Karelia-ammattikorkeakoulu
Tradenomi, ylempi ammattikorkeakoulututkinto
Johtaminen ja liiketoimintaosaaminen

Digiturvallisuus osaksi henkilöstön työarkea Ammattiopisto Luovissa

Miia Kauppinen

Opinnäytetyö, toukokuu 2023

www.karelia.fi

Karelia AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Toukokuu 2023
Johtaminen ja liiketoimintaosaaminen, yamk

Tikkarinne 9
80200 JOENSUU
+358 13 260 600 (vaihde)

Tekijä
Miia Kauppinen

Nimeke
Digiturvallisuus osaksi henkilöstön työarkea Ammattiopisto Luovissa

Toimeksiantaja
Ammattiopisto Luovi Oy

Tiivistelmä

Työelämä on jatkuvassa murroksessa erityisesti digitalisaation vuoksi. Työn muutos edellyttää myös organisaatioiden henkilöstöltä uudenlaista osaamista, kuten kykyä toimia digiturvallisesti. Tämän opinnäytetyön tarkoituksena oli luoda Ammattiopisto Luovin henkilöstölle digiturvallisuusosaamisen kehittämissuunnitelma, joka sisältää digiturvakoulutuksen. Toimeksiantona oli löytää keinoja henkilöstön digiturvaosaamisen kehittämiseen Luovin turvallisuuden parantamiseksi. Tavoitteena oli selvittää Luovin henkilöstön ja johdon edustajien tarpeet digiturvakoulutukselle ja löytää toimivin tapa koulutuksen järjestämiselle. Lisäksi tehtävänä oli selvittää koulutuksen lisäksi muita keinoja, joilla digiturva saadaan luontevaksi osaksi henkilöstön työarkea.

Opinnäytetyö toteutettiin tutkimuksellisena kehittämistyönä yhdistäen tapaustutkimusta ja konstruktiivista tutkimusta. Aineisto kerättiin Luovin henkilöstölle toteutetun verkkokyselyn, johdon edustajille pidetyn verkkohaastattelun ja Luovin asiantuntijoiden kanssa pidettyjen suunnittelupajojen avulla. Kerätyn aineiston ja teoriatiedon perusteella opinnäytetyön tuotoksena luotiin kattava, monipuolinen ja käytännönläheinen Luovin henkilöstön digiturvallisuusosaamisen kehittämissuunnitelma ja sen osana henkilöstölle pidettävän digiturvakoulutuksen runko. Työn tuloksia voidaan hyödyntää muissa ammatillisissa erityisoppilaitoksissa ja sovellettuna kaikissa organisaatioissa, sillä teknologisen kehityksen myötä digiturvallisuustaitoja tarvitaan jokaisessa työyhteisössä.

Jatkotutkimuksena voitaisiin selvittää laaditun henkilöstön digiturvallisuusosaamisen kehittämissuunnitelman toimivuutta muutaman vuoden kuluttua toteutettavalla seurantatutkimuksella. Toisena jatkotutkimuksena voitaisiin selvittää opiskelijoiden digiturvaosaamisen kehittämistä, koska oppilaitoksissa henkilöstön digiturvaosaamisen lisäksi olennainen osa turvallisuutta on opiskelijoiden digiturvallisuusosaaminen.

Kieli
suomi

Sivuja 117
Liitteet 4
Liitesivumäärä 9

Asiasanat
digitalisaatio, digiturvallisuus, osaamisen kehittäminen, koulutus

THESIS
May 2023
Master's Program in Business Management and Leadership

Tikkarinne 9
80200 JOENSUU
FINLAND
+ 358 13 260 600 (switchboard)

Author
Miia Kauppinen

Title
Digital Security as Part of the Personnel's Everyday Work at Luovi Vocational College

Commissioned by
Luovi Vocational College Ltd

Abstract

Working life is constantly changing, especially due to digitalization. The changes in work also require new skills from the personnel of organizations, such as the ability to operate safely in digital environments. The purpose of this thesis was to provide the personnel of Luovi Vocational College with a development plan for digital security competence, which includes digital security training. The assignment was to find ways to develop the digital security skills among the employees in order to improve security at Luovi. The aim of the thesis was to find out the training needs of the personnel and management representatives regarding digital security and to find the most efficient way to organize such training at Luovi. In addition, the thesis aimed at identifying other ways to make digital security a natural part of the personnel's everyday work.

The thesis was carried out as a research-based development project, combining a case study and constructive research. The material was collected through an online survey from the personnel, with an online interview with the management representatives, and in the planning workshops held with the experts at Luovi. As a result of the thesis, a comprehensive, versatile and practical development plan for digital security competence was developed based on the collected material and theoretical knowledge.

The results of the thesis can be used in other colleges providing special vocational education. Moreover, they can be applied in all organizations, because technological development has created needs for digital security skills in every work community. To follow up the effectiveness of the development plan, another study could be carried out in a few years. In another follow-up study, the development of the students' digital security skills could be investigated. In educational institutions the digital security skills of the students are also an essential part of the organisation's security.

Language
Finnish

Pages 117
Appendices 4
Pages of Appendices 9

Keywords
digitalization, digital security, competence development, training

Sisältö

Liitteet

Määritelmät

Digiturvallisuus
on tavoitetila, jossa digitaaliseen toimintaympäristöön voidaan luottaa. Digitaaliseen turvallisuuteen kuuluvat tietosuoja, tietoturva, riskienhallinta, jatkuvuuden hallinta ja kyberturvallisuus. Digiturvalla varmistetaan, että digitaalinen toimintaympäristö on luotettava, turvallinen ja saatavilla. (Mukaillen Digi- ja väestötietovirasto 2023.)

Eheys
tarkoittaa sitä, että tiedot ovat loogisesti oikein ja niihin tehdään vain oikeutettuja muutoksia (Kyberturvallisuuskeskus 2020a).

Erityiset henkilötietoryhmät
määritellään tietosuoja-asetuksessa. Niitä ovat esimerkiksi terveystiedot, rotu tai etninen alkuperä, ammattiliiton jäsenyys, poliittiset mielipiteet ja uskonnollinen tai filosofinen vakaumus. (Tietosuojavaltuutetun toimisto 2023a.)

Henkilötieto
tarkoittaa kaikkia tietoja, joiden perusteella luonnollinen henkilö voidaan tunnistaa suoraan tai välillisesti esimerkiksi yhdistämällä yksittäinen tieto johonkin toiseen tietoon. Henkilötietoja ovat esimerkiksi nimi, henkilötunnus ja auton rekisterinumero. (Mukaillen Tietosuojavaltuutetun toimisto 2023c.)

Informaatiovaikuttaminen
on toimintaa, jolla pyritään järjestelmällisesti vaikuttamaan yleiseen mielipiteeseen, yksilöiden käyttäytymiseen ja päätöksentekijöihin sekä sitä kautta yhteiskunnan toimintakykyyn (Valtioneuvoston kanslia 2019, 16).

Kyberuhka
tarkoittaa digitaalisin keinoin toteutettavaa uhkaa, joka kohdistuu digitaaliseen omaisuuteen, järjestelmään tai palveluun. Toteutuessaan kyberuhkan vaikutukset ovat huomattavia sekä taloudellisesti että yhteiskunnallisesti. (Traficom 2020.)

Kyberturvallisuus
on keino turvata organisaation ja yhteiskunnan elintärkeät ja kriittiset toiminnot (Digi- ja väestötietovirasto 2023).

Luottamuksellisuus
tarkoittaa tietojen suojaamista ulkopuolisilta, jotta tiedot ovat ainoastaan niihin oikeutettujen käytettävissä (Opetushallitus 2023).

Monivaiheinen tunnistautuminen (MFA)
tarkoittaa henkilöllisyyden varmistamista käyttäjätunnuksen ja salasanan lisäksi erillisen turvatiedon, kuten puhelinnumeron avulla. MFA:n ollessa käytössä kirjautuminen ei onnistu ainoastaan käyttäjätunnuksella ja salasanalla, vaan se täytyy vahvistaa turvatiedon avulla. (Traficom 2023b.)

Osaamisen kehittäminen
tarkoittaa tietojen ja taitojen lisäämistä. Osaamisen kehittämistä on esimerkiksi uusien taitojen ja kykyjen hankkiminen henkilöstölle työelämän muuttuessa ja kehittyessä. (Mukaillen Viitala 2021, 121.)

Poikkeamista toipuminen
tarkoittaa toiminnan palauttamista lähtötilanteeseen erilaisten häiriötilanteiden jälkeen. Toipumissuunnitelmassa määritellään toimet, joiden avulla esimerkiksi tietojärjestelmä saadaan uudelleen toimivaksi. (Digi- ja väestötietovirasto 2023.)

Poikkeamien tunnistaminen
on normaalioloista poikkeavan toiminnan havaitsemista (Digi- ja väestötietovirasto 2023).

Poikkeamiin varautuminen
tarkoittaa toimintaa, jolla pyritään ennakoimaan mahdollisia tavallista toimintaa häiritseviä tilanteita ja varautumaan niihin (Digi- ja väestötietovirasto 2023).

Rekisterinpitäjä
on organisaatio (tai ihminen), joka määrittelee, millä tavalla ja mihin tarkoitukseen henkilötietoja käsitellään (Tietosuojavaltuutetun toimisto 2023c). Rekisterinpitäjä voi olla esimerkiksi oppilaitos, joka käsittelee henkilöstön ja opiskelijoiden henkilötietoja.

Rekisteröity
on henkilö, jonka henkilötietoja käsitellään (Tietosuojavaltuutetun toimisto 2023c). Rekisteröityjä ovat esimerkiksi työntekijät ja oppilaitoksen opiskelijat.

Riskien analysointi
tarkoittaa riskien suuruuden ja luonteen arvioimista. Riskien luonteen arviointiin kuuluu todennäköisyyden ja vaikutusten määrittely. (Valtiovarainministeriö 2020.)

Riskien hallinta
on prosessi, jonka tavoitteena on minimoida tietyn asian riskit ja niiden vaikutukset (mukaillen Viitala & Jylhä 2019, 206).

Sähköiset häiriötilanteet
ovat tilanteita, jolloin sähköiset palvelut eivät toimi normaalisti. Tilanteet voivat olla ennakoimattomia tai ne voivat olla ennalta tiedossa, kuten ajoitetut sähkökatkot. (Ammattiopisto Luovi 2023a.)

Tietosuoja
turvaa henkilöiden oikeudet henkilötietoja käsiteltäessä. Tietosuoja on perusoikeus ja kaikilla henkilöillä on oikeus henkilötietojensa suojaan. (Tietosuojavaltuutetun toimisto 2023c.)

Tietosuojaperiaatteet
määritellään tietosuoja-asetuksessa. Niitä ovat esimerkiksi käsiteltävien henkilötietojen minimointi, tietojen päivitysvelvollisuus sekä luottamuksellinen ja turvallinen henkilötietojen käsittely. (Tietosuojavaltuutetun toimisto 2023c.)

Tietoturva
tarkoittaa tiedon eheyden, luottamuksellisuuden ja saatavuuden ylläpitämistä. Tietoturva on myös yksi tietosuojan toteuttamisen keino, jonka tarkoituksena on suojata tietoaineistot ja tietojärjestelmät. (Tietosuojavaltuutetun toimisto 2023c.)

Tietoturvaloukkaus henkilötietoja koskien
on tapahtuma, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu tai niitä luovutetaan oikeudettomasti tai niihin on pääsy henkilöillä, joilla siihen ei ole oikeutta (Tietosuojavaltuutetun toimisto 2023e).

Tietoturvapoikkeama
tarkoittaa esimerkiksi tietojen kalastelua, palvelunestohyökkäyksiä ja tietomurtoja tai näiden yrityksiä (Kyberturvallisuuskeskus 2020b).

Turvatulostus
tarkoittaa tulostamistapaa, jossa tuloste tulostuu ulos tulostimesta vasta, kun tulostaja on tulostimen äärellä ja vapauttaa tulostuksen (Ammattiopisto Luovi 2023a).

1 Johdanto

Digitalisaatio ja teknologian kehittyminen ovat olleet jo vuosien ajan tulevaisuuden megatrendejä, jotka muokkaavat työtä ja tapoja tehdä työtä (Dufva, Wartiovaara & Vataja 2021). Suomalainen työelämä on lähes täysin digitalisoitunut (Sutela, Pärnänen & Keyriläinen 2019, 104) ja teknologian nopea kehittyminen vaatii organisaatioita muokkaamaan ajattelu- ja toimintamallejaan (Sitra 2020). Teknologisten muutosten myötä eteen tulevien haasteiden ratkaiseminen edellyttää sekä organisaatioilta että yksilöiltä uudenlaista osaamista ja elinikäistä oppimista (Dufva ym. 2021).

Digitaalisuus on läsnä kaikilla työpaikoilla ja kaikessa työssä (Hagert & Toivanen 2022, 226). Teknologinen kehitys vaatii työelämässä uuden opettelua, mutta organisaatiot voivat vaikuttaa tapoihin, joilla ne ottavat teknologioita käyttöön ja soveltavat niitä (Työterveyslaitos 2022). Organisaatioiden on tärkeää mahdollistaa henkilöstölleen digitaitojen ylläpito ja mahdollisuus oppia uutta, jotta digiajan edut saadaan kattavasti hyödynnettyä (Sutela ym. 2019, 93). Teknologioiden hyödyntäminen ja sen myötä digiturvallisuus ovat jollakin tavalla osa kaikkien organisaatioiden henkilöstön työarkea. Valveutuneet organisaatiot luovat digiturvallisen kulttuurin erilaisten ohjeistusten ja koulutusten avulla. Tällöin niiden henkilöstö osaa toimia digiympäristön vaatimusten mukaisesti. (Rousku, Kirves & Kinnunen 2019.)

Digitaalinen turvallisuus eli digiturva on terminä melko uusi ja osin vakiintumaton. Digiturva koostuu viidestä osa-alueesta, jotka ovat tietosuoja, tietoturva, riskienhallinta, toiminnan jatkuvuuden hallinta ja kyberturvallisuus. (Valtiovarainministeriö 2020.) Digiturvassa onnistuminen edellyttää kykyä varautua digitaaliseen toimintaympäristöön kohdistuviin uhkiin ja kykyä kestää häiriötilanteita. Poikkeamista on pystyttävä myös palautumaan mahdollisimman hyvin ja nopeasti. (Digi- ja väestötietovirasto 2023.) Digiturvallinen toiminta vähentää poikkeamatilanteiden todennäköisyyttä ja pienentää poikkeamien vaikutuksia. Kun henkilöstö hallitsee digiturvan osa-alueiden perusteet, he pystyvät toimimaan vastuullisemmin, jolloin organisaation turvallisuus paranee. (Rousku ym. 2019.)

Tämä opinnäytetyö on toteutettu Ammattiopisto Luovin (myöhemmin Luovi) toimeksiantona ja sen tavoitteena on parantaa Luovin turvallisuutta. Opinnäytetyö on laadittu Luovin tiedonhallinnan asiantuntijan työn ohessa. Työn tarkoituksena on löytää ja tuoda ilmi monipuolisesti eri keinoja, joiden avulla Luovi voi kehittää koko henkilöstönsä digiturvaosaamista. Digiturvan tulee olla luonteva osa henkilöstön työarkea, koska digiturvallisuus on olennainen osa organisaation toimintaa ja siitä huolehtiminen kuuluu koko henkilöstölle. Digiturvallisuusosaamisen kehittämisellä Luovin mahdollisuudet hyödyntää uusia teknologioita parantuvat. Digiturvallinen toiminta lisää myös organisaation toiminnan luotettavuutta.

1.1 Opinnäytetyön tavoitteet

Opinnäytetyön tavoitteena on Ammattiopisto Luovin koko henkilöstön digiturvallisuusosaamisen syventäminen siten, että digiturvasta huolehtimisesta tulee luonteva osa heidän työarkeaan. Digiturvaosaamisen kehittämisellä varmistetaan organisaation, henkilöstön, opiskelijoiden ja sidosryhmien turvallisuutta. Opinnäytetyön tavoitteena on luoda Luovin henkilöstön digiturvaosaamisen kehittämissuunnitelma, joka sisältää henkilöstölle vuonna 2023 pidettävän digiturvakoulutuksen rungon. Kehittämissuunnitelman sisältämän koulutuksen ja suunnitelmassa kerrottavien muiden toimenpiteiden avulla on tarkoitus parantaa henkilöstön digiturvaosaamista. Laadittava kehittämissuunnitelma sisältää ehdotuksia toimenpiteiden sisällölle ja aikataululle. Tavoitteena on luoda käytännönläheinen kehittämissuunnitelma, jonka toteuttamisella Luovin koko henkilöstön digiturvaosaaminen kehittyy ja sitä pystytään ylläpitämään.

Ensimmäisenä tehtävänä on kartoittaa henkilöstön digiturvakoulutustarpeita ja johdon edustajien näkemyksiä digiturvasta. Koulutustarpeita selvitetään henkilöstölle laadittavalla kyselyllä ja johdon edustajille järjestettävällä haastattelulla. Kyselyssä ja haastattelussa hyödynnetään sekä digiturvallisuuteen että osaamisen kehittämiseen liittyvää teoriatietoa. Teoriatiedon sekä tutkimuksessa saadun aineiston perusteella luodaan Luovin henkilöstön digiturvaosaamisen kehittämissuunnitelma, joka sisältää digiturvakoulutuksen.

