LAUREA AMMATTIKORKEAKOULU Uuden edellä

# Henkilöstön tietoturvakoulutuksen toteuttaminen valtionhallinnossa

Vallasvuo, Kaisa

2012 Leppävaara

**Laurea-ammattikorkeakoulu**
Laurea Leppävaara

# Henkilöstön tietoturvakoulutuksen toteuttaminen valtionhallinnossa

Kaisa Vallasvuo
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Marraskuu, 2012

**Laurea-ammattikorkeakoulu** **Tiivistelmä**
Laurea Leppävaara
Turvallisuusalan koulutusohjelma

Vallasvuo, Kaisa

**Henkilöstön tietoturvakoulutuksen toteuttaminen valtionhallinnossa**

Vuosi 2012 Sivumäärä 78

Tässä opinnäytetyössä tutkittiin henkilöstön tietoturvakoulutuksen suunnittelua ja toteutusta valtionhallinnossa sekä verkkokoulutusta koulutusmuotona. Tavoitteena oli tunnistaa tietoturvakoulutuksen suunnitteluun ja toteutukseen liittyviä vaiheita, niihin vaikuttavia tekijöitä sekä arvioida verkkokoulutuksen soveltuvuutta tietoturvakoulutukseen.

Opinnäytetyö on muodoltaan tapaustutkimus, jonka tulokset on kerätty kvalitatiivisilla tutkimusmenetelmillä kirjallisuuskatsaus ja haastattelu. Kirjallisuuskatsauksen avulla laadittiin teoreettinen kehys tietoturvakoulutuksesta sekä verkosta opetuksen välineenä. Tämän jälkeen haastateltiin kolmea valtionhallinnon organisaatiota tietoturvakoulutuksen järjestämisestä. Haastattelut olivat muodoltaan teemahaastatteluja, joiden kysymykset laadittiin teoreettisen kehyksen pohjalta.

Tutkimuksen lopputuloksena syntyi tietoturvakoulutuksen suunnittelua ja toteutusta kuvaava prosessimalli. Prosessimallissa kuvataan tietoturvakoulutuksen vaiheet ja vaiheisiin vaikuttavat tekijät. Keskeisimmät tietoturvakoulutuksen suunnitteluun ja toteutukseen vaikuttavat tekijät ovat koulutuksen tavoite ja kohderyhmä, käytössä olevat resurssit, viestintä, motivointi sekä johdon tuki.

Teoreettisen kehyksen sekä haastattelujen perusteella verkkokoulutuksen voidaan katsoa soveltuvan tietoturvakoulutuksen toteuttamiseen. Tulosten perusteella voidaan todeta, että kohderyhmän ollessa laaja tulisi verkkokoulutusta käyttää enemmänkin työntekijän valittavissa olevana vaihtoehtona muille koulutusmuodoille. Verkkokoulutus soveltuu parhaiten pienille kohderyhmille ja uusien työntekijöiden perehdyttämiskoulutukseen.

Asiasanat: tietoturvakoulutus, tietoturvatietoisuus, verkkokoulutus

**Laurea University of Applied Sciences** **Abstract**
Laurea Leppävaara
Bachelor's Degree Programme in Security Management

Vallasvuo, Kaisa

**Personnel's information security training in state administration**

Year 2012 Pages 78

This thesis investigates the design and implementation of information security training in state administration and online training as a form of education. The objectives were to identify stages relating to the design and implementation of information security training and factors affecting the stages. In addition, the objective was to evaluate the suitability of online environment for information security training.

The thesis is a case study, the results of which have been collected by using qualitative research methods: literature review and theme interviews. The theoretical basis of the research was established by a literature review of information security training and network as a teaching environment. The theme interviews were used to collect experiences of three state administration organizations about their information security training. The questions of the theme interviews were based on the theoretical basis.

A process model to describe the stages of information security training was created as the result of the research. The process model illustrates the stages and affecting factors of the design and implementation of information security training. The essential factors discovered were the objective of training, target audience, resources available, communication, motivation and executive support.

Based on the theoretical basis and interview, online training can be considered suitable for information security training. However, for a large target audience, online training should be used more as an alternative training method chosen by employees. Online training is best suitable for small target audience and for new employees' orientation.

Keywords: information security training, information security awareness, online training

Sisällys

# 1 Johdanto

Julkishallinnon toiminta on pitkälti riippuvainen erilaisten tietoaineistojen käsittelystä ja tiedonsiirrosta. Merkitystä ovat lisänneet tietoyhteiskunnan kehittyminen, kansainvälistyminen, verkostoituminen sekä toimintojen ja palveluiden siirtyminen tietoverkkoihin. (VAHTI 6/2003, 5.) Riippuvuus on huomioitu myös viranomaisia koskevassa lainsäädännössä, jossa valtionhallinnon organisaatioilta edellytetään hyvää tiedonhallintatapaa. Hyvään tiedonhallintatapaan kuuluu tietoturvallisuudesta huolehtiminen, jonka tarkoitukseksi usein mielletään salassa pidettävien tietojen suojaaminen. Tietoturvallisuudella voidaan kuitenkin suojata tiedon luottamuksellisuuden lisäksi myös eheyttä tai käytettävyyttä. (VAHTI 2/2010, 8.) Tietoturva on pettänyt silloin, kun tiedon suojattavaan ominaisuuteen kohdistuu jokin loukkaus, esimerkiksi salassa pidettävää tietoa paljastuu ulkopuolisille tai tietoa muutetaan oikeudettomasti.

Tietoturvallisuuden toteuttamiskeinoina pidetään usein teknisiä ratkaisuja, esimerkiksi salasanat, tiedon salaaminen, varmuuskopiointi, käyttöoikeuksien hallinta ja kulunvalvonta. Tietoturvallisuus on kuitenkin viime kädessä riippuvainen ihmisten toimintatavoista. Tietoturvavahingoissa onkin useimmiten kyse työntekijöiden vääränlaisista toimintatavoista. Tekniset tietoturvaratkaisut ovat tehottomia, mikäli työntekijät eivät noudata organisaation tietoturvakäytäntöjä ja -ohjeita. (Chapple, Gibson & Stewart 2012, 257.) Syynä voi olla esimerkiksi, ettei tietoturvauhkaa ole tiedostettu, oikeita toimintatapoja tiedetty tai haluttu noudattaa. (VAHTI 11/2006, 11.)

Ihmisten toiminnasta johtuvien tietoturvavahinkojen ennaltaehkäisyssä on kyse tietoturvatietoisuudesta ja sen tasosta. Tietoturvatietoinen ihminen tunnistaa tilanteet, joissa voi olla kyse tietoturva-asiasta ja osaa toimia tilanteen edellyttämällä tavalla. Tietoturvakoulutus on keskeisessä roolissa, kun kyseessä on tietoturvatietoisuuden edistäminen. Lisääntynyt verkkorikollisuus ja lainsäädännön velvoitteiden täyttäminen ovat saaneet organisaatiot kouluttamaan henkilöstöään.

Verkkokoulutus on koulutusmuotona löytänyt hiljalleen tiensä koulu- ja oppilaitosympäristöstä työelämän organisaatioihin. Koulutusmuoto on suosittu muun muassa sen organisaatiolle tuomien kustannussäästöjen vuoksi. Lisäksi organisaatioissa on ymmärretty, että kilpailukyvyn säilyttäminen edellyttää jatkuvaa tiedon ja osaamisen kehittämistä, eikä perinteisten koulutusmenetelmien käyttö yksinään tehosta ja helpota työntekijöiden oppimista. (Mäkitalo & Wallinheimo 2012, 38.) Organisaatioilta edellytetäänkin nopeampia ja joustavampia koulutusmenetelmiä, jotka eivät ole tiettyyn aikaan tai paikkaan sidottuja. Oppimisesta saadaan myös tehokasta ja nopeaa, kun koulutus järjestetään oikeassa paikassa ja oikeaan aikaan. (Alamäki & Luukkonen 2002, 16–17.) Toisaalta säästötoimenpiteet edellyttävät organisaatioilta tehokkaampien koulutusmuotojen etsimistä perinteisten menetelmien rinnalle.

## 1.1 Opinnäytetyön aihe ja tavoite

Tämän opinnäytetyön aiheena on tutkia henkilöstön tietoturvakoulutuksen suunnittelua ja toteutusta, sekä verkkokoulutusta koulutusmuotona kolmessa valtionhallinnon organisaatiossa. Tavoitteena on tunnistaa tietoturvakoulutuksen suunnitteluun ja toteutukseen liittyviä vaiheita, niihin vaikuttavia tekijöitä sekä arvioida verkkokoulutuksen soveltuvuutta tietoturvakoulutukseen.

## 1.2 Tutkimusstrategia ja -menetelmät

Opinnäytetyön tutkimusstrategiana on kartoittava tapaustutkimus, jolle tyypillisiä piirteitä ovat yksityiskohtaisen ja intensiivisen tiedon saaminen yksittäisestä tapauksesta tai pienestä joukosta toisiinsa suhteessa olevista tapauksista. (Hirsjärvi, Remes & Sajavaara 2010, 134; Eriksson & Koistinen 2005, 15). Kartoittavan tutkimuksen tarkoituksena on muun muassa etsiä uusia näkökulmia, katsoa mitä tapahtuu ja löytää uusia ilmiöitä. (Hirsjärvi, Remes & Sajavaara 2010, 138).

Aineiston keräämiseen käytetään kvalitatiivisia tutkimusmenetelmiä. Kvalitatiivisessa eli laadullisessa tutkimusmenetelmässä lähtökohtana on todellisen elämän kuvaaminen, jossa erilaiset tapahtuvat vaikuttavat samanaikaisesti toisiinsa ja tutkimuksen kohdetta pyritään tutkimaan kokonaisvaltaisesti (Hirsjärvi, Remes & Sajavaara 2010, 161). Laadulliselle tutkimusmenetelmälle on tyypillistä, että kohdejoukko valitaan tarkoituksenmukaisesti eikä satunnaisella otannalla, kuten määrällisessä tutkimuksessa (Hirsjärvi, Remes & Sajavaara 2010, 164).

Laadullisen tutkimusotteen ideana on luoda kuvaava malli tutkittavalle ilmiölle sekä ymmärtää ja tulkita sitä. Pisimmälle vietynä laadullinen tutkimusmenetelmä etenee siis empiriasta teoriaan. Tästä syystä laadullinen tutkimus tarvitsee viitekehyksen, jota vasten ilmiöstä tehtyjä havaintoja tarkastellaan. Laadullisessa tutkimuksessa käytetään aineistonkeruumenetelminä muun muassa haastatteluja, havainnointia ja tutkijan muistiinpanoja. (Pitkäranta 2010, 20–21.) Tässä opinnäytetyössä käytetään tutkimuksen aineiston keräämiseksi kirjallisuuskatsausta ja haastatteluja.

### 1.2.1 Kirjallisuuskatsaus

Opinnäytetyön teoreettinen viitekehys rakennetaan kirjallisuuskatsauksen avulla. Käytettävä kirjallisuuskatsaus on tyypiltään kuvaileva, joka sopii yleiskatsauksen luomiseen ilman tiukkoja tai tarkkoja sääntöjä. Tämä näkyy muun muassa siten, että tutkimuksessa voidaan käyttää laajoja aineistoja eikä käytettävän aineiston valintaa määrää metodiset säännöt. (Salminen 2011, 6.) Kirjallisuuskatsaus on myös tutkimuksen tekijälle oppimismahdollisuus, jolla tekijä

voi osoittaa kykenevänsä hakemaan kirjallisuudesta tutkimuksen kannalta keskeiset pääasiat ja rakentamaan tutkimuksen perustan omin sanoin. Kirjallisuuskatsauksen avulla rakennettua teoreettista viitekehystä verrataan tutkimuksen lopussa saatuihin tuloksiin. (Hirsjärvi, Remes & Sajavaara 2010, 259.) Tämän opinnäytetyön teoreettinen kehys rakentuu tietoturvakoulutuksen ja verkko-opetuksen näkökulmista.

### 1.2.2 Haastattelu

Haastattelu on laadulliselle tutkimukselle tyypillinen aineistonkeruumenetelmä, sillä useimmiten tutkimusaineistoksi haetaan ihmisten kokemuksia. Aineistoksi soveltuu niin ikään esimerkiksi esineet, kuva- ja tekstiaineistot, päiväkirjat, kirjeet, lehdet, mainokset ja elämäkerrat. Haastattelumuotoja ovat lomakehaastattelu, avoin haastattelu ja teemahaastattelu. (Vilkka 2005, 100–101.) Lomakehaastattelussa kysymykset ovat strukturoidussa muodossa eli kysymysten muoto ja järjestys ovat ennalta määrättyjä. Avoimessa haastattelussa kysymysten esittäminen on vapaamuotoista. Esitettävät kysymykset muovautuvat haastattelun edetessä riippuen haastateltavan ajatuksista, mielipiteistä, tunteista ja käsityksistä. (Hirsjärvi, Remes & Sajavaara 2010, 208–209.)

Opinnäytetyöhön valittiin haastattelumuodoksi teemahaastattelu, joka on lomake- ja avoimen haastattelun välimuoto. Teemahaastattelulle on ominaista keskeisten aiheiden ja teemojen valinta teoreettisen viitekehyksen pohjalta, ja jotka ovat oleellisia tutkimusongelmaan vastaamiseksi. Teemojen ja sen myötä kysymysten järjestyksellä ei ole haastattelussa väliä. (Vilkka 2005, 102.) Teemahaastattelu soveltuu tähän opinnäytetyöhön myös siksi, että haastattelun aiheet ovat tiedossa, mutta kysymysten tarkkaa muotoa ja järjestystä voidaan vaihdella tarpeen mukaan haastattelun edetessä. (Hirsjärvi, Remes & Sajavaara 2010, 208.)

## 1.3 Keskeiset käsitteet

**Tietoturvallisuus** tai tietoturva tarkoittaa tiedon, palvelujen, järjestelmien ja tietoliikenteen suojaamista hallinnollisilla, teknisillä sekä näiden lisäksi muilla toimenpiteillä. Tietoturvallisuudella pyritään suojaamaan tiedon *luottamuksellisuus, eheys* ja *käytettävyys* normaali- ja poikkeusoloissa. (VAHTI 3/2007, 13.) Tiedon luottamuksellisuudella tarkoitetaan, että tietoon pääsee käsiksi vain tietoon oikeutetut henkilöt. Eheys korostaa tiedon oikeellisuutta ja käyttökelpoisuutta eli tietoa ei ole muutettu oikeudettomasti esimerkiksi hävittämällä tai lisäämällä tietoa. Käytettävyydellä viitataan tiedon saatavuuteen eli tietoon oikeutetut henkilöt pääsevät käsiksi tietoon haluttuna aikana ja tavalla. (Kerko 2001, 23–24.)

**Tietoturvatietoisuudella** tarkoitetaan työntekijöiden kykyä ymmärtää tietoturva-asioita sekä heidän sitoutumistaan tietoturvallisuuteen. Hyvä ja kehittynyt tietoturvatietoisuus näkyy

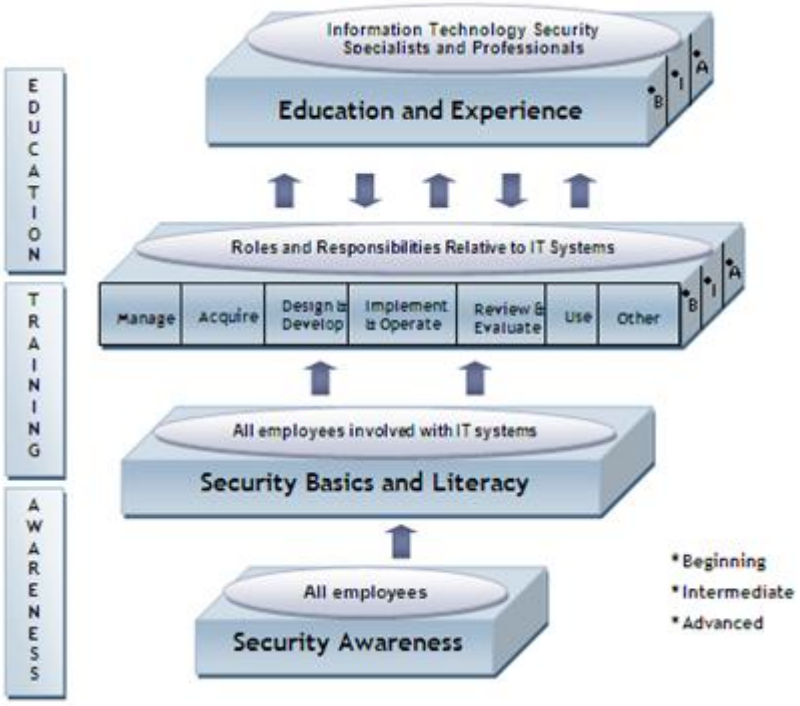
työntekijöiden asenteiden ja tietoturvakäyttäytymisen muuttumisena. Tietoturvatietoinen työntekijä lisäksi raportoi havaitsemistaan tietoturvaongelmista eteenpäin. Tietoturvatietoisuudella voidaan myös tarkoittaa työntekijöiden huomion kiinnittämistä tietoturva-asioihin. (Hash & Wilson 2003, 8-9.)

**Verkkokoulutus** tai verkko-opetus on yleisesti tunnettu käsite, mutta sen tarkka määritelmä on vielä toistaiseksi vakiintumaton eikä käsitteen tarkasta sisällöstä ja rajauksesta olla yksimielisiä. Verkkokoulutus voidaan muun muassa määritellä opetukseksi minkä tahansa sähköisen median kautta. (Alamäki & Luukkonen 2002, 12–13; Sandars 2006, 1.) Tässä opinnäytetyössä verkkokoulutuksella tarkoitetaan verkko-oppimisympäristössä tapahtuvaa opettamista.

**Verkko-oppimisympäristöllä** tarkoitetaan usein verkko-opetuksessa hyödynnettävää verkkopalvelua, jota käytetään www-selaimella. Verkko-oppimisympäristö luodaan verkkoon siihen tarkoitetulla ohjelmalla ja palvelu toimii www-palvelimella. Verkko-oppimisympäristöstä voidaan käyttää myös esimerkiksi nimityksiä oppimisalusta ja virtuaalinen oppimisympäristö. Verkko-oppimisympäristötuotteita ovat muun muassa Moodle, WebCT, Discendum Optima, Fronter ja Oppimappi. (Keränen & Penttinen 2007, 28–29.) Tässä opinnäytetyössä verkko-oppimisympäristöllä tarkoitetaan ympäristön luomiseen tarkoitetun ohjelmiston ja sen alustalle rakennetun oppimateriaalin kokonaisuutta.

## 2 Tietoturvakoulutus- ja tietoisuusohjelma

Tietoturvakoulutus- ja tietoisuusohjelma (*eng. A Security Education, Training and Awareness Program*) voidaan määritellä koulutuskokonaisuudeksi, joka on suunniteltu vähentämään organisaation työntekijöiden tietoturvaohjeiden vastaisesta toiminnasta johtuvien tietoturvaloukkausten määrää (Hight 2005, 1). Tietoturvakoulutus- ja tietoisuusohjelman tavoitteena on edistää työntekijöiden tietoturvatietoisuutta ja siten muuttaa heidän tietoturvakäyttäytymistä toivottuun suuntaan. Ohjelma perustuu oppimisen tasoja kuvaavaan malliin (kuva 1), joka rakentuu kolmesta osatekijästä: *awareness*, *training* ja *education*. Mallin lähtökohtana on oppimisen näkeminen jatkumona, joka alkaa tietoisuudesta ja jatkuu käytännön harjoitteluun ja siitä syvemmälle oppimisen, tiedon ja kokemuksen tasolle. (Ippolito, Pitcher, Tressler & de Zafra 1998, 13.)




Kuva 1: Malli oppimisen tasoista (Ippolito, Pitcher, Tressler & de Zafra 1998, 13)

National Institute of Standards and Technology, NIST, on laatinut tietoturvakoulutuksen ja -tietoisuuden viitekehyksen, joka esittää näiden osatekijöiden ominaisuuksia ja toistensa välisiä suhteita (NIST 1995, 147). Viitekehys on kuvattu taulukossa 1.

| | AWARENESS | TRAINING | EDUCATION |
|---|---|---|---|
| Attribute: | "What" | "How" | "Why" |
| Level: | Information | Knowledge | Insight |
| Learning Objective | Recognition and Retention | Skill | Understanding |
| Example Teaching Method: | Media<br>- Videos<br>- Newsletters<br>- Posters | Practical Instruction<br>- Lecture and/or demo<br>- Case study<br>- Hands-on practice | Theoretical Instruction<br>- Seminar and discussion<br>- Reading and study<br>- Research |
| Test Measure: | True/False<br>Multiple Choice<br><br>(identify learning) | Problem Solving, i.e., Recognition and Resolution<br><br>(apply learning) | Essay<br><br>(interpret learning) |
| Impact Timeframe: | Short-term | Intermediate | Long-term |

Taulukko 1: Tietoturvakoulutuksen- ja tietoisuuden viitekehys (Ippolito, Pitcher, Tressler & de Zafra 1998, 18)

Tietoturvatietoisuuden edistäminen voidaan nähdä varsinaista tietoturvakoulutusta edeltävänä vaiheena, jolla pyritään muuttamaan asenteita siten, että organisaatiossa ymmärretään tietoturvallisuuden tärkeys organisaation toiminnan kannalta sekä tuodaan esille tietoturvan pettäessä siitä organisaatiolle koituvat vahingolliset seuraukset. Viitekehystä kuvaavasta taulukosta 1 käy ilmi, että *awareness* (suom. tietoisuus) hakee vastausta kysymykseen ”mitä”. Se siis muistuttaa työntekijöitä organisaation tietoturvakäytäntöjen olemassaolosta ja niiden noudattamisen tärkeydestä päivittäisessä työssä. (NIST 1995, 146.)

Tietoturvatietoisuuden edistämiseksi voidaan käyttää erilaisia menetelmiä. Ne voivat olla esimerkiksi videoita, julisteita, tietoiskuja, tiedotteita, esitteitä tai oheistuotteita kuten mukeja, hiirimattoja, avainnauhoja, jotka käsittelevät jotakin tiettyä tietoturva-aiheista teemaa. (Mattord & Whitman 2010, 201.) Tehokas tietoturvatietoisuuden edistäminen edellyttää kuitenkin luovuutta ja säännöllisesti vaihtuvia menetelmiä, joilla tietoturva-asioita viestitään organisaatiossa, sillä ihmisillä on taipumus olla lopulta reagoimatta. Esimerkiksi tietoturva-aiheinen juliste organisaation kahvihuoneessa sulautuu aikanaan osaksi ympäristöä, eikä siihen kiinnitetä enää samalla tavoin huomiota. (NIST 1995, 148.)

Suomen kielestä ei löydy yllä esitettyyn viitekehykseen sopivia vastineita englanninkielisille sanoille *training* ja *education*, vaan niistä käytetään alan suomenkielisessä kirjallisuudessa yhteistä nimitystä ”koulutus”. *Training* viittaa koulutukseen, jossa organisaation työntekijöille tarjotaan yksityiskohtaiset tiedot ja käytännön ohjeet (Mattord & Whitman 2010, 193). Viitekehyksen mukaan *training* vastaa kysymykseen ”miten” eli oppimisen tavoitteena on saada riittävä tietämys ja taidot, joiden avulla työntekijöiden on mahdollista suoriutua työtehtävistä tietoturvakäytäntöjen edellyttämällä tavalla. Esimerkiksi työntekijä osaa salata luottamuksellista tietoa sisältävän sähköpostiviestin, joka ilman riittävää osaamista lähetettäisiin salaamattomana, mikä on useimmiten yrityksissä tietoturvaohjeiden vastaista. *Education* eroaa *training* muotoisesta koulutuksesta siten, että kyseessä on pidempiaikainen, esimerkiksi ammattilaisille suunnattu tutkintokoulutus yliopistossa tai ammattikorkeakoulussa (Hash & Wilson 2003, 10). Vaikka oppimisen kolmas taso (kts. kuva 1) on suunnattu alan ammattilaisten osaamisen kehittämiseen, voisi tasoa soveltaa tietyiltä osin tietoturvakoulutus- ja tietoisuusohjelmassa myös organisaation muihin työntekijöihin, sillä ”mitä” ja ”miten” kysymysten sijaan *education* tavoittelee ymmärrystä ja oivalluskykyä eli ”miksi” tietoturvatyötä tehdään.

Tietoturvakoulutus- ja tietoisuusohjelmille on yhteistä se, että niiden tavoitteena on ohjata työntekijöiden tietoturvakäyttäytymistä toivottuun suuntaan. Työntekijöiden vääränlaiset toimintatavat vaarantavat organisaation tieto-omaisuuden turvallisuuden. Työntekijöiden riittävä informoiminen tietoturvauhista ja niiden ilmenemismuodoista yhdessä tietoturvakäytäntöjen harjoittelun kanssa vähentävät riskiä, jossa tietoaineiston luottamuksellisuus, eheys tai käytettävyys vaarantuu. (Mattord & Whitman 2010, 200.)

## 2.1 Tietoturvakoulutus

Tietoturvakoulutuksella ja tietoisuuden edistämisellä pyritään vaikuttamaan organisaation henkilöstön tietoturvakäyttäytymiseen. Tietoturvakoulutuksen tavoitteena on parantaa työntekijöiden tietoturvatietoisuutta sekä muuttaa asenteita ja vääränlaisia toimintatapoja. Tarkoituksena on, että työntekijät noudattaisivat organisaation laatimaa tietoturvapolitiikkaa ja siihen liittyviä ohjeita, joilla suojataan organisaation tieto-omaisuutta. (Nykänen 2011, 20.) Laaksosen, Nevasalon & Tomulan (2006, 258) mukaan työntekijöiden tulisi ymmärtää omaan työhönsä liittyvät tietoturvariskit sekä millaisilla toimintatavoilla tietoturvariskien toteutumista voidaan ehkäistä. Olennaisinta ei siis ole tietää kaikesta kaikkea, vaan tunnistaa omaan työhön liittyvät tietoturvauhat ja hallita toimenpiteet niiden torjumiseksi.

Asenteilla on yhteys käyttäytymiseen. Myönteinen asenne, esimerkiksi tietoturvakoulutusta kohtaan, johtaa yleensä siihen, että kohdetta halutaan lähestyä eli asiasta ollaan kiinnostuneita. Kielteinen asenne näkyy puolestaan kohteen välttelynä. (Lahikainen & Pirttilä-Backman 2006, 91.) Lahikaisen & Pirttilä-Backmanin (2006, 92) mukaan asenteet muodostuvat vuorovaikutustilanteissa joko oman kokemuksen pohjalta tai muiden kertomana. Esimerkiksi jos yhteisössä suhtaudutaan yleisesti ottaen kielteisesti tietoturvakoulutukseen, voi neutraalin tai myönteisen asenteen omaava työntekijä alkaa suhtautua itsekin negatiivisesti. Vastaavasti yleinen myönteinen suhtautuminen tietoturvakoulutukseen voi muuttaa asenteita myönteiseen suuntaan myös yksilötasolla.

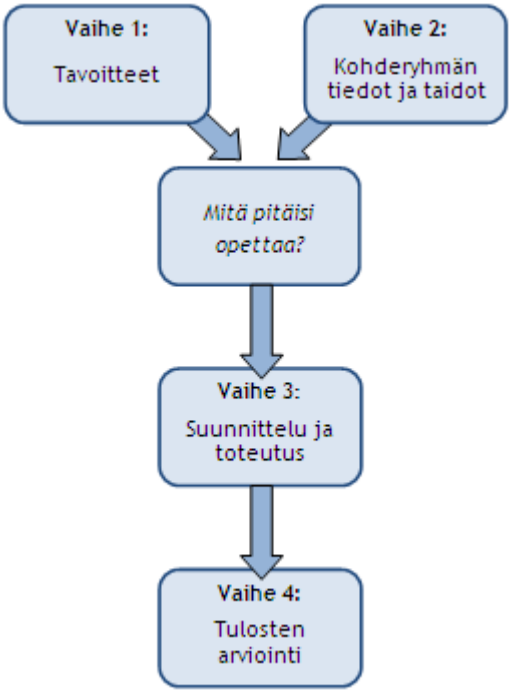
Lafleurin (1992) näkemyksen mukaan tietoturvakoulutuksen tulisi perustua objektiiviseen asenteeseen, jonka pyrkimyksenä on saada työntekijä ymmärtämään oma roolinsa tietoturvakäytäntöjen toteuttajana. Objektiivinen asenne ilmenee siten, että työntekijän henkilökohtainen näkemys ja asenne eivät vaikuta päätökseen noudattaa tai olla noudattamatta tietoturvaohjeita. Koulutuksessa tulisi lisäksi ottaa huomioon sosiaalinen näkökulma, sillä motivaatio ja asenteet vaikuttavat olennaisesti siihen, miten työntekijät suhtautuvat organisaation tietoturvaohjeisiin. Tietoturvakoulutuksen tulisikin pitää sisällään myös eettistä koulutusta asenteiden muuttamiseksi sekä tietoturvan tärkeyden tiedostamiseksi, jotta organisaatiossa voidaan muuttaa työntekijöiden omaksumia vääränlaisia toimintatapoja. (Nykänen 2011, 21–22).

Tietoturvakoulutuksella voi olla erilaisia kohderyhmiä. Kohderyhmä voi olla organisaation koko henkilöstö tai jokin erityisryhmä esimerkiksi ylin johto, esimiehet, tietohallinto, henkilöstöhallinto tai viestintäyksikkö. Organisaation tulisi kouluttaa oman henkilöstönsä lisäksi tarpeen mukaan myös organisaation toimintaverkostoon kuuluvat henkilöt. Tällaisia henkilöitä ovat alihankkijat, konsultit, palveluntuottajat ja -toimittajat sekä muut kolmannet osapuolet, joilla on pääsy organisaation tietoaineistoihin ja -järjestelmiin. (Krause & Tipton 2009, 96.)

Tietoturvakoulutuksesta voi vastata organisaation oma tietoturva-asiantuntija tai koulutusta varten voidaan hankkia ulkopuolinen kouluttaja. Usein tietoturvakoulutuksesta vastaa organisaation tietoturvapäällikkö tai tietoturva-asiantuntija. Tällöin kouluttaja on usein aiheen asiantuntija, mutta kouluttajalta voi puuttua pedagoginen osaaminen. (Mattord & Whitman 2010, 197.) Pedagogisen osaamisen puuttuminen voi osaltaan johtaa siihen, ettei koulutuksessa osata ottaa huomioon riittävästi koulutuksen kohteina olevia työntekijöitä sekä heidän lähtökohtiaan, kuten aiempaa tietoa ja osaamista. Lisäksi koulutus mielletään usein yhdensuuntaiseksi tiedon välittämiseksi, jossa kouluttaja välittää tiedon kuuntelijoille puhumalla. Tällainen lähestymistapa ei ota huomioon erilaisia oppijoita tai oppimistyylejä. (Herold 2011, 58–59.)

