme toteuttaneet tarvittavat toimenpiteet riittävälle tasolle. (**1,00**)
- **Osittain –** Lähes valmis; Olemme tehneet lähes kaikki tarvittavat toimenpiteet asian kehittämiseksi riittävälle tasolle. (**0,75**)
- **Osittain –** Käynnissä; Olemme määritelleet tavoitetason ja suunnitelleet tarvittavat toimenpiteet. (**0,50**)
- **Osittain –** Tunnistettu kehityskohteet; Olemme tunnistaneet, että asia on merkityksellinen organisaatiomme digiturvalle, mutta emme ole vielä aloittaneet toimenpiteitä. (**0,25**)
- **Ei**; Emme ole tunnistaneet toimenpiteitä, tai emme aio kehittää asiaa. (**0,00**)
- **Ei koske meitä**; Voimme osoittaa, että kysyttävä asia tai vaatimus ei koske meitä. (**ei huomioida keskiarvossa**)



Kuvio 1. Digiturvakyselyn eri osioiden keskiarvot vastaajaryhmittäin

Kuvion 1 tiedot on esitetty alla taulukkomuodossa (taulukko 1). Lisäksi taulukkoon on sisällytetty koko kyselyn toimialakohtaiset keskiarvot.

Taulukko 1. Digiturvakyselyn eri osioiden keskiarvot vastaajaryhmittäin (suluissa 2025 tulokset)

	Kaikki organisaatiot 204 kpl	**Kunta 102 kpl**	**Kuntayhtymä 24 kpl**	**Hyvinvointialue ja muut sote-toimijat 21 kpl**	**Korkeakoulu 9 kpl**	**Valtionhallinto 37 kpl**	**Muu 11 kpl**
Johtaminen	**0,69 (0,69)**	0,63 (0,61)	0,72 (0,71)	0,75 (0,75)	0,78 (0,69)	0,76 (0,77)	0,84 (0,84)
Riskienhallinta	**0,71 (0,70)**	0,64 (0,63)	0,78 (0,74)	0,76 (0,76)	0,76 (0,73)	0,75 (0,75)	0,88 (0,92)
Toiminnan jatkuvuus ja varautuminen	**0,70 (0,69)**	0,67 (0,65)	0,66 (0,68)	0,76 (0,73)	0,65 (0,62)	0,77 (0,74)	0,83 (0,83)
Tietoturvallisuus	**0,80 (0,80)**	0,77 (0,76)	0,79 (0,79)	0,84 (0,81)	0,73 (0,73)	0,88 (0,86)	0,88 (0,86)
Tietosuoja	**0,80 (0,81)**	0,76 (0,76)	0,82 (0,84)	0,85 (0,83)	0,82 (0,83)	0,85 (0,85)	0,90 (0,90)
Kyberturvallisuus	**0,67 (0,66)**	0,61 (0,58)	0,69 (0,69)	0,75 (0,72)	0,62 (0,61)	0,76 (0,74)	0,81 (0,79)
Keskiarvo	**0,74 (0,73)**	**0,69 (0,68)**	**0,74 (0,75)**	**0,79 (0,77)**	**0,73 (0,70)**	**0,80 (0,79)**	**0,86 (0,86)**

Korkeimmat vastauskeskiarvot saavutettiin tietosuojan ja tietoturvan (kaikkien vastausten keskiarvo 0,80) ja matalimmat kyberturvallisuuden (0,67) alueilla. Näiden ero on kuitenkin hiukan pienentynyt viime vuosina. Vuonna 2025 vastaavat luvut olivat 0,80 tietoturva ja 0,81 tietosuoja ja 0,66 kyberturva.

Huomionarvoista on, että kaikki osa-alueet ovat kehittyneet parempaan 2021–2026, huolimatta hetkellisistä laskuista tai vuoden 2026 tietosuojan keskiarvojen alenemisesta. Organisaatiotyyppien sisällä kehitys on ollut vielä voimakkaampaa.

Vastaajaryhmät on muodostettu kyselyyn osallistuneiden organisaatioiden (yht. 204 organisaatiota) toimialajaottelun perusteella, ja ne ovat seuraavat:

- kunta (102 vastaajaa),
- kuntayhtymä (24 vastaajaa),
- hyvinvointialue tai muu sote-toimija (21 vastaajaa),
- korkeakoulu (9 vastaajaa),
- valtionhallinto (37 vastaajaa),
- joku muu (11 vastaajaa).

Vastaajamäärissä eri organisaatiotyyppiluokissa tapahtuu vuosittain vaihtelua. Kaikki organisaatiot eivät vastaa säännöllisesti vuosittain. Tästä syystä eri vuosien keskiarvoja ei voida suoraan verrata toisiinsa. Julkisen hallinnon vastaajien määrää vähentää tekninen rajoite, joka toistaiseksi estää palvelun käytön Y-tunnuksettomilta organisaatioilta.

Kaikkien vastaajien osalta kyselyn keskiarvotulos on 0,74. Korkein toimialakohtainen keskiarvo on ryhmässä ”muut”, johon kuuluu mm. välillistä valtionhallintoa, kuten rahastoja, säätöitä ja laitoksia (0,86), jota seuraa valtionhallinto (0,80), hyvinvointialueet (0,79), kuntayhtymät (0,74), korkeakoulut (0,73), sekä kunnat (0,69).

2.2 Tilannekuva 2026

Digiturvan kokonaiskuva on kohtalaisella tasolla (keskiarvo 0,74) ja kehittyy hitaasti ylöspäin.

Perustason käytännöt ovat laajasti käytössä, mutta digiturva on monin paikoin epätasapainossa: hallinnollinen tietoturva suojaus ja sääntelyvelvoitteet ovat hallinnassa paremmin kuin johtaminen, varautuminen ja kybertoimintakyky.

2.2.1 Keskeiset havainnot koko julkishallinnon osalta

Vahvimmat osa-alueet

Tietoturva ja tietosuoja (0,80) ovat vakiintuneet koko kentässä.

Sääntely, ohjaus ja auditointivaatimukset näkyvät korkeana perustasona erityisesti valtionhallinnossa ja sote-toimijoilla.

Heikoimmat osa-alueet

Kyberturvallisuus (0,67) ja digiturvan johtaminen (0,69) jäävät jälkeen muista osa-alueista. Kyky havaita, torjua ja toipua kyberhäiriöistä on monissa organisaatioissa

rajallinen. Digiturva ei ole vielä systemaattinen osa strategista johtamista ja päätöksentekoa.

Myös varautumisen ja jatkuvuuden (0,70) kehitys on käynnissä, mutta käytännön valmius vakaviin häiriöihin on edelleen puutteellinen etenkin kunnissa, kuntayhtymissä ja korkeakouluissa. Riski toimintakyvyn merkittävästä heikkenemisestä pitkittyneissä häiriöissä on todellinen.

Toimijaryhmittäinen tilanne

Valtionhallinto ja hyvinvointialueiden tilanne on paras eli saanut korkeimman yleisarvosanan ja tasapainoisen tilanteen digiturvan kannalta.

Kuntien kokonaistilanne on selvästi matalampi; resurssi- ja osaamisvaje korostuvat toimijaryhmän tuloksissa.

Korkeakoulusektori on saavuttanut suhteellisen hyvä johtamisen tason, mutta operatiivinen kyber- ja jatkuvuuskyvykkyys on vaihtelevaa.

Kehityssuunta

Kokonaisuutena tuloksissa on huomattavissa lievää parannusta edellisvuoteen verrattuna. Kehitys on pääosin reaktiivista, ei vielä johdonmukaisesti kypsyysmallien tai ennakoivan riskienhallinnan ohjaamaa.

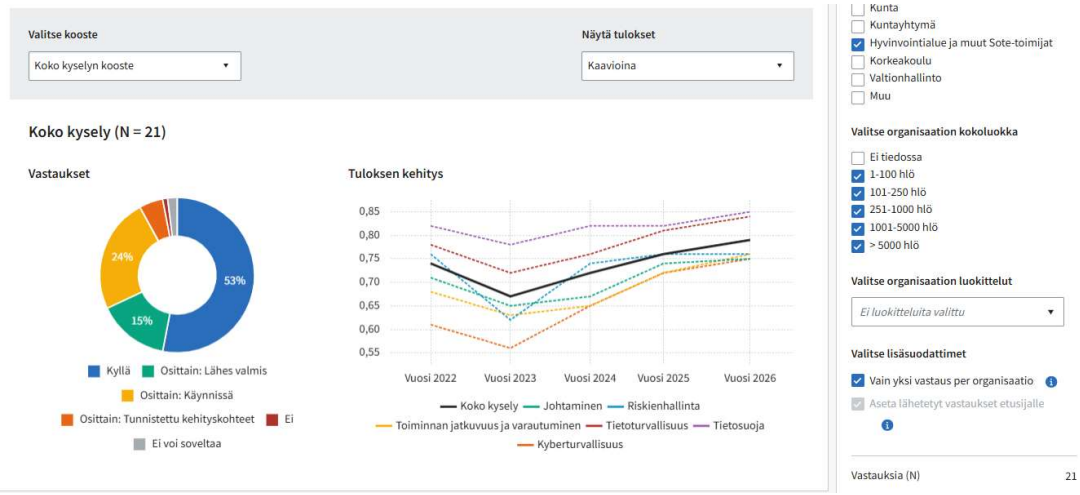
Johtopäätöksenä voidaan siis sanoa, että digiturva turvaa tiedon, mutta ei vielä systemaattisesti organisaatioiden toimintakykyä. Suurin riski ei ole yksittäinen tekninen puute, vaan johtamisen, kyberkyvykkyyden ja varautumisen yhteisvaikutus: häiriöihin varaudutaan liian kapea-alaisesti suhteessa nykyiseen uhkaympäristöön.

2.2.2 Johdolle avainkysymys jatkokehittämistä varten

Miten digiturva kytketään selkeästi johtamiseen, varautumiseen ja toiminnan jatkuvuuden varmistamiseen – ei vain vaatimusten täyttämiseen?

2.2.3 Hyvinvointialueiden kehitys

Eri vuosien vastauksia vertailtaessa on huomattava, että hyvinvointialueiden toiminta käynnistyi vasta vuoden 2023 alussa. Digiturvan kokonaiskuvapalvelussa kartoitetaan organisaation toimintaprosesseja ja menettelyitä. Nämä ovat kuitenkin aloittavissa organisaatioissa väistämättä vasta kehitysvaiheessa. Tästä syystä sote-toimijoiden tulokset putosivat huomattavasti vuodesta 2022, jolloin ne menestyivät hyvin erityisesti riskienhallinnassa ja jatkuvuuden hallinnassa. Vuosien 2024 ja 2025 kampanjoissa hyvinvointialueiden tulokset kuitenkin paranivat voimakkaasti. 2026 kampanjan keskiarvioissa hyvinvointialueet ovat nousseet lähes valtiohallinnon tasolle.



Kuvio 2. Hyvinvointialueiden digiturvan osa-alueiden kehitys vuosina 2021 - 2025

Verrattaessa sote-toimijoiden vastauksia edellisiin vuosiin voidaan havaita, että positiivinen kehitys on jatkunut hyvinvointialueilla kaikilla digiturvan osa-alueilla.

3 Osa-aluekohtaiset tulokset

Taulukoissa 2–8 eritellään Digiturvakyselyn osa-alueiden – johtaminen, riskienhallinta, jatkuvuus ja varautuminen, tietoturvallisuus, tietosuoja, kyberturvallisuus ja havainnointi – väittämäkohtaiset vastauskeskiarvot sekä kaikkien vastaajien osalta että toimialakohtaisesti. Taulukon keskiarvot ovat värikoodattu. Samaa värikoodausta käytetään kaikkien osa-alueiden väittämien keskiarvoissa. Mitä lähempänä arvoa 1,00 keskiarvo on, sitä parempi tilanne ko. väittämän osalta on. Värikoodit ja niiden arvot:

- Punainen: arvot 0,00–0,29 (Suurin osa vastauksista ei ja osittain – tunnistettu kehityskohteet, vain vähän kyllä vastauksia)
- Oranssi: arvot 0,30–0,59
- Keltainen: arvot 0,60–0,79
- Vihreä: arvot 0,80–1,00 (Suurin osa vastauksista kyllä ja osittain – lähes valmis)

3.1 Johtaminen

Taulukossa 2 esitetään johtamisosion 13 väittämän vastauskeskiarvot. Taulukossa suluissa on merkitty vuoden 2025 kyselyn vastauskeskiarvot.

Taulukko 2. Johtaminen – kysymyskohtaiset keskiarvot. Suluissa vuoden 2025 tulokset

Johtaminen / Väittämä	Kaikki organisaatiot 204 (203) kpl	Kunta 102 (93) kpl	Kuntayhtymä 24 (22) kpl	Hyvinvointialue ja muut Sote-	Korkeakoulu 10 (14) kpl	Valtionhallinto 37 (43) kpl	Muu 11 (10) kpl

				toimijat 21 (21) kpl			
1. Organisaation digitaalisen turvallisuuden tehtävät ja vastuut on tunnistettu ja kuvattu selkeästi.	0,77 (0,76)	0,71 (0,67)	0,75 (0,81)	0,85 (0,84)	0,90 (0,77)	0,84 (0,84)	0,89 (0,95)
2. Organisaatio on kartoittanut sen digitaalista turvallisuutta ohjaavan lainsäädännön ja tunnistanut siitä aiheutuvat velvoitteet.	0,77 (0,76)	0,67 (0,64)	0,81 (0,75)	0,93 (0,95)	0,85 (0,80)	0,84 (0,89)	0,91 (0,80)
3. Organisaatio on kartoittanut keskeiset sidos- ja asiakasryhmät sekä niiltä tulevat digiturvavaatimukset.	0,71 (0,70)	0,63 (0,58)	0,73 (0,71)	0,81 (0,76)	0,80 (0,73)	0,81 (0,81)	0,95 (0,95)
4. Organisaatiossa on riittävästi osaavaa henkilöstöä digiturvallisuuden eri osa-alueilla.	0,53 (0,53)	0,47 (0,45)	0,59 (0,64)	0,54, (0,58)	0,75 (0,52)	0,55(0,60)	0,61 (0,65)
5. Organisaatiolla on riittävä budjetti digiturvallisuuden ylläpitoon sekä kehittämiseen.	0,59 (0,61)	0,56 (0,53)	0,64 (0,76)	0,54 (0,59)	0,75 (0,54)	0,63 (0,65)	0,70 (0,75)
6. Organisaation johto on sitoutunut digitaalisen turvallisuuden kehittämiseen.	0,77 (0,77)	0,70 (0,69)	0, 79 (0,78)	0,80 (0,80)	0,83 (0,75)	0,87 (0,87)	0,84 (0,88)
7.Organisaation digitaalisen turvallisuuden osa-alueita kehitetään järjestelmällisesti.	0,67 (0,63)	(0,52)	0,73 (0,75)	0,69 (0,67)	0,83 (0,70)	0,73 (0,70)	0,84 (0,88)
8. Henkilöstölle on olemassa riittävä ohjeistus digitaalisesta turvallisuudesta.	0,73 (0,72)	0,67 (0,69)	0,76 (0,74)	0,76 (0,65)	0,75 (0,73)	0,76 (0,75)	0,84 (0,83)

9. Henkilöstölle annetaan säännöllisesti koulutusta digitaalisesta turvallisuudesta.	0,72 (0,70)	0,67 (0,65)	0,77 (0,64)	0,79 (0,78)	0,68 (0,55)	0,76 (0,80)	0,82 (0,85)
10. Organisaatiolla on olemassa prosessi väärinkäytöksiin reagoimiseksi.	0,81 (0,84)	0,75 (0,79)	0,83 (0,84)	0,87 (0,87)	0,93 (0,84)	0,86 (0,90)	0,91 (0,98)
11. Digitaaliseen turvallisuuteen liittyvät mittarit on määritelty.	0,42 (0,40)	0,33 (0,32)	0,38 (0,35)	0,53 (0,48)	0,65 (0,48)	0,49 (0,48)	0,75 (0,68)
12. Digitaalisen turvallisuuden tilaa seurataan jatkuvasti.	0,79 (0,79)	0,75 (0,73)	0,84 (0,86)	0,81 (0,78)	0,95 (0,86)	0,81 (0,82)	0,89 (0,88)
13. Digitaalisen turvallisuuden kokonaistilanteesta raportoidaan säännöllisesti organisaation johdolle.	0,73 (0,74)	0,64 (0,67)	0,71 (0,64)	0,78 (0,79)	0,70 (0,64)	0,93 (0,88)	0,98 (0,90)

3.1.1 Digiturvan johtamisen osa-alue

Johtamisen osa-alueen tulosten perusteella digiturvan perusrakenteet ovat laajasti olemassa, erityisesti vastuiden tunnistamisen, johdon sitoutumisen ja häiriöihin reagoinnin osalta. Sen sijaan systemaattinen ohjaus, mittaaminen ja resurssien pitkäjänteinen varmistaminen muodostavat edelleen selkeitä kehityskohteita. Kokonaisuutena johtaminen tukee digiturvaa, mutta ei vielä kaikilta osin ohjaa sitä tavoitteellisesti ja mitattavasti.

Keskiarvot ovat kokonaisuutena kohtalaisen hyvällä tasolla, mutta vaihtelu on merkittävää eri kysymysten välillä. Vahvuudet painottuvat rakenteisiin ja johdon sitoutumiseen, kun taas mittarointi, resurssit ja osaamisen systemaattinen kehittäminen jäävät selvästi heikommalle tasolle.

Kolme keskeistä positiivista havaintoa

1. Johdon sitoutuminen digiturvaan on vahvaa

Väittämä *”Organisaation johto on sitoutunut digitaalisen turvallisuuden kehittämiseen”* sai keskiarvon 0,77, joka on pysynyt samalla hyvällä tasolla kuin edellisvuonna.

Tämä luo edellytykset pitkäjänteiselle kehittämiselle ja strategiselle ohjaukselle.

2. Väärinkäytöksiin reagointi ja jatkuva seuranta ovat hyvällä tasolla

Reagointiprosessien olemassaolo (0,81) ja digiturvan tilan jatkuva seuranta (0,79) ovat osa-alueen vahvimpia tuloksia.

Tulokset viittaavat siihen, että operatiivinen toiminta digiturvassa on monissa organisaatioissa jo melko kehittynyt.

3. Vastuut ja velvoitteet on pääosin tunnistettu

Digiturvatehtävien ja vastuiden tunnistaminen (0,77) sekä lainsäädäntövelvoitteiden kartoitus (0,77) ovat vakiintuneita käytäntöjä ja osoittavat hyvää hallinnollista perustaa.

3.1.2 Kolme keskeistä kehityskohdetta

1. Digiturvan mittarointi on selvästi heikoin osa-alue

Väittämä *"Digitaaliseen turvallisuuteen liittyvät mittarit on määritelty"* sai vain keskiarvon 0,42. Lievää parannusta edellisvuoteen on kuitenkin nähtävissä (0,40 → 0,42).

Ilman mittareita johdon on vaikea tehdä tietoon perustuvia päätöksiä.

2. Osaavien resurssien riittävyys on puutteellista

Henkilöstön osaamisen riittävyys digiturvan eri osa-alueilla jäi keskiarvoon 0,53, eikä kehitystä edellisvuoteen ole tapahtunut.

Tämä on rakenteellinen riski digiturvan jatkuvuudelle.

3. Budjetointi ja systemaattinen kehittäminen ontuvat

Digiturvan budjetointi (0,59) on hieman heikentynyt edellisvuodesta.

Vaikka järjestelmällinen kehittäminen on parantunut (0,63 → 0,67), resurssit eivät vielä ole riittävällä tasolla.

Kehityssuunta verrattuna edellisvuoteen

Kokonaisuutena johtamisen osa-alueessa nähdään lievää myönteistä kehitystä, erityisesti:

- digiturvan systemaattisessa kehittämisessä
- sidosryhmävaatimusten tunnistamisessa
- koulutuksen järjestämisessä

Samaan aikaan resursointi, mittarointi ja budjetointi eivät ole kehittyneet toivotulla tavalla, mikä hidastaa vaikuttavaa edistymistä.

3.1.3 Kehitysehdotukset julkishallinnolle

1. **Johdon käyttöön selkeä digiturvan mittaristo**

- Määrittele 5–10 keskeistä digiturvan KPI-mittaria (esim. riskitaso, poikkeamien määrä, koulutusaste).
- Hyödynnä tilannekuvan seurannassa digiturvan kokonaiskuvapalvelua ja Kyber-mittaria
- Kytke mittarit osaksi normaalia johtoryhmäraportointia.

2. Vahvista osaamista roolipohjaisesti

- Hyödynnä Digiturvan tietopankin tukimateriaaleja
- Kohdenna syvempi koulutus niihin rooleihin, joissa riskivaikutus on suurin.
- Tue koko henkilöstön osaamisen kehittämistä rooleihin ja vastuisiin perustuen

3. Nosta digiturva osaksi strategista ja taloudellista suunnittelua

- Sisällytä digiturva osaksi talousarvioprosessia ja strategisia tavoitteita.
- Hyödynnä riskiperusteista lähestymistapaa investointien priorisointiin.

3.2 Riskienhallinta

Taulukossa 3 esitetään riskienhallinnan yhdeksän väittämän vastauskeskiarvot.

Taulukko 3. Riskienhallinta – kysymyskohtaiset keskiarvot

Riskienhallinta / Väittämä	**Kaikki organisaatiot 209 kpl**	**Kunta** 93 kpl	**Kuntayhtymä** 22 kpl	**Hyvinvointialue ja muut Sote-toimijat** 21 kpl	**Korkeakoulu** 14 kpl	**Valtionhallinto** 43 kpl	**Muu** 10 kpl
14. Organisaatiolla on johdon hyväksymät, toimintaan sovitetut riskienhallinnan linjaukset, vastuut ja prosessi.	0,77 (0,78)	0,69 (0,68)	0,83 (0,80)	0,81 (0,81)	0,85 (0,84)	0,88 (0,88)	0,86 (0,90)
15. Organisaatio tekee digiturvallisuuteen liittyvää säännöllistä riskienarviointia, jossa huomioidaan uudet ilmiöt, toimintaympäristön muutokset ja oman toiminnan vaikutukset sidosryhmien ja asiakkaiden tilanteeseen.	0,65 (0,61)	0,55 (0,52)	0,70 (0,57)	0,73 (0,75)	0,73 (0,70)	0,71 (0,67)	0,84(0,93)
16. Organisaatiossa viestitään digiturvallisuuden riskitilanteesta	0,81 (0,80)	0,78 (0,79)	0,84 (0,82)	0,83 (0,80)	0,70 (0,75)	0,81 (0,76)	0,95(0,95)

ja uusista riskeistä koko organisaation laajuisesti.							
17. Organisaatiossa raportoidaan riskitilanteesta johdolle säännöllisesti.	0,76 (0,78)	0,69 (0,69)	0,82 (0,82)	0,82 (0,85)	0,83 (0,80)	0,82 (0,84)	0,98(1)
18. Organisaation tunnistamat kriittiset riskit raportoidaan johdolle välittömästi.	0,86 (0,88)	0,85 (0,84)	0,91 (0,98)	0,80 (0,90)	0,80 (0,82)	0, 90 (0,91)	0,93(1)
19. Organisaatio seuraa riskien ja niiden hallintatoimenpiteiden tilannetta säännöllisesti.	0,70 (0,70)	0,64 (0,64)	0,81 (0,74)	0,77 (0,75)	0,74 (0,71)	0,70 (0,72)	0,83(0,93)
20. Organisaation ylin johto sekä organisaation hallitus (tai vastaava) seuraa merkittävien riskien ja niiden hallintatoimenpiteiden tilannetta säännöllisesti.	0,58 (0,55)	0,49 (0,46)	0,71 (0,64)	0,61 (0,59)	0,65 (0,63)	0,64 (0,62)	0,89(0,85)
21. Organisaatiossa arvioidaan jäännösriskejä riskienhallintatoimenpiteiden toteuttamisen jälkeen ja jäännösriskit käsitellään asianmukaisella tasolla.	0,56 (0,55)	0,47 (0,48)	0,68 (0,58)	0,68 (0,66)	0,68 (0,50)	0,59 (0,62)	0,75(0,78)
22. Organisaatiossa kehitetään riskienhallintaprosessia saatujen riskienhallinnan tavoitteiden tai saatujen kokemusten perusteella.	0,69 (0,68)	0,62 (0,59)	0,74 (0,70)	0,77 (0,74)	0,80 (0,79)	0,72 (0,72)	0,86(0,9)

Riskienhallinnan kokonaiskuvan tulokset osoittavat, että organisaatioissa on vakiintuneita käytäntöjä erityisesti riskien raportoinnissa ja viestinnässä. Sen sijaan riskienhallinnan ennakoivuudessa, jatkuvuudessa sekä johdon strategisessa ohjauksessa on edelleen kehitettävää.

Korkein keskiarvo saavutetaan väittämässä, joka koskee kriittisten riskien raportoimista johdolle välittömästi (0,86). Myös riskien viestintä organisaation sisällä (0,81) sekä säännöllinen raportointi johdolle (0,76) ovat hyvällä tasolla.