1.2 Opinnäytetyön rajaus

Opinnäytetyö on rajattu koskemaan Ammattiopisto Luovin henkilöstön digiturvallisuusosaamisen kehittämistä. Opinnäytetyön ulkopuolelle on rajattu Luovin opiskelijoiden digiturvaosaamisen kehittäminen, vaikka myös se on oleellinen osa oppilaitoksen turvallisuutta. Työstä on rajattu ulkopuolelle myös henkilöstölle järjestettävän digiturvakoulutuksen aineisto lukuun ottamatta paria yleisen tason esimerkkiä. Digiturvallisuuskoulutuksen varsinaista sisältöä ei esitellä, koska koulutus sisältää ainoastaan luovilaisille tarkoitettuja konkreettisia ohjeita.

Opinnäytetyössä käsitellään digiturvakokonaisuutta mukaillen Valtiovarainministeriön (2020) määrittelyä, jonka mukaisesti digitaaliseen turvallisuuteen kuuluvat riskienhallinta, toiminnan jatkuvuuden hallinta ja varautuminen, kybertuvallisuus, tietoturvallisuus ja tietosuoja. Opinnäytetyöstä on rajattu ulkopuolelle digiturvallisuuden arkkitehtuuri, digiturvaan liittyvät laatujärjestelmät ja pilvipalvelut sekä uusimpien teknologioiden, kuten tekoälyn ja Metaversen, tarkastelu työn laajuuden kohtuullistamiseksi. Opinnäytetyö keskittyy esittelemään digiturvan viidestä osa-alueesta niiden keskeisimmän sisällön henkilöstön osaamisen kehittämisen näkökulmasta. Lähemmässä tarkastelussa osa-alueista ovat tietosuoja ja tietoturva, koska niiden merkitys on suurin henkilöstön työarjessa.

1.3 Opinnäytetyön rakenne

Tämä opinnäytetyö rakentuu yhdeksästä luvusta. Johdantoluvussa esitellään opinnäytetyön tavoite, rajaus ja rakenne sekä kahden digiosaamisen kehittämiseen liittyvän aiemman yamk-opinnäytetyön tuloksia. Luvussa kaksi esitellään Ammattiopisto Luovin toimintaa ja sen strategia sekä digitaalisuuden hyödyntämistä Luovissa. Opinnäytetyön teoriaosuus koostuu digitalisaatiosta ja digiturvasta sekä osaamisen kehittämisestä. Luvussa kolme esitellään digiturvallisuuden viisi eri osa-aluetta painottaen tietosuojaa ja tietoturvaa niiden merkittävyyden vuoksi. Luvussa neljä käydään läpi osaamisen kehittämistä ja tämän työn kannalta olennaisia osaamisen kehittämiskeinoja.

Tutkimuksellisen kehittämistyön laadinta käydään läpi luvussa viisi. Työn käytännön toteuttaminen on esitelty luvussa kuusi. Koulutustarvekyselystä ja tutkimushaastattelusta saadut tulokset ovat luvussa seitsemän. Luvussa kahdeksan esitellään tämän työn tuotokset eli digiturvallisuusosaamisen kehittämissuunnitelma ja osaksi kehittämissuunnitelmaa kuuluvan sisäisen digiturvakoulutuksen runko. Luvun kahdeksan tuotokset sisältävät luvussa seitsemän olevista tutkimuksen tuloksista tehdyt johtopäätökset. Yhdeksännessä luvussa on yhteenveto työn toteutuksesta ja tuloksista sekä niiden vertaamista aiempiin tutkimuksiin ja tietoperustaan. Luku sisältää myös pohdintaa opinnäytetyön prosessista, työn luotettavuudesta ja eettisyydestä sekä työn hyödyntämisestä ja jatkokehityskohteista digiturvallisuuden kehittämisessä.

1.4 Aikaisempien opinnäytetöiden tutkimustuloksia

Digitaalisen osaamisen kehittämistä on käsitelty Jarno Kyllösen vuonna 2019 tekemässä opinnäytetyössä *Digitaalisen osaamisen kehittäminen itsensä johtamisen kautta Pohjois-Karjalan Osuuspankissa*. Finanssialan digitalisaatioon liittyvässä opinnäytetyössä selvitettiin, kuinka henkilöstön digitaalista osaamista voidaan kehittää ja miten olemassa olevien työvälineiden käyttöä saataisiin aktivoitua jokapäiväiseen käyttöön henkilöstön itsensä johtamisen kautta. Kyllönen toteutti opinnäytetyönsä tapaustutkimuksena, jossa hän kävi läpi 20 henkilön haastatteluaineiston. (Kyllönen 2019.)

Tulosten mukaan digitaalisen osaamisen kehittäminen itsensä johtamisen kautta Pohjois-Karjalan Osuuspankissa oli pääosin kunnossa. Vastaajien motivaatio ja asenne digitaalisuutta kohtaan olivat hyvällä tasolla. Yksittäisiä poikkeuksia lukuun ottamatta muutosvastarintaa uutta kohtaan ei ilmennyt. Tulosten mukaan Pohjois-Karjalan Osuuspankin henkilöstö tiedosti hyvin oman vastuunsa oppimisesta ja aktiivisuudesta. Kehittämiskohteena havaittiin työparityöskentely, tiimipalaverit, sisäisen motivaation kehittäminen ja koulutuksen järjestäminen. Kehittämistoimien tarkoituksena olisi varmistaa toinen toisiltaan oppiminen. Digipalavereissa jaettaisiin kokemuksia, vinkkejä ja ideoita. Näillä kehittämistoimilla varmistettaisiin myös digitaalisen osaamisen kehittämisen

pysyminen esillä ja aktivoitaisiin digitaalisten työvälineiden käyttöä, kun henkilöstön digiosaaminen ja tiedot lisääntyisivät. (Kyllönen 2019.)

Kyllösen opinnäytetyön tuloksissa näkyi vastaajien monimuotoisuus. Vastaajat olivat eri tasoilla digiosaamisessa ja sen kehittämisessä. Suurin osa vastaajista oli kuitenkin motivoitunut osaamisen kehittämiseen. Vastaajat olivat valmiita ottamaan käyttöön uusia työvälineitä ja laajentamaan omaa digiosaamistaan. Vastaajilla oli halu pysyä mukana digitalisaation kehityksessä. (Kyllönen 2019.)

Vuonna 2018 laatimassaan opinnäytetyössä *Digiajan työntekijän kehittämissuunnitelma* Aija-Maria Jokilammi toteutti tapaustutkimuksen, jonka lähtökohtana oli tutkia osaamisen kehittämistä digitalisaation kontekstissa 14 henkeä työllistävässä taloushallintoalan yrityksessä. Opinnäytetyön tavoitteena oli luoda suunnitelma osaamisen kehittämisestä digitalisaation näkökulmasta. Jokilammi työsti osaamisen kehittämisen tueksi vuosikellon, jossa hän pilkkoi kalenterivuoden kolmeen osaan rakentaen kuhunkin osaan omat osaamisen kehittämisen tavoitteet ja menetelmät. Ensimmäisen kolmanneksen teemana on toimintaympäristön muutokset, toisen kolmanneksen valmentava johtaminen ja viimeisen teknologia ja oppiminen. Vuosikellon mukaisesti organisaatiossa tulisi järjestää koulutuksia ja jakaa opittuja tietoja yhteisissä keskusteluissa. (Jokilammi 2018.)

Jokilammi tutki opinnäytetyössään käsiteanalyysin keinoilla, mitä osaamisen kehittäminen on ja kuinka digitalisaatio on vaikuttanut ja tulee alan ammattilaisten mielestä vaikuttamaan osaamisen kehittämiseen taloushallintoalan yrityksessä. Opinnäytetyön tavoitteena oli kartoittaa, vastaako henkilöstön nykyinen osaaminen työn ja uusien työkalujen sekä teknologioiden vaatimuksia. Toisena tavoitteena oli kartoittaa, minkälaisia haasteita digitalisaatio tuo osaamisvaatimuksille. Opinnäytetyön tuloksina Jokilammi havaitsi, että investoinnit teknologian kehittämiseen eivät yksinään riitä, vaan myös osaamisen kehittämiseen tulee panostaa. Digiajan organisaatiossa edellytetään uudenlaista osaamista ja osaamispääoma on merkittävä digiajan menestystekijä nopeasti muuttuvassa toimintaympäristössä. Opinnäytetyön tuloksena nousi esiin myös havainto digitalisaation vaikutuksista teknologian lisäksi viestintään, organisaatiokulttuuriin ja johtamiseen sekä asiakaskokemukseen. (Jokilammi 2018.)

Jokilammi haki opinnäytetyössään vastauksia siihen, millaista osaamista kohdeyritys tarvitsee digitalisoituneessa tietotyössä ja miten osaamista tulisi kehittää. Opinnäytetyössä toteutetun tutkimuksen mukaan kohdeyrityksen henkilöstön substanssiosaaminen oli erinomaisella tasolla. Osaamisen kehittämiskohteiksi nousivat teknologiaosaaminen sekä kyky analyyttiseen taitoon tulkita ja hyödyntää dataa. Opinnäytetyön tulosten mukaan työn murros on muuttanut merkittävästi työn osaamisvaateita, ja digitalisaation vaikutukset näkyvät työelämässä myös ajatusmallien muutoksina organisaatiokulttuuria uudistaen. (Jokilammi 2018.)

2 Ammattiopisto Luovi

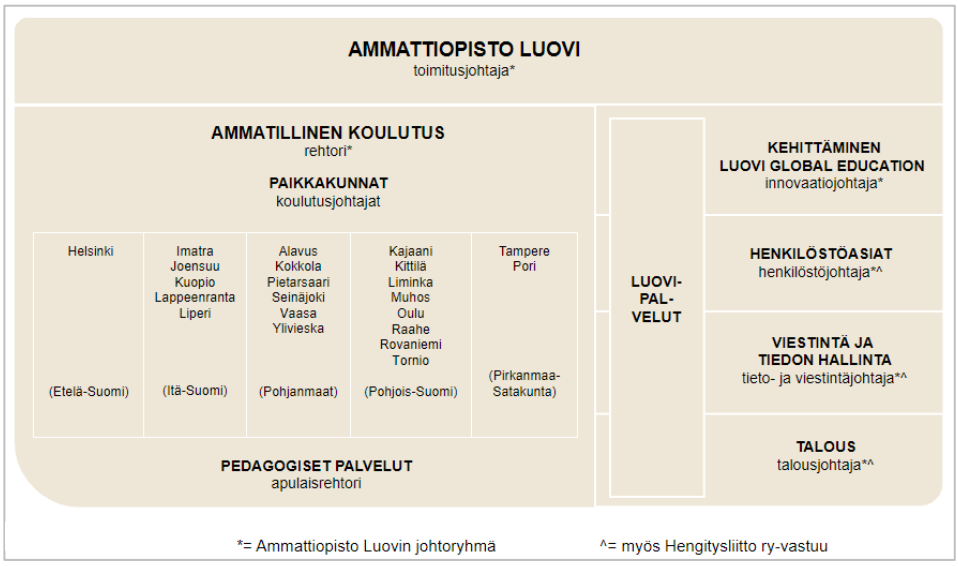
2.1 Suomen suurin ammatillinen erityisoppilaitos

Ammattiopisto Luovi on ammatillinen erityisoppilaitos, joka järjestää koulutusta vaativaa erityistä tukea opinnoissaan tarvitseville. Luovi toimii ympäri Suomen kaikkiaan 31 paikkakunnalla, kuten Alavudella, Helsingissä, Lappeenrannassa, Liperissä, Oulussa, Rovaniemellä, Tampereella ja Vaasassa. Luovi on Suomen suurin ammatillinen erityisoppilaitos sekä ammatillisen erityisopetuksen merkittävä kehittäjä. (Ammattiopisto Luovi 2023d.)

Vuoden 2023 alussa Luovista tuli osakeyhtiö. Koulutuksen järjestäjä ja työnantaja on Ammattiopisto Luovi Oy ja oppilaitos on nimeltään Ammattiopisto Luovi. Luovissa työskentelee noin 870 työntekijää. Henkilöstömäärä on kasvanut voimakkaasti oppivelvollisuuslain (1214/2020) tultua voimaan. Opetus- ja ohjaustehtävissä sekä opiskeluhyvinvoinnin parissa henkilöstöstä työskentelee 90 prosenttia. Muu henkilöstö työskentelee hallinnollisissa ja ydintehtävää tukevissa Luovi-palveluissa. (Ammattiopisto Luovi 2023c.) Opiskelijoita on ympäri Suomea sekä lähiopetuksessa että satelliittiopetuksessa yhteensä yli 2.000. Luovissa voi opiskella valmentavassa koulutuksessa sekä suorittaa ammatillisia tutkintoja. (Ammattiopisto Luovi 2022.)

Valmentavia koulutuksia ovat tutkintokoulutukseen valmentava koulutus (TUVA) ja työhön ja itsenäiseen elämään valmentava koulutus (TELMA). Ammatillisia perustutkintoja ovat esimerkiksi eläintenhoitaja, IT-tukihenkilö, kiinteistönhoitaja, kokki, kuorma-autonkuljettaja, leipuri-kondiittori, levyseppähitsaaja, maalari, mediapalvelujen toteuttaja, merkonomi, puuseppä ja puutarhuri. Luovi on sopiva opiskelupaikka henkilöille, jotka tarvitsevat opinnoissaan ja työllistymisessään yksilöllistä tukea ja ohjausta. Vaativan erityisen tuen palveluja ovat esimerkiksi henkilökohtainen oppimisen tuki, opetusjärjestelyt, hyvinvointia tukevat palvelut ja monialainen työskentely verkostojen kanssa. (Ammattiopisto Luovi 2023d.)

Luovin organisaatio koostuu ammatillisesta koulutuksesta ja valtakunnallisesti toteutettavista Luovi-palveluista. Luovi-palvelut mahdollistavat ydintehtävää eli vaativan erityisen tuen ammatillisen koulutuksen järjestämistä sekä ammatillisen erityisopetuksen kehittämis-, ohjaus- ja tukitehtävää. Luovi-palveluihin kuuluvat digi-, haku- ja neuvonta-, henkilöstö-, kehittämis-, talous- ja hankinta- ja viestintäpalvelut sekä pedagogiset palvelut. Kuviossa 1 on esitetty Luovin vuoden 2023 organisaatio. (Ammattiopisto Luovi 2023c.)



Kuvio 1. Ammattiopisto Luovin organisaatio (Ammattiopisto Luovi 2023c).

Hengitysliitto ry omistaa 100 prosenttia Ammattiopisto Luovin osakkeista. Luovi tuottaa omistajalleen eli Hengitysliitolle palvelusopimuksen mukaisesti henkilöstö-, talous-, tiedonhallinta- ja digipalveluja. Luovi hankkii Hengitysliitolta kiinteistöpalvelut. (Ammattiopisto Luovi 2023c.)

2.2 Luovin kurssi

Luovin strategia on nimeltään Luovin kurssi. Luovin kurssi kuvaa toiminnan yhteistä suuntaa ja päämäärää ja siihen on kirjattu Luovin arvot, missio, visio, toimintaympäristön analyysi, strategiset tavoitteet, kehittämisen painopisteet sekä Luovin toimintaa ohjaavat keskeiset linjaukset ja tavoitteet. Luovin tehtävänä on vaativan erityisen tuen ammatillinen koulutus ja sen uudistaminen. (Ammattiopisto Luovi 2022.)

Luovin missio: ”Oma väylä työhön ja hyvään elämään” on Luovin olemassaolon perusta ja täsmentää Luovin yhteiskunnallista tehtävää. Luovin visio: ”Paras paikka monenlaisten osaajien maailmassa” on tulevaisuudessa sijaitseva tavoitekuva, jota kohti Luovin kompassi on osoitettu. Visio antaa luovilaisten työlle merkityksen ja suunnan. Vision mukaisesti Luovissa:

- luodaan yhdessä työelämän kanssa uudenlaisia oppimisen keinoja, jotta jokainen opiskelija löytää juuri hänelle parhaan, ihmisen kokoisen paikan
- tehdään työtä, jonka kautta muuttuvasta maailmasta tulee suvaitsevaisempi ja sallivampi – monenlaisten osaajien maailma
- on opiskelijoilleen paras opiskeluympäristö hankkia osaamista ja henkilöstölleen paras työyhteisö työskennellä. (Ammattiopisto Luovi 2022.)

Luovin tavoitteet ovat:

- ”Täsmätyöhön ja hyvään elämään edistyksellisesti ja yhteistyöllä.”
- ”Erinomaisiin tuloksiin pääsemme tunnustetulla Luovi-laadulla******.”
- ”Tavoitteet todeksi tasapainoisella taloudella.”
- ”Huippuosaajiksi ilon kautta.” (Ammattiopisto Luovi 2022).

Luovi toimii vastuullisesti ja yhteisten periaatteiden mukaisesti. Jokainen luovilainen vastaa itse omassa työssään Luovi-laadun toteuttamisesta. Jokainen luovilainen huolehtii myös talouden pitämisestä tasapainossa sekä ennakoi muutoksen tuulia. Luovissa iloitaan yhdessä arjen onnistumisista. Luovin tavoitteet antavat toiminnalle suuntaviivat kohti visiota. Kehittämisen painopisteiksi on Luovissa valittu ne asiat, joissa täytyy onnistua, jotta matka voi edetä maaliin toivotulla tuloksella. (Ammattiopisto Luovi 2022.)