### 2.1.1 Tietoturvakoulutuksen suunnittelu ja toteutus

Tietoturvakoulutuksen lähtökohtana on koulutukselle tunnistettu tarve, joka voi olla esimerkiksi organisaation uudet tietoturvaohjeet tai lakimuutoksen myötä muuttuvat tietoturvakäytännöt ja -velvoitteet. Onnistunut tietoturvakoulutus edellyttää huolellista suunnittelua ja toteutusta. Kuvassa 2 on hahmotettu tietoturvakoulutuksen neljä vaihetta: tavoitteet, kohderyhmä, suunnittelu ja toteutus sekä tulosten arviointi. Kuvan havainnollistamiseksi käytetään vaiheiden selitysten yhteydessä kuvitteellista esimerkkiä. Esimerkkinä toimiva kuvitteellinen organisaatio käsittelee luottamuksellista tietoa kuten tuotehintoja sekä asiakas- ja tuotetietoja.




Kuva 2: Tietoturvakoulutuksen vaiheet (Schott & Driscoll 1997, 162)

Tunnistettu tarve määrittelee koulutukselle asetettavat tavoitteet (vaihe 1) eli mitä työntekijöiden halutaan oppivan. Mitä työntekijöiden tulee tietää ja miksi? Miten työntekijöiden tulisi ajatella ja toimia koulutuksen jälkeen? (Alexander, Finch, Sutton & Taylor 2008, 146.) Esimerkin organisaation toteuttamista selvityksistä käy ilmi, että organisaation työntekijät noudattavat organisaation tietoturvaohjeita ja -käytäntöjä lukuun ottamatta sähköpostia. Organisaation sähköpostin tietototurvaohjeistusten mukaan luottamukselliset tiedot tulee aina lähettää salattuna. Ohjeistuksesta huolimatta organisaation myyntitiimin työntekijät eivät salaa sähköposteja. Tällöin organisaatiolla on tarve tietoturvakoulutukselle, jonka tavoitteena on saada myyntitiimin työntekijät noudattamaan sähköpostin tietoturvapolitiikkaa. (Puhakainen 2006, 74.)

Kun koulutuksen tavoitteet ovat selvillä, tarkastellaan kohderyhmän nykytietämystä koulutettavasta aiheesta (vaihe 2). Mitä asioita kohderyhmä osaa ja hallitsee ennestään? Työntekijöiden nykytietämyksen ja koulutettavan aiheen välinen ero määrittelee mitä työntekijöiden tulee vielä oppia (Schott & Driscoll 1997, 162). Nykänen (2011, 18) korostaa, että nykytietämyksen lisäksi tulee tunnistaa, miten motivoitunutta ja millaisia asenteita kohderyhmällä on tieturvallisuuteen liittyen. Esimerkin organisaation nykytilanteen kartoitus osoittaa, että myyntitiimin työntekijät eivät ymmärrä luottamuksellisen tiedon salaamisen tärkeyttä organisaation näkökulmasta. Lisäksi heillä ei ole riittävää tietämystä luottamuksellisen tiedon luokitteluperiaatteista. Näin ollen tietoturvakoulutuksessa tulee keskittyä tiedon luokittelun periaatteisiin sähköpostin tietoturvapolitiikan sijaan sekä saada työntekijät ymmärtämään tiedon salaamisen merkitys organisaation näkökulmasta. (Puhakainen 2006, 75.)

Onnistunut tietoturvakoulutus edellyttää huolellista suunnittelua (vaihe 3). Tässä vaiheessa ratkaistaan millaisia pedagogisia menetelmiä käytetään: onko koulutus vuorovaikutteista keskustelua vai yksisuuntaista koulutusmateriaalin läpikäyntiä opettajan johdolla tai mahdollisesti itseopiskelua? Lisäksi tulee ratkaista millaista kanavaa koulutukseen käytetään. (Puhakainen 2006, 75.) Koulutuskanava voi olla esimerkiksi organisaation Intranet, verkko-oppimisympäristö, ryhmäkokous tai kohderyhmälle järjestettävä koulutustilaisuus. Oleellista on tuntea kohderyhmä, jotta koulutus voidaan toteuttaa kohderyhmälle parhaiten soveltuvalla tavalla.

Esimerkin organisaatio järjestää myyntitiimille koulutustilaisuuden, joka alkaa ryhmäkeskustelulla. Keskustelun aiheena ovat Internetin riskit ja uhat sekä organisaation sähköpostipolitiikka, jonka jälkeen työntekijät tunnistavat opettajan johdolla millaisia kriittisiä tietoja myyntitiimissä käsitellään. Tämän tarkoituksena on aktivoida työntekijöiden ennakkotietoja aiheesta. Seuraavaksi työntekijät arvioivat millaisia vaikutuksia, esimerkiksi tiedon paljastumisella ulkopuolisille voi olla työntekijöiden omalle työlle ja organisaation liiketoiminnalle. Tavoitteena on ymmärtää miksi tietoaineistojen oikeanlainen luokittelu ja käsittely ovat tär-

keitä. Lopuksi käydään läpi miten tietoaineistojen suojaaminen tehdään käytännössä. (Puhakainen 2006, 76.)

Tietoturvakoulutuksen tuloksia tulee myös arvioida (vaihe 4), jotta tiedetään missä määrin koulutuksen tavoitteet ovat saavutettu. Tuloksia voidaan tutkia esimerkiksi kyselyllä tai haastattelemalla. (Puhakainen 2006, 76.) Tietoturvakoulutuksen vaikuttavuuden arviointia käsitellään enemmän kohdassa 2.2.

Tietoturvakoulutuksen onnistumisen kannalta on tärkeää saada koulutukselle johdon tuki. Pelkkä resurssien myöntäminen koulutusta varten ei riitä, vaan tuen tulee olla myös henkilöstölle näkyvää toimintaa. Johto osoittaa esimerkillään muulle henkilöstölle kuinka tärkeänä tietoturvallisuutta organisaatiossa pidetään. Mikäli johto ja esimiehet eivät esimerkiksi noudata tietoturvaohjeita tai osallistu kaikille yhteisiin tietoturvakoulutuksiin, on todennäköistä, että suuri osa henkilöstöstä seuraa johdon esimerkkiä. (Herold 2011, 89.)

### 2.1.2 Tietoturvakoulutuksen jatkuvuus

Säännöllinen tietoturvakoulutus on edellytys organisaation työntekijöiden tietoturvatietoisuuden ylläpitämiselle ja edistämiselle. Hyvä tietoturvatietoisuus näkyy osana organisaation turvallisuuskulttuuria, joka tukee työntekijöiden turvallisuutta ja turvallista työntekoa ja varmistaa siten osaltaan organisaation toiminnan jatkuvuuden. (Laulajainen 2012.) Usein tietoturvakoulutus ja tietoisuuden edistäminen sekä siihen liittyvät ohjelmat epäonnistuvat juurikin vähäisen tai olemattoman jatkon takia, jolloin koulutus jää ainutkertaiseksi toteutukseksi (Peltier 2005, 40).

Koulutuksen jatkuvuus ei ole aina organisaation omasta tahtotilasta kiinni, vaan esimerkiksi lainsäädäntö ja erilaiset normistot voivat edellyttää organisaatiota järjestämään tietoturvakoulutusta säännöllisesti. Erityisesti julkishallinnossa perusteet säännölliselle koulutukselle tulevat lainsäädännöstä. Lakien ja normistojen lisäksi organisaation sisäisessä ja ulkoisessa toimintaympäristössä tapahtuvat muutokset esimerkiksi lainsäädännössä, organisaation tietoturvapolitiikassa ja –ohjeissa, tietojärjestelmissä tai käytössä olevassa teknologiassa edellyttävät organisaatiolta henkilöstön jatkuvaa kouluttamista työntekijöiden riittävän tietämyksen ja osaamisen ylläpitämiseksi. (Laulajainen 2012.)

Säännöllistä koulutusta voidaan ylläpitää esimerkiksi laatimalla koulutussuunnitelma, jota päivitetään organisaatiossa vuosikellon mukaan. Koulutussuunnitelmaan voidaan esimerkiksi määrittää, että organisaatio järjestää koko henkilöstöä koskevan tietoturvallisuuden peruskoulutuksen kolmen vuoden välein. Sen lisäksi peruskoulutuksen käy jokainen organisaatioon tuleva uusi työntekijä perehdytyksen yhteydessä. Organisaatioon tuleva työntekijä voi olla

myös sidosryhmästä. Sidosryhmille kuten konsulteille ja palvelutoimittajille on suunnitelmassa oma koulutuksensa, jossa käydään läpi miten heidän tulee käsitellä organisaation tietoja. (Laulajainen 2012.)

Laulajaisen (2012) mukaan tämän kaltaisen koulutussuunnitelman ylläpitäminen ja hallinnointi on kunnianhimoista ja vaatii paljon resursseja. Koska organisaatiolla on usein käytössä koulutusta varten rajalliset resurssit, on tärkeää sovittaa koulutussuunnitelma organisaation tarpeita vastaavaksi. Etusijalla tulee aina olla organisaation oma henkilöstö, sillä he ovat organisaation toiminnassa avainasemassa. Tietoturvakoulutusta koskevan koulutussuunnitelman ylläpitämisessä ja hallinnoimisessa kannattaa tehdä yhteistyötä organisaation koulutusosaajien esimerkiksi henkilöstöosaston koulutusvastaavien kanssa. Koulutussuunnitelmaa ei kuitenkaan pidä seurata liian tiiviisti vuosikellon mukaan, sillä tietoturvakoulutusta tulisi järjestää aina ilmenneen tarpeen mukaan. Tällainen voi olla esimerkiksi ajankohtainen tietoturvaa koskeva ilmiö kuten uusi huijaustekniikka käyttäjätunnusten ja salasanojen anastamiseksi. Koulutus voi olla luonteeltaan informatiivista esimerkiksi huijaustekniikasta kertova uutinen tai blogikirjoitus organisaation Intranetissä, jolloin yhteistyötä voidaan tehdä organisaation viestinnästä vastaavien henkilöiden kanssa. (Laulajainen 2012.)

## 2.2 Tietoturvakoulutuksen vaikuttavuuden arviointi

Tietoturvakoulutuksen ylläpidon ja kehittämisen kannalta on hyödyllistä arvioida ja mitata onko koulutukselle asetetut oppimistavoitteet saavutettu. Tietoturvakoulutuksen vaikuttavuutta voidaan arvioida muun muassa mittaamalla työntekijöiden tietoturvaan liittyviä asenteita, selvittämällä kuinka paljon tietoturvarikkomuksia on tapahtunut, missä määrin työntekijät noudattavat tietoturvaohjeita sekä keräämällä suoraan työntekijöiltä palautetta koulutuksen jälkeen. Vaikuttavuuden arvioiminen auttaa organisaatioita myös tunnistamaan ongelmakohtia. (Mattord & Whitman 2010, 198.)

Organisaatiot eivät juuri kiinnitä huomiota siihen tai arvioi millaista hyötyä koulutuksesta todellisuudessa on organisaatiolle. Arviointiin käytettävien mallien vähäisyys voi olla yksi syy miksi vain harvat organisaatiot tekevät koulutuksen vaikuttavuuden arviointeja. Donald Kirkpatrick on kirjoittanut koulutuksen vaikuttavuuden arvioinnin neljästä tasosta, jotka ovat reaktio, oppiminen, käyttäytyminen ja tulokset. Jako perustuu siis siihen, mitä mieltä oppijat olivat koulutuksesta, miten paljon he oppivat, muuttuiko käyttäytyminen sekä miten koulutus on vaikuttanut tavoiteltaviin tuloksiin. (Cohen 2009.)

***Ensimmäisellä tasolla*** arvioidaan miten koulutukseen osallistuneet kokivat koulutustilaisuuden. Koettiinko koulutus hyväksi: riittävästi taukoja, ajankäytön tehokkuus, miellyttävät koulutusmenetelmät, selkeä ja ammattimainen kouluttaja. ***Toisella tasolla*** arvioidaan itse op-

pimista. Tässä voidaan käyttää apuna esimerkiksi materiaaliin perustuvaa testiä, tenttiä tai näyttökoetta. Tavoitteena on arvioida, ovat osallistujat omaksuneet ja ymmärtäneet koulutuksessa käsitellyt asiat sekä hallitsevatko he periaatteet ja kokonaisuuden. ***Kolmas taso*** kattaa toiminnan eli sen, miten opittua voidaan soveltaa käytännössä eli muuttaako työntekijä toimintatapojaan koulutuksen jälkeen. ***Neljännellä tasolla*** arvioidaan vaikutusta organisaatiotasolla. Tarkastella voi esimerkiksi ovatko tietoturvaongelmat vähentyneet ja tekevätkö työntekijät vähemmän virheitä tai osaavatko he ennakoida riskejä. (VAHTI 11/2006, 39.) Vaikka Kirkpatrickin tasojen jälkeen on yritetty luoda vaihtoehtoisia malleja, on kyseinen malli säilyttänyt suosionsa vaikuttavuuden arviointimenetelmänä (Cohen 2009). Valtionhallinnon tietoturvallisuuden johtoryhmän, VAHTI, näkemyksen mukaan vaikuttavuuden arvioinnista tekee kuitenkin haasteellista juuri mahdollisuus kohdistaa arviointi monelle tasolle, eivätkä käytettävät mittarit välttämättä arvioi sitä, mitä halutaan mitata (VAHTI 11/2006, 39).

# 3 Verkko koulutuksen välineenä

Oppimiselle on kehitetty erilaisia teorioita. Oppimisteoriat voivat perustua esimerkiksi konstruktivistiseen, kognitiiviseen, behavioristiseen, humanistiseen tai sosiaaliseen oppimisnäkemykseen. Oppimisteoreettiset näkemykset luovat pohjan pedagogisille malleille, jotka ohjaavat puolestaan opetuksen toteutusta sekä oppimisprosessin etenemistä ja vaiheistamista. (Tenno 2011, 25–26.) Mutta millaista on hyvä oppiminen? Nevgin & Tirrin (2003, 29) mukaan hyvää oppimista voidaan luonnehtia ymmärtämiseen pyrkiväksi ja opiskelijan omaa ajattelua sisältäväksi merkitykselliseksi toiminnaksi. Konstruktivistinen oppimiskäsitys on syrjäyttänyt vuosikymmeniä vallinneen behavioristisen oppimiskäsitykseen perustuvan perinteisen kouluoppimisen, jossa oppiminen nähdään tiedon siirtämisenä opettajalta oppijalle (Nevgi & Tirri 2003, 29; Mäkinen 2002). Konstruktivistisen oppimiskäsityksen mukaan oppiminen ei ole erillinen tiedon siirtoon perustuva prosessi, vaan oppija rakentaa eli konstruoi tiedon itse muun muassa omien käsityksien, odotusten, tavoitteiden ja aiemman kokemuksen pohjalta (Rauste-von Wright, von Wright & Soini 2003, 53).

Verkko oppimisympäristönä ja teknologian kehityksen vaikutus opetusvälineisiin on johtanut tarpeeseen pohtia uusia oppimiskäsityksiä. Perinteisten oppimiskäsitysten rinnalle on ehdotettu uutta oppimisteoriaa: konnektivismia. Konnektivismissa on kyse tietoverkossa tapahtuvasta yhteisöllisestä oppimisesta teknologian mahdollistamilla välineillä. (Nurmi 2011, 15.) Häkkinen, Järvelä & Lehtinen (2006, 8) muistuttavat, ettei oppimista paranneta tietotekniikan mahdollistamilla työvälineillä, vaan muuttamalla oppimisprosessia. Verkon opetuskäytön tuleekin perustua oppimisteoreettisesti perusteltuihin ratkaisuihin. Tennon (2011, 27) mukaan viimeaikainen oppimisen tutkimus suosittelee käytettäväksi yhteisölliseen tiedonrakenteluun perustuvia pedagogisia malleja, sillä yhteisöllinen oppiminen johtaa yksin opiskelua useammin parempiin oppimistuloksiin.

Erilaisia mahdollisuuksia hyödyntää verkko-opetusta löytyy paljon, mutta verkko-opetuksen voi karkeasti jaotella Kallialan (2002, 20) mukaan kolmeen tyyppiin: verkon tukemaan lähiopetukseen, monimuoto-opetukseen ja itseopiskeluun verkossa. Lähiopetuksella voidaan tarkoittaa muun muassa luokkatilassa tapahtuvaa opetusta, joka voi olla esimerkiksi luento tai käytännön harjoittelutilanne (Keränen & Penttinen 2007, 19–20). Verkko-opetusta voidaan käyttää lähiopetuksen tukena monella tavoin. Esimerkiksi verkko-oppimisympäristöön voidaan viedä lähiopetuksessa käytetyt oppimateriaalit ja muita oheislukemistoja. Lisäksi opiskelijat voivat suorittaa verkossa tehtäviä, palauttaa projekti- ja kotitehtäviä verkko-oppimisympäristöön, jossa heillä on mahdollisuus myös tutustua muiden opiskelijoiden töihin ja antaa niistä palautetta. (Hämäläinen & Jaakkola 2007.)

Monimuoto-opetuksessa yhdistetään yleensä lähi- ja etäopetus, jolloin opetus voidaan siirtää osittain tai kokonaan verkko-oppimisympäristöön. Etäopetus voi olla ohjattua tai itsenäistä opiskelua, mutta myös työssä oppimista. Lähiopetuksen rooli muuttuu lähinnä tarkistuspisteiksi, tiedotus-, kysely- ja palautetilaisuuksiksi, jotka voidaan tarvittaessa toteuttaa myös videoneuvottelun avulla. Opettaja toimii opettajan roolin lisäksi verkossa ohjaajana ja tukijana, joka auttaa selvittämään ongelmatilanteita ja vastaa opiskelijoiden kysymyksiin. (Kalliala 2002, 23; Keränen & Penttinen 2007, 22.)

Itseopiskelussa on kyse itsenäisestä opiskelusta esimerkiksi verkkokurssilla. Verkkokurssi on verkossa jatkuvasti ja opiskelija voi edetä kurssilla käsiteltäviä aiheita haluamassaan järjestyksessä ja itselleen sopivina ajankohtina. Itseopiskelussa vuorovaikutus on vähäistä tai sitä ei ole lainkaan, eikä kurssilla ole välttämättä opettajaa tai tutoria. Muun muassa tästä syystä itseopiskelua varten laadittu verkkokurssi tarvitsee hyvin laaditut opasteet ja ohjeet. (Kalliala 2002, 27–28.) Itseopiskelu soveltuu hyvin opiskeluun, jossa haetaan perustiedon oppimista. Sen sijaan syvempää oppimista tavoitteleva, esimerkiksi akateeminen koulutus tai asiantuntijuuden kehittäminen, edellyttää monimuotoisempia lähestymistapoja kuten monimuoto-opetusta. (Nurmela & Suominen 2011, 32.)

Myös Keränen & Penttinen (2007, 19–25) jaottelevat Kallialan tavoin verkko-opetuksen oppimistilanteet lähiopetuksen tukemiseen ja monimuoto-opetukseen (*eng. blended learning*). Keränen & Penttinen (2007, 25) puhuvat myös lisäksi ”nopeasta” verkko-oppimisesta, jolla he tarkoittavat lyhytkestoista koulutusta. Aiemmin esimerkiksi henkilöstökoulutukset ovat olleet kestoltaan vähintään puolesta päivästä yhteen päivää, eikä tätä lyhyempiä koulutustilaisuuksia järjestelyihin kuluvien resurssien takia ole ollut järkevää toteuttaa. Verkko-opetuksen myötä koulutustilaisuuksien lisäksi on alettu järjestämään lyhytkestoisia verkossa tapahtuvia oppimistilanteita. Englanninkielisiä nimityksiä lyhytkestoisille oppimistilanteille ovat esimerkiksi *Rapid-e-Learning* ja *Just-In-Time-learning*. Käsitteille ei ole olemassa vielä suomenkielisiä vastineita. Rapid-e-Learning on pienimuotoinen verkkokurssi tai oppimisaihio, joka tuote-

taan nopeasti ja edullisesti. Just-In-Time-learning viittaa tarvelähtöiseen oppimistilanteeseen, jota varten voidaan toteuttaa esimerkiksi itseopiskeluna toteutettava verkkokurssi. Ideana on, ettei erikseen tarvitse järjestää erityistä koulutusta, vaan kurssi suoritetaan itsenäisesti sitten, kun siihen on tarve. (Keränen & Penttinen 2007, 25.)

## 3.1 Verkko-opetuksen etuja ja haasteita

Organisaation ottaessa käyttöön verkkokoulutus ja verkko-oppimisympäristö, on organisaatiolla odotuksena usein niiden toiminnalle tuoma konkreettinen hyöty. Odotukset voivat koskea niin työntekijöiden yksilöllistä oppimista kuin organisaation toiminnan parantamista ja tehostamista.

| Verkkokoulutuksen hyötyjä | Verkkokoulutuksen haasteita |
|---|---|
| • Riippumattomuus ajasta ja paikasta<br>• Itseohjautuvuus<br>• Kustannussäästöt<br>• Koulutuksen oikea-aikaisuus<br>• Tiedon ja tarpeen kohtaaminen<br>• Oppimateriaalin monipuolisuus<br>• Erilaisten oppimistyylien huomioiminen<br>• Käyttäjäseuranta ja raportointi | • Kognitiivinen ylikuormitus<br>• Heikkolaatuinen oppimisympäristö ja oppimateriaali<br>• Heikko itseohjautuvuus<br>• Päämäärätön vaeltelu<br>• Keskeyttäminen<br>• Ohjauksen tai tuutoroinnin puute<br>• Tekniset ongelmat |

Taulukko 2: Verkkokoulutuksen hyötyjä ja haasteita (Alamäki & Luukkonen 2002, 42–64)

Ehkä yleisin tunnistettu verkkokoulutuksen etu on riippumattomuus ajasta ja paikasta. Opiskelu tapahtuu oppijalle parhaiten sopivana ajankohtana eikä edellytä matkustamista opetuspaikalle kuten perinteisessä luokkaopetuksessa. (DelVecchio & Loughney 2006, 5.) Ajankäytön joustavuus antaa opiskelijalle mahdollisuuden edetä kurssilla omaan tahtiin. Oppimisesta tulee tällöin tehokkaampaa, kun opiskelija voi hypätä yli itselleen ennestään tutut asiat ja keskittyä niihin asioihin, jotka tuntuvat vaikeilta. Oppimateriaali on mahdollista jakaa myös pienempiin kokonaisuuksiin, jolloin kaikkea ei tarvitse opiskella ja yrittää sisäistää yhdellä kertaa. (Burgess & Russell 2003, 294.)

Yksi syy siihen, että organisaatioissa on herännyt kiinnostus verkkokoulutukseen, on verkko-opetuksen tuomat kustannussäästöt. Verkkokoulutuksen kustannussäästöt muodostuvat sen tehokkaasta tuottamisesta. Opiskelun riippumattomuus ajasta ja paikasta mahdollistaa sen, ettei organisaation tarvitse hankkia erillisiä koulutustiloja ja kouluttajaa, tai niitä tarvitaan

vähemmän. Tällöin matkakuluista koulutuspaikalle ja matkustukseen kuluvasta työajasta aiheutuvat kustannukset vähenevät tai niitä ei muodostu lainkaan. Sähköisessä muodossa oleva opiskelumateriaali puolestaan karsii muun muassa tulostuksesta ja jakelusta aiheutuvia materiaalikuluja. Lisäksi verkko-oppimateriaalin päivittäminen on nopeaa ja tehokasta verrattuna paperimuotoisen opiskelumateriaalin uudelleen tuottamiseen, tulostukseen ja jakeluun. (Burgess & Russell 2003, 297.) Alamäki & Luukkonen (2002, 46) muistuttavat, että verkkokoulutukseen investoinnista aiheutuneet kustannukset voivat olla aluksi suuria, jolloin koulutuskustannukset on laskettava useammalle vuodelle verrattaessa verkkokoulutuksen tuomia kustannussäästöjä perinteiseen koulutukseen nähden.

Teknologian kehittyminen, lainsäädännölliset ja yhteiskunnalliset muutokset sekä henkilöstön vaihtuvuus muovaavat organisaation toimintaympäristöä. Toimintaympäristössä tapahtuvat muutokset edellyttävät organisaatioilta huolehtimista työntekijöiden riittävästä osaamisesta ja ammattitaidosta järjestämällä tarpeen mukaista koulutusta. Oppimisen kannalta on tärkeää tarjota koulutus oikeaan aikaan. Perinteiset luokkahuonetyyppiset kurssit ja seminaarit ovat usein tiettyihin päivämääriin sidottuja, jolloin koulutusta voidaan tarjota työntekijöille liian aikaisin tai liian myöhään (Alamäki & Luukkonen 2002, 49). Liian aikaisin tarjotun koulutuksen varjopuolena on opittujen tietojen unohtaminen ennen kuin niitä tarvitaan. Liian myöhään tarjottu koulutus puolestaan voi muun muassa vaikuttaa siihen, miten työntekijät suhtautuvat koulutettavaan asiaan - omaksutaanko esimerkiksi organisaation tietoturvapolitiikka sekä politiikan edellyttämät toimintamallit ja ohjeet.

Usein organisaatioiden järjestämät koulutustilaisuudet, esimerkiksi uusien työntekijöiden yhteinen perehdytyskoulutus ja turvallisuuskoulutus, toteutetaan kerran kaksi vuodessa. Tällöin uusi työntekijä on voinut työskennellä organisaatiossa jo useamman kuukauden ennen seuraavia koulutustilaisuuksia. Verkkokoulutuksen etuna on mahdollisuus tarjota esimerkiksi uuden työntekijän perehdytys- ja turvallisuuskoulutukset heti palvelusuhteen alettua. Verkkokoulutus kaventaa myös tiedon ja tarpeen välistä kuilua, kun koulutuksia voidaan organisoida ilmenneiden tarpeiden mukaan. Tunnistettujen tarpeiden lisäksi koulutuksen sisältö on mahdollista kohdistaa tarkemmin tiettyihin asioihin ja käyttäjäryhmille (Alamäki & Luukkonen 2002, 51).

Digitaalisessa muodossa oleva oppimateriaali mahdollistavaa monipuolisen tavan rakentaa verkko-oppimisympäristö ja tapoja esittää siellä tietoa. Opetuksessa voidaan käyttää verkkokirjojen lisäksi ääntä, videoita sekä erilaisia pelejä ja simulaatioita. Materiaalin tuottamisen monipuolisuus mahdollistaa lisäksi erilaisten oppimistyylien huomioimisen. Oppimistyyli kuvaa yksilölle ominaista tapaa omaksua, käsitellä ja muistaa tietoa. (Felder & Henriques 1995, 21). Erilaisia oppijoita voidaan kuvata esimerkiksi aistihavaintoihin perustuen auditiivisiksi, visuaalisiksi, kinesteettisiksi ja taktiilisiksi oppijoiksi. Auditiivinen oppija oppii parhaiten kuuntele-

malla ja visuaalinen näkemällä. Kinesteettisen oppijan oppiminen perustuu sen sijaan tuntohavaintoon ja taktiilisen käsillä tekemiseen: esimerkiksi piirtämiseen, kirjoittamiseen ja mallien rakentamiseen. (Koponen ym. 2011, 9-10.)

Verkko-oppimisympäristön luomiseen käytettävissä ohjelmissa on lähes poikkeuksetta mukana raportointityökalu. Raportointityökalu on hyvä apuväline muun muassa esimiehille, koulutusvastaaville ja henkilöstöhallinnolle, sillä työkalun avulla pystytään seuraamaan esimerkiksi rekisteröityneiden käyttäjien määrää, kurssisuorituksia ja -arviointeja. Raportointityökalun avulla voidaan lisäksi koota erilaisia tilastoja: esimerkiksi johdolle voidaan esitellä, kuinka moni työntekijä on suorittanut tietoturvakoulutuksen ja millaisia arvosanoja kurssin suorittaneet ovat saaneet. (Alamäki & Luukkonen 2002, 50.)

Monien hyötyjen lisäksi liittyy verkkokoulutukseen myös haasteita. Eräs merkittävä haaste on kognitiivinen ylikuormitus. Termi ”*kognitio*” tarkoittaa käsitteenä muun muassa yksilön tiedonhankintaan ja tietämiseen liittyviä toimintoja kuten muistia, havaitsemista, päättelyä ja tarkkaavaisuutta (Kajannes & Kirstinä 2000, 9). Pälli (2003, 46) kuvailee kognitiota informaation prosessoinniksi, joka voidaan karkeasti jakaa kahteen näkemykseen: yksilön päänsisäiseen toimintaan sekä yhteisölliseen ja toiminnalliseen informaation prosessointiin.

Työmuistiin tallentuu informaatio, jota ihminen tarvitsee sen hetkisessä tilanteessa tai toiminnassa. Eräiden tutkimusten mukaan ihminen kykenee pitämään työmuistissaan kerrallaan viidestä seitsemään asiaa. Toisten tutkimusten mukaan määrä olisi kolmesta yhdeksään. (Alamäki & Luukkonen 2002, 56.) Työmuistin ylikuormittaminen vaikeuttaa oppimista ja se onkin Alamäen & Luukkosen (2002, 57) mukaan edelleen haittaava tekijä useissa verkko-oppimisratkaisuissa. Ylikuormitusta aiheuttavat huonosti laadittu verkko-oppimisympäristö ja opiskelumateriaali, jotka edellyttävät opiskelijalta useiden asioiden muistamista kerralla. Verkko-oppimisympäristöjen rakentamiseen tarkoitettujen ohjelmistoalustojen runsas saatavuus ja uusien ohjelmistoalustojen nopea kehitys sekä tarjoaminen markkinoille tekevät tarjonnasta laadullisesti vaihtelevaa. (Alamäki & Luukkonen 2002, 64). Ohjelmistoalusta ja sen käyttöliittymä vaikuttavat pitkälti siihen millaisia verkko-oppimisympäristöjä sillä pystytään rakentamaan. Verkko-oppimisympäristöjen laadulliseen arviointiin löytyy useita laatukriteerejä ja tarkistuslistoja. Laatua voidaan arvioida esimerkiksi tuotannollisten, käytettävyyden, esteettömyyden sekä pedagogisten laatukriteerien näkökulmista. Keskeistä on valita arvioinnin kohteen kannalta merkitykselliset kriteerikokonaisuudet, sillä kaikki kriteerit eivät sovellu kaikentyyppisten verkko-oppimisympäristöjen sekä niiden sisältämien oppimateriaalien arvioimiseen. (Hyötyniemi ym. 2005, 11). Opiskelijan näkökulmasta verkko-oppimisympäristöä ja oppimateriaalia voidaan arvioida esimerkiksi käytettävyyden ja pedagogisten ominaisuuksien osalta.