Heikoimmat tulokset liittyvät ylimmän johdon ja hallituksen aktiiviseen riskien seurantaan (0,58) sekä jäännösriskien arviointiin ja käsittelyyn (0,56). Lisäksi säännöllinen ja toimintaympäristön muutokset huomioiva riskienarviointi jää keskimääräistä heikommaksi (0,65).

Tarkastelun perusteella riskienhallinta painottuu edelleen reaktiivisiin käytäntöihin. Organisaatioissa kyetään tunnistamaan ja raportoimaan riskejä, mutta ennakoiva riskienhallinta sekä riskienhallinnan kytkentä strategiseen johtamiseen ei ole vielä riittävällä tasolla.

Vastaajaryhmien välillä on kuitenkin eroja. Valtionhallinto ja korkeakoulut saavuttavat keskimäärin parempia tuloksia, kun taas kunnissa tulokset jäävät useilla osa-alueilla heikommiksi. Hyvinvointialueilla ja sote-toimijoilla kehitys on ollut selvästi positiivista viime vuosina.

3.2.1 Kehitys suhteessa vuoden 2025 tuloksiin

Tuloksissa on nähtävissä maltillista kehitystä useilla osa-alueilla.

Säännöllinen digiturvallisuuteen liittyvä riskienarviointi on parantunut (0,61 → 0,65), mikä viittaa siihen, että riskien tarkastelua tehdään aiempaa systemaattisemmin ja toimintaympäristön muutoksia huomioiden.

Ylimmän johdon ja hallituksen tekemä riskien seuranta on myös hieman vahvistunut (0,55 → 0,58), mutta taso on edelleen osa-alueen heikoin.

Kriittisten riskien välitön raportointi on säilynyt korkealla tasolla, vaikka tuloksessa on havaittavissa lievä lasku (0,88 → 0,86).

Jäännösriskien arvioinnissa ja käsittelyssä ei ole tapahtunut merkittävää muutosta (0,55 → 0,56), mikä osoittaa kehityksen olevan hidasta tässä osa-alueessa.

Vastaajaryhmistä erityisesti hyvinvointialueet ja muut sote-toimijat ovat parantaneet tuloksiaan merkittävästi.

3.2.2 Riskienhallinnan kehittämiskohteet

Kehittämiskohde – Johdon roolin vahvistaminen riskienhallinnassa
Organisaatioiden ylimmällä johdolla ja hallituksella on kehitettävää merkittävien riskien ja niiden hallintatoimenpiteiden säännöllisessä seurannassa. Riskienhallinta tulee integroida nykyistä tiiviimmin strategiseen johtamiseen ja päätöksentekoon. Johdolle suunnattua raportointia tulee kehittää siten, että se tukee päätöksentekoa ja riskien kokonaisvaltaista ymmärtämistä.

Kehittämiskohde – Ennakoiva ja jatkuva riskienarviointi
Riskien arviointia tulee toteuttaa nykyistä systemaattisemmin ja jatkuvammin. Riskienhallinnan tulee kattaa toimintaympäristön muutokset, uudet ilmiöt sekä organisaation toiminnan vaikutukset sidosryhmiin ja asiakkaisiin. Riskien arviointi tulee kytkeä osaksi muutostenhallintaa, hankkeita sekä häiriö- ja poikkeamatilanteita.

Kehittämiskohde – Jäännösriskien hallinta ja läpinäkyvyys
Jäännösriskien arviointi ja käsittely on yksi keskeisimmistä kehittämiskohteista. Organisaatioiden tulee varmistaa, että riskienhallintatoimenpiteiden jälkeen jäljelle jäävät riskit tunnistetaan, arvioidaan ja käsitellään asianmukaisella tasolla. Jäännösriskien hyväksyntä ja raportointi tulee tehdä näkyväksi erityisesti johdolle.

3.3 Toiminnan jatkuvuus ja varautuminen

Toiminnan jatkuvuus ja varautuminen -osion 16 väittämän vastauskeskiarvot ovat taulukossa 4.

Taulukko 4. Toiminnan jatkuvuus ja varautuminen – kysymyskohtaiset keskiarvot

Toiminnan jatkuvuus ja varautuminen / Väittämä	Kaikki organisaatiot 209kpl	Kunta 104 kpl	Kuntayhtymä 24 kpl	Hyvinvointialue ja muut Sote-toimijat 21 kpl	Korkeakoulu 10 kpl	Valtionhallinto 39 kpl	Muu 11 kpl
23. Organisaation tehtävät ja vastuut ovat selkeät myös poikkeustilanteissa ja poikkeusoloissa.	0,82 (0,84)	0,80 (0,84)	0,80 (0,85)	0,86 (0,83)	0,85 (0,87)	0,83 (0,81)	0,89 (0,93)
24. Organisaatiolla on prosessi ja valmiudet nopeaan ja tehokkaaseen digiturvallisuuden häiriöiden, uhkien ja poikkeamien käsittelyyn.	0,77 (0,77)	0,70 (0,69)	0,76 (0,85)	0,88 (0,81)	0,75 (0,75)	0,85 (0,84)	0,91 (0,90)
25. Organisaatio on kuvannut jatkuvuuden hallinnan periaatteet, tavoitteet, organisoinnin ja vastuut.	0,66 (0,63)	0,61 (0,56)	0,60 (0,64)	0,69 (0,63)	0,65 (0,64)	0,78 (0,76)	0,75 (0,70)
26. Organisaatio on tunnistanut ja dokumentoinut suojattavat kohteet.	0,69 (0,69)	0,66 (0,66)	0,73 (0,74)	0,70 (0,69)	0,58 (0,68)	0,77 (0,73)	0,89 (0,85)
27. Suojattavien kohteiden tunnistamiseen ja kriittisyyden määrittelyyn on dokumentoitu ja hyväksytty menetelmä.	0,63 (0,67)	0,58 (0,60)	0,71 (0,72)	0,70 (0,75)	0,58 (0,71)	0,71 (0,76)	0,81 (0,81)
28. Organisaatio on määritellyt kuinka pitkiä toimintakatkoksia kriittiset toiminnot sietävät organisaation toiminnan häiriintymättä.	0,57 (0,56)	0,54 (0,53)	0,57 (0,60)	0,61 (0,60)	0,40 (0,34)	0,66 (0,63)	0,70 (0,58)
29. Toiminnan jatkuvuuden edellyttämät palvelutasovaatimukset ovat osa hankintavaatimuksia ja sopimuksia.	0,70 (0,69)	0,67 (0,66)	0,65 (0,69)	0,75 (0,75)	0,68 (0,70)	0,76 (0,71)	0,77 (0,85)
30. Jatkuvuuteen liittyviä riskejä ja riskitilanteen muutosta arvioidaan säännöllisesti.	0,59 (0,58)	0,53 (0,49)	0,61 (0,57)	0,71 (0,71)	0,50 (0,43)	0,68 (0,66)	0,80 (0,88)
31. Organisaatiolle ja sen kriittisille toiminnoille/palveluille on laadittu jatkuvuussuunnitelmat, jotka perustuvat tunnistettuihin riskeihin.	0,56 (0,54)	0,55 (0,49)	0,43 (0,43)	0,60 (0,55)	0,33 (0,39)	0,63 (0,66)	0,77 (0,80)
32. Kriittisille tietojärjestelmille on laadittu toipumissuunnitelmat.	0,58 (0,59)	0,51 80,49)	0,56 (0,63)	0,76 (0,71)	0,45 (0,45)	0,67 (0,67)	0,80 (0,88)

33. Organisaatiolla on häiriö- ja kriisitilanteiden viestintäsuunnitelma.	0,88 (0,87)	0,87 (0,86)	0,75 (0,81)	0,89 (0,88)	0,95 (0,73)	0,94 (0,91)	0,95 (0,98)
34. Suunnitelmien sisältö on koulutettu häiriötilanteiden hallintaan osallistuville henkilöille.	0,65 (0,61)	0,65 (0,60)	0,52 (0,57)	0,69 (0,57)	0,68 (0,59)	0,63 (0,62)	0,73 (0,70)
35. Organisaatiossa on luotu yhteydet ja verkostot tarvittavien sidosryhmien väliseen viestintään poikkeamatilanteissa.	0,74 (0,72)	0,73 (0,71)	0,62 (0,65)	0,80 (0,75)	0,70 (0,57)	0,81 (0,77)	0,86 (0,80)
36. Organisaatiolla on olemassa menettely sen toimintaa kohdistuvien häiriöiden, hyökkäysten ja loukkausten ilmoittamiseksi keskeisille viranomaisille.	0,94 (0,92)	0,93 (0,90)	0,89 (0,93)	0,98 (0,98)	0,95 (0,88)	0,98 (0,96)	1 (0,95)
37. Organisaatio harjoittelee säännöllisesti sen toimintaan kohdistuvien häiriöiden, poikkeamien ja hyökkäysten havainnointia, reagointia ja johtamista.	0,77 (0,72)	0,76 (0,68)	0,68 (0,57)	0,82 (0,80)	0,80 (0,71)	0,83 (0,76)	0,82 (0,83)
38. Jatkuvuus-, toipumis- ja viestintäsuunnitelmia päivitetään harjoitusten tai toteutuneiden häiriötilanteiden perusteella.	0,69 (0,66)	0,69 (0,64)	0,65 (0,63)	0.73 (0,71)	0,63 (0,50)	0,71 (0,66)	0,82 (0,85)

3.3.1 Toiminnan jatkuvuus ja varautuminen

Toiminnan jatkuvuuden ja varautumisen osa-alueen keskiarvo on 0,69, mikä kuvaa kokonaisuutena kohtalaista kyvykkyystasoa. Osa-alueella on tapahtunut lievää parannusta, mutta kehitys on epätasaista eri teemoissa ja organisaatiotyypeissä.

Korkeimmat tulokset liittyvät häiriö- ja kriisitilanteiden hallinnan käytäntöihin, kun taas matalammat tulokset kohdistuvat jatkuvuuden hallinnan riskiperusteisuuteen ja suunnitelmallisuuteen. Tämä viittaa siihen, että organisaatioiden operatiivinen valmius on kehittyneempi kuin systemaattinen ennakoiva johtaminen.

3.3.2 Keskeiset havainnot

Osa-alueen vahvimmat tulokset liittyvät viranomaisilmoituksiin, viestintään sekä roolien ja vastuiden määrittelyyn. Lähes kaikilla organisaatioilla on menettely häiriö-, hyökkäys- ja loukkaustilanteiden ilmoittamiseen keskeisille viranomaisille (0,94). Myös häiriö- ja kriisitilanteiden viestintäsuunnittelu on hyvällä tasolla (0,88), ja tehtävät sekä vastuut poikkeustilanteissa on kuvattu kattavasti (0,82). Lisäksi organisaatiot harjoittelevat aiempaa systemaattisemmin häiriötilanteiden hallintaa (0,77), mikä tukee operatiivista valmiutta ja reagointikykyä.

Heikoimmat tulokset liittyvät jatkuvuuden hallinnan riskiperusteisuuteen. Jatkuvuuteen liittyviä riskejä ja niiden muutoksia arvioidaan vain osittain systemaattisesti

(0,59), ja riskiperusteisten jatkuvuussuunnitelmien laadinta on edelleen puutteellista (0,56). Myös kriittisten toimintojen sietokyvyn määrittely (0,57) sekä toipumissuunnitelmien kattavuus (0,58) ovat kehityskohteita.

Havainnot osoittavat, että jatkuvuuden hallinta painottuu edelleen enemmän yksittäisiin toimenpiteisiin kuin kokonaisvaltaiseen ja riskilähtöiseen toimintamalliin.

3.3.3 Kehitys

Osa-alueen keskiarvo on noussut hieman (0,67 → 0,69), mikä osoittaa maltillista positiivista kehitystä.

Organisaatiotyypeittäin tarkasteltuna kehitys on erisuuntaista. Hyvinvointialueilla ja muilla sote-toimijoilla on tapahtunut merkittävää parannusta, mikä viittaa toiminnan vakiintumiseen ja kehittämistoimenpiteiden vaikuttavuuteen. Valtionhallinnossa kehitys on ollut lievästi positiivista. Kunnissa ja korkeakouluissa kehitys on ollut vähäistä, ja kuntayhtymissä tulokset ovat hieman heikentyneet. Muut -ryhmässä on havaittavissa selkeää parannusta, mutta vastaajamäärän vähäisyys lisää tulosten vaihtelua.

Kokonaisuutena kehitys positiiviseen suuntaan tukee havaintoa, että kohdennetut kehittämistoimenpiteet ja systemaattinen ohjaus vaikuttavat positiivisesti kyvykkyyden kehittymiseen.

3.3.4 Kehitys verrattuna vuoteen 2025

Vuoden 2025 tuloksiin verrattuna toiminnan jatkuvuuden ja varautumisen osa-alueella kehitys on kokonaisuutena lievästi positiivista, mutta osa-alueiden välillä on edelleen eritahtisuutta.

Parannusta on havaittavissa erityisesti operatiivisissa kyvykkyyksissä. Harjoittelu, viestintävalmiudet sekä häiriötilanteiden hallintaan liittyvät menettelyt ovat vahvistuneet, mikä näkyy useiden väittämien keskiarvojen nousuna. Myös tehtävien ja vastuiden selkeydessä sekä viranomaisilmoitusmenettelyissä taso on pysynyt korkeana ja osin edelleen parantunut.

Sen sijaan riskiperusteiseen jatkuvuuden hallintaan liittyvissä osa-alueissa kehitys on ollut hitaampaa tai paikoin jopa negatiivista. Erityisesti riskien systemaattinen arviointi, kriittisyyksien määrittelyyn liittyvät menetelmät sekä jatkuvuus- ja toipumissuunnitelmien riskilähtöisyys eivät ole kehittyneet samalla tavalla, ja joissakin väittämissä on havaittavissa hienoista heikkenemistä.

Kokonaisuutena vertailu osoittaa, että organisaatiot ovat vahvistaneet käytännön varautumista ja reagointikykyä, mutta jatkuvuuden hallinnan strateginen ja ennakoiva ulottuvuus kehittyy edelleen hitaammin.

3.3.5 Johtopäätökset

Toiminnan jatkuvuuden ja varautumisen taso on kokonaisuutena kohtalainen ja kehittymässä, mutta osa-alueella on selkeä rakenteellinen epätasapaino.

Organisaatioiden vahvuudet liittyvät erityisesti häiriötilanteiden operatiiviseen hallintaan, kuten viestintään, ilmoitusmenettelyihin ja harjoitteluun. Sen sijaan jatkuvuuden

hallinnan keskeiset perusrakenteet, kuten riskiperusteinen suunnittelu, kriittisyyksien määrittely ja toipumisen tavoitteiden asettaminen, ovat vielä kehittymässä.

Jatkuvuuden hallinnan kehittämisessä keskeistä on siirtyminen yksittäisistä käytännöistä kohti systemaattista, riskilähtöistä ja johdettua toimintamallia.

3.3.6 Toiminnan jatkuvuuden ja varautumisen kehittämiskohteet

Kehittämiskohde: Riskilähtöinen jatkuvuuden hallinta

Jatkuvuuden hallintaa tulee kehittää kokonaisuutena siten, että se perustuu ajantasaiseen riskikuvaan. Organisaatioiden tulee tunnistaa kriittiset toiminnot ja niihin kohdistuvat riskit sekä arvioida riskien muutoksia säännöllisesti. Jatkuvuussuunnitelmien tulee perustua tähän riskitarkasteluun.

Kehittämiskohde: Kriittisten toimintojen palautumistavoitteet

Organisaatioiden tulee määritellä systemaattisesti kriittisten toimintojen hyväksyttävät toimintakatkokset ja toipumisaikavaatimukset. Näiden tulee ohjata sekä jatkuvuussuunnittelua että hankintoja ja sopimuksia, jotta palveluiden palautuminen voidaan varmistaa hallitusti.

Kehittämiskohde: Suunnitelmien jalkauttaminen ja jatkuva kehittäminen

Jatkuvuus-, toipumis- ja viestintäsuunnitelmat tulee laatia kaikille kriittisille palveluille, ja niiden toimivuutta tulee varmistaa säännöllisellä koulutuksella ja harjoittelulla. Suunnitelmia tulee myös päivittää systemaattisesti harjoitusten ja toteutuneiden häiriötilanteiden perusteella.

3.4 Tietoturvallisuus

Taulukossa 5 esitetään Tietoturvallisuus-osion 16 väittämän vastauskeskiarvot.

Taulukko 5. Tietoturvallisuus – kysymyskohtaiset keskiarvot

Tietoturva / Väittämä	Kaikki organisaatiot 209 kpl	Kunta 104 kpl	Kuntayhtymä 24 kpl	Hyvinvointialue ja muut Sote-toimijat 21 kpl	Korkeakoulu 10 kpl	Valtionhallinto 39 kpl	Muu 11 kpl
39. Organisaatiolla on johdon hyväksymä tietoturvapolitiikka tai vastaava tietoturvallisuuden toteuttamista ohjaava asiakirja.	0,94 (0,95)	0,91 (0,94)	0,84 (0,94)	0,99 (0,98)	0,98 (0,95)	0,99 (0,93)	0,95 (1,00)
40. Organisaatiolla on olemassa henkilöiden	0,58 (0,59)	0,44 (0,39)	0,36 (0,37)	0,88 (0,89)	0,33 (0,25)	0,94 (0,97)	0,75 (0,50)

taustatarkistuksiin liittyvä menettely, joka kattaa oman ja palvelutoimittajien henkilöstön.							
41. Organisaatiolla on olemassa käyttövaltuuspolitiikka ja prosessi käyttövaltuuksien hallintaan.	0,80 (0,80)	0,77 (0,78)	0,74 (0,76)	0,85 (0,78)	0,80 (0,79)	0,87 (0,83)	0,91 (0,90)
42. Käyttövaltuuksien ajantasaisuus varmistetaan säännöllisesti.	0,71 (0,68)	0,71 (0,67)	0,76 (0,74)	0,65 (0,66)	0,65 (0,63)	0,72 (0,71)	0,75 (0,65)
43. Organisaatio on määrittänyt fyysisesti suojatut turvallisuusalueet asiakirjojen käsittelyn ja tietojärjestelmien suojaamiseksi.	0,72 (0,72)	0,66 (0,64)	0,68 (0,65)	0, 70 (0,66)	0,64 (0,71)	0,88 (0,90)	0,88 (0,86)
44. Organisaation tietojärjestelmät ja laitteet ovat kattavasti järjestelmänhallinnan piirissä.	0,89 (0,89)	0,89 (0,88)	0,95 (0,93)	0,87 (0,88)	0,80 (0,89)	0,89 (0,88)	0,91 (0,95)
45.Organisaatiolla on käytössä monivaiheinen tunnistus etäkäytössä.	0,87 (0,87)	0,83 (0,82)	0,92 (0,91)	0,94 (0,93)	0,85 (0,80)	0,99 (0,97)	0,80 (0,78)
46. Toimitilojen ulkopuolella työskenneltäessä yhteydet organisaation ICT-palveluihin sallitaan vain VPN-yhteydellä.	0,88 (0,87)	0,90 (0,92)	0,89 (0,77)	0,94 (0,91)	0,72 (0,75)	0,85 (0,83)	0,83 (0,89)

47. Organisaatiolla on olemassa tarvittavat tekniset ratkaisut ja menettelyt haittaohjelmien tunnistamiseen ja estämiseen.	0,96 (0,95)	0,94 (0,94)	0,98 (0,95)	0,96 0,95)	0,98 (0,91)	0,97 (0,95)	0,98 (1,00)
48. Organisaation tiedoista ja järjestelmistä otetaan säännöllisesti varmuuskopiot.	0,92 (0,92)	0,92 (0,92)	0,95 (0,99)	0,93 (0,89)	0,80 (0,88)	0,92 (0,92)	0,98 (0,98)
49. Varmuuskopioiden palautusta testataan säännöllisesti.	0,59 (0,59)	0,60 (0,60)	0,69 (0,67)	0,52 (0,55)	0,35 (0,50)	0,56 (0,56)	0,84 (0,70)
50. Tietojärjestelmien käytöstä ja tietojen luovutuksista kerätään riittävät lokitiedot.	0,72 (0,70)	0,70 (0,69)	0,69 (0,72)	0,77 (0,73)	0,58 (0,55)	0,77 (0,78)	0,84 (0,78)
51. Käytössä olevien tietojärjestelmien teknisiin haavoittuvuuksiin liittyviä tiedotteita seurataan ja niihin reagoidaan.	0,93 (0,94)	0,91 (0,93)	0,91 (0,92)	0,96 (0,93)	0,98 (0,93)	0,99 (0,95)	0,93 (0,98)
52. Tietoturvallisuuteen ja tietojärjestelmiin liittyviä auditointeja tehdään säännöllisesti.	0,58 (0,56)	0,46 (0,44)	0,51 (0,51)	0,56 (0,52)	0,70 (0,45)	0,81 (0,76)	0,86 (0,83)
53. Tietoturva- ja tietosuojavaatimukset ovat osa hankintavaatimuksia ja sopimuksia.	0,86 (0,88)	0,80 (0,82)	0,82 (0,83)	0,98 (0,94)	0,83 (0,86)	0,97 (0,94)	0,95 (0,93)

54. Tietoturva- ja tietosuojavaatimukset otetaan huomioon myös järjestelmien ja palveluiden kehittämisessä sekä ylläpidossa.	0,84 (0,83)	0,82 (0,80)	0,85 (0,88)	0,87 (0,86)	0,70 (0,70)	0,90 (0,87)	0,89 (0,95)

3.4.1 Tilannekuva

Tietoturvallisuuden kokonaiskuva vuoden 2026 arvioinnissa osoittaa, että organisaatioiden tietoturva on perustasoltaan hyvä ja keskeiset suojatoimenpiteet ovat laajasti käytössä. Erityisesti tekniset tietoturvakontrollit, kuten haittaohjelmien torjunta, varmuuskopiointi sekä järjestelmien hallinta, ovat korkealla tasolla ja muodostavat vahvan perustan tietojen, järjestelmien ja palveluiden suojaamiselle. Myös tietoturvapolitiikat ja muut ohjaavat asiakirjat ovat pääosin olemassa ja johdon hyväksymiä, mikä tukee tietoturvan johtamista ja yhtenäisiä toimintamalleja.

Samanaikaisesti voidaan havaita, että tietoturvan toteutuksessa on eroja erityisesti niillä osa-alueilla, jotka liittyvät toiminnan jatkuvuuden varmistamiseen, kontrollien käytännön toteutukseen sekä niiden systemaattiseen todentamiseen. Kokonaisuutta tarkastellessa voi huomata, että tietoturva on siirtynyt perustason käyttöönotosta vaiheeseen, jossa painopiste on yhä enemmän toimivuuden varmistamisessa ja kyvykkyyden osoittamisessa.

3.4.2 Keskeiset havainnot

Tietoturvan vahvuudet painottuvat teknisiin ja rakenteellisiin ratkaisuihin. Haittaohjelmien torjunta on erittäin hyvällä tasolla, ja valtaosalla organisaatioista on käytössään tarvittavat tekniset ratkaisut uhkien tunnistamiseen ja estämiseen. Vastaavasti varmuuskopiointi toteutuu kattavasti, ja järjestelmät sekä laitteet ovat pääsääntöisesti hallitusti ylläpidettyjä. Myös haavoittuvuustiedotteiden seuranta ja niihin reagointi on organisaatioissa aktiivista, mikä tukee kykyä sopeutua nopeasti muuttuvaan uhkaympäristöön.

Käyttövaltuushallinnan osalta tilanne on kaksijakoinen. Vaikka käyttövaltuuksien hallintaan liittyvät periaatteet ja politiikat ovat pääosin olemassa, käyttöoikeuksien ajantasaisuuden säännöllinen varmistaminen ei ole samalla tasolla. Tämä viittaa siihen, että määritellyt toimintamallit eivät kaikilta osin toteudu käytännön operatiivisessa toiminnassa.

Jatkuvuudenhallinnan näkökulmasta merkittävin havainto liittyy varmuuskopioiden palauttamisen testaamiseen. Vaikka varmuuskopioita otetaan säännöllisesti, niiden palautettavuutta testataan huomattavasti harvemmin. Tämä muodostaa keskeisen riskin, sillä ilman säännöllistä testausta ei voida varmistua palautumiskyvystä todellisissa häiriötilanteissa.

Auditointikäytännöt muodostavat toisen selkeän kehityskohteen. Tietoturvaan ja tietojärjestelmiin liittyviä auditointeja tehdään suhteellisen vähän, mikä heikentää organisaatioiden kykyä arvioida kontrollien toimivuutta ja tunnistaa kehitystarpeita systemaattisesti. Samalla lokitietojen keruu ja hyödyntäminen on vain kohtalaisella tasolla, vaikka niiden merkitys korostuu tietoturvapoikkeamien havaitsemisessa ja selvittämisessä.

Tietoturvan inhimillinen ja toimitusketjuun liittyvä ulottuvuus näyttäytyy kokonaisuudessa heikompana. Henkilöstöön ja palvelutoimittajiin kohdistuvat taustatarkistukset ovat keskimäärin matalalla tasolla verrattuna muihin osa-alueisiin. Vaikka tietoturva- ja tietosuojavaatimuksia sisällytetään hankintoihin ja sopimuksiin melko kattavasti, niiden käytännön toteutuksessa ja valvonnassa on edelleen kehitettävää.