Luovin arvot ovat:

- **L**uottamus (Ammattiopisto Luovi 2023b)
- **U**udistajuus
- **O**saaminen
- **V**älittäminen
- **I**lo (Ammattiopisto Luovi 2022).

Aikaisemmin Luovin arvona oli luovuus, mutta se muutettiin luottamukseksi. Luottamus on keskeinen edellytys toimivalle esihenkilötyölle ja työyhteisölle sekä tulevaisuudessa menestyvälle organisaatiolle. Luottamuksen merkitys on korostunut Luovin sisällä eri toiminnoissa ja laajemmin yhteiskunnassa esimerkiksi epävarmuutta lisäävän maailmanpoliittisen tilanteen takia. Luovuus sisältyy edelleen arvoihin osana uudistajuutta ja osaamista. (Ammattiopisto Luovi 2023b.) Osaaminen on arvo, joka näkyy Luovin toiminnassa esimerkiksi siten, että sen avulla halutaan varmistaa Luovin toiminnan laadukkuus. Luovin toiminnan on tarkoitus luoda arvoa laajalle joukolle (kuvio 2).

Kuvio 2. Luovi luo arvoa (Ammattiopisto Luovi 2022).

Luovi luo toiminnallaan arvoa muun muassa opiskelijoille, opiskelijoiden huoltajille, työelämälle ja yhteiskunnalle. Luovi haluaa luoda arvoa myös omalle henkilöstölleen. Henkilöstön osaamisesta huolehtiminen on yksi arvon luomisen keinoista. (Ammattiopisto Luovi 2022.)

2.3 Digitaalinen Luovi

Digitalisaatio näkyy Luovin toiminnassa vahvasti ja digiturvallisuuteen liittyvän osaamisen merkittävyys on tunnistettu. Luovissa on käytössä esimerkiksi useita erilaisia digilaitteita, kuten 3D-tulostin, robotit, VR-lasit, taikalattia, Yeti-tablet ja dokumenttikamera. Luovi haluaa olla edelläkävijä ja hyödyntää toiminnassaan digitalisaatiota. Luovissa otetaan rohkeasti käyttöön uutta tekniikkaa, uusia työkaluja ja digipalveluja silloin, kun ne tuottavat lisäarvoa toiminnalle, henkilöstölle, opiskelijoille tai sidosryhmille. (Ammattiopisto Luovi 2023a.) Digitaalisuuden hyödyntäminen edellyttää henkilöstöltä digiturvaosaamista.

Luovissa hyödynnetään digitalisaatiota myös monimuotoisen opiskelun mahdollistajana. Tavoitteena on mahdollistaa digitaalinen oppiminen mahdollisimman monin tavoin. (Jokelainen 2023.) Kuviossa 3 on esitetty erilaisia digitaalisen oppimisen mahdollisuuksia paikan ja ajan suhteen, joita Luovin koulutuksen henkilöstö voi hyödyntää työssään.

Kuvio 3. Opiskelijan digitaalisen oppimisen mahdollisuudet (Jokelainen 2023).

Ammattiopisto Luovissa digiosaamisen kasvattamisesta halutaan huolehtia ja digiturvallisuuteen liittyvä osaaminen koetaan keskeiseksi koko henkilöstöltä vaadittavaksi taidoksi tulevaisuuden työelämässä. Digiturvallisuus on määritelty

Luovissa tavoitetilaksi, jossa digitaaliseen toimintaympäristöön voidaan luottaa. Digiturvallinen toiminta on turvallista ja hallittua sekä tavallisissa oloissa että häiriötilanteissa. (Ammattiopisto Luovi 2023a.)

Luovi osallistui syksyllä 2022 kalasteluharjoitukseen, jossa henkilöstölle lähetettiin huijausviesti, joka sisälsi kehotuksen vaihtaa salasana välittömästi viestissä tulleen linkin kautta. Valitettavasti harjoituksen tulokset eivät olleet erinomaiset. Liian moni klikkasi viestin linkkiä sen sijaan, että olisi malttanut rauhoittua viestin äärelle ja varmistaa sen todenmukaisuutta. Kalasteluharjoitus järjestettiin, koska Luovissa oli jo tunnistettu tarve digiturvallisuusosaamisen kehittämiselle. (Ammattiopisto Luovi 2023a.)

Harjoituksen jälkeen Luovissa kehitettiin digiasioita muun muassa päivittämällä Luovin Satamassa (henkilöstön intra) olevaa Digisivustoa. Digisivustolla on muun muassa Digiturvallisuusosio, joka sisältää ohjeita digiturvaan liittyen (Ammattiopisto Luovi 2023a). Kuviossa 4 on esitetty ote Digiturvallisuusosiossa tällä hetkellä olevista aiheista.

Kuvio 4. Ote Digiturvallisuusosiosta Luovin intrassa (Ammattiopisto Luovi 2023a).

Luovilaiset käsittelevät työssään paljon henkilötietoja ja hyödyntävät erilaisia digilaitteita ja -ohjelmia. (Ammattiopisto Luovi 2023a.) On tärkeää, että koko henkilöstö osaa toimia digiturvallisesti, jotta Luovi pystyy suojaamaan hallussaan olevat tiedot ja varmistamaan toiminnan luotettavuuden. Kun henkilöstöllä on riittävä digiturvaosaaminen, Luovi voi turvallisesti hyödyntää käytössä olevia digityökaluja ja -palveluja sekä ottaa myös uudenlaisia digityökaluja ja -palveluja tulevaisuudessa käyttöön.

2.4 Luovin osaamiskartta

Luovin kurssin eli strategian mukaisena tavoitteena on, että osaaminen vastaa ja ennakoi sille asetettuja tavoitteita. Luovissa osaamisen kehittäminen perustuu strategian pohjalta laadittuun osaamiskarttaan (kuvio 5), joka sisältää esimerkiksi digitaidot. Tällä hetkellä digitaidot tarkoittavat Luovissa kykyä käyttää digitaalisia palveluja ja laitteita ja hyödyntää niitä omassa työssään. (Ammattiopisto Luovi 2022.)

Kuvio 5. Luovin osaamiskartta (Ammattiopisto Luovi 2022).

Jokainen luovilainen osallistuu osaamiskartan pohjalta ja oman tiimin tavoitteisiin peilaten tiiminsä tärkeimpien osaamisten määrittelyyn sekä osaamisen kehittämisen suunnitteluun. Luovissa tehdään sparrauskeskustelujen (tiimien kanssa käytävät keskustelut) yhteydessä osaamisen kehittämisen suunnittelua, joka toimii pohjana jokaisen työntekijän henkilökohtaiselle osaamisen kehittämiselle, jota jokainen luovilainen käy läpi esihenkilönsä kanssa Luotsi-keskusteluissa eli kehityskeskusteluissa. (Ammattiopisto Luovi 2022.) Tulevaisuudessa digiturvallisuuden halutaan olevan vahvana osana Luovin henkilöstön osaamisen kehittämistä. Digitaidot sisältävät myös digiturvallisuudesta huolehtimisen ja siinä onnistuminen edellyttää digiturvan osa-alueiden perusteiden hallintaa.

3 Digitaalinen yhteiskunta

3.1 Digitalisaatio

Digitalisaatio eli digitaalisen teknologian käyttö palveluissa ja ihmisten välisessä vuorovaikutuksessa on nykyään jo arkipäivää. Teknologia kehittyy nopeasti ja se muuttaa toimintamalleja. (Sitra 2020.) Perinteisten organisaatioiden muutosta digitaalisiksi voidaan kutsua digimuutokseksi. Osana digimuutosta on lähes aina myös organisaation kulttuurillinen muutos, jossa henkilöstön käytökseen ja ajatteluun pyritään vaikuttamaan. (Savolainen & Lehmuskoski 2017, 13, 17.) Teknologinen kehitys vaatii työelämässä uuden opettelua. Organisaatioiden on tärkeää tarjota uuteen toimintaympäristöön soveltuvia koulutus- ja kehittymismahdollisuuksia henkilöstölleen. (Työterveyslaitos 2022.)

Organisaatioille digitalisaatio on keino uudistaa ja kehittää toimintaa (Pyyhtiä 2019, 125). Digitalisaatio mahdollistaa asiakaslähtöisyyden, tuottavuuden parantumisen ja paremman laadun, mutta samalla se haastaa organisaatioita toiminnalliseen muutokseen (Valtioneuvosto 2022). Käytännössä digitalisaatiossa on siis kyse uuden mahdollistamisesta ja organisaatiokulttuurin muutoksesta (Kasvi 2019). Organisaatiokulttuurin puutteet ovat merkittävä este organisaatioiden menestykselle digitaalisessa maailmassa (Goran, LaBerge & Srinivasan 2017). Menestyäkseen organisaatioiden on kyettävä kehittämään osaamista ja uudistuttava jatkuvasti (Valtioneuvosto 2022).

Koronapandemian aikana monen organisaation toiminta uudistui pakon sanelemana merkittävästi. Esimerkiksi etäyhteyksien käyttäminen yleistyi runsaasti. Teknologinen muutos jatkuu vieläkin ja on odotettavissa, että teknologiaosaamisen merkitys työelämässä korostuu edelleen. (Dufva & Rekola 2023, 48, 54.) Digitalisaation onnistuminen edellyttää, että henkilöstöllä on pääsy tarvittavaan tietoon ja osaamiseen, koska digitalisaation ytimessä on tiedonhallinta. Digitalisaatio perustuu sille, että organisaatio tietää, mitä tietovarantoja ja -virtoja sillä on. Lisäksi organisaation täytyy tietää, mistä tiedot kerätään, mihin niitä käytetään ja miten niitä hallitaan. (Kasvi 2019.)

Koronapandemia herätti näkemään myös digitaalisten riskien maailmaa. (Korpiola & Poutanen 2021, 10). Digitalisaatio avaa uusia kanavia esimerkiksi syrjinnälle, vihalle ja sodalle (Lindgren, Mokka, Neuvonen & Toponen 2019, 19). Ukrainan sotakin on osoittanut, että yksi sodankäynnin muoto ovat nykyisin kyberhyökkäykset. Ei olekaan ihme, että joitakin digitalisaatio myös pelottaa. Digitaalista luottamusta uhkaavat esimerkiksi myös verkkohäirintä, perättömät ilmiannot, tietovuodot ja datan väärinkäytökset (Korpiola & Poutanen 2021, 151). Digitalisaatio on haastava ilmiö (Lindgren ym. 2019, 18).

Digitalisaatiossa on kyse myös resurssien ja vallan uudelleenjaosta. Digitalisaation myötä on muotoutunut uusia vallan ja hallinnan keinoja sekä rakenteita. Esimerkiksi alustat säätelevät ihmisten käyttäytymistä ja vieläpä huomaamattomasti. Onkin tärkeää, että ihmiset ymmärtäisivät digitaalista maailmaa. (Lindgren ym. 2019, 19, 21.) Teknisten valmiuksien lisäksi on ymmärrettävä teknologiaa. Voidaan puhua digitaalisesta sivistyksestä, jonka avulla pystyy huolehtimaan turvallisuudesta, oikeuksista ja velvollisuuksista digitalisoituvassa yhteiskunnassa. Digitaalinen sivistys mahdollistaa muun muassa verkossa tarjolla olevien sisältöjen arvioinnin ja valeinformaation tunnistamisen sekä datatalouden ymmärtämisen. (Dufva & Rekola 2023, 54.)

Digitaalinen talous koostuu muun muassa internetistä, digilaitteista, verkostoista, ohjelmistoista ja digitaalisista palveluista (kuvio 6). Digitaalinen talous sisältää liiketoiminnan, ihmiset, laitteet, datan ja tuotteet. (Hiltunen 2023.) ”Internet on parasta ja pahinta, mitä meille on tapahtunut” kirjoittaa Hyppönen (2021, 9). Hiltunen (2023) tarkentaa, että digitalisaatio on parasta, mitä meille on tapahtunut, mutta siellä tosiaan on mukana myös pieni paha, joka täytyy osata huomioida. Digitalisaatioon liittyy puolia, joista on oltava tietoisia, jotta emme olisi niin haavoittuvaisia. Digitalisaatiota voidaan käyttää esimerkiksi myös perusteettoman valvonnan välineenä. Kun osaamme varautua, pystymme hyödyntämään digitalisaatiota turvallisesti. (Hiltunen 2023.) Digitaalisen toiminnan turvaamisen onnistuminen edellyttää myös organisaatioiden henkilöstön osaamisen kehittämistä (Valtiovarainministeriö 2020, 10).

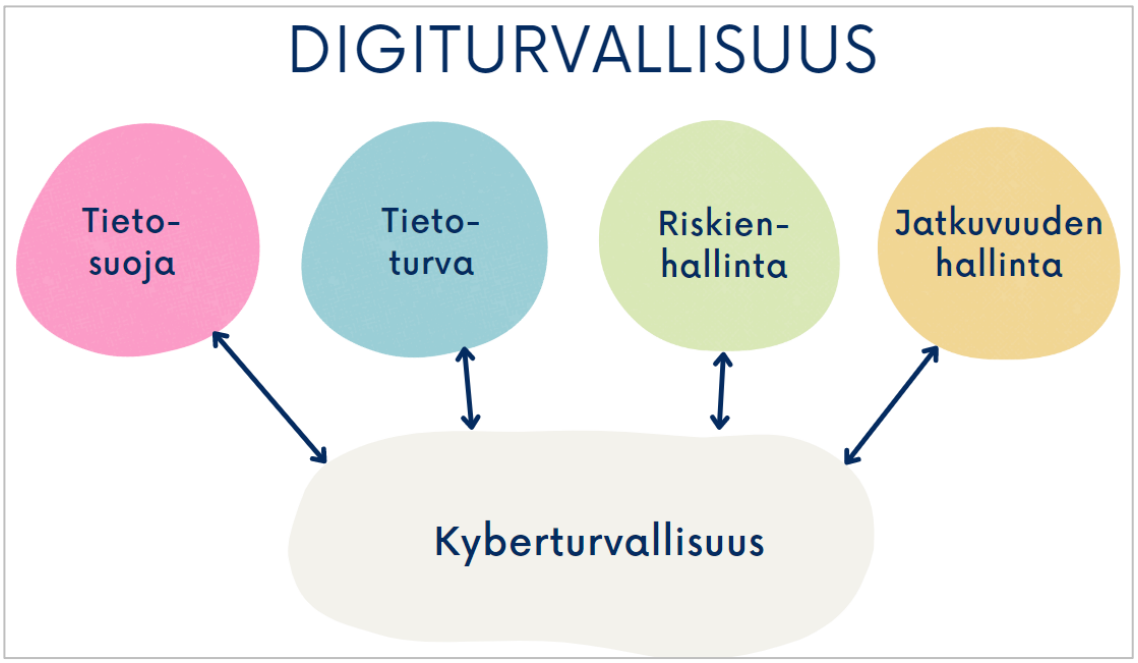
Kuvio 6. Digitaalinen talous (Hiltunen 2023).

Organisaation kannattaa kehittää henkilöstönsä kykyä varautua digitaalisen maailman uhkiin lisäämällä henkilöstön digiturvallisuustietoisuutta. Tällöin henkilöstö osaa varautua myös esimerkiksi informaatiovaikuttamisen uhkiin. Kun digiturvatietoisuus lisääntyy, kehittyy yksilön digiturva-asenne, jolloin hänen käytöksestään tulee digiturvallisempaa. (Kirves, Pelttari & Vänttinen 2022.)

3.2 Digiturvallisuus

Digitaalinen turvallisuus on terminä melko uusi ja osin vielä vakiintumaton. Digitaaliseen turvallisuuteen voidaan määritellä kuuluvaksi tietosuoja, tietoturva, riskienhallinta, toiminnan jatkuvuuden hallinta ja kyberturvallisuus. (Valtiovarainministeriö 2020.) Digi- ja väestötietovirasto (2023) on määritellyt, että: ”Digitaalisella turvallisuudella eli digiturvalla pyritään varmistamaan, että digitaalinen toimintaympäristö on luotettava, turvallinen ja saatavilla.”. Digiturvallisuudessa onnistuminen edellyttää kykyä varautua digitaaliseen toimintaympäristöön kohdistuviin uhkiin ja kykyä kestää häiriötilanteita. Lisäksi niistä on pystyttävä palautumaan mahdollisimman hyvin ja nopeasti. (Digi- ja väestötietovirasto 2023.)

Digiturvallisuus on tavoitetila, jossa digitaaliseen toimintaympäristöön voidaan luottaa. Digiturvallinen toiminta on turvallista ja hallittua sekä tavallisissa oloissa että häiriötilanteissa. (Digi- ja väestötietovirasto 2022.) Digiturvan avulla kehitetään turvallisuutta ja ylläpidetään luottamusta organisaation toimintaan (Rousku ym. 2019). Kuviossa 7 on määritelty digiturvallisuuden osa-alueiden suhteet toisiinsa mukaillen Valtiovarainministeriön (2020) määrittelyä.



Kuvio 7. Digiturvallisuuden osa-alueet (mukaillen Valtiovarainministeriö 2020).