Käytettävyydellä tarkoitetaan opiskelijan kokemusta verkko-oppimisympäristön käytön helppoudesta ja sujuvuudesta. Laadullisesti heikko verkko-oppimisympäristö on käytettävyydeltään sekava, jossa opiskelijalla kuluu aikaa muun muassa oppimisympäristön toimintojen hahmottamiseen ja opetteluun. Käytettävyyttä heikentävät myös toimimattomat linkit, virheilmoitukset sekä puutteellinen ohjeistus virhetilanteissa. (Hyötyniemi ym. 2005, 17.) Pedagogisesti huonosti tuotettu verkko-oppimateriaali ei puolestaan tue opetusta ja oppimista, eikä siten tuo opiskelulle lisäarvoa. Verkko-oppimateriaali ei saisi aiheuttaa tiedon ylikuormitusta eli opiskelija voi keskittyä yksityiskohtien sijaan kokonaisuuksiin. Laadukas verkko-oppimateriaali on muun muassa aktivoivaa, kuvaa oppimistavoitteet ja huomioi erilaiset oppimistyylit, opiskelijoiden tason sekä yksilölliset erot. (Saarinen 2005, 62–69.) Erityisesti itseopiskelukurssilla hyvin laaditun verkko-oppimisympäristön ja -materiaalin merkitys korostuu, sillä se edesauttaa opiskelija motivaatiota opiskella.

Lähtökohtaisesti verkko oppimisympäristönä tarjoaa monia mahdollisuuksia oppimiselle, mutta oppijalla itsellään on vastuu oman oppimisensa ohjaamisesta ja hallitsemisesta (Niemi 2001). Itseohjautuvuus tarkoittaa yksilön kykyä ohjata omaa oppimisprosessiaan. Vahvasti itseohjautuvat henkilöt ovat oma-aloitteisia ja toimivat aktiivisesti itselleen asettamiensa oppimistavoitteiden saavuttamiseksi. Sen sijaan heikon itseohjautuvuuden omaavilta henkilöiltä oma-aloitteisuus ja aktiivisuus puuttuvat. Heillä ei ole omakohtaista tietoa oppimistavoitteistaan tai tunnetta siitä, miten tarvittava tieto ja osaaminen voitaisiin hankkia. Heikko itseohjautuvuus voi johtua myös heikoista opiskelu- ja oppimistekniikoista tai torjuvasta asenteesta uutta tietoa kohtaan. (Alamäki & Luukkonen 2002, 61–62.)

Verkko-oppimateriaali, jonka rakenteeseen ja pedagogiseen etenemiseen ei ole kiinnitetty huomioita, voi johtaa opiskelijan päämäärättömään vaelteluun kurssilla. Tällöin opiskelija navigoi kurssilla umpimähkään etenemättä loogisesti aiheesta toiseen. (Alamäki & Luukkonen 2002, 58.) Päämäärätön vaeltelu kurssilla voi heikentää opiskelijan opiskelumotivaatiota. Lisäksi se voi herättää tuntemuksia, joissa opiskelija kokee, ettei saa opiskelusta otetta ja oppiminen vaikeutuu. Nämä voivat osaltaan johtaa kurssin keskeyttämiseen. Verkkokurssin keskeyttämiseen voi Nevgin ja Tirrin (2003, 163) mukaan vaikuttaa myös opiskelijan kokemat vaikeudet, jotka voivat liittyä ohjeiden tai palautteen puutteeseen, kurssin liian vaikeaan tasoon, teknisiin asioihin kuten tietotekniikkaan tai verkkoyhteyksiin. Keskeyttämisen syy voi toisaalta liittyä opiskelijan henkilökohtaisiin asioihin esimerkiksi elämäntilanteeseen, aikatauluongelmiin, motivaation puutteeseen tai oppimisvaikeuksiin.

Opetuksen siirtyessä verkkoon, ajatellaan, ettei opettajaa tai ohjausta enää tarvita (Nurmela & Suominen 2011, 31). Verkko-opiskelu voi kuitenkin olla opiskelijalle ennalta tuntematon opiskelumuoto (Kiviniemi 2000, 83). Alamäki & Luukkonen (2002, 62–63) tuovat esille ongelman, joka liittyy opiskelijoiden sisäistämään tapaan opiskella opettajajohtoisesti. Opiskelijat

ovat tottuneet siihen, että opettaja kertoo mitä tehdään ja opiskelijat tekevät opettajan antamia tehtäviä. Opiskelijat eivät siis ole tottuneet itsenäiseen ja omatoimiseen opiskeluun, joka edellyttää opiskelijalta myös itseohjautuvuutta. Ohjauksella opiskelijoita voidaan tukea itsenäiseen opiskeluun ja oppimiseen. Ohjauksella ja tuutoroinnilla voidaan vähentää opiskelijoiden verkkokurssin keskeyttämistä, joka on verkkokoulutukseen liittyvä yleinen ongelma (Nurmela & Suominen 2011, 31).

Ohjauksen tarve voi liittyä joko kurssin suorittamiseen tai teknisiin asioihin. Verkkokurssin tulisikin aina sisältää opiskeluohjeen ja kuvauksen oppimateriaalin sisällön rakenteesta. Opiskeluohjeessa opiskelijalle voidaan selittää esimerkiksi opiskelun eteneminen, kurssin arviointiin ja tehtävien palautukseen liittyviä asioita, aikataulu, palautteen saaminen sekä yhteystiedot mahdollisissa ongelmatilanteissa. Teknistä ohjausta voidaan tarvita puolestaan esimerkiksi rekisteröitymisen, ohjelma- ja selainlaajennusten asennuksien sekä asetuksien kanssa. (Alamäki & Luukkonen 2002, 63.) Ohjauksen puuttuminen voi osaltaan johtaa opiskelijan päämärättömään vaelteluun kurssilla, opiskelumotivaation laskuun tai kurssin keskeyttämiseen.

Verkkokoulutukseen liittyy myös oleellisesti teknisiä haasteita, joita voivat kohdata sekä verkkokurssin toteuttajat että opiskelijat. Eräs tyypillinen tekninen ongelma liittyy käyttäjän vaikeuksiin luoda kurssille kirjautumista varten käyttäjätunnus ja salasana (Alamäki & Luukkonen 2002, 64). Syynä voi olla muun muassa puutteelliset ohjeet, verkko-oppimisympäristön palveluntarjoajan päässä ilmenevä ongelma tai sähköpostiin saapuvan vahvistusviestin ohjautuminen käyttäjän roskapostisuodattimeen. Unohdetun käyttäjätunnuksen ja salasanan palauttamisessa voi niin ikään ilmetä vastaavanlaisia ongelmia. Alamäen & Luukkosen (2002, 64) mukaan teknisiä ongelmia voi esiintyä lisäksi verkko-oppimateriaalin sisällön ja mediaelementtien kuten videoiden, äänen ja kuvan toimimattomuutena. Esimerkiksi videoilla voi kestää latautua tai katsoessa video pätkii kohtuuttomasti, äänitiedostot tai kuvat eivät lataudu. Tällaiset ongelmat liittyvät usein siihen, että käyttäjältä puuttuu jokin esittämisen edellyttämä selainlaajennus. Muita teknisiä ongelmia voi ilmetä esimerkiksi mahdollisesti tarvittavien ohjelma-ajureiden ja selainlaajennusten asetusten, ruudun resoluution, verkkoyhteyksien kanssa (Alamäki & Luukkonen 2002, 64).

## 3.2 2010-luvun verkko-oppimisympäristöt

Internetin hyödyntäminen opetuksessa rajoittui sähköpostin ja keskustelufoorumeiden käyttöön aina 1990-luvulle asti, sillä suurien tietomäärien lähettäminen Internetin välityksellä oli vaikeaa johtuen tuolloin käytettävissä olevan tekniikan, esimerkiksi kaistanleveyden, rajoitteista ja lähettämisen kalleudesta. World Wide Web –hypertekstijärjestelmän eli WWW:n kehittäminen mahdollisti suurien sisältöjen, erityisesti tekstin ja grafiikan, edullisen luomisen,

tallentamisen, hakemisen ja lähettämisen Internetissä. Järjestelmän toiminta perustuu siihen, että tieto hajotetaan ensin pieniksi paketeiksi ja kootaan uudelleen määränpäässä. WWW:tä käytetään usein erheellisesti Internetin synonyymina, vaikka kyseessä on Internetin palvelumuoto. (Lee & McLoughlin 2011, 23.)

1990-luvulla WWW:n myötä verkkoa alettiin hyödyntää opetuksessa. Opettajat rakensivat itse www-sivuja ja verkkokursseja HTML-kielellä (Hypertext Markup Language). Pian markkinoille ilmestyi kaupallisia tuotteita, joilla pystyttiin rakentamaan verkko-oppimisympäristöjä sekä liittämään niihin oppimateriaalien lisäksi tehtäviä, testejä ja keskustelualueita - E-oppiminen käsitteenä alkoi kehittyä. (Lee & McLoughlin 2011, 23.) E-oppiminen (*eng. E-learning*) tai verkko-oppiminen viittaa verkossa tapahtuvaan, tietoverkkoja, teknologiaa ja digitaalisia tietokantoja hyödyntävään opiskeluun (Frank & Liebowitz 2011, 51). Verkko-oppimisympäristöt ovat oleellinen osa verkko-opetusta, sillä ne tarjoavat työvälineitä verkko-opetuksen järjestämiselle. Kaupallisten tuotteiden lisäksi saatavilla on myös ilmaisia avoimeen lähdekoodiin perustuvia tuotteita (Mäkitalo & Wallinheimo 2012, 22).

Verkko-oppimisympäristöjen perusominaisuuksia ovat verkkokurssien luomiseen sekä oppimisympäristön ylläpitoon ja hallintaan liittyvät toiminnot. Verkko-oppimisympäristöön voidaan luoda verkkokurssi oppimateriaaleineen sekä sisällyttää testejä, joilla voidaan arvioida opiskelijoiden osaamista. Ylläpitoon ja hallintaan liittyviä ominaisuuksia ovat muun muassa käyttäjätunnusten- ja profiilien hallinta, aineiston ja tiedostojen hallinta, kurssin hallinta sekä varmuuskopiointi. Verkko-oppimisympäristöissä voidaan antaa opiskelijoille palautetta ja arviointeja suoritetuista tehtävistä ja testeistä. Lisäksi ominaisuuksiin voi sisältyä vielä viesti- ja kalenteritoimintoja verkko-oppimisympäristöstä riippuen. (Keränen & Penttinen 2007, 31.)

Verkkokurssi on verkko-oppimisympäristöön rakennettu kurssi, jolle on määritelty tavoite, sisältö, laajuus ja arviointi. Verkkokurssi muodostuu Keräsen & Penttisen (2007, 3) mukaan verkko-oppimateriaalista, tehtävistä sekä vuorovaikutuksesta opettajan ja opiskelijoiden välillä. (Keränen & Penttinen 2007, 2-3.) Verkkokurssin toteutus voi vaihdella opiskelijoiden välisestä aktiivisesta ja vuorovaikutteisesta osallistumisesta opiskelijan itsenäiseen opiskeluun. Opettajan rooli ja työmäärä verkkokurssilla riippuu verkkokurssin toteutustavasta. (Nevgi & Tirri 2003, 23.)

Verkkokurssilla käytettävä, digitaalisessa muodossa oleva oppimateriaali, mahdollistaa erilaisten tapojen käytön materiaalin esittämiseen verkkokurssilla. Kurssilla voidaan nimittäin käyttää esimerkiksi verkkokirjaa, muuta tekstimuodossa olevaa materiaalia, ääntä, liikkuvaa kuvaa tai näiden yhdistelmiä eli audiovisuaalista materiaalia, pelejä ja simulaatioita. (Kalliala 2002, 14.) Nurmelan ja Suomisen (2011, 67) mukaan on haaste ymmärtää, etteivät perinteiset oppikirjan kaltaiset materiaalit toimi verkossa. Haasteellisuudesta kertoo se, että verkko-

oppimismateriaalit ovat vieläkin useimmiten oppikirjamaisia, ja joista puuttuu erilaisten mediaelementtien käyttö ja vuorovaikutteisuus.

Web 2.0 kuvaa käsitteenä niin sanotusti Internetin toista tulemista. Web 2.0 ei ole käsitteenä uusi, sillä Tim O'Reilly loi termin vuonna 2005 markkinointitarkoituksiin kuvaamaan Internetin uusia menestyksellisiä toimintatapoja ja -malleja (Hintikka 2007, 6). Web 2.0 kuvaa myös osaltaan hyvin www-ympäristön muuttumista. Aiemmin informaatiota pelkästään vietiin www-ympäristöön, mutta nykyisin se toimii ympäristönä, jossa tietoa luodaan, jaetaan ja uudelleen muokataan. Painopiste on siirtynyt vuorovaikutteiseen viestintään ja yhteisölliseen sisällöntuotantoon. (Downes 2005; Nurmela & Suominen 2011, 93.)

Web 2.0 myötä kehittyneet uudet välineet ja palvelut ovat rikastuttaneet verkko-opetusta ja oppimista sekä tehneet verkko-oppimisympäristöistä avoimia. Verkko-oppimisympäristöjen luomiseen käytettävien oppimisalustojen, esimerkiksi Moodle, Fronter ja Optima, roolit suljettuina oppimisympäristöinä ovat muuttuneet. Esimerkiksi siinä missä opiskelu tapahtui oppimisalustalle rakennetussa verkko-oppimisympäristössä, kuten verkkokurssilla, käytetään oppimisalustaa nykyisin porttina muihin oppimisympäristöihin sekä opetusta ja oppimista tukeviin välineisiin. Oppimisalustojen rooli opetuksessa on nykyisin pääasiassa hallinnollista: opetussuunnitelmat, oppimistehtävät, ohjeet, tiedotukset, tehtäväpalautukset, oppimisen edistymisen seuranta. (Aarreniemi-Jokipelto 2011, 30.)

Taulukkoon 3 on koottu esimerkkejä apuvälineistä, joita voidaan käyttää verkko-opetuksen ja oppimisen tukemiseen.

| *Väline:* | *Mahdollinen käyttötarkoitus:* |
|---|---|
| **Adobe Connect Pro** | • Luennot ja niiden tallenteet<br>• Tapaamiset (pienryhmät, ohjauskeskustelut, tehtävien purut) |
| **Skype** | • Internet-puhelut<br>• Pikaviestintä |
| **Blogger, WordPress** | • Oppimis- ja reflektiopäiväkirjat |
| **Doodle** | • Tapaamisten sopiminen |
| **Delicious** | • Verkossa oleva kirjallisuus<br>• Oppimistehtäviin liittyvä materiaali<br>• Opiskelijoiden löytämät kiinnostavat sivut |

| | |
|---|---|
| **Second Life** | • Opetustuokiot<br>• Ohjaus<br>• Pienryhmien keskustelu ja vuorovaikutus |
| **Facebook** | • Keskustelu ja vuorovaikutus<br>• Pikaviestintä |
| **Youtube, Vimeo** | • Videotallennustila ja videomateriaalien jakaminen |
| **Voxopop** | • Äänitallenteiden tekeminen |
| **Hot Potatoes** | • Monivalinta-, aukko-, sanaristikko- ja kyselytehtävien toteuttaminen |
| **Google Apps -sovellukset** | • Mm. sähköposti, kalenteri, yhteiskäyttöinen dokumenttiympäristö |
| **SnagIt** | • Ohjelma ruutukaappausten tekemiseen esim. ohjeita varten |

Taulukko 3: Verkko-opetusta ja opiskelua tukevia välineitä (Mäkitalo & Wallinheimo 2012, 25-29; Aarreniemi-Jokipelto 2011, 30-31)

### 3.3 Verkkokoulutuksen suunnittelu ja toteutus

Koulutuksen suunnittelun ja toteuttamisen jakaminen vaiheisiin selkeyttää ja tehostaa sen tuottamista (Manninen & Matikainen 2001). Verkko-opetusta käsittelevää kirjallisuutta tarkastellessa voidaan havaita, että vaihtoehtoja vaiheistaa verkkokoulutuksen tuottaminen, on yhtä monta kuin kirjoittajia. Lisäksi se, millaisia vaiheita tuottamiseen liittyy, riippuu organisaation lähtökohdista. Esimerkiksi organisaatiolla voi olla jo valmiiksi käytössään jokin verkko-oppimisalustan ohjelmisto, jolloin ohjelmiston hankintaan ja käyttöönottoon liittyvät vaiheet eivät ole olennaisia.

Vaikka tapoja jakaa tuotantoprosessi eri vaiheisiin on useita, on malleille tunnistettavissa yhteisiä piirteitä. Selkeästi tunnistettavissa on jako suunnittelu- ja toteutusvaiheisiin. Nämä vaiheet pitävät puolestaan sisällään useita pienempiä vaiheita, joita ovat muun muassa kokonaiskonseptin suunnittelu, käsikirjoitus, oppimateriaalin tuottaminen, toteutuksen rakentaminen, testaus ja käytettävyyden arviointi ja käyttöönotto.

### 3.3.1 Suunnitteluvaihe

Verkkokoulutuksen suunnittelu lähtee liikkeelle laatimalla verkkokoulutukselle kokonaiskonsepti, joka rakentuu teknisistä ja sisällöllisistä asioista. Teknisten asioiden osalta tulee pohtia toiminnallisia ominaisuuksia kuten koulutukseen käytettävää kanavaa ja tuotantoteknologiaa. Määritellä tulisi käytetäänkö kanavana Internetiä, organisaation Intranetiä, Ekstranetiä tai erityistä verkko-oppimisalustaa ja toteutetaanko se esimerkiksi HTML:llä, Flash:llä, Java:lla tai jollakin muulla teknologialla. Sisällönsuunnittelun osalta keskeisessä roolissa ovat muun muassa oppimistavoitteet, kohderyhmä, opiskelumuoto, opiskeluun käytettävissä oleva aika sekä asiasisältöjen laajuus ja syvyys. (Alamäki & Luukkonen 2002, 188–189.)

Jotta sisällönsuunnittelu olisi mahdollista, tulee verkkokoulutukselle asettaa oppimistavoitteet. Mitä opiskelijan halutaan oppivan? Lisäksi tulee määrittää menetelmät, joilla oppimistavoitteet ovat saavutettavissa ja arvioitavissa. Kohderyhmän tarkastelu on tärkeää, jotta tiedetään millaiselle ryhmälle koulutusta ollaan rakentamassa. Tarkasteltavia asioita voivat olla muun muassa kohderyhmän taustat ja aiempi tietämys aiheesta eli onko koulutettavana ryhmä asiantuntijoita vai ryhmä, jolle aihe ei ole ennestään tuttu. Muita huomiota kaipaavia kohteita ovat kohderyhmän motivaatio ja suhtautuminen verkkokoulutukseen sekä tekninen osaaminen. Teknisen osaamisen taso vaikuttaa esimerkiksi siihen, millaisia toimintoja verkko-oppimisympäristöön kannattaa rakentaa. (Kanerva, Lehtinen, Löfström, Nevgi & Tuuttila 2006, 36–38.)

Sisällönsuunnitteluun vaikuttaa oleellisesti valittu opiskelumuoto. Onko kyseessä itseopiskelu, monimuoto-opiskelu tai työryhmätyöskentely? Opiskelumuoto vaikuttaa siihen, miten laajaa ja syvälle aiheeseen menevää verkko-oppimateriaalista kannattaa tehdä ja millaisia pedagogisia ratkaisuja käyttää. Asiasisällön laajuuteen ja syvyyteen vaikuttaa myös se, kuinka paljon aikaa opiskelijoille on resursoitu verkkokoulutuksen suorittamiseen. Vaikka aikaa olisi, ei verkko-oppimateriaalista kannata tehdä liian laajaa muun muassa kognitiivisen ylikuormituksen takia.

### 3.3.2 Toteutusvaihe

Kun verkkokoulutukselle on laadittu kokonaiskonsepti, siirrytään suunnittelemaan verkko-oppimisympäristön rakenne. Tässä kohtaa pohditaan, miten verkko-oppimisympäristö rakennetaan käytännössä, jotta se tukee sekä kurssikokonaisuuden toteutumista että koulutukselle asetettujen oppimistavoitteiden saavuttamista. Oppimisympäristön rakenne kannattaa suunnitella huolella, sillä se ohjaa opiskelijan oppimisprosessia (Kanerva, Lehtinen, Löfström, Nevgi & Tuuttila 2006, 48). Rakenteen suunnittelussa voidaan käyttää esimerkiksi Mind map -tekniikkaa, vuokaaviota tai rakennepuuta. Mind map -tekniikka sopii asiakokonaisuuksien ja

niiden välisten suhteiden hahmottamiseen. Vuokaaviota ja rakennepuuta voidaan käyttää verkko-oppimisympäristöön tulevien elementtien sijoituspaikkojen hahmottamiseen. Elementtejä ovat esimerkiksi oppimateriaalit (tekstit, videot, kuvat, äänet), oppimistehtävät ja niiden palautus, keskustelualueet, ohjeistukset ja osaamiseen arviointiin liittyvät tehtävät kuten testit ja tentit. Lisäksi verkko-oppimisympäristön rakennetta ja koulutuksen etenemistä voidaan selkeyttää muun muassa järjestelemällä ja luokittelemalla rakenne numeroilla tai aakkosilla, vaiheistamalla työskentelyprosessi opintomoduuleihin tai kalenteriviikkoihin. Myös jakaminen opiskelumuodon ja työryhmien perusteella on mahdollista. (Mänty & Nissinen 2005, 40.) Verkko-oppimisympäristön rakenteen suunnitteluvaiheesta näkee käytettävän nimityksiä käsikirjoitus, rakennesuunnitelma ja sisältösuunnitelma.

Oppimisympäristön rakenteen suunnittelun jälkeen on aika tuottaa oppimateriaali. Alamäki & Luukkonen (2002, 196) korostavat, ettei oppimateriaalin työstämistä saa aloittaa ennen kuin verkkokurssin sisällöstä on tehty suunnitelma. Mikäli materiaalista halutaan tehdä laadullisesti hyvä, on siihen varattava riittävästi aikaa. Lisäksi tulee huomioida, että verkko-oppimateriaalin tekeminen eroaa jonkin verran perinteisen oppimateriaalin tuottamisesta (Mänty & Nissinen 2005, 45). Valmista materiaalia on varsinkin Internetissä runsaasti saatavilla ja sitä kannattaa hyödyntää mahdollisuuksien mukaan, mutta tällöin on muistettava tekijänoikeuksiin liittyvät kysymykset. (Nurmela & Suominen 2011, 85).

Verkko-oppimismateriaalin tuottamisen rinnalla rakentuu itse verkko-oppimisympäristö. Kun oppimisympäristö on saanut sisältönsä ja muotonsa, tulee ympäristö testata ennen pilotointia ja varsinaista käyttöönottoa. Alamäki & Luukkonen (2002, 213) jakavat testauksen kolmeen näkökulmaan: sisällöllinen testaus, käytettävyyden testaus ja tietotekninen testaus. Sisällöntestauksessa yritetään karsia materiaalin sisällöllisiä asiavirheitä. Pienetkin virheet esimerkiksi tekstissä voivat muuttaa asian merkityksen kokonaan. Käytettävyyden testauksella pyritään löytämään mahdollisia toiminnallisia virheitä, joita voivat olla esimerkiksi epäloogiset siirtymiset ja navigoinnin hitaus, toimimattomat linkit, latautumattomat kuvat, äänitiedostot ja videot. Tietoteknisessä testauksessa tehdään käyttösimulaatiota, jolla yritetään löytää tietotekniikasta johtuvia virheitä esimerkiksi sovelluksen kaatumista tai jumiutumista. Tietotekniseen testaukseen kuuluvat myös tarvittavien selainlaajennusten ja ajureiden asennukset ja käyttöönottotestaus.

Hosio & Rissanen (2004, 6) sekä Saarinen ym. (2002, 117–118) puolestaan käsittelevät käytettävyyden testausta ja arviointia laajemmasta näkökulmasta. Käytettävyyttä voidaan arvioida erilaisilla arviointimenetelmillä teknisten asioiden lisäksi myös pedagogisesta näkökulmasta. Esimerkkejä arviointimenetelmistä ovat heuristinen arviointi, kognitiivinen läpikävely, ominaisuuksien katsaus ja käyttäjätestaus. Heuristista arviointia yhdessä käyttäjätestauksen

kanssa pidetään tehokkaimpina tapoina löytää virheet. Heuristinen arviointi perustuu Jakob Nielsenin (2005) kymmeneen heuristiseen sääntöön, jotka ovat:

1. Yksinkertaisen ja luonnollisen dialogin käyttö
   - Informaatio ei sisällä epäolennaisia asioita tai ole vaikeasti tulkittavaa

2. Käyttäjälähtöisen kielen käyttö
   - Informaatio ilmaistaan käyttäjälle tutuin sanoin, lausein ja merkityksin

3. Muistikuorman minimoiminen
   - Käyttäjän ei tarvitse muistaa monimutkaisia tapahtumaketjuja

4. Yhdenmukaisuus
   - Sanat, tilanteet ja toiminnot tarkoittavat samoja asioita kaikkialla verkko-oppimisympäristössä

5. Järjestelmän tilan näkyvyys
   - Järjestelmä antaa käyttäjälle palautetta järjestelmän tilasta kohtuullisessa

6. Selkeät poistumistiet
   - Käyttäjän valitessa väärän toiminnon poistuminen on tehty helpoksi

7. Käytön joustavuus ja tehokkuus
   - Järjestelmän käyttö sopii sekä vasta-alkajille että kokeneemmille käyttäjille

8. Virhetilanteiden välttäminen
   - Ympäristö suunnitellaan niin hyvin, että virhetilanteilta vältytään

9. Virheilmoituksien selkeys
   - Virhetilanteen tapahtuessa virheilmoituksessa kerrotaan selkeästi mistä virhe johtuu

10. Avun antaminen ja dokumentointi
    - Järjestelmässä on selkeät ja riittävät ohjeet käyttäjille, jotka tarvitsevat apua

Testausvaiheen ja sen yhteydessä tunnistettujen kehitystarpeiden korjausten jälkeen verkko-koulutus on valmis julkaistavaksi.

## 3.4 Verkkokoulutuksen käyttö valtionhallinnossa

Verkkokoulutuksen käyttöä valtiohallinnossa selvitettiin vuonna 2001, kun valtiovarainministeriö antoi HAUS kehittämiskeskus Oy:lle toimeksiannon selvittää valtiohallinnon organisaatioiden kokemuksia ja suunnitelmia verkkokoulutuksesta henkilöstön kouluttamisen välineenä. Tavoitteena oli kartoittaa verkko-oppimisen nykytilanne valtionhallinnossa sekä kuvata kehittämistarpeet. Nykytilanteen selvityksellä haettiin muun muassa valtiohallinnon organisaatioiden tavoitteita hyödyntää verkkokoulutusta, selvittää millaisia kehittämishankkeita organisaatioille on, millaista yhteistyötä organisaatioiden välillä on tehty ja onko verkkokoulutushankkeiden vaikuttavuutta arvioitu tai tarkoitus arvioida. Kehittämistarpeiden kuvaamisen tavoitteena oli kartoittaa verkkokoulutuksen parhaimmat sovellusalueet, keskeisimmät ongelmat sekä kehittämishaasteet. (Hanelius, Kanerva & Merikanto 2002, 5-6.) Selvitys valmistui keväällä 2002, jonka jälkeen vastaavanlaista selvitystyötä ei ole tehty.

Selvityksessä lähetettiin 160 organisaatiolle verkko-oppimista kartoittava kysely. Kyselyyn vastasi 69 organisaatiota (vastausprosentti 40 %). Selvityksestä käy ilmi, että verkko-opetusta oli vielä selvityksen aikoihin valtionhallinnossa toteutettu vain vähän, sillä 16 organisaatiota 69:stä kertoi hyödyntävän henkilöstön kouluttamiseen verkkoa. Osalla organisaatioista käytössä oli yksi tai useampi oppimisalusta, joiden ylläpidosta organisaatiot huolehtivat suurimmaksi osaksi itse. Kaikki verkkokoulutusta toteuttaneet organisaatiot kertoivat pitävänsä verkko-oppimiseen käytettävää aineistoa joko organisaation lähiverkossa Intranetissä tai Internetissä. Oppimateriaalin esitysmuotona käytettiin enimmäkseen HTML (Hypertext Markup Language) muodossa olevaa tekstiä sekä tekstiä liitetiedostoina. Kuvia, ääntä ja videoita käytettiin esitysmuotona hieman vähemmän. (Hanelius, Kanerva & Merikanto 2002, 8-10.)

Kyselyssä pyydettiin organisaatioita arvioimaan kuinka paljon henkilöstö kaipaa tukea verkko-oppimiseen. Vastauksista ilmenee varsin mielenkiintoinen seikka: organisaatiot, joissa oli toteutettu verkkokoulutusta, enemmistö arvioi henkilöstön opastustarpeen olevan jatkuvaa, kun taas organisaatioissa, joissa verkkokoulutusta ei ollut toteutettu, opastustarve arvioitiin vähäisemmäksi. Ensisijaisesti opastusta arvioitiin tarvitsevan teknisiin asioihin, mutta myös opiskelutapoihin kuten ajankäyttöön. (Hanelius, Kanerva & Merikanto 2002, 10.)

Kyselyyn vastanneista lähes kaikki organisaatiot pitivät verkkokoulutuksen parhaana puolena riippumattomuutta ajasta ja paikasta. Positiivisena pidettiin myös koulutuksen opiskelijakohtaista räätälöitävyyttä, monimuotoista vuorovaikutusta sekä soveltuvuutta tiedonhankintataitojen parantamiseen. Ongelmallisena nähtiin puolestaan verkkokoulutuksen organisoinnin resursointi, opiskeluun käytettävän ajan takaaminen opiskelijalle, tietoturvakysymykset ja riittävän ohjauksen varmistaminen. Tulevaisuutta ajatellen verkkokoulutuksen kehittämisen tueksi organisaatiot kertoivat kaipaavansa muun muassa muiden organisaatioiden kokemuksia

verkkokoulutuksesta, tietoa tekniikasta ja käytettävissä olevista vaihtoehdoista, sisällön tuottamisesta sekä verkkopedagogiikasta. (Hanelius, Kanerva & Merikanto 2002, 11–12.)

# 4 Tietoturvakoulutuksen järjestäminen valtionhallinnon organisaatioissa

Lainsäädäntö asettaa lähtökohdat valtionhallinnon organisaatioiden tietoturvallisuudelle ja tietoturvatoiminnalle. Suomessa ei ole yhtenäistä tietoturvalainsäädäntöä, vaan tietoturvatoimintaa ja -velvoitteita löytyy useista laeista ja asetuksista. Lakien ja asetuksien lisäksi erilaiset ohjeet ja määräykset voivat asettaa vaatimuksia tietoturvallisuudelle. (VAHTI 6/2003, 19–20.) Viranomaisten tietoturvatoimintaan ja -velvoitteisiin liittyviä lakeja ja asetuksia ovat esimerkiksi: Laki viranomaisen toiminnan julkisuudesta (621/1999), Asetus tietoturvallisuudesta valtionhallinnossa (681/2010), Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004), Henkilötietolaki (523/1999), Valmiuslaki (1080/1991) sekä viranomaisten toimialakohtainen erityislainsäädäntö.