Etätyön turvallisuuskäytännöt ovat sen sijaan kehittyneet myönteisesti. Monivaiheinen tunnistautuminen ja VPN-yhteyksien käyttö ovat laajasti käytössä, mikä osoittaa, että organisaatiot ovat pystyneet vastaamaan hajautetun työn vaatimuksiin tietoturvan näkökulmasta.

3.4.3 Kehityssuunta

Vuoden 2025 ja 2026 vertailu osoittaa, että tietoturvan kehitys on ollut pääosin maltillista. Joillakin osa-alueilla, kuten käyttövaltuuksien ajantasaisuuden varmistamisessa, auditointien toteutuksessa ja lokitietojen keruussa, on nähtävissä lievää parannusta. Nämä muutokset viittaavat siihen, että organisaatiot ovat alkaneet kiinnittää enemmän huomiota kontrollien käytännön toimivuuteen.

Toisaalta useat keskeiset kehityskohteet, kuten varmuuskopioiden palautustestaus ja taustatarkistusten toteuttaminen, eivät ole kehittyneet merkittävästi, vaan ovat pysyneet ennallaan tai jopa hieman heikentyneet. Tämä kertoo siitä, että siirtymä perustason toteutuksesta kohti systemaattista varmistamista ja jatkuvaa kehittämistä on vielä kesken.

Kokonaisuudessaan kehityssuunta osoittaa, että tekninen tietoturva on saavuttanut melko kypsän tason, mutta hallinnollisten käytäntöjen ja jatkuvuuden varmistamisen kehittäminen etenee hitaammin.

3.4.4 Johtopäätökset

Tietoturvan nykytila muodostuu vahvasta teknisestä perustasta, jota tukevat toimivat keskeiset kontrollit ja laajasti käyttöönotetut suojamekanismit. Organisaatioilla on hyvät valmiudet torjua yleisimpiä uhkia ja ylläpitää tietojärjestelmiensä perusturvallisuutta.

Kehittämistarpeet kohdistuvat erityisesti siihen, miten näiden kontrollien toimivuus varmistetaan käytännössä ja miten organisaatiot voivat osoittaa tietoturvakykynsä häiriö- ja poikkeustilanteissa. Keskeisiä haasteita ovat jatkuvuudenhallinnan käytännöt, auditointien vähäisyys sekä henkilöstöön ja toimitusketjuun liittyvien riskien hallinta.

Kokonaiskuva viittaa siihen, että tietoturvan toteutus julkishallinnossa on siirtymässä vaiheeseen, jossa organisaatioiden tulee siirtyä yksittäisten ratkaisujen

käyttöönotosta kohti niiden vaikuttavuuden systemaattista todentamista, mittaamista ja jatkuvaa parantamista.

3.4.5 Kehittämissuositukset

Varmuuskopiot

Tietoturvan kehittämisessä keskeiseksi painopisteeksi nousee varmuuskopioiden palautustestauksen systematisointi siten, että palautumiskykyä harjoitellaan ja todennetaan säännöllisesti osana jatkuvuudenhallintaa.

Auditointi

Lisäksi organisaatioiden tulisi vahvistaa auditointikäytäntöjään ottamalla käyttöön suunnitelmallinen ja riskiperusteinen auditointiohjelma, jonka tuloksia hyödynnetään aktiivisesti toiminnan kehittämisessä.

Henkilöstö- ja toimittajaturvallisuus

Kolmantena keskeisenä kehittämiskohteena on henkilöstö- ja toimittajaturvallisuuden parantaminen, mikä edellyttää taustatarkistuskäytäntöjen laajentamista sekä tietoturvavaatimusten nykyistä systemaattisempaa seurantaa koko toimitusketjussa.

3.5 Tietosuoja

Taulukossa 6 esitetään tietosuojaosion 15 väittämän vastauskeskiarvot.

Taulukko 6. Tietosuoja – kysymyskohtaiset keskiarvot

Tietosuoja / Väittämä	Kaikki organisaatiot 203 kpl	Kunta 104 kpl	Kuntayhtymä 24 kpl	Hyvinvointialue ja muut Sotetoimijat 21 kpl	Korkeakoulu 10 kpl	Valtionhallinto 39 kpl	Muu 11 kpl
55. Organisaatiolla on tiedossa, mitä henkilötietoja se käsittelee (TsA 4 art. 1 kohta).	0,93 (0,92)	0,92 (0,91)	0,98 (0,95)	0,87 (0,85)	0,83 (0,88)	0,97 (0,97)	0,95 (0,98)
56. Henkilötietojen käsittelyn oikeusperusteet on tunnistettu (TsA 6, 9 ja 10 art. TsL 6 ja 29 §, TtsL 2, 3, 5 ja 6 luku).	0,93 (0,93)	0,91 (0,90)	0,96 (0,98)	0,94 (0,93)	0,90 (0,96)	0,95 (0,95)	0,93 (1,00)
57. Organisaatio on tunnistanut, milloin se toimii rekisterinpitäjänä ja milloin se toimii käsittelijänä (TsA 4 art. 7-8 kohta).	0,92 (0,92)	0,90 (0,89)	0,96 (0,99)	0,96 (0,94)	0,98 (0,96)	0,92 (0,92)	0,98 (1,00)
58. Sopimukset henkilötietojen käsittelystä on tehty ja sopimusten hallinta on	0,77 (0,78)	0,71 (0,70)	0,74 (0,81)	0,88 (0,83)	0,83 (0,79)	0,86 (0,85)	0,95 (1,00)

kunnossa (TsA 28 art).							
59. Yhteisrekisterinpitäjyystilanteet tunnistetaan ja yhteisrekisterinpitäjyyttä koskevista vastuista on sovittu (TsA 26 art., huom. myös EDPB:n ohje).	0,70 (0,74)	0,64 (0,64)	0,70 (0,74)	0,82 (0,79)	0,88 (0,88)	0,80 (0,82)	0,84 (0,89)
60. Henkilötietojen käsittelyyn liittyvät oman organisaation sisäiset roolit ja vastuut on tunnistettu ja vahvistettu (TihL 4.2. §, TsA 37 art.).	0,85 (0,85)	0,82 (0,80)	0,86 (0,93)	0,92 (0,93)	0,90 (0,84)	0,86 (0,84)	0,91 (0,90)
61. . Tietosuojavastaavan asema ja rooli on määritelty (TsA 37 – 39 art.).	0,93 (0,94)	0,92 (0,92)	0,95 (0,99)	0,94 (0,95)	0,93 (0,95)	0,96 (0,97)	0,98 (0,95)
62. Seloste käsittelytoimista on laadittu (TsA 30 art.).	0,79 (0,81)	0,74 (0,75)	0,84 (0,84)	0,82 (0,81)	0,78 (0,86)	0,86 (0,88)	0,91 (0,90)
63. Organisaatiolla on tiedossa missä tietojärjestelmissä henkilötietoja käsitellään.	0,89 (0,89)	0,87 (0,88)	0,97 (0,95)	0,83 (0,83)	0,88 (0,88)	0,90 (0,90)	0,95 (0,95)
64. Rakenteeton tieto on tunnistettu ja sen hallinta on kuvattu.	0,46 (0,47)	0,45 (0,45)	0,52 (0,52)	0,57 (0,50)	0,33 (0,39)	0,42 (0,49)	0,66 (0,63)
65. Informointikäytännöt on määritelty ja niitä noudatetaan (TsA 12-14 art. Laki digitaalisten palveluiden tarjoamisesta (306/2019).	0,77 (0,78)	0,71 (0,70)	0,75 (0,81)	0,86 (0,85)	0,88 (0,84)	0,84 (0,85)	0,90 (0,86)
66. Organisaatiolla on olemassa prosessi vaikutustenarvioinnin tarpeen tunnistamiseksi (TsA 35 (1) art.).	0,74 (0,71)	0,69 (0,63)	0,72 (0,64)	0,90 (0,90)	0,75 (0,86)	0,77 (0,74)	0,83 (0,86)
67. Organisaatiolla on olemassa henkilötietojen tietoturvaloukkausten hallintaprosessi (TsA 33-34 art.).	0,91 (0,92)	0,88 (0,89)	0,89 (0,89)	0,96 (0,96)	0,88 (0,96)	0,96 (0,96)	0,98 (0,95)
68. Jos henkilötietoja siirretään kolmansiin maihin, organisaatio on selvittänyt siirron edellytykset (TsA 5 luku).	0,73 (0,77)	0,67 (0,72)	0,62 (0,78)	0,83 (0,75)	0,78 (0,77)	0,88 (0,85)	0,81 (0,86)

69. Organisaatiossa tietosuojasta huolehtiminen on muuttunut toiminnaksi, kulttuuriksi ja asenteeksi (TSA 5 art.).	0,69 (0,69)	0,64 (0,63)	0,77 (0,75)	0,63 (0,60)	0,68 (0,64)	0,79 (0,78)	0,84 (0,83)

Tietosuojan kokonaiskuva vuoden 2026 arvioinnissa osoittaa, että organisaatioilla on vahva perusta henkilötietojen käsittelyn keskeisten vaatimusten hallinnassa. Valtaosassa organisaatioista on hyvä käsitys siitä, mitä henkilötietoja käsitellään, millä oikeusperusteilla käsittely tapahtuu sekä missä roolissa organisaatio toimii suhteessa henkilötietoihin. Myös tietosuojavastaavan rooli on pääosin selkeästi määritelty, ja tietoturvaloukkausten hallintaprosessit ovat laajasti käytössä.

Tämä viittaa siihen, että tietosuoja-asetuksen (GDPR) keskeiset vaatimukset on pääosin tunnistettu ja jalkautettu organisaatioiden toimintaan. Tietosuojan perusrakenteet ovat vakiintuneita, ja organisaatioilla on kyvykkyyttä hallita henkilötietojen käsittelyn keskeisiä osa-alueita.

Kokonaiskuvaa kuitenkin heikentää se, että tietosuojan käytännön toteutuksessa ja systemaattisessa hallinnassa esiintyy vaihtelua. Erityisesti tiedonhallinnan, sopimushallinnan ja jatkuvan kehittämisen osa-alueilla on havaittavissa puutteita, jotka vaikuttavat tietosuojan kypsyyteen.

3.5.1 Keskeiset havainnot

Tietosuojan vahvuudet liittyvät erityisesti henkilötietojen käsittelyn perusteiden hallintaan. Organisaatiot tunnistavat hyvin käsittelemänsä henkilötiedot, käsittelyn oikeusperusteet sekä rekisterinpitäjän ja käsittelijän roolit. Myös tietosuojavastaavan asema ja rooli ovat vakiintuneita, ja tietoturvaloukkausten hallintaan on olemassa toimivat prosessit.

Toisaalta sopimuksiin ja vastuiden määrittelyyn liittyy epäyhtenäisyyttä. Henkilötietojen käsittelyä koskevat sopimukset ovat pääosin kunnossa, mutta niiden hallinta ei ole kaikilta osin systemaattista. Erityisesti yhteisrekisterinpitäjyyteen liittyvien vastuiden tunnistaminen ja sopiminen jää keskimääräisesti heikommalle tasolle, mikä voi aiheuttaa epäselvyyttä vastuista käytännön tilanteissa.

Tietosuojan dokumentointi ja tiedonhallinta muodostavat keskeisen kehityskohteen. Selosteet käsittelytoimista ovat olemassa monissa organisaatioissa, mutta niiden ajantasaisuudessa ja kattavuudessa on vaihtelua. Lisäksi rakenteettoman tiedon tunnistaminen ja hallinta on selvästi heikoin osa-alue, mikä viittaa siihen, että organisaatioilla ei ole riittävää näkyvyyttä kaikkiin henkilötietojen käsittelyn muotoihin.

Vaikutustenarviointien (DPIA) osalta tunnistetaan, milloin arviointi on tarpeen, mutta käytännön toteutus ja systemaattisuus vaihtelevat. Informointikäytännöt ovat kohtuullisella tasolla, mutta eivät täysin yhdenmukaisia. Samoin henkilötietojen siirtoihin kolmansiin maihin liittyvät käytännöt ovat osin kehittymättömiä, mikä on merkittävää erityisesti kansainvälisiä palveluja käytettäessä.

Tietosuojakulttuurin osalta tulokset osoittavat, että tietosuoja ei ole vielä kaikissa organisaatioissa täysin juurtunut osaksi arjen toimintaa, johtamista ja

organisaatiokulttuuria. Tämä näkyy erityisesti siinä, että toiminta ei kaikilta osin ole systemaattista tai ennakoivaa, vaan perustuu osin yksittäisiin toimenpiteisiin.

3.5.2 Kehityssuunta

Vuoden 2025 ja 2026 vertailu osoittaa, että tietosuojan kehitys on kokonaisuutena vakaata, mutta edennyt vain rajallisesti. Useimmat vahvat osa-alueet, kuten henkilötietojen tunnistaminen, oikeusperusteiden määrittely sekä roolien selkeys, ovat pysyneet hyvällä tasolla ilman merkittäviä muutoksia. Tämä viittaa siihen, että perustason vaatimukset on saavutettu eikä niissä ole tapahtunut merkittäviä heilahteluja.

Joillakin osa-alueilla on nähtävissä lievää parannusta, kuten vaikutustenarviointiprosessin tunnistamisessa, mikä viittaa kasvavaan ymmärrykseen riskiperusteisen lähestymistavan merkityksestä.

Samanaikaisesti useilla keskeisillä kehityskohteilla on havaittavissa heikentymistä tai paikallaan pysymistä. Rakenteettoman tiedon hallinta on pysynyt matalalla tasolla, eikä siinä ole tapahtunut käytännössä kehitystä. Myös yhteisrekisterinpitäjyyteen, sopimushallintaan ja kolmansien maiden siirtoihin liittyvät käytännöt ovat paikoin heikentyneet.

Kokonaisuutena kehityssuunta osoittaa, että tietosuojassa on saavutettu vakaa perustaso, mutta siirtymä kohti systemaattisempaa, kattavampaa ja aidosti riskiperusteista toimintamallia etenee hitaasti.

3.5.3 Johtopäätökset

Tietosuojan nykytila heijastaa tilannetta, jossa organisaatioilla on vahva ymmärrys sääntelyn keskeisistä vaatimuksista ja niiden perusteet ovat pääosin kunnossa. Tämä luo hyvän pohjan henkilötietojen lainmukaiselle käsittelylle.

Keskeiset haasteet liittyvät kuitenkin kokonaisuuden hallintaan ja käytännön toteutuksen systemaattisuuteen. Tietosuojan dokumentointi, tiedonhallinta sekä sopimus- ja vastuukysymykset eivät ole kaikilta osin riittävän yhdenmukaisia. Erityisesti puutteet rakenteettoman tiedon hallinnassa ja toimitusketjuihin liittyvissä käytännöissä heikentävät näkyvyyttä ja hallintaa henkilötietojen käsittelyyn.

Lisäksi tietosuojan juurtuminen osaksi organisaatiokulttuuria on vielä kesken. Tämä näkyy siinä, että tietosuoja ei kaikilta osin toimi ennakoivana ja ohjaavana periaatteena, vaan toteutuu osin reaktiivisesti.

Kokonaiskuvan tulokset viittaavat siihen, että tietosuojan kehittämisessä siirrytään seuraavaan vaiheeseen, jossa painopiste on kokonaisvaltaisessa hallinnassa, jatkuvassa kehittämisessä ja tietosuojan integroimisessa osaksi kaikkea toimintaa.

3.5.4 Kehittämissuositukset

Tiedonhallinta ja dokumentointi

Tietosuojan kehittämisessä keskeiseksi suositukseksi nousee tiedonhallinnan vahvistaminen erityisesti rakenteettoman tiedon osalta, jotta organisaatioilla olisi kattava näkyvyys kaikkiin henkilötietojen käsittelytilanteisiin. Tähän liittyy myös selosteiden ja dokumentaation ajantasaisuuden varmistaminen.

Sopimukset ja vastuut

Toiseksi keskeiseksi kehittämiskohteeksi nousee sopimus- ja vastuunhallinnan systematisointi siten, että henkilötietojen käsittelyä koskevat sopimukset, yhteisrekisterinpitäjyyden vastuut sekä kansainväliset siirrot ovat selkeästi määriteltyjä ja hallittuja.

Kulttuurin kehittäminen

Kolmantena suosituksena on tietosuojakulttuurin vahvistaminen siten, että tietosuoja integroidaan nykyistä tiiviimmin osaksi organisaation johtamista, kehittämistä ja päivittäistä toimintaa. Tämä edellyttää jatkuvaa koulutusta, selkeitä toimintamalleja sekä johdon aktiivista ohjausta ja seurantaa.

3.6 Kyberturvallisuus

Kyberturvallisuus-osion 10 väittämän vastauskeskiarvot ovat taulukossa 7.

Taulukko 7. Kyberturvallisuus – kysymyskohtaiset keskiarvot

Kyberturvallisuus / Väittämä	Kaikki organisaatiot n. 206 kpl	Kunta 104 kpl	Kuntayhtymä 24 kpl	Hyvinvointialue ja muut Sotetoimijat 21 kpl	Korkeakoulu 10 kpl	Valtionhallinto 39 kpl	Muu 11 kpl
70. Organisaatio on huomioinut digitaalisen turvallisuuden osana kokonaisarkkitehtuuria.	0,74 (0,71)	0,70 (0,69)	0,77 (0,74)	0,75 (0,63)	0,68 (0,70)	0,77 (0,72)	0,93 (0,98)
71. Organisaatiolla on riittävät resurssit ja osaaminen digitaalisen turvallisuuden kehittämiseen osana kokonaisarkkitehtuuria.	0,55 (0,55)	0,45 (0,42)	0,67 (0,73)	0,53 (0,54)	0,65 (0,61)	0,62 (0,62)	0,80 (0,83)
73. Organisaatio on tunnistanut oman roolinsa YTS:n mukaisissa tehtävissä sekä kansallisesta että kansainvälisestä näkökulmasta.	0,73 (0,70)	0,65 (0,59)	0,63 (0,66)	0,86 (0,90)	0,73 (0,59)	0,88 (0,87)	0,80 (0,75)
74. Organisaatiossa on tunnistettu ne kriittiset palvelut, joilla on merkittävä vaikutus toisten organisaatioiden tai yhteiskunnan toimintaan.	0,82 (0,81)	0,78 (0,73)	0,84 (0,81)	0,87 (0,93)	0,82 (0,85)	0,87 (0,89)	0,91 (0,89)

75. Organisaatiossa on kattavasti tunnistettu kriittisten palveluiden riippuvuudet ulkoisista palvelutoimittajista.	0,76 (0,77)	0,72 (0,73)	0,84 (0,86)	0,80 (0,79)	0,68 (0,71)	0,80 (0,81)	0,86 (0,90)
76. Organisaation kriittisten palveluiden palveluntuottajien kanssa yhteistyössä arvioidaan ja hallitaan riskejä säännöllisesti.	0,56 (0,55)	0,53 (0,50)	0,48 (0,58)	0,63 (0,54)	0,40 (0,45)	0,63 (0,63)	0,77 (0,70)
77. Kriittisten toimittajien ja alihankkijoiden kanssa käsitellään digiturvallisuutta säännöllisesti toimittaja/palvelunhallintakokouksissa.	0,60 (0,59)	0,57 (0,55)	0,53 (0,65)	0,69 (0,70)	0,35 (0,36)	0,70 (0,68)	0,77 (0,70)
78. Organisaatio on varautunut ja laatinut suunnitelman siihen kohdistuvan mustamaalaus- tai vaikuttamiskampanjan varalta.	0,49 (0,47)	0,39 (0,36)	0,45 (0,36)	0,60 (0,56)	0,53 (0,50)	0,71 (0,63)	0,59 (0,53)
79. Organisaatio seuraa säännöllisesti toimintaympäristönsä digitaalisen turvallisuuden tilannekuvaa.	0,76 (0,73)	0,66 (0,63)	0,83 (0,76)	0,88 (0,83)	0,78 (0,68)	0,86 (0,82)	0,84 (0,85)
80. Organisaatiolla on toiminnalliset ja tekniset menettelyt tietojenkäsittely-ympäristönsä digitaalisen turvallisuuden valvontaan ja havainnointiin.	0,72 (0,66)	0,68 (0,60)	0,80 (0,73)	0,88 (0,78)	0,73 (0,66)	0.75 (0,68)	0,84 (0,80)

Kyberturvallisuuden kokonaiskuva vuoden 2026 arvioinnissa osoittaa, että organisaatioiden kyvykkyys hallita digitaaliseen toimintaympäristöön liittyviä riskejä on kehittynyt, mutta kokonaisuus on edelleen epätasainen. Monissa organisaatioissa kyberturvallisuus on huomioitu osana kokonaisarkkitehtuuria ja kriittiset palvelut on

tunnistettu, mikä luo perustan riskienhallinnalle ja varautumiselle. Lisäksi toimintaympäristön tilannekuvan seuranta sekä tekniset valvonta- ja havainnointikyvykkyydet ovat kohtalaisella tasolla ja kehittyneet edellisvuoteen verrattuna.

Kokonaiskuvaa kuitenkin heikentää se, että kyberturvallisuuden kehittämiseen liittyvät resurssit ja osaaminen eivät ole kaikissa organisaatioissa riittävät. Lisäksi riippuvuuksien hallinta ja yhteistyö toimittajien kanssa jäävät selvästi teknisiä kyvykkyyksiä heikommalle tasolle. Tämä viittaa siihen, että kyberturvallisuuden hallinta keskittyy edelleen pitkälti organisaation sisäisiin näkökulmiin, eikä ulkoisiin riippuvuuksiin liittyviä riskejä hallita vielä riittävän systemaattisesti.

3.6.1 Keskeiset havainnot

Kyberturvallisuuden vahvuudet liittyvät erityisesti toiminnan perusteiden tunnistamiseen. Organisaatiot ovat kohtuullisen hyvin huomioineet digitaalisen turvallisuuden osana kokonaisarkkitehtuuria, ja kriittiset palvelut on pääosin tunnistettu. Myös ymmärrys organisaation roolista yhteiskunnan turvallisuusstrategian mukaisissa tehtävissä on vahvistunut, mikä osoittaa kypsymistä strategisessa tarkastelussa.

Samoin toimintaympäristön tilannekuvaa seurataan aktiivisemmin kuin aiemmin, ja teknisiä sekä toiminnallisia valvonta- ja havainnointimenettelyjä on kehitetty. Tämä parantaa organisaatioiden kykyä havaita poikkeamia ja reagoida kyberuhkiin.

Sen sijaan merkittävimmät puutteet liittyvät resurssien ja osaamisen riittävyyteen. Arvioiden perusteella monilla organisaatioilla ei ole riittäviä valmiuksia kehittää kyberturvallisuutta osana kokonaisarkkitehtuuria, mikä hidastaa kyvykkyyksien systemaattista kehittämistä ja ylläpitoa.

Toinen keskeinen kehityskohde liittyy toimitusketjujen hallintaan. Vaikka kriittisten palveluiden riippuvuudet ulkoisista toimittajista tunnistetaan melko hyvin, riskien arviointi ja hallinta yhteistyössä palveluntuottajien kanssa jää vähäiseksi. Myös säännöllinen kyberturvallisuuden käsittely toimittajien kanssa ei ole vakiintunut käytäntö. Tämä muodostaa merkittävän riskin, sillä ulkoiset palvelut ja kumppanit ovat keskeinen osa organisaatioiden toimintaa.

Lisäksi organisaatioiden varautuminen informaatio- ja vaikuttamiskampanjoihin on heikolla tasolla. Mustamaalaus- tai vaikuttamiskampanjoihin varautuminen on yksi heikoimmin toteutuneista osa-alueista. Tämä viittaa siihen, että kyberturvallisuuden laajempi hybridiuhkien näkökulma ei ole vielä täysin integroitunut organisaatioiden varautumiseen.

3.6.2 Kehityssuunta

Vuoden 2025 ja 2026 vertailu osoittaa, että kyberturvallisuudessa on tapahtunut pääosin maltillista kehitystä, mutta edistys on kohdentunut epätasaisesti eri osa-alueille. Positiivista kehitystä on nähtävissä erityisesti kokonaisarkkitehtuurin huomioimisessa, organisaation roolin tunnistamisessa sekä tilannekuvan seurannassa. Myös valvonta- ja havainnointikyvykkyydet ovat parantuneet, mikä viittaa kasvaneeseen painotukseen operatiivisessa kyberturvallisuudessa.

Toisaalta resurssien ja osaamisen riittävyydessä ei ole tapahtunut parannusta, vaan tilanne on pysynyt ennallaan. Tämä muodostaa merkittävän pullonkaulan kyberturvallisuuden kehittämiselle.

Toimitusketjujen hallintaan liittyvissä käytännöissä kehitys on ristiriitaista. Riippuvuuksien tunnistaminen on pysynyt melko hyvällä tasolla, mutta yhteistyöhön ja riskienhallintaan liittyvät käytännöt eivät ole merkittävästi kehittyneet, ja paikoin niissä on jopa heikentymistä.