Digitaalinen turvallisuus ei ole organisaation tai yhteiskunnan muusta toiminnasta erillinen kokonaisuus, vaan sen toteutusalueet ulottuvat digitaalisen maailman ulkopuolellekin. Digiturvallisuus on olennainen osa organisaatioiden kaikkea toimintaa. (Digi- ja väestötietovirasto 2023.) Kuviossa 8 on esitetty Digi- ja väestötietoviraston määrittely digiturvallisuudesta. Valtiovarainministeriö (2020) on määritellyt, että:

> Digitaalisen turvallisuuden kehittäminen on riskienhallintaan perustuvaa toiminnan jatkuvuuden ja varautumisen, tietoturvallisuuden ja tietosuojan avulla tapahtuvaa turvallisuuden kehittämistä, joka samalla on myös kyberturvallisuuden kehittämistä.

Kuvio 8. Digiturvallisuuskokonaisuus (Digi- ja väestötietovirasto 2023).

Digitaalinen turvallisuus voi olla vahva kilpailuetu tai merkittävä digitalisaation hidastaja ja epävarmuutta aiheuttava asia. Digiturvallisuuden merkitys korostuu, kun aiempaa suurempi osuus organisaatioiden liiketoiminnasta muodostuu tietojenkäsittelyn hyödyntämisellä. Turvallisuus mahdollistaa digitalisaation täysimääräisen hyödyntämisen. Digitalisaation onnistumisen välttämättömiä edellytyksiä ovat tietoturva ja tietosuoja. Jokaisen organisaation on tarpeen saada henkilötietojen käsittelyn ja tietosuojaosaamisen perusasiat ja perusta kuntoon. (Andreasson & Ylipartanen 2022, 54.)

3.3 Tietosuoja

Tietosuoja tarkoittaa ihmisten yksityisyyden suojaamista ja henkilöä koskevien tietojen suojaamista oikeudettomalta käytöltä henkilötietoja käsiteltäessä (Valtiovarainministeriö 2020). Tietosuoja on perusoikeus eli jokaisella henkilöllä on oikeus henkilötietojensa suojaan. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietojen käsittely on mahdollista. Tietosuoja turvaa rekisteröidyn eli henkilön, jonka henkilötietoja käsitellään, oikeuksien ja vapauksien toteutumisen. (Tietosuojavaltuutetun toimisto 2023b.)

Tietosuoja-asetuksen ((EU) 2016/679, GDPR) artiklassa 4 on määritelty, että henkilötiedoilla tarkoitetaan:

> ”kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä ’rekisteröity’, liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella”.

Henkilötiedon käsite on laaja ja lähtökohtaisesti kaikki tunnistettavissa olevaa luonnollista henkilöä koskevat tiedot ovat henkilötietoja, joiden käsittelyyn sovelletaan tietosuoja-asetusta. Tietyt henkilötiedot saattavat olla erityisen riskialttiita yksityisyyden kannalta. Näistä aikaisemmin arkaluonteisiksi kutsutuista henkilötiedoista käytetään tietosuoja-asetuksessa nimitystä erityiset henkilötietoryhmät. (Korpisaari, Pitkänen & Warma-Lehtinen 2022, 58, 167.)

Erityisten henkilötietoryhmien tietojen käsittely on lähtökohtaisesti kiellettyä. Näitä tietoja ovat terveystiedot, uskonnollinen tai filosofinen vakaumus, seksuaalinen suuntautuminen tai käyttäytyminen, rotu tai etninen alkuperä, poliittiset mielipiteet ja ammattiliiton jäsenyys. Myös geneettisten tai biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten on kiellettyä. (GDPR 9 artikla.) Erityisiin henkilötietoryhmiin kuuluvien tietojen käsittely on kuitenkin mahdollista, jos jokin käsittelyedellytyksistä ja erityisistä käsittelyperusteista täyttyvät (Korpisaari ym. 2022, 167).

Luovissa opiskelijoista käsitellään perustietojen lisäksi myös terveyteen liittyviä tietoja opintojen järjestämiseksi. Opiskelijoiden terveystiedot ovat erityisten henkilötietoryhmien tietoja, mutta niitä voidaan käsitellä, koska ammatillisen erityisopetuksen järjestäminen edellyttää tietojen käsittelemistä. Henkilötietoja on osattava käsitellä oikein, koska esimerkiksi niiden joutuminen vääriin käsiin altistaa opiskelijat identiteettivarkauksille ja jopa kiristysyrityksille.

Varmistamalla koko henkilöstön tietosuojaosaamisen, organisaatio saavuttaa merkittäviä hyötyjä ja etuja itselleen, henkilöstölleen ja asiakkailleen. Se hyötyy muun muassa tuottavuuden, tehokkuuden ja palvelun laadun parantumisena

sekä riskien todennäköisyyksien ja vaikutusten pienentymisenä. Henkilöstö hyötyy oman oikeusturvansa parantumisena, kun esimerkiksi henkilöstöosasto osaa käsitellä työntekijöiden tietoja oikein. Henkilöstö kartuttaa myös nykyään tarvittavia kansalaistaitoja, joita ovat esimerkiksi tietosuoja ja -turvaosaaminen. Henkilöstön työviihtyvyys parantuu myös, kun henkilötietoja ei tarvitse käsitellä enää epävarmuudessa. Tällöin myös henkilöstön työteho paranee. Asiakkaat hyötyvät ennen kaikkea siten, että voivat luottaa heidän tietojaan käsiteltävän lainmukaisesti. Investointi henkilöstön tietosuojaosaamiseen maksaa itsensä takaisin tuottoina, kustannussäästöinä ja tehokkuutena. (Andreasson & Ylipartanen 2022, 53–54.)

3.3.1 Tietosuojalainsäädäntö

Henkilötietojen suoja perustuu pitkälti EU-sääntelyyn. Merkittävä uudistus EU:n tietosuojasääntelyssä tapahtui keväällä 2018, jolloin EU:n tietosuoja-asetusta (GDPR) alettiin soveltaa kaikissa EU-maissa. GDPR:n mahdollistaman sääntelyliikkumavaran toteuttamiseksi Suomessa on säädetty kansallinen tietosuojalaki (1050/2018). Tietosuojalaki ei ole itsenäinen sääntelykokonaisuus, vaan sillä täydennetään ja täsmennetään tietosuoja-asetusta. Siten tietosuojalakia sovelletaan rinnakkain tietosuoja-asetuksen kanssa. (Alapuranen 2020, 8.)

Suomessa on voimassa paljon myös muuta henkilötietojen käsittelyä koskevaa erityislainsäädäntöä, erityisesti koskien työntekijän henkilötietojen käsittelyä. Työntekijän henkilötietojen käsittelyyn sovelletaan lakia yksityisyyden suojasta työelämässä (759/2004), sähköisen viestinnän palvelulakia (917/2014), työterveyshuoltolakia (1383/2001) ja turvallisuusselvityslakia (726/2014), jossa säädetään perusteista, joilla työntekijälle voi tehdä turvallisuusselvityksen. (Bruun 2022, 264.) Tietosuoja-asetuksen, tietosuojalain sekä muun tietosuojasääntelyn lisäksi Luovi noudattaa toiminnassaan muun muassa Opetushallituksen suositusta julkisuudesta ja tiedonhallinnasta opetustoimessa. Luovin henkilöstöllä tulee olla runsaasti monipuolisia tietoja ja taitoja, jotta he osaavat käsitellä henkilötietoja oikein.

3.3.2 Henkilötietojen käsittely

Riippumatta organisaation toimialasta ja muodosta, tiedot ja erityisesti henkilötiedot, ovat yksi organisaatioiden tärkeimmistä omaisuuksista (Warma-Lehtinen 2021, 9). Henkilötiedot ovat arvokkaita inhimillisistä ja taloudellisista syistä (Järvinen 2022a, 134). Data on rahaa, toteaa Hyppönen (2021, 33). Dataa tulisikin käsitellä organisaatioissa yhtä huolellisesti kuin niissä on totuttu käsittelemään rahoja.

Henkilötietoja saa käsitellä, kun sille on jokin tietosuoja-asetuksessa määritelty peruste. Näitä perusteita ovat:

- rekisterinpitäjän lakisääteinen velvoite
- sopimus
- rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu
- yleistä etua koskeva tehtävä tai julkinen valta
- elintärkeiden etujen suojaaminen
- rekisteröidyn suostumus (viimesijainen peruste, jota voidaan käyttää vain perustellusti ja vain silloin, kun mikään yllä oleva ei käy perusteeksi). (GDPR, artikla 6.)

Henkilötietojen käsittelyä koskevien periaatteiden mukaan henkilötietoja on:

- käsiteltävä lainmukaisesti, asianmukaisesti ja läpinäkyvästi,
- kerättävä ja käsiteltävä tiettyä, nimenomaista ja laillista tarkoitusta varten,
- kerättävä vain tarpeellinen määrä käsittelyn tarkoitukseen nähden,
- päivitettävä aina tarvittaessa: epätarkat ja virheelliset henkilötiedot on poistettava tai oikaistava viipymättä,
- säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamiseksi,
- käsiteltävä luottamuksellisesti ja turvallisesti (GDPR artikla 5).

Luovissa opiskelijoista käsiteltäviä tietoja ovat esimerkiksi nimi, henkilötunnus, osoite, puhelinnumero, sähköpostiosoite, asuinkunta, kotikunta ja äidinkieli sekä vaativan erityisen tuen tiedot. Opetushallituksen linjauksen mukaisesti ammatillisessa erityisoppilaitoksessa opiskelevan opiskelijan nimi on salassa pidettävä

tieto (Vehkamäki, Lahtinen & Vanttaja 2018, 20). Luovissa käsitellään myös salassa pidettäviä opiskelijoiden terveydentilaa koskevia tietoja lakiin ammatillisesta koulutuksesta (531/2017) perustuen. Terveyteen liittyviä tietoja on oikeus käsitellä ammatillisen erityisopetuksen järjestämiseksi.

Työntekijöistä käsiteltäviä henkilötietoja ovat esimerkiksi nimi, henkilötunnus, kotiosoite, palkkatiedot, koulutustiedot ja mahdollinen ammattiliiton jäsenyys sekä mahdolliset ulosottotiedot. Ammattiliiton jäsenyys on erityisten henkilötietoryhmien tieto, jota voidaan käsitellä ammattiliiton jäsenmaksun veloittamiseksi suoraan palkasta työntekijän suostumuksella. Työntekijöiden henkilötietojen oikeanlainen käsittely edellyttää henkilöstöpalveluissa vahvaa osaamista, vastuullisuutta ja kykyä noudattaa toimintaohjeita.

Rekisterinpitäjällä on vastuu siitä, että se pystyy osoittamaan, että sen toiminnassa noudatetaan tietosuojaperiaatteita (GDPR artikla 5). Rekisterinpitäjän täytyy toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että käsittelyssä noudatetaan tietosuoja-asetusta ja osoittaa, että käsittelytoimet ovat myös tehokkuudeltaan tietosuoja-asetuksen mukaisia. (Andreasson & Ylipartanen 2022, 213.) Osoitusvelvollisuutta todennetaan Luovissa muun muassa tietosuojadokumentaatiolla, jonka osana Luovissa on laadittu Luovi.fi-sivustolle ja Satamaan (intra) myös tietosuojaselosteita, joiden avulla toteutetaan henkilötietojen käsittelystä informointia.

3.3.3 Henkilötietojen käsittelystä informointi

Rekisterinpitäjän on informoitava henkilötietojen käsittelystä rekisteröityjä. Informointivelvollisuus on osa rekisterinpitäjän dokumentointivelvollisuutta, koska henkilötietojen käsittelystä informoinnin on oltava saatavilla sähköisessä tai kirjallisessa muodossa. (Voutilainen 2019, 95–96.) Rekisteröityjä tulee informoida henkilötietojen käsittelystä läpinäkyvästi. Tiedot voidaan antaa eri tavoilla, kunhan ne ovat helposti ymmärrettävässä ja saatavilla olevassa muodossa sekä tiiviisti esitettynä. (Alapuranen 2020, 92.)

Henkilötietojen käsittelystä tulee informoida, jotta rekisteröidyt voivat käyttää heidän oikeuksiaan (Voutilainen 2019, 95). Rekisteröidyllä on muun muassa oikeus saada tietää, käsitteleekö rekisterinpitäjä hänen henkilötietojaan (Krakau & Haapalehto 2020, 218). Rekisteröidyn oikeudet määräytyvät tietosuoja-asetuksen mukaisesti. Rekisteröidyllä voi olla oikeus:

- saada tieto, käsitelläänkö hänen henkilötietojaan vaiko ei,
- saada tutustua tietoihin,
- oikaista tietoja,
- tulla unohdetuksi ja poistaa tietoja,
- käsittelyn rajoittamiseen,
- siirtää tiedot järjestelmästä toiseen,
- vastustaa käsittelyä,
- olla joutumatta automaattisen päätöksenteon kohteeksi. (Tietosuojavaltuutetun toimisto 2023b.)

Rekisteröity ei voi käyttää kaikkia oikeuksiaan kaikissa tilanteissa, vaan oikeudet vaihtelevat henkilötietojen käsittelyn perusteen mukaisesti (Tietosuojavaltuutetun toimisto 2023b). Esimerkiksi viranomaisrekistereistä ei voi pyytää poistettavaksi kaikkia tietoja. Organisaation on osattava käsitellä henkilötietojen tarkastuspyynnöt. (Tietosuojavaltuutetun toimisto 2023b.) Henkilöstön on hyvä tiedostaa, että he ovat itse rekisteröityjä suhteessa työnantajaan, jolloin he voivat saada neuvoja tietosuojavastaavalta myös omaa asiaansa koskien (Tietosuojavaltuutetun toimisto 2023d).

3.3.4 Tietosuojavastaava

Tietosuojavaltuutetun toimisto (2023d) määrittelee, että: ”Tietosuojavastaava on organisaation sisäinen asiantuntija, joka seuraa henkilötietojen käsittelyä ja auttaa tietosuojasäännösten noudattamisessa.”. Riippumaton tietosuojavastaava on erityisasiantuntija, joka toimii rekisterinpitäjän apuna. Tietosuojavastaava auttaa asiakkaita, henkilöstöä ja johtoa. Johtoa tietosuojavastaava avustaa tietosuoja-asioiden suunnittelemisessa ja toimeenpanossa. (Andreasson & Ylipartanen 2022, 106.)

Tietosuojavastaavalla on vastuu siitä, että hän hoitaa tietosuoja-asetuksen mukaiset tietosuojavastaavalle ainakin kuuluvat tehtävät (Andreasson & Ylipartanen 2022, 106). Tietosuojavastaavan tehtävänä on muun muassa antaa neuvoja sekä rekisterinpitäjälle että rekisteröidyille, seurata organisaatiossa tietosuojalainsäädännön noudattamista, kouluttaa henkilöstöä, tehdä tarkistuksia, valvoa vaikutustenarvioinnin toteutusta ja toimia yhteyshenkilönä tietosuojavaltuutetulle eli henkilötietojen käsittelyn lainmukaisuutta valvovalle viranomaiselle. Tehtäviään suorittaessa tietosuojavastaavan on huomioitava käsittelytoimiin liittyvä riski käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset huomioiden. (GDPR, artikla 39.) Yllä mainittu tehtävälista ei ole tyhjentävä, vaan rekisterinpitäjällä on mahdollisuus määritellä tietosuojavastaavalle muitakin tehtäviä (Korpisaari ym. 2022, 442).

Rekisterinpitäjä eli organisaation johto vastaa henkilötietojen käsittelyn lainmukaisuudesta (Voutilainen 2019, 122). Johdon on tarpeen toimia myös esimerkkinä henkilötietojen asianmukaisessa käsittelyssä. Henkilöstön tehtävänä on noudattaa annettuja ohjeita ja ilmoittaa havaitsemistaan poikkeamista (kuvio 9). (Andreasson & Ylipartanen 2022, 130–131.)

Kuvio 9. Tietosuojavastuut (mukaillen Voutilainen 2019, 122 ja Andreasson & Ylipartanen 2022, 106, 130–131).

Tietosuojavastaava on tehtäviään hoitaessaan vaitiolovelvollinen (Voutilainen 2019, 613). Tietosuojavastaavaa ei voi erottaa tai rangaista sen vuoksi, että hän

hoitaa GDPR:n mukaista tehtäväänsä (Andreasson & Ylipartanen 2022, 109). Tietosuojavastaava tekee tarvittaessa henkilötietojen vaarantumisesta tietoturvaloukkausilmoituksen tietosuojavaltuutetun toimistolle. Tietosuojavastaavan yhteystiedot on ilmoitettava tietosuojavaltuutetulle nimittämisen yhteydessä (Nyyssölä 2020, 283), jotta tietosuojavaltuutettu voi tarvittaessa olla yhteydessä tietosuojavastaavaan. Tietosuojavastaavan tulee olla helposti myös rekisteröityjen tavoitettavissa, joten hänen yhteystietonsa kannattaa laittaa helposti saataville (Korpisaari ym. 2022, 441) esimerkiksi organisaation kotisivuille.

Tietosuojavastaava tulee ottaa kehitystoimien suunnitteluun mukaan mahdollisimman aikaisessa vaiheessa. Tietosuojavastaavan tulee olla luotettu keskustelukumppani, jolla on tarvittavaa osaamista, sillä yksi organisaation pahimmista tietosuojariskeistä on osaamaton tietosuojavastaava. (Andreasson & Ylipartanen 2022, 110–111.) Osaava tietosuojavastaava pystyy auttamaan organisaatiota ja sen henkilöstöä henkilötietojen käsittelyssä ja varmistamaan, että organisaatio toimii tietosuojasääntelyn mukaisesti. Tietosuojavastaava tekee usein kehittämistä yhteistyössä tietoturvan parissa työskentelevien henkilöiden kanssa.