Lainsäädännöstä voidaan löytää viitteitä viranomaisten velvollisuudesta järjestää tietoturvakoulutusta. Esimerkiksi laki viranomaisen toiminnan julkisuudesta, niin kutsuttu julkisuuslaki, edellyttää viranomaisilta hyvää tiedonhallintatapaa. Hyvään tiedonhallintatapaan kuuluu muun muassa velvollisuus huolehtia siitä, että viranomaisen palveluksessa olevilla henkilöillä ”*…on tarvittava tieto käsiteltävien asiakirjojen julkisuudesta sekä tietojen antamisessa ja käsittelyssä sekä niiden ja asiakirjojen ja tietojärjestelmien suojaamisessa noudatettavista menettelyistä, tietoturvallisuusjärjestelyistä ja tehtävänjaosta*…”. (Laki viranomaisen toiminnan julkisuudesta 621/1999, 18 §.)

Tietoturvakoulutusta sivutaan myös asetuksessa tietoturvallisuudesta valtionhallinnossa eli tietoturvallisuusasetuksessa. Lokakuussa 2010 voimaan tullut asetus toi mukanaan tietoturvatasot, jotka asettavat organisaation hallinnolle ja tietojenkäsittely-ympäristölle erityisiä tietoturvavaatimuksia. Tasoja on yhteensä kolme: perustaso, korotettu taso ja korkea taso. Valtionhallinnon organisaatioilta edellytetään vähintään tietoturvallisuuden perustason täyttämistä kolmen vuoden kuluessa asetuksen voimaantulosta (VAHTI 2/2010, 7). Tietoturvallisuuden perustason vaatimuksiin kuuluu henkilöstön sekä muiden organisaation palveluksessa toimivien henkilöiden ohjeistus ja koulutus: ”*…henkilöstölle ja muille asiakirjojen käsittelyyn liittyviä tehtäviä hoitaville annetaan ohjeet ja koulutusta asiakirjojen ja niihin sisältyvien tietojen asianmukaisesta käsittelystä…*” (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 681/2010, 5 § 9k).

Valtionhallinnon tietoturvallisuuden johtoryhmä, VAHTI, on laatinut tietoturvallisuusasetuksesta ohjeen ”Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta”, jonka tarkoituksena on tehostaa ja yhdenmukaistaa asetuksen täytäntöönpanoa

valtionhallinnossa. VAHTI on valtiovarainministeriön asettama elin, joka ohjaa, koordinoi sekä kehittää valtionhallinnon tietoturvallisuutta. (VAHTI 2/2010, 10.) Pian asetuksen voimaantulon jälkeen julkaistussa ohjeessa kuvataan muun muassa yksityiskohtaisemmin tietoturvatasojen vaatimukset. Tietoturvakoulutuksen osalta ohjeesta (VAHTI 2/2010, 106) löytyy seuraavaa:

Perustasolla

- Tietoturvakoulutusta järjestetään henkilöstölle ja muille avainryhmille säännöllisesti sekä ylläpidetään ja kehitetään tietoturvahenkilöstön osaamista
- Tietoturva-asiat sisältyvät perehdytykseen
- Tietoturvaohjeiden ja -käytäntöjen muuttumisesta tiedotetaan organisaatiossa
- Tietoturvaohjeiden ja -käytäntöjen noudattamista seurataan ja rikkomuksiin puututaan

Korotetulla tasolla

- Organisaatiolla on kirjallinen koulutussuunnitelma
- Perehdytyksessä käsiteltävistä tietoturva-asioista on kirjallinen lista
- Organisaatiossa seurataan henkilöstön osallistumista tietoturvakoulutuksiin
- Tietoturvamääräysten ja -ohjeiden noudattamatta jättämisestä koituvat seuraukset on kuvattu sekä tiedotettu kaikille työntekijöille
- Esimies ja alainen keskustelevat vuosittain työhön liittyvistä tietoturvavastuista sekä tarpeista kehittää osaamista.
- Organisaatio varmistaa henkilöstön tietoturvaosaamisen

Korkeimmalla tasolla

- Tietoturvakoulutuksessa huomioidaan organisaatiossa ja lähiympäristössä tapahtuneet muutokset ja tietoturvapoikkeamat
- Hyvästä tietoturvatoiminnasta annetaan positiivista huomiota ja palautetta.

Osana Valtiokonttoria toimiva Valtion IT-palvelukeskus tarjoaa maksutta valtionhallinnon asiakkaiden käyttöön tietoturvallisuuden verkkokursseja, joiden materiaalit on laadittu VAHTI-ohjeiden pohjalta. Verkkokurssit on toteutettu avoimeen lähdekoodiin perustuvalla Moodle-oppimisalustalla. Verkkokurssin käyttöönottavalle organisaatiolle perustetaan oma koulutusympäristö, jota organisaatio voi itse hallinnoida ja ylläpitää. Verkkokurssitarjonnasta löytyvät muun muassa henkilöstön tietoturvakurssi, johdon tietoturvakurssi, sosiaalisen median

tietoturvakurssi, tietoaineistojen luokittelu ja käsittely -kurssi, ICT-hankintojen tietoturvakurssi sekä tietoturvatasot -kurssi.

Henkilöstön tietoturvakurssilla käsitellään tietoturvallisuuden keskeisimpiä perusasioita. Kurssilla käydään läpi muun muassa käyttöturvallisuutta työasemien ja kannettavien, matkapuhelimien sekä tietojärjestelmien osalta. Muita käsiteltäviä asioita ovat salasanaturvallisuus, Internetin, sähköpostin ja sosiaalisen median käyttö, yleiset toimitilaturvallisuuteen liittyvät asiat tietoturvallisuuden näkökulmasta sekä toiminta ongelmatilanteissa. Lisäksi kurssilla käsitellään pintapuolisesti tietoaineistojen salassapitoa sekä tiedon luokittelua ja käsittelyä koskevia asioita, sillä saatavilla on erillinen verkkokurssi tietoaineiston luokittelusta ja käsittelystä. Kurssilla on myös aiheeseen liittyvä testi, joka sisältää monivalintakysymyksiä. Testillä työntekijä voi testata osaamisensa ja organisaatio puolestaan seurata kurssisuorituksia ja tietoturvaosaamisen tasoa. Verkkokurssia voi käyttää sellaisenaan, mutta on suositeltavaa, että organisaatiot räätälöivät kurssia sisällöllisesti vastaamaan omia tarpeitaan esimerkiksi lisäämällä oman organisaationsa tietoturvallisuusohjeita ja -käytäntöjä.

Seuraavissa alaluvuissa kuvataan kolmen valtionhallinnon organisaation tietoturvakoulutuksen toteuttaminen. Kaikki kolme organisaatiota ovat ottaneet käyttöön Valtion IT-palvelukeskuksen tarjoaman henkilöstön tietoturvakurssin. Tapauksissa kuvatut organisaatiot eivät halua nimeään julkisuuteen, joten toiminnan kuvaaminen tehdään anonyymisti erottaen organisaatiot toisistaan kirjaimilla A, B ja C. Opinnäytetyössä haastateltavana olevat organisaatioiden edustajat ovat tietoturva-ammattilaisia. Valtiohallinnon organisaation A:n edustaja toimii organisaatiossa tietoturva-asiantuntijana. Valtionhallinnon organisaatioiden B:n ja C:n edustajat työskentelevät organisaatioissa tietoturvapäällikköinä.

## 4.1 Valtionhallinnon organisaatio A

Organisaatio on laatinut tietoturvakoulutus- ja tietoisuusohjelman, joka käynnistettiin vuonna 2010. Tietoturvakoulutusta toteutettiin luokkakoulutuksena osana organisaation yleistä turvallisuuskoulutusta. Turvallisuuskoulutus järjestettiin ensimmäiseksi organisaation esimiehille, jonka jälkeen hyvää palautetta saanut koulutus järjestettiin kaikilla toimialoilla. Organisaatiossa edistetään lisäksi tietoturvatietoisuutta muun muassa julkaisemalla Intranetissä tietoturva-aiheisia tietoiskuja ajankohtaisista aiheista. Vuonna 2011 organisaatiossa päätettiin toteuttaa henkilöstön tietoturvakoulutus verkkokoulutuksena.

Verkkokoulutukseen päädyttiin, sillä verkkokurssin avulla organisaation oli mahdollista seurata ketkä ovat suorittaneet kaikille pakollisen tietoturvakurssin. Lisäksi organisaatiossa haluttiin mitata työntekijöiden tietoturvatietoisuuden tasoa, joka onnistui kurssiin kuuluvan tentin avulla. Muita syitä verkkokoulutuksen valintaan olivat kurssin maksuttomuus ja mahdollisuus

muokata materiaalia sisällöllisesti vastaamaan organisaation omia tarpeita. Johdon tuen saamiseksi verkkokoulutusta perusteltiin johdolle edellä mainittujen asioiden lisäksi tietoturvallisuusasetuksella ja viranomaisilta edellytettävältä tietoturvallisuuden perustason vaatimuksilla, joka edellyttää esimerkiksi säännöllistä koulutusta. Koulutusmenetelmä saikin johdon hyväksynnän johtoryhmän kokouksessa. Koulutuksesta keskusteltiin vielä sekä riskienhallinta- ja ICT -koordinaatioryhmien kanssa. Koordinaatioryhmät koostuvat toimialojen tietohallintopäälliköistä ja riskienhallintavastaavista. Keskustelujen jälkeen tieto tulevasta koulutuksesta vietiin toimialojen esimiehille.

Verkkokoulutukselle asetettiin kokonaistavoitteeksi, että jokainen organisaation työntekijä suorittaa kurssin. Kurssin materiaalia räätälöitiin jonkin verran. Materiaalista poistettiin muun muassa tietoaineistojen luokittelua ja käsittelyvaatimuksia koskevat aiheet, sillä ne eivät olleet organisaatiolle ajankohtaisia. Ennen varsinaista julkaisua kurssi testattiin organisaation tietoturvaryhmän sisällä, jonka jälkeen riskienhallintaryhmässä toteutettiin pilotointi ja saadun palautteen perusteella tehtiin viimeiset muutokset. Verkkokurssin julkaisuvaiheessa organisaation Intranetiin tehtiin uutinen riskienhallintajohtajan allekirjoittamana, jossa annettiin ohjeet verkkokurssin suorittamiseksi. Intranetin lisäksi lähetettiin sähköpostilla muistutusviesti koulutukseen osallistumisesta, jonka allekirjoittajana toimi organisaation ylimmän johdon edustaja. Henkilökuntaa pyrittiin motivoimaan esimerkiksi siten, että sähköpostilla lähetettävässä muistutusviestissä mainittiin ylimmän johdon edustajan ja riskienhallintajohtajan tentistä saamat tulokset.

Verkkokoulutuksen aikana ilmeni ongelmia, jotka liittyivät rekisteröitymiseen ja kurssin suorittamiseen. Ohjeista huolimatta työntekijöillä oli vaikeuksia luoda itselleen kirjautumista varten käyttäjätunnus ja salasana. Organisaatio arvioi, ettei ohjeita jaksettu lukea, vaikka ohjeet oli pyritty laatimaan lyhyesti ja selkeästi. Vain muutamalla työntekijällä vaikeudet liittyivät siihen, että järjestelmä ei hyväksynyt työntekijän käyttäjätunnuksena toimivaa työsähköpostiosoitetta tai työntekijä ei saanut järjestelmän lähettämää vahvistusviestiä sähköpostiinsa, eikä näin voinut suorittaa rekisteröitymistä loppuun. Lisäksi työntekijöiden tuli rekisteröitymisen yhteydessä määrittää itse käyttäjäprofiiliinsa osasto, jossa työntekijä työskentelee. Työntekijät kokivat tämän niin ikään hankalaksi. Osaston määrittäminen oli organisaatiolle oleellinen tieto seurantaa ja raportointia varten.

Organisaatio tarkasteli kurssin suorittamiseen käytettyjä aikoja, joista selvisi, etteivät kaikki työntekijät olleet lukeneet materiaalia tai tenttikysymyksiä. Tämä oli pääteltävissä suoritusajoista, jotka olivat osalla suhteettoman nopeita. Toisin sanoen, osa työntekijöistä oli siirtynyt suoraan tenttiin ja rastittanut satunnaisesti kysymysten vastaukset lukematta koulutusmateriaalia tai tenttikysymyksiä. Tähän saattoi olla osaksi syynä, ettei tenttiin asetettu läpäisyrajaa, jonka perusteella kurssi katsottaisiin suoritetuksi.

Kurssin suorituksia seurattiin tiiviisti ja koulutuksen päättyessä laadittiin erikseen luettelo henkilöistä, jotka eivät olleet kurssia suorittaneet. Työntekijöitä, joilta suoritusmerkintä puuttui, lähestyttiin henkilökohtaisella muistutusviestillä, puhelimitse ja muutamassa tapauksessa koulutuksen koordinoinnista vastannut henkilö kävi paikalla henkilökohtaisesti. Lopulta kurssin suoritti 94 % organisaation työntekijöistä, joka katsottiin hyväksi saavutukseksi. Kurssi jäi suorittamatta erinäisistä syistä 6 %:lta työntekijöistä. Organisaatio arvioi, että suurimmaksi osaksi kyseessä oli suorittamatta jättäneiden osalta motivaation puute ja asenteet eli työntekijät eivät yksinkertaisesti vain suostuneet suorittamaan kurssia, vaikka kurssin suoritusvelvollisuudesta muistutettiin useaan otteeseen. Tentin suorituksia arvioitiin asteikolla 1-10. Kurssisuoritusten kokonaiskeskiarvo oli 8,4, johon organisaatiossa oltiin tyytyväisiä. Verkkokoulutukseen varattiin alun perin aikaa kuukausi, mutta koulutus vei loppujen lopuksi kaksi kuukautta.

Koulutuksen jälkeen organisaatiossa ei toteutettu erikseen palautekyselyä. Palautetta saatiin muutamilta työntekijöiltä suoraa. Saatu palaute oli enimmäkseen negatiivista joka koski vaikeuksia luoda verkkokurssille kirjautumistunnukset. Lisäksi negatiivista palautetta annettiin tenttikysymyksistä, joista osa koettiin sellaisiksi, joiden vastausvaihtoehdot eivät olleet työntekijöiden mielestä yksiselitteisiä. Organisaatio sai myös positiivista palautetta, joka liittyi tietoturvakoulutuksen järjestämiseen. Palautteenantajien mielestä oli hyvä asia ja tärkeää, että organisaatio järjestää tietoturvakoulutusta.

Organisaatio arvioi, että verkkokoulutusta ei tulla järjestämään tulevaisuudessa koko organisaatiota koskevalla laajuudella ennen kuin siihen liittyvät ongelmat on saatu ratkaistua. Verkkokoulutusta tullaan kuitenkin käyttämään eri kohderyhmille suunnatuissa koulutuksissa, joissa koulutuksen osallistujamäärät ovat pieniä.

## 4.2 Valtionhallinnon organisaatio B

Valtionhallinnon organisaatio B:llä ei toistaiseksi ole tietoturvakoulutus- ja tietoisuusohjelmaa, mutta alustavaa suunnittelutyötä on tehty. Koulutusohjelma on tarkoitus saada valmiiksi syksyn 2012 aikana. Vaikka organisaatiolla ei ole varsinaista koulutusohjelmaa, järjestetään tietoturvakoulutusta säännöllisesti. Keväällä 2012 organisaatiossa päätettiin ottaa luokkaopetuksena järjestettävän tietoturvakoulutuksen rinnalle verkkokoulutus, sillä koulutusmuoto on ajasta ja paikasta riippumatonta. Työntekijöille haluttiin tarjota mahdollisuus suorittaa koulutus itselleen parhaiten sopivana ajankohtana. Lisäksi koulutusmuodon valintaan vaikuttivat koulutuksen toteuttamisen edullisuus ja kustannussäästöt. Johdolle verkkokoulutuksen hyödyntämistä tietoturvakoulutuksessa perusteltiin kustannussäästöillä, sekä yksinkertaisena ja helppona tapana toteuttaa luokkaopetuksen rinnalla. Lisäksi koulutusmuotoa perusteltiin

opiskeluajan ja paikan valinnan joustavuudella, joka mahdollistaisi paremmin kiireisten työntekijöiden osallistumisen koulutukseen.

Verkkokoulutuksen sisällön ja toteutuksen suunnittelun yhteydessä organisaatiossa toteutettiin pienimuotoinen tietoturvakysely, jolla kartoitettiin henkilöstön suhtautumista ja asenteita tietoturva-asioihin. Kyselystä saatujen tulosten perusteella organisaatio aikoo tulevaisuudessa kehittää henkilöstölle suunnatun tietoturvakoulutuksen sisältöä. Tulosten avulla voidaan arvioida mitkä tietoturvakoulutuksen aiheista ovat työntekijöillä hallinnassa, jolloin koulutuksessa ei tarvitse painottaa kyseisiä aiheita. Sen sijaan koulutuksessa voidaan keskittyä niihin tietoturva-asioihin, joissa on havaittu puutteita. Laajamittaista henkilöstön tietoturvakäyttäytymisen nykytilaa koskevaa kartoitusta ei ole tehty. Tietoturvakyselyn toteutukseen ja tuloksiin voi tutustua liitteessä 1.

Tietoturvakoulutuksen kokonaistavoitteeksi asetettiin organisaation tietoturvakulttuurin parantaminen edistämällä työntekijöiden tietoturvatietoisuutta. Lisäksi tavoitteeksi asetettiin, että koko henkilöstö on suorittanut tietoturvakoulutuksen osallistumalla joko verkko- tai luokkakoulutukseen vuoden 2012 loppuun mennessä. Koulutuksella määriteltiin myös seuraavat oppimistavoitteet: työntekijät tutustuvat tietoturvallisuuden tärkeimpiin asioihin, hallitsevat koulutuksen jälkeen tietoturvallisuuden perusasiat ja tietävät mistä löytää tarvittaessa lisätietoa.

Verkkokurssin sisältö räätälöitiin organisaatiolle sopivaksi tekemällä materiaalin sisältöön pieniä muutoksia. Kokonaisuudessaan materiaalista haluttiin tehdä tiivis kokonaisuus, johon lisättiin organisaatiota koskevia yksityiskohtia ja yhteistietoja. Lisäksi materiaalista jätettiin pois esimerkiksi salassa pidettävien tietoaineistojen luokittelua ja käsittelyä koskevat asiat, sillä organisaatio aikoo myöhemmin toteuttaa aiheesta erillisen koulutuksen. Huomiota kiinnitettiin myös tekstin selkeyteen, sillä koulutus oli suunnattu koko henkilöstölle, joten materiaalin tuli olla kaikkien ymmärrettävissä. Räätälöinti koettiin tärkeäksi, sillä koulutuksen haluttiin näyttävän ja tuntuvan organisaation omalta eli työntekijä kokee verkkokurssin materiaalin koskevan työntekijän omia työtehtäviä ja organisaatiota. Verkkokoulutuksesta haluttiin tehdä helposti lähestyttävä ja helppokäyttöinen, sillä se on koulutusmuotona organisaatiossa uutta.

Organisaatiossa päätettiin, että henkilökohtaisten käyttäjätunnusten sijaan verkkokurssille kirjaudutaan yhteiskäyttötunnuksilla. Yhteiskäyttötunnukset ovat nimensä mukaisesti yhteisessä käytössä oleva yksittäinen käyttäjätunnus ja salasana. Ratkaisuun päädyttiin, sillä henkilökohtaisten käyttäjätunnusten luominen koettiin hankalaksi. Tällaisella ratkaisulla koulutusympäristön käyttö on verrattavissa Intranetin käyttöön. Verkkokurssiin kuuluva tentti päätettiin myös jättää pois, sillä tentin suorittaminen olisi edellyttänyt kirjautumista verkkokurs-

sille henkilökohtaisella käyttäjätunnuksella ja salasanalla. Kurssisuoritusten seuraamisen osalta organisaatiossa päädyttiin ratkaisuun, jossa työntekijä ilmoittaa sähköpostilla tietoturvapäällikölle kurssin suorittamisesta.

Kurssin sisällön ja toteutuksen suunnittelun jälkeen oli vuorossa testausvaihe, jota seurasi pilotointi. Pilottivaihe toteutettiin kevään 2012 aikana. Pilotointivaiheessa verkkokoulutukseen kutsuttiin osallistumaan pieni joukko työntekijöitä. Tarkoituksena oli kerätä palautetta ja käyttökokemuksia, sekä tehdä palautteiden perusteella viimeiset muutokset ennen kuin koulutus julkaistaisiin koko henkilöstölle. Verkkokurssi sai pilotointiin osallistuneelta ryhmältä positiivista palautetta. Kurssia pidettiin tiiviinä, mutta informatiivisena kokonaisuutena. Materiaaliin esitettiin lisättäväksi vielä muutamia täsmennyksiä.

Henkilöstön motivoimiseksi organisaatio päätti kohdistaa verkkokoulutuksesta viestimisen osastokohtaiseksi. Lisäksi osastojen esimiehet velvoitettiin seuraamaan koulutukseen osallistumista. Kohdennettu viestintä nähtiin henkilökohtaisemmaksi lähestymistavaksi kuin ilmoittaminen yleistasolla Intranetissä. Osastojen työntekijöille lähetettiin ylimmän johdon edustajan allekirjoittama sähköpostiviesti, jossa kerrottiin koulutuksesta ja työntekijän velvollisuudesta suorittaa tietoturvakoulutus verkkokurssina tai osallistumalla luokkaopetukseen ja suorituksia tultaisiin myös seuraamaan.

Johdon tuki tietoturvakoulutukselle näkyi koulutuksen valmistelussa ohjauksena sekä tarvittavien resurssien myöntämisenä. Johto teki esimerkiksi linjauksia koulutuksen laajuudesta ja toteutustavasta. Johdon sitoutuminen näkyi myös viestinnässä, jossa henkilöstölle osoitettujen, koulutusta koskevien, sähköpostiviestien allekirjoittajana toimi johdon edustaja.

Organisaatio koki verkkokoulutuksen suurimmaksi hyödyksi sen, että koulutustapa tavoittaa henkilöstön helposti. Pilottivaiheen aikana haasteelliseksi koettiin kuitenkin henkilökunnan motivoiminen osallistumaan koulutukseen. Organisaatio arvioi, että syynä motivoinnin haasteellisuuteen on työntekijöiden kiire sekä muun tarjolla olevan koulutuksen suuri määrä. Motivointia lukuun ottamatta kohdatut haasteet olivat pieniä yksittäistapauksia. Esimerkiksi muutama verkkokurssin suorittanut työntekijä unohti ilmoittaa kurssin suorittamisesta tietoturvapäällikölle.

Tulevaisuudessa tietoturvakoulutuksen verkkototeutusta on tarkoitus kehittää ja ottaa laajempaan käyttöön. Lisäksi organisaatio aikoo toteuttaa salassa pidettävien tietoaineistojen luokitteluun ja käsittelyyn liittyvän tietoturvakoulutuksen ainakin osittain verkkokoulutuksena. Tässä verkkokoulutuksessa on käytössä henkilökohtaiset käyttäjätunnukset ja kurssin suoritukseen kuuluu pakollinen tentti. Uusien työntekijöiden osalta koulutuksesta ja sen suorittamisesta kerrotaan jatkossa perehdytyksen yhteydessä.

## 4.3 Valtionhallinnon organisaatio C

Valtionhallinnon organisaatio C:llä ei ole erillistä tietoturvakoulutus- ja tietoisuusohjelmaa. Organisaatiossa on käynnissä tietoturvallisuusasetuksen edellyttämän tietoturvatason saavuttamista koskeva hanke, jonka projektisuunnitelma toimii vuoden 2012 osalta tietoturvallisuuden vuosisuunnitelmana. Projektisuunnitelmaan on sisällytetty ohjelma henkilöstön tietoturvakoulutuksesta. Osana hanketta tietoturvakoulutus liitetään osaksi organisaation normaalia koulutussuunnitelmaa. Henkilöstön tietoturvakoulutuksen lisäksi organisaatio aikoo toteuttaa johdolle suunnatun tietoturvakoulutuksen.

Henkilöstön tietoturvakoulutuksen toteutusmuotoa pohdittiin organisaatiossa jonkin verran. Vaihtoehtoina olivat luokkakoulutus, verkkokoulutus tai näiden yhdistelmä. Tietoturvakoulutuksen toteutuksesta vastaava henkilö tarkasteli yhdessä henkilöstöhallinnon kanssa vaihtoehtojen hyviä puolia sekä organisaation historiaa ja kokemusta eri koulutusvaihtoehdoista. Verkkokoulutuksen käyttö herätti keskustelua johtuen organisaation aiemmista kokemuksista. Organisaatiossa päädyttiin lopulta ratkaisuun toteuttaa tietoturvakoulutus sekä verkko- että luokkakoulutuksena. Verkkokoulutusta perusteltiin johdolle kustannussäästöillä, koulutuksen tavoitettavuudella sekä raportointimahdollisuudella.

Organisaatio ei ole toteuttanut henkilöstön tietoturvakäyttäytymisen nykytilaa kuvaavaa kartoitusta. Tietoturvakäyttäytymisen nykytilaa on kuitenkin arvioitu keskustelemalla henkilöstön, tietohallinnon ja tietoturvasta vastaavien henkilöiden kanssa. Henkilöstön tietoturvakoulutuksen kokonaistavoitteeksi asetettiin henkilöstön tietoturvatietoisuuden parantaminen eli työntekijä tuntee ja hallitsee omaan työhönsä liittyvät tietoturvallisuuden perusasiat. Lisäksi tavoitteeksi asetettiin, että koko henkilöstö suorittaa tietoturvakoulutuksen osallistumalla joko verkko- tai luokkakoulutukseen. Johdolle suunnatussa koulutuksessa tavoitteena on, että organisaation johto ymmärtää johdon velvollisuudet tietoturvallisuuden hallinnan, seurannan ja raportoinnin osalta.

Organisaatiossa räätälöitiin verkkokoulutuksen materiaali organisaatiolle sopivaksi. Materiaaliin tehtiin paljon muutoksia: aiheita karsittiin ja materiaaliin tuotiin paljon organisaation omia ohjeistuksia. Tavoitteena oli saada verkkokoulutuksesta tiivis kokonaisuus. Materiaalista jätettiin pois esimerkiksi lainsäädäntöä ja tietoaineiston luokittelua koskevat asiat. Lainsäädäntöä koskevat osuudet päätettiin jättää pois ja tuoda esille muussa yhteydessä. Organisaatiossa lähdettiin siitä, että työntekijöillä on suhteellisen hyvin tiedossa omia työtehtäviä koskeva tietoturvallisuuteen liittyvä lainsäädäntö. Koulutuksessa käsitellään ainoastaan uusi tietoturvallisuusasetus ja sen tuomat velvoitteet. Lisäksi tietoaineiston käsittelyä koskevat asiat jätettiin pois, sillä organisaatiossa ei vielä ole otettu käyttöön tietoturvallisuusasetuksen mukaista tietoaineistojen luokittelua, joka edellyttää organisaatiolta luokittelupäätöksen teke-

mistä ja uusia käsittelyohjeita. Tietoaineistojen luokittelu ja käsittely -koulutus on tarkoitus toteuttaa erikseen.

Organisaation työntekijät rekisteröityvät verkkokurssille omalla käyttäjätunnuksella ja salasanalla. Verkkokoulutuksen osalta kurssisuorituksia seurataan kurssiin kuuluvan tentin avulla. Luokkakoulutuksessa osallistujien nimet ja osasto kerätään nimilistaan. Organisaatio ei pidä yhteiskäyttötunnusten käyttöä tässä yhteydessä ongelmallisena, mutta seurannan ja raportoinnin kannalta päädyttiin henkilökohtaisten tunnusten käyttöön.

Organisaatiossa on yhdistetty verkkokoulutuksen testaus- ja pilotointivaiheet. Vaiheeseen osallistuu kaksi henkilöä sekä viestinnästä että henkilöstöhallinnosta. Vaiheeseen osallistuvat työntekijät eivät ole olleet mukana verkkokoulutuksen suunnittelutyössä. Saadun palautteen perusteella verkkokoulutukseen tehdään vielä viimeiset muutokset ennen koulutuksen käyttöönottoa.

Organisaatiolla on käytössä Intranetissä koulutuskalenteri, johon on koottu kaikki henkilöstölle suunnatut koulutukset. Koulutuskalenterin lisäksi tietoturvakoulutuksesta tehdään organisaation Intranetiin uutinen, jonka allekirjoittajana toimii organisaation ylimmän johdon edustaja. Uutisessa kerrotaan tulevasta koulutuksesta, sen syistä ja tavoitteista ja työntekijän velvollisuudesta osallistua joko verkko- tai luokkakoulutukseen. Lisäksi uutiseen on liitetty työntekijöille ohjeet verkkokoulutukseen rekisteröitymisestä ja sen suorittamisesta, sekä luokkakoulutuksen osalta linkki, jolla työntekijä voi ilmoittautua luokkakoulutukseen. Uutista koulutuksesta nostetaan koulutuksen aikana tasaisesti esille Intranetin uutisosiossa muistutuksena.

Henkilöstön motivointiin on lähdetty viestinnän kautta, mistä johtuen mukana suunnittelussa on ollut alusta asti viestinnän henkilö. Intranetiin tulevasta uutisesta on pyritty muotoilemaan motivoiva ja kannustava. Muita motivointikeinoja ovat koulutuksen pakollisuus, ylimmän johdon tuki sekä osallistumisen seuraaminen. Esimiehillä on velvollisuus valvoa ja seurata, että työntekijät osallistuvat koulutukseen ja tarvittaessa muistuttava koulutuksen pakollisuudesta.

Koulutuksen suunnittelutyö aloitettiin maaliskuussa 2012, noin kolme kuukautta ennen verkko- ja luokkakoulutusten käynnistymistä. Koulutuksen suorittamiseen on varattu aikaa käytännössä kuusi viikkoa, mutta verkkokoulutus tullaan pitämään koulutuksen jälkeen auki, jotta työntekijöillä on tarvittaessa mahdollisuus palata materiaaliin. Luokkakoulutus järjestetään verkkokoulutuksen kanssa samaan aikaan Non-Stop tyyppisesti neljänä päivänä, jolloin työntekijöillä on mahdollisuus osallistua tunninmittaiseen koulutukseen.

Verkkokoulutukseen liittyvät suurimmat haasteet liittyvät organisaation aiempiin negatiivisiin kokemuksiin koulutusmuodon käytöstä. Verkkokoulutus on koettu organisaatiossa hankalaksi, mikä on osaltaan vaikuttanut vähäisiin osallistujamääriin. Organisaatiolla ei ole vielä loppukäyttäjien kokemuksia nykyisestä verkkokoulutuksesta, mutta pilotointi- ja testausvaiheessa esimerkiksi käyttäjätunnusten luominen on koettu hankalaksi. Lisäksi organisaatio näkee haasteellisena järjestelmän edellyttämät monimutkaiset salasanat, jotka unohtuvat käyttäjältä helposti. Organisaatio arvioi, että työntekijän kynnys palata materiaaliin on korkea unohdettujen salasanojen vuoksi.