Varautuminen vaikuttamiskampanjoihin on hieman parantunut, mutta jää edelleen matalalle tasolle. Tämä osoittaa, että kyberturvallisuuden laajempi yhteiskunnallinen ulottuvuus ei ole vielä kehittynyt samassa tahdissa teknisten kyvykkyyksien kanssa.

3.6.3 Johtopäätökset

Kyberturvallisuuden nykytila kuvastaa vaihetta, jossa organisaatioilla on kohtalaiset valmiudet tunnistaa keskeiset riskit ja suojata omaa toimintaansa, mutta kyvykkyys hallita laajempia, verkottuneeseen toimintaympäristöön liittyviä riskejä on vielä puutteellinen.

Tekniset ja operatiiviset kyvykkyydet ovat kehittyneet, ja tilannekuvan ylläpito sekä valvonta ovat parantuneet. Tämä vahvistaa organisaatioiden kykyä reagoida kyberuhkiin.

Keskeiset haasteet liittyvät kuitenkin resurssien riittävyyteen, osaamiseen sekä erityisesti toimitusketjujen ja kumppaniverkoston hallintaan. Näiden osa-alueiden puutteet heikentävät kokonaisvaltaista kyberturvallisuuden tasoa ja altistavat organisaatiot epäsuorille riskeille.

Lisäksi varautuminen hybridiuhkiin, kuten vaikuttamiskampanjoihin, on vielä kehittymätöntä. Tämä osoittaa, että kyberturvallisuutta ei vielä kaikilta osin tarkastella osana laajempaa turvallisuusympäristöä.

Kokonaisuudessaan kehityksen seuraava vaihe edellyttää siirtymistä teknisestä ja organisaatiokeskeisestä näkökulmasta kohti verkottunutta, riskiperusteista ja ennakoivaa kyberturvallisuuden hallintaa.

3.6.4 Kehittämissuositukset

Resurssit ja osaamisen kehittäminen

Kyberturvallisuuden kehittämisessä keskeiseksi suositukseksi nousee resurssien ja osaamisen vahvistaminen siten, että kyberturvallisuus voidaan integroida systemaattisesti osaksi organisaation kokonaisarkkitehtuuria ja kehittämistoimintaa. Tämä edellyttää sekä osaamisen kehittämistä että riittävien resurssien kohdentamista pitkäjänteisesti.

Toimitusketjujen hallinta

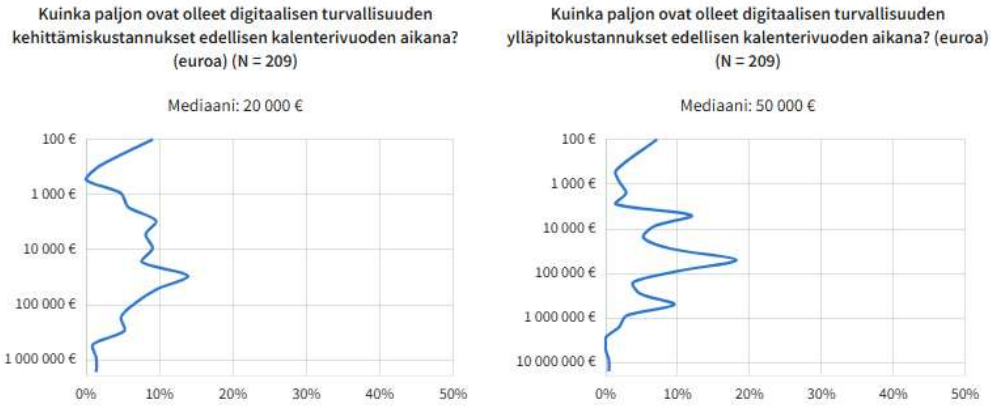
Toiseksi keskeiseksi kehittämiskohteeksi nousee toimitusketjujen ja kumppanuuksien hallinnan vahvistaminen. Organisaatioiden tulisi kehittää käytäntöjä, joilla kriittisten toimittajien kanssa tehtävää riskienhallintaa, seurantaa ja yhteistyötä toteutetaan säännöllisesti ja systemaattisesti.

Varautuminen hybridiuhkiin

Kolmantena suosituksena on varautumisen laajentaminen kattamaan myös hybridiuhat ja vaikuttamiskampanjat. Tämä edellyttää selkeitä toimintamalleja, viestinnällistä varautumista sekä kyvykkyyttä seurata ja analysoida toimintaympäristön muutoksia myös informaatioympäristön näkökulmasta.

3.7 Rahalliset ja ajalliset panostukset

Kuva 4 digitaalisen turvallisuuden kehittämis- ja ylläpitokustannukset



Digitaalisen turvallisuuden kehittämiskustannukset sekä ylläpitokustannukset edellisen kalenterivuoden aikana (N = 209) on esitetty kuvassa 4. Molempien jakaumat ovat selvästi oikealle vinoja, mikä tarkoittaa, että suurin osa organisaatioista sijoittuu suhteellisen alhaisiin kustannuksiin, mutta pieni joukko organisaatioita käyttää huomattavasti suurempia summia.

Kehittämiskustannusten mediaani on 20 000 euroa, kun taas ylläpitokustannusten mediaani on 50 000 euroa. Tämä osoittaa, että jatkuva ylläpito on keskimäärin selvästi kehittämistä suurempi kustannuserä organisaatioille.

3.7.1 Keskeiset havainnot

Kehittämiskustannusten jakauma osoittaa, että valtaosa organisaatioista sijoittuu alle 50 000 euron tasolle, ja suurin keskittymä näyttää olevan erityisesti 5 000–30 000 euron välillä. Pienempi joukko organisaatioita investoi kehittämiseen huomattavasti enemmän, jopa satoja tuhansia euroja, mutta nämä muodostavat selvästi pienemmän osuuden kokonaisuudesta. Tämä viittaa siihen, että kehittämistoimenpiteet ovat monissa organisaatioissa melko rajattuja ja kohdennettuja, eikä laaja-alaisia investointeja tehdä laajasti.

Ylläpitokustannusten jakauma poikkeaa tästä jonkin verran. Vaikka myös ylläpitokustannuksissa suurin osa organisaatioista sijoittuu alle 100 000 euron tasolle, jakauma on leveämpi ja ulottuu useammin korkeampiin kustannusluokkiin. Merkittävä osa organisaatioista sijoittuu noin 20 000–100 000 euron väliin. Lisäksi joukossa on selvästi

enemmän organisaatioita, joiden kustannukset ylittävät 100 000 euroa tai jopa lähestyvät miljoonan euron tasoa.

Tämä viittaa siihen, että digitaalisen turvallisuuden ylläpito vaatii jatkuvia, ja usein merkittäviä panostuksia. Nämä panostukset voivat koostua esimerkiksi palveluista, valvonnasta, lisensseistä ja henkilöstöresursseista. Kehittäminen on sen sijaan luonteeltaan enemmän kertaluonteista tai projektimuotoista.

3.7.2 Kustannusrakenteen tulkinta

Kokonaisuutena kustannusrakenne kertoo painopisteen olevan ylläpidossa. Koska ylläpitokustannukset ylittävät kehittämiskustannukset mediaanitasolla yli kaksinkertaisesti, organisaatiot käyttävät enemmän resursseja olemassa olevien ratkaisujen ylläpitämiseen kuin uusien kyvykkyyksien kehittämiseen.

Jakaumien muoto korostaa myös organisaatioiden välistä eriytymistä. Osa organisaatioista toimii hyvin pienillä panostuksilla, kun taas toisilla kustannukset ovat moninkertaiset. Tämä voi heijastaa eroja toiminnan laajuudessa, kriittisyydessä, riskitasossa tai kypsyystasossa digitaalisen turvallisuuden hallinnassa.

3.7.3 Johtopäätökset

Tulosten perusteella digitaalisen turvallisuuden rahoitus painottuu selvästi jatkuvaan operatiiviseen toimintaan, kun taas kehittämiseen kohdistuvat panostukset ovat keskimäärin pienempiä ja keskittyvät rajatumpiin toimenpiteisiin. Tämä voi pitkällä aikavälillä hidastaa kyvykkyyksien kehittymistä, mikäli kehittämiseen ei kohdenneta riittäviä resursseja suhteessa toimintaympäristön kasvaviin vaatimuksiin.

Lisäksi kustannusten suuri vaihtelu viittaa siihen, että organisaatioiden välillä on merkittäviä eroja siinä, miten digitaaliseen turvallisuuteen panostetaan. Tämä voi tarkoittaa, että osa organisaatioista on edelleen kehityksen alkuvaiheessa, kun taas toisilla turvallisuus on jo integroitunut kiinteäksi osaksi toimintaa.

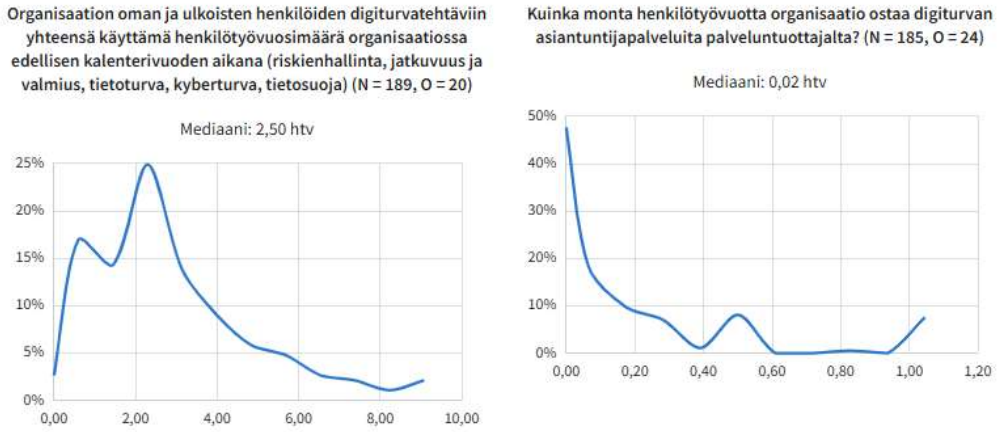
3.7.4 Kehittämisnäkökulmat

Tulosten perusteella keskeiseksi kehittämistarpeeksi nousee kustannusten tasapainottaminen siten, että myös kehittämiseen kohdennetaan riittävästi resursseja suhteessa ylläpitoon. Samalla on tärkeää varmistaa, että ylläpitokustannukset ovat hallittuja ja perustuvat aidosti riskienhallinnan tarpeisiin.

Lisäksi organisaatioiden tulisi tarkastella kustannusrakennettaan suhteessa omaan riskiprofiiliinsa ja toiminnan kriittisyyteen, jotta panostukset kohdentuvat tarkoituksenmukaisesti. Erityisesti pienempien panostusten organisaatioissa tulisi varmistaa, että vähäiset resurssit kohdistuvat tehokkaasti keskeisimpiin tietoturva- ja kyberturvallisuustoimenpiteisiin.

3.8 Henkilöresurssit

Kuva 5 organisaatioiden omat ja ostetut henkilöresurssit



Yllä olevassa kuvassa esitetään kahden eri näkökulman kautta digiturvan henkilöstöresurssien käyttö organisaatioissa edellisen kalenterivuoden aikana. Vasemmanpuoleinen jakauma kuvaa organisaation omien ja ulkoisten henkilöiden yhteenlaskettua työpanosta digiturvatehtäviin henkilötyövuosina (N = 189, joista 20 raportoi arvon 0). Oikeanpuoleinen jakauma puolestaan kuvaa erikseen ulkoisina asiantuntijapalveluina ostettua työpanosta henkilötyövuosina (N = 185, joista 24 raportoi arvon 0).

Kokonaisresursoinnin mediaani on 2,50 henkilötyövuotta, kun taas ulkoisten asiantuntijapalveluiden mediaani on hyvin pieni, 0,02 henkilötyövuotta. Tämä osoittaa, että digiturvatyö perustuu ensisijaisesti organisaatioiden omaan henkilöstöön, ja ulkoista työpanosta hyödynnetään keskimäärin rajallisesti.

3.8.1 Keskeiset havainnot

Kokonaisresursoinnin jakauma osoittaa, että suurin osa organisaatioista sijoittuu noin 1–4 henkilötyövuoden väliin. Selkeä huippu on havaittavissa noin 2 henkilötyövuoden kohdalla, minkä ympärille merkittävä osa havainnoista keskittyy. Tämä viittaa siihen, että tyypillinen organisaatio osoittaa digiturvatehtäviin melko rajatun mutta kuitenkin selkeästi erillisen resurssin.

Jakauman muoto on oikealle vino, ja häntä ulottuu jopa noin 8–10 henkilötyövuoteen asti. Tämä tarkoittaa, että pieni joukko organisaatioita panostaa digiturvaan huomattavasti enemmän resursseja. Tämä voi liittyä esimerkiksi organisaation kokoon, toiminnan kriittisyyteen tai kypsyystasoon. Samanaikaisesti mukana on myös organisaatioita, joissa digiturvatehtäviin ei ole kohdennettu lainkaan erillistä resurssia, mikä korostaa suurta vaihtelua organisaatioiden välillä.

Ulkoisten asiantuntijapalveluiden osalta jakauma on vielä selkeämmin painottunut hyvin pieniin arvoihin. Lähes puolet havainnoista sijoittuu hyvin lähelle nollaa, ja suuri osa organisaatioista käyttää ulkoista työpanosta vain hyvin vähän tai ei lainkaan. Pieni nousu jakaumassa noin 0,3–0,6 henkilötyövuoden kohdalla viittaa siihen, että

osa organisaatioista hyödyntää ulkoisia asiantuntijoita säännöllisemmin, mutta nämä tapaukset ovat vähemmistössä.

Jakauman oikea häntä ulottuu noin yhteen henkilötyövuoteen, mikä osoittaa, että joissakin organisaatioissa ulkoinen työpanos muodostaa merkittävän osan digiturvan resursseista. Nämä organisaatiot erottuvat selvästi joukosta.

3.8.2 Resurssirakenteen tulkinta

Kokonaiskuva osoittaa, että digiturvan resursointi perustuu pääosin organisaation omiin henkilöihin. Ulkoisten asiantuntijapalveluiden rooli on keskimäärin täydentävä, ei keskeinen. Tämä viittaa siihen, että digiturvaa pidetään ydinosaamisalueena, jota ylläpidetään ensisijaisesti omilla resursseilla.

Samalla jakaumat paljastavat kaksi erilaista toimintamallia. Suurin osa organisaatioista toimii rajallisilla mutta vakiintuneilla sisäisillä resursseilla ja käyttää ulkoista tukea satunnaisesti. Toisaalta pienempi joukko organisaatioita rakentaa digiturvaa selvästi laajemmalla resurssipohjalla ja hyödyntää myös ulkoisia asiantuntijoita merkittävässä määrin.

Nollavastausten esiintyminen molemmissa jakaumissa on merkittävä havainto. Se viittaa siihen, että osassa organisaatioista digiturvatehtäviä ei ole resursoitu erillisinä kokonaisuuksina, vaan ne voivat olla hajautuneina muiden tehtävien yhteyteen tai hoitamatta systemaattisesti.

3.8.3 Johtopäätökset

Tulokset osoittavat, että digiturvan resursointi on useimmissa organisaatioissa melko rajallista, mutta kuitenkin olemassa olevaa ja vakiintunutta. Keskimääräinen taso viittaa siihen, että digiturvaa hoidetaan pienillä asiantuntijatiimeillä, mikä voi olla riittävä perustasolla, mutta muodostaa haasteita toimintaympäristön vaatimusten kasvaessa.

Merkittävä vaihtelu organisaatioiden välillä kertoo eritasoisesta kypsyydestä ja priorisoinnista. Osa organisaatioista panostaa digiturvaan merkittävästi enemmän, mikä voi parantaa niiden kykyä hallita riskejä ja kehittää toimintaansa. Toisaalta hyvin matalat resurssitasot ja nollavastaukset viittaavat siihen, että kaikilla organisaatioilla ei ole riittäviä valmiuksia vastata digitaalisen turvallisuuden vaatimuksiin.

Ulkoisten asiantuntijapalveluiden vähäinen käyttö korostaa sitä, että organisaatioiden on pitkälti kyettävä toimimaan omalla osaamisellaan. Tämä voi olla haaste erityisesti tilanteissa, joissa tarvitaan syvällistä erityisosaamista tai kykyä vastata nopeasti kehittyviin uhkiin.

3.8.4 Kehittämisnäkökulmat

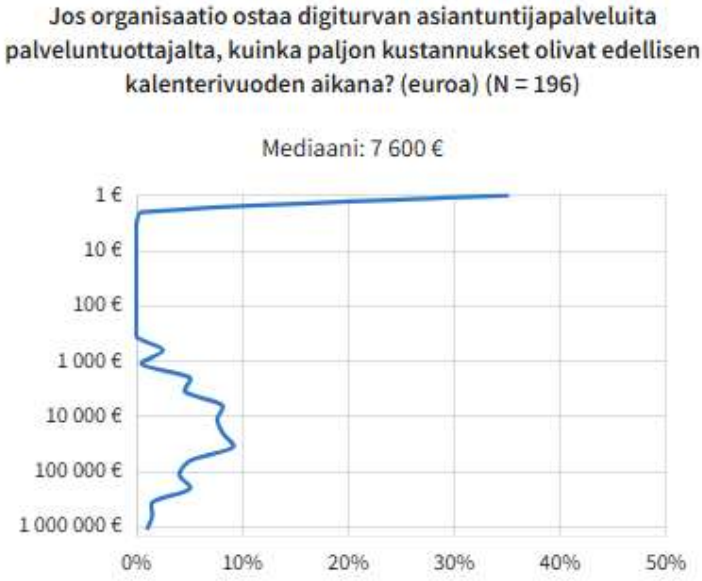
Tulosten perusteella keskeiseksi kehittämiskohteeksi nousee digiturvan resurssien riittävyyden varmistaminen suhteessa organisaation riskitasoon ja toiminnan kriittisyyteen. Resursoinnin tulisi perustua systemaattiseen arvioon tarvittavasta osaamisesta ja työmäärästä, ei pelkästään historiallisiin rakenteisiin.

Lisäksi organisaatioiden tulisi tarkastella sisäisten ja ulkoisten resurssien tasapainoa. Ulkoisten asiantuntijapalveluiden hyödyntäminen voi täydentää omaa osaamista

erityisesti vaativissa tai tilapäisissä tarpeissa, mutta edellyttää suunnitelmallista käyttöä ja selkeää roolitusta.

Kokonaisuutena kehittämisen painopisteenä tulisi olla resursoinnin vahvistaminen ja joustavuuden lisääminen siten, että organisaatiot pystyvät vastaamaan sekä päivittäisiin tietoturvavaatimuksiin että nopeasti muuttuviin kyberturvallisuusuhkiin.

3.9 Asiantuntijapalveluiden hankinta



.

Kuva 5 digiturvan ostopalveluihin käytetyt kustannukset ja mediaani

Yllä olevassa kuvassa esitetään organisaatioiden digiturvan asiantuntijapalveluihin kohdistuvat kustannukset edellisen kalenterivuoden aikana (N = 196). Jakauma on selvästi oikealle vino, mikä tarkoittaa, että suurin osa organisaatioista käyttää asiantuntijapalveluihin melko pieniä summia, mutta pieni joukko organisaatioita investoi niihin huomattavasti enemmän.

Kustannusten mediaani on 7 600 euroa, mikä osoittaa, että yli puolet organisaatioista sijoittuu alle tämän tason. Verrattuna kokonaisiin kehittämis- ja ylläpitokustannuksiin asiantuntijapalveluiden osuus näyttäytyy keskimäärin melko kohtuullisena, mutta niiden merkitys voi olla kriittinen erityisosaamista vaativissa tilanteissa.

3.9.1 Keskeiset havainnot

Jakauman tarkastelu osoittaa, että merkittävä osa organisaatioista sijoittuu hyvin mataliin kustannusluokkiin, usein alle 10 000 euroon. Erityisen tiheä keskittymä on havaittavissa muutaman tuhannen euron tasolla sekä mediaanin läheisyydessä. Tämä viittaa siihen, että asiantuntijapalveluja hyödynnetään monessa organisaatiossa rajatusti, esimerkiksi yksittäisiin selvityksiin, auditointeihin tai konsultointiin.

Samalla jakauman alaosassa, erityisesti alle 1 000 euron tasolla, on suuri joukko organisaatioita, mikä voi viitata siihen, että osa organisaatioista käyttää ulkoisia asiantuntijapalveluja vain satunnaisesti tai hyvin rajatusti, tai vaihtoehtoisesti tukeutuu pääasiassa sisäiseen osaamiseen.

Jakauman häntä ulottuu kuitenkin huomattavasti korkeammille kustannustasoille, aina kymmeniin tai jopa satoihin tuhansiin euroihin saakka. Tämä osoittaa, että pieni joukko organisaatioita hyödyntää asiantuntijapalveluja laajasti, esimerkiksi jatkuvana palveluna, laajoissa kehittämishankkeissa tai vaativissa tietoturva- ja kyberturvallisuustilanteissa.

3.9.2 Kustannusrakenteen tulkinta

Kokonaisuutena jakauma kuvastaa kahta erilaista toimintamallia asiantuntijapalveluiden hyödyntämisessä. Suurin osa organisaatioista käyttää palveluja täydentävänä resurssina, usein tarveperusteisesti ja rajattuihin kokonaisuuksiin. Tällöin kustannukset pysyvät suhteellisen matalina.

Toisaalta pienempi joukko organisaatioita hyödyntää asiantuntijapalveluja systemaattisemmin ja laajamittaisemmin. Näissä tapauksissa ulkoiset palvelut voivat olla keskeinen osa organisaation digiturvan toteutusta, esimerkiksi jatkuvan valvonnan, kehittämisen tai erityisosaamisen hankinnan näkökulmasta.

Jakauman muoto viittaa myös siihen, että organisaatioiden välillä on merkittäviä eroja osaamisessa, resursoinnissa ja toimintamalleissa. Organisaatiot, joilla on vähemmän omaa asiantuntemusta, voivat tukeutua enemmän ulkoisiin palveluihin, kun taas osa organisaatioista hoitaa vastaavat tehtävät pääosin omilla resursseillaan.

3.9.3 Johtopäätökset

Tulosten perusteella digiturvan asiantuntijapalveluiden käyttö on yleistä, mutta useimmiten rajattua. Valtaosa organisaatioista hyödyntää ulkopuolista osaamista täydentävästi, eikä palveluiden käyttö muodostu merkittäväksi kustannuseräksi kokonaisbudjetissa.

Samalla havaitaan, että organisaatioiden välillä on merkittäviä eroja siinä, miten asiantuntijapalveluja hyödynnetään. Pieni osa organisaatioista tekee huomattavia panostuksia ulkoisiin palveluihin, mikä voi viitata joko korkeampiin vaatimuksiin, suurempaan riskiprofiiliin tai vähäisempään sisäiseen osaamiseen.

Kokonaiskuva viittaa siihen, että asiantuntijapalveluiden rooli digiturvassa on kasvava, mutta niiden käyttö ei ole vielä täysin systemaattista kaikissa organisaatioissa. Palveluiden hyödyntäminen vaihtelee riippuen organisaation kypsyydestä, koosta ja toimintaympäristöstä.

3.9.4 Kehittämisnäkökulmat

Tulosten perusteella keskeiseksi kehittämiskohteeksi nousee asiantuntijapalveluiden tarkoituksenmukainen ja strateginen hyödyntäminen. Organisaatioiden tulisi arvioida, missä tilanteissa ulkoinen osaaminen tuo eniten lisäarvoa, ja varmistaa, että palveluiden käyttö tukee pitkäjänteistä kehittämistä eikä jää yksittäisiksi toimenpiteiksi.

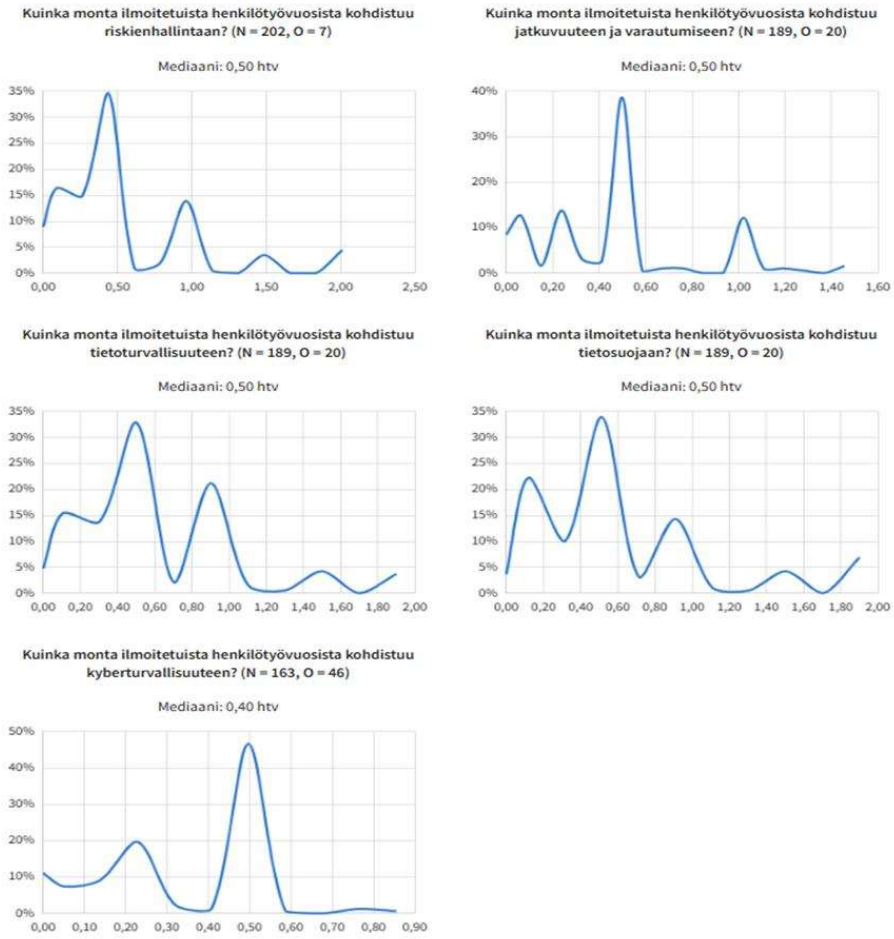
Lisäksi organisaatioiden on tärkeää tasapainottaa sisäisen osaamisen ja ulkopuolisten palveluiden käyttöä. Riittävä oma osaaminen mahdollistaa tehokkaan yhteistyön palveluntuottajien kanssa ja varmistaa, että hankittu asiantuntijatuki voidaan hyödyntää täysimääräisesti.