3.4 Tietoturva

Yksi tietosuojan toteuttamisen keino on tietoturva. Tietoturvan tarkoituksena on suojata organisaation tietoaineisto ja tietojärjestelmät. Tietoturva tarkoittaa myös esimerkiksi organisatorisia ja teknisiä toimenpiteitä, joiden avulla varmistetaan rekisteröidyn oikeuksien toteutuminen, järjestelmien käytettävyys sekä tiedon luottamuksellisuus ja eheys. (Tietosuojavaltuutetun toimisto 2023c.) Tietoturvan osalta kaikki voidaan kiteyttää kolmeen tavoitteeseen: luottamuksellisuus, eheys ja käytettävyys (Järvinen 2022b, 13–14).

Tiedon luottamuksellisuus tarkoittaa tietojen suojaamista ulkopuolisilta eli tiedot ovat vain niihin oikeutettujen käytettävissä (Opetushallitus 2023). Suojattavia tietoja ovat esimerkiksi liikesalaisuudet, palkanmaksutiedot ja sähköpostien sisältö. Teknisesti tietojen salaaminen on helppoa. Sen sijaan vaikeaa on saada

henkilöstö toimimaan siten, että he eivät tahattomasti vuoda luottamuksellisia tietoja tai päädy vahingossa huijareiden ansaan. Vielä vaativampaa on suojata organisaation laitteet ja verkko oikeudettomalta ulkopuoliselta käytöltä. (Järvinen 2022b, 13.)

Tietojen eheydellä tarkoitetaan sitä, että tiedot ovat loogisesti oikein ja niihin tehdään vain oikeutettuja muutoksia (Kyberturvallisuuskeskus 2020a). Esimerkiksi koko henkilöstöllä ei saa olla pääsyä palkkatietoihin. Tämä edellyttää käyttäjien tunnistamisen ja todentamisen lisäksi pääsyn hallintaa. (Järvinen 2022b, 14.) Pääsynhallinnan avulla varmistetaan, että tietoa ei käytetä ilman lupaa (Opetushallitus 2023). Tietojen eheys voi pettää esimerkiksi siten, että ohjelmistovika muuttaa tietoja tai hakkerit pääsevät murtautumaan organisaation verkkosivulle ja muuttamaan sen tietoja (Järvinen 2022b, 14).

Käytettävyys tarkoittaa sitä, että tiedot ovat niiden käyttöön oikeutettujen hyödynnettävissä esteettä (Kyberturvallisuuskeskus 2020a). Tietojen saatavuusongelmat eli laitteiden ja palveluiden toimimattomuus ovat kaikille tuttuja haasteita. Ongelmana voi olla, että tietokone ei käynnisty, nettiyhteys toimii pätkien tai tarvittavia tiedostoja ei löydy. Tietojen saatavuutta suojataan enimmäkseen teknisin keinoin. (Järvinen 2022b, 14–15.)

Tietoturvasta huolehtiminen jakaantuu tekniseen turvallisuuteen ja hallinnollisiin toimenpiteisiin (Rousku 2017, 71). Organisaation ja käyttäjien tulee huolehtia tietoturvasta suunnittelemalla, toteuttamalla ja valvomalla. Toimenpiteet voidaan Opetushallituksen (2023) mukaan jakaa kahdeksaan eri osa-alueeseen, jotka ovat:

1. hallinnollinen ja organisatorinen tietoturvallisuus
2. henkilöstöturvallisuus
3. fyysinen turvallisuus
4. tietoliikenneturvallisuus
5. laitteistoturvallisuus
6. ohjelmistoturvallisuus
7. tietoaineistoturvallisuus
8. käyttöturvallisuus (Opetushallitus 2023).

Organisaatioiden on osattava ratkaista erilaiset tietoturvaongelmat hyödyntääkseen digitalisaatiota (Gebremeskel, Jonathan & Yalew 2023, 50). Savolainen & Lehmuskoski (2017, 234) toteavat, että vanhan sanonnan mukaisesti tietoturva on yhtä vahva kuin heikoin lenkki. Tietoturvassa onnistuminen edellyttääkin muun muassa sitä, että henkilöstöllä on kyky kirjautua palveluihin turvallisesti.

3.4.1 Turvallinen kirjautuminen

Käyttäjätunnuksen ja salasanan sekä monivaiheisen tunnistautumisen avulla varmistetaan turvallinen kirjautuminen. Monivaiheinen tunnistautuminen tarkoittaa henkilöllisyyden varmistamista käyttäen kahta tai useampaa eri tunnistautumistapaa. Vaikka rikollinen saisi haltuunsa käyttäjätunnuksen ja salasanan, palveluun ei pysty kirjautumaan ilman lisätunnistetta. Kuviossa 10 on esitetty monivaiheinen tunnistautuminen. (Traficom 2023b.)

Kuvio 10. Monivaiheinen tunnistautuminen (Traficom 2023b).

Salasanan perimmäisenä olemuksena on toimia käyttäjän ja järjestelmän yhteisenä salaisuutena. Kokonaiset lauseet ovat hyviä salasanoja. Salasanassa kannattaa käyttää myös suomalaisia kirjaimia å, ä ja ö, jos palvelu hyväksyy kyseiset kirjaimet salasanaan, koska ulkomaiset hakkerit eivät yleensä osaa ääkkösiä. Tärkeintä on, että jokaista palvelua varten on oma salasanansa. Nykyohjeena on tehdä vahvat salasanat, joita vaihdetaan vain, jos niiden epäillään paljastuneen. Kaikista tärkein salasana on sähköpostin salasana. Siitä tulee tehdä

vahva ja se tulee suojata erittäin hyvin. Yleensä salasanojen vaihtolinkit lähetetään sähköpostiin, joten jos hakkeri onnistuu saamaan pääsyn siihen, mahdollistuu pääsy myös muihin järjestelmiin. (Järvinen 2022b, 94–98.)

Luovissa on käytössä monivaiheinen tunnistautuminen. Henkilöstöä on myös selkeästi ohjeistettu siitä, että käyttäjätunnukset ja salasanat ovat henkilökohtaisia. Lisäksi annetut ohjeet sisältävät salasanan muotovaatimukset. Henkilöstöä on neuvottu ottamaan monivaiheinen tunnistautuminen käyttöön kaikissa palveluissa, joissa se on mahdollista eli myös henkilökohtaisissa palveluissa. (Ammattiopisto Luovi 2023a.) Tämä senkin takia, jos henkilöstö käyttää ohjeiden vastaisesti henkilökohtaisissa palveluissa samoja salasanoja kuin työkäytössä olevissa sovelluksissa. Monivaiheinen tunnistautuminen lisää merkittävästi digipalvelujen käytön turvallisuutta (Traficom 2023b).

3.4.2 Digilaitteiden ja -palvelujen käyttö

Digilaitteiden ja -palvelujen turvallinen käyttö edellyttää henkilöstöltä monenlaista osaamista. Henkilöstön täytyy tietää, kuinka he voivat käyttää digilaitteita turvallisesti ja mitä ohjelmia ja sovelluksia he voivat käyttää. Henkilöstön tulee myös osata käyttää esimerkiksi turvatulostusta, lähettää sähköposteja turvallisesti sekä huolehtia tietoturvapäivitysten asentumisesta. (Ammattiopisto Luovi 2023a.)

Tietoturvapäivitykset ovat ensiarvoisen tärkeitä, jotta järjestelmät sekä laitteet pysyvät mahdollisimman hyvin suojattuina ulkoisia uhkia sekä virhetilanteita vastaan ja kaikki niille kehitetyt toiminnallisuudet tulevat käyttöön. Luovissa järjestelmien ylläpitäjät huolehtivat tietoturvapäivitysten säännöllisestä asentamisesta palvelimille ja jakelusta käyttäjien digilaitteille. Käyttäjien vastuulla on liittää laitteensa työpaikan tietoverkkoon säännöllisesti päivitysten asennuksen mahdollistamiseksi. (Ammattiopisto Luovi 2023a.) Päivitysten kohdalla ajalla on merkitystä. Erityisesti kriittisiksi merkityt päivitykset ja nollapäivähaavoittuvuuden korjaavat päivitykset täytyy asentaa välittömästi. (Järvinen 2022b, 36.)

Korona-ajan digiloikka on näkynyt erityisesti etätyön yleistymisenä. Esimerkiksi virtuaalisia työtiloja ja kokouksia hyödynnetään aiempaa enemmän. (Alasoini 2023, 278.) Etätyön lisääntyminen edellyttää aiempaa laajempaa osaamista henkilöstöltä, sillä etätyö tuo mukanaan riskejä digiturvallisuuteen. Käyttäjien on noudatettava työnantajan antamia ohjeita etätyöskentelyssä, jotta digiturvariskit voidaan minimoida. Lähtökohta digiturvalliselle etätyölle on työnantajan laitteiden käyttö. Lisäksi on tärkeää, että etätyötä tehdään vain luotetussa ja suojatussa verkossa. Työpaikan ulkopuolella tapahtuvassa työskentelyssä on myös tärkeää varmistua siitä, ettei ulkopuolisilla henkilöillä ole pääsyä työhön liittyviin aineistoihin eikä kuuloyhteyttä työhön liittyviin keskusteluihin. (Ammattiopisto Luovi 2023a.)

Työpaikalla fyysinen turvallisuus tulee niin sanotusti talon puolesta. Etätyössä työntekijän on vastattava fyysisestä turvallisuudesta itse. Työntekijän tulee nostaa työhuoneen turvallisuus työpaikan tasolle, mikäli hän käsittelee liikesalaisuuksia, henkilötietoja tai muita luottamuksellisia asioita. Työlaitteet ja työmateriaalit tulee siirtää lukittuun kaappiin työskentelyn päättyessä. Asunto tarvitsee suojakseen myös murtohälyttimet, sillä kodit ovat rikollisille helpompia kohteita kuin vartioidut ja lukitut toimistot. (Järvinen 2022b, 186.) Sekä lähi- että etätyössä on vaarana joutua myös digihuijausten uhriksi.

3.4.3 Digihuijaukset

Digihuijauksia ovat esimerkiksi haittaohjelmat, netti-, sähköposti- ja yrityshuijaukset, tietojenkalastelu ja kohdistetut hyökkäykset (Järvinen 2017, 73–100). Huijausten onnistumisen taustalla ovat esimerkiksi ihmisten varomattomuus ja hyväuskoisuus (Haasio 2017, 75). Erilaisissa tutkimuksissa on arvioitu, että yli 80 prosenttia erilaisista tietosuojaan ja tietoturvaan liittyvistä poikkeamista ja loukkauksista aiheutuu henkilöiden tahattoman, inhimillisen toiminnan takia (Kirves ym. 2022).

Huijausviestejä voi yrittää tunnistaa virheellisen sivuston osoitteen, uhkailun ja kiristyksen sekä poikkeustilanteeseen vetoamisen perusteella. Lisäksi

huijausviestin voi tunnistaa katteettomista lupauksista, kuten ainutlaatuisesta tarjouksesta tai voitosta arvonnassa, johon ei ole edes osallistunut. Huijauksilta voi yrittää suojautua esimerkiksi tarkastelemalla huolellisesti viestin lähettäjän tietoja ja verkkosivustojen osoitteita. (Traficom 2023a.) Varovaisuus ja terve epäily ovat perusasioita, jotka jokaisen täytyy muistaa (Haasio 2017, 75).

Tietojen kalastelu tarkoittaa käyttäjän huijaamista siten, että hänet houkutellaan kirjautumaan väärennetylle sivulle. Huijari kaappaa kirjautumistiedot ja mahdollisesti siirtää uhrin oikealle sivulle, jolloin uhri ei edes heti huomaa joutuneensa huijatuksi. Kalasteluviestien kehittyneempi muoto ovat keihäskalasteluviestit, jossa kohteet valitaan tarkoin ja huijausviestit näyttävät tulevan oman organisaation sisältä, kenties omalta esihenkilöltä. (Järvinen 2022b, 54–55.) Tyypillisesti huijaus pyritään lähettämään tietohallinnon nimissä, jolloin työntekijät todennäköisemmin lankeavat huijaukseen (Haasio 2017, 82).

Valitettavasti tietomurroista vaietaan usein (Kangas, Nenonen & Välimäki 2021, 225). Todellisuudessa niitä tapahtuu merkittävästi enemmän kuin uutisoidaan (Barzilay 2023). Viime aikoina muutamat organisaatiot ovat kertoneet avoimesti hyökkäyksen kohteeksi joutumisestaan. Tietoturvapäällikkö Matti Kuosmanen Savonia-ammattikorkeakoulusta kertoi vuoden 2022 lokakuussa Digiturvaviikon webinaarissa hyökkäyksestä, jonka kohteeksi Savonia joutui helmikuussa 2022. Tapauksessa ulkopuolinen hyökkääjä onnistui tekemään tietomurron opiskelijan tunnusten avulla todennäköisesti siksi, että opiskelija oli käyttänyt samaa käyttäjätunnusta ja salasanaa henkilökohtaisella some-tilillään, eikä Savonian opiskelijoilla ollut tuolloin käytössä monivaiheista tunnistautumista.

Hyökkääjä onnistui kirjautumaan opiskelijan tunnuksilla Savonian verkkoon ja löysi heikon kohdan vanhimmasta terveyspuolen opinnoissa käytössä olevasta älylääkevaunusta, johon ei ollut pystytty enää asentamaan päivityksiä. Hyökkääjä onnistui varastamaan noin 700 Savonian nykyisen tai entisen opiskelijan henkilötietoja, kuten nimen ja henkilötunnuksen ja julkaisi tietoja pimeässä Torverkossa. Osa opiskelijoista vaihtoi henkilötunnuksensa. Tapahtumasta seurasi Savoniassa kuukausien työ, kymmenien tuhansien eurojen kustannukset sekä mainehaittaa. (Kuosmanen 2022.)

Keski-Uudenmaan koulutuskuntayhtymä Keudaan kohdistui marraskuussa 2022 kyberhyökkäys, joka pysäytti sen koko IT-ympäristön lähes kuukaudeksi. Kyberhyökkäys toteutettiin LockBit-kiristyshaittaohjelmalla, joka sai saastutettua arviolta 60 prosenttia kaikista Keudan työasemista ja palvelimista. Hyökkäys koetteli voimakkaasti jatkuvuuden hallintaa. Tämän hetken tietojen mukaan hyökkäyksessä ei saatu haltuun tietosuojan piirissä olevia tietoja, mutta varmuudella asiaa ei ole saatu poissuljettua. Pelkästään hyökkäyksen suorat kustannukset nousevat yli 100.000 euroon. (Anttolainen 2023, 3.)

Organisaatioiden kannattaa olettaa, että ne joutuvat kyberhyökkäyksen kohteeksi. Kun hyökkäykseen varautuu, ovat sen seuraukset todennäköisesti pienemmät. (Barzilay 2023.) Verkkorikollisilta tulee suojautua sekä teknisin keinoin että henkilöstön toimintaohjein (Haasio 2017, 97). Käytännön vinkit peruskäyttäjille ovat tärkeitä, sillä koko henkilöstön tulisi osata tunnistaa yleiset huijaukset (Järvinen 2022b, 50, 239). Lisäksi organisaation tulee luoda kulttuuri, jossa henkilöstöä kannustetaan ilmoittamaan havaitsemistaan poikkeamista, haavoittuvuuksista ja uhkista sekä oppimaan virheistään (Kirves ym. 2022).

3.4.4 Tietoturvapoikkeamat

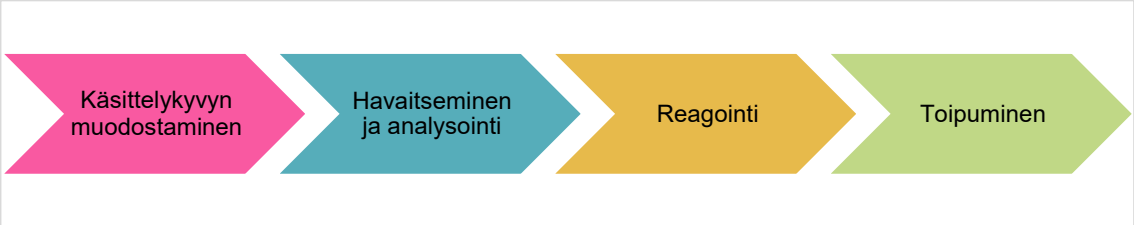
Tietoturvapoikkeamilla tarkoitetaan esimerkiksi palvelunestohyökkäyksiä, tietomurtoja ja tietojen kalastelua tai näiden yrityksiä (Kyberturvallisuuskeskus 2020b). Valitettavan usein organisaatioissa tietoturvapoikkeamista ei ilmoiteta kuvitellen, että joku muu on kuitenkin asiasta ilmoittanut. Ilmoittaminen kuuluu kuitenkin kaikille työntekijöille ja kyseessä on kaikkien asia. Henkilöstöllä tulee olla käytössään turvalliset työkalut ja organisaation tulee kannustaa henkilöstöään ilmoittamaan havaitsemistaan poikkeamista. (Rousku 2017, 43–44). Organisaatiolla tulee myös olla selkeät toimintamallit tietoturvapoikkeamien käsittelyyn (Valtiovarainministeriö 2017).