Organisaatio aikoo kerätä koulutuksen jälkeen palautteen, mutta palautteessa kysyttäviä asioita ei ole vielä suunniteltu. Palautekysely suunnitellaan yhdessä henkilöstöhallinnon edustajan kanssa, joka vastaa henkilöstön kehittämisestä ja toteutetaan Digium Enterprise-ohjelmistolla. Palautteella halutaan kerätä kokemuksia nimenomaan verkkokoulutuksen osalta, koska ennakkoasenteet verkkokoulutusta kohtaan ovat olleet negatiiviset. Lisäksi palautteen avulla aiotaan kehittää tietoturvakoulutuksen laatua.

Organisaatio pitää verkkokoulutuksen suurimpina hyötyinä kustannussäästöjä, sillä työntekijä voi suorittaa kurssin omalta työpisteeltä itselleen sopivana ajankohtana eikä koulutusta varten tarvitse siirtyä toiseen paikkaan. Toinen tunnistettu hyöty on henkilöstön tavoitettavuus eli kaikilla työntekijöillä on mahdollisuus suorittaa koulutus sijainnista riippumatta. Kolmantena hyötynä nähdään kurssisuoritusten seuraamisen helppous. Organisaatio saa verkkokurssin raportointityönkalun avulla ajantasaisen raportin kurssisuorituksista.

Verkkokoulutusta olisi tarkoitus käyttää tulevaisuudessakin, mutta jatko riippuu organisaation saamasta palautteesta sekä työntekijöiden vastaanottavuudesta. Muuten tietoturvakoulutuksen osalta koulutus tulee olemaan säännöllistä. Vaikka verkkokoulutusta ei jatkossa käytettäisi, tullaan verkkokurssin materiaali hyödyntämään eri tavoin. Esimerkiksi organisaation Intranetiin ollaan tekemässä tietoturvallisuudesta wiki -tyyppistä sivustoa, jonka runkona toimii verkkokoulutuksen materiaali. Lisäksi materiaalista aiotaan laatia tiiviimpi kokonaisuus organisaation uusien työntekijöiden perehdytystä varten.

# 5 Johtopäätökset

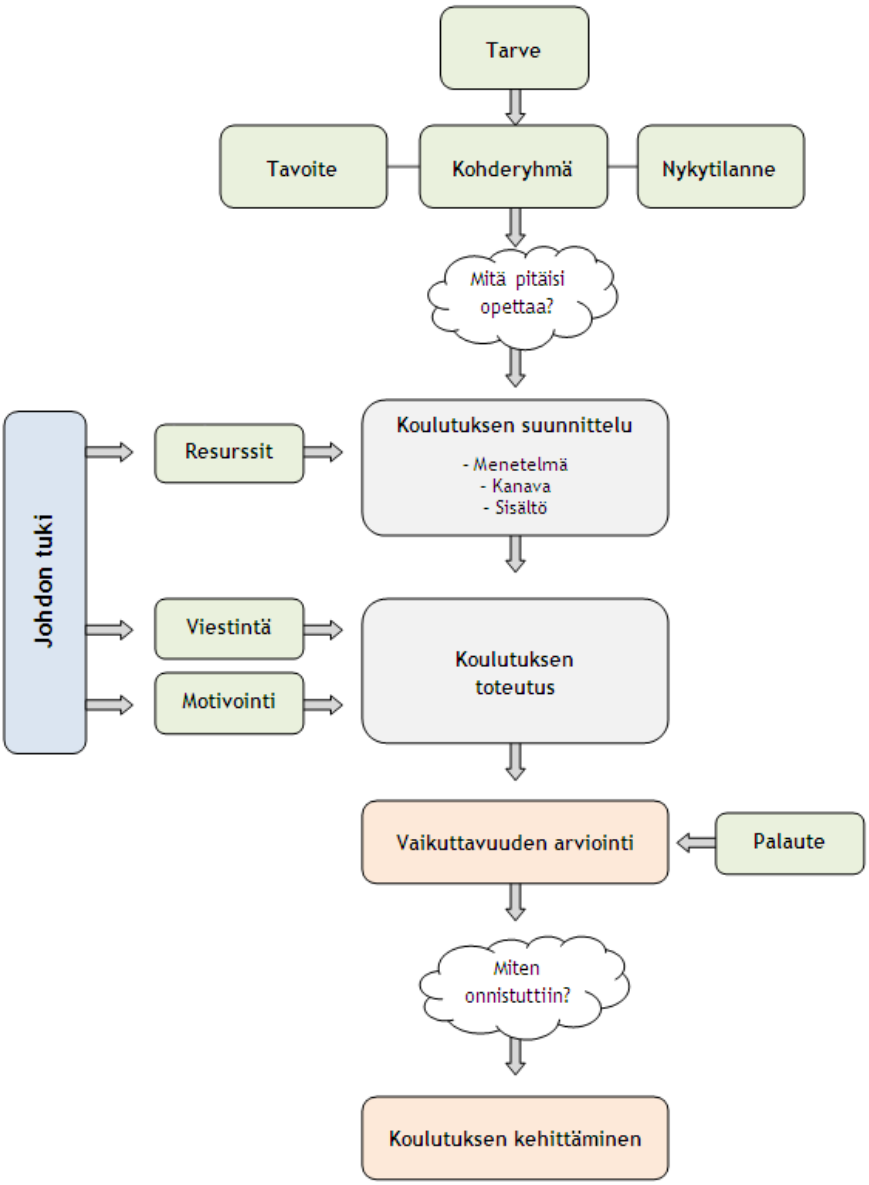
Valtionhallinnon organisaatioiden tietoturvatoimintaa koskevat velvoitteet tulevat lähtökohtaisesti lainsäädännöstä. Suomessa ei ole yhtenäistä tietoturvalainsäädäntöä, vaan velvoitteita löytyy useista laeista ja asetuksista. Näistä keskeisimmät ovat laki viranomaisen toiminnan julkisuudesta sekä asetus tietoturvallisuudesta valtionhallinnossa. Viranomaisia koskevien yhteisten lakien ja asetuksien lisäksi tietoturvavelvoitteista on säädetty viranomaisten omissa toimialakohtaisissa erityislaeissa.

Tietoturvakoulutuksen tavoitteena on edistää työntekijöiden tietoturvatietoisuutta sekä muuttaa vääränlaisia toimintatapoja, jotka vaarantavat organisaation tietoaineistojen turvallisuuden. Käyttäytymisen muutos edellyttää työntekijöiden asenteiden muuttamista ja motivointia toimia tietoturvallisesti. Tietoturvakoulutus on onnistunut silloin, kun sille asetettu tavoite on saavutettu. On tavallista, että tietoturvakoulutuksen jälkeen organisaation tietoturvakulttuuri voi hetkellisesti parantua, mutta ajan kanssa työntekijät palaavat vanhoihin toimintatapoihin. Tietoturvatietoisuuden ylläpitäminen edellyttääkin työntekijöiden säännöllistä kouluttamista.

Tietoturvakoulutuksen epäonnistuminen on todennäköistä silloin, kun koulutukselle ei ole asetettu tavoitetta eikä ole pohdittu miten asetettuun tavoitteeseen päästäisiin. Koulutus on siis tehotonta, mikäli se järjestetään ”vain koska on pakko” tai esimerkiksi työntekijöiden oletetaan lukevan oma-aloitteisesti organisaation tietoturvaohjeistukset Intranetistä.

## 5.1 Tietoturvakoulutuksen prosessimalli

Hyvä tietoturvakoulutus edellyttää koulutuksen huolellista suunnittelua. Kirjallisuuskatsauksen ja valtionhallinnon organisaatioiden haastattelujen pohjalta syntyi tietoturvakoulutuksen prosessimalli (kuva 3). Malli jakaantuu kolmeen osaan, joissa kuvataan tietoturvakoulutuksen vaiheita sekä tekijöitä, jotka vaikuttavat koulutuksen suunnitteluun ja toteuttamiseen. Ensimmäisessä osassa tarkastellaan tekijöitä, jotka tulisi ottaa huomioon ennen koulutuksen suunnittelua ja toteutusta. Toisessa osassa tarkastellaan puolestaan koulutuksen suunnitteluja toteutusvaiheita ja kolmannessa vaiheita koulutuksen jälkeen.




Kuva 3: Tietoturvakoulutuksen prosessimalli

Tietoturvakoulutuksen prosessi alkaa tunnistamalla koulutukselle tarve, sillä koulutukselle tulee aina olla jokin syy miksi koulutusta järjestetään. Tarve voi muodostua esimerkiksi silloin, kun organisaatiossa laaditaan uudet tietoturvaohjeet tai lainsäädännössä tapahtuu jokin organisaation tietoturvakäytäntöihin tai -velvoitteisiin vaikuttava muutos. Haastateltavien organisaatioiden tarpeet tietoturvakoulutuksen toteuttamiselle olivat samat: säännöllisesti järjestettävän koko henkilöstön tietoturvallisuuden peruskoulutuksen toteuttaminen.

Ennen koulutuksen suunnittelua ja toteutusta tulee pohtia mitä koulutukseen osallistuville pitäisi opettaa. Tähän vaikuttavat koulutuksen tavoite, kohderyhmä ja nykytilanne. Tunnistetusta tarpeesta johdetaan koulutukselle tavoite eli mitä koulutuksella halutaan saavuttaa. Tavoitteen asettaminen on tärkeää, jotta olisi päämäärä, johon koulutuksella pyritään. Orga-

nisaatiot A, B ja C asettivat koulutuksen tavoitteeksi koko henkilöstön osallistumisen tietoturvallisuuden peruskoulutukseen. Lisäksi organisaatio B ja C toivat esille, että koulutuksen tavoitteena oli organisaation tietoturvakulttuurin parantaminen edistämällä henkilökunnan tietoturvatietoisuutta.

Tavoitteen lisäksi tulee tarkastella koulutuksen kohderyhmää, jolle koulutus tulee suunnata tavoitteen saavuttamiseksi: koulutetaanko koko henkilöstö vai jokin erityisryhmä esimerkiksi organisaation osasto tai sidosryhmän henkilöitä. Esimerkkinä toimivissa organisaatioissa kohderyhmän määrittely oli helppoa, sillä henkilöstön tietoturvallisuuden peruskoulutuksen kohderyhmänä on organisaation koko henkilöstö. Yhtä hyvin peruskoulutuksen kohderyhmänä voisi olla organisaation yksittäinen osasto, jonka työntekijöiden tietoturvakäyttäytymisessä havaittu muutostarve edellyttää koulutuksen järjestämistä kohdennetusti juuri kyseiselle osastolle ennen muuta henkilöstöä.

Nykytilanne on usein tekijä, joka unohdetaan suunniteltaessa tietoturvakoulutusta. Nykytilanteen kartoituksessa tulisi tarkastella muun muassa kohderyhmän nykytietämystä, osaamista, asenteita ja motivaatiota. Tämä on tärkeää, jotta tunnettaan millaiselle kohderyhmälle koulutusta ollaan suunnittelemassa. Kohderyhmän nykytilanteen kartoituksen avulla tiedetään millaisia menetelmiä tulisi käyttää, jotta tavoite saavutetaan. Lisäksi nykytilanteen selvittäminen auttaa koulutuksen sisällön suunnittelussa, sillä tiedetään mihin asioihin koulutuksessa tulisi keskittyä ja mitä aiheista voidaan käydä läpi pintapuolisesti. Haastatelluista organisaatioista organisaatiot B ja C selvittivät kohderyhmän nykytilannetta. Organisaatio B laati tietoturva-asenteita ja -käyttäytymistä kartoittavan mielipidekyselyn (kts. Liite 1). Organisaatiossa C nykytilannetta kartoitettiin keskustelemalla henkilöstön, tietohallinnon ja tietoturvavastaavien kanssa.

Tunnistettu tarve, asetettu tavoite, kohderyhmän ja nykytilanteen kartoitus toimivat pohjana koulutuksen suunnittelulle ja toteutukselle. Tässä kohtaan koulutukselle tulee saada viimeistään johdon tuki. Johto myöntää viime kädessä koulutukseen käytettävät resurssit, jotka vaikuttavat olennaisesti koulutuksen suunnitteluun ja sen myötä toteutukseen. Käytettävissä olevat resurssit vaikuttavat esimerkiksi suunnittelun osalta koulutuksen sisällölliseen laajuuteen - kuinka paljon työntekijät voivat käyttää työaikaa koulutukseen osallistumiseksi. Koulutuksen laajuus vaikuttaa puolestaan siihen, millaisia menetelmiä ja kanavia koulutuksen toteuttamiseksi voidaan käyttää. Esimerkiksi organisaation B johto antoi koulutuksen valmisteluihin ohjausta ja teki linjauksia liittyen koulutuksen laajuuteen ja toteutustapaan.

Koulutuksen suunnittelussa tulee valita koulutusmenetelmäksi kohderyhmälle parhaiten soveltuva tapa esimerkiksi itseopiskelu tai luentotilaisuus. Oikean menetelmän valitseminen edellyttää kohderyhmän tuntemista. Valittu menetelmä vaikuttaa siihen, millaista kanavaa esi-

merkiksi luokkahuone, verkko-oppimisympäristö, organisaation Intranet tai sähköposti, voidaan käyttää. Organisaatio A käytti menetelmänä itseopiskelua, jonka kanavana toimi verkko-oppimisympäristö. Organisaatiot B ja C käyttivät verkko-oppimisympäristössä tapahtuvan itseopiskelun lisäksi luokkahuonetyyppistä luentotilaisuutta. Organisaatioiden B ja C toteuttamilla nykytilannekartoituksilla oli vaikutusta koulutuskanavan valintaan. Muun muassa organisaatio C pohti tulisiko verkkokoulutusta käyttää laisinkaan.

Johdon tuen tulisi näkyä myös viestinnässä sekä henkilökunnan motivoinnissa. Osallistumalla viestintään, johto osoittaa muulle henkilöstölle, että tietoturvallisuutta pidetään tärkeänä ja sen kehittämiseen ollaan sitoutuneita. Johto voi myös omalla toiminnallaan vaikuttaa työntekijöiden motivaatioon toimimalla muille esimerkkinä. Mikäli johto ei pidä tietoturvallisuutta tärkeänä, miksi muun henkilöstön pitäisi pitää? Organisaatio A:n johto osallistui viestintään siten, että organisaation Intranetiin tehdyn koulutusta koskevan uutisen allekirjoittajana toimi riskienhallintajohtaja. Organisaation pääjohtaja allekirjoitti puolestaan työntekijöille sähköpostilla lähetetyn muistutusviestin, johon oli lisäksi liitetty työntekijöiden motivoimiseksi ja johdon tuen osoittamiseksi pääjohtajan ja riskienhallintajohtajan saamat tulokset verkkokurssiin kuuluvasta tentistä. Myös organisaatiot B ja C pyrkivät motivoimaan henkilöstöä osoittamalla johdon tuen koulutukselle.

Viestintä ja motivointi vaikuttavat oleellisesti siihen, miten työntekijät saadaan osallistumaan koulutukseen. Haastatellut organisaatiot käyttivät viestintään Intranetiä, johon tehtiin uutinen tulevasta tietoturvakoulutuksesta. Uutisen lisäksi koulutuksesta lähetettiin työntekijöille sähköpostilla muistutusviestejä. Organisaatioista B käytti osastokohtaisesti kohdennettua viestintään muun muassa henkilökunnan motivoimiseksi. Muita organisaatioiden käyttämiä motivointikeinoja olivat koulutuksen pakollisuus ja suoritusten seuraaminen. Mikäli työntekijöillä on velvollisuus osallistua koulutukseen, tulee osallistumista seurata. Organisaatio A laati verkkokoulutuksen jälkeen listan koulutuksen suorittaneista työntekijöistä. Koulutuksen koordinoinnista vastannut henkilö lähestyi listan perusteella niitä henkilöitä, joilta suoritus puuttui. Organisaatiot B ja C velvoittivat osastojen esimiehet seuraamaan työntekijöidensä osallistumista koulutukseen.

Tietoturvakoulutuksen jälkeen tulee arvioida koulutuksen vaikuttavuutta, jotta tiedetään miten koulutuksessa onnistuttiin ja miten koulutusta tulisi kehittää tulevaisuudessa. Koulutuksen vaikuttavuuden arvioimiseksi tulee laatia mittarit, jotka mittaavat asetetun tavoitteen saavuttamista. Lisäksi koulusta voidaan arvioida keräämällä palautetta. Palautteessa voidaan kysyä esimerkiksi oltiinko koulutukseen tyytyväisiä, mikä koulutuksessa oli hyvää ja mitä tulisi kehittää. Vaikuttavuutta voidaan arvioida myös havainnoimalla tai haastattelemalla eli näkyykö esimerkiksi tietoturvaohjeiden noudattaminen työntekijöiden toiminnassa: lukitaanko

tietokone useammin poistuttaessa työpisteeltä, käytetäänkö henkilökorttia, osataanko luottamukselliset tiedot lähettää salattuna sähköpostilla.

## 5.2 Verkkokoulutuksen soveltuvuuden arviointi

Verkkokoulutus on organisaatioissa kasvattanut suosiotaan koulutusmuotona muun muassa koulutukseen liittyvien hyötyjä vuoksi. Erityisiä hyötyjä organisaatiolle ovat kustannussäästöt, koulutettavien tavoitettavuus ja raportointimahdollisuudet esimerkiksi kurssisuoritusten osalta. Työntekijän kannalta verkkokoulutuksen etuja ovat koulutuksen joustavuus: työntekijä voi suorittaa koulutuksen haluamaan ajankohtana ja mahdollisuudet edetä omaan tahtiin. Organisaatiot A, B ja C kertoivat valinneensa verkkokoulutuksen edellä mainituista syistä.

Organisaatiot saattavat erheellisesti olettaa, että verkkokoulutuksen toteuttaminen on yksinkertaista ja helppoa, kun koulutusympäristö hankitaan valmiina palveluntarjoajalta. Koulutusympäristö saatetaan ottaa käyttöön sellaisenaan, vaikka verkkokoulutus vaatii yhtä lailla suunnittelua ja valmisteluja kuin perinteinen luokkakoulutus. Keskeisintä on räätälöidä kurssimateriaalin sisältö vastaamaan organisaatiota omia tarpeita. Esimerkiksi aiheet tai ohjeistukset, jotka eivät liity organisaation toimintaan ja toimintatapoihin, aiheuttavat hämmennystä. Huomiota tulee kiinnittää myös koulutusympäristön käytettävyyteen. Esimerkiksi työntekijä voi kokea käyttäjätunnusten luomisen ja kirjautumisen verkkokurssille hankalaksi. Rekisteröintiä ja kirjautumista varten tulee olla selkeät ja lyhyet ohjeet, jotta käyttäjä jaksaa ne lukea. Kirjallisten ohjeiden sijaan voidaan käyttää myös videoituja ohjeita. Vaihtoehtoisesti käyttäjätunnukset voidaan luoda valmiiksi etukäteen tai pohtia yhteiskäyttötunnusten käytön mahdollisuutta. Yhteiskäyttötunnusten haittapuolena on, ettei kurssisuorituksia voida yksilöidä käyttäjäkohtaisesti. Tällöin on mietittävä muita tapoja suoritusten seuraamiseksi. Lisäksi liikkuminen ja toiminnot verkko-oppimisympäristössä tulee olla selkeitä.

Vaikka verkkokoulutus olisi hyvin suunniteltu, koulutuksen tavoite ei täyty, mikäli työntekijä ei lue kurssimateriaalia. Syynä voivat olla esimerkiksi negatiivinen suhtautuminen koulutukseen. Velvollisuuden asettaminen koulutuksen suorittamiselle ei ole ratkaisu. Siksi koulutukseen tulee sisällyttää asioiden sisäistämistä mittaava tehtävä, esimerkiksi tentti, jolle on määritetty läpäisyraja. Läpäisyrajan lisäksi kurssisuorituksia tulee myös seurata.

Verkkokoulutus sopii todennäköisesti paremmin suppeaan, kuin laaja-alaiseen käyttöön, esimerkiksi erityisryhmien kouluttamiseen ja uusien työntekijöiden perehdytyskoulutuksiin. Mikäli tavoitteena on kouluttaa koko henkilöstö, kannattaa verkkokoulutus toteuttaa pienissä ryhmissä esimerkiksi osastokohtaisesti. Pientä ryhmää on helpompi hallinnoida ja motivoida, kuin suurta. Verkkokoulutus voi olla sopiva väline kouluttaa uudelle työntekijälle tietoturvallisuuden perusasiat, sillä työntekijälle ei ole vielä muodostunut henkilökohtaisia asenteita or-

ganisaation toimintatavoista. Lisäksi uusi työntekijä on luultavasti vanhoja työntekijöitä vastaanottavaisempi koulutusmuodon sekä koulutettavan asian suhteen.

# 6 Yhteenveto

Opinnäytetyöni aiheena oli tutkia henkilöstön tietoturvakoulutuksen toteuttamista valtionhallinnossa. Opinnäytetyön aihe on valtionhallinnossa ajankohtainen, sillä viranomaisilta edellytetään tietoturvallisuusasetuksen edellyttämän tietoturvallisuuden perustason täyttämistä 30.9.2013 mennessä. Tietoturvallisuuden perustason vaatimuksiin kuuluu muun muassa säännöllinen henkilöstön tietoturvakoulutus. Tietoturvakoulutuksella on keskeinen rooli henkilöstön tietoturvatietoisuuden edistämisessä ja sen myötä hyvän tiedonhallintatavan toteutumisessa.

Ensimmäisessä asettamassani tutkimuskysymyksessä oli kyse tietoturvakoulutukseen suunnitteluun ja toteutukseen liittyvistä vaiheista ja tekijöistä, jotka vaikuttavat vaiheiden osalta tehtäviin ratkaisuihin. Organisaatioissa ei aina ymmärretä tietoturvakoulutuksen suunnittelun merkitystä. Voi olla, ettei organisaatiossa toteuteta erillistä tietoturvakoulutusta, vaan aihetta käsitellään perehdytyksen tai muun turvallisuuskoulutuksen yhteydessä. Lisäksi riittävänä koulutuksena voidaan pitää organisaation Intranetiin vietyjä dokumentteja, jossa ne saattavat kuitenkin hukkua muiden dokumenttien joukkoon.

Opinnäytetyöni tutkimustuloksena syntynyt tietoturvakoulutuksen prosessimalli kuvaa selkeästi ja johdonmukaisesti kokonaisuutta, jonka ympärille tietoturvakoulutus rakentuu. Prosessimallista nähdään, että tietoturvakoulutuksen suunnittelu ja toteutus ovat laaja kokonaisuus, johon vaikuttavat erilaiset tekijät. Koulutuksen suunnitteluun ja toteutukseen vaikuttaa muun muassa se, millaisia resursseja organisaatiolla on käytettävissään tai millaisesta kohderyhmästä on kyse. Tietoturvakoulutus usein epäonnistuukin siitä syystä, ettei koulutuksen kohderyhmää tunneta tai sitä ei ole otettu riittävästi huomioon.

Prosessimalliin liittyvät jatkotutkimusaiheet voisivat liittyä nykytilanteen kartoitukseen ja henkilöstön motivointiin. Nykytilanteen kartoituksen osalta opinnäytetyössä voidaan tutkia tapaa toteuttaa nykytilanteen kartoitus. Tutkimuskysymyksinä voisivat olla ”Miten nykytilanteen kartoitus tulee toteuttaa?” sekä ”Millaisia osa-alueita kartoituksessa tulee käsitellä?”. Jatkotutkimusaihe on hyödyllinen, sillä nykytilanteen kartoitus vaikuttaa ratkaisuihin mitä kohderyhmälle tulee opettaa ja miten. Henkilökunnan motivointia käsittelevässä jatkotutkimuksessa voitaisiin tutkia motivointia henkilökunnan näkökulmasta. Motivaatio on tekijä, joka vaikuttaa viime kädessä siihen, osallistuuko työntekijä tietoturvakoulutukseen ja jos osallistuu, niin miten koulutukseen suhtaudutaan. Tutkimuskysymyksenä voisi olla ”Millaisia koulutusmuotoja organisaation työntekijät toivovat tietoturvakoulutukselta?”.

Toinen asettamani tutkimuskysymys käsitteli verkkokoulutuksen soveltuvuutta tietoturvakoulutukseen. Verkkokoulutus on koulutusmuotona kasvattanut suosiotaan organisaatioissa muun muassa kustannussäästösyistä. Lisäksi koulutusmuotoa pidetään helppona ja nopeana tapana toteuttaa tietoturvakoulutus laajemmallekin kohderyhmälle. Verkkokoulutuksen käyttö edellyttää samalla tavoin aikaa ja huolellista suunnittelua kuin perinteinen luokkakoulutus. Tämä saattaa unohtua erityisesti silloin, kun verkkokurssi hankintaan organisaation ulkopuolelta. Vaikka verkkokoulutuksen kokonaiskonsepti olisi valmiiksi suunniteltu, on verkko-oppimateriaali tärkeää räätälöidä organisaatiolle sopivaksi, jotta työntekijät tuntevat koulutuksen koskevan omaa organisaatiota eivätkä esimerkiksi koulutuksen tietoturvaohjeet ole ristiriidassa organisaation tietoturvaohjeiden kanssa.

Arvioin opinnäytetyössä verkkokoulutuksen soveltuvuutta tietoturvakoulutukseen. Tutkimustuloksena syntyneen olettamuksen mukaan verkkokoulutus soveltuu paremmin pienelle kuin suurelle kohderyhmälle. Verkko-opetusta käsittelevä alan kirjallisuus ei ottanut kantaa kerralla koulutettavana olevan kohderyhmän laajuuteen. Tutkimustuloksen olettamukseen päädyinkin valtionhallinnon organisaatioiden haastattelujen pohjalta. Tutkimustulosta voidaan pitää enemmänkin suuntaa antavana, sillä olettamus on johdettu kolmen organisaation kokemusten perusteella. Lisäksi olettamuksen paikkansapitävyys voidaan kyseenalaistaa sillä, valtionhallinnon organisaatioiden tietoturvakoulutukset olivat haastattelujen aikaan eri vaiheissa. Olettamus perustuu kahden organisaation käytännönkokemuksiin. Toisella organisaatiolla oli käytännönkokemusta koko henkilökunnan suorittamasta koulutuksesta, kun taas toisella organisaatiolla kokemukset perustuivat pilotointivaiheeseen. Kolmannen organisaation tietoturvakoulutus ei ollut vielä edennyt käytännön toteutukseen.

Verkkokoulusta koskevassa jatkotutkimusaiheessa voitaisiin tutkia henkilökunnan suhtautumista verkkokoulutuksena järjestettävään tietoturvakoulutukseen esimerkiksi kysely- tai haastattelututkimuksena. Toisaalta, koska kustannussäästöt ovat organisaatioilla keskeinen syy verkkokoulutuksen valinnalle, voisi jatkotutkimusaihe käsitellä koulutusmuodon käytöstä koituvia todellisia kustannussäästöjä. Tutkimuskysymyksenä voisi olla esimerkiksi ”Mistä verkkokoulutuksen kustannussäästöt syntyvät?”.

Opinnäytetyön tekeminen opetti minulle ihmisenä kärsivällisyyttä ja sopeutumista muuttuviin tilanteisiin. Opinnäytetyön tekeminen työelämän piirissä ei aina ole mutkatonta, eivätkä asiat ole aina opinnäytetyön tekijän itsensä käsissä. Asioiden eteneminen voi kestää tai tilanteet muuttua odottamattomasti. Tällöin opinnäytetyön tekijältä odotetaan kärsivällisyyttä ja kykyä sopeutua muuttuviin tilanteisiin. Opinnäytetyön tekeminen opetti minulle myös kykyä ajatella kriittisesti. Määritellessäni tutkimuskysymystä verkkokoulutuksen soveltuvuuteen liittyen, olin jo muodostanut henkilökohtaisen mielipiteen koulutusmuodosta. Tuolloin ajattelin, että verkkokoulutus on hyvä koulutusmuoto siinä missä perinteinen luokkahuonekoulutus,

kunhan koulutusmateriaali on laadukasta. Opinnäytetyön edetessä tuo käsitys muuttui: en ollut ymmärtänyt kuinka laajasta kokonaisuudesta koulutuksen suunnittelussa ja toteuttamisessa onkaan kyse.

Tunnen päässeeni asettamiini henkilökohtaisiin tavoitteisiin, jotka olivat kehittyminen asiantuntijana sekä luominen työn lopputuloksena jotain, josta on työelämälle hyötyä. Vaikka en koe luoneeni varsinaisesti uutta tietoa, olen tyytyväinen tutkimustuloksena syntyneeseen prosessimalliin. Rakentaessani teoreettista kehystä, en löytänyt aihetta käsittelevästä kirjallisuudesta viitteitä vastaavanlaisen mallin olemassaolosta.

Tähän lopuksi haluan vielä kiittää haastateltavina olleita valtionhallinnon organisaatioiden edustajia, sekä Valtiokonttorissa toimivan Valtion IT-palvelukeskuksen tietoturvaryhmää. Kiitos tietoturva-asiantuntija Kirsi Janhuselle opinnäytetyön ohjaamisesta työelämän puolelta sekä kannustuksesta saattaa opinnäytetyö valmiiksi. Erityiskiitoksen haluan lausua johtavalle tietoturva-asiantuntijalle Antti Laulajaiselle opinnäytetyön aikana saamastani tuesta, ohjauksesta ja sparrauksesta tämän kuluneen vuoden aikana.