Kokonaisuutena tarkastellen asiantuntijapalveluiden käytön kehittäminen edellyttää siirtymistä satunnaisesta hyödyntämisestä kohti suunnitelmallista ja riskiperusteista toimintamallia, jossa ulkoinen osaaminen integroidaan osaksi organisaation digiturvan kokonaisuutta.

3.10 Digiturvan resurssit osa-aluekohtaisesti

Alla olevassa kuvassa esitetään digiturvan henkilötyövuosien jakautuminen viiteen keskeiseen osa-alueeseen: riskienhallintaan, jatkuvuuteen ja varautumiseen, tietoturvallisuuteen, tietosuojaan sekä kyberturvallisuuteen. Kaikissa tarkastelluissa osa-alueissa mediaani sijoittuu hyvin lähelle toisiaan, pääosin 0,50 henkilötyövuoteen, poikkeuksena kyberturvallisuus, jossa mediaani on hieman alhaisempi, 0,40 henkilötyövuotta.

Jakaumat ovat kaikissa osa-alueissa oikealle vinoja, mikä osoittaa, että suurin osa organisaatioista kohdentaa kuhunkin osa-alueeseen melko rajallisen työpanoksen, mutta pienempi joukko organisaatioita panostaa selvästi enemmän resursseja. Lisäksi kaikissa osa-alueissa esiintyy jonkin verran nollavastauksia, mikä tarkoittaa, että kaikissa organisaatioissa ei ole kohdennettu erillistä resurssia kyseisiin tehtäviin.



Kuva 6 digiturvan eri osa-alueisiin käytetyt henkilöresurssit

3.10.1 Keskeiset havainnot

Riskienhallinnan osalta jakauma keskittyy voimakkaasti noin 0,3–0,6 henkilötyövuoden tasolle, jossa myös mediaani sijaitsee. Jakaumassa on kuitenkin nähtävissä toinen pienempi keskittymä noin yhden henkilötyövuoden kohdalla, mikä viittaa siihen, että osa organisaatioista on panostanut riskienhallintaan selvästi enemmän. Samalla pieni joukko organisaatioita sijoittuu huomattavasti tätä korkeammille tasoille, mikä korostaa eroja organisaatioiden lähestymistavoissa.

Jatkuvuuden ja varautumisen osalta jakauma on samankaltainen, mutta hieman hajanaisempi. Keskeinen huippu on selvästi median lähellä 0,5 henkilötyövuotta, mutta jakaumassa on lisäksi pienempiä keskittymiä sekä alemmilla että hieman korkeammilla tasoilla. Tämä viittaa siihen, että jatkuvuudenhallinta on monissa organisaatioissa tunnistettu tärkeäksi, mutta resurssien kohdentaminen vaihtelee merkittävästi.

Tietoturvallisuuden ja tietosuojan osalta jakaumat ovat hyvin samankaltaisia ja suhteellisen tasapainoisia verrattuna muihin osa-alueisiin. Molemmissa näkyy selkeä päähuippu median ympärillä sekä toinen, pienempi keskittymä hieman korkeammalla tasolla. Tämä viittaa siihen, että nämä osa-alueet ovat kehittyneet ja vakiintuneet osaksi organisaatioiden normaalia toimintaa, mutta resurssien taso pysyy edelleen melko rajallisena.

Kyberturvallisuuden jakauma poikkeaa muista osa-alueista. Vaikka myös tässä keskeinen keskittymä on lähellä 0,4–0,5 henkilötyövuotta, jakauma on jyrkempi ja keskittyneempi. Suurin osa organisaatioista sijoittuu hyvin kapealle vaihteluvälille, ja korkeampien resurssitasojen esiintyminen on vähäisempää. Tämä viittaa siihen, että kyberturvallisuuden resursointi on monissa organisaatioissa vielä varsin niukkaa ja vähemmän kehittynyttä kuin muilla osa-alueilla.

3.10.2 Resurssien kohdentumisen tulkinta

Kokonaisuutena tarkasteltuna resurssien kohdentuminen eri osa-alueille on melko tasapainoista mediaanitasolla, mutta jakaumat paljastavat merkittäviä eroja organisaatioiden välillä. Useimmissa organisaatioissa kukin osa-alue saa suhteellisen pienen, noin puolen henkilötyövuoden suuruisen panostuksen, mikä viittaa siihen, että vastuut voivat olla yhdistettyinä samaan rooliin tai jakautuneina useiden henkilöiden kesken.

Toisaalta jakaumien leveys ja useat paikalliset huiput osoittavat, että osa organisaatioista on valinnut selvästi erilaisen lähestymistavan ja kohdentaa enemmän resursseja tietyille osa-alueille. Tämä voi heijastaa organisaation toiminnan luonnetta, riskiprofiilia tai kypsyystasoa.

Erityisesti kyberturvallisuuden muita osa-alueita matalampi mediaani viittaa siihen, että kyberturvallisuus ei vielä kaikilta osin ole yhtä vahvasti resursoitu kuin tietoturva, tietosuoja tai riskienhallinta. Tämä on merkityksellistä, koska kyberturvallisuus muodostaa keskeisen osan digitaalisen toimintaympäristön kokonaisturvallisuutta.

3.10.3 Johtopäätökset

Tulokset osoittavat, että digiturvan osa-alueiden resursointi on useimmiten hajautettua ja perustuu suhteellisen pieniin yksittäisiin panostuksiin. Vaikka kokonaisuutena

eri osa-alueet ovat huomioitu, resurssitaso voi olla haasteellinen suhteessa kasvaviin vaatimuksiin ja uhkiin.

Organisaatioiden välinen vaihtelu on merkittävää, mikä viittaa eritasoiseen kypsyyteen ja priorisointiin. Osa organisaatioista on panostanut selvästi enemmän tiettyihin osa-alueisiin, kun taas toisissa resursointi on hyvin vähäistä tai puuttuu kokonaan.

Kyberturvallisuuden suhteellisesti alhaisempi resursointi on keskeinen havainto, joka voi heikentää organisaatioiden kykyä vastata kehittyviin ja yhä monimutkaisempiin kyberuhkiin. Samanaikaisesti riskienhallinnan, tietoturvan ja tietosuojan tasainen mutta varsin maltillinen resursointi viittaa siihen, että digiturvaa hoidetaan usein minimiresurssein.

3.10.4 Kehittämisnäkökulmat

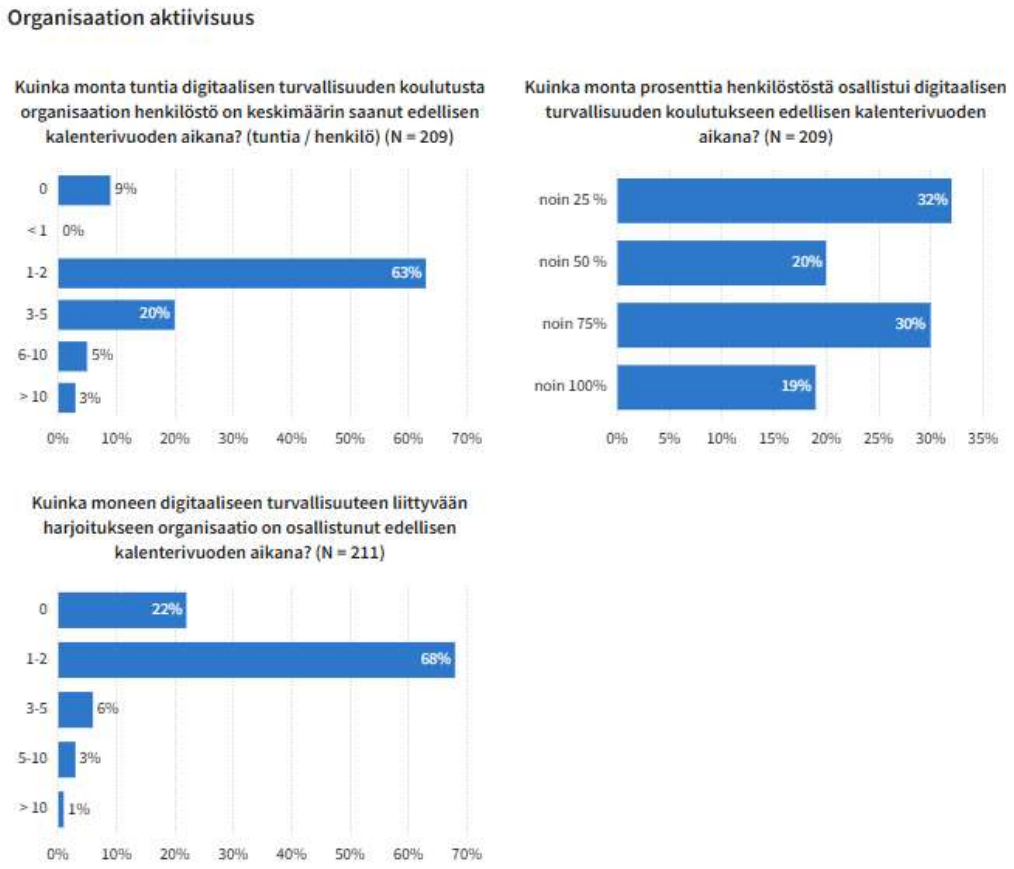
Keskeiseksi kehittämistarpeeksi nousee resurssien kohdentamisen tarkastelu kokonaisuutena siten, että eri osa-alueiden välinen tasapaino vastaa organisaation riskitasoa ja toimintaympäristöä. Erityisesti kyberturvallisuuden resursointia tulisi vahvistaa vastaamaan sen kasvavaa merkitystä.

Lisäksi organisaatioiden tulisi arvioida, ovatko nykyiset resurssitasot riittäviä vai perustuuko toiminta osittain alimitoitettuun resursointiin. Tämä korostaa tarvetta siirtyä kohti systemaattisempaa ja riskiperusteista resursointimallia.

Kokonaisuutena tarkastellen kehittämisen painopisteenä tulisi olla resurssien vahvistaminen, kohdentamisen selkeyttäminen sekä osa-alueiden välisen koordinaation parantaminen, jotta digiturva muodostaa yhtenäisen ja vaikuttavan kokonaisuuden.

3.11 Osaamisen kehittäminen

Kuva 7 Organisaatioiden digiturvakoulutukset ja harjoittelu



Yllä olevassa kuvassa esitetään organisaatioiden aktiivisuutta digitaalisen turvallisuuden kehittämisessä kolmen näkökulman kautta: henkilöstön saama koulutus, koulutukseen osallistuneen henkilöstön osuus sekä osallistuminen digiturvaa koskeviin harjoituksiin edellisen kalenterivuoden aikana. Tulokset osoittavat, että digiturvaan liittyvää toimintaa toteutetaan organisaatioissa melko laajasti, mutta toiminnan intensiteetti ja kattavuus vaihtelevat merkittävästi.

Kokonaisuutena tarkasteltuna koulutus ja harjoittelu ovat vakiintunut osa toimintaa useimmissa organisaatioissa, mutta toteutus jää usein määrällisesti varsin rajalliselle tasolle.

3.11.1 Keskeiset havainnot

Digitaalisen turvallisuuden koulutuksen määrää tarkasteltaessa havaitaan, että selvästi suurin osa organisaatioista sijoittuu luokkaan 1–2 tuntia henkilöä kohden vuodessa. Tähän ryhmään kuuluu noin 63 prosenttia organisaatioista. Seuraavaksi suurin ryhmä on 3–5 tunnin tasolla, jossa on noin 20 prosenttia organisaatioista. Tätä

suuremmat koulutusmäärät ovat selvästi harvinaisempia: 6–10 tuntia koskee noin 5 prosenttia ja yli 10 tuntia vain 3 prosenttia organisaatioista. Lisäksi noin 9 prosenttia organisaatioista ei tarjoa koulutusta lainkaan.

Tämä osoittaa, että koulutusta toteutetaan laajasti, mutta sen määrä jää useimmiten melko vähäiseksi. Koulutus on tyypillisesti lyhytkestoista ja keskittyy perusasioihin, eikä syvällisempään osaamisen kehittämiseen panosteta laajasti.

Henkilöstön osallistumisastetta tarkasteltaessa havaitaan, että koulutus tavoittaa monissa organisaatioissa merkittävän osan henkilöstöstä. Noin 32 prosentissa organisaatioista koulutukseen osallistuu noin neljännes henkilöstöstä, ja noin 30 prosentissa osallistumisaste nousee noin 75 prosenttiin. Lisäksi noin 19 prosentissa organisaatioista lähes koko henkilöstö osallistuu koulutukseen. Toisaalta noin 20 prosentissa organisaatioista osallistumisaste jää noin puoleen henkilöstöstä.

Tämä viittaa siihen, että vaikka koulutusta tarjotaan suhteellisen vähän, se pystytään monissa organisaatioissa skaalaamaan laajalle henkilöstöjoukolle. Samalla osallistumisasteen vaihtelu kertoo siitä, että koulutuksen kattavuus ei ole kaikissa organisaatioissa yhdenmukainen.

Harjoitustoiminnan osalta tulokset osoittavat, että suurin osa organisaatioista osallistuu 1–2 digitaalisen turvallisuuden harjoitukseen vuodessa, mikä koskee noin 68 prosenttia organisaatioista. Noin 22 prosenttia organisaatioista ei osallistu harjoituksiin lainkaan, ja vain pieni osa osallistuu useampiin harjoituksiin: 3–5 harjoitukseen noin 6 prosenttia ja yli viiteen harjoitukseen vain muutama prosentti.

Tämä osoittaa, että harjoittelu on monissa organisaatioissa tunnistettu tarpeelliseksi, mutta se toteutuu pääosin melko vähäisessä laajuudessa.

3.11.2 Aktiivisuuden tulkinta

Kokonaisuutena tarkasteltuna aktiivisuus digiturvassa on määrällisesti suhteellisen maltillista, mutta kattavaa. Useimmat organisaatiot tarjoavat jonkin verran koulutusta ja osallistuvat ainakin yksittäisiin harjoituksiin, mutta panostukset jäävät usein perus- tai minimitasolle.

Koulutuksen osalta voidaan tunnistaa toimintamalli, jossa lyhyitä koulutuksia tarjotaan laajalle henkilöstöjoukolle. Tämä tukee perustason tietoisuuden ylläpitoa, mutta ei välttämättä riitä kehittämään syvällisempää osaamista tai vastaamaan kehittyvän uhkaympäristön vaatimuksiin.

Harjoitustoiminnan osalta tilanne viittaa siihen, että organisaatiot keskittyvät yksittäisiin vuosittaisiin harjoituksiin, mutta jatkuva ja systemaattinen harjoittelu ei ole vielä vakiintunut käytäntö. Harjoitusten vähäinen määrä voi heikentää organisaatioiden kykyä toimia tehokkaasti häiriö- ja poikkeustilanteissa.

3.11.3 Johtopäätökset

Tulokset osoittavat, että digiturvaan liittyvä koulutus ja harjoittelu ovat osa organisaatioiden normaalia toimintaa, mutta niiden laajuus ja syvyys eivät kaikilta osin vastaa toimintaympäristön vaatimuksia. Koulutus painottuu lyhytkestoisiin toimenpiteisiin, ja harjoittelun määrä jää usein vähäiseksi.

Organisaatioiden välillä on merkittävää vaihtelua erityisesti koulutuksen kattavuudessa ja harjoituksiin osallistumisessa. Osa organisaatioista onnistuu tavoittamaan lähes koko henkilöstönsä, kun taas toiset jäävät selvästi alhaisemmalle tasolle. Samoin harjoitustoiminnassa osa organisaatioista on aktiivisia, kun taas merkittävä osa ei harjoittele lainkaan.

Kokonaiskuva viittaa siihen, että digiturvan kehittäminen on monessa organisaatiossa edelleen tasolla, jossa perustoimenpiteet on otettu käyttöön, mutta toiminnan systemaattisuus, jatkuvuus ja vaikuttavuus vaativat vahvistamista.

3.11.4 Kehittämisnäkökulmat

Keskeiseksi kehittämistarpeeksi nousee koulutuksen määrän ja laadun vahvistaminen siten, että koulutus ei rajoitu pelkästään lyhyisiin tietoiskuihin, vaan tukee myös syvällisempää osaamisen kehittämistä eri rooleissa.

Lisäksi organisaatioiden tulisi varmistaa koulutuksen kattavuus siten, että se tavoittaa järjestelmällisesti koko henkilöstön ja huomioi erilaiset tehtävät ja riskiprofiilit.

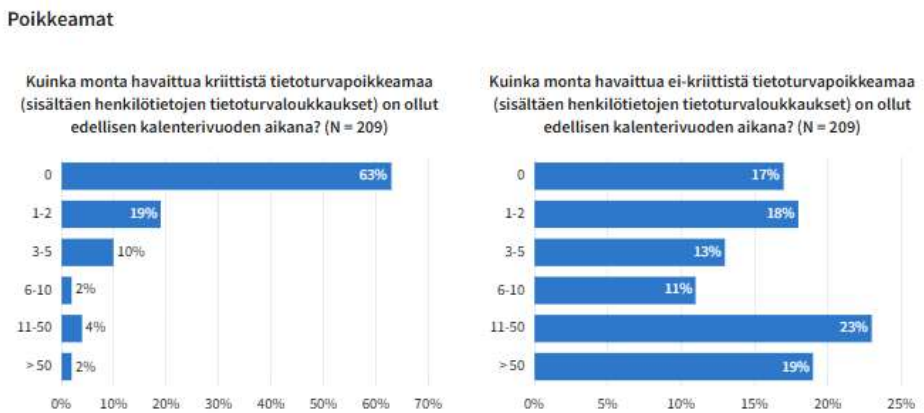
Harjoitustoiminnan osalta keskeistä on siirtyä yksittäisistä harjoituksista kohti säännöllistä ja suunnitelmallista harjoittelua, joka kehittää organisaation valmiutta toimia erilaisissa häiriötilanteissa.

Kokonaisuutena tarkastellen aktiivisuuden kehittäminen edellyttää siirtymistä yksittäisistä toimenpiteistä kohti jatkuvaa ja systemaattista toimintamallia, jossa koulutus ja harjoittelu muodostavat keskeisen osan organisaation digiturvan kokonaisuutta.

3.12 Poikkeamat ja kustannukset

Alla olevassa kuvassa esitellään vastaajaorganisaatioiden näkemyksiä kriittisistä ja ei kriittisistä tietoturvapoikkeamista, jotka sisältävät myös henkilötietoihin kohdistuneet tietoturvaloukkaukset. Lisäksi kuvassa esitetään tietoturvapoikkeamien aiheuttamat välittömät kustannukset.

Kuva 8 kriittisten ja ei-kriittiset tietoturvapoikkeamat



Vähintään joka kolmas vastaajaorganisaatio on kokenut vähintään yhden kriittisten poikkeaman, mikä on merkittävä määrä. Kuitenkin 67 % organisaatioista ei ole kokenut yhtään kriittistä poikkeamaa. Koska kriittiset poikkeamat hyvin todennäköisesti havaitaan, on tämä tulos todennäköisesti luotettava.

22 % organisaatioista ei ole havainnut yhtään ei-kriittistä poikkeamaa. Tämä voi viitata puutteelliseen monitorointiin ja havaintokykyyn. 19 % vastaajista on tunnistanut yli 50 ei-kriittistä poikkeamaa. Tämä viittaa siihen, että viidenneksellä vastaajista on kehittynyt havaintokyky.

Suurin osa organisaatioista, 78 % on havainnut vähintään yhden ei-kriittisen poikkeaman vuoden aikana. Tämä viittaa siihen, että kyber- ja digiturvan hallinta sekä kehittäminen edellyttää pitkäjänteistä ja suunnitelmallista työtä.

Poikkeamien kustannukset eivät jakaudu tasaisesti. Yli puolet vastaajista ei ole tunnistanut suoria kuluja tietoturvapoikkeamista. Toisaalta osalle vastaajista aiheutuu merkittäviä kustannuksia poikkeamista. Yli miljoonan euron menetykset ovat harvinaisia, mutta niiden olemassaolo muistuttaa kyber- ja digiturvariskien realisoitumisen vakavuudesta.

Kun tarkastelee vastaajaorganisaatioiden henkilöresursseja, kehittämis- ja ylläpitokustannuksia, koulutusmääriä, harjoittelua ja havaittuja poikkeamia ja niiden kustannuksia, vaikuttaa siltä että havaitsemis- ja kustannusraportointikyvykkyys vaihtelee merkittävästi. Tällä on suora vaikutus organisaatioiden riskienhallinnan tehokkuuteen. Tilanteen parantaminen edellyttää mittaristojen ja prosessien kehittämistä, valvonnan kehittämistä, kouluttamisen ja harjoittelun lisäämistä sekä tehokkaampaa kustannusten seurantaa digiturvan ylläpidon ja kehittämisen sekä kriittisten ja ei-kriittisten kustannusten osalta. Lisäksi on hyvä huomioida, että tietoturvapoikkeamista voi seurata myös epäsuoria kustannuksia, jotka voivat olla merkittäviä.

3.12.1 Tietoturvapoikkeamien kustannukset

Alla olevassa kuvassa esitetään tietoturvapoikkeamien, hyökkäysten ja loukkausten aiheuttamien välittömien kustannusten jakauma organisaatioissa edellisen kalenterivuoden aikana (N = 209). Jakauma on voimakkaasti vino oikealle, mikä tarkoittaa, että suurin osa organisaatioista raportoi hyvin pieniä kustannuksia, kun taas pieni joukko organisaatioita kohtaa huomattavan suuria kustannuksia.

Mediaanikustannus on 300 euroa, mikä on huomattavan matala verrattuna digitaalisen turvallisuuden kehittämis- ja ylläpitokustannuksiin. Tämä osoittaa, että yli puolet organisaatioista on kokenut hyvin vähäisiä tai lähes olemattomia suoria taloudellisia vaikutuksia tietoturvapoikkeamista tarkastelujaksolla.

3.12.2 Keskeiset havainnot

Jakauman tarkastelu osoittaa, että merkittävä osa organisaatioista sijoittuu kustannusluokkiin alle 1 000 euroa, ja suurin keskittymä näyttää olevan erityisesti välillä 0–500 euroa. Tämä viittaa siihen, että suurimmassa osassa organisaatioista tietoturvapoikkeamat ovat olleet joko vähäisiä tai hyvin hallittuja, eikä niistä ole aiheutunut merkittäviä suoria kustannuksia.

Samanaikaisesti jakauman häntä on pitkä ja ulottuu jopa kymmeniin tuhansiin euroihin ja yksittäistapauksissa vielä tätäkin korkeammalle tasolle. Tämä tarkoittaa, että pieni osa organisaatioista kohtaa selvästi vakavampia poikkeamia, joilla on huomattavia taloudellisia vaikutuksia. Vaikka nämä tapaukset ovat harvinaisempia, ne nostavat kokonaisriskitasoa merkittävästi.

On myös huomionarvoista, että kustannusten jakauma ei ole tasainen, vaan siinä on havaittavissa useita pieniä huippuja eri kustannustasoilla, esimerkiksi noin 1 000 euron ja 5 000–10 000 euron välillä. Tämä voi viitata siihen, että tietoturvapoikkeamat jakautuvat tyypillisesti muutamaan tunnistettavaan vakavuusluokkaan, joissa kustannusrakenteet ovat samankaltaisia.

3.12.3 Kustannusrakenteen tulkinta

Kokonaisuutena tulokset viittaavat siihen, että tietoturvapoikkeamien suorat kustannukset ovat useimmissa organisaatioissa melko rajallisia, mutta jakaumaan sisältyy merkittävä vaihtelu. Suurin osa kustannuksista syntyy pienistä ja toistuvista tapahtumista, kun taas kokonaisriskin kannalta merkittävin tekijä on harvinaisten mutta vaikutuksiltaan suurten poikkeamien esiintyminen.