Luovissa on määritelty, että tietoturvapoikkeamat tarkoittavat tahallisia tai tahattomia tapahtumia, joiden seurauksena Luovin vastuulla olevien tietojen ja palvelujen luottamuksellisuus, eheys tai tarkoituksenmukainen käytettävyystaso

vaarantuvat tai saattavat vaarantua. Luovin Satamassa (intra) on ohjeet henkilöstölle tietoturvapoikkeamista ilmoittamiseen sekä konkreettisia esimerkkejä, joiden avulla henkilöstö voi tunnistaa tietoturvapoikkeamia. (Ammattiopisto Luovi 2023a.)

Poikkeamatilanteita kannattaa harjoitella säännöllisin väliajoin, ainakin vähintään vuosittain. Tietoturvapoikkeamiin liittyvää ohjeistusta ja toimintamalleja on hyvä kehittää harjoituksissa mahdollisesti havaittujen puutteiden avulla. (Kyberturvallisuus 2023.) Luovi on osallistunut esimerkiksi Digi- ja väestötietoviraston vuosittain järjestämään Taisto-harjoitukseen. Luovissa pidetään myös sisäisiä harjoituksia, joiden avulla kehitetään tietoturvapoikkeamien hallintaa. (Ammattiopisto Luovi 2023a.)

Tietoturvapoikkeamien hallintaprosessin tarkoituksena on häiriötilanteisiin varautuminen, toiminnan jatkuvuuden turvaaminen minimoimalla häiriön aiheuttamat vahingolliset seuraukset ja häiriöiden muodostumisen estäminen. Tietoturvapoikkeamiin on reagoitava nopeasti, jotta niiden haitalliset vaikutukset voidaan minimoida. (Valtiovarainministeriö 2017.) Hallintaprosessi koostuu Valtiovarainministeriön (2017) mukaan käsittelykyvyn muodostamisesta, havaitsemisesta ja analysoinnista, reagoinnista ja toipumisesta (kuvio 11).

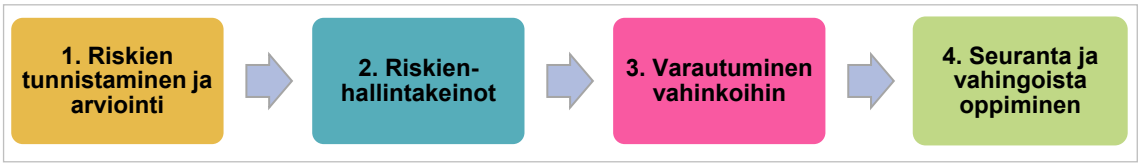


Kuvio 11. Tietoturvapoikkeamien hallintaprosessi (Valtiovarainministeriö 2017).

Organisaation täytyy selvittää, miten ja miksi vahinko on päässyt tapahtumaan. Kun tapahtumia käydään läpi, on tärkeää miettiä, mitä tapauksesta voidaan oppia. (Järvinen 2022b.) Tietoturvapoikkeaminen hallintaprosessin sisältö riippuu riskienhallinnan avulla määritellyistä turvakontrolleista, joiden avulla poikkeamat koitetaan estää kokonaan tai ainakin havaita ajoissa (Valtiovarainministeriö 2017). Tietoturvapoikkeamat tulee siis huomioida osana organisaatioiden riskienhallintaa.

3.5 Riskienhallinta

Riskienhallinta voidaan määritellä ennakoivaksi, suunnitelmalliseksi ja järjestelmälliseksi toiminnaksi riskien ja niistä aiheutuvien vahinkojen välttämiseksi ja vähentämiseksi. Ihmisten, tiedon, omaisuuden, maineen ja ympäristön turvaaminen sekä organisaation toiminnan häiriöttömyyden varmistaminen päivittäisessä työarjessa ovat riskienhallinnan perusta. (Viitala & Jylhä 2019, 206.) Riskienhallinta osana digiturvallisuutta tarkoittaa järjestelmällistä toimintaa, joka sisältää riskien analysoinnin sekä tarvittavien toimenpiteiden suunnittelun, toteutuksen ja seurannan sekä korjaavat toimenpiteet (Valtiovarainministeriö 2020). Riskienhallinta on oppimista, jonka tarkoituksena on kehittää toimintaa ja estää vahinkojen syntyminen (Ilmonen, Kallio, Koskinen & Rajamäki 2022, 231). Kuviossa 12 on esitetty yksi näkemys riskienhallinnan kokonaisuudesta.



Kuvio 12. Riskienhallinnan kokonaisuus (Viitala & Jylhä 2019, 206).

Riskienhallinnan lisäksi digiturvan organisointi vaatii johtamista. Digiturvan hallinnan pitäisi olla luonnollinen osa koko organisaation turvallisuutta, hallintoa ja johtamista. Riskienhallinta on olennainen osa ennakoivassa johtamisessa ja organisaation päätöksenteossa, jossa tulee pyrkiä kehittämään toimintatapoja tunnistettujen uhkien ja havaittujen mahdollisuuksien perusteella. (Digi- ja väestötietovirasto 2023.) Digitaalisessa riskiyhteiskunnassa ihminen ja inhimillinen toiminta ovat keskeisiä riskejä (Korpiola & Poutanen 2021, 167).

Luovissa esimerkiksi tietoturvallisuus on huomioituna osana riskienhallintaa. Siihen liittyviksi hallintakeinoiksi on tunnistettu muun muassa käyttöoikeudet, vahva tunnistautuminen, turvaohjelmistot ja henkilöstön osaaminen sekä tietoturvallisuusohjeet ja koulutukset. (Ammattiopisto Luovi 2023a.) Digiturva on riskienhallinnassa huomioitava asia, koska digitaalisuuteen liittyy myös useita erilaisia uhkia.

Organisaatioiden toiminnassa ovat päivittäin läsnä digitalisaation mukanaan tuomat uhat (Barzilay 2023). Digiturvallisuuteen liittyen hallittavia riskejä ovat esimerkiksi tietoturva- ja kyberriskit ja tietosuojariskit. Merkittävin vaatimus lainsäädännöllisesti tietosuojariskeissä on GDPR, joka edellyttää, että organisaation on rakennettava tietosuojariskien hallitsemiseksi tarvittavat tekniset järjestelyt ja tunnistettava jatkuvasti asiakkaidensa ja henkilöstönsä henkilötietojen käsittelyyn liittyviä riskejä. (Ilmonen ym. 2022, 179–193.) Työkalu henkilötietojen käsittelyn riskien tunnistamiseen on vaikutustenarviointi.

Vaikutustenarvioinnin tarkoituksena on auttaa organisaatiota analysoimaan henkilötietojen käsittelyyn liittyviä riskejä. Tarkoituksena on tunnistaa ja arvioida riskit ja saada ne hallintaan. Vaikutustenarviointi täytyy tehdä ennen henkilötietojen käsittelyn aloittamista ja sitä tulee päivittää muutostilanteissa, koska se on tarkoitettu riskien tunnistamisen ja hallinnan jatkuvaksi apuvälineeksi. (Tietosuojavaltuutetun toimisto 2023f.)

Luovissa on ohjeistettu laatimaan yhteistyössä tietosuojavastaavan kanssa alkukartoitus esimerkiksi aina, kun ryhdytään suunnittelemaan uutta prosessia tai järjestelmähankintaa. Alkukartoituksen avulla selvitetään, onko vaikutusten arvioinnin laadinta tarpeen. Vaikutustenarvioinnissa hyödynnetään tietosuojavaltuutetun laatimaa kirjaamistyökalua. Luovissa on laadittu vaikutustenarviointi esimerkiksi Whistleblowing-ilmoituskanavaan liittyen. (Ammattiopisto Luovi 2023a.) Vaikutustenarvioinneissa voi tulla esille myös jatkuvuuden hallinnassa huomioitavia asioita.

3.6 Jatkuvuuden hallinta

Jatkuvuuden hallinnan avulla organisaatio pystyy kohtaamaan erilaiset yllättävät tilanteet ja kriisit. Ympäristön tarkkailu mahdollistaa organisaatioon vaikuttavien asioiden havainnoinnin ja oikea-aikaisen reagoinnin niihin. (Työterveyslaitos 2023.) Jatkuvuuden hallinnalla tarkoitetaan organisaation prosessia, jolla tunnistetaan toiminnan uhat ja arvioidaan niiden vaikutukset sekä organisaatiossa että sen toimijaverkostossa ja luodaan häiriötilanteita varten toimintatapa

(Valtiovarainministeriö 2022). Digi- ja väestötietovirasto (2023) määrittelee, että jatkuvuudenhallinnan avulla ennaltaehkäistään häiriötilanteita ja varaudutaan niihin, palaudutaan niistä ja hallitaan niiden vaikutuksia. Jatkuvuuden hallinta tarkoittaa organisaation toiminnan jatkuvuuden varmistamista (Digi- ja väestötietovirasto 2023).

Organisaatioissa ja niiden toimintaympäristössä tapahtuu koko ajan sekä pieniä että suuria muutoksia, joiden kanssa organisaatioiden tulee olla valppaana. Organisaatiossa voi sattua esimerkiksi läheltä piti -tilanteita tai asiakkaat voivat havaita puutteita toiminnassa. Näihin kannattaa reagoida ketterästi ja selvittää asia. Toimintaympäristön muutos on jatkuvaa ja se voi vaikuttaa organisaation toimintaan myös yllättävillä tavoilla. (Työterveyslaitos 2023.)

Organisaation tulee varmistaa, että sen toiminta pystyy jatkumaan poikkeustilanteiden jälkeen. Organisaatiossa tulee huolehtia esimerkiksi siitä, että sen käytössä ei ole laitteita tai sovelluksia, joiden käytön tuntee vain yksi henkilö. Myös osaamisen kohdalla tulee varmistua siitä, että mikään osaaminen ei ole ainoastaan yhden henkilön takana. (Järvinen 2022b, 49.) Organisaatiot voivat järjestelmällisellä jatkuvuudenhallinnan kehittämisellä vähentää häiriöistä aiheutuvia kustannuksia, parantaa henkilöstön kykyä toimia häiriötilanteissa ja nopeuttaa toiminnan palautumista. (Huoltovarmuuskeskus 2023.)

3.7 Kyberturvallisuus

Organisaation ja yhteiskunnan elintärkeät ja kriittiset toiminnot pyritään turvamaan kyberturvallisuuden avulla (Digi- ja väestötietovirasto 2023). Kyberturva tarkoittaa digitaalisen ja verkottuneen organisaation turvallisuutta (Valtiovarainministeriö 2020) ja kyberturvallisuus on niitä toimenpiteitä, joiden avulla organisaatio suojaa liiketoiminnassa tarvitsemansa järjestelmät, laitteet ja tietoliikenneyhteydet kyberuhkilta (Traficom 2020, 4). Järvisen (2022b, 16) mukaan termin merkitys vaihtelee puhujan mukaan, mutta hän itse määrittelee kyberturvallisuutta viittamaan siihen tietoturvaan, joka koskee maanpuolustusta ja arjen infrastruktuuria. Esimerkiksi sähkönjakelu, vesihuolto, terveydenhuolto ja kauppa

toimivat tietokoneiden ja verkkojen varassa. Jos näiden tietoturva pettää, vaarassa ovat myös ihmisten henki ja hyvinvointi eikä kyseessä ole enää vain taloudelliset tappiot. (Järvinen 2022b, 16.) Kyberturvallisuuden avulla varmistetaan, että kybertoimintaympäristöön voidaan luottaa ja sen tarkoituksenmukaisesta toiminnasta pystytään huolehtimaan (Peltomäki & Norppa 2015, 179).

Kyberturva voi tuntua organisaatiosta kalliilta, mutta oikeasti kalliita ovat vahingot (Järvinen 2022b, 34). Hyökkäyksen kohteeksi joutuminen on organisaatiolle taloudellinen riski sekä merkittävä maineriski (Peltomäki & Norppa 2015, 98). Varautuminen on taloudellisesti kannattavaa, kun riskit suhteutetaan kustannuksiin (Järvinen 2022b, 35).

Turvallisuuden vaarantuminen tapahtuu aina joko teknisestä tai inhimillisestä virheestä johtuen. Tekniset virheet voivat olla kalliita, hitaita ja vaikeita korjata, mutta ne voidaan korjata. Inhimillisten virheiden korjaaminen on huomattavasti vaikeampaa ja inhimillisiä virheitä on lukematon määrä. Valitettavasti ihmiset esimerkiksi käyttävät samaa salasanaa useammassa palvelussa ja avaavat sähköpostin liitetiedoston, vaikka lähettäjä olisi aivan kummallinen. (Hyppönen 2021, 102.) Uhkakuvien sijaan digitaalisen maailman turvallisuus olisi hyvä nähdä teknologian ja digitaalisen kehityksen mahdollistajana sekä luottamuksen ylläpitäjänä (Limnéll, Hiltunen & Dufva 2022, 242).

Parhaimmillaan kyberturva on kilpailukykytekijä. Tällöin organisaatiossa on myönteinen kyberturvakulttuuri ja organisaatiossa tehdään investointeja kyberturvallisuuteen ja sitä hallitaan asianmukaisesti. Organisaatioiden tulee huolehtia siitä, että niillä on kyberturvallisuushaasteiden ratkaisemiseen kykenevää henkilöstöä. (Traficom 2020, 22, 27.) Nykyisessä yhteiskunnassa digitaalisuus koskettaa jollakin tasolla kaikkia organisaatioita ja niiden tulee huolehtia henkilöstön digiosaamisesta (Hagert & Toivanen 2022, 230–231). Ihmisten digiturvallisuusosaaminen tarvitsee päivitystä ja ainoa tapa siihen on jatkuva koulutus (Hyppönen 2021, 102). Valveutunut organisaatio huolehtii henkilöstönsä digiturvallisuusosaamisesta ja sen jatkuvasta kehittämisestä (Kirves ym. 2022).

4 Osaamisen kehittäminen työelämässä

4.1 Osaamisen kehittäminen

Työelämään kuuluu jatkuva muutos. Työelämään itsessään kuuluu muutos ja lisäksi muutoksia tuovat ajassa kiinni olevat asiat ja ilmiöt. Suurin yksittäinen työelämää muuttava ilmiö on digitalisaatio. (Hagert & Toivanen 2022, 199, 225.) Elämme jatkuvan muutoksen aikaa. Ympäristömme ei ole vakaa eikä hallittavissa. Kehittyvä organisaatio valmistautuu tulevaisuuteen ja kehittää sekä toimintaansa että henkilöstöään. (Eulenberger 2021, 166–167.)

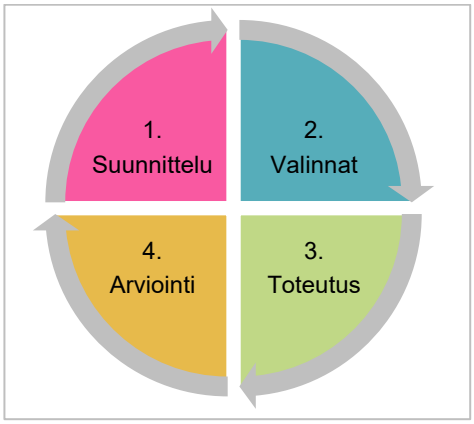
Osaamisen kehittäminen sisältää kaikki prosessit ja toimenpiteet, joiden avulla organisaatiossa tarvittavaa tietotaitoa kehitetään (Viitala 2021, 121). Osaamisvajeen tunnistaminen toimii pohjana osaamisen kehittämiselle (Kaijala & Tolvanen 2020, 177). Osaamistarpeet määrittyvät myös organisaation vision ja strategian mukaisesti (Eklund 2021, 194). Kun osaamistarpeita verrataan nykytilaan, havaitaan, mitä osaamista tulee kehittää. Osaamistarpeiden selvityksessä voi käyttää lähtökohtana myös toimintaympäristön muutoksia ja organisaation arvoja. (Otala 2002, 224.) Kehittämisen onnistumiseen vaikuttaa merkittävästi se, kuinka hyvin ja realistisesti nykytila pystytään arvioimaan (Ranta 2021, 98).

Osaava henkilöstö on organisaation oleellinen voimavara (Clegg, Kornberger, Pitsis & Mount 2019, 153), jota kannattaa kehittää. Menestyneimmät organisaatiot ymmärtävät ihmisten olevan tärkeimmän resurssinsa ja haluavat panostaa osaamiseen (Hiila, Tukiainen & Hakola 2019, 39). Työntekijän tulee sitoutua myös itse osaamisensa kehittämiseen, koska tehtävät ovat nykyisessä työelämässä muuttuvia (Nieto 2014, 203). Sitoutuneiden ja motivoituneiden työntekijöiden osaamista on helpompaa kehittää (Sinokki 2016, 57).

Strategisesti osaamisen kehittäminen on merkittävää, koska organisaation kilpailukyky riippuu siitä, mitä siellä osataan, miten osaamista hyödynnetään ja kuinka nopeasti pystytään oppimaan uutta (Viitala 2021, 121). Erityisesti digitalisaatio edellyttää jatkuvaa osaamisen kehittämistä. Työssä on tärkeää hallita

erilaisia teknologioita, koska digitaalisuus on läsnä kaikilla työpaikoilla. (Hagert & Toivanen 2022, 206, 226.) Valveutuneet organisaatiot luovat digiturvallisen kulttuuriin erilaisilla ohjeistuksilla ja koulutuksilla, jolloin niiden henkilöstö osaa toimia vaativassa digiympäristössä. (Rousku ym. 2019.)

Osaamisen kehittämisessä tärkeintä on organisaation palveluksessa olevan henkilöstön osaamisen kehittyminen. Osaamisen kehittämisen tavoitteita ovat esimerkiksi osaamisperustan turvaaminen, toiminnan tehostaminen ja laadun parantaminen ja uudistumisen mahdollistaminen. (Viitala 2021, 122, 126.) Karkeasti luokiteltuna osaamisen kehittämisen tavat ovat olemassa olevan osaamisen sitouttaminen, sen kehittämiseen investoiminen, osaamisen ostaminen, sen lainaaminen ja tarpeettoman osaamisen siirtäminen pois (Viitala 2013, 186). Osaamisen kehittämistä voi tarkastella jatkumona (kuvio 13). Uudistuminen muodostuu suunnittelun, valintojen ja toteutuksen vuoropuhelusta (Ranta 2021, 124). Kehittämistoimien tuloksellisuutta tulee myös arvioida. Organisaation tulee määritellä osaamisen kehittämiselle suunta ja luoda oppimiselle suotuisat edellytykset. (Viitala 2021, 123, 139.)



Kuvio 13. Osaamisen kehittämisen jatkumo (mukaillen Ranta 2021, 124 ja Viitala 2021, 139).

Osaamisen kehittämisessä on välttämätöntä laittaa asioita tärkeysjärjestykseen, joten organisaation on tehtävä valintoja. Osaamisen kehittämiselle on oltava riittävästi aikaa ja riittävät resurssit, jotta uudistuminen voi onnistua. (Viitala 2013, 186.) Osaamisen kehittyminen vaatii jatkuvaa työtä ja työelämässä oppiminen sujuukin parhaiten yhteistyöllä (Kupias & Peltola 2019, 38–39).

4.2 Osaaminen ja oppiminen

Oppimista ei pidä käsitteenä sotkea osaamiseen, vaikka ne kuuluvatkin erottamattomasti yhteen. Osaaminen on seurausta oppimisesta ja osaamattomuus johtuu oppimisen puutteesta tai unohtamisesta. Oppiminen vaatii aikaa ja osaamisen ajan tasalla pitäminen edellyttää jatkuvaa ja elinikäistä oppimista. (Koskinen 2020, 6–7.) Sydänmaanlakka (2004, 33) määrittelee, että: ”Oppiminen on prosessi, jossa yksilö hankkii uusia tietoja, taitoja ja asenteita, kokemuksia ja kontakteja, jotka johtavat muutoksiin hänen toiminnassaan.”. Kun työpaikalle luodaan edellytykset oppimiselle, se on panostus organisaation kilpailukykyyn (Otala & Meklin 2021, 12). Organisaation kannattaa mahdollistaa muun muassa digiturvan oppiminen. Kun organisaation henkilöstö hallitsee digiturvan viiden osa-alueen perusteet, osaavat he toimia vastuullisesti, jolloin organisaation turvallisuus lisääntyy (Rousku ym. 2019).

Oppiminen voi tapahtua opiskelemalla, opettelemalla tai harjoittelemalla. Oppimista voi tapahtua myös kokemuksen, esimerkin tai ympäristön vaikutuksen avulla. (Koskinen 2020, 6.) Oppimista voi tapahtua eri tasoilla: oppiminen voi olla henkilökohtaista tai organisaation sisällä tapahtuvaa. Organisaation sisällä voidaan oppia tiiminä tai koko työyhteisönä. Oppiminen voi liittyä myös verkostoihin. Kehittyvä organisaatio huolehtii oppimisesta, sillä ilman sitä työyhteisö todennäköisesti jämähtää paikalleen eikä enää kykene toimimaan parhaalla mahdollisella tavalla jatkuvasti muuttuvassa maailmassa. (Koskinen 2020, 17, 24.) Hiltunen (2019) uskoo, että tulevaisuudessa oppiminen kulkee ihmisen rinnalla koko työelämän ajan.

Oppimista tapahtuu työelämässä useissa eri tilanteissa. Kaikki tilanteet eivät vaadi rahaa tai edes erityisiä järjestelyjä. Esimerkiksi oppiminen osana työtä ei vaadi erillisiä järjestelyjä, vaan sitä tapahtuu, kun työtehtävissä tulee eteen uudenlainen selvitettävä tilanne. (Viitala 2021, 129.) Jopa suurin osa työelämän oppimisesta tapahtuu huomaamatta työtä tekemällä eli arjen haasteita ratkoen (Eklund 2021, 37). Tätä epäformaalia ja kokemusperäistä oppimista voi tehostaa ottamalla käyttöön esimerkiksi oppimista tukevia palaverikäytäntöjä, ryhmätyömenetelmiä ja arviointikäytäntöjä. (Viitala 2021, 129.)

Formaaleja osaamisen kehittämisen keinoja ovat esimerkiksi perehdyttäminen, koulutustilaisuudet, tiimityö, kokeilut ja kehittämisprojektit. Näissä määritellään etukäteen sisältö ja tavoitteet sekä aikataulu ja järjestämispaikka. Formaalit osaamisen kehittämiskeinot vaativat suunnittelua, resurssointia ja toteuttamista. (Viitala 2021, 129–130.) Toimet tulee suunnitella organisaation liiketoiminnasta, tarpeista ja ydinosaamisesta käsin. Organisaation täytyy tunnistaa kehittämistarpeet yksilö- ja työyhteisötasolla sekä nykyisten työtehtävien suhteen että tulevaisuutta ajatellen. (Joki 2021, 120.) Tärkeintä organisaatioissa on miettiä, kuinka oppimista ja osaamisen kehittymistä edistetään mahdollisimman monella tavalla. Eli kuinka työpaikasta saadaan hyvä oppimisympäristö erilaisiin tarpeisiin. (Kupias & Peltola 2019, 24.)

4.3 Osaamisen jakaminen

Organisaatioissa huolehditaan digiturvallisuudesta eri tavalla eri roolien mukaisesti. Johdolla on aina kokonaisvastuu digiturvan eri osa-alueista, joten johto myös luonnollisesti päättää digiturvallisuuden linjauksista, vastuista ja resursseista. Johdon apuna linjausten ja ohjeiden laadinnassa toimivat useimmiten organisaation palveluksessa olevat asiantuntijat. (Rousku ym. 2019.)

Organisaatiossa voi olla sen koosta riippuen nimettynä vastuuhenkilöt jokaiselle digiturvan osa-alueelle tai yksi henkilö voi vastata niistä kaikista. Esihenkilöt huolehtivat, että linjauksia ja ohjeita noudatetaan heidän vastuualueillaan ja he vastaavat osaltaan myös siitä, että henkilöstöllä on riittävä digiturvaosaaminen. Henkilöstön velvoitteena on osallistua koulutuksiin ja noudattaa annettuja ohjeita sekä ilmoittaa havaitsemistaan poikkeamista. (Rousku ym. 2019.) Organisaatiosta eri roolien mukaisesti löytyvää osaamista kannattaa jakaa.

Osaamisen kehittymisen kannalta on tärkeää, että yksilön ympäriltä löytyy riittävästi henkilöitä, joilta voi oppia (Eklund 2021, 169). Organisaation sisäisten asiantuntijoiden osaaminen ja kokemus ovat tärkeitä osaamisresursseja ja osaamista onkin tärkeää saada hyödynnettyä yhtä yksikköä laajemmin organisaatiossa (Otala 2018, 221). Kun osaamista saadaan jaettua riittävästi henkilöstön

kesken, ei esimerkiksi yksittäisten henkilöiden poistuminen organisaatiosta pienennä osaamistasoa niin merkittävästi kuin tilanteessa, jossa osaaminen olisi keskitettynä vain harvoille henkilöille (Eklund 2021, 173).

Osaamisen jakamista voi tapahtua muun muassa palavereissa ja henkilöstöinfoissa. Tällaiset tilaisuudet voivat olla joko osallistavia tai informatiivisia tai myös molempia yhtä aikaa. Osaamisen kehittymisen kannalta palavereiden hyöty riippuu siitä, kuinka tehokkaiksi ja avoimeksi ne onnistutaan saamaan. (Viitala 2021, 136.) Osaamisen jakamiseen sopivat hyvin myös sisäiset koulutukset. Hyvä tiedonjakamisen keino on valjastaa organisaation asiantuntijat toimimaan kouluttajina sisäisissä koulutuksissa. (Otala 2018, 221.)

4.4 Koulutustilaisuudet

Koulutuksen tulee lähteä aina tarpeesta. Kun tarve on tunnistettu, voidaan selvittää, miten tarvittavaa osaamista saadaan hankittua koulutuksen avulla. Organisaation johdon sitoutuminen ja kiinnostus koulutusta kohtaan on tärkeää. Koulutustapahtumia voidaan toteuttaa usealla eri tavalla ja monenlaisia opetusmenetelmiä hyödyntäen. (Joki 2021, 136–137.) Organisaatiossa voidaan hyödyntää sisäisiä tai kaikille avoimia koulutuksia ja ne voivat olla lyhyitä tai kestää pidempään. Yleisiä taitoja voi hakea avoimista koulutuksista, mutta osa teemoista on selkeästi sellaisia, joiden käsittelyä hyödyttää se, että keskustelu tapahtuu sisäisesti organisaatiossa. (Kupias, Peltola & Pirinen 2014, 102.)

Organisaation sisäisesti järjestettävällä koulutuksella on useita etuja, kuten mahdollisuus huomioida organisaation tarpeet ja erityispiirteet koulutuksen sisällössä. Koulutuksessa käsiteltävät asiat saadaan sovellettua suoraan organisaatioon ja sen aitoihin tilanteisiin. Sisäinen koulutus on mahdollista toteuttaa organisaatiolle parhaiten sopivana ajankohtana, jolloin voidaan kouluttaa suurikin määrä henkilöstöä kerralla. Organisaatiolle räätälöity koulutus mahdollistaa myös asioiden soveltamisen käytäntöön nopeasti. (Joki 2021, 137.) Sisäisissä koulutuksissa hyötynä on myös mahdollisuus samalla kehittää ja edistää organisaation sisäistä yhteistyötä (Viitala 2021, 135).

Organisaation sisäinen koulutus on antoisin, kun työyhteisöstä tuodaan aitoja ongelmatilanteita työstettäväksi asiantuntevalle kouluttajalle ja muulle ryhmälle. Tällöin saadaan konkreettisia työkaluja työyhteisön arkisen työskentelyn tueksi. (Joki 2021, 137.) Sisäisen koulutuksen tärkeimpänä etuna on mahdollisuus keskittyä oman organisaation haasteisiin ja tilanteeseen (Eklund 2021, 161). Täysin sisäisin voimin toteutettava koulutus mahdollistaa uuden tiedon kytkemisen organisaation toimintaan ja tavoitteisiin (Viitala 2021, 135).

Tehokas oppiminen perustuu omaehtoisesti tapahtuvaan tiedon prosessointiin. Koulutuksissa onkin yleistynyt tapa aktivoida oppijaa oppijan lähtökohdista sekä liittää koulutukseen ryhmätöiden tekemistä. (Viitala 2021, 135.) Usein koulutukset sisältävät ryhmätöitä ja tapausharjoituksia. Monesti koulutuksissa kaivataan ongelmanratkaisua teoriatiedon rinnalle, jolloin tapausharjoitukset ovat toimivia tehtäviä osaamisen lisäämiseksi. Aitojen työelämässä sattuneiden tapausten pohdinta on motivoivampaa kuin hypoteettisten, kaukana todellisuudesta olevien tilanteiden pohdinta. (Joki 2021, 137.) Kortesuo (2010, 122) toteaa, että jokaiselle ryhmälle kannattaa antaa eri tehtävä, jolloin kaikkien mielenkiinto pysyy yllä, kun lopuksi käydään läpi erilaisia tapauksia.

Tilanteen mukaan koulutukseen voi yhdistää sisäisen osuuden lisäksi myös ulkopuolisen asiantuntijuuden (Joki 2021, 137). Kokonaan ulkopuolisten asiantuntijoiden pitämien koulutusten etuna on mahdollisuus rikastaa osaamista organisaation ulkopuolisen kouluttajan tarjoamilla uusilla näkökulmilla (Viitala 2021, 135). Kaikille avoimissa koulutuksissa osallistujat pääsevät kuulemaan muiden ihmisten kokemuksia (Eklund 2021, 161), vaihtamaan näkemyksiään asioista (Joki 2021, 138) ja verkostoitumaan (Viitala 2021, 135).

Koulutustoiminta on investointi, jonka laatua kannattaa kehittää ja arvioida (Juuti & Vuorela 2010, 73). Koulutustilaisuuksista tulee kerätä palautetta. Palautteen kerääminen ja dokumentointi kehittämisehdotuksineen auttaa seuraavan koulutuksen järjestämisessä. (Joki 2021, 137.) Kaikki koulutus tähtää siihen, että koulutuksen anti näkyy osallistujien työssä. Koulutuksiin osallistuminen on sitä motivoivampaa mitä paremmin koulutuksen sisällöt ovat linkitettävissä osallistujien työhön. (Kupias ym. 2014, 103–104.)

4.5 Tiimioppiminen

Yhdessä oppimisessa on voimaa ja hyvä yhteys työkavereihin lisää oppimisen motivaatiota (Kupias & Peltola 2019, 134). Tiimityöskentely on oppimisen kannalta hyvä tapa organisoida työskentelyä, koska mitä tietoisemmin tiimi pystyy kehittämään yhteistä tekemistään, sitä taitavammaksi se ja organisaatio tulevat. Tiimit, jotka pystyvät reflektoimaan toimintaansa, osaavat arvioida säännöllisesti vuorovaikutustaan ja toimintatapojaan. Sen avulla ne löytävät keinoja, joilla voivat päästä aiempaa kehittyneemmälle tasolle. Tällöin jokaisen tiimin jäsenen henkilökohtainen osaaminen kehittyy myös. (Viitala 2021, 136.) Tiimit ovat älykkäämpiä kuin yksikään sen jäsen yksin, mikäli tiimi toimii hyvin (Otala 2018, 140).

Organisaatiossa toimii useimmiten useita erilaisia tiimejä. Olennaista organisaatioissa on se, kuinka tiimit saadaan toimimaan yhdessä. Millaisia kehittyneempiä työkäytäntöjä saadaan luotua ja miten varmistetaan jatkuva uudistuminen. (Kupias & Peltola 2019, 136.) Tiimin kehittymisen edellytyksenä on luottamuksellinen ja positiivinen ilmapiiri, joka antaa tukevan pohjan yhteiselle kehittämiselle (Kupias ym. 2014, 157).

Digitalisaation tuottamassa murroksessa perinteiset tiimityön mallit eivät välttämättä toimi, koska pysyvien tiimien tilalla on esimerkiksi projektitiimejä ja virtuaalityön malleja. Tiimit ovat myös muuttuvia ja tiimityötä tehdään paljon aiempaa enemmän. Organisaatioiden onkin lisättävä koko henkilöstön tiimityöskentelytaitoja eli tiimiälyä. Tiimiälyä kehittämällä tiimi ja sen jäsenet voivat paremmin, koska tiimiin rakentuu resilienssiä eli kykyä kestää työelämässä tapahtuvat muutokset. (Hiila ym. 2019, 48.) Olennaista on, että organisaatiossa toimitaan yhdessä, luodaan parempia työkäytäntöjä ja uudistutaan jatkuvasti. Tämä vaatii osaamisen kehittämistä. Tiimeissä oppimisen pitäisi olla myös yhteistä. Samalla organisaation täytyy huolehtia siitä, että tiimin jäsenet edistyvät myös omissa taidoissaan. (Kupias & Peltola 2019, 163, 177.) Sekä tiimien että yksilöiden osaamisen kehittämisessä voidaan hyödyntää verkko-oppimista.

4.6 Verkko-oppiminen

Verkko-oppiminen on oppimistyöskentelyn muoto, jossa hyödynnetään tieto- ja viestintäteknologiaa. Verkko-oppimisympäristöjä ovat esimerkiksi Moodle ja Microsoft 365 ja niissä voidaan esimerkiksi jakaa materiaaleja, käydä keskusteluja, palauttaa tehtäviä ja kehitellä ideoita. Verkko-oppimisympäristöjä voidaan hyödyntää esimerkiksi työtehtävissä tarvittavien faktatietojen päivitykseen. (Viitala 2021, 135.)

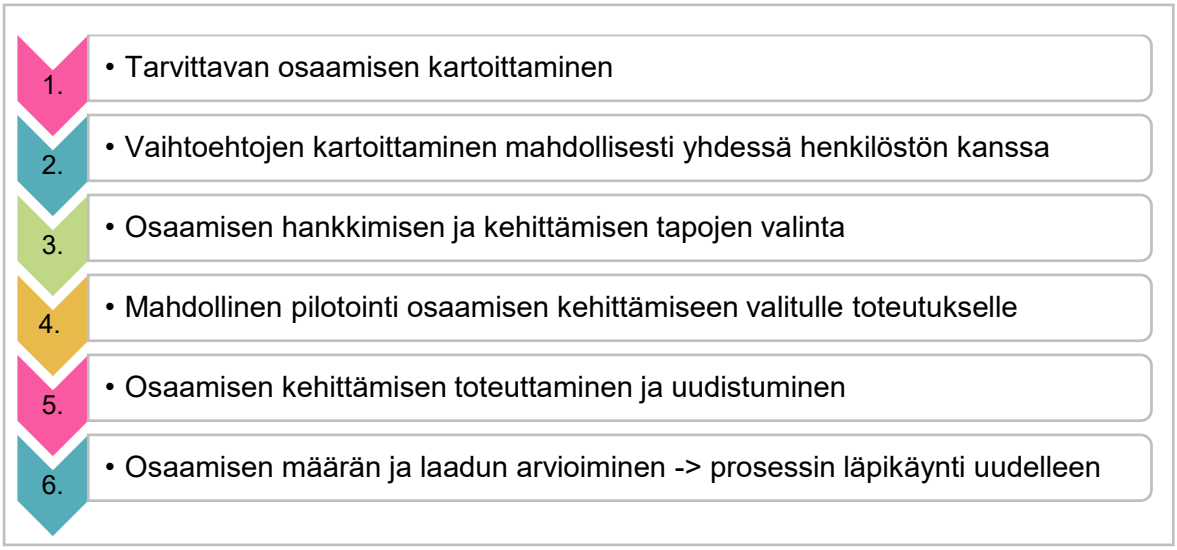
Viitalan (2021, 136) mukaan verkko-oppimisen etuna on niiden ajasta, paikasta ja tahdista riippumattomuus. Verkko-oppiminen mahdollistaa myös opiskelun itseohjautuvasti, joka on Kupiaksen & Peltolan (2019, 254) mukaan taito, jota tulevaisuuden työntekijöiltä vaaditaan. Itseohjautuvassa opiskelussa on mahdollista hyödyntää esimerkiksi Digi- ja väestötietoviraston luomaa Digiturvallinen elämä -mobiilipeliä, joka opettaa työelämässä ja etätyössä tarvittavia digiturvataitoja (Digi- ja väestötietovirasto 2023).

Olennaisinta organisaatioissa on löytää sellaiset osaamisen kehittämiskeinot, jotka soveltuvat parhaiten asetettujen tavoitteiden saavuttamiseen. Osaamista kannattaa kehittää mahdollisimman monipuolisesti ja monipuolisilla keinoilla. Osaamisen lisäämiskeinoja onkin käytettävissä useita, mutta niitä kannattaa hyödyntää suunnitelmallisesti (Joki 2021, 120).

4.7 Osaamisen suunnitelmallinen kehittäminen

Osaamisen kehittäminen käynnistyy tarpeiden määrittelystä. Kun tarve on tiedossa, tulee tunnistaa erilaiset osaamisen kehittämisen vaihtoehdot. Eri keinojen vertailuun perustuen valitaan ne, joilla osaamista hankitaan ja kehitetään. Toteuttamisessa on hyvä tavoitella tehokkuutta, taloudellisuutta ja laatua. Osallistuvien henkilöiden tulee kokea osallistuminen helpoksi. Heidän tulee myös kokea hyötyvänsä toteutuksesta. Osaamisen riittävyyttä ja laatua sekä keinojen vaikuttavuutta tulee arvioida erityisesti toteutuksen jälkeen, mutta myös koko osaamisen kehittämisen prosessin ajan. (Viitala 2021, 122–123.)

Rannan (2021) tekemässä kehittämisprosessin vaiheiden määrittelyssä henkilöstö otetaan vahvasti mukaan kehittämisprosessiin. Kehittämisen vaiheita ovat nykytilan tunnistaminen, kehityksen esteiden tiedostaminen, henkilöstön osallistaminen, muutoksen suunnittelu yhdessä henkilöstön kanssa, toimintaprosessien uudistamisen käynnistäminen ja kehittämistyön tekeminen, pilotointi, yksityiskohtainen toteuttaminen ja uudistuminen. (Ranta 2021, 71–75.) Kuviossa 14 on esitetty esimerkki osaamisen kehittämisen prosessista.



Kuvio 14. Osaamisen kehittämisen prosessi (mukaillen Viitala 2021, 123 ja Ranta 2021, 71–75).

Osaamisen kehittäminen on keskeinen tuottavuuteen ja tuloksellisuuteen vaikuttava asia. Siten siitä tulisikin puhua investointina, eikä kustannuksina. Osaamiseen tehtäviä investointeja on syytä suunnitella yhtä huolellisesti kuin muitakin. (Viitala 2013, 186.) Osaamisen kehittämisen toimet voivat kohdistua koko henkilöstöön, ryhmään tai yksilöön (Viitala 2021, 129). Osaamista hyvä tarkastella kaikilla näillä tasoilla (Kaijala & Tolvanen 2020, 176).

Aiemman yhteistoimintalain mukaisesti yrityksissä, joissa on säännöllisesti vähintään 20 henkilöä töissä, tuli laatia henkilöstö- ja koulutussuunnitelma (Viitala 2021, 126). Uudistetussa yhteistoimintalaissa (1333/2021, YTL) puhutaan työyhteisön kehittämissuunnitelmasta, jonka sisällön tulee elää (Paanetoja & Salminen 2022, 94) ja siihen on muun muassa kirjattava nykytila ja tiedossa olevat kehityskulut, joilla voi olla vaikutusta henkilöstön osaamisen tarpeisiin. Lisäksi on kirjattava päämäärät ja toimet, joiden avulla henkilöstön

osaamista kehitetään sekä määriteltävä toimenpiteiden vastuut, aikataulu ja seuranta. (YTL 9 §.) Osaamisen kehittäminen on Luovissa siis lakisääteistäkin.

Osaamisen kehittämiseen voi laatia kokonaissuunnitelman, joka kattaa koko henkilöstöä, yksiköitä, tiimejä ja yksilöjä koskevat suunnitelmat. Suunnitelma kannattaa tehdä tavoitteiden, eri analyysien sekä osaamistarvekartoitusten pohjalta. Siinä voi määritellä, missä asioissa osaamista halutaan kehittää, mikä on tavoitetaso, mitä on tehtävä, aikataulu ja resurssit sekä tulosten seuranta. (Viitala 2013, 186–187.) Kehittämistoimien tuloksellisuutta tulee arvioida järjestelmällisesti ja usealla tasolla, esimerkiksi yksilöiden tietojen kehittymisenä ja muutosten vaikutuksina työyhteisöön. Arvioinnin tulisi ulottua toimien eri vaiheisiin. Käytettyjä resursseja tulee myös verrata saatuihin hyötyihin koko organisaation kannalta. Erityisen tärkeää arvioinnissa on suunnitella, kuinka osaamista kehitetään tulevaisuudessa. Osaaminen on edellytys myös työssä onnistumiselle ja mielekkyyden säilymiselle. Muuttuvat työtehtävät vaativat uudistuvaa osaamista henkilöstöltä. (Viitala 2021, 121, 139.)

Digiturva tarvitsee toteutuakseen ihmistä, joten henkilöstöä kannattaa kouluttaa ja laatia ymmärrettäviä ja helposti löydettäviä digiturvallisuusohjeita. Esimerkiksi Digi- ja väestötietoviraston maksuttomien koulutusten lisäksi tarvitaan organisaation omaa materiaalia. Paraskin palomuuri voi olla hyödytön, jos työntekijä klikkaa esimerkiksi huijauslinkkiä ja organisaation tiedot vaarantuvat. Koulutusten ja harjoittelun lisäksi organisaatioiden kannattaakin panostaa myös ajankohtaisista asioista, kuten digiturvallisuusuhkista tiedottamiseen. (Kirves ym. 2022.)

Digiturva tulee nähdä uhkien ja kieltojen korostamisen sijaan ennen kaikkea mahdollisuutena (Andreasson 2022, 54). Digiturvaosaamiseen investointi on henkilöstön osaamisen kehittämisen toimi, joka maksaa itsensä takaisin, sillä se mahdollistaa organisaation menestymistä. Onnistuneella digitalisaatiolla voidaan myös parantaa ihmisten elämänlaatua sekä suojella ilmastoa ja luontoa (Hagert & Toivanen 2022, 232). Vastuulliset organisaatiot huolehtivat myös digitalisaatiosta vastuullisesti. Digiturvallisuuden toteuttaminen on kaikkien yhteinen asia eli yhteistyötä, jossa koko organisaation tulee huolehtia siitä oman roolinsa ja vastuualueensa mukaisesti (Rousku ym. 2019).

5 Tutkimuksellinen kehittämistyö

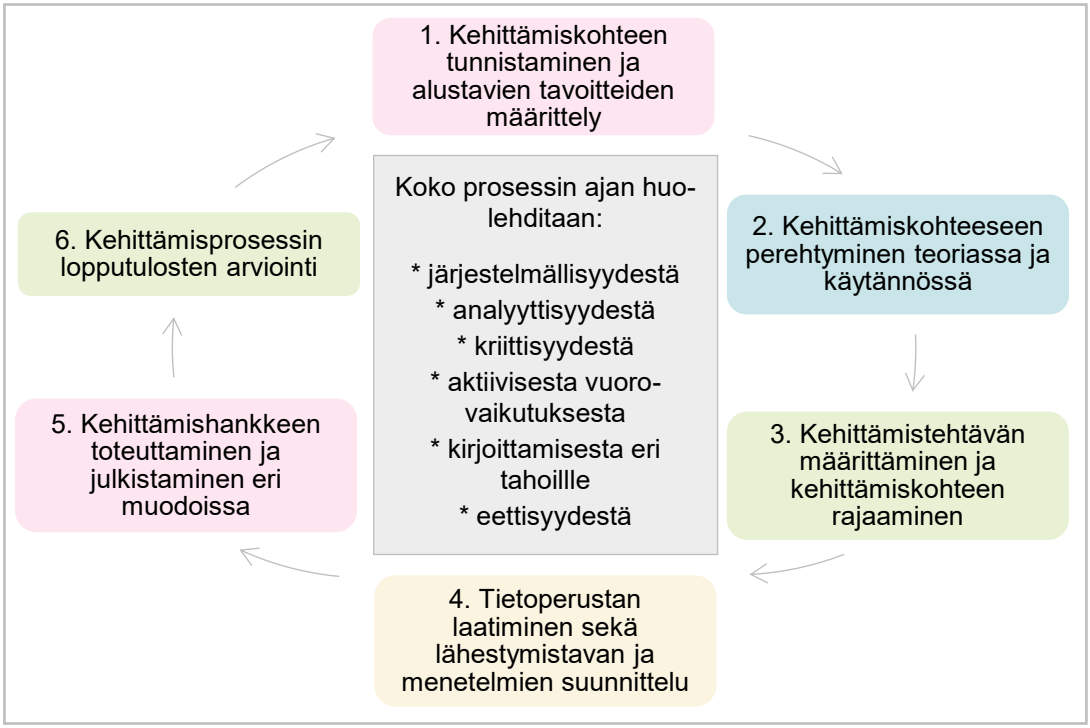
Jatkumossa, jonka toisessa ääripäässä on tieteellinen tutkimus ja toisessa arkiajatteluun perustuva kehittäminen, tutkimuksellinen kehittämistyö asettuu keskelle (Ojasalo, Moilanen & Ritalahti 2014, 17). Tieteellinen tutkimus on ongelmanratkaisua, jonka avulla pyritään selvittämään tutkimuskohteen toimintaperiaatteita ja lainalaisuuksia empiirisellä eli havainnoivalla tutkimuksella tai teoreettisella kirjoituspöytätutkimuksella (Heikkilä 2014, 12). Arkiajatteluun perustuva kehittäminen tapahtuu organisaatiossa jo olevien uskomusten ja asenteiden pohjalta ilman tutkimusta (Ojasalo ym. 2014, 21).

Tutkimuksellinen kehittämistoiminta yhdistää tutkimuksellisen lähestymistavan ja konkreettisen kehittämistoiminnan (Toikko & Rantanen 2009, 19). Työelämän kehittämiseen sopiva toimintamalli on tutkimuksellinen kehittäminen, jossa hyödynnetään tieteellisen tutkimuksen menetelmiä ja kehitetään käytännön työelämää. Tutkimuksellisessa kehittämistyössä ei ole tieteellisen tutkimuksen tavoin tavoitteena ainoastaan asioiden kuvaaminen tai selittäminen, vaan parempien vaihtoehtojen etsiminen ja asioiden kehittäminen. Kehittämistyössä kehittäminen toteutetaan järjestelmällisesti, kriittisesti ja analyyttisesti toisin kuin arkiajattelulla kehittämisessä, jossa kehittämispäätökset perustuvat paljolti omiin ideoihin, joita ei ole arvioitu kriittisesti. (Ojasalo ym. 2014, 18-21.)

Tutkimuksellisella kehittämisellä pyritään ratkaisemaan työelämässä esiin tulleita ongelmia tai uudistamaan käytäntöjä sekä monesti myös luomaan työelämän käytännöistä uutta tietoa. Kehittämistyön tarkoituksena on tyypillisesti suunnitella, kehittää ja ottaa käyttöön uusia ratkaisuja eli tuoda parannuksia työelämään. (Moilanen, Ojasalo & Ritalahti 2022, 30.) Kehittämistöille ominaista on käytännönläheisyys, innovatiivisuus ja arvioitavuus sekä hyödynnettävyys (Anttila 2007, 12). Kehittämisen kohde voi olla konkreettinen tuote, toimintaprosessi, yksittäinen henkilö, työyhteisö tai organisaatio (Toikko & Rantanen 2009, 17). Kehittämisen tavoitteena voi olla esimerkiksi uuden työkulttuurin kehittäminen, uusi liiketoimintamalli tai prosessien kehittäminen ja uudistus (Moilanen ym. 2022, 37).

Tutkimuksellisessa kehittämisessä käytetään monipuolisesti eri tutkimus- ja kehittämismenetelmiä ja hyödynnetään vuorovaikutusta eri tahojen kanssa. Kehittämisen tueksi kerätään kriittisesti arvioiden tietoa sekä käytännöstä että teoriasta. (Ojasalo ym. 2014, 18.) Työn tutkimuksellinen puoli toteutetaan noudattaen tutkimukseen kuuluvia toimintamalleja esittämällä täsmällisesti tutkimusongelma, tutkimuskysymykset ja tavoitteet (Vilkka 2021, 39). Empiirisen tutkimuksen tavoitteena on saada vastaus tutkimusongelmista johdettuihin kysymyksiin ja se voidaan jakaa määrälliseen ja laadulliseen. Määrällinen vastaa kysymyksiin mikä, missä, paljonko ja kuinka usein ja laadullinen miksi, miten ja millainen. (Heikkilä 2014, 12–15.) Laadullisessa tutkimuksessa tarkoituksena on ymmärtää tarkastelussa olevaa ilmiötä tutkimuksen kohteena olevien näkökulmasta selvittämällä heidän ajatuksiaan asiasta (Juuti & Puusa 2020, 9).

Tutkimuksellisessa kehittämistyössä käytetään usein sekä laadullisia että määrällisiä menetelmiä tutkimusosiossa. Monipuolisesti eri menetelmiä käyttämällä kehittämistyön tueksi saa erilaisia näkökulmia ja erilaista tietoa. Tutkimuksellisen kehittämistyön tyypillinen prosessi on esitetty kuviossa 15. Käytännössä prosessi ei kuitenkaan etene selkeästi vaiheesta toiseen, vaan niissä liikutaan jonkin verran edestakaisin. (Ojasalo ym. 2014, 23–24.)



Kuvio 15. Tutkimuksellisen kehittämistyön prosessi (Ojasalo ym. 2014, 24).

Tämä opinnäytetyö on tutkimuksellinen kehittämistyö, jossa tavoitteena on Ammattiopisto Luovin henkilöstön digiturvallisuusosaamisen syventäminen siten, että digiturvasta huolehtimisesta tulee luonteva osa heidän työarkeaan. Opinnäytetyön tutkimusongelma on se, kuinka digiturva saadaan henkilöstön työarkeen. Työssä luodaan digiturvakoulutuksen sisältävä digiturvaosaamisen kehittämissuunnitelma, jonka toteuttamisella digiturvaosaamista voidaan kehittää ja ylläpitää. Työssä selvitetään vastauksia seuraaviin tutkimuskysymyksiin:

1. Mitkä ovat Luovin henkilöstön digiturvallisuuskoulutustarpeet?
2. Mitkä ovat johdon edustajien näkemykset digiturvallisuudesta?
3. Miten digiturvallisuuskoulutus kannattaa toteuttaa henkilöstölle?
4. Miten henkilöstön digiturvallisuusosaamista voidaan kehittää ja ylläpitää?

5.1 Kehittämistyön lähestymistapoja

Kehittämiskohdetta on mahdollisuus lähestyä eri tavoin. Ennen varsinaisten kehittämistyössä käytettävien menetelmien valintaa ja työn tarkempaa suunnittelua on kannattavaa valita, minkälaisella lähestymistavalla kehittämistyötä viedään eteenpäin. Lähestymistavan valinta auttaa työn suunnittelussa ja tutkimuksellisuus on helpompi liittää kehittämiseen. Lähestymistavan valinnassa ei valita vielä konkreettisia menetelmiä, vaan tapa, jolla työtä edistetään. Kehittämistyön lähestymistapoja voivat olla esimerkiksi tapaus-, toiminta- tai konstruktiivinen tutkimus ja innovaatioiden tuottaminen. Lisäksi mahdollisia näkökulmia ovat ennakointi ja verkostotutkimus. (Ojasalo ym. 2014, 36–39, 51.)

Kehittämistehtävä määrittää parhaan lähestymistavan. Jos kehittämistehtävänä on tuottaa kehittämisehdotuksia organisaatiolle, todennäköisin lähestymistapa on tapaustutkimus. Jos tehtävänä on tuottaa henkilöstön perehdyttämisopas, sopiva lähestymistapa on konstruktiivinen tutkimus. (Ojasalo ym. 2014, 36.) Tutkimuