

# TUTKIMUS PÄIJÄTHÄMÄLÄISTEN PK- YRITYSTEN TIETOTURVAN JA TIETOSUOJAN HALLINNASTA

LAHDEN AMMATTIKORKEAKOULU  
Insinööri (AMK)  
Tietokone-elektroniikka  
Kevät 2019  
Juhani Haikka

## Tiivistelmä

Tekijä(t) Haikka, Juhani	Julkaisun laji Opinnäytetyö, AMK	Valmistumisaika Kevät 2019
	Sivumäärä 29	
Työn nimi <b>Tutkimus päijäthämäläisten pk-yritysten tietoturvan ja tietosuojan hallinnasta</b>		
Tutkinto Tietotekniikan koulutusohjelma, Insinööri (AMK)		
<p>Tiivistelmä</p> <p>Opinnäytetyön tarkoituksena oli tehdä tietoturva- ja tietosuojakartoituksia muutamiin päijäthämäläisiin pk-yrityksiin ja kartoitusten perusteella analysoida, kuinka yritykset olivat hoitaneet tietoturvaansa sekä kuinka yritykset olivat valmistautuneet EU:n uuteen, 25.5.2018 voimaantulleeseen tietosuoja-asetukseen (GDPR).</p> <p>Kartoitukset tehtiin alkuvuodesta 2018 erään tietoturvayrityksen kehittämän kartoitusohjelmiston avulla. Näiden kartoitusten perusteella yritysten tuloksia vertailtiin keskenään anonymisti.</p> <p>Työssä käydään läpi kartoitustuloksia ja pohditaan, mitkä asiat vaikuttivat eri osa-alueiden vaihtelevaan suoritustasoon.</p> <p>Kaiken kaikkiaan kohdeyritykset saivat paremman kuvan senhetkisestä tilanteestaan tietoturvan ja tietosuojan kannalta katsottuna ja samalla osviittaa, mihin asioihin tulisi keskittyä lähitulevaisuudessa.</p>		
Asiasanat GDPR, tietoturva, tietosuoja, tietoturvan hallinta, tietosuojan hallinta		

## Abstract

Author(s) Haikka, Juhani	Type of publication Bachelor's thesis	Published Spring 2019
	Number of pages 29	
Title of publication Information security and data protection management in small and medium-sized companies in Päijät-Häme.		
Name of Degree Bachelor of Engineering, Information and Communications Technology		
<p>Abstract</p> <p>The purpose of this thesis was to analyze the data protection (GDPR-readiness) and information security of small and medium-sized companies in Päijät-Häme, Finland, and compare the results anonymously.</p> <p>Analysis tools were provided by an information security company. The analyses were made in early 2018 one to four months before the implementation of GDPR. The names of the companies included in this thesis are confidential and therefore made anonymous and compared anonymously as well (Non-Disclosure Agreements).</p> <p>As a result of the thesis, the companies involved gained a better understanding of their current situation concerning data protection and information security and what could be done better in the near future.</p>		
<p>Keywords</p> <p>GDPR, information security, data protection, information security management, data protection management</p>		

## SISÄLLYS

1	JOHDANTO .....	1
2	TUTKIMUKSEN TAVOITE JA TARKOITUS.....	2
3	KÄSITTEITÄ .....	3
4	TEOREETTINEN TAUSTA .....	5
4.1	Mitä tietoturvan hallinta on .....	5
4.2	Opinnäytetyössä käytetyn tietoturvakartoituksen rakenne.....	5
4.3	Opinnäytetyössä käytetty tietosuojakartoitus .....	7
5	TUTKIMUKSEN LÄPIKÄYNTI.....	9
5.1	Tietoturvan hallinta .....	9
5.2	GDPR-kartoitus .....	11
5.3	ICT-hallinta .....	14
5.4	Henkilöstö.....	15
5.5	Käyttövaltuudet.....	16
5.6	PC:t ja mobiililaitteet .....	17
5.7	Kiinteistöt.....	19
5.8	Tietojärjestelmät .....	20
5.9	Yhteenvetokuvaaja .....	21
6	YHTEENVETO .....	23
	LÄHTEET .....	25

## 1 JOHDANTO

Opinnäytetyön aiheena oli tutkia pääjätthämäläisten pk-yritysten tietoturvan ja tietosuojan hallintaa. Työn ensimmäinen vaihe oli tehdä tietoturva- ja tietosuojakartoituksia muuttamaan pääjätthämäläiseen pk-yritykseen. Työssä käydään läpi näistä kartoituksista saatuja tuloksia ja pohditaan yritysten kartoitusmenestystä tai sen puutetta ja tähän johtaneita syitä.

Työskennellessäni Lahden ammattikorkeakoulun (LAMK) harjoittelujaksolla eräässä tietoturva-yrityksessä aloitin 2017-2018 vuodenvaihteessa työskentelemään tietoturva- ja tietosuojakartoituksien parissa.

Sain tästä aihealueesta idean opinnäytetyöhöni, jossa suoritin muutamiin Pääjät-Hämäläisiin yrityksiin noin yhdestä kahteen tuntia kestävän tietoturva- ja tietosuojakartoituksen. Näiden kartoitustulosten myötä tutkin kohdeyritysten tietoturvan ja tietosuojan hallinnan tasoa. Yrityksiä käsitellään tässä opinnäytetyössä anonymisti ja niihin viitataan sanoilla ”Yritys 1, Yritys 2...”. Myös kartoituskysymykset ovat salassapidettävää tietoa ja tämän takia tutkimuksen läpikäynti -osiossa niitä ei kuvailla kovinkaan yksityiskohtaisesti.

Opinnäytetyössä käytetty kartoitus sisälsi tietoturvan tilaa käsittelevän kartoituksen, joka koostui lukuisista tietoturvan eri osa-alueista. Nämä alueet on selitetty auki opinnäytetyön teoriaosuudessa. Osa-alueet luokiteltiin kategorioittain johdonmukaisesti, jotta yritykset saivat selkeän kuvan, millä osa-alueilla oli parantamisen varaa ja mitkä osa-alueet oli hyvin toteutettu.

Kartoituksen toinen osio käsitteli tietosuojaa ja sen vaatimuksia, erityisesti 25.5.2018 voimaantulleen EU:n yleisen tietosuoja-asetuksen (GDPR) näkökulmasta. Tämä tietosuojaosuus kesti ajallisesti läpikäytynä noin puolet kartoitukseen käytetystä 1 - 2 tunnista.

Kartoituksien tekoaikaan varsinkin tietosuojapuolen kartoitus oli hyvin ajankohtainen, sillä EU:n uuden tietosuoja-asetuksen voimaantuloon oli enää keskimäärin pari kuukautta aikaa ja tämä tietosuoja-asetus koski kaikenkokoisia henkilötietoja käsitteleviä yrityksiä alaan katsomatta (vaikka yrityksillä ei olisi henkilöasiakkaita, ne käsittelevät kuitenkin oman henkilökuntansa henkilötietoja).

## 2 TUTKIMUKSEN TAVOITE JA TARKOITUS

Työn tarkoituksena oli tehdä tietoturva- ja tietosuojakartoituksia Päijät-Hämeen alueella toimiviin pk-yrityksiin ja näiden kartoitusten avulla analysoida tietoturvan ja tietosuojan hallintaa ja muodostaa kartoitustulosten avulla kokonaiskuva tietoturvan ja tietosuojan tilasta sekä pohtia, mitä voisi jatkossa toteuttaa paremmin ja miksi yritykset suoriutuivat joillakin osa-alueilla heikommin kuin toisilla.

EU:n tietosuoja-asetuksen suhteen kartoituksiin varautuminen oli kartoitusten tekoaikaan vielä heikohkoa, koska voimaantuloon oli aikaa ensimmäistä kartoitusta tehtäessä neljä kuukautta ja viimeistä kuukausi. Täytyy myös ottaa huomioon, että resursseja tämän ko-koisissa yrityksissä on rajatusti. Tietoturvapuolen kartoituskysymykset olivat kuitenkin melko yleismaailmallisia tietosuojapuolen kartoitukseen verrattuna ja näitä käsiteltäessä sai hyvän kuvan senhetkisestä tietoturvan toteutuksen tilanteesta.

### 3 KÄSITTEITÄ

GDPR – GDPR (General Data Protection Regulation) on EU:n yleinen tietosuoja-asetus (2016/679) (Euroopan unionin virallinen lehti 2016). Se on uusi henkilötietojen käsittelyä sääntelevä laki, jota sovelletaan kaikissa EU-maissa 25.5.2018 alkaen. GDPR antaa paremman suojan henkilötiedoille ja enemmän keinoja hallita tietojen käsittelyä. Uuden lain-säädännön tavoitteena on parantaa henkilötietojen suojaa ja tietosuojaoikeuksia, vastata uusiin digitalisaatioon ja globalisaatioon liittyviin tietosuojakysymyksiin, yhtenäistää tietosuojasääntelyä kaikissa EU-maissa ja edistää digitaalisten sisämarkkinoiden kehittymistä (Tietosuojavaltuutetun toimisto 2019e). Se on tärkein henkilötietoja koskeva tietosuojauudistus kahteenkymmeneen vuoteen (EU GDPR Portal 2019).

TIETOTURVA - Tietoturvalla tarkoitetaan tietojen, tietojärjestelmien, palveluiden ja verkkoliikenteen suojaamista. Tietoturvallisuuden katsotaan koostuvan luottamuksellisuudesta (engl. confidentiality), eheydestä (engl. integrity) ja käytettävyydestä tai saatavuudesta (engl. availability). Tietoturvan hallinta pitää sisällään muun muassa riskienhallintaa, suojausmenettelyiden rakentamista niin henkilöstö-, fyysisen- ja tietoteknisen turvallisuuden näkökulmasta sekä tietoturvapoikkeamien käsittelyä. Näistä tulee luonnollisesti kommunikoida henkilöstölle ohjeistuksen muodossa, ihminen on kuitenkin tietoturvallisuuden heikoin osa. Osa-alueina voivat olla esimerkiksi pääsynhallinta, käyttövaltuudet, henkilöstöasiat, tietojärjestelmät, mobiililaitteet ja niin edelleen. (Kyberturvallisuuskeskus 2019.)