Matala mediaani voi myös osittain heijastaa sitä, että tarkastelu kattaa vain välittömät kustannukset. Epäsuorat vaikutukset, kuten mainehaitat, toiminnan keskeytykset tai henkilöstön työajan käyttö poikkeamien käsittelyyn, eivät välttämättä näy tässä tarkastelussa, vaikka niiden vaikutus voi olla merkittävä.

Lisäksi jakauma voi kuvastaa organisaatioiden eroja havaintokyvyssä ja raportoinnissa. Organisaatiot, joilla on kehittyneemmät valvonta- ja raportointikäytännöt, saattavat tunnistaa ja kirjata poikkeamien kustannuksia systemaattisemmin kuin organisaatiot, joissa seuranta on vähemmän kypsää.

3.12.4 Johtopäätökset

Tulokset osoittavat, että vaikka tietoturvapoikkeamat aiheuttavat keskimäärin melko pieniä välittömiä kustannuksia, organisaatioiden riskiprofiiliin sisältyy harvinaisia mutta potentiaalisesti merkittäviä taloudellisia vaikutuksia aiheuttavia tapahtumia. Tämä korostaa tarvetta tarkastella tietoturvaa riskienhallinnan näkökulmasta, jossa huomio kiinnittyy paitsi todennäköisiin tapahtumiin myös vaikutuksiltaan suuriin poikkeamiin.

Matala mediaanikustannus ei siten yksin kuvaa kokonaisriskin tasoa, vaan rinnalle tarvitaan ymmärrys jakauman ääripäistä ja niiden vaikutuksista. Organisaatioiden välinen vaihtelu viittaa siihen, että kyvykkyys ennaltaehkäistä ja hallita poikkeamia vaihtelee merkittävästi.

3.12.5 Kehittämisnäkökulmat

Tulosten perusteella keskeiseksi kehittämiskohteeksi nousee kyky tunnistaa ja hallita erityisesti vakavien tietoturvapoikkeamien riskiä. Tämä edellyttää ennakoivia toimenpiteitä, kuten riskiperusteista suojautumista, valvonnan kehittämistä sekä poikkeamien hallintaprosessien vahvistamista.

Lisäksi organisaatioiden on tärkeää kehittää kustannusten seurantaa ja raportointia siten, että myös epäsuorat vaikutukset tulevat huomioiduiksi. Tämä parantaa kokonaiskuvaa tietoturvariskien taloudellisista vaikutuksista ja tukee päätöksentekoa.

Kokonaisuutena tarkastellen tulokset tukevat tarvetta siirtyä pelkästä kustannusten tarkastelusta kohti kokonaisvaltaisempaa riskienhallintaa, jossa huomioidaan sekä poikkeamien todennäköisyys että niiden mahdollinen vaikutus organisaation toimintaan.

Kuva 9 Tietoturvapoikkeamien aiheuttamat välittömät kustannukset

4 Organisaatiotyyppien vertailu

Tässä osiossa vertaillaan neljän keskeisen vastaajaorganisaatiotyypin vastauksia keskenään. Organisaatiotyypit ovat kunnat, hyvinvointialueet, korkeakoulut ja valtionhallinto.

Alla olevassa kuvassa esitetään digitaalisen turvallisuuden kokonaistaso sekä osa-aluekohtaiset tulokset eri organisaatiotyypeissä vuonna 2026. Tarkastelussa ovat kunnat (n = 104), hyvinvointialueet ja muut sote-toimijat (n = 21), korkeakoulut (n = 10) sekä valtionhallinto (n = 39). Kokonaistulokset vaihtelevat välillä 0,69–0,80, mikä viittaa kohtalaisen hyvään, mutta vielä kehittyvään kypsyystasoon kaikissa organisaatioryhmissä.

Valtionhallinto saavuttaa korkeimman kokonaistason (0,80), kun taas kuntien taso jää matalimmaksi (0,69). Hyvinvointialueet (0,79) ja korkeakoulut (0,73) sijoittuvat näiden väliin. Tulokset osoittavat, että organisaatiotyyppi vaikuttaa selvästi digiturvan kypsyystasoon.

4.1 Keskeiset havainnot

Johtamisen osa-alueella korkeakoulut saavuttavat korkeimman arvon (0,80), kun taas kunnissa tulos on selvästi matalampi (0,63). Hyvinvointialueet (0,75) ja valtionhallinto (0,76) sijoittuvat näiden väliin. Tämä viittaa siihen, että johtamiskäytännöt ovat vahvimmillaan korkeakouluissa, mutta kunnissa johtamiseen liittyy selkeä kehittämistarve.

Riskienhallinnan osalta hyvinvointialueet ja muut sote-toimijat saavuttavat korkeimman tason (0,76), kun taas kunnat jäävät alemmalle tasolle (0,64). Korkeakoulut ja valtionhallinto sijoittuvat hyvin lähelle toisiaan tasolle 0,75. Tämä osoittaa, että riskienhallinta on kehittyneintä sote-sektorilla, mikä voi liittyä toiminnan luonteeseen ja sääntelyn vaatimuksiin.

Toiminnan jatkuvuuden ja varautumisen osalta hyvinvointialueet ja valtionhallinto saavuttavat saman korkean tason (0,76), kun taas kunnissa (0,67) ja erityisesti korkeakouluissa (0,65) taso jää selvästi matalammaksi. Tämä viittaa siihen, että kriittisiin häiriötilanteisiin varautuminen on vahvinta toimijoilla, joiden toiminta on yhteiskunnan kannalta välittömästi kriittistä.

Tietoturvallisuuden osa-alueella valtionhallinto erottuu selvästi korkeimmalla tasolla (0,88), kun taas hyvinvointialueet (0,84), kunnat (0,77) ja korkeakoulut (0,73) jäävät tämän alapuolelle. Tämä kuvastaa vahvaa panostusta tietoturvaan valtionhallinnossa sekä eroja kypsyystasossa eri sektoreiden välillä.

Tietosuojassa hyvinvointialueet ja valtionhallinto saavuttavat korkeimmat arvot (0,85), kun taas korkeakoulut (0,81) ja kunnat (0,77) jäävät hieman jälkeen. Tämä viittaa siihen, että sote-sektorin ja valtionhallinnon toimijat ovat panostaneet erityisesti henkilötietojen käsittelyn vaatimuksiin.

Kyberturvallisuuden osalta erot ovat jälleen merkittäviä. Valtionhallinto (0,76) ja hyvinvointialueet (0,75) ovat selvästi edellä, kun taas kunnat ja korkeakoulut jäävät tasolle

0,62. Tämä osoittaa, että kyberturvallisuuden kehittäminen on edennyt pidemmälle kriittisillä toimialoilla kuin muilla sektoreilla.

4.1.1 Tulosten tulkinta

Kokonaisuutena tarkasteltuna tulokset osoittavat selkeän rakenteellisen eron organisaatiotyyppien välillä. Valtionhallinto ja hyvinvointialueet saavuttavat järjestelmällisesti korkeammat tulokset lähes kaikilla osa-alueilla. Tämä viittaa korkeampaan kypsyystasoon, joka voi johtua esimerkiksi tiukemmasta sääntelystä, suuremmista resursseista sekä toiminnan kriittisyydestä.

Kunnat jäävät useimmilla osa-alueilla alhaisimmalle tasolle, mikä viittaa resurssi- ja osaamisrajoitteisiin sekä mahdollisesti hajautuneempiin toimintamalleihin. Korkeakoulut sijoittuvat usein kuntien ja muiden toimijoiden väliin, mutta erityisesti jatkuvuudenhallinnan ja kyberturvallisuuden osalta tulokset ovat suhteellisen matalia.

Erityisen huomionarvoista on, että tietoturva ja tietosuoja ovat kaikilla organisaatiotyypeillä keskimäärin korkeammalla tasolla kuin kyberturvallisuus, jatkuvuus ja riskienhallinta. Tämä viittaa siihen, että perinteiset vaatimukset ovat vakiintuneet paremmin kuin laajemmat, strategisemmat digiturvan osa-alueet.

4.1.2 Johtopäätökset

Tulokset osoittavat, että digiturvan kypsyys vaihtelee merkittävästi organisaatiotyypeittäin. Valtionhallinto ja hyvinvointialueet muodostavat kypsyystason kärjen, kun taas kunnat jäävät selvästi jälkeen useimmilla osa-alueilla.

Keskeinen havainto on, että erot eivät rajoitu yksittäisiin osa-alueisiin, vaan ovat systemaattisia koko digiturvan kokonaisuudessa. Tämä viittaa siihen, että erot johtuvat rakenteellisista tekijöistä, kuten resursseista, osaamisesta ja ohjausmalleista.

Lisäksi tulokset vahvistavat aiemmissa analyyseissa esiin nousseen ilmiön, jossa tietoturva ja tietosuoja ovat kehittyneempiä kuin kyberturvallisuus ja jatkuvuudenhallinta. Tämä kertoo kypsyystason epätasaisesta kehittymisestä.

4.1.3 Kehittämisnäkökulmat

Keskeiseksi kehittämistarpeeksi nousee erityisesti kuntasektorin tukeminen digiturvan kehittämisessä. Tämä voi edellyttää yhteisiä toimintamalleja, keskitettyjä palveluja sekä osaamisen vahvistamista, jotta erot muihin sektoreihin eivät kasva.

Toiseksi kehittämisen painopisteenä tulisi olla kyberturvallisuuden ja jatkuvuudenhallinnan vahvistaminen kaikissa organisaatiotyypeissä, koska nämä osa-alueet jäävät systemaattisesti tietoturvaa ja tietosuojaa heikommalle tasolle.

Kolmantena keskeisenä kehittämiskohteena on kokonaisvaltaisen digiturvan johtamisen vahvistaminen siten, että eri osa-alueet kehittyvät tasapainoisesti eikä yksittäisiin osa-alueisiin keskitytä muiden kustannuksella.

Valitse tarkastelujakso

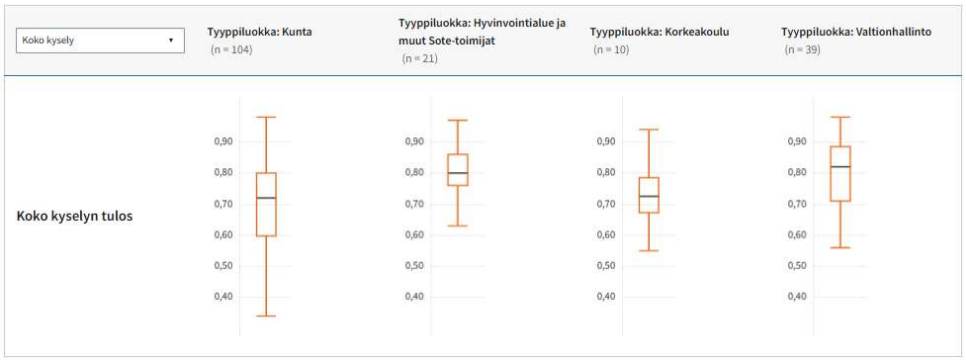
Vuosi 2026

	Tyyppiluokka: Kunta (n = 104)	Tyyppiluokka: Hyvinvointialue ja muut Sote-toimijat (n = 21)	Tyyppiluokka: Korkeakoulu (n = 10)	Tyyppiluokka: Valtionhallinto (n = 39)
Koko kyselyn tulos	**0,69**	**0,79**	**0,73**	**0,80**
Johtaminen	0,63	0,75	0,80	0,76
Riskienhallinta	0,64	0,76	0,75	0,75
Toiminnan jatkuvuus ja varautuminen	0,67	0,76	0,65	0,76
Tietoturvallisuus	0,77	0,84	0,73	0,88
Tietosuoja	0,77	0,85	0,81	0,85
Kyberturvallisuus	0,62	0,75	0,62	0,76

4.2 Organisaatiotyyppien vastausten hajonta

Alla olevassa kuvaajassa janan yläpään ja alapään viikset kuvaavat kyseisen vastaajaryhmän suurinta ja pienintä arvoa ja siten myös vastausten keskiarvojen hajontaa. Janan keskellä oleva suorakaide kuvaa kvartaaliväliä, johon asettuu 50 % keskimmäisistä vastauskeskiarvoista. Laatikon yläpuolella on siis yläkvartaali, 75 % vastauksista on näitä tuloksia pienempi. Laatikon alapuolella on alakvartaali, laatikon alareunan alapuolella on 75 % on tätä keskiarvoa parempia. Musta viiva kuvaa vastausten mediaania.

Kuvaaja koko kyselyn tulos digitaalinen turvallisuus



Yllä olevassa kuvassa esitetään digiturvan kokonaistuloksen jakauma eri organisaatiotyypeissä laatikkokaavioiden (boxplot) avulla. Tarkastelussa ovat kunnat, hyvinvointialueet ja muut sote-toimijat, korkeakoulut sekä valtionhallinto. Kaavio kuvaa kunkin ryhmän mediaania, vaihteluväliä sekä hajontaa, mikä mahdollistaa kypsyystason lisäksi myös organisaatioiden välisten erojen tarkastelun.

Kaikkien organisaatiotyyppien tulokset sijoittuvat pääosin välille noin 0,55–0,95, mikä viittaa siihen, että digiturvan kypsyys on yleisesti kohtalaisella tai hyvällä tasolla. Erot organisaatiotyyppien välillä näkyvät kuitenkin sekä mediaanitasoissa että hajonnassa.

4.2.1 Keskeiset havainnot

Kuntien osalta jakauma on selvästi laajin. Alimmat arvot ulottuvat noin tasolle 0,35, kun taas ylimmät arvot nousevat lähelle 0,95. Mediaani sijoittuu noin 0,70:n tuntumaan, mutta hajonta on merkittävä. Tämä osoittaa, että kuntien välillä on suuria eroja digiturvan kypsyydessä: osa organisaatioista on saavuttanut hyvän tason, kun taas toisilla taso jää selvästi matalammaksi.

Hyvinvointialueiden ja muiden sote-toimijoiden jakauma on kapeampi ja sijoittuu pääosin korkeammalle tasolle. Mediaani on noin 0,80, ja suurin osa havainnoista keskittyy välille 0,75–0,85. Alimmat havainnot jäävät noin 0,63:n tasolle, mutta vaihtelu on selvästi pienempää kuin kunnissa. Tämä viittaa tasaisempaan ja keskimäärin korkeampaan kypsyystasoon sote-sektorilla.

Korkeakoulujen osalta jakauma sijoittuu kuntien ja sote-toimijoiden väliin. Mediaani on noin 0,72–0,75, ja vaihteluväli ulottuu noin 0,55:stä hieman yli 0,90:een. Hajonta on kohtalainen, mikä osoittaa, että korkeakoulujen välillä on eroja, mutta ne eivät ole yhtä suuria kuin kunnissa.

Valtionhallinnon jakauma sijoittuu korkealle tasolle ja on samalla suhteellisen laaja. Mediaani on noin 0,82, mutta vaihteluväli ulottuu noin 0,55:stä lähes 0,95:een. Tämä kertoo, että vaikka keskimääräinen taso on korkea, organisaatioiden välillä on edelleen merkittävää vaihtelua.

4.2.2 Tulosten tulkinta

Kaaviot korostavat kahta keskeistä ilmiötä: organisaatiotyyppien välistä tasoeroa sekä organisaatioiden sisäistä vaihtelua.

Valtionhallinto ja hyvinvointialueet sijoittuvat mediaanitasolla korkeimmalle, mikä viittaa kehittyneempään digiturvan kypsyyteen. Tämä voi liittyä toiminnan kriittisyyteen, ohjauksen vahvuuteen sekä käytettävissä oleviin resursseihin.

Kuntien osalta suuri hajonta on keskeinen havainto. Se kertoo, että digiturvan kehitys ei ole edennyt tasaisesti, vaan erot organisaatioiden välillä ovat merkittäviä. Osa kunnista toimii hyvällä tasolla, kun taas osa jää selvästi jälkeen. Tämä heijastaa todennäköisesti eroja resursseissa, osaamisessa ja toimintamalleissa.

Korkeakoulut edustavat keskitason ryhmää, jossa kypsyystaso on kohtuullinen, mutta ei yhtä korkea kuin valtionhallinnossa tai sote-toimijoilla. Hajonta viittaa siihen, että osa korkeakouluista on panostanut digiturvaan enemmän kuin toiset.

4.2.3 Johtopäätökset

Tulokset osoittavat, että digiturvan kokonaistaso vaihtelee merkittävästi organisaatiotyypeittäin ja myös organisaatioiden sisällä. Valtionhallinto ja hyvinvointialueet muodostavat kypsyystason kärjen, kun taas kuntasektorilla erot ovat suurimmat ja keskimääräinen taso matalampi.

Keskeinen havainto on, että korkea mediaani ei poista vaihtelua: myös korkean tason organisaatioryhmissä on toimijoita, joiden kypsyys jää selvästi alle ryhmän

keskitason. Tämä korostaa tarvetta tarkastella digiturvaa paitsi keskiarvojen myös hajonnan näkökulmasta.

Kokonaiskuva viittaa siihen, että digiturvan kehitys on edennyt pidemmälle niissä organisaatioissa, joissa on vahvempi ohjaus, enemmän resursseja ja suurempi toiminnan kriittisyys.

4.2.4 Kehittämisnäkökulmat

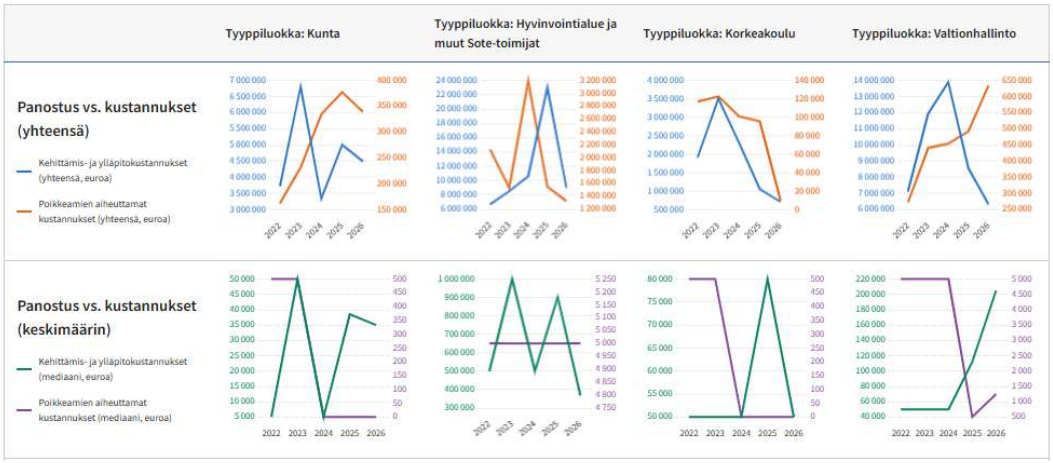
Keskeiseksi kehittämistarpeeksi nousee erityisesti kuntasektorin tukeminen, jotta suurta hajontaa voidaan vähentää ja vähimmäistasoa nostaa. Tämä voi edellyttää yhteisiä ratkaisuja, palveluita ja ohjausmalleja, jotka tukevat heikomman kypsyystason organisaatioita.

Lisäksi tulokset korostavat tarvetta seurata kehitystä myös hajonnan näkökulmasta. Pelkkä keskiarvotason tarkastelu ei riitä, vaan on tärkeää tunnistaa ne organisaatiot, jotka jäävät keskiarvon alapuolelle, ja kohdentaa kehittämistoimenpiteitä niihin.

Kokonaisuutena tarkastellen kehittämisen painopisteenä tulisi olla kypsyystason tasoittaminen organisaatioiden välillä sekä parhaiden käytäntöjen laajempi hyödyntäminen eri sektoreilla.

4.3 Panostukset vs. kustannukset

Kuvaaja. Digiturvaan kohdistetut kehittämis- ja ylläpitoresurssit suhteessa tietoturvapoikkeamien aiheuttamat kustannukset



Kuvassa tarkastellaan digitaalisen turvallisuuden kehittämis- ja ylläpitokustannusten sekä tietoturvapoikkeamien aiheuttamien kustannusten suhdetta eri organisaatiotyypeissä vuosina 2022–2026. Tarkastelu on esitetty sekä kokonaiskustannuksina että mediaanitasoisina (keskimääräisinä) arvoina.

Kokonaisuutena kuva osoittaa, että digiturvaan kohdistuvat panostukset ja poikkeamien kustannukset vaihtelevat huomattavasti sekä ajallisesti että organisaatiotyypeittäin. Kehitys ei ole lineaarista, vaan sisältää selviä vuosittaisia vaihteluita, jotka viittaavat sekä yksittäisten tapahtumien vaikutuksiin että investointien ajoittumiseen.

4.3.1 Keskeiset havainnot

Kuntien osalta kokonaiskustannukset vaihtelevat merkittävästi tarkastelujaksolla. Kehittämis- ja ylläpitokustannuksissa on selvä huippu vuonna 2023, minkä jälkeen taso laskee, mutta pysyy edelleen verrattain korkeana. Samanaikaisesti poikkeamien kustannukset kasvavat erityisesti vuosina 2024–2025, jonka jälkeen ne tasaantuvat hieman. Mediaanitarkastelu osoittaa samansuuntaisen ilmiön: kehittämispanokset vaihtelevat voimakkaasti, ja poikkeamakustannuksissa nähdään ajoittaisia nousuja.

Hyvinvointialueilla ja muilla sote-toimijoilla vaihtelu on vielä korostuneempaa. Erityisesti vuonna 2024 nähdään merkittävä poikkeamien kustannuspiikki, joka erottuu selvästi muista vuosista. Kehittämis- ja ylläpitokustannukset vaihtelevat myös voimakkaasti, tämä ehdottaa panostuksien olevan osittain projektiperusteisia tai sidoksissa tiettyihin kehitysvaiheisiin. Mediaanitasolla vaihtelu on myös huomattavaa, mikä kertoo organisaatioiden välisistä eroista.

Korkeakoulujen osalta kehitys on kokonaisuudessaan laskeva erityisesti kehittämis- ja ylläpitokustannusten osalta. Samanaikaisesti poikkeamien kustannukset ovat korkeimmillaan tarkastelujakson alussa ja laskevat myöhempinä vuosina, vaikka yksittäisiä vaihteluita esiintyy. Mediaanitasolla tarkasteltuna kehittämispanokset vaihtelevat, mutta poikkeamakustannukset pysyvät suhteellisen matalina.

Valtionhallinnossa kehittämis- ja ylläpitokustannukset kasvavat selvästi erityisesti vuosina 2023–2024, minkä jälkeen taso laskee. Samaan aikaan poikkeamien kustannukset kasvavat tasaisesti tarkastelujakson aikana. Mediaanitasolla tarkasteltuna kehittämiskustannukset pysyvät suhteellisen vakaina, mutta poikkeamakustannuksissa nähdään selvä nousutrendi, mikä viittaa joko lisääntyneeseen raportointiin tai vakavampiin poikkeamiin.

4.3.2 Panostuksen ja kustannusten suhteen tulkinta

Kokonaisuutena tarkasteltuna panostusten ja poikkeamien kustannusten välinen suhde ei ole suoraviivainen. Joissakin tapauksissa kasvavat panostukset näyttävät edeltävän poikkeamakustannusten kasvua, kun taas toisissa tapauksissa investoinnit seuraavat suuria poikkeamia. Organisaatiot siis reagoivat usein tapahtuneisiin poikkeamiin lisäämällä panostuksiaan, mutta ennakoiva investointi ei ole vielä kaikilta osin vakiintunutta.

Kuntien ja valtionhallinnon osalta voidaan havaita viitteitä siitä, että korkeammat panostukset eivät välittömästi johda poikkeamakustannusten pienenemiseen, mikä korostaa viivettä investointien ja niiden vaikutusten välillä. Hyvinvointialueilla yksittäiset poikkeamahuiput vaikuttavat voimakkaasti kokonaiskuvaan, mikä voi johtua yksittäisten suurten tapausten vaikutuksesta.

Mediaanitarkastelu tuo esiin, että keskimääräinen taso on huomattavasti tasaisempi kuin kokonaiskustannukset. Tämä kertoo suurimpien vaihteluiden selittyvän yksittäisillä organisaatioilla tai tapahtumilla, eikä koko kentän kehitys ole yhtä voimakasta kuin kokonaislukujen perusteella voisi päätellä.

4.3.3 Johtopäätökset

Tulokset osoittavat, että digiturvan rahoitus ja poikkeamien kustannukset ovat vahvasti sidoksissa organisaatioiden toimintaympäristöön, kehitysvaiheeseen ja yksittäisiin tapahtumiin. Kokonaiskustannusten voimakas vaihtelu kertoo, että digiturvaan liittyvät investoinnit eivät ole kaikissa organisaatioissa täysin ennakoivia tai systemaattisia.

Keskeinen havainto on, että poikkeamien kustannukset eivät vähene tasaisesti panostusten kasvaessa, vaan suhde on monimutkainen ja sisältää viivettä. Tämä korostaa tarvetta pitkäjänteiselle kehittämiselle sekä vaikutusten systemaattiselle arvioinnille.

Lisäksi organisaatiotyyppien väliset erot ovat merkittäviä. Valtionhallinto ja sote-toimijat kohtaavat suurempia kustannusvaihteluita, kun taas kunnissa ja korkeakouluissa vaihtelu näkyy erityisesti panostusten epätasaisuutena. Tämä viittaa erilaiseen riskiprofiiliin ja kyvykkyyksiin eri sektoreilla.

4.3.4 Kehittämisnäkökulmat

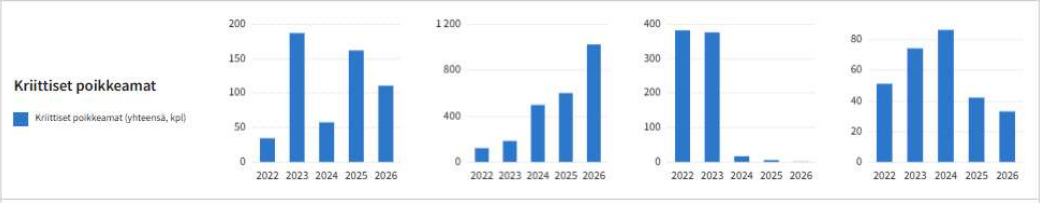
Tulosten perusteella keskeiseksi kehittämistarpeeksi nousee panostusten ennakoivuuden vahvistaminen. Organisaatioiden tulisi siirtyä reaktiivisesta mallista kohti suunnitelmallista ja pitkäjänteistä investointia, jossa panostukset perustuvat riskiarvioon eikä yksittäisiin tapahtumiin.

Lisäksi on tärkeää kehittää mekanismeja, joilla voidaan arvioida panostusten vaikuttavuutta suhteessa poikkeamien kustannuksiin. Tämä edellyttää parempaa kustannusten seurantaa sekä yhtenäisiä mittareita, joiden avulla kehitystä voidaan vertailla ajassa ja organisaatioiden välillä.

Kokonaisuutena kehittämisen painopisteenä tulisi olla kustannusten hallinnan ja vaikuttavuuden johtamisen vahvistaminen siten, että digiturvaan kohdistuvat investoinnit tukevat pitkäjänteisesti organisaation riskienhallintaa ja toimintavarmuutta.

4.4 Kriittiset poikkeamat

Kuvaaja. Kriittiset poikkeamat yhteensä, kunnat, HVA:t, Korkeakoulut, Valtiohallinto



Kuvassa esitetään kriittisten tietoturvapoikkeamien kokonaismäärät vuosina 2022–2026 neljässä organisaatiotyypissä: kunnissa, hyvinvointialueilla ja muissa sote-toimijoissa, korkeakouluissa sekä valtionhallinnossa. Pylväsdiagrammit kuvaavat vuosittaista kehitystä organisaatioryhmittäin samassa järjestyksessä kuin aiemmissa tarkasteluissa.

Kokonaisuutena tarkasteltuna kehitys on eri organisaatiotyypeissä hyvin erisuuntaista. Osassa ryhmistä kriittisten poikkeamien määrä kasvaa voimakkaasti, kun taas toisissa suunta on laskeva tai vaihteleva. Tämä viittaa sekä toimintaympäristön muutoksiin että eroihin havaintokyvyssä, raportoinnissa ja riskitasossa.

4.4.1 Keskeiset havainnot

Kuntien osalta kehitys on vaihtelevaa, mutta kokonaiskuvassa näkyy selviä heilahteluja vuosien välillä. Vuonna 2022 kriittisiä poikkeamia on vähän, minkä jälkeen vuonna 2023 tapahtuu selvä kasvu noin 180 tapaukseen. Vuonna 2024 määrä laskee merkittävästi, mutta nousee jälleen vuonna 2025 ja pysyy verrattain korkealla tasolla myös vuonna 2026. Tämä viittaa epävakaaseen kehitykseen, jossa yksittäiset vuodet tai tapahtumat vaikuttavat kokonaiskuvaan merkittävästi.

Hyvinvointialueiden ja muiden sote-toimijoiden osalta kehitys on tasaisemmin nouseva. Vuodesta 2022 alkaen poikkeamien määrä kasvaa asteittain, ja erityisesti vuosina 2024–2026 kasvu kiihtyy selvästi. Vuonna 2026 kokonaismäärä nousee jo lähelle 1 000 tapausta, mikä on tarkastelun korkein taso. Tämä osoittaa merkittävää lisääntymistä joko poikkeamien määrässä tai niiden tunnistamisessa ja raportoinnissa.

Korkeakoulujen osalta kehitys on päinvastainen. Vuosien 2022 ja 2023 raportoidut määrät ovat selvästi korkeimmalla tasolla, noin 350–380 poikkeamaa, mutta tämän jälkeen määrä laskee jyrkästi. Vuonna 2024 taso romahtaa alle 50 tapaukseen ja pysyy erittäin matalana myös vuosina 2025 ja 2026. Tämä viittaa merkittävään muutokseen joko toimintaympäristössä, raportointikäytännöissä tai poikkeamien hallinnassa.

Valtionhallinnon osalta kehitys on aluksi kasvavaa ja saavuttaa huipun vuonna 2024 noin 90 tapauksessa. Tämän jälkeen poikkeamien määrä vähenee vuosina 2025 ja 2026, mutta pysyy edelleen korkeammalla tasolla kuin tarkastelujakson alussa. Kehitys viittaa siihen, että kriittisten poikkeamien määrä on kasvanut ja sen jälkeen mahdollisesti saatu osittain hallintaan.

4.4.2 Kehityksen tulkinta

Organisaatiotyyppien välillä on selviä eroja kehityssuunnissa. Hyvinvointialueiden voimakas kasvu erottuu selvästi muista ja kertoo joko nopeasti kasvaneesta uhkaympäristöstä, lisääntyneestä toiminnan digitalisoitumisesta tai merkittävästi parantuneesta kyvystä havaintoon ja raportointiin.

Kuntien vaihteleva kehitys puolestaan viittaa epätasaiseen kyvykkyyteen hallita ja raportoida poikkeamia. Suuret vuosittaiset vaihtelut voivat johtua yksittäisistä merkittävistä tapauksista tai eroista raportointikäytännöissä.

Korkeakoulujen jyrkkä lasku on poikkeuksellinen ilmiö. Se voi viitata joko merkittävään parannukseen tietoturvatasossa tai vaihtoehtoisesti muutoksiin raportoinnin kattavuudessa. Ilman lisätietoja ei voida yksiselitteisesti päätellä kummasta ilmiöstä on kyse.

Valtionhallinnon kehitys osoittaa ensin kasvavaa havaintomäärää ja tämän jälkeen tasaantumista. Tämä voi viitata siihen, että havaintokyky on ensin parantunut ja tämän jälkeen toimenpiteet ovat alkaneet vaikuttaa poikkeamien määrään.

4.4.3 Johtopäätökset

Tulokset osoittavat, että kriittiset tietoturvapoikkeamat eivät kehity yhtenäisesti eri organisaatiotyypeissä, vaan kehitykseen vaikuttavat useat tekijät, kuten toimintaympäristö, kypsyystaso, raportointikäytännöt ja yksittäiset tapahtumat.

Keskeinen havainto on, että poikkeamamäärien kasvu ei välttämättä tarkoita heikompaa turvallisuustilannetta, vaan voi kuvastaa parempaa havaintokykyä ja raportointia. Tämä korostaa tarvetta tulkita tuloksia kontekstissa eikä pelkästään määrällisesti.

Hyvinvointialueiden voimakas kasvu ja korkeakoulujen jyrkkä lasku ovat erityisen merkittäviä ilmiöitä, jotka viittaavat rakenteellisiin muutoksiin digiturvan toteutuksessa eri sektoreilla.

4.4.4 Kehittämisnäkökulmat

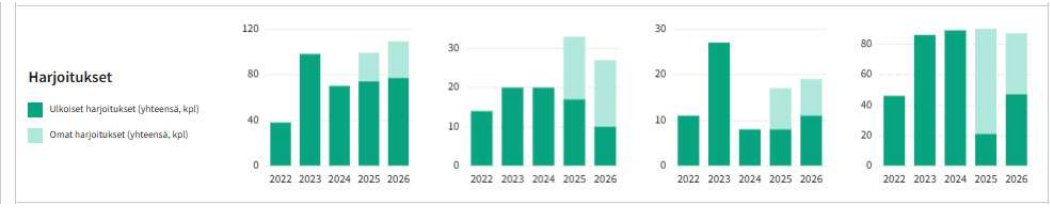
Keskeiseksi kehittämistarpeeksi nousee poikkeamien raportoinnin ja tulkinnan yhtenäistäminen, jotta organisaatioiden välinen vertailu olisi luotettavampaa ja kehityssuunnat helpommin tulkittavia.

Lisäksi organisaatioiden tulisi kiinnittää huomiota siihen, että kasvavat poikkeamamäärät analysoidaan systemaattisesti, jotta voidaan erottaa toisistaan todellinen riskitason kasvu ja havaintokyvyn paraneminen.

Kokonaisuutena kehittämisen painopisteenä tulisi olla poikkeamatiedon parempi hyödyntäminen johtamisessa, ennakoivien toimenpiteiden vahvistaminen sekä parhaiden käytäntöjen jakaminen eri organisaatioryhmien välillä, jotta kehityseroja voidaan tasoittaa.

4.5 Harjoittelu

Kuvaaja. Harjoitustoiminta, ulkoiset harjoitukset ja omat harjoitukset yhteensä. Kunnat, HVA:t, Korkeakoulut, Valtiohallinto



Kuvassa esitetään digitaaliseen turvallisuuteen liittyvien harjoitusten määrät vuosina 2022–2026 neljässä organisaatiotyypissä: kunnissa, hyvinvointialueilla ja muissa sote-toimijoissa, korkeakouluissa sekä valtionhallinnossa. Harjoitukset on jaoteltu kahteen kategoriaan: ulkoisiin harjoituksiin (esimerkiksi kansalliset tai yhteiset harjoitukset) sekä organisaatioiden omiin sisäisiin harjoituksiin.

Kokonaisuutena tarkasteltuna harjoitustoiminta on yleistä kaikissa organisaatiotyypeissä, mutta määrissä ja kehityssuunnissa on merkittäviä eroja. Useissa organisaatioryhmissä harjoitusten kokonaismäärä kasvaa tarkastelujakson aikana, mutta kehitys ei ole tasainen.

4.5.1 Keskeiset havainnot

Kuntien osalta harjoitusten määrä vaihtelee tarkastelujaksolla melko voimakkaasti. Vuonna 2022 harjoituksia on vähän, mutta vuonna 2023 kokonaismäärä kasvaa selvästi, erityisesti ulkoisten harjoitusten osalta. Vuonna 2024 kokonaismäärä laskee, mutta kasvaa jälleen vuosina 2025 ja 2026, jolloin saavutetaan tarkastelujakson korkeimmat tasot. Omien harjoitusten osuus kasvaa loppuvuosina, mikä viittaa lisääntyvään sisäiseen kehittämiseen.

Hyvinvointialueiden ja sote-toimijoiden osalta kehitys on tasaisempaa, mutta sisältää merkittäviä vaihteluita. Ulkoisten harjoitusten määrä pysyy melko vakaana vuosina 2023–2024, mutta kasvaa selvästi vuonna 2025 ja hieman laskee vuonna 2026. Omien harjoitusten osuus korostuu erityisesti vuosina 2025–2026, jolloin kokonaismäärä nousee korkeimmalle tasolle tarkastelujaksolla. Tämä viittaa kyvykkyyden systemaattiseen vahvistumiseen.

Korkeakoulujen osalta harjoitustoiminta on määrältään muita vähäisempää, mutta vaihtelu on selkeää. Vuonna 2023 ulkoisten harjoitusten määrä nousee selvästi korkeimmalle tasolle, minkä jälkeen se laskee. Vuosina 2025–2026 nähdään kasvua erityisesti omien harjoitusten osalta, mikä viittaa siihen, että painopiste siirtyy ulkoisista tapahtumista organisaation sisäiseen kehittämiseen.

Valtionhallinnon osalta harjoitustoiminta on laajinta ja systemaattisinta. Ulkoisten harjoitusten määrä on korkealla tasolla erityisesti vuosina 2023–2024, minkä jälkeen se laskee vuonna 2025, mutta palautuu jälleen vuonna 2026. Omien harjoitusten määrä kasvaa tarkastelujakson loppua kohden ja muodostaa merkittävän osan kokonaisuudesta. Tämä osoittaa kypsää ja monipuolista harjoitustoimintaa.

4.5.2 Harjoitustoiminnan tulkinta

Kokonaisuutena tarkasteltuna harjoitustoiminta on kehittynyt useimmissa organisaatiotyypeissä kohti monipuolisempaa mallia, jossa yhdistyvät sekä ulkoiset että sisäiset harjoitukset. Erityisesti omien harjoitusten lisääntyminen viittaa siihen, että organisaatiot pyrkivät kehittämään valmiuksiaan systemaattisemmin ja organisaatiokohtaisesti.

Kuntien ja korkeakoulujen osalta kehitys on kuitenkin epätasaisempaa, mikä viittaa siihen, että harjoitustoiminta ei ole vielä täysin vakiintunut tai suunnitelmallinen. Sen sijaan valtionhallinnossa ja hyvinvointialueilla harjoitustoiminta näyttää olevan enemmän jatkuvaa ja strategisesti ohjattua.

Ulkoisten harjoitusten merkitys näkyy erityisesti tarkastelujakson alkuvuosina, mutta myöhemmin painopiste siirtyy monin paikoin sisäisiin harjoituksiin. Tämä voi viitata siihen, että organisaatiot ovat siirtymässä yleisistä harjoituksista kohti omiin riskeihin ja toimintaympäristöön paremmin kohdistettuja harjoitteita.

4.5.3 Johtopäätökset

Tulokset osoittavat, että digiturvan harjoitustoiminta on laajentunut ja kehittynyt tarkastelujaksolla, mutta organisaatiotyyppien välillä on merkittäviä eroja sekä määrässä että kypsyydessä. Valtionhallinto ja hyvinvointialueet erottuvat kokonaisuutena

aktiivisempina ja systemaattisempina toimijoina, kun taas kunnissa ja korkeakouluissa toiminta on vaihtelevampaa.

Erityisesti omien harjoitusten kasvava osuus on keskeinen havainto, sillä se kertoo siirtymästä kohti kohdennetumpaa ja organisaatiolähtöistä varautumista. Samalla kuitenkin havaitaan, että harjoitusten kokonaismäärä vaihtelee voimakkaasti joissakin organisaatioryhmissä, mikä heikentää toiminnan ennustettavuutta.

4.5.4 Kehittämisnäkökulmat

Keskeiseksi kehittämistarpeeksi nousee harjoitustoiminnan systematisointi erityisesti niissä organisaatiotyypeissä, joissa toiminta on vaihtelevaa. Harjoittelun tulisi perustua suunnitelmalliseen vuosikelloon ja riskiperusteiseen lähestymistapaan.

Lisäksi organisaatioiden tulisi tasapainottaa ulkoisten ja omien harjoitusten käyttöä siten, että ulkoiset harjoitukset tukevat verkostoyhteistyötä ja omat harjoitukset kehittävät organisaation sisäistä toimintakykyä.

Kokonaisuutena kehittämisen painopisteenä tulisi olla harjoitusten määrän lisäksi niiden laadun ja vaikuttavuuden parantaminen, jotta harjoitustoiminta tukee tehokkaasti organisaation kykyä toimia häiriö- ja poikkeustilanteissa.

Hyvä kehityskohde harjoittelun osalta on mm. TAISTO-harjoitus, jonka digi- ja väestötietovirasto järjestää vuosittain marraskuussa. TAISTO on helppo ja kustannustehokas tapa harjoitella digiturvaa. TAISTO on maksuton ja siihen voi osallistua useita harjoitusryhmiä yksittäisestä organisaatiosta. Ilmoittautuminen vuoden 2026 marraskuun Taisto-harjoitukseen käynnistyy elokuun lopussa, lisätietoa: https://dvv.fi/taisto.

Harjoittelutoiminta on keskeinen tapa toteuttaa kyber- ja digiturvaa, joten kannustamme organisaatioita suunnittelemaan vuosittaisen harjoitusohjelman, jonka organisaation johto hyväksyy ja resursoi riittävästi.

Lisätietoa harjoitustoiminnasta saa mm. Digiturvan tietopankista: Harjoitustoiminta - Kyberturvallisuuden ja digitaalisen turvallisuuden tietopankki - Suomi.fi kehittäjille

4.6 Digitaaliseen turvallisuuteen käytetty htv vs. poikkeamat

Kuvaaja. Digiturvaan käytetyt henkilötyövuodet suhteessa tietoturvapoikkeamiin. Kuvaajassa kunnat, HVA:t, Korkeakoulut, Valtiohallinto

Yllä olevassa kuvassa tarkastellaan digiturvaan kohdennetun työpanoksen (omat ja ostetut henkilötyövuodet) sekä kriittisten ja ei-kriittisten poikkeamien kokonaismäärien välistä suhdetta vuosina 2022–2026 neljässä organisaatiotyypissä: kunnissa, hyvinvointialueilla ja muissa sote-toimijoissa, korkeakouluissa sekä valtionhallinnossa.

Kokonaisuutena tarkasteltuna kuva yhdistää resurssien määrällisen kehityksen ja poikkeamien kehityksen samaan tarkasteluun. Tämä mahdollistaa sen arvioinnin, onko työpanoksen lisäämisellä yhteyttä poikkeamien määrään tai niiden kehityssuuntaan.

4.6.1 Keskeiset havainnot

Kuntien osalta organisaation oma työpanos kasvaa selvästi vuosien 2022 ja 2023 välillä ja saavuttaa huipun vuonna 2023, minkä jälkeen se vaihtelee mutta pysyy suhteellisen korkealla tasolla. Ostettujen resurssien käyttö on vähäisempää, mutta kasvaa hieman tarkastelujakson loppupuolella. Samaan aikaan ei-kriittisten poikkeamien määrä kasvaa voimakkaasti erityisesti vuosina 2023 ja 2026, kun taas kriittiset poikkeamat pysyvät matalina koko tarkastelujakson ajan. Tämä kertoo tilanteesta, jossa resurssien kasvu ei suoraan vähennä poikkeamien määrää, vaan voi liittyä parempaan havaintokykyyn.

Hyvinvointialueilla ja sote-toimijoissa kehitys on voimakkaammin korostunut. Oma työpanos kasvaa tasaisesti ja saavuttaa korkeimman tason vuonna 2026, samalla kun ostettujen resurssien käyttö lisääntyy huomattavasti erityisesti vuosina 2025–2026. Tässä ryhmässä ei-kriittisten poikkeamien määrä kasvaa erittäin voimakkaasti, erityisesti vuosina 2024–2026, jolloin ylletään selvästi korkeimpiin lukemiin koko aineistossa. Kriittiset poikkeamat kasvavat myös, mutta selvästi maltillisemmin. Tämä kehitys ehdottaa, että resurssien lisääntyminen kulkee käsi kädessä havaintojen lisääntymisen kanssa.

Korkeakoulujen osalta kokonaiskuva on erilainen. Oma työpanos kasvaa hieman vuosien 2022–2023 välillä, mutta laskee tämän jälkeen ja pysyy alhaisemmalla tasolla vuosina 2024–2026. Ostettu työpanos on hyvin vähäistä koko tarkastelujakson ajan. Poikkeamien osalta nähdään merkittävä lasku erityisesti vuoden 2023 jälkeen, jolloin ei-kriittisten poikkeamien määrä putoaa hyvin matalalle tasolle ja kriittiset poikkeamat lähes katoavat. Tämä voi viitata joko aidosti vähentyneisiin poikkeamiin tai muutoksiin raportointikäytännöissä.

Valtionhallinnossa oma työpanos on kasvava vuosina 2022–2024 ja saavuttaa huipun vuonna 2024, minkä jälkeen se hieman laskee. Ostettujen resurssien käyttö kasvaa selvästi tarkastelujakson loppua kohti. Poikkeamien osalta ei-kriittisten tapausten määrä kasvaa tasaisesti ja saavuttaa huipun vuonna 2026, kun taas kriittiset poikkeamat pysyvät vähäisinä koko ajanjakson ajan. Tämä viittaa siihen, että lisääntynyt työpanos on yhteydessä kasvaneeseen havaintokykyyn.

4.6.2 Resurssien ja poikkeamien suhteen tulkinta

Kokonaisuutena tarkasteltuna kuvasta ei ole havaittavissa yksinkertaista lineaarista suhdetta työpanoksen ja poikkeamien määrän välillä. Useimmissa organisaatiotyypeissä resurssien kasvu ei johda poikkeamien vähenemiseen, vaan usein päinvastoin poikkeamien määrä kasvaa samaan aikaan.

Tämä ilmiö selittyy todennäköisesti sillä, että resurssien lisääntyminen parantaa organisaatioiden kykyä havaita, analysoida ja raportoida poikkeamia. Näin ollen kasvava poikkeamien määrä voi kuvata parempaa kyvykkyyttä eikä heikompaa turvallisuustilannetta.

Erityisesti hyvinvointialueilla voimakas samanaikainen kasvu sekä resursseissa että poikkeamissa viittaa merkittävään kyvykkyyden kehitysvaiheeseen, jossa organisaatiot rakentavat aktiivisesti digiturvan hallintaa ja samalla parantavat näkyvyyttään uhkiin.

Korkeakoulujen kehitys poikkeaa muista, mikä korostaa sitä, että resurssien ja poikkeamien välinen suhde ei ole universaali, vaan riippuu myös toimintaympäristöstä ja käytännöistä.

4.6.3 Johtopäätökset

Tulokset osoittavat, että digiturvaan käytettävän työpanoksen lisääntyminen ei automaattisesti vähennä poikkeamien määrää, ainakaan lyhyellä aikavälillä. Päinvastoin kehitysvaiheessa resurssien kasvu voi johtaa poikkeamien määrän kasvuun, kun havaintokyky ja raportointi paranevat.

Kriittisten poikkeamien pysyminen suhteellisen matalalla tasolla kaikissa organisaatiotyypeissä on kuitenkin merkittävä havainto, joka viittaa siihen, että vakavien häiriöiden hallinta on keskimäärin hyvässä tasossa.

Ei-kriittisten poikkeamien kasvu korostaa operatiivisen tietoturvan merkitystä ja tarvetta käsitellä suuri määrä havaintoja tehokkaasti.

Lisäksi organisaatiotyyppien välillä on merkittäviä eroja kehitysdynamiikassa, mikä viittaa erilaisiin kypsyystasoihin, resursseihin ja toimintamalleihin.

4.6.4 Kehittämisnäkökulmat

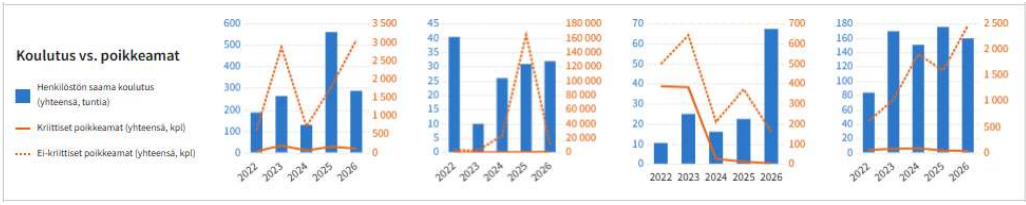
Keskeiseksi kehittämistarpeeksi nousee resurssien vaikuttavuuden arviointi. Organisaatioiden tulisi pystyä yhdistämään työpanos, havaittujen poikkeamien määrä ja niiden käsittelyn tehokkuus yhdeksi kokonaisuudeksi, jotta resurssien kohdentaminen olisi mahdollisimman tarkoituksenmukaista.

Lisäksi on tärkeää kehittää mittareita, jotka erottavat toisistaan havaintokyvyn paranemisen ja todellisen riskitason muutoksen. Tämä auttaa tulkitsemaan kasvavia poikkeamamääriä oikeassa kontekstissa.

Kokonaisuutena kehittämisen painopisteenä tulisi olla siirtyminen pelkästä resurssien lisäämisestä kohti niiden vaikuttavaa käyttöä, jossa tavoitteena on sekä poikkeamien ehkäisy että niiden tehokas hallinta.

4.7 Koulutus vs. poikkeamat

Kuvaaja. Digiturvan koulutukset henkilöstölle suhteessa tietoturvapoikkeamiin. Kuvaajassa kunnat, HVA:t, Korkeakoulut, Valtiohallinto



Kuvassa tarkastellaan henkilöstön saaman digitaalisen turvallisuuden koulutuksen määrän (tunnit yhteensä) sekä kriittisten ja ei-kriittisten tietoturvapoikkeamien kokonaismäärän kehitystä vuosina 2022–2026 neljässä organisaatiotyypissä: kunnissa, hyvinvointialueilla ja muissa sote-toimijoissa, korkeakouluissa sekä valtionhallinnossa.

Koulutusta kuvaava pylväsdiagrammi on yhdistetty kahteen viivaan, jotka kuvaavat kriittisiä ja ei-kriittisiä poikkeamia. Näin voidaan tarkastella, onko koulutuksen määrällä yhteyttä poikkeamien kehitykseen.