Lähteet

Aarreniemi-Jokipelto, P. 2011. Kohti yhteisöllisen ja henkilökohtaisen oppimisen tilaa sosiaalisen median välinein. Teoksessa Ihanainen, P., Kalli, P. & Kiviniemi, K. (toim.) Sosiaalinen media ja verkostoituminen. Helsinki: Okka

Alamäki, A. & Luukkonen, J. 2002. eLearning - Osaamisen kehittämisen digitaaliset keinot: strategia, sisällöntuotanto, teknologia ja käyttöönotto. Helsinki: Edita

Burgess, J. & Russell, J. 2003. The effectiveness of distance learning initiatives in organizations. Journal of Vocational Behavior. Viitattu 25.7.2012. Saatavilla http://www.qou.edu/arabic/researchProgram/distanceLearning/effectivenessDistance.pdf

Chapple, M., Gibson, D. & Stewart, J. 2012. CISSP: Certified Information Systems Security Professional - Study Guide. Ca: Sybex

Cohen, K. 2009. Evaluating the Effectiveness of Regulatory Training and Awareness Solutions. Viitattu 24.9.2012. http://www.fifth-business.co.uk/TrainingEval.pdf

DelVecchio, K. & Loughney M. 2006. E-Learning Concepts and Techniques. Viitattu 8.8.2012. http://iit.bloomu.edu/Spring2006_eBook_files/ebook_spring2006.pdf

Downes, S. 2005. E-learning 2.0. eLearn Magazine: Education and Technology in Perspective. Viitattu 19.11.2012. http://elearnmag.acm.org/featured.cfm?aid=1104968

Felder, R. & Henriques, E. 1995. Learning and Teaching Styles in Foreign and Second Launguage Education. Foreign Language Annals. 28. No. 1, 1995. Viitattu 10.8.2012. http://www4.ncsu.edu/unity/lockers/users/f/felder/public/Papers/FLAnnals.pdf

Frank, M. & Liebowitz, J. 2011. Knowledge Management and E-learning. Boca Raton: Auerbach Publications

Hanelius, P., Kanerva, L. & Merikanto, N. 2002. Verkko-oppiminen valtionhallinnossa. Valtiovarainministeriö. Tutkimukset ja selvitykset 1/2002. Viitattu 31.8.2012. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/06_valtion_tyomarkkinalaitos/9305/9294_fi.pdf

Hash, J. & Wilson, M. 2003. National Institute of Standards and Technology. Building an Information Technology Security Awareness and Training Program. SP 800-50. Viitattu 2.4.2012. http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

Herold, R. 2011. Managing an Information Security and Privacy Awareness and Training Program. US: Auerbach Publications

Hintikka, K. A. 2007. Web 2.0 - johdatus internetin uusiin liiketoimintamahdollisuuksiin. Helsinki: TIEKE Tietoyhteiskunnan kehittämiskeskus

Hosio, M. & Rissanen, K. 2004. Verkkokussien hankinta ja käyttöönotto. Käsikirja. Hämeenlinna: Hämeen ammattikorkeakoulu

Hyötyniemi, Y., Ilomäki, L., Kiesi, E., Koskinen, K., Leinonen, A., Lind, L., Mattsson, O., Nummi, T., Puro, H., Rannikko, S., Salmio, K., Sankila, T., Sirola, R., Sumkin, T., von Nandelstadh, M. & Wulff, A. 2005. Verkko-oppimateriaalin laatukriteerit. Työryhmän raportti. Viitattu 24.8.2012. http://www.edu.fi/download/47132_verkko-oppimateriaalin_laatukriteerit.pdf

Häkkinen, P., Järvelä, S. & Lehtinen, E. 2006. Oppimisen teoria ja teknologian opetuskäyttö. Porvoo: WSOY Oppimateriaalit

Hämäläinen, E. & Jaakkola, M. 2007. Verkko-opettajan nettiopas. Viitattu 17.4.2012. http://lukiot.tampere.fi/seututarjotin/vopas/index.php?sivu=3

Ippolito, J., Pitcher, S., Tressler, J., Wilson, M. & de Zafra D. 1998. National Institute of Standards and Technology. Information Technology Security Training Requirements: A Role- and Performance-Based Model. SP 800-16. Viitattu 2.4.2012. http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf

Kajannes, K. & Kirstinä, L. 2000. Kirjallisuus, kieli ja kognitio: kognitiivisesta kirjallisuuden- ja kielentutkimuksesta. Helsinki: Yliopistopaino

Kalliala, E. 2002. Verkko-opettamisen käsikirja. Helsinki: Finn Lectura

Kanerva, K., Lehtinen, A., Löfström, E., Nevgi, A. & Tuuttila, L. 2006. Laadukkaasti verkossa: Verkko-opetuksen käsikirja yliopisto-opettajalle. Viitattu: 20.9.2012. http://www.helsinki.fi/julkaisut/aineisto/hallinnon_julkaisuja_33_2006.pdf

Keränen, V. & Penttinen, J. 2007. Verkko-oppimateriaalin tuottajan opas. Jyväskylä: WSOY-pro

Kiviniemi, K. 2000. Johdatus verkkopedagogiikkaan. Kokkola: Keski-Pohjanmaan ammattikorkeakoulu

Koponen, S., Lehtinen, M., Myllyharju, K., Nurkka, A., Salojärvi, H., Talikka, M., Tapola, V., Vanhainen, M. & Kotivirta, S. 2011. Opiskelun ja oppimisen opas - kuinka opiskelen laadukkaasti LUT:ssa. Viitattu 13.8.2012. http://www.lut.fi/fi/lut/introduction/quality/qualitybook/Documents/opiskelijan_laatuopas_suomi.pdf

Krause, M. & Tipton, H. 2009. Information Security Management Handbook. Volume 3. US: Auerbach Publications

Lahikainen, A. & Pirttilä-Backman, A-M. 2006. Sosiaalipsykologian perusteet. Helsinki: Otava

Laki viranomaisen toiminnan julkisuudesta 621/1999. Viitattu 12.9.2012. http://www.finlex.fi/fi/laki/ajantasa/1999/19990621

Manninen, J. & Matikainen, J. Aikuiskoulutus verkossa: verkkopohjaisten oppimisympäristöjen teoriaa ja käytäntöä. Lahti: Helsingin yliopiston Lahden tutkimus- ja koulutuskeskus

Mattord, H. & Whitman, M. 2010. Management of Information Security. Boston, MA: Course Technology Cengage Learning

Mäkinen, P. 2002. Verkko-tutor. Mitä on oppiminen?. Viitattu 18.11.2012. http://www.uta.fi/tyt/verkkotutor/oppimin.htm

Mäkitalo, E. & Wallinheimo, K. 2012. Virtuaaliset ympäristöt: Innostava oppiminen, tehokas koulutus. Helsinki: Talentum

Mänty, I. & Nissinen, P. 2005. Ideasta toteutukseen - verkko-opetuksen suunnittelu ja hallinta. Helsinki: Edita

Nevgi, A. & Tirri, K. 2003. Hyvää verkko-opetusta etsimässä. Turku: Suomen kasvatustieteellinen seura

Niemi, H. 2001. Vahvaksi verkossa - kohti itseohjautuvuutta ja oppimisen taitoja. Viitattu 20.8.2012. https://www.edu.helsinki.fi/svy/kvanti/mittavaline/mat/vahvaksi_verkossa.pdf

NIST. 1995. National Institute of Standards and Technology. An Introduction to Computer Security: The NIST Handbook. SP 800-12. Viitattu 1.4.2012.
http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf
Nurmela, S. & Suominen, R. 2011. Verkko-opettaja. Helsinki: WSOYpro

Nurmi, H. 2011. Onko virtuaalimaailmassa helpompi muuttua kuin tavallisessa? Teoksessa Ihanainen, P., Kalli, P. & Kiviniemi, K. (toim.) Sosiaalinen media ja verkostoituminen. Helsinki: Okka

Nykänen, K. 2011. Tietoturvakoulutuksen vaikuttavuuden arviointi yksilön ja organisaation tietoturvakäyttäytymiseen. Tampere: Oulun Yliopisto, luonnontieteiden tiedekunta, tietojenkäsittelytieteiden laitos

Peltier, T. 2005. Implementing an Information Security Awareness Program. Viitattu 4.4.2012.
http://www.infosectoday.com/IT%20Today/Peltier_awareness.pdf

Puhakainen, P. 2006. A Design Theory for Information Security Awareness. Oulu: Oulun Yliopisto, luonnontieteiden tiedekunta, tietojenkäsittelytieteiden laitos
Pälli, P. 2003. Ihmisryhmä diskurssissa ja diskurssina. Akateeminen väitöskirja. Tampere: Tampereen yliopistopaino. Viitattu 17.8.2012. http://acta.uta.fi/pdf/951-44-5580-0.pdf

Rauste-von Wright, M., von Wright, J. & Soini, T. 2003. Oppiminen ja koulutus. Helsinki: WSOY

Saarinen, J. 2005. eValuator - Digitaalisten oppimateriaalien, oppimisympäristöjen ja mobiilioppimisen menetelmien arviointi. Viitattu 24.8.2012.
http://portal.hamk.fi/portal/page/portal/HAMKJulkisetDokumentit/Yleisopalvelut/Julkaisupalvelut/Kirjat/opetus_ohjaus_ja_osaaminen/eValuator.pdf

Schott, F. & Driscoll, M. 1997. On the Architectonics of Instructional Theory. US: Lawrence Erlbaum Associates

Tenno, T. 2011. Surffaajat ja syventyjät - verkko-oppimisympäristön pedagogisen rakenteen ja opiskelijoiden toimintaorientaatioiden tarkastelua. Rovaniemi: Lapin yliopistokustannus

VAHTI 6/2003. Opas julkishallinnon tietoturvakoulutuksen järjestämisestä. Valtionhallinnon tietoturvallisuuden johtoryhmä. Viitattu 12.9.2012.
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53763/53760_fi.pdf

VAHTI 11/2006. Tietoturvakouluttajan opas. Valtionhallinnon tietoturvallisuuden johtoryhmä. Viitattu 10.4.2012.
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20061128Tietot/Vahti_11_06.pdf

VAHTI 2/2010. Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. Valtionhallinnon tietoturvallisuuden johtoryhmä. Viitattu 12.9.2012.
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101028Ohjeti/02_Ohje_tietotuvallisuudesta_valtionhallinnossa.pdf

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa. 681/2010. Viitattu 12.9.2012.
http://www.finlex.fi/fi/laki/alkup/2010/20100681

Julkaisemattomat lähteet

Laulajainen, A. 2012. Johtava tietoturva-asiantuntija. Valtion IT-palvelukeskus. Henkilökohtainen tiedoksianto 2.10.2012.

Kuvat

Taulukot

Liitteet

Liite 1 Organisaatio B:n tietoturvakyselyn tulokset

Valtionhallinnon organisaatio B toteutti pienimuotoisen mielipidekyselyn kartoittaakseen henkilökuntansa suhtautumista ja asenteita tietoturvallisuutta kohtaan. Tietoturvakyselyn tavoitteena oli tunnistaa tietoturvallisuuden kehittämistarpeita erityisesti tietoturvakoulutuksen osalta – mitä tietoturvalliseen työskentelyyn liittyviä asioita tulevaisuudessa järjestettävissä tietoturvakoulutuksissa tulisi korostaa.

Tietoturvakysely jaettiin kahteen osa-alueeseen: yleisesti tietoturvallisuus ja tietoturvakäyttäytyminen. Yleisesti tietoturvallisuutta käsittelevät kysymyksissä kysyttiin muun muassa johdon sitoutumisesta tietoturvallisuuteen, henkilökohtaisen tuen saamisesta tietoturva-asioissa sekä tietoturvakoulutuksen järjestämisen tärkeydestä. Tietoturvakäyttäytymistä kartoittavassa osiossa kysymykset laadittiin periaatteella ”organisaation tärkeimmät tietoturvaohjeet työntekijälle”. Kysymykset haluttiin pitää perusasioissa, sillä ne muodostavat perustan tietoturvalliselle työskentelylle. Henkilöstölle esitettiin seuraava kysymykset:

**Yleinen tietoturvallisuus**

1. Työntekijät noudattavat organisaation tietoturvaohjeita
2. Johto kehittää ja arvioi tietojen ja asiakirjojen käsittelyn turvallisuutta
3. Tietoturva-asiat ovat osa perehdytystä
4. Tietoturva-asioissa saa tarvittaessa henkilökohtaista tukea
5. Organisaatio järjestää tietoturvakoulutusta
6. Tietoturvakoulutukseen osallistuu koko henkilöstö
7. Tietoturvakoulutus järjestetään perinteisenä luokkaopetuksena

**Tietoturvakäyttäytyminen**

8. Tietoaineistoja käsitellään sellaisissa ympäristöissä, jotka on toteutettu tarvittavan suojaustason mukaisesti (riittävä käyttäjähallinta, salaus jne.)
9. Tärkeistä tietoaineistoista otetaan varmuuskopiot
10. Eri tietojärjestelmissä ei käytetä samoja salasanoja
11. Tietojärjestelmissä käytetään sellaisia salasanoja, joita ei ole helppo arvata (esim. erikoismerkit, pituus, numerot)
12. Käyttäessä Internetiä työnantajan välineillä, noudatetaan varovaisuutta (esim. tietokoneelle ei saa ladata ohjelmia)
13. Henkilökohtaista salasanaa ei luovuteta muille, edes IT-tuelle
14. Työasema lukitaan poistuessa työpisteeltä
15. Toimitiloissa ei liiku ulkopuolisia ilman valvontaa

16. Salassa pidettävissä keskusteluissa huolehditaan siitä, etteivät ulkopuoliset kuule niitä
17. Työpisteessä huolehditaan ”puhtaan pöydän” – periaatteesta (esim. pöydälle ei jätetä salassa pidettävää tietoaineistoa asiattomien ulottuville tai nähtäville)
18. Työasioiden hoitamiseen ei käytetä yksityistä sähköpostiosoitetta
19. Salassa pidettäviä tietoaineistoja ei luovuteta ulkopuolisille
20. Salassa pidettävät tietoaineistot hävitetään ohjeiden mukaisesti

Työntekijöiden tuli arvioida kuinka tärkeäksi he kokevat kysymyksen käyttämällä seuraavaa asteikkoa:

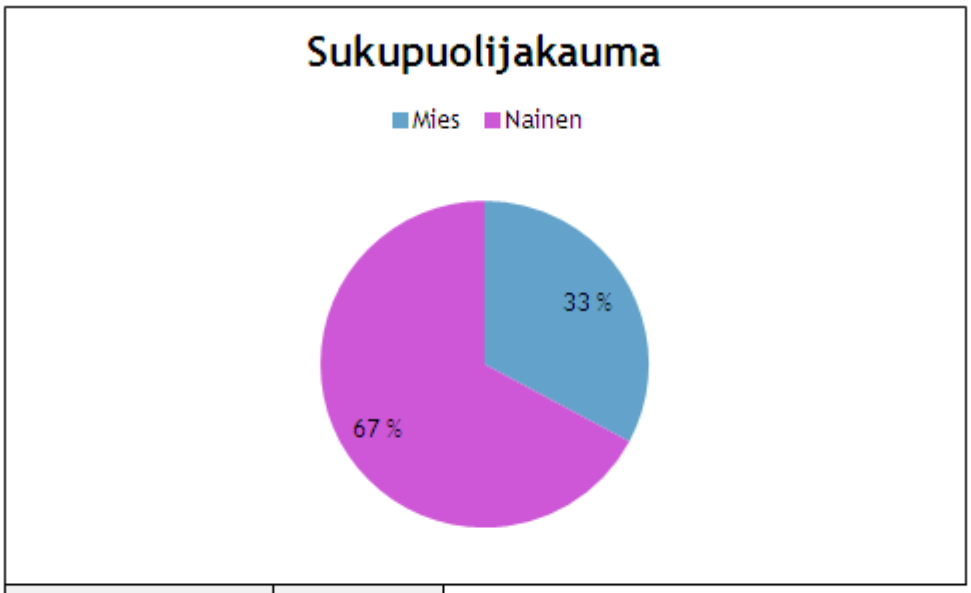
5 = Erittäin tärkeää
4 = Tärkeää
3 = Osittain tärkeää
2 = Ei kovin tärkeää
1 = Ei lainkaan tärkeää

Tietoturvakysely laadittiin Digium Enterprise – ohjelmistolla ja kysely julkaistiin 24. tammikuuta 2012. Organisaation henkilökunnalle lähetettiin sähköpostiviesti ennakkotietona tulevasta tietoturvakoulutuksen verkkokoulutuksesta, jonka yhteyteen liitettiin linkki tietoturvakyselyyn. Tietoturvallisuuden verkkokurssi julkaistiin muutama viikko myöhemmin, jonka jälkeen kyselyyn pääsi vastaamaan sähköpostiviestin lisäksi myös verkkokurssin kautta. Kysely suljettiin 7. elokuuta 2012.

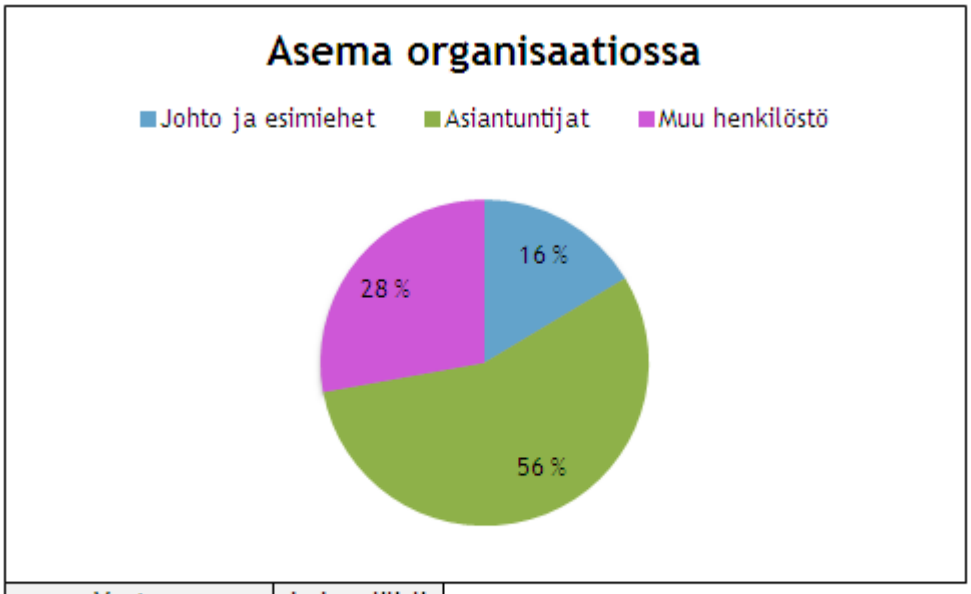
Seuraavissa taulukoissa on esitetty tietoturvakyselyn tulokset. Ensimmäisessä osiossa on esitetty kyselyyn vastanneiden taustatiedot: sukupuoli, asema organisaatiossa ja palvelusuhteen kesto. Toisessa osiossa on esitetty vastauksien prosentuaalinen jakautuminen eli kuinka tärkeäksi vastaajat kokivat kysymyksessä esitetyn asian. Kolmanteen osioon on koottu henkilöstöryhmittäin (johto ja esimiehet, asiantuntija, muu henkilöstö) vastauksien keskiarvot.

**Taustatiedot**

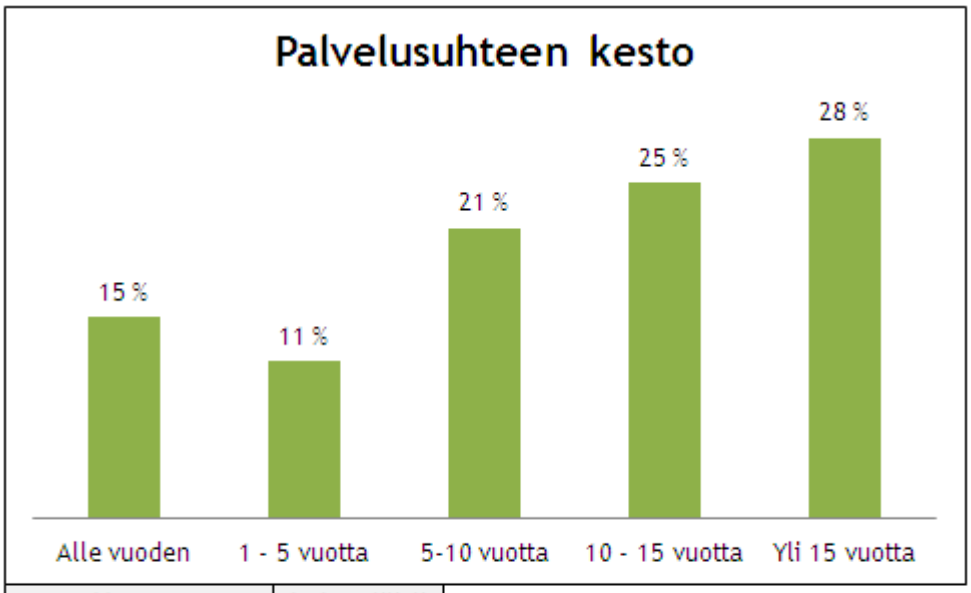
Kyselyyn vastasi yhteensä 61 työntekijää. Vastaajista naisia oli 41 (67 %) ja miehiä 20 (33 %). Yli puolet, 34 vastaajaa (56 %), työskentelee organisaatiossa asiantuntijana. Vastaajista 17 työntekijää (28 %) kuuluu muuhun henkilökuntaan ja 10 (16 %) toimii johto- tai esimiestehtävissä. Eniten vastaajista, 17 työntekijää (28 %), oli vastaushetkellä työskennellyt organisaatiossa yli 15 vuotta, 15 työntekijää (25 %) kymmenestä viiteentoista vuotta ja 13 vastaajaa (21 %) viidestä kymmeneen vuotta. Yhdestä viiteen vuotta työskennelleitä oli 7 (11 %). Alle vuoden organisaatiossa oli työskennellyt 9 vastaajaa (15 %).




| Vastaus | Lukumäärä |
|---|---|
| Mies | 20 |
| Nainen | 41 |



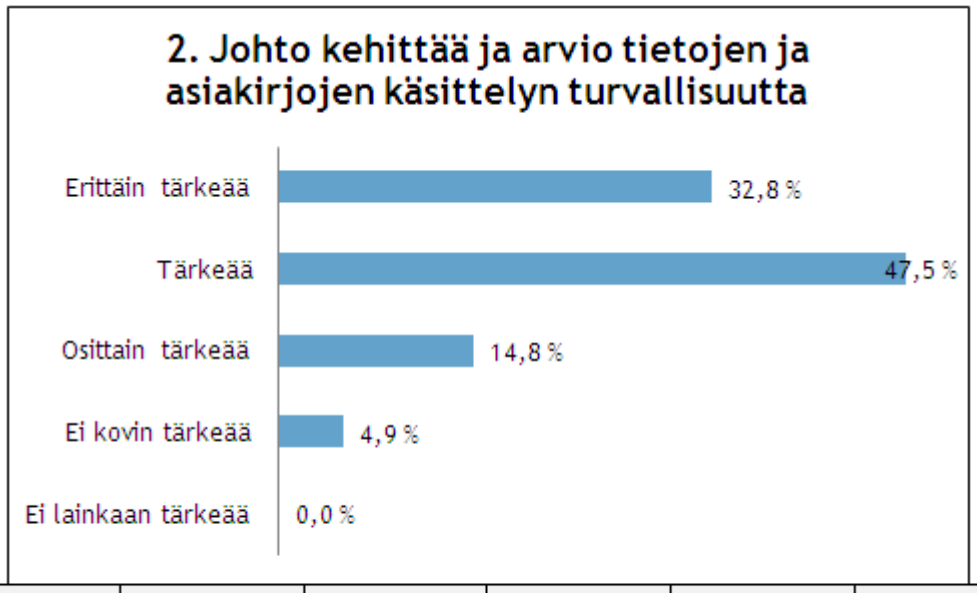

| Vastaus | Lukumäärä |
|---|---|
| Johto ja esimiehet | 10 |
| Asiantuntijat | 34 |
| Muu henkilöstö | 17 |



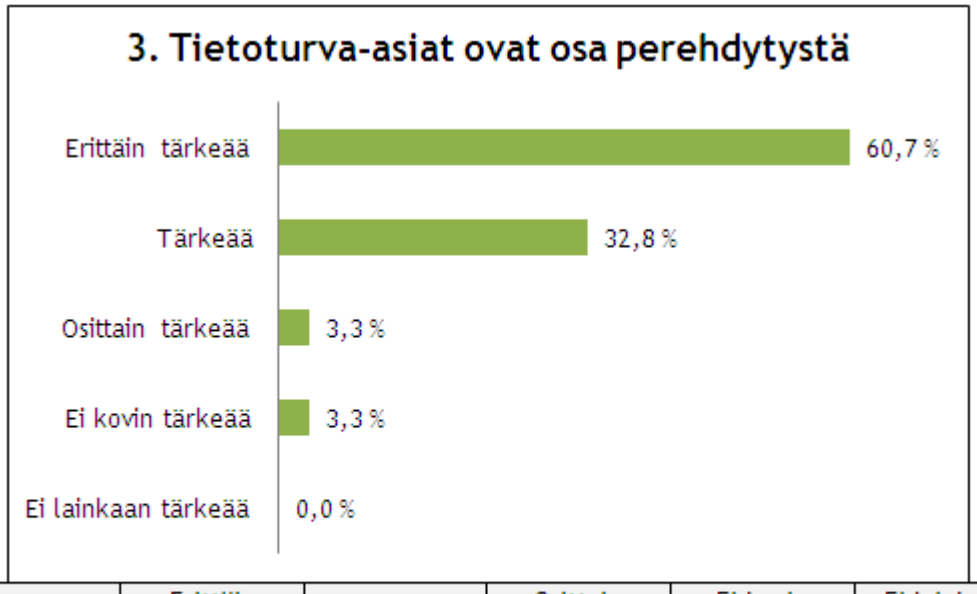

| Vastaus | Lukumäärä |
|---|---|
| Alle vuoden | 9 |
| 1 - 5 vuotta | 7 |
| 5 - 10 vuotta | 13 |
| 10 - 15 vuotta | 15 |
| Yli 15 vuotta | 17 |

**Vastausten prosentuaalinen jakautuminen**


| N = 61 | Erittäin tärkeää | Tärkeää | Osittain tärkeää | Ei kovin tärkeää | Ei lainkaan tärkeää |
|---|---|---|---|---|---|
| Vastausten lukumäärä: | 40 | 16 | 3 | 1 | 1 |

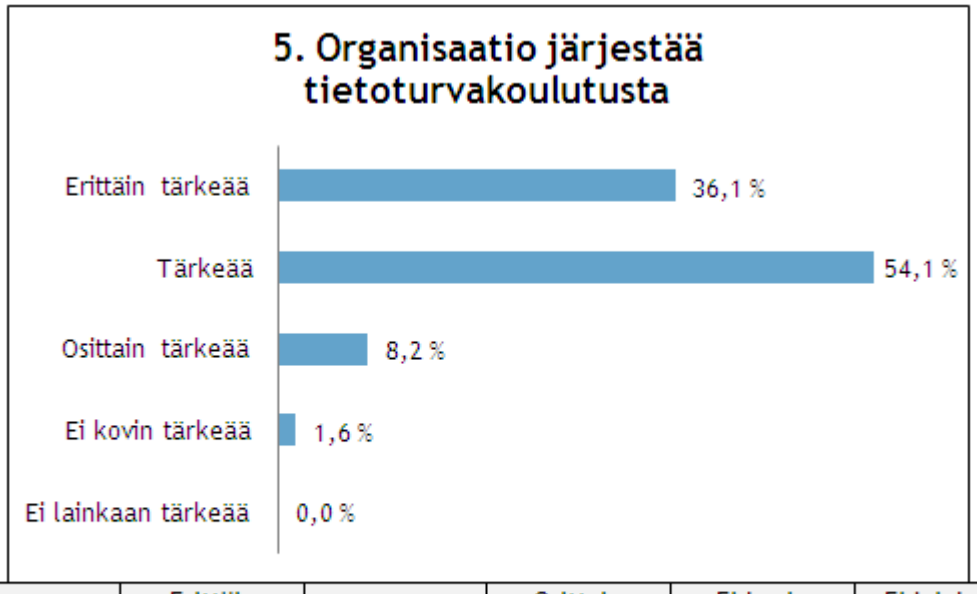



| N = 61 | Erittäin tärkeää | Tärkeää | Osittain tärkeää | Ei kovin tärkeää | Ei lainkaan tärkeää |
|---|---|---|---|---|---|
| Vastausten lukumäärä: | 20 | 29 | 9 | 3 | 0 |

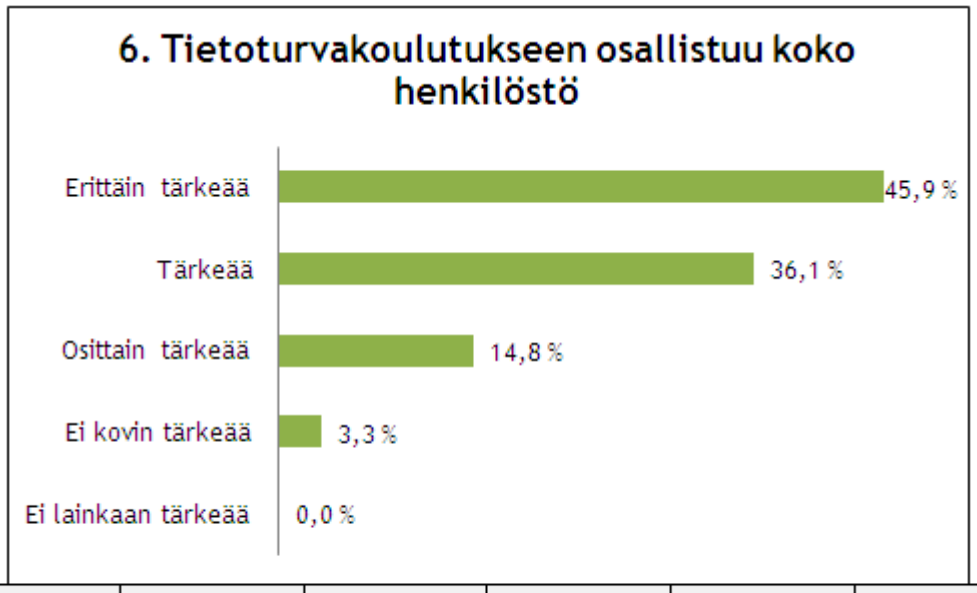



| N = 61 | Erittäin tärkeää | Tärkeää | Osittain tärkeää | Ei kovin tärkeää | Ei lainkaan tärkeää |
|---|---|---|---|---|---|
| Vastausten lukumäärä: | 37 | 20 | 2 | 2 | 0 |

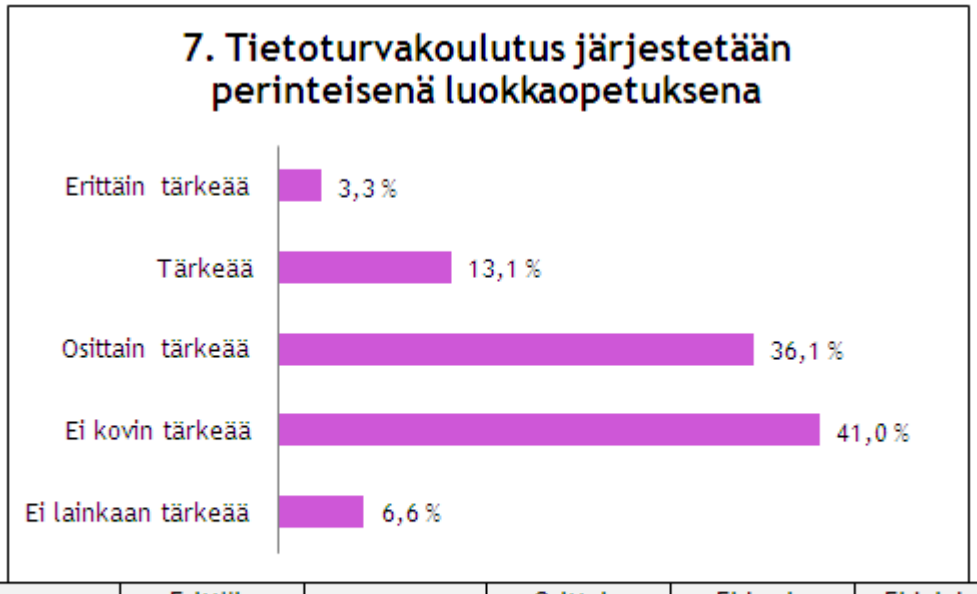

| N = 61 | Erittäin tärkeää | Tärkeää | Osittain tärkeää | Ei kovin tärkeää | Ei lainkaan tärkeää |
|---|---|---|---|---|---|
| Vastausten lukumäärä: | 28 | 28 | 4 | 1 | 0 |