TIETOSUOJA - Tietosuoja on perusoikeus, joka turvaa rekisteröidyn (henkilö, jonka henkilötietoja käsitellään) oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä. (Tietosuojavaltuutetun toimisto 2019c.)

ICT – Information and communications technology, tieto- ja viestintätekniikka.

Vähimpien oikeuksien periaate – Esimerkiksi työtehtävässään toimivalle henkilölle/taholle annetaan oikeuksia vain sen verran, kuin hän tarvitsee tehtäviensä toteuttamiseen. (Tampereen teknillinen yliopisto (TUTWiki) 2010.)

SaaS – SaaS on lyhenne englannin sanoista Software as a Service. SaaS-palvelulla tarkoitetaan pilvessä sijaitsevaa ohjelmistoa, jota ylläpidetään palveluntarjoajan toimesta. SaaS-palvelut välitetään verkkoselaimen kautta, applikaationa tai näiden hybridinä. Verkkoselaimen kautta välittäminen on suosituin tapa näistä kolmesta. (Pilvi Cloud Company 2019.)

**Osoitusvelvollisuus** - Osoitusvelvollisuus on keskeinen periaate tietosuoja-asetuksessa (GDPR). Jos rekisterinpitäjä havaitsee esimerkiksi tietoturvaloukkauksen, rekisterinpitäjä voi osoitusvelvollisuuden avulla näyttää, että se on aktiivisesti pyrkinyt tunnistamaan tietosuojaan liittyviä riskejä ja ottanut käyttöön tarvittavia toimenpiteitä henkilötietojen suojaamiseksi. Jos rekisterinpitäjä ei pysty osoittamaan noudattavansa tietosuoja-asetuksen velvoitteita, se voi aiheuttaa maineriskin lisäksi hallinnollisia seuraamuksia. (Tietosuojavaal-  
tuutetun toimisto 2019b.)

**Anonymisointi** - Henkilötiedon tunnistettavuuden poistaminen siten, että yhdistäminen rekisteröityyn ei enää ole mahdollista. (Valtiovarainministeriö 2019.)

**Rekisteriseloste** – Rekisteriselosteen tarkoituksena on ollut informoida rekisteröityä henkilötietojen käsittelystä. Henkilötietolaki (523/1999) velvoitti rekisteriselosteiden laatimista. Laki kumoutui 1.1.2019 uuden tietosuojalain voimaantulon jälkeen. Tämä uusi tietosuoja-laki (1050/2018) täydentää EU:n yleistä tietosuoja-asetusta. (Tietosuojavaal-  
tuutetun toimisto 2019a; Tietosuojavaal-  
tuutetun toimisto 2019d.)

**Sisäänrakennettu- ja oletusarvoinen tietosuoja** – Tietosuoja-  
periaatteiden sisällyttäminen aikaisessa vaiheessa henkilötietojen käsittelyn osaksi. Periaatteiden huomioiminen käsittelytapojen määrittelyn ja itse käsittelyn yhteydessä siten, että varmistetaan käsittelyn vastuuvuus tietosuoja-asetuksen vaatimusten kanssa. Tästä tulee huolehtia aina käsiteltävien henkilötietojen elinkaaren loppuun saakka. (Valtiovarainministeriö 2019.)

**Profilointi** - Mikä tahansa henkilötietojen automaattinen käsittely, jossa henkilötietojen avulla arvioidaan tiettyjä henkilön ominaisuuksia tai analysoidaan tai ennakoitetaan näkökohtia, jotka liittyvät kyseiseen henkilöön. (Valtiovarainministeriö 2019.)



## 4 TEOREETTINEN TAUSTA

### 4.1 Mitä tietoturvan hallinta on

Tietoturvan hallinnalla tarkoitetaan toimenpiteitä ja keinoja varmistua tietoturvallisuuden toteutumisesta. Hallinnollisia arvoja ovat muun muassa jo käsitteissä mainittu tiedon laadun ja eheyden (integriteetin) säilyttäminen sekä tiedon luottamuksellisuuden suojaaminen teknisin ja hallinnollisin keinoin. (OpiTietosuoja.fi 2019.)

Lisäksi tietoturvallisuuteen kuuluu jatkuvuussuunnittelu, joka on tietojen, järjestelmien, palveluiden ja tietoliikenteen asianmukaista suojaamista normaali- ja poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä turvataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhilta ja vahingoilta. (OpiTietosuoja.fi 2019.)

Tietoturvan hallintaan on hyvä valita yritysympäristössä koulutukseltaan tehtävään sopiva henkilö. Myös tietosuojavastaavan nimittäminen kuuluu EU:n uuden tietosuoja-asetuksen velvollisuuksiin, mikäli asetuksen ehdot tähän täyttyvät. Tarvittaessa näitä osa-alueita voi myös ulkoistaa. (OpiTietosuoja.fi 2019.)

### 4.2 Opinnäytetyössä käytetyn tietoturvakartoituksen rakenne

Tässä kyseisessä työssä käytin tietoturvaa koskevaa yleiskuvakartoitusta, joka sisälsi seuraavat osa-alueet:

#### **Tietoturvallisuuden hallinta**

Tietoturvallisuuden hallinta -kategoria piti sisällään kysymyksiä kohdeyrityksen tavasta hoitaa tietoturvapolitiikkansa ohjeistuksineen, sekä mahdolliset tietoturvan (säännölliset) kehityssuunnitelmat ja organisaation tietoturvallisuuden tason seuraaminen, arviointi, kehittäminen ja dokumentointi.

Kategoriassa käsiteltiin myös tietoturvallisuuden johtamista tietoturvaorganisaation näkökulmasta. Pk-tason yrityksissä kysymykset nousivat entistä aiheellisemmiksi EU:n uuden tietosuoja-asetuksen voimaantulon aikana (tästä lisää seuraavassa tietosuoja koskevassa osuudessa). Aiheina oli muun muassa tietoturvallisuuden riittävä resursointi ja tietoturvallisuuden tilasta sekä mahdollisista poikkeamista raportointi.

Seuraavaksi käytiin läpi riskienhallintaa, joka ei lähtökohtaisesti pk-tason firmoissa ole niin suuressa osassa kuin isommissa yrityksissä. Muita osa-alueita tässä kategoriassa olivat mm. turvallisuusluokittelu, tietoturvallisuuden suojausmenettelyjen hallinta sekä tietoturva-poikkeamien käsittely.

### **ICT-hallinta**

ICT-hallinta pitää sisällään kysymyksiä ICT-laitteiden, ohjelmistojen, tietojärjestelmien sekä käytössä olevien verkkopalveluiden hallinnasta. Laite- ja ohjelmistorekisterit sekä näistä vastaavat henkilöt tuli olla nimetty ja dokumentoitu ja niin edelleen.

ICT-hallinta -kategoriaan liittyivät myös varmuuskopiointi, turvallinen käyttöönotto ja käytöstä poistaminen (tietojärjestelmien ja laitteiden), ICT-palvelusopimukset, päivitykset ja haittaohjelmat.

### **Henkilöstö**

Henkilöstö -kategoriassa perehdyttiin henkilöstöturvallisuuteen. Tästä esimerkkeinä henkilöstön tietoturvaohjeistuksesta huolehtiminen, turvaluokittelun kuvaaminen mukaan lukien yrityssalaisuudet ja muun luottamuksellisen tiedon asianmukainen hallinnointi ja näistä ohjeistaminen. Lisäksi kategoriaan kuuluivat salassapitosopimukset, rekrytoinnin yhteydessä taustojen tarkistaminen sekä esimerkiksi työsuhteen päättyessä käyttöoikeuksien poistosta ja työlaitteiden palauttamisesta huolehtiminen.

### **Käyttövaltuudet**

Käyttövaltuuksien ja pääsynhallinta on yksi olennaisimpia tietoturvallisuuden osa-alueita. Tässä kategoriassa käytiin läpi käyttövaltuuksien hallintaperiaatteita johdonmukaisesti (esimerkiksi ”vähimpien oikeuksien periaatteen” mukaan toimiminen). Käsiteltäviä asioita olivat myös käyttövaltuuksien ylläpito, salasanat ja esimerkkinä vielä vahvemmat todennusmenetelmät (esimerkiksi älykortit, biometrinen todentaminen tai mobiilivarmenne). Pk-tason yrityksissä tätä viimeisimpänä mainittua menetelmää ei tosin sovellettu sen ollessa tässä kartoitusympäristössä epärelevantti (ei voida vaatia oletusarvoisesti).

## **PC:t ja mobiililaitteet**

PC:t ja mobiililaitteet -kategoriassa käytiin läpi henkilökohtaisten tietokoneiden ja mobiililaitteiden tietoturvaa. Kartoituskysymykset sisälsivät muun muassa salaukseen, ohjeistukseen, pääsynvalvontaan ja paikannukseen liittyviä kysymyksiä.

## **Kiinteistöt**

Kiinteistöt -kategoriassa tietoturvaa tarkasteltiin toimitilojen sekä ICT-laitetilojen näkökulmasta. Toimitiloissa käytiin läpi mm. toimitilojen eri osia, käyttötarkoituksia ja suojausvaatimuksia sekä näiden tunnistamista ja luokittelua tarvittaessa. Tämän lisäksi asiaa muun muassa kulunvalvonnasta, murtosuojauksesta ja paloturvallisuudesta. Laitetiloja koskevat kartoituskysymykset olivat hyvin samankaltaisia toimitiloja käsitelleen osion kysymysten kanssa, lukuun ottamatta ICT-laitteiden asianmukaista huolehtimista koskevia kohtia.

## **Tietojärjestelmät**

Tietojärjestelmät -kategoriassa käsiteltiin organisaatioiden tapaa käsitellä sähköpostin, pilvipalveluiden sekä mahdollisesti käytössä olevien SaaS-palveluiden tietoturvallisuutta. Kysymykset mukailivat muun muassa ohjeistuksen tärkeyttä, salauksen ja ohjelmistojen asianmukaista hallintaa sekä mahdollisia poikkeustilanteita.

### **4.3 Opinnäytetyössä käytetty tietosuojakartoitus**

Perehdyin harjoittelujakson aikana EU:n keväällä 2018 voimaantulleeseen tietosuoja-asetukseen (2016/679) siinä määrin, että olin itsekin toteuttamassa tässä opinnäytetyössä käyttämäni tietosuojakartoitusta.

Tietosuoja-asetuksen ollessa hyvin laaja kokonaisuus, keskityttiin kartoitukseen rajamaan oleellisimpia ja tärkeimmiksi koettuja seikkoja, jotta kartoitus olisi aikamäärällisesti järkevä toteuttaa.

Kartoituksen alkupuolella perehdyttiin johdon sitoutumiseen tietosuojatyön näkökulmasta. Tämä sisälsi tietosuoja-asetuksen voimaantulon ja sen asettamien velvoitteiden läpikäymistä organisaation kannalta. Seuraava kappale käsitteli organisaation tietosuojapolitiikkaa ja -periaatteita. Tämän jälkeen käytiin läpi tietosuojatyön organisointia, muun muassa

henkilötietoja käsittelevien yksiköiden ja henkilöiden näkökulmasta. Myös aiemman lain-säädännön vaatimusten täyttämistä käsiteltiin lyhyesti ja tämän jälkeen valmistautumista EU:n tietosuoja-asetuksen velvoitteiden täyttämiseen, joka käsitteli keskeisiä tietosuoja-asetuksen seikkoja kuten hallinnolliset sakot ja tietosuojavastaavan nimittäminen.

Seuraavana käsiteltiin tietosuojaa järjestelmä- ja sovelluskehityksessä. Tähän kuuluivat muun muassa sisäänrakennetun- ja oletusarvoisen tietosuojan periaatteiden ymmärtäminen ja järjestelmä- ja sovelluskehityksessä käytettävän tietosuojan tekninen toteutus.

Tämän jälkeen käytiin läpi rekisterinpitäjän ja henkilötietojen käsittelijän välisiä sopimuksia. Tähän liittyi roolien vastuuttamista ja dokumentointia sekä tietosuoja-asetuksen vaatimuksia henkilötietojen siirtoa Euroopan talousalueen ulkopuolelle koskien.

Seuraavana vuorossa oli rekisteröidyn oikeudet. Nämä käsittivät esimerkiksi ”oikeuden tulla unohdetuksi”, henkilötietojen siirtämisen järjestelmästä toiseen (siirto-oikeus) sekä rekisteröidyn oikeuden vastustaa automaattista päätöksentekoa ja profilointia.

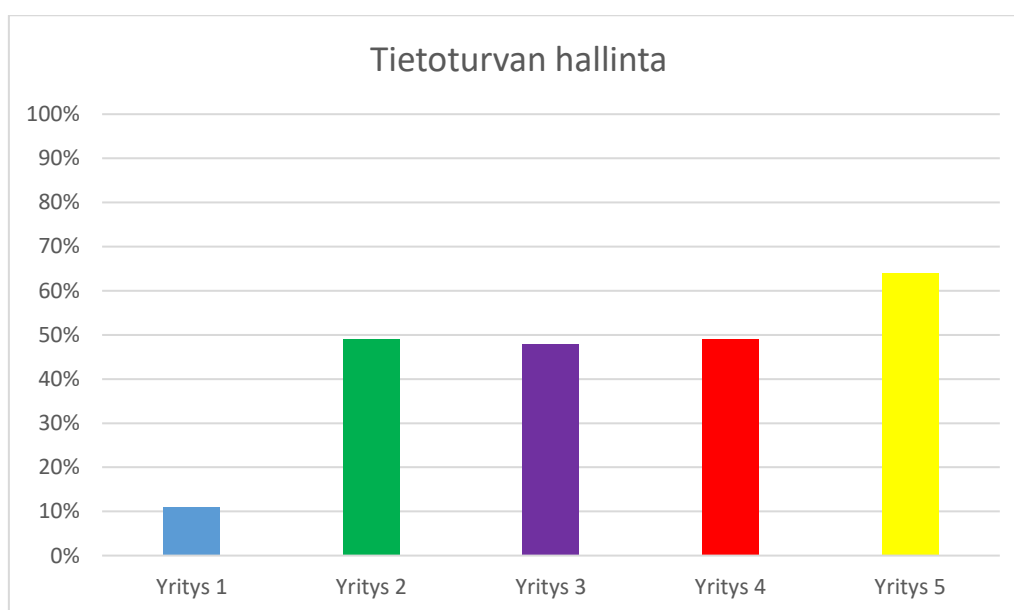
Tämän jälkeen käsiteltiin osoitusvelvollisuutta. Tarkoittaen sitä, että henkilötietoja käsittelevä organisaatio kykenee osoittamaan, että asetusta noudatetaan henkilötietojen käsittelyssä. Tämä sisältää muun muassa selosteen käsittelytoimista, joka toisaalta oman opinäytetyöni kohdeyrityksillä (pk-yritykset) ei ollut relevanttia (ei velvoita organisaatiota, jolla on alle 250 työntekijää).

Viimeisenä osiona käsiteltiin tietoturvallisuuden toteuttamista tietosuojan näkökulmasta. Tämä sisälsi asiaa esimerkiksi tietoturvamenettelyjen tehokkuuden arvioinnista sekä henkilötietoihin kohdistuvasta riskiarvioinnista.

## 5 TUTKIMUKSEN LÄPIKÄYNTI

### 5.1 Tietoturvan hallinta

Tutkimuksen läpikäynti -osiossa käyn kategoria kerrallaan läpi kartoitustuloksia. Kaaviokuvat havainnollistavat yritysten suoriutumistasoa. Toisissa kategorioissa läpikäytyjä kohtia on huomattavasti enemmän kuin toisissa; jos kategoriassa on esimerkiksi 25 kohtaa, joista jokainen on täysin toteutettu (ei esimerkiksi keskeneräiseksi merkitty tai osaksi toteutettu) yksittäinen kohta vastaa 4 % kokonaistuloksesta. Kartoitusaineisto on peräisin yritykseltä, jossa suoritin koulun harjoittelujaksoani (osaksi olen ollut myös mukana kehittämässä tietosuojakartoitusta).



Kuvio 1. Tietoturvan hallinta

Tietoturvan hallinta -kategoriassa käytiin läpi ensimmäisenä kohtana tietoturvallisuuden hallintaa: tässä osiossa yhtenäistä oli, että johdon kannanotto tietoturvallisuuden hoitamisesta oli kommunikoitu henkilöstölle ja sen noudattamista edellytetty. Kirjallista ohjeistusta tietoturvallisuuden hoitamisesta sen sijaan ei ollut toteutettu kuin kahdessa yrityksessä. Millään kartoitusyrityksellä ei myöskään ollut säännöllistä tietoturvan kehittämissuunnitelmaa vielä toteutettuna ja vain yhdellä yrityksellä tietoturvallisuuden tason seuraaminen oli jotakuinkin toteutettu (toimenpiteet kesken/kehitysvaiheessa). Henkilöstölle pidettävä tietoturvakoulutus voisi olla paikallaan esimerkiksi vuosittain ja rekrytoinnin yhteydessä. Myös kirjalliset ohjeistukset kaikista tarvittavista osa-alueista olisivat hinta-laatusuhteeltaan hyvä parannus yritysmaailman tietoturvaan.

Seuraavana tarkasteltiin tietoturvaa tietoturvaorganisaation näkökulmasta: vain yhdessä yrityksessä vastuu tietoturvallisuudesta johtoryhmätasolla oli osoitettu sekä dokumentoitu. Toisessa yrityksessä edellä mainitun lisäksi oltiin alettu hahmotella tietoturvallisuutta operatiivisen vastuun näkökulmasta. Neljässä viidestä yrityksestä tietoturvallisuuteen oli varattu kartoituksen mukaan riittävästi resursseja. Suurimmassa osassa yrityksiä tietoturvallisuuden tilasta ja tapahtuneista poikkeamista raportoidaan kartoituksen mukaan johdolle säännöllisesti. Yhdessä kartoituksen mikroyrityksessä tätä kohtaa ei sovellettu.

Seuraavaksi käytiin läpi riskienhallintaa: lähtökohtaisesti riskienhallintaan ei ollut panostettu tai perehdytty kovinkaan hyvin. Eräs IT-alan yritys erottui muista selkeästi edukseen tässä osiossa. Tässä kyseisessä yrityksessä riskienhallinnan prosessi oli dokumentointia vaille toteutettu ja kattoi kartoituksen mukaan tietoriskien käsittelyn. Riskienhallinnan väjyys liittyy mielestäni yritysten kokoon. Pk-tason yrityksissä ei voi olettaa, että tämän tason toimenpiteisiin on automaattisesti resursseja, toisin kuin suurissa yrityksissä.

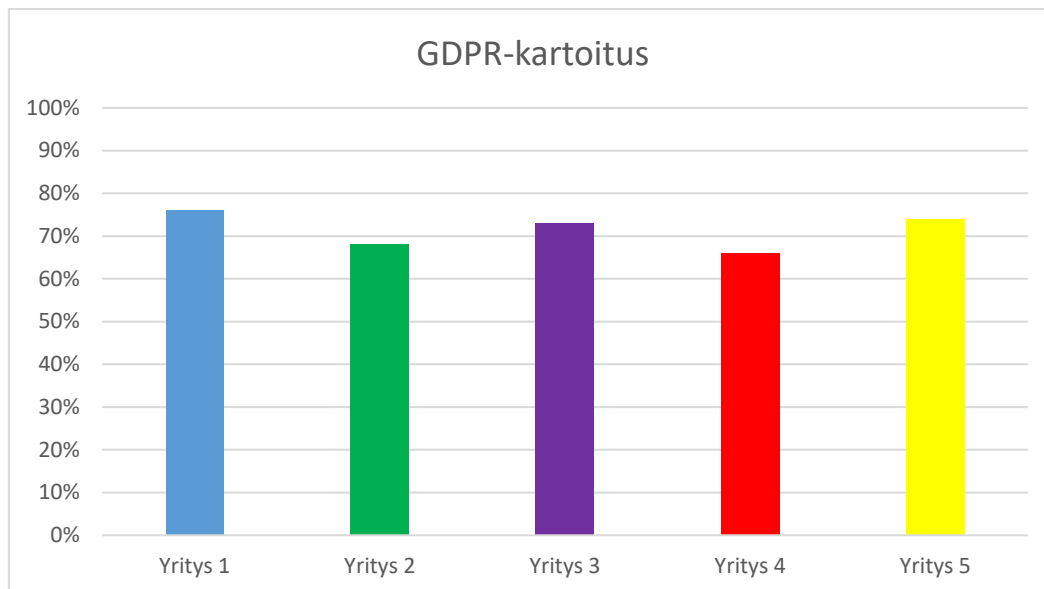
Turvallisuusluokittelu-osio piti sisällään organisaation käsittelemien tietojen luokittelua sekä yrityssalaisuuksiksi luokiteltavien tietojen tunnistamista ja tiedottamista henkilöstölle. Nämä asiat olivat neljässä yrityksessä viidestä toteutettu kokonaan tai vähintään suurimmilta osin. Yhdessä yrityksessä tuloksista oltiin epävarmoja. Tämä osio tulisi mielestäni hoitaa jokaisessa yrityksessä kokoon katsomatta kirjalliseksi edes pääpiirteissään.

Seuraavana vuorossa oli tietoturvallisuuden suojausmenettelyjen hallinta. Kaikkien viiden kartoitukseen osallistuneen yrityksen mukaan tietoturvallisuuden suojausmenettelyjen hallinta oli heidän yrityksissään järjestelmällistä. Kahdessa yrityksessä viidestä oltiin kartoituksen mukaan sitä mieltä, että heidän tapansa hoitaa edellä mainittuja toimenpiteitä oli erittäin korkealla tasolla toteutettu (verrattavissa alan parhaisiin käytäntöihin). Kartoituksessa nämä seikat käsiteltiin yksityiskohtaisemmin, mutta täytyy todeta, että asiat tuskin olivat hoidettu niin hyvin kuin vastaukset antoivat ymmärtää.

Tietoturvapoikkeamien käsittely: vain yhdessä yrityksessä tietoturvapoikkeamien käsittelyn vastuuttaminen ja kirjallinen kuvaaminen oli kehitteillä (dokumentointi puuttui). Tietoturvapoikkeamien käsittelyä ei ollut missään firmassa ohjeistettu ja tiedotettu henkilöstölle. Mielestäni poikkeamien varalle tulisi olla vähintään jonkin tasoinen kirjallinen ohjeistus, jotta henkilöstö ymmärtäisi raportoida johdolle mahdollisista tietoturvapoikkeamista. Monen (varsinkin pk-koon) yrityksen kohdalla ei luultavasti ole vielä kohdattu vakavia tietoturvapoikkeamia ja tämän takia ohjeistus puuttuu.

## 5.2 GDPR-kartoitus

GDPR-kartoitus edusti kartoitusistunnon tietosuojapuolta. Tämän läpikäymiseen käytettiin noin puolet kartoitusajasta.



Kuvio 2. GDPR-kartoitus

GDPR-kartoitus -kategorian ensimmäinen osio käsitteli johdon sitoutumista tietosuojatyöhön. Lyhyesti kerrottuna tässä osiossa käydyt asiat liittyivät EU:n tietosuoja-asetuksen velvoitteiden ja voimaantulon tiedostamiseen ja näiden velvoitteiden täyttämiseen voimaantuloon mennessä. Lisäksi tiedusteltiin johdon seuraamista organisaation tietosuojatyön kannalta. Tämä osio oli jokaisessa yrityksessä toteutettu.

Seuraavassa osiossa käsiteltiin organisaation tietosuojapolitiikkaa ja -periaatteita. Osiolla suositeltiin, että organisaatiolla on johdon hyväksymä tietosuojapolitiikka tai muu vastaava asiakirja, joka kuvaa organisaation henkilötietojen käsittelyn peruseriaatteita ja tietosuojan merkitystä organisaatiolle. Lisäksi nämä edellä mainitut periaatteet tuli tiedottaa kaikille osapuolille, joiden työnkuvaan tietosuoja liittyy. Kahdessa yrityksessä viidestä näitä ei oltu toteutettu vielä ja jäljelle jäävässä kolmessa toteuttaminen oli osittain kesken.

Seuraavaksi käytiin läpi tietosuojatyön resursseja ja organisointia. Tässä osiossa tiedusteltiin, onko johto sitoutunut antamaan ohjausta ja tukea organisaation tietosuojatyölle. Tämä oli kaikissa kartoitusyrityksissä toteutettu. Seuraavaksi käytiin läpi henkilötietoja käsittelevien yksiköiden johtamista. Yhdessä yrityksessä viidestä nämä kartoitusmateriaaleissa mainitut kohdat oli toteutettu, muissa neljässä prosessi oli enemmän tai vähemmän

kesken kartoituksen tekovaiheessa. Suuressa osassa yrityksiä puutteena oli dokumentoinnin vajavaisuus.

Seuraavassa kohdassa yrityksiltä kysyttiin, onko henkilötietoja käsitteleville henkilöille osoitettu riittävät resurssit tehtävien hoitamiseen, riittävä koulutus mukaan lukien. Nämä asiat oli kartoituksen mukaan lähes yksimielisesti toteutettu. Yhdessä yrityksessä todettiin, että GDPR:n velvoitteisiin tulee tutustua paremmin. Viimeisenä kohtana tässä osiossa käsiteltiin tietosuoja koskevan dokumentaation katselmointia ja päivittämisen vastuuttamista. Tämä oli toteutettu neljässä viidestä yrityksestä.

Seuraava osio käsitteli aiemman lainsäädännön vaatimusten täyttämistä (lainsäädäntö ennen GDPR:n voimaantuloa). Organisaation käsittelemien henkilötietojen tunnistaminen oli kaikissa yrityksissä jotakuinkin toteutettu, suuressa osassa yrityksiä tämän lisäksi vaadittu dokumentointi kylläkin puuttui tai siinä oli parantamisen varaa. Henkilötietolaissa (523/1999) säädettävä rekisteriseloste (Tietosuojavaltuutetun toimisto 2019d) oli laadittu valmiiksi yhdessä yrityksessä, muissa tämä oli kesken tai ei toteutettu. Kartoituksen teko aikana voimassaolevan lainsäädännön vaatimukset henkilötietojen käsittelyssä olivat kartoituksen mukaan toteutettu kaikissa yrityksissä. Tosin osassa yrityksistä aiheesta heräsi kysymyksiä ja sen hetkisten vaatimusten suhteen oli havaittavissa pientä epäselvyyttä.

Seuraava osio tutki valmistautumista EU:n tietosuoja-asetuksen velvoitteiden täyttämiseen. Tässä tiedusteltiin ensimmäiseksi, oliko organisaatio asettanut kehittämisprojektin EU:n tietosuoja-asetuksen velvoitteiden täyttämiseksi sen voimaantuloon mennessä, asetuksen soveltamisohjeiden seuraamisen vastuuttamista sekä hallinnollisten sakkojen tiedostamista. Nämä edellä mainitut seikat olivat kartoituksen mukaan kaikissa viidessä yrityksessä toteutettu. Tässä osiossa tiedusteltiin vielä muun muassa oliko organisaatio selvittänyt velvollisuutensa nimittää tietosuojavastaava. Tietosuojariskien arviointi oli toteutettu vain yhdessä yrityksessä viidestä, mutta tietosuojavastaavan nimittämisen velvollisuus oli selvitetty kaikissa yrityksissä.

Seuraava osio koski tietosuoja järjestelmä- ja sovelluskehityksessä. Sisäänrakennetun ja oletusarvoisen tietosuojan periaatteet olivat tiedossa kaikissa viidessä yrityksessä, järjestelmä- ja sovelluskehityksessä käytettävän tietosuojan asianmukainen tekninen toteutus oli kartoituksen mukaan kolmessa yrityksessä toteutettu. Yhdessä yrityksessä asian suhteen oli epävarmuutta, tämä merkittiin selvitettäväksi jatkossa. Myös jäljelle jäävässä viimeisessä yrityksessä asia jäi epäselväksi.

Seuraavassa kartoituksen kohdassa kysyttiin muun muassa, vaatiiko organisaatio järjestelmä- ja sovelluskehittäjiltä sisäänrakennetun ja oletusarvoisen tietosuojan toteutumista



henkilötietoja käsittelevien järjestelmien kehitysprosesseissa. Kolmessa yrityksessä viidestä nämä seikat oli toteutettu, yhdessä näitä ei sovellettu ja viimeisessä asiat jäivät osittain epäselväksi kartoituksen tekohetkellä. Osion viimeinen kohta käsitteli henkilötietojen elinkaaresta huolehtimista ja kolmessa yrityksessä tämä oli toteutettu, kahdessa jäljelle jäävässä yrityksessä puolestaan asian suhteen oli ongelmia, jotka merkittiin selvitettäväksi lähitulevaisuudessa.

Seuraava osio käsitteli rekisterinpitäjän ja henkilötietojen käsittelijän välisiä sopimuksia. Ensimmäisenä käytiin läpi henkilötietojen käsittelijöiden, näiden käsittelemien henkilötietojen sekä vastuiden dokumentointia. Tämä oli yhdessä yrityksessä toteutettu ja lopuissa neljässä kesken. Tämän jälkeiset kohdat käsittelivät henkilötietojen käsittelijöiden kanssa tehtyjä sopimuksia EU:n tietosuoja-asetuksen vaatimusten täyttämisen kannalta sekä henkilötietojen siirtoa Euroopan talousalueen (ETA:n) ulkopuolelle. Näistä kohdista oltiin vielä kartoituksen tekovaiheessa epävarmoja. Yksi yritys oli kartoituksen mukaan tietoinen asetuksen vaatimuksista ja niiden täyttämisestä koskien henkilötietojen siirtämistä ETA:n ulkopuolelle.

Seuraavana käytiin läpi kartoituksen kannalta hyvin keskeistä asiaa: rekisteröidyn oikeuksia. Kahdella yrityksellä viidestä oli epäselvyyttä tiedonantovelvoitteistaan ja EU:n tietosuoja-asetuksen tuomista uusista vaatimuksista tiedonannolle. Muuten yrityksissä kaikki tätä osiota koskevat kohdat olivat kartoituksen mukaan toteutettu. Kohdat käsittelivät mm. rekisteröidyn oikeutta ”tulla unohdetuksi”, siirto-oikeutta, automaattisen käsittelyn vastustamista sekä valmiutta ilmoittaa henkilötietojen tietoturvaloukkauksista.

Seuraavan kohtana oli osoitusvelvollisuus. Neljässä yrityksessä viidestä oltiin tietoisia osoitusvelvollisuudesta. Asetuksen vaatimaa selostetta käsittelytoimista ei sovellettu kartoituksen kohdeyrityksiin senhetkisten tietojen perusteella. Neljä yritystä viidestä kykeni myös kartoituksen mukaan osoittamaan, että henkilötietojen käsittely noudattaa tietosuoja-asetuksen artiklan 5 periaatteita (”henkilötietojen käsittelyä koskevat periaatteet”). Kaikki viisi yritystä pystyivät kartoituksen mukaan osoittamaan, että henkilötietojen käsittelyssä toteutuvat rekisteröityjen oikeudet.

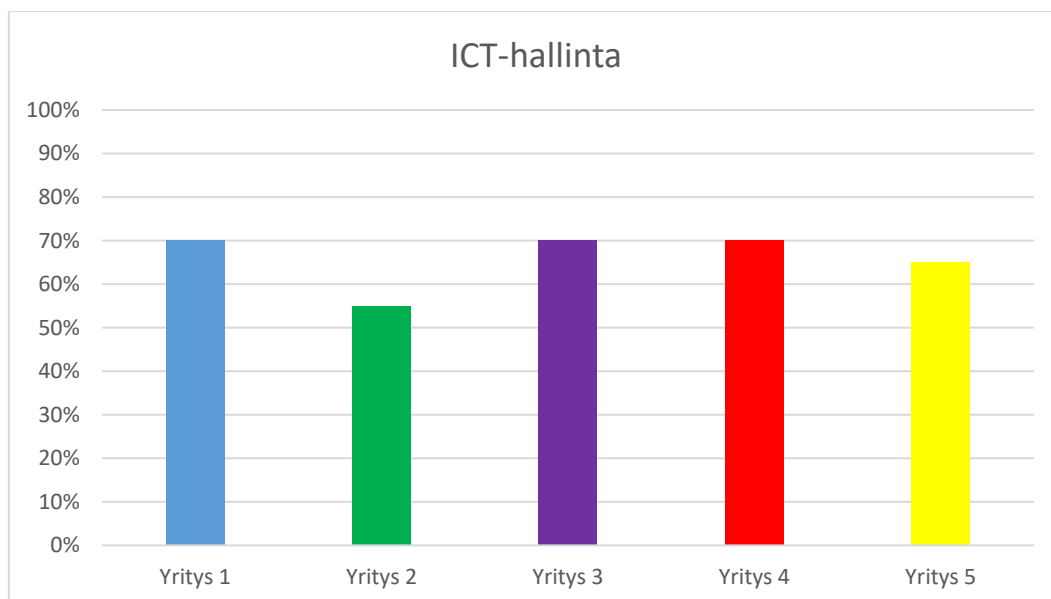
Viimeisenä osiona tässä kategoriassa oli tietoturvallisuuden toteuttaminen tietosuojan näkökulmasta. Ensimmäisessä kohdassa tiedusteltiin henkilötietojen käsittelyyn kohdistuvien riskien arviointia. Tämä oli kartoituksen mukaan toteutettu kahdessa yrityksessä, kahdessa se oli kesken ja jäljelle jäävässä yrityksessä sitä ei oltu toteutettu. Sen sijaan neljä viidestä yrityksestä oli kartoituksen mukaan toteuttanut riskien hallitsemiseksi riittävät tietoturvamenettelyt, joilla voidaan varmistaa jatkuva henkilötietojen ja tietojärjestelmien luotamuksellisuus, eheys ja käytettävyys. Yhdessä yrityksessä tätä ei oltu toteutettu vielä.

Neljällä yrityksellä viidestä ei ollut säännöllistä menettelyä tietoturvamenettelyjen tehokkuuden arviointiin. Yhdellä yrityksellä tämä prosessi oli kesken.

Kolmella yrityksellä viidestä oli kartoituksen mukaan kyky havaita henkilötietoihin kohdistuvat loukkaukset tietojärjestelmässä ja valmius tietoturvaloukkauksista ilmoittamiseen, jäljelle jäävällä kahdella yrityksellä tämä oli vielä epäselvää. Kartoituksen mukaan kaksi yritystä kykeni osoittamaan, että henkilötietojen käsittelyyn kohdistuvat riskit on arvioitu ja toimenpiteet niiden hallitsemiseksi on toteutettu. Myöskään kahdella yrityksellä tätä ei oltu toteutettu ja jäljelle jäävällä yrityksellä toteutus oli kesken. Viimeisenä kohtana tästä osiosta tiedusteltiin yritysten kykyä osoittaa, tietoturvamenettelyiden olevan asianmukaisesti toteutettu ja niiden tehokkuutta arvioitavan säännöllisesti. Tämä oli toteutettu kahdessa yrityksessä, kahdessa yrityksessä prosessi oli kesken ja yhdessä yrityksessä ei toteutettu.

### 5.3 ICT-hallinta

ICT-hallinta piti sisällään kysymyksiä ICT-laitteista, ohjelmistoista, tietojärjestelmistä sekä käytössä olevien verkkopalveluiden hallinnasta.



Kuvio 3. ICT-hallinta

ICT-hallinta -kategoriassa käytiin ensimmäisenä läpi ICT-laitteiden, ohjelmistojen ja tietojärjestelmien sekä käytössä olevien verkkopalveluiden kirjaamista laite- ja ohjelmistorekistereihin. Nämä oli toteutettu kolmessa yrityksessä viidestä.

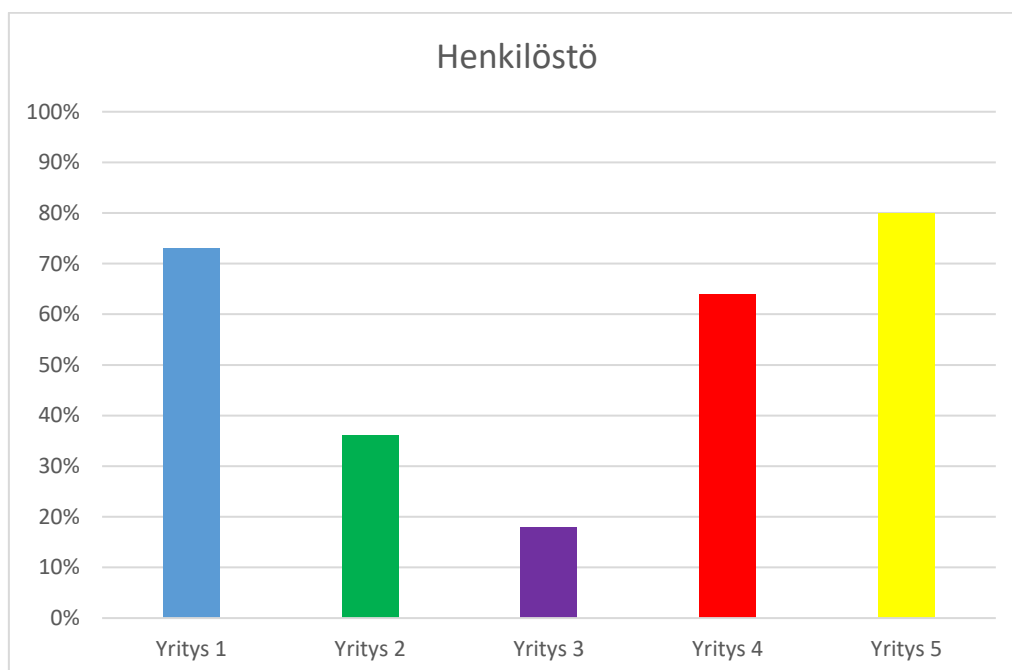
Seuraavana yrityksiltä kysyttiin, onko ICT-laitteista, ohjelmistoista ja tietojärjestelmistä vastaavat henkilöt nimetty ja dokumentoitu. Tämä oli toteutettu kahdessa yrityksessä ja

yhdessä yrityksessä toteutuksesta puuttui dokumentointi. ICT-laitteiden ja tietojärjestelmien käyttöönotosta ja turvallisesta käytöstä poistamisesta kirjallista ohjeistusta ei ollut toteutettu yhdessäkään kartoituksen kohdeyrityksessä.

Tietoturvallisuus oli huomioitu ICT-palvelusopimuksissa neljässä yrityksessä viidestä. Tietojen varmuuskopiointi oli suunniteltua ja dokumentoitua kahdessa yrityksessä. Lopuista kolmesta yrityksestä dokumentointi tämän suhteen puuttui tai oli kesken. Varmuuskopioiden asianmukainen suojaaminen oli hallinnassa kolmessa yrityksessä. Yhdessä tätä ei oltu toteutettu ja yhdessä se oli kesken. Osion viimeiset kohdat liittyivät ohjelmistojen päivitysten ajantasaisuuteen sekä haittaohjelmien torjuntaan ja nämä olivat kaikissa viidessä yrityksessä kartoituksen mukaan toteutettu.

## 5.4 Henkilöstö

Henkilöstö -kategoriassa perehdyttiin henkilöstöturvallisuuteen.



Kuvio 4. Henkilöstö

Henkilöstö -kategoriassa käsiteltiin henkilöstöturvallisuutta. Kategorian läpikäyminen alkoi henkilöstön tietoturvaohjeistuksesta ja tämän henkilöstön saatavilla olevasta kirjallisesta versiosta. Kartoituksen mukaan kolmessa yrityksessä oli henkilöstön tietoturvaohjeistus. Kahdessa näistä kolmesta yrityksestä se löytyi myös kirjallisena henkilöstön saatavilla ja jäljelle jäävässä kahdessa yrityksessä näitä kohtia ei oltu toteutettu. Seuraavana käytiin

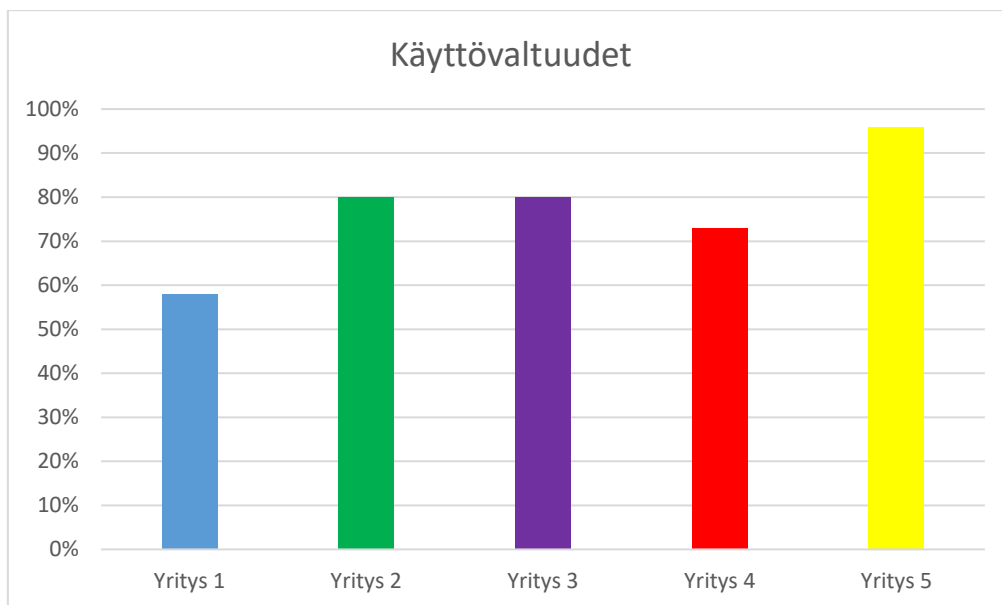
läpi, sisältääkö ohjeistus tietojen turvaluokittelun tai jos sellaista ei ole, kuvauksen yrityssalaisuuksista tai muista luottamuksellisista tiedoista, joita ei saa luovuttaa ulkopuolisille. Tämä kohta oli toteutettu kahdessa yrityksessä, kahdessa toteutus oli kesken ja jäljelle jäävässä yhdessä yrityksessä tätä ei ollut toteutettu. Tämän jälkeinen kohta käsitteli henkilöstön salassapitosopimuksia. Tämä oli toteutettu kolmessa yrityksessä joko työsopimuksen yhteydessä tai muuten. Yhdessä yrityksessä vastauksesta oltiin epävarmoja ja yhdessä yrityksessä tätä kohtaa ei oltu toteutettu.

Seuraavat kohdat liittyivät henkilöstön ohjeistukseen henkilökohtaisten tietokoneiden ja mobiililaitteiden suojaamiseen kannalta sekä turvalliseen toimimiseen organisaation tietojärjestelmissä. Nämä kohdat olivat neljässä yrityksessä viidestä kokonaan tai osittain toteutettu ja yhdessä yrityksessä näitä kohtia ei oltu toteutettu. Missään kartoituksen kohdeyrityksessä ei oltu määritelty seuraamuksia ohjeistuksen vastaisesta toiminnasta tai tiedotettu näistä henkilöstölle.

Seuraavat kohdat käsittelevät henkilöstölle järjestettävää tietoturvakoulutusta suunnitellusti sekä uusien työntekijöiden perehdyttämiseen kuuluvaa tietoteknistä- ja tietoturvalisuskoulutusta. Kolmessa yrityksessä kartoituksen mukaan uusien työntekijöiden perehdyttämiseen kuuluva koulutus oli toteutettu, mutta muuten edellä mainitut kohdat jäivät kaikkien yritysten osalta toteuttamattomaksi. Viimeisenä läpikäytävänä asiana tässä kategoriassa olivat toimenpiteet rekrytointitilanteessa sekä työsuhteen päättyessä. Nämä seikat olivat kartoituksen mukaan toteutettu kaikissa viidessä kartoituksen kohdeyrityksessä.

## 5.5 Käyttövaltuudet

Käyttövaltuudet -kategoria käsitteli käyttövaltuuksia ja pääsynhallintaa. Käsiteltäviä asioita olivat muun muassa käyttövaltuuksien ylläpito, salasana- ja lokitietojen valvonta sekä ylläpito.



Kuvio 5. Käyttövaltuudet

Käyttövaltuudet -kategoriassa käsiteltiin käyttövaltuuksia ja pääsynhallintaa. Kategorian läpikäynti alkoi käyttövaltuuksien hallinnalla, joka oli toteutettu kolmessa kartoituksen kohdeyrityksessä viidestä. Kahdessa yrityksessä tämä oli dokumentoinnin osalta vielä kesken.

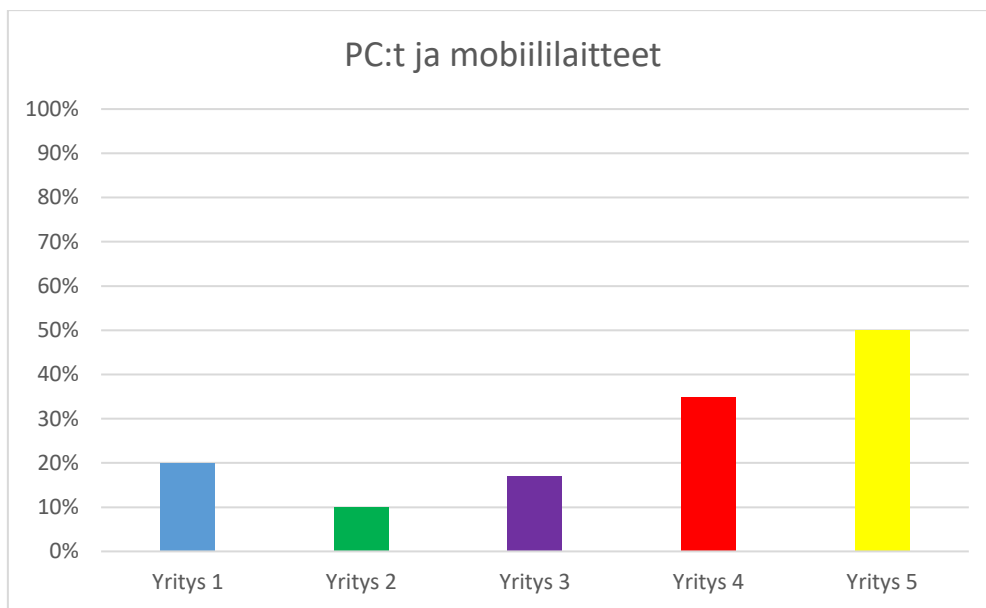
Seuraavat kohdat käsitelivät käyttövaltuuksien asianmukaista myöntämistä ja poistamista sekä käyttövaltuuksien dokumentointia.

Yhdessä yrityksestä viidestä tämä edellä mainittu dokumentointi puuttui, muuten nämä kohdat (yksityiskohtaisemmin kartoitusmateriaaleissa) olivat kaikissa viidessä yrityksessä toteutettu. Kolmessa yrityksessä viidestä käyttövaltuudet katselmoitiin kartoituksen mukaan säännöllisesti niiden ajantasaisuuden varmistamiseksi.

Viimeinen sovellettava kohta käsitteli salasanojen riittävien vaatimusten määrittelyä ja ohjeistamista henkilöstölle. Tämä oli toteutettu kolmessa kartoituksen kohdeyrityksessä.

## 5.6 PC:t ja mobiililaitteet

PC:t ja mobiililaitteet -kategoriassa käytiin läpi henkilökohtaisten tietokoneiden ja mobiililaitteiden tietoturva. Kartoituskysymykset sisälsivät muun muassa salaukseen, ohjeistukseen, pääsynvalvontaa ja paikannukseen liittyviä kysymyksiä.



Kuvio 6. PC:t ja mobiililaitteet

Henkilökohtaisia tietokoneita koskevassa osiossa alettiin kartoitusta käymään läpi henkilökohtaisten tietokoneiden käyttöä ja tietoturvaa koskevasta ohjeistuksesta. Kolmessa yrityksessä ohjeistus kartoituksen mukaan oli olemassa, muttei kirjallisena tai siinä oli vähintäänkin puutteita. Kahdessa yrityksessä tätä kohtaa ei oltu toteutettu.

Seuraava kohta liittyi myös ohjeistukseen. Ohjeistuksen tulisi velvoittaa käyttäjiä lukitsemaan tietokoneensa sen läheisyydestä poistuttaessa ja tämän lisäksi tietokoneiden tulisi lukittautua automaattisesti organisaation määrittelemän ajan kuluttua. Tämä kohta oli yhdessä yrityksessä toteutettu ja muissa neljässä kesken tai ei toteutettu.

Seuraava osion aihe velvoitti käyttäjiä suojaamaan kannettavia tietokoneitaan matkoilla eri tilanteissa. Kartoituksen kohdeyritysten suhteen todennäköisesti melko epärelevantti, sillä yhdelläkään yrityksellä ei näitä asioita ohjeistuksesta löytynyt. Käyttäjakohtaisten kirjautumistietojen suojaaminen oli toteutettu kartoituksen mukaan neljässä yrityksessä viidestä.

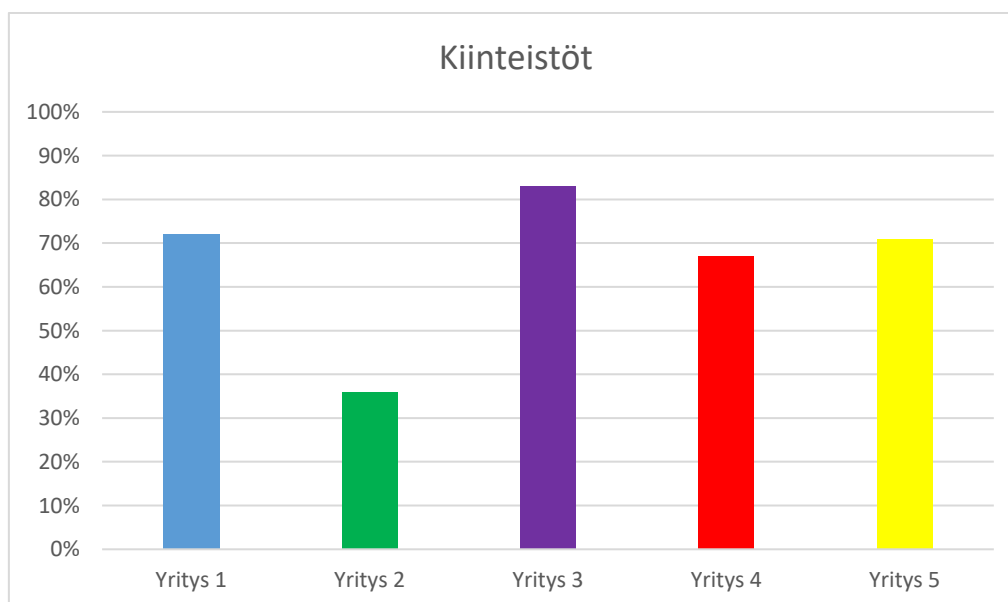
Mobiililaitteita käsittelevä osio alkoi samankaltaisesti mobiililaitteiden tietoturvaa koskevaa kirjallista ohjeistusta tiedustelemalla. Tämä kohta edellytti myös, että käyttäjät olivat velvoitettu noudattamaan tätä ohjeistusta ja heille oli tiedotettu mobiililaitteisiin liittyvistä riskeistä. Kartoituksen mukaan vain yhdellä yrityksellä oli tähän jonkinlainen ohjeistus, muttei kirjallisena. Seuraavaksi tiedusteltiin, oliko organisaatiolla mobiililaitteista ja niiden hallijoista ylläpidetty rekisteri, sisältäen asianmukaiset käyttäjäkohtaiset tiedot. Tämä kohta oli kartoituksen mukaan toteutettu kolmessa yrityksessä viidestä.

Osion toiseksi viimeinen asia liittyi mobiililaitteiden suojausmenetelmien aktivointiin. Tämä kohta oli toteutettu kahdessa yrityksessä viidestä. Viimeinen kohta osiossa käsitteli toimenpiteitä mobiililaitteen katoamisen varalle. Tätä kohtaa ei oltu toteutettu yhdessäkään kohdeyrityksistä.

Kartoituksen kohdeyritysten koosta johtuen työpuhelimia ei ole laajalti käytössä. Tämä on vähintään osasyynä suhteellisen heikkoon suoriutumiseen kategoriassa.

## 5.7 Kiinteistöt

Kiinteistöt -kategoriassa tietoturvaa tarkasteltiin toimitilojen ja ICT-laitetilojen näkökulmasta.



Kuvio 7. Kiinteistöt

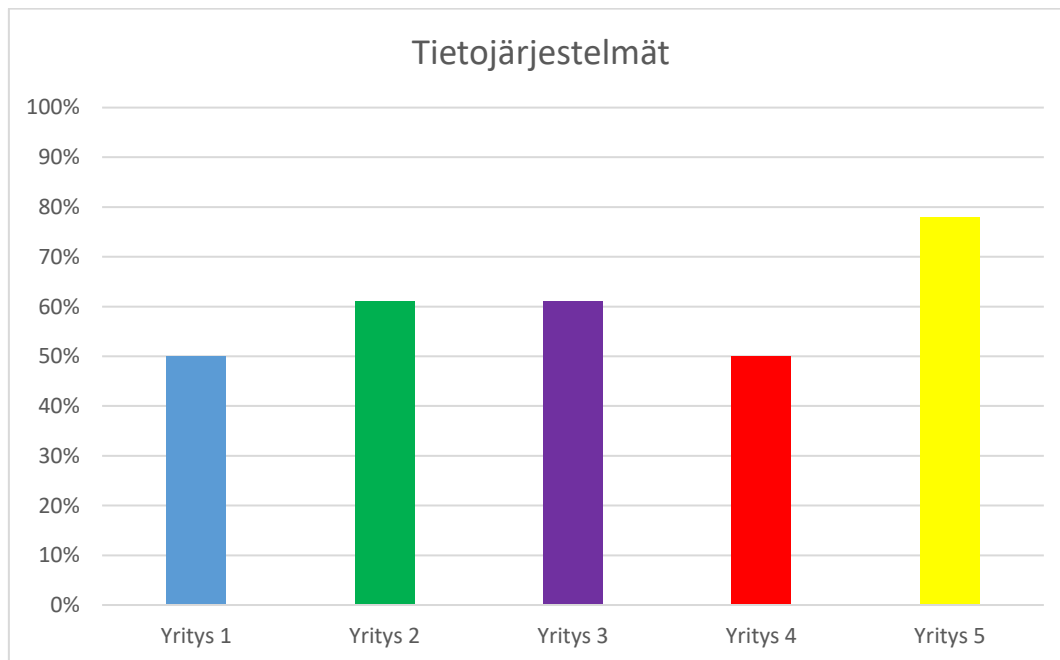
Kiinteistöt -kategoria käsitteli toimitilojen sekä ICT-laitetilojen turvallisuutta. Ensimmäinen toimitilojen turvallisuutta koskeva osio edellytti, että organisaation toimitilojen eri osat tunnistetaan ja luokitellaan asianmukaisesti. Tämä kohta oli toteutettu kolmessa viidestä kartoituksen kohdeyrityksestä. Seuraava osion kohta käsitteli tilojen käyttötarkoitukseen nähden riittävän lukituksen ja kulunvalvontamenettelyjen toteuttamista. Kaikki viisi kartoituksen kohdeyritystä kokivat toteuttaneensa tämän kohdan. Seuraavat kohdat käsittelivät toimitilojen eri osien pääsynhallintaa ja tämän dokumentoimista. Nämä seikat olivat kaikissa viidessä kartoituksen kohdeyrityksessä suurimmilta osin kunnossa. Tämän jälkeen tiedus-

teltiin, onko toimitilojen turvallisuudesta olemassa ohjeistus henkilöstölle, sisältäen asianmukaiset kulunvalvonnalliset seikat. Kartoituksen mukaan kaikki viisi kohdeyritystä olivat toteuttaneet tämän kohdan. Luottamuksellisia dokumentteja säilytettiin kartoituksen mukaan asianmukaisesti kolmessa viidestä kartoituksen kohdeyrityksestä. Toimitilojen paloturvallisuudesta ja murtosuojauksesta huolehtiminen oli kartoituksen mukaan hyvällä mallilla kaikissa viidessä kartoituksen kohdeyrityksessä.

ICT-laittilojen turvallisuutta käsittelevään osioon kuului samankaltaisia aihealueita, kuin yllä mainitulla toimitilojen turvallisuuden osiolla. Nämä oli kuvailtu yksityiskohtaisemmin kartoitusmateriaaleissa. Tästä osiosta oli monenlaisia vastauksia, josta voisi todeta yhteenvetona, että suurimmassa osassa kartoituksen kohdeyrityksistä asioista oli osittain huolehdittu ja kahdessa yrityksessä näitä ei sovellettu ollenkaan. Lähtökohtaisesti koko osio oli kartoitusyritysten kannalta melko epärelevantti.

## 5.8 Tietojärjestelmät

Tietojärjestelmät -kategoriassa käsiteltiin organisaatioiden tapaa käsitellä sähköpostin, pilvipalveluiden sekä mahdollisesti käytössä olevien SaaS-palveluiden tietoturvallisuutta.



Kuvio 8. Tietojärjestelmät



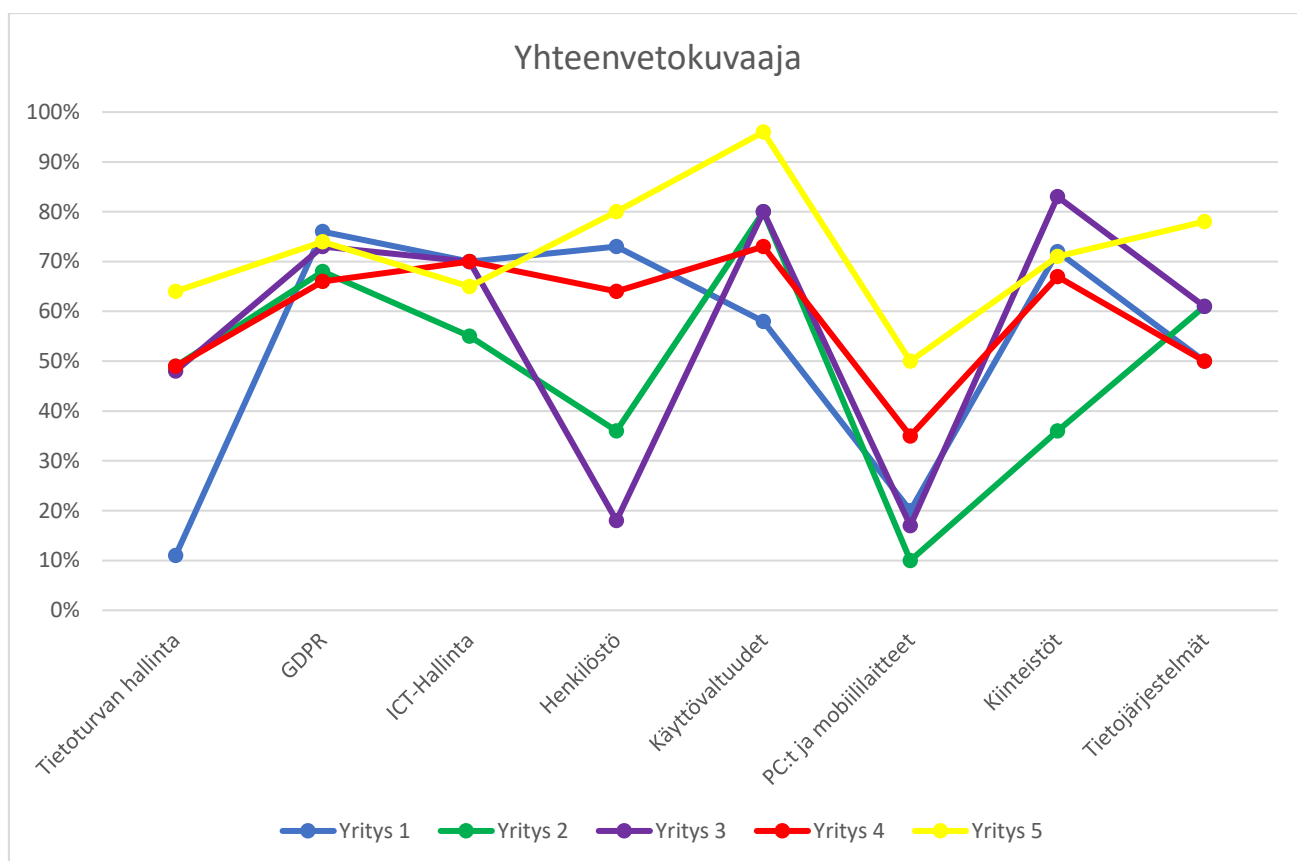
Tietojärjestelmät -kategoriassa käytiin lyhyesti läpi tietoturvallisuutta sähköpostin, pilvipalveluiden ja SaaS-palveluiden näkökulmasta. Sähköposti-osiossa ensimmäiseksi tiedusteltiin, oliko organisaatiolla olemassa sähköpostin käyttöä koskeva kirjallinen ohjeistus. Tätä ei löytynyt yhdestäkään kartoituksen kohdeyrityksestä. Tämän jälkeiset kohdat koskivat käyttäjien kouluttamista ymmärtämään sähköpostiviestinnän riskit, tunnistamaan haittaohjelmat ja huijausviestit sekä suojaamaan luottamukselliset sähköpostiviestit. Kahdessa kartoituksen kohdeyrityksessä suurin osa näistä kohdista oli toteutettu, lopuissa kolmessa kohdeyrityksessä ei mitään näistä. Roskapostien suodattaminen oli käytössä jokaisessa kartoituksen kohdeyrityksessä ja ohjeistus käyttäjän sähköpostien avaamisesta tämän ollessa estynyt oli toteutettu kahdessa kartoituksen kohdeyrityksessä.

Toinen osio käsitteli pilvipalveluita. Tässä osiossa aloitettiin tiedustelemalla, onko organisaatio arvioinut pilvipalveluiden soveltuvuuden niihin tallennettavien tietojen säilytykseen käyttöönoton yhteydessä. Tämä kohta oli kaikissa kartoituksen kohdeyrityksissä toteutettu. Seuraavaksi tiedusteltiin, onko organisaatiossa ohjeistus pilvipalveluiden käytöstä. Ohjeistus löytyi kartoituksen mukaan kahdesta kohdeyrityksestä. Viimeisenä tässä osiossa tiedusteltiin, onko organisaatio tietoinen, missä maassa tai alueella pilvipalveluun vietävät tiedot sijaitsevat. Tästä seikasta tietoisia oli kartoituksen mukaan kolme viidestä kohdeyrityksestä.

Viimeisenä kategorian osiona käytiin läpi SaaS-palveluja. Läpikäytävät kohdat koskivat muun muassa SaaS-palveluiden tietoturvallisuuden arvioimista, verkkopalveluiden käytöstä solmittuja sopimuksia, sisältäen kuvaukset palvelutasosta ja tietoturvasta sekä käytössä olevien verkkopalveluiden todentamista yhteyttä muodostettaessa ja tietoliikennetyksien salausta. Kolmessa kartoituksen kohdeyrityksessä nämä asiat olivat merkattu toteutetuksi. Kahdessa jäljelle jäävässä yrityksessä asian suhteen oltiin epävarmoja.

## 5.9 Yhteenvetokuvaaja

Yhteenvetokuvaajassa kartoituksen kaikkien kahdeksan kategorian tulokset ovat näkyvillä yrityskohtaisesti. Tästä kuviosta saa selkeimmän kuvan tulosten keskinäisestä hajonnasta kategorioiden välillä.



Kuvio 9. Yhteenvetokuvaaja

## 6 YHTEENVETO

Työn tarkoituksena oli tehdä tietoturva- ja tietosuojakartoituksia muutamiin pääjähämäläisiin yrityksiin ja näiden kartoitusten tuloksia läpikäymällä saada kuva yritysten tietoturvan ja tietosuojan hallinnasta sekä pohtia yritysten suoritustasoa ja siihen johtaneita syitä.

Ensimmäisenä asiana nousi mieleen, että tietoturva pienehköissä yrityksissä on keskimäärin (pois lukien esimerkiksi IT-alan yritykset) saanut todennäköisesti melko pintapuolisesti huomiota ja resursseja. Pk-yrityksiltä ei voida vaatia samaa tietoturvan toteuttamisen tasoa ja resursointia kuin suurilta yrityksiltä.

Tietosuojakartoitus herätti myös enemmän kysymyksiä kuin tietoturvapuolen kartoitus asian ollessa hyvin uutta. Tulee myös huomioida, että kartoituksia tehdessä voimaantulo oli vielä muutaman kuukauden päässä ainakin osalla yrityksistä (ensimmäinen kartoitus suoritettiin tammikuun lopussa ja viimeinen huhtikuun lopussa).

Lisäksi kartoitusten suorittamisen aikaiset versiot tietoturva- ja tietosuojakartoituksista oli suunnattu myös suurille yrityksille, mikä johti siihen, että osaa kartoituksen kohdista ei voitu soveltaa pk-yritysympäristössä (esimerkkinä yli 250 henkilön yrityksiä koskevat asiat EU:n tietosuojasetuksen suhteen ja mobiililaitteiden tietoturvan kartoituskategorian keskimääräinen heikko suoriutuminen johtuu suurelta osin siitä, että kohdeyritysten kokoisissa yrityksissä työn puolesta käytettävät mobiililaitteet ovat melko harvassa). Osaa kysymyksistä ei myöskään välttämättä ymmärretty täysin, koska yritysten kartoituksiin vastanneiden henkilöiden tietoturva- sekä tietosuojaosaamisen ja koulutuksen taso oli melko vaihtelevaa. Tähän lisättynä on hyvä ottaa huomioon vielä edellä mainittu fakta, EU:n tietosuojasetus ei ollut vielä tullut voimaan vaan voimaantulo oli noin kuukauden tai neljän kuukauden päässä (ensimmäisen ja viimeisen kartoituksen suoritusajankohdan välinen ero).

Kartoituksen tuloksia lienee vääristänyt osaksi myös kohdat, joihin on vastattu toteutuksen olevan kesken. Tästä annettu prosentuaalinen toteutusaste vaihteli yrityskohtaisesti yhdestä yhdeksäänkymmeneenhdeksään. Mahdotonta sinänsä tietää, kuinka tarkkoja arviot olivat. Kysymykset olivat osaltaan myös melko haastavia henkilölle, joka ei omaa vahvaa tietoteknistä taustaa tai ole muuten tutustunut tietoturvaan ja tietosuojaan. Tätä tietenkin voisi helpottaa selittämällä kysymyksiä auki enemmän ja hakemalla tietoturvaa vähemmän tuntevalle henkilölle sopivampaa lähestymistapaa kirjoitusasuun suhteen.

Osaltaan tuloksien tarkkuuteen vaikutti, että yritysten otanta jäi melko pieneksi. Alkuperäinen suunnitelma oli saada noin 20-30 yritystä mukaan kartoitukseen, tästä olisi saanut luonnollisesti vielä tarkemman kuvan aiheesta.

Senhetkistä kartoitusversiota olisi voinut jatkoa ajatellen räätälöidä pk-yritysympäristöön sopivammaksi muotoilemalla kysymyksiä helpommiksi ymmärtää ilman tietoteknistä taustaa sekä typistämällä osaa korkeamman suojausluokituksen tai suuria organisaatioita koskevista kysymyksistä.

Tutkimuksen läpikäynnin kartoituskysymykset ovat salattua tietoa, mistä johtuen asiasältö piti muokata sen mukaiseksi. Tämä vaikutti osaltaan sisällöntuotantoon.

## LÄHTEET

EU GDPR Portal 2019. EU GDPR.ORG [viitattu 27.3.2019]. Saatavissa: <https://eugdpr.org>

Euroopan unionin virallinen lehti 2016. EU yleinen tietosuoja-asetus [viitattu 27.3.2019]. Saatavissa: [www.privacy-regulation.eu/fi/](http://www.privacy-regulation.eu/fi/)

Kyberturvallisuuskeskus 2018. Tietoturva [viitattu 27.3.2019]. Saatavissa: <https://www.kyberturvallisuuskeskus.fi/fi/tietoturva>

OpiTietosuoja.fi 2019. Yleistä tietoturvasta [viitattu 23.4.2019]. Saatavissa: <https://opitietosujaa.fi/fi/aloitus/tietoturva>

Pilvi Cloud Company 2019. Mikä on SaaS-palvelu? [viitattu 18.4.2019]. Saatavissa: <https://www.pilvi.com/fi/mika-on-saas-palvelu/>

Tampereen teknillinen yliopisto (TUTWiki) 2010. Turvasuunnittelun yleisperiaatteita [viitattu 17.4.2019]. Saatavissa: <https://wiki.tut.fi/Tietoturva/TurvasuunnittelunYleisperiaatteita>

Tietosuojavaltuutetun toimisto 2019a. Henkilötietolaki [viitattu 5.5.2019]. Saatavissa: <https://tietosuoja.fi/henkilotietolaki>

Tietosuojavaltuutetun toimisto 2019b. Osoita noudattavasi tietosuojasäännöksiä [viitattu 22.4.2019]. Saatavissa: <https://tietosuoja.fi/osoitusvelvollisuus>

Tietosuojavaltuutetun toimisto 2019c. Tietosuoja [viitattu 27.3.2019]. Saatavissa: <https://tietosuoja.fi/tietosuoja>

Tietosuojavaltuutetun toimisto 2019d. Tietosuoja-asetus ei edellytä entisen kaltaista rekisteri- tai tietosuojaselostetta [viitattu 5.5.2019]. Saatavissa: [https://tietosuoja.fi/artikkeli/-/asset\\_publisher/tietosuoja-asetus-ei-edellyta-entisen-kaltaista-rekisteri-tai-tietosuojaselostetta](https://tietosuoja.fi/artikkeli/-/asset_publisher/tietosuoja-asetus-ei-edellyta-entisen-kaltaista-rekisteri-tai-tietosuojaselostetta)

Tietosuojavaltuutetun toimisto 2019e. Usein kysyttyä EU:n tietosuoja-asetuksesta [viitattu 27.3.2019]. Saatavissa: <https://tietosuoja.fi/gdpr>

Valtiovarainministeriö 2019. VAHTI-raportti 1/2016 [viitattu 4.4.2019]. Saatavissa: <https://www.vahtiohje.fi/web/guest/vahti-raportti-1/2016>