Kokonaisuutena tarkasteltuna koulutuksen määrä kasvaa useimmissa organisaatiotyypeissä tarkastelujakson aikana, mutta kehitys ei ole tasainen. Poikkeamien määrissä nähdään samanaikaisesti merkittäviä vaihteluita, eikä yhteys koulutuksen määrän ja poikkeamien välillä ole yksiselitteinen.

4.7.1 Keskeiset havainnot

Kuntien osalta koulutusmäärä kasvaa selvästi tarkastelujakson aikana ja saavuttaa huipun vuonna 2025, jonka jälkeen taso hieman laskee mutta pysyy edelleen korkeana. Samanaikaisesti ei-kriittisten poikkeamien määrä vaihtelee voimakkaasti: vuonna 2023 nähdään selvä huippu, jota seuraa lasku ja uusi kasvu vuoteen 2026 mennessä. Kriittiset poikkeamat pysyvät koko tarkastelujakson ajan vähäisinä. Tämä ehdottaa, että koulutuksen lisääntyminen ei suoraan vähennä havaittuja poikkeamia.

Hyvinvointialueiden ja sote-toimijoiden osalta koulutuksen määrä kasvaa tasaisesti vuoden 2022 matalalta tasolta kohti vuotta 2025, jonka jälkeen se hieman laskee vuonna 2026. Ei-kriittisten poikkeamien määrä kasvaa erityisesti vuosina 2024–2025, jolloin saavutetaan selvä huippu, ja laskee tämän jälkeen. Kriittiset poikkeamat pysyvät vähäisinä koko tarkastelujakson ajan. Kehitys viittaa siihen, että koulutuksen lisääntyminen ajoittuu samaan aikaan havaintojen kasvun kanssa.

Korkeakoulujen osalta koulutuksen määrä on kokonaisuudessaan maltillisempi, mutta kasvaa selvästi tarkastelujakson aikana ja saavuttaa korkeimman tason vuonna 2026. Poikkeamien kehitys on kuitenkin laskeva: ei-kriittisten poikkeamien määrä on korkeimmillaan vuonna 2023, minkä jälkeen se laskee selvästi. Kriittiset poikkeamat pysyvät hyvin matalalla tasolla koko tarkastelujakson ajan. Tämä organisaatioryhmä on ainoa, jossa koulutuksen kasvu yhdistyy poikkeamien vähenemiseen.

Valtionhallinnossa koulutusmäärä kasvaa tasaisesti koko tarkastelujakson ajan ja saavuttaa korkeimman tason vuonna 2026. Samanaikaisesti ei-kriittisten poikkeamien määrä kasvaa voimakkaasti, erityisesti vuosina 2023–2025, ja pysyy korkealla tasolla myös vuonna 2026. Kriittiset poikkeamat pysyvät vähäisinä. Tämä viittaa siihen, että koulutus ei suoraan vähennä havaittujen poikkeamien määrää, vaan voi liittyä havaintokyvyn paranemiseen.

4.7.2 Koulutuksen ja poikkeamien suhteen tulkinta

Kokonaiskuva osoittaa, että koulutuksen määrän ja poikkeamien määrän välillä ei ole yksinkertaista tai lineaarista yhteyttä. Useimmissa organisaatiotyypeissä koulutuksen lisääntyminen ei johda poikkeamien määrän vähenemiseen, vaan usein päinvastoin poikkeamien määrä kasvaa samanaikaisesti.

Tämä ilmiö on johdonmukainen aiempien tarkastelujen kanssa, joissa havaittiin, että kyvykkyyksien kehittyminen lisää myös havaintojen määrää. Koulutus parantaa henkilöstön tietoisuutta ja valmiutta tunnistaa poikkeamia, mikä voi lisätä raportointia erityisesti ei-kriittisten tapausten osalta.

Korkeakoulujen poikkeava kehitys, jossa koulutuksen kasvu yhdistyy poikkeamien vähenemiseen, voi viitata joko tehokkaaseen osaamisen kehittymiseen tai muutoksiin raportointikäytännöissä. Tämä korostaa sitä, että organisaatiokohtaiset tekijät vaikuttavat merkittävästi tuloksiin.

Kriittisten poikkeamien vähäisyys kaikissa organisaatiotyypeissä on tärkeä havainto. Se viittaa siihen, että vakavien poikkeamien hallinta on keskimäärin hyvällä tasolla, eikä koulutuksen määrän vaihtelu näytä vaikuttavan merkittävästi niiden esiintymiseen.

4.7.3 Johtopäätökset

Tulokset osoittavat, että koulutus on keskeinen osa digiturvan kehittämistä, mutta sen vaikutukset eivät näy lyhyellä aikavälillä poikkeamien määrän vähenemisenä. Päinvastoin koulutuksen lisääntyminen voi johtaa poikkeamien määrän kasvuun, kun henkilöstön kyky tunnistaa ja raportoida poikkeamia paranee.

Ei-kriittisten poikkeamien kasvu useimmissa organisaatiotyypeissä korostaa operatiivisen tietoturvan merkitystä ja tarvetta käsitellä havaintoja tehokkaasti. Samalla kriittisten poikkeamien pysyminen matalalla tasolla ehdottaa, että vakavimmat riskit ovat hallinnassa.

Organisaatiotyyppien välillä on eroja siinä, miten koulutus ja poikkeamat kehittyvät suhteessa toisiinsa. Tämä viittaa siihen, että koulutuksen vaikuttavuus riippuu myös muista tekijöistä, kuten prosesseista, teknologioista ja johtamisesta.

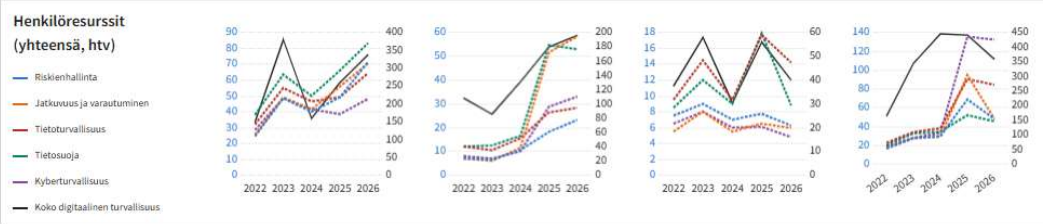
4.7.4 Kehittämisnäkökulmat

Keskeiseksi kehittämistarpeeksi nousee koulutuksen vaikuttavuuden parempi arviointi. Pelkkä koulutusmäärän lisääminen ei riitä, vaan organisaatioiden tulee varmistaa, että koulutus kohdistuu oikeisiin riskeihin ja tukee käytännön toimintaa.

Lisäksi organisaatioiden tulisi kehittää mittareita, jotka ottavat huomioon havaintokyvyn paranemisen vaikutuksen poikkeamamääriin. Tämä auttaa tulkitsemaan kehitystä oikein ja välttämään virheelliset johtopäätökset.

Kokonaisuutena kehittämisen painopisteenä tulisi olla koulutuksen laadun, kohdennuksen ja vaikuttavuuden vahvistaminen siten, että se tukee sekä poikkeamien ennaltaehkäisyä että niiden tehokasta tunnistamista ja hallintaa.

4.8 Henkilöresurssien kehityksen vertailu



Kuvassa esitetään digiturvan henkilöstöresurssien (henkilötyövuosien) jakautuminen ja kehitys vuosina 2022–2026 viidellä osa-alueella: riskienhallinta, jatkuvuus ja varautuminen, tietoturvallisuus, tietosuoja sekä kyberturvallisuus. Lisäksi esitetään näiden yhteenlaskettu kokonaisresurssi ("koko digitaalinen turvallisuus"). Tarkastelu on jaettu neljään organisaatiotyyppiin: kunnat, hyvinvointialueet ja muut sote-toimijat, korkeakoulut sekä valtionhallinto.

Kokonaisuutena kaikissa organisaatiotyypeissä nähdään kasvava tai vähintään vaihteleva kehityssuunta, jossa digiturvaan kohdennettujen resurssien määrä kasvaa tarkastelujakson loppua kohti. Samalla eri osa-alueiden välinen resursointi ei ole tasapainoista, vaan painottuu erityisesti tietoturvaan ja kokonaisuuden kasvattamiseen.

4.8.1 Keskeiset havainnot

Kuntien osalta kokonaisresurssi kasvaa selvästi tarkastelujakson aikana, nousten noin 40 henkilötyövuodesta vuonna 2022 yli 80 henkilötyövuoteen vuonna 2026. Kehityksessä on kuitenkin notkahdus vuonna 2024, jonka jälkeen kasvu jatkuu. Tietosuoja ja tietoturva muodostavat suurimman resurssiosuuden koko ajanjakson ajan, kun taas kyberturvallisuus jää tasaisesti muita osa-alueita pienemmäksi. Riskienhallinta ja jatkuvuus kehittyvät tasaisesti mutta maltillisesti.

Hyvinvointialueilla ja sote-toimijoilla kehitys on voimakkaampaa. Kokonaisresurssi kasvaa erityisesti vuosien 2023–2025 välillä, nousten noin 30 henkilötyövuodesta lähes 60 henkilötyövuoteen. Kaikki osa-alueet kasvavat samanaikaisesti, mutta erityisesti jatkuvuus ja varautuminen sekä tietoturvallisuus lisääntyvät voimakkaasti. Vuonna 2026 nähdään lievä lasku kokonaisresurssissa, mikä voi viitata resurssien uudelleenkohdentamiseen.

Korkeakoulujen osalta kehitys on epätasaisempaa. Kokonaisresurssi vaihtelee selvästi vuosittain ja saavuttaa huipun vuosina 2023 ja 2025, mutta laskee taas vuonna 2026. Osa-aluekohtaisesti tietoturva ja tietosuoja ovat suurimmat, mutta niidenkin osalta nähdään merkittävää vaihtelua. Kyberturvallisuus pysyy koko ajan pienimpänä osa-alueena. Tämä viittaa siihen, että resursointi ei ole täysin vakiintunutta.

Valtionhallinnossa kehitys on selkeimmin kasvavaa. Kokonaisresurssi kasvaa tasaisesti koko tarkastelujakson ajan ja saavuttaa korkeimman tason vuonna 2025, jonka jälkeen taso hieman tasaantuu. Tietoturvallisuus ja tietosuoja muodostavat merkittävimmän osan resursseista. Kuitenkin myös riskienhallinta ja jatkuvuus kasvavat. Kyberturvallisuus kasvaa tarkastelujaksolla, mutta pysyy edelleen pienempänä muihin osa-alueisiin verrattuna.

4.8.2 Resurssirakenteen tulkinta

Kuvasta nousee esiin selkeä rakenne, jossa tietoturva ja tietosuoja ovat kaikissa organisaatiotyypeissä vahvimmin resursoituja osa-alueita. Tämä viittaa siihen, että perinteiset sääntelyyn ja vaatimustenmukaisuuteen liittyvät osa-alueet ovat vakiinnuttaneet asemansa organisaatioissa.

Riskienhallinta ja jatkuvuus kehittyvät pääosin tasaisesti, mutta niiden resurssitaso jää monin paikoin alemmaksi kuin tietoturvan ja tietosuojan. Tämä tukee aiemmissa analyyseissa havaittua ilmiötä, jossa strategisemmat ja poikkileikkaavat osa-alueet eivät ole yhtä vahvasti resursoituja.

Kyberturvallisuus erottuu kaikissa organisaatiotyypeissä heikoimmin resursoituna osa-alueena. Vaikka siinä on havaittavissa kasvua, taso jää systemaattisesti muiden osa-alueiden alapuolelle. Tämä viittaa siihen, että kyberturvallisuus ei ole vielä saavuttanut samaa prioriteettia kuin muut digiturvan osa-alueet.

4.8.3 Johtopäätökset

Tulokset osoittavat, että digiturvan henkilöstöresurssit ovat kasvaneet useimmissa organisaatiotyypeissä. Tämä ehdottaa digitaaliseen turvallisuuteen panostuksen lisääntymistä. Kasvu ei kuitenkaan ole tasaista, vaan siihen liittyy vaihtelua sekä vuosittain että organisaatiotyypeittäin.

Keskeinen havainto on, että resurssit kohdentuvat epätasaisesti eri osa-alueille. Tietoturva ja tietosuoja ovat vakiintuneita ja vahvasti resursoituja, kun taas kyberturvallisuus sekä osittain riskienhallinta ja jatkuvuus jäävät vähemmälle huomiolle.

Organisaatiotyyppien välillä erot ovat merkittäviä. Valtionhallinto ja hyvinvointialueet näyttävät kehittyvän systemaattisemmin, kun taas kunnissa ja korkeakouluissa kehitys on epätasaisempaa ja riippuu enemmän yksittäisistä vuosista.

4.8.4 Kehittämisnäkökulmat

Keskeiseksi kehittämistarpeeksi nousee resurssien tasapainottaminen eri digiturvan osa-alueiden välillä. Erityisesti kyberturvallisuuteen tulisi kohdentaa enemmän resursseja, jotta se vastaisi sen kasvavaa merkitystä toimintaympäristössä.

Lisäksi organisaatioiden tulisi pyrkiä vähentämään vuosittaista vaihtelua resursoinnissa ja siirtyä kohti pitkäjänteisempää ja ennakoivampaa resursointimallia. Tämä tukisi kyvykkyyksien tasaisempaa kehitystä.

Kokonaisuutena tarkastellen kehittämisen painopisteenä tulisi olla digiturvan kokonaisuuden hallinta siten, että kaikki keskeiset osa-alueet kehittyvät samassa tahdissa ja muodostavat yhtenäisen, vaikuttavan turvallisuuskokonaisuuden

5 Havainnot

Tässä osiossa organisaatiot raportoivat, kuinka eri uhat ovat toteutuneet niiden toiminnassa edellisenä kalenterivuonna. Seuraavalla sivulla on esitetty digiturvapoikkeamien havainnointiin liittyviä tuloksia.

Henkilötietojen ja luottamuksellisten tietojen käsittelyyn liittyvät poikkeamat muodostavat aineiston merkittävimmän ilmiön. Ohjeiden vastainen tietojen käsittely luvattomilla laitteilla tai palveluissa koskee noin neljännestä organisaatioista (24 %), ja havaintojen kokonaismäärä on korkea. Lisäksi henkilötietojen tietoturvaloukkaukset, jotka edellyttävät ilmoitusta viranomaiselle (42 %) tai rekisteröidyille (39 %), ovat yleisiä.

Tekniset häiriöt kriittisissä palveluissa ovat kaikkein yleisin havaintotyyppi. Jopa 65 prosenttia organisaatioista raportoi jonkin verran toimintaa haitanneita teknisiä häiriöitä. Merkittävästi toimintaa haitanneet häiriöt ovat harvinaisempia (36 %), mutta niiden vaikutus on luonnollisesti suurempi.

Käyttäytymiseen ja inhimillisiin tekijöihin liittyvät havainnot korostuvat myös. Esimerkiksi päätelaitteiden varastaminen koskee 29 prosenttia organisaatioista, ja salassa pidettävien tietojen luvaton käsittely työntekijän toimesta, vaikka harvinaisempaa (4 %), on edelleen merkittävä riski.

Tietoturvauhkista korostuvat huijausviestit ja vaikuttamispyrkimykset. Noin 36 prosenttia organisaatioista raportoi huijausviestejä organisaation nimissä, ja lisäksi sekä sosiaalisen median vaikuttamisyritykset (9 %) että organisaatioon kohdistuva informaatiovaikuttaminen (10 %) ovat havaittavia ilmiöitä.

Toimitusketjuun liittyvät riskit näkyvät siinä, että 22 prosenttia organisaatioista raportoi palvelutoimittajan tai kumppanin toimineen vastoin tietoturva- tai tietosuojakäytäntöjä.

5.1 Havaintojen jakauman tulkinta

Tuloksissa korostuu vahvasti havaintojen epätasainen jakautuminen. Vaikka mediaani on lähes kaikissa tapauksissa nolla, maksimiarvot ovat monin paikoin erittäin korkeita. Esimerkiksi yksittäisissä tapauksissa on raportoitu satoja tai jopa tuhansia havaintoja yhden ilmiön osalta.

Tämä kertoo organisaatioiden välillä olevan merkittäviä eroja joko riskialttiudessa, toimintaympäristössä tai kyvykkyydessä havaita ja kirjata poikkeamia. Suuret arvot voivat kuvastaa esimerkiksi laajamittaisia tapahtumia, automatisoitua havaintoa tai kehittynyttä valvontaa.

Lisäksi tulokset osoittavat selkeän eron harvinaisten mutta vakavien tapahtumien ja yleisten mutta vähemmän vakavien poikkeamien välillä. Esimerkiksi tietomurrot tai haittaohjelmat päätelaitteissa ovat harvinaisia, kun taas tekniset häiriöt ja ohjeiden vastainen toiminta ovat selvästi yleisempiä.

5.1.1 Johtopäätökset

Tulokset osoittavat, että digiturvan keskeiset riskit liittyvät erityisesti arjen toimintaan, tiedonkäsittelyyn ja tekniseen toimintavarmuuteen. Vakavat kyberhyökkäykset tai merkittävät tietomurrot ovat suhteellisen harvinaisia, mutta niiden vaikutukset voivat olla merkittäviä.

Keskeinen havainto on, että inhimilliset tekijät ja toimintaprosessit muodostavat merkittävän osan riskeistä. Ohjeiden vastainen tietojen käsittely, huijausviestit ja toimitusketjujen haasteet korostavat sitä, että tekninen tietoturva ei yksin riitä.

Lisäksi tulokset viittaavat siihen, että organisaatioiden havaintokyky ja raportointikäytännöt vaihtelevat merkittävästi. Suurten havaintomäärien esiintyminen yksittäisissä organisaatioissa voi kuvastaa kypsää valvontaa, ei pelkästään korkeaa riskitasoa.

5.1.2 Tulkintaa havaintojen luonteesta

1. Tietosuoja- ja henkilötietoloukkaukset

Erityisesti nämä ovat vakavia, koska ne voivat johtaa viranomaisprosesseihin, rekisteröityjen informointiin, mainehaittaan ja korjaaviin velvoitteisiin.

2. Julkisten järjestelmien kriittiset haavoittuvuudet

Kriittiset haavoittuvuudet ovat erittäin merkittävä, koska hyödynnettävissä oleva haavoittuvuus voi nopeasti muuttua laajaksi tietomurroksi tai palveluhäiriöksi. Näiden määrän pelätään kasvavan merkittävästi seuraavan vuoden aikana tekoälymallien kehittymisen myötä.

3. Kriittisten palveluiden jatkuvuushäiriöt

Tekniset häiriöt ovat yleisiä ja vaikuttavat suoraan organisaation toimintakykyyn

5.1.3 Kehittämisnäkökulmat

Keskeiseksi kehittämistarpeeksi nousee inhimillisten riskien hallinta. Organisaatioiden tulisi vahvistaa ohjeistusta, koulutusta ja valvontaa erityisesti henkilötietojen käsittelyyn ja laitteiden käyttöön liittyen.

Toiseksi tärkeäksi kehittämiskohteeksi nousee jatkuvuuden ja toimintavarmuuden parantaminen, koska tekniset häiriöt ovat yleisimpiä havaittuja ilmiöitä. Tämä edellyttää sekä teknisiä että organisatorisia toimenpiteitä.

Kolmantena keskeisenä näkökulmana on toimitusketjujen ja ulkoisten toimijoiden hallinta. Tulokset osoittavat, että kumppaneihin liittyvät riskit ovat merkittäviä, ja niiden hallinta edellyttää systemaattisia sopimus- ja valvontakäytäntöjä.

Neljäntenä näkökulmana voidaan pitää kvanttivarautumisen kehittämistä lähitulevaisuudessa. Digiturvan kokonaiskuvapalvelu ei vielä mittaa kvanttivarautumisen tasoa, mutta siltä osin kokonaiskuvapalvelua tullaan kehittämään. Julkishallinnon organisaatioiden näkökulmasta kvanttivarautuminen tulee olla jo käynnissä kvantti-inventaarion muodossa. Kvanttiturvalliset ratkaisut tulee olla käytössä 2029 vuoden loppuun mennessä ja kvanttiturvallinen organisaatioiden tulee olla 2030-luvun puoliväliin mennessä.

Kokonaisuutena tarkasteltuna kehittämisen painopisteenä tulisi olla siirtyminen yksittäisten poikkeamien tarkastelusta kohti kokonaisvaltaista riskienhallintaa, jossa huomioidaan sekä tekniset, inhimilliset että organisatoriset tekijät.

DIGI- JA VÄESTÖTIETO-VIRASTO

Havainnointi						
Vastausten lkm (N)	Osuus vastauksista, joissa havaintoja yli 0 kpl	Minimi	Mediaani	Maksimi	Summa	Kysymys
198	12% (24)	0	0	5	46	1. Organisaation itse tuottamiin palveluihin on kohdistunut onnistunut hyökkäys, joka on aiheuttanut tietomurron, tietovuodon tai henkilötietojen tietoturvaloukkauksen (havaintoja, kpl)
197	20% (40)	0	0	15	101	2. Organisaatio on vastaanottanut ICT-palvelutoimittajilta ilmoituksen hyökkäyksestä, joka on aiheuttanut tietomurron, tietovuodon tai henkilötietojen tietoturvaloukkauksen. (havaintoja, kpl)
196	24% (47)	0	0	627	872	3. Organisaation salassa pidettäviä tietoja tai henkilötietoja on käsitelty ohjeiden vastaisesti luvattomilla laitteilla tai luvattomissa palveluissa. (havaintoja, kpl)
197	42% (82)	0	0	593	2246	4. Organisaation käytössä olevaan palveluun on kohdistunut henkilötietojen tietoturvaloukkaus, joka on edellyttänyt ilmoitusta valvontaviranomaiselle. (havaintoja, kpl)
198	39% (78)	0	0	270	1295	5. Organisaation käytössä olevaan palveluun on kohdistunut henkilötietojen tietoturvaloukkaus, joka on edellyttänyt ilmoitusta rekisteröidyille. (havaintoja, kpl)
197	65% (128)	0	1	500	1860	6. Organisaation käyttämissä kriittisissä palveluissa on ollut tekninen häiriö, joka on jonkin verran haitannut organisaation toimintaa. (havaintoja, kpl)
198	36% (71)	0	0	64	389	7. Organisaation käyttämissä kriittisissä palveluissa on ollut tekninen häiriö, joka on merkittävästi haitannut organisaation toimintaa. (havaintoja, kpl)
197	3% (5)	0	0	3	12	8. Organisaation käytössä olevaan päätelaitteeseen on päässyt haittaohjelma, joka on esim. lukinnut päätelaitteen salaamalla tai aiheuttanut tietovuodon. (havaintoja, kpl)
197	1% (2)	0	0	1	2	9. Organisaation käytössä olevaan palveluun on päässyt haittaohjelma, joka on esim. estänyt palvelun käytön tai aiheuttanut tietovuodon. (havaintoja, kpl)
197	19% (38)	0	0	11	82	10. Organisaation käytössä olleeseen palveluun on kohdistunut palvelunestohyökkäys, joka on jonkin verran haitannut organisaation toimintaa. (havaintoja, st)
197	3% (5)	0	0	2	7	11. Organisaation käytössä olleeseen palveluun on kohdistunut palvelunestohyökkäys, joka on merkittävästi haitannut organisaation toimintaa. (havaintoja, kpl)
198	29% (57)	0	0	10	132	12. Organisaation omistama päätelaite on varastettu (havaintoja, kpl)
197	30% (60)	0	0	1600	1822	13. Organisaation julkiseen verkkoon näkyvässä tietojärjestelmässä tai verkossa on ollut kriittinen ja hyödynnettävissä ollut tietoturvahaavoittuvuus. (havaintoja, kpl)
198	16% (32)	0	0	24	102	14. Organisaation työntekijä on tietoisesti luvattomasti käsitellyt salassa pidettäviä tietoja tai henkilötietoja. (havaintoja, kpl)
197	4% (8)	0	0	5	14	15. Organisaation kriittisiä tai lakisääteisesti säilytettäviä tietoja on korruptoitunut tai tuhoutunut lopullisesti. (havaintoja, kpl)
198	36% (72)	0	0	600	1036	16. Organisaation nimissä on lähetetty huijausviestejä, jossa yritetään urkkia asiakkaiden tai muiden henkilöiden tietoja. (havaintoja, kpl)
198	22% (43)	0	0	67	291	17. Organisaation palveluita tuottava toimittaja, alihankkija tai kumppani on toiminut vastoin sovittuja tietoturva- tai tietosuojakäytäntöjä. (havaintoja, kpl)
197	14% (28)	0	0	55	156	18. Organisaation web- tai sosiaalisen median kanaviin on ulkopuolisten tahojen toimesta yritetty vaikuttaa bottien, trollitilien tai vastaavien avulla tai muilla keinoilla. (havaintoja, kpl)
194	9% (18)	0	0	100	259	19. Organisaation henkilöstöön tai organisaation toimintaan on yritetty vaikuttaa informaatiovaikuttamisen keinoin, esim. painostamalla tai muilla mielipidevaikuttamisen keinoilla, jotka ovat organisaation arvojen vastaisia. (havaintoja, kpl)
197	10% (20)	0	0	20	74	20. Organisaatio on ollut räätälöidyn, kohdistetun tietoturva- tai kyberhyökkäyksen kohteena. (havaintoja, kpl)