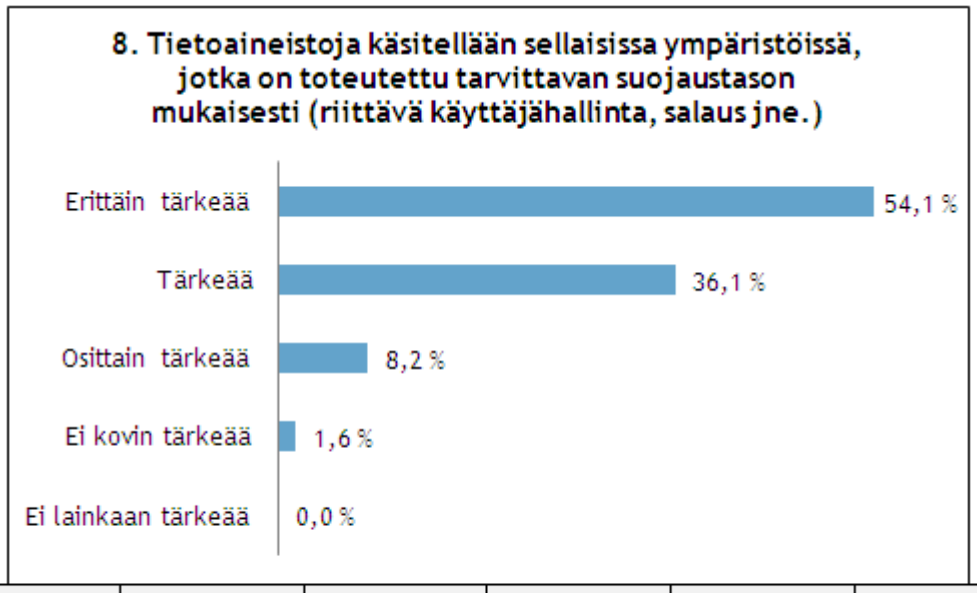

| N = 61 | Erittäin tärkeää | Tärkeää | Osittain tärkeää | Ei kovin tärkeää | Ei lainkaan tärkeää |
|---|---|---|---|---|---|
| Vastausten lukumäärä: | 22 | 33 | 5 | 1 | 0 |




| N = 61 | Erittäin tärkeää | Tärkeää | Osittain tärkeää | Ei kovin tärkeää | Ei lainkaan tärkeää |
|---|---|---|---|---|---|
| Vastausten lukumäärä: | 28 | 22 | 9 | 2 | 0 |

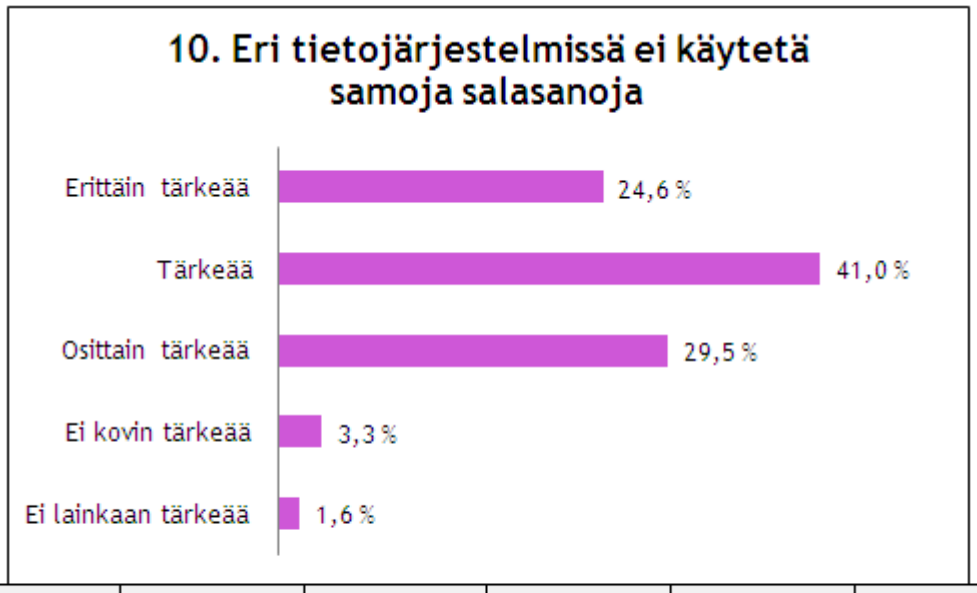



| N = 61 | Erittäin tärkeää | Tärkeää | Osittain tärkeää | Ei kovin tärkeää | Ei lainkaan tärkeää |
|---|---|---|---|---|---|
| Vastausten lukumäärä: | 2 | 8 | 22 | 25 | 4 |

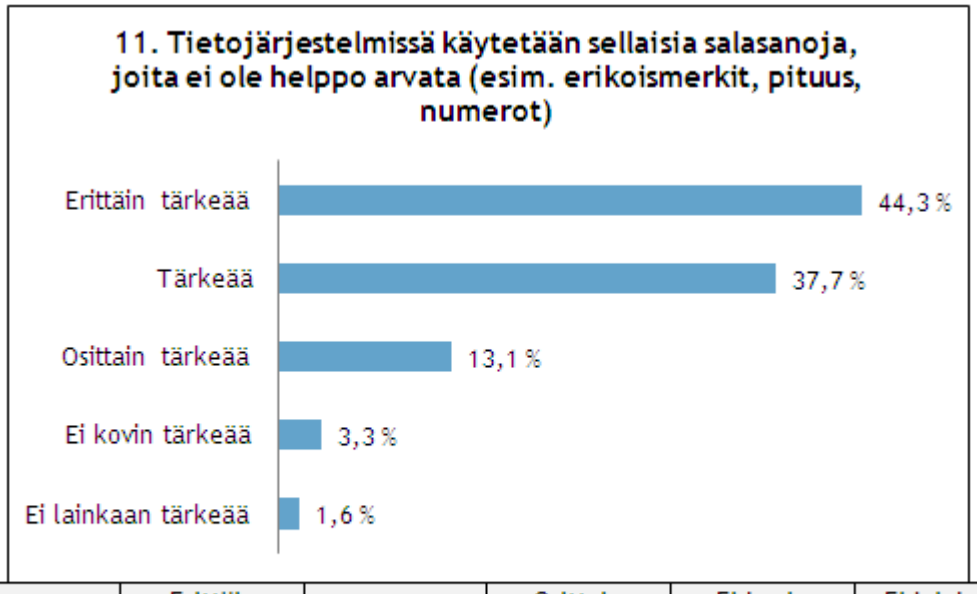



| N = 61 | Erittäin tärkeää | Tärkeää | Osittain tärkeää | Ei kovin tärkeää | Ei lainkaan tärkeää |
|---|---|---|---|---|---|
| Vastausten lukumäärä: | 33 | 22 | 5 | 1 | 0 |


| N = 61 | Erittäin tärkeää | Tärkeää | Osittain tärkeää | Ei kovin tärkeää | Ei lainkaan tärkeää |
|---|---|---|---|---|---|
| Vastausten lukumäärä: | 35 | 21 | 3 | 2 | 0 |

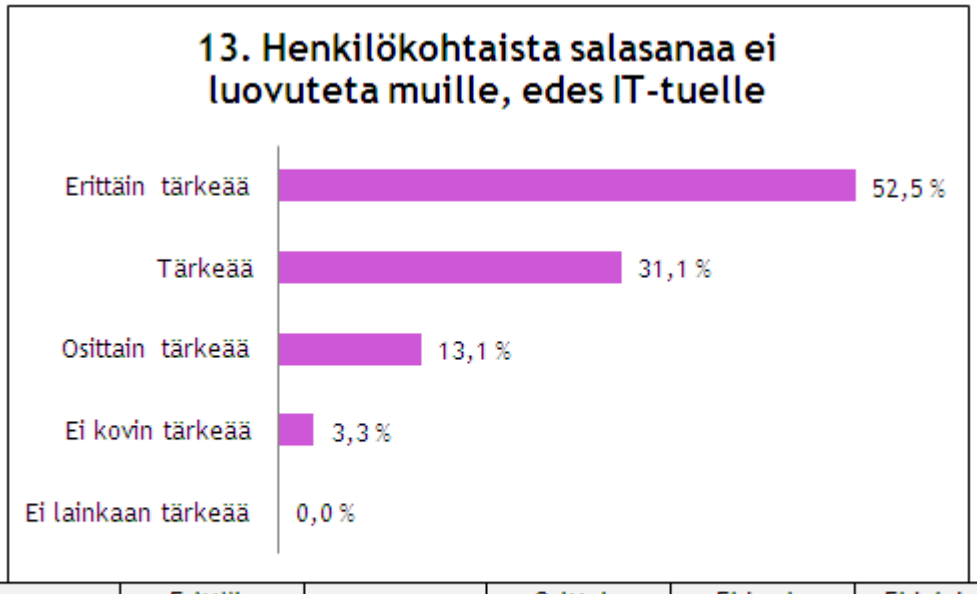



| N = 61 | Erittäin tärkeää | Tärkeää | Osittain tärkeää | Ei kovin tärkeää | Ei lainkaan tärkeää |
|---|---|---|---|---|---|
| Vastausten lukumäärä: | 15 | 25 | 18 | 2 | 1 |

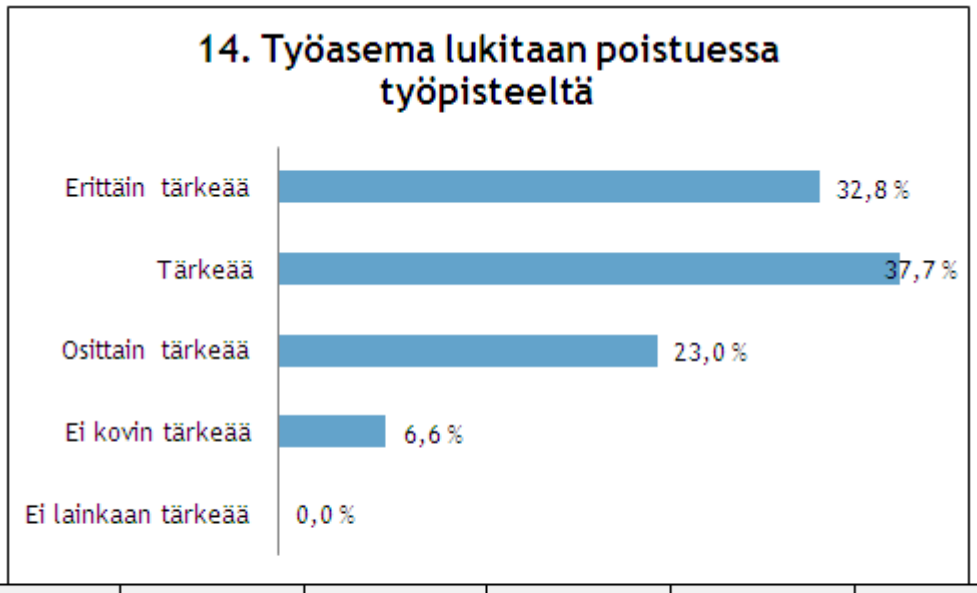



| N = 61 | Erittäin tärkeää | Tärkeää | Osittain tärkeää | Ei kovin tärkeää | Ei lainkaan tärkeää |
|---|---|---|---|---|---|
| Vastausten lukumäärä: | 27 | 23 | 8 | 2 | 1 |

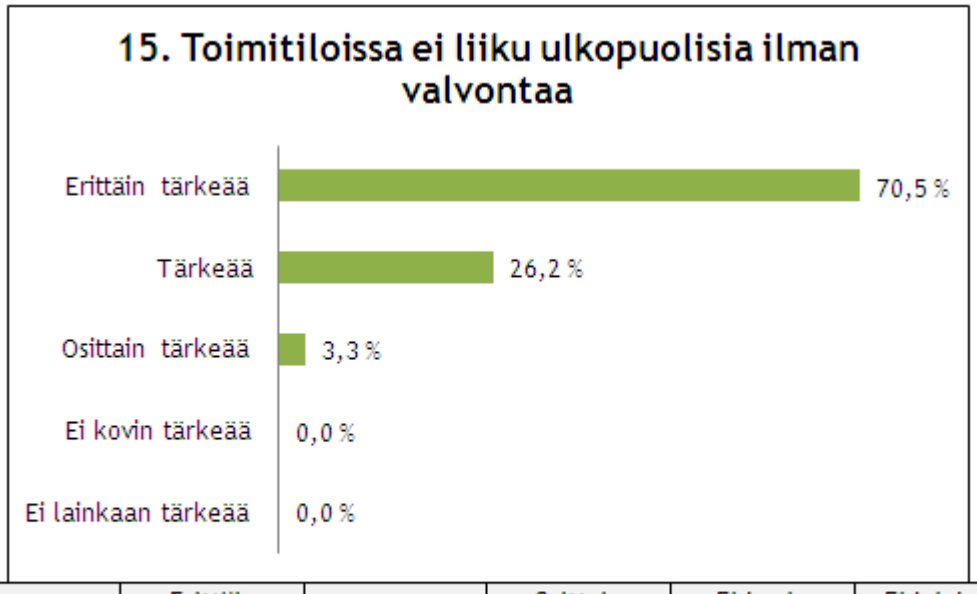

| N = 61 | Erittäin tärkeää | Tärkeää | Osittain tärkeää | Ei kovin tärkeää | Ei lainkaan tärkeää |
|---|---|---|---|---|---|
| Vastausten lukumäärä: | 28 | 26 | 6 | 1 | 0 |



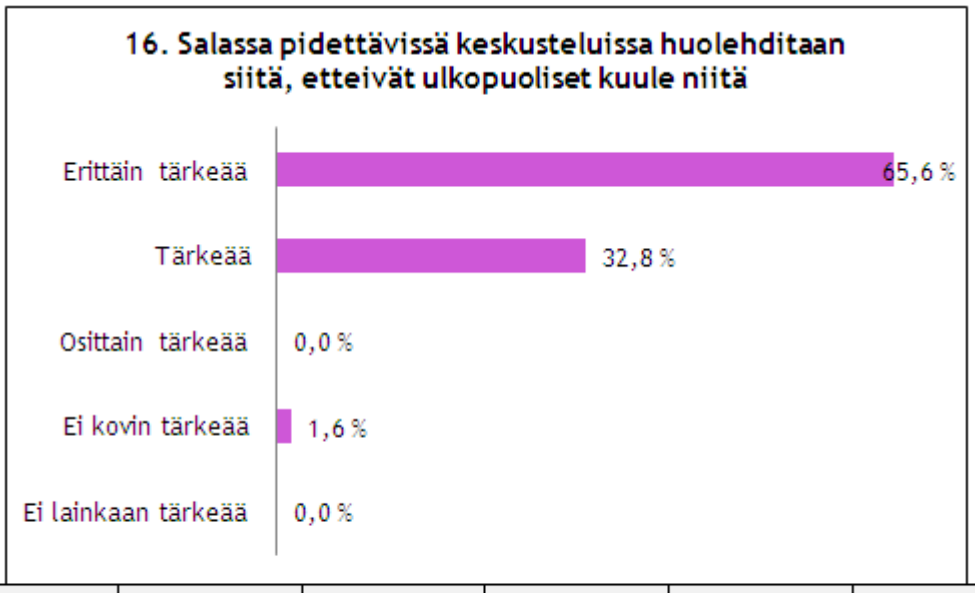

| N = 61 | Erittäin tärkeää | Tärkeää | Osittain tärkeää | Ei kovin tärkeää | Ei lainkaan tärkeää |
|---|---|---|---|---|---|
| Vastausten lukumäärä: | 32 | 19 | 8 | 2 | 0 |



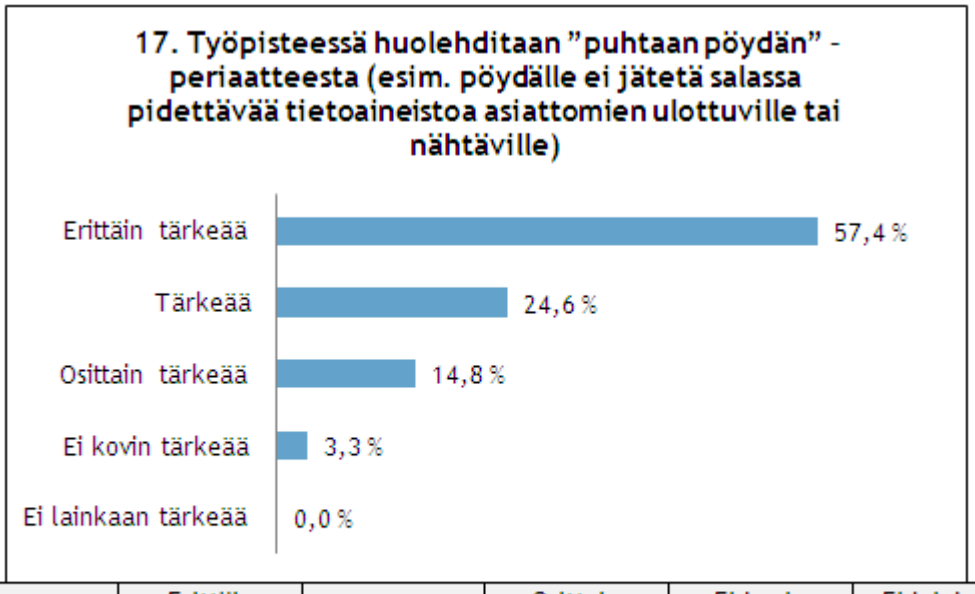

| N = 61 | Erittäin tärkeää | Tärkeää | Osittain tärkeää | Ei kovin tärkeää | Ei lainkaan tärkeää |
|---|---|---|---|---|---|
| Vastausten lukumäärä: | 20 | 23 | 14 | 4 | 0 |



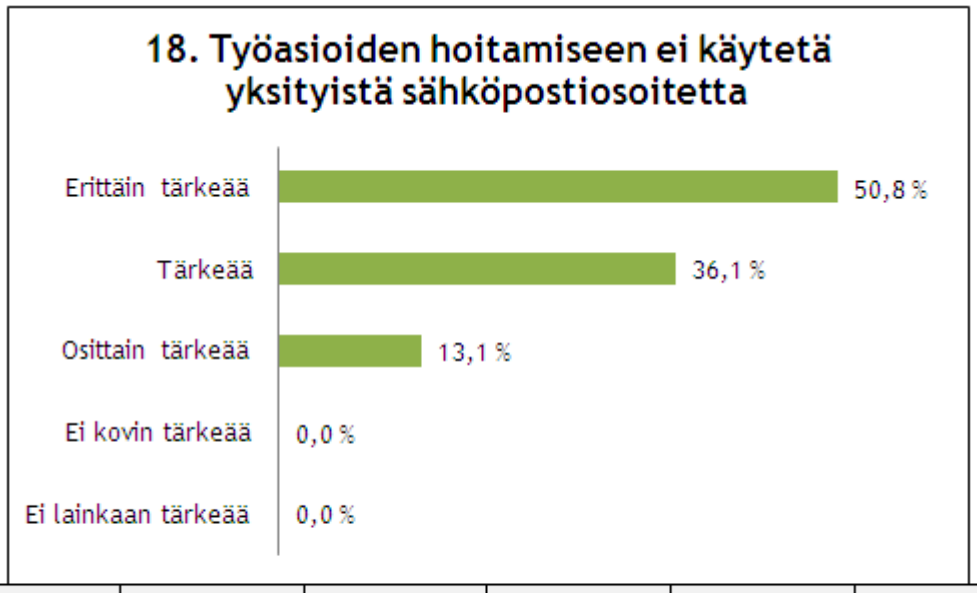

| N = 61 | Erittäin tärkeää | Tärkeää | Osittain tärkeää | Ei kovin tärkeää | Ei lainkaan tärkeää |
|---|---|---|---|---|---|
| Vastausten lukumäärä: | 43 | 16 | 2 | 0 | 0 |




| N = 61 | Erittäin tärkeää | Tärkeää | Osittain tärkeää | Ei kovin tärkeää | Ei lainkaan tärkeää |
|---|---|---|---|---|---|
| Vastausten lukumäärä: | 40 | 20 | 0 | 1 | 0 |




| N = 61 | Erittäin tärkeää | Tärkeää | Osittain tärkeää | Ei kovin tärkeää | Ei lainkaan tärkeää |
|---|---|---|---|---|---|
| Vastausten lukumäärä: | 35 | 15 | 9 | 2 | 0 |



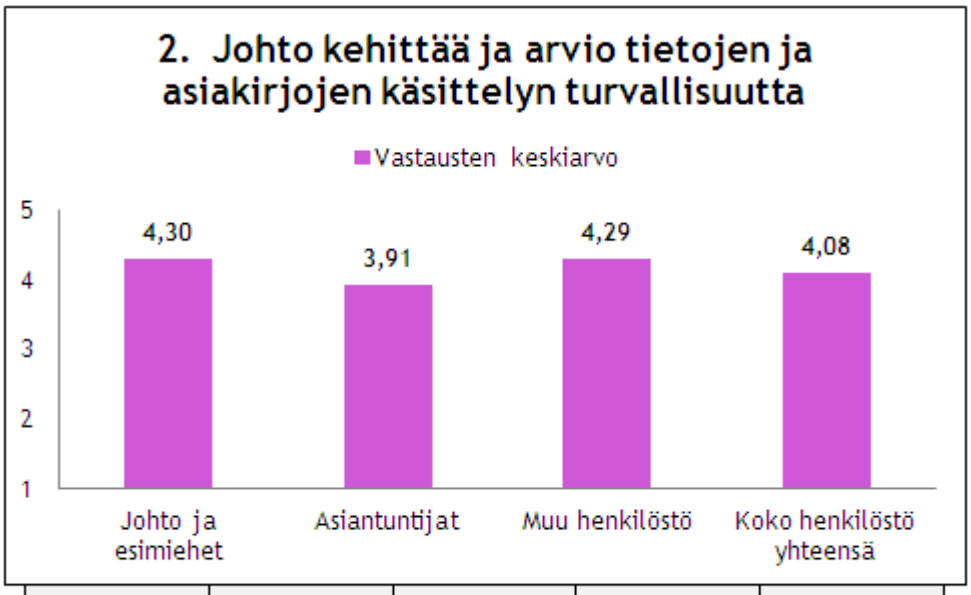

| N = 61 | Erittäin tärkeää | Tärkeää | Osittain tärkeää | Ei kovin tärkeää | Ei lainkaan tärkeää |
|---|---|---|---|---|---|
| Vastausten lukumäärä: | 31 | 22 | 8 | 0 | 0 |

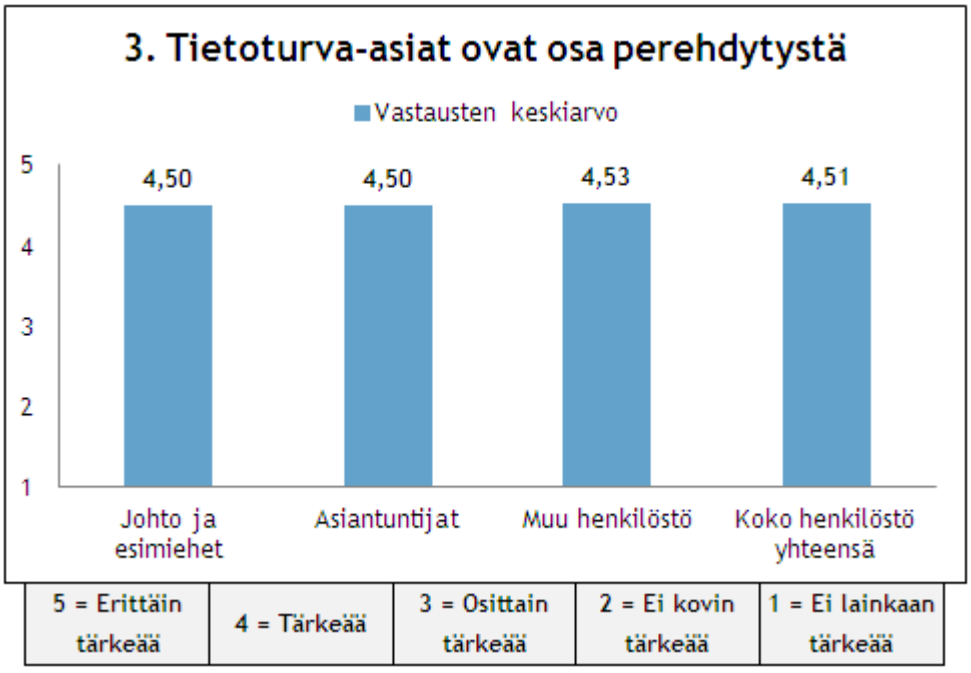

| N = 61 | Erittäin tärkeää | Tärkeää | Osittain tärkeää | Ei kovin tärkeää | Ei lainkaan tärkeää |
|---|---|---|---|---|---|
| Vastausten lukumäärä: | 55 | 5 | 1 | 0 | 0 |

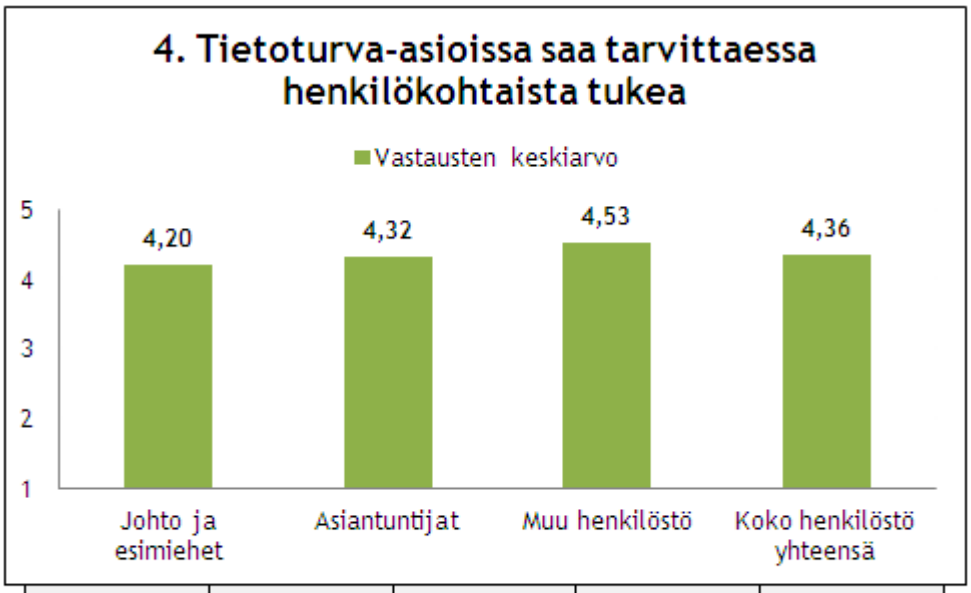

| N = 61 | Erittäin tärkeää | Tärkeää | Osittain tärkeää | Ei kovin tärkeää | Ei lainkaan tärkeää |
|---|---|---|---|---|---|
| Vastausten lukumäärä: | 53 | 7 | 1 | 0 | 0 |

**Vastauksien keskiarvot henkilöstöryhmittäin**


| 5 = Erittäin tärkeää | 4 = Tärkeää | 3 = Osittain tärkeää | 2 = Ei kovin tärkeää | 1 = Ei lainkaan tärkeää |
|---|---|---|---|---|

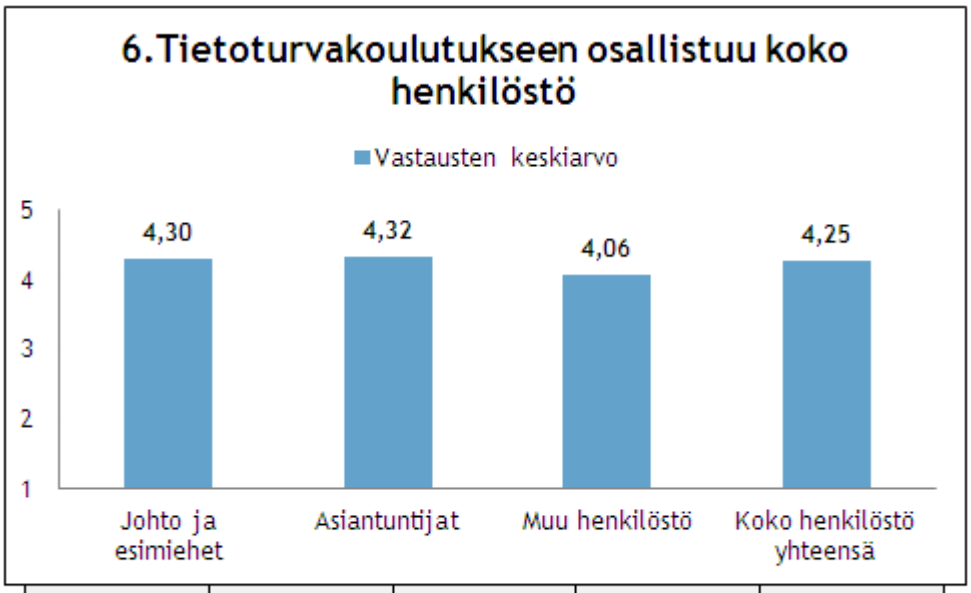

2. Johto kehittää ja arvio tietojen ja asiakirjojen käsittelyn turvallisuutta
Vastausten keskiarvo
5
4
3
2
1
4,30
3,91
4,29
4,08
Johto ja esimiehet
Asiantuntijat
Muu henkilöstö
Koko henkilöstö yhteensä
5 = Erittäin tärkeää
4 = Tärkeää
3 = Osittain tärkeää
2 = Ei kovin tärkeää
1 = Ei lainkaan tärkeää


3. Tietoturva-asiat ovat osa perehdytystä
Vastausten keskiarvo
5
4
3
2
1
4,50
4,50
4,53
4,51
Johto ja esimiehet
Asiantuntijat
Muu henkilöstö
Koko henkilöstö yhteensä
5 = Erittäin tärkeää
4 = Tärkeää
3 = Osittain tärkeää
2 = Ei kovin tärkeää
1 = Ei lainkaan tärkeää

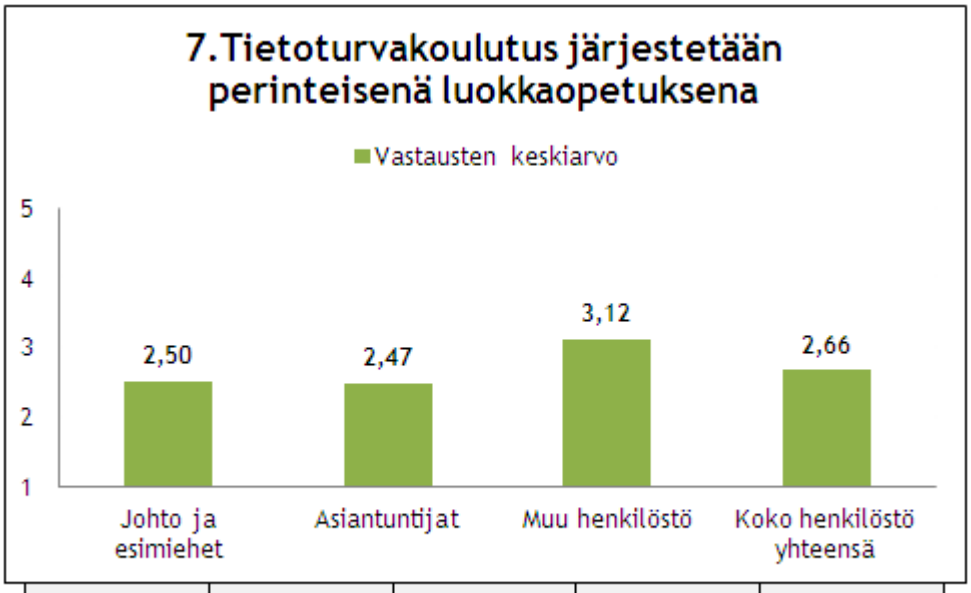



| 5 = Erittäin tärkeää | 4 = Tärkeää | 3 = Osittain tärkeää | 2 = Ei kovin tärkeää | 1 = Ei lainkaan tärkeää |
|---|---|---|---|---|

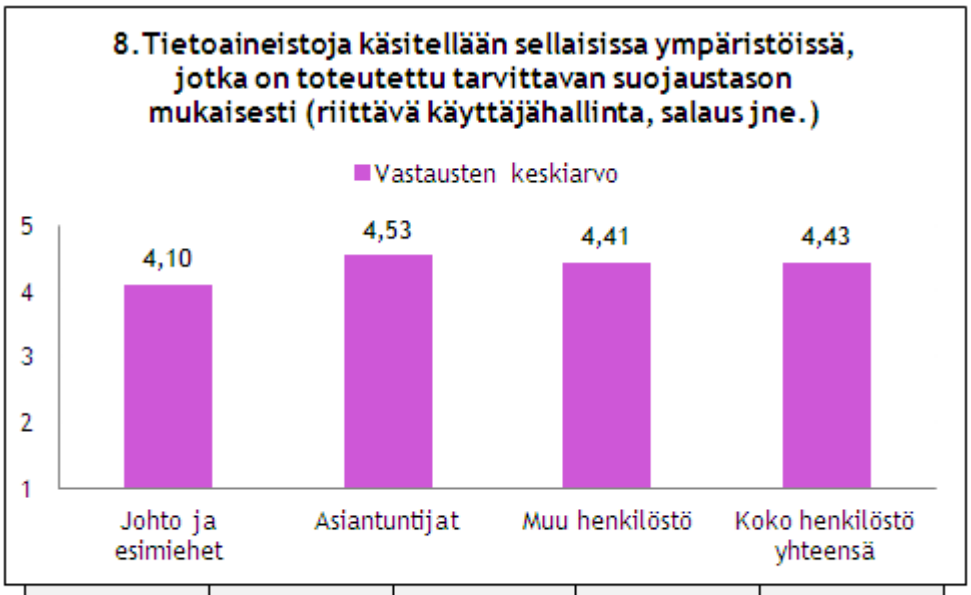

| 5 = Erittäin tärkeää | 4 = Tärkeää | 3 = Osittain tärkeää | 2 = Ei kovin tärkeää | 1 = Ei lainkaan tärkeää |
|---|---|---|---|---|

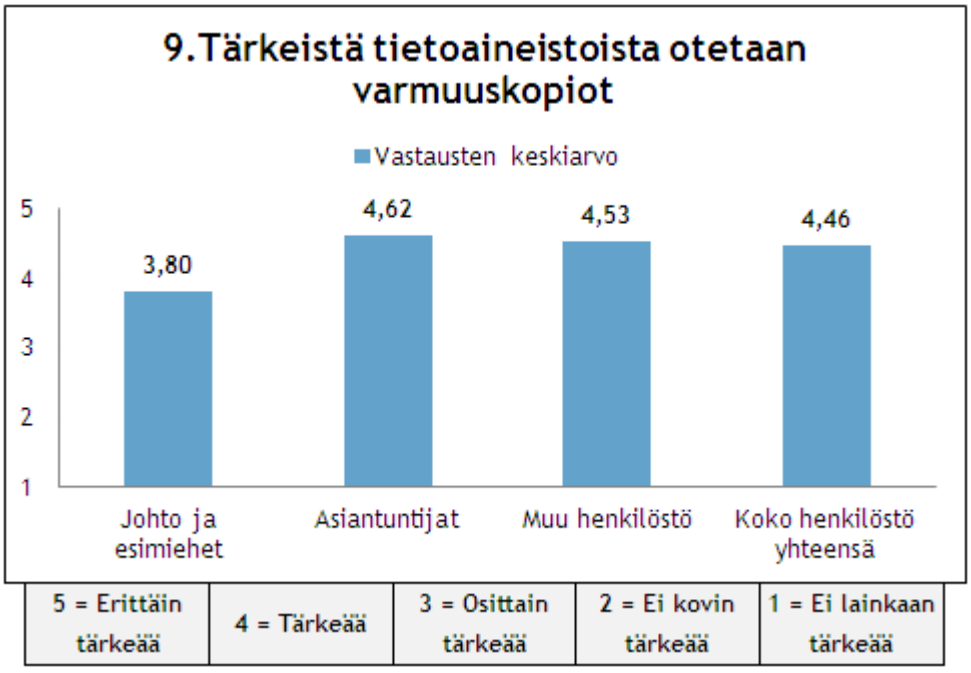


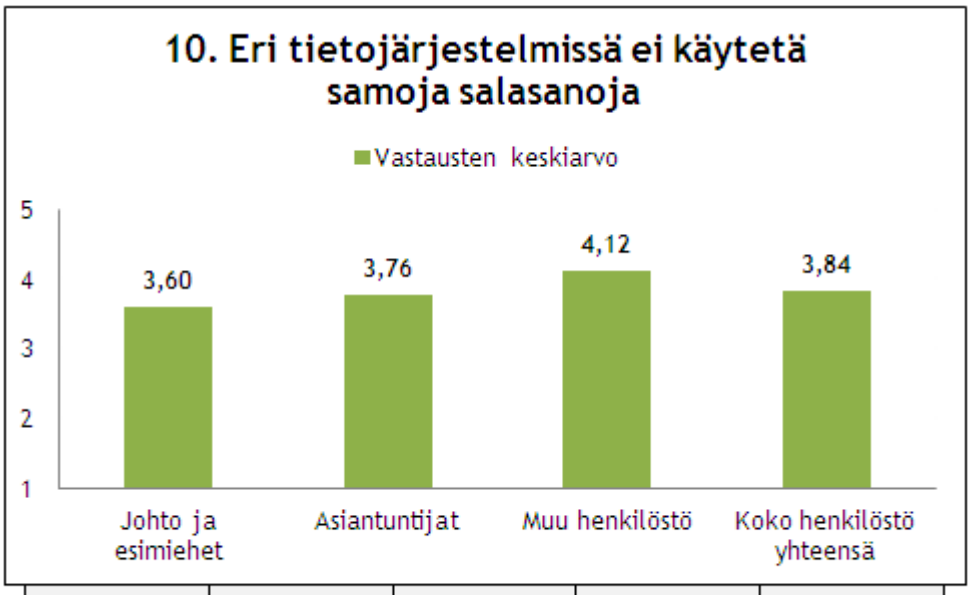

| 5 = Erittäin tärkeää | 4 = Tärkeää | 3 = Osittain tärkeää | 2 = Ei kovin tärkeää | 1 = Ei lainkaan tärkeää |
|---|---|---|---|---|



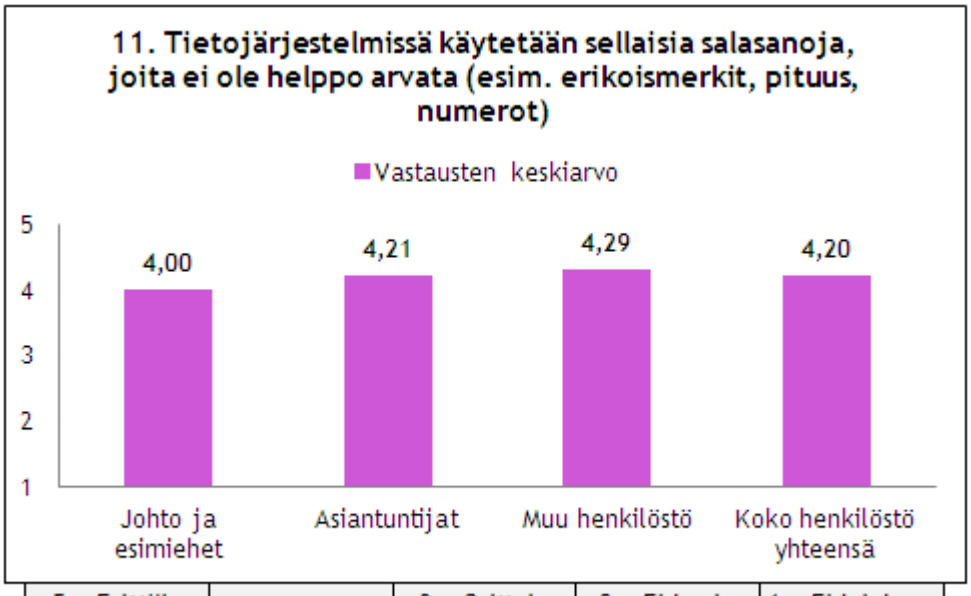

| 5 = Erittäin tärkeää | 4 = Tärkeää | 3 = Osittain tärkeää | 2 = Ei kovin tärkeää | 1 = Ei lainkaan tärkeää |
|---|---|---|---|---|


8. Tietoaineistoja käsitellään sellaisissa ympäristöissä, jotka on toteutettu tarvittavan suojaustason mukaisesti (riittävä käyttäjähallinta, salaus jne.)
Vastausten keskiarvo
5
4
3
2
1
4,10
4,53
4,41
4,43
Johto ja esimiehet
Asiantuntijat
Muu henkilöstö
Koko henkilöstö yhteensä
5 = Erittäin tärkeää
4 = Tärkeää
3 = Osittain tärkeää
2 = Ei kovin tärkeää
1 = Ei lainkaan tärkeää

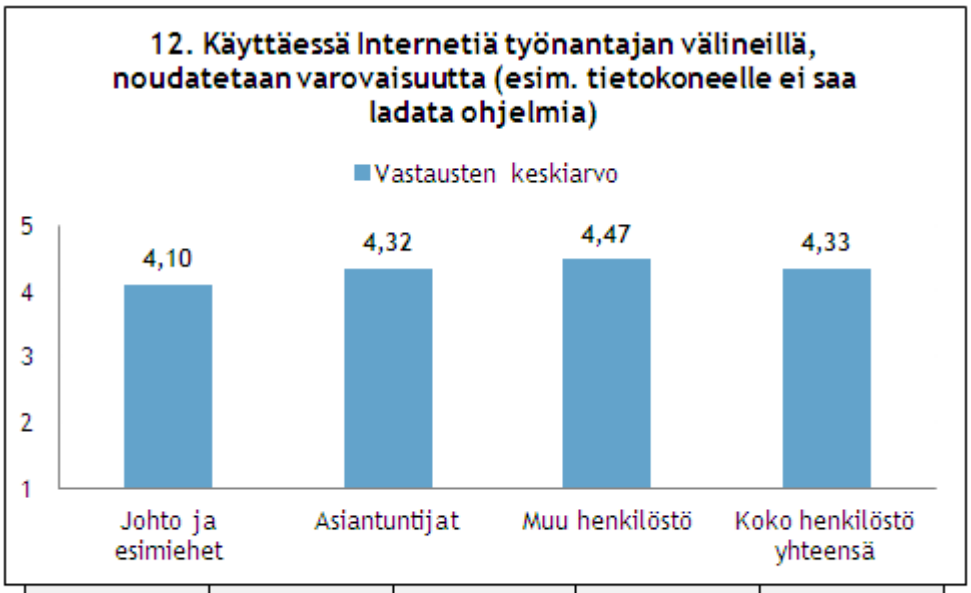

9. Tärkeistä tietoaineistoista otetaan varmuuskopiot
Vastausten keskiarvo
5
4
3
2
1
3,80
4,62
4,53
4,46
Johto ja esimiehet
Asiantuntijat
Muu henkilöstö
Koko henkilöstö yhteensä
5 = Erittäin tärkeää
4 = Tärkeää
3 = Osittain tärkeää
2 = Ei kovin tärkeää
1 = Ei lainkaan tärkeää



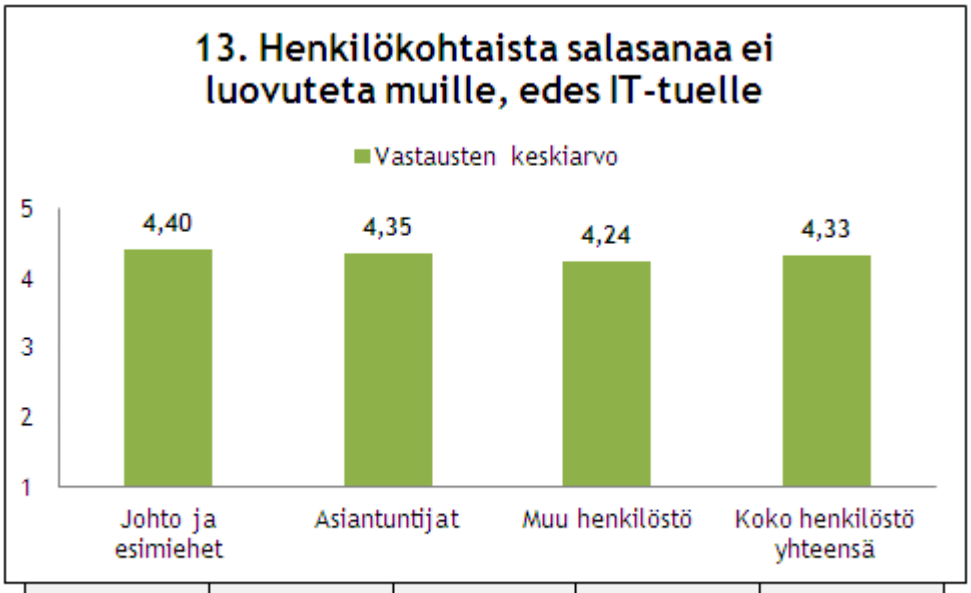

| 5 = Erittäin tärkeää | 4 = Tärkeää | 3 = Osittain tärkeää | 2 = Ei kovin tärkeää | 1 = Ei lainkaan tärkeää |
|---|---|---|---|---|



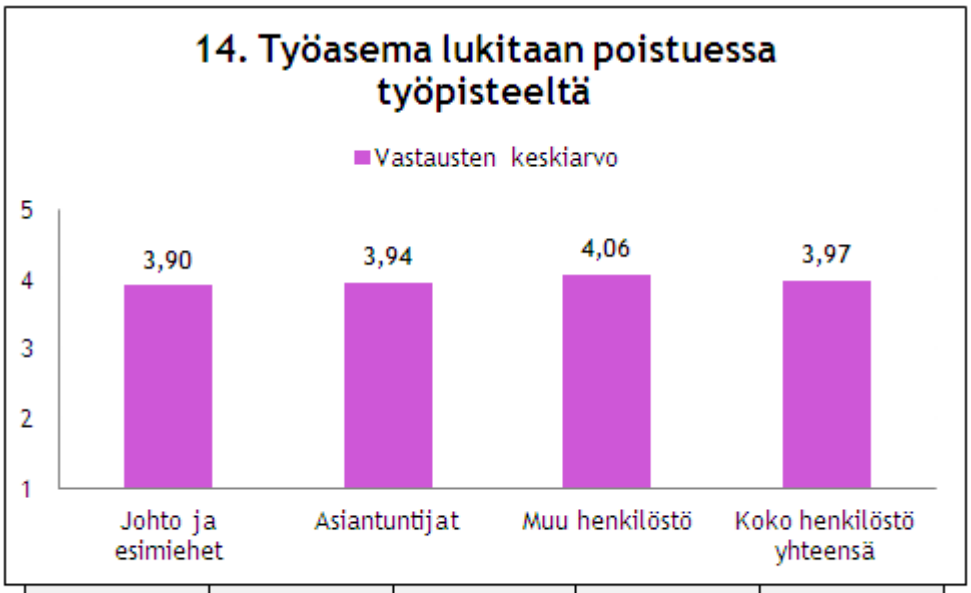

| 5 = Erittäin tärkeää | 4 = Tärkeää | 3 = Osittain tärkeää | 2 = Ei kovin tärkeää | 1 = Ei lainkaan tärkeää |
|---|---|---|---|---|

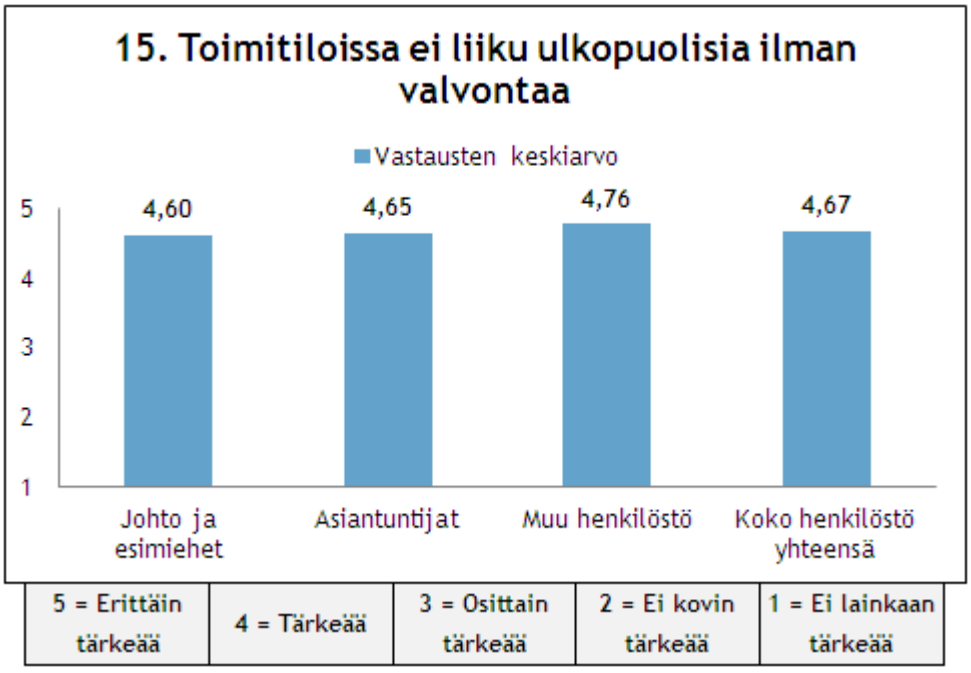


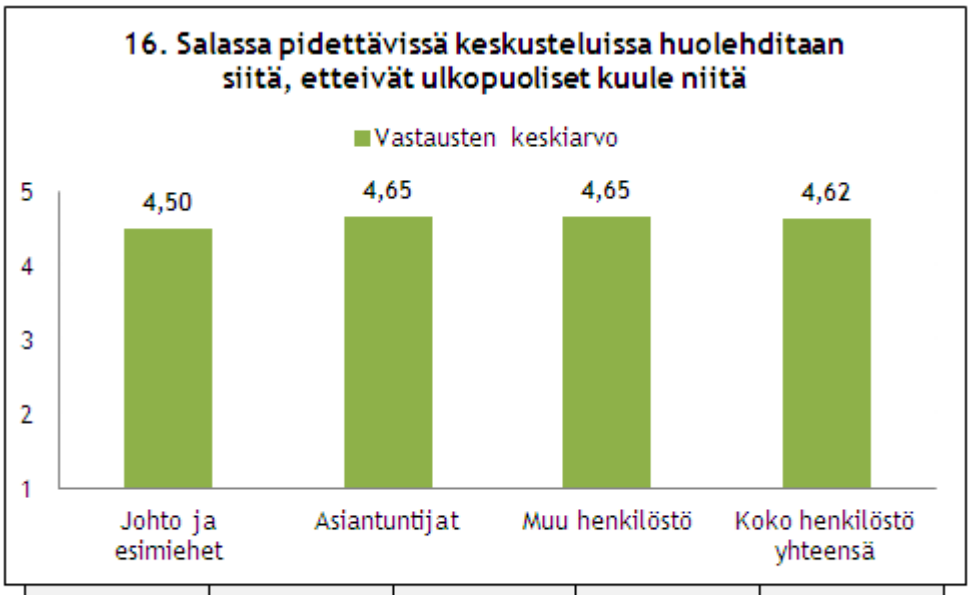

| 5 = Erittäin tärkeää | 4 = Tärkeää | 3 = Osittain tärkeää | 2 = Ei kovin tärkeää | 1 = Ei lainkaan tärkeää |
|---|---|---|---|---|



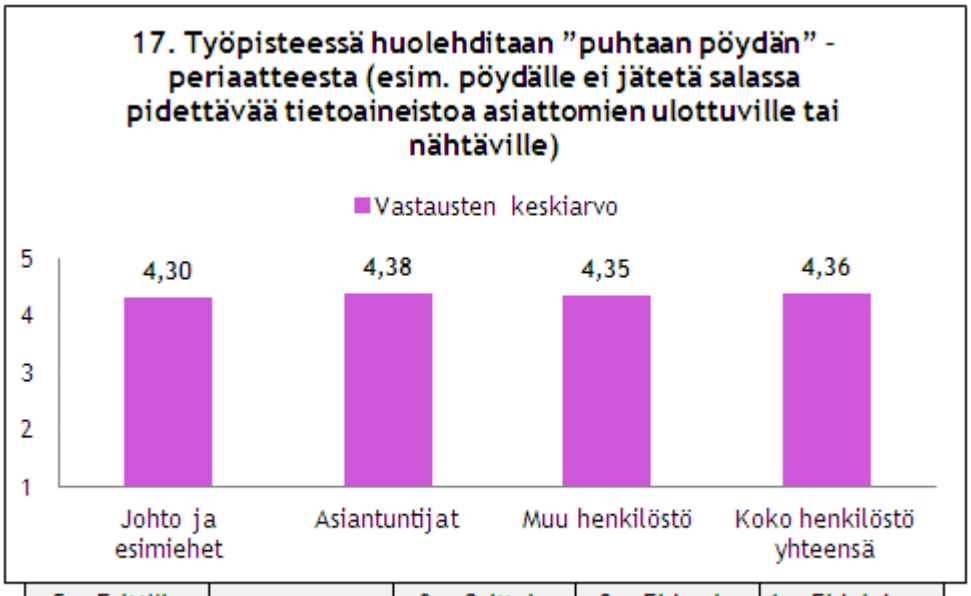

| 5 = Erittäin tärkeää | 4 = Tärkeää | 3 = Osittain tärkeää | 2 = Ei kovin tärkeää | 1 = Ei lainkaan tärkeää |
|---|---|---|---|---|


14. Työasema lukitaan poistuessa työpisteeltä
Vastausten keskiarvo
5
4
3
2
1
3,90
3,94
4,06
3,97
Johto ja esimiehet
Asiantuntijat
Muu henkilöstö
Koko henkilöstö yhteensä
5 = Erittäin tärkeää
4 = Tärkeää
3 = Osittain tärkeää
2 = Ei kovin tärkeää
1 = Ei lainkaan tärkeää

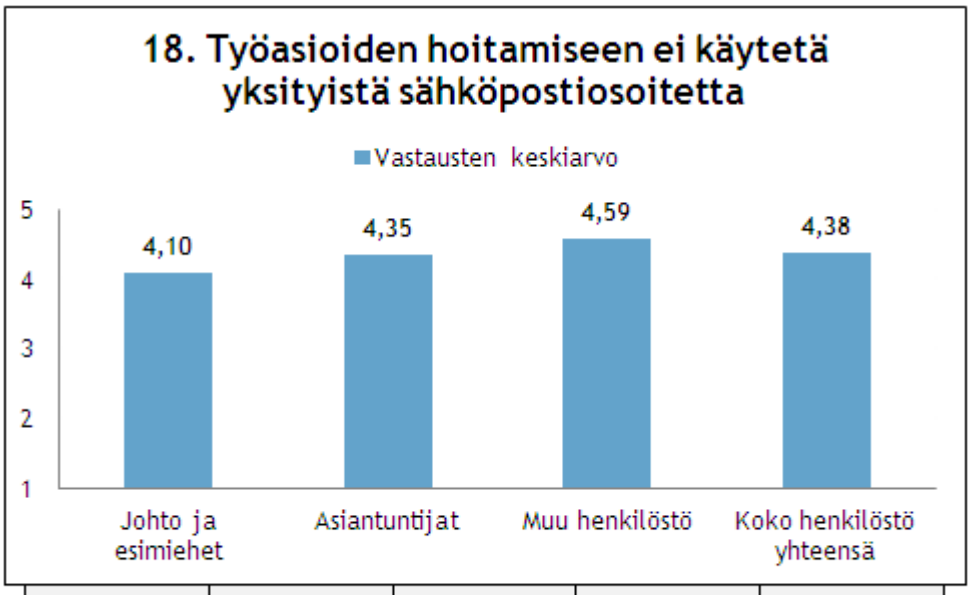

15. Toimitiloissa ei liiku ulkopuolisia ilman valvontaa
Vastausten keskiarvo
5
4
3
2
1
4,60
4,65
4,76
4,67
Johto ja esimiehet
Asiantuntijat
Muu henkilöstö
Koko henkilöstö yhteensä
5 = Erittäin tärkeää
4 = Tärkeää
3 = Osittain tärkeää
2 = Ei kovin tärkeää
1 = Ei lainkaan tärkeää



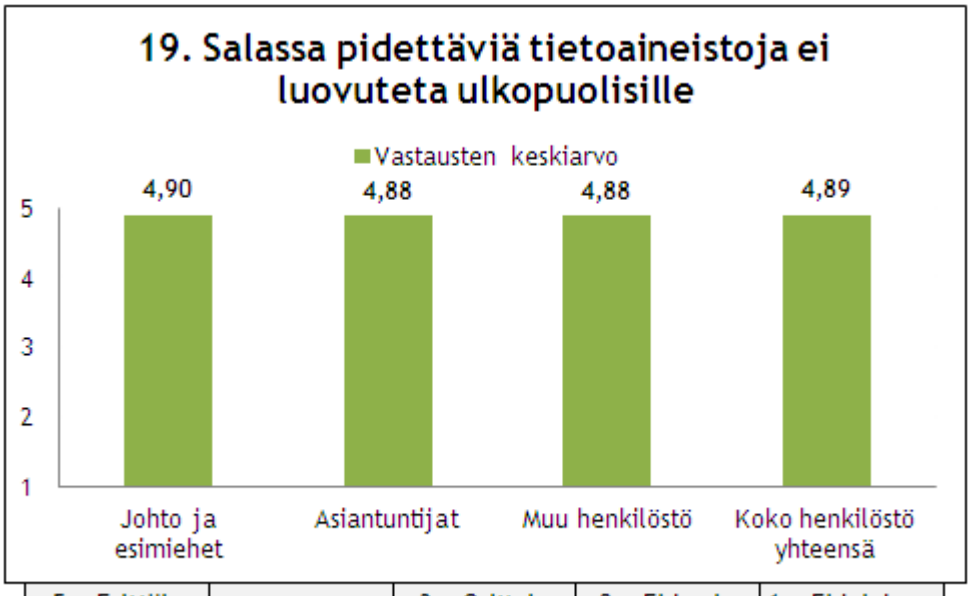

| 5 = Erittäin tärkeää | 4 = Tärkeää | 3 = Osittain tärkeää | 2 = Ei kovin tärkeää | 1 = Ei lainkaan tärkeää |
|---|---|---|---|---|



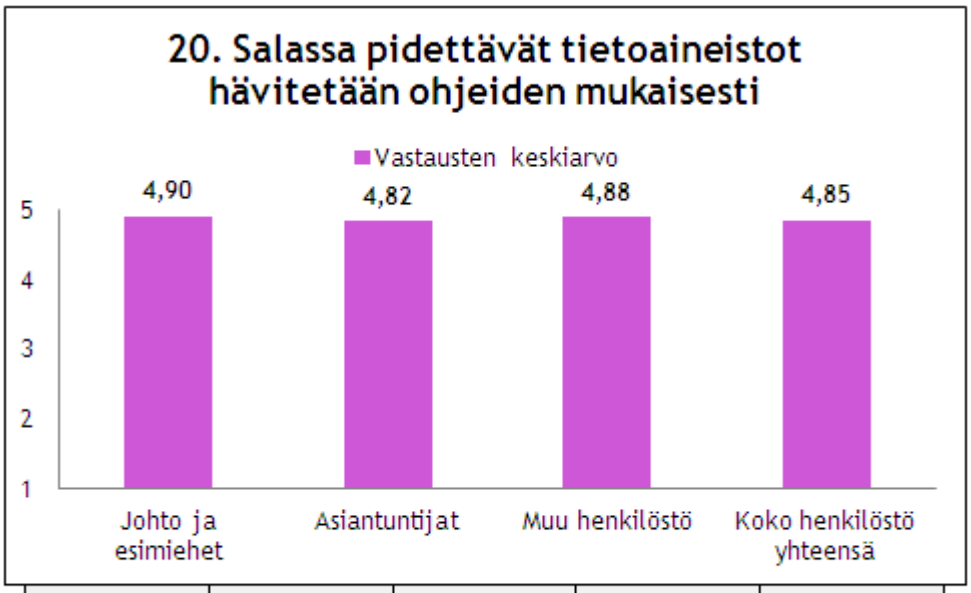

| 5 = Erittäin tärkeää | 4 = Tärkeää | 3 = Osittain tärkeää | 2 = Ei kovin tärkeää | 1 = Ei lainkaan tärkeää |
|---|---|---|---|---|




| 5 = Erittäin tärkeää | 4 = Tärkeää | 3 = Osittain tärkeää | 2 = Ei kovin tärkeää | 1 = Ei lainkaan tärkeää |
|---|---|---|---|---|




| 5 = Erittäin tärkeää | 4 = Tärkeää | 3 = Osittain tärkeää | 2 = Ei kovin tärkeää | 1 = Ei lainkaan tärkeää |
|---|---|---|---|---|




| 5 = Erittäin tärkeää | 4 = Tärkeää | 3 = Osittain tärkeää | 2 = Ei kovin tärkeää | 1 = Ei lainkaan tärkeää |
|---|---|---|---|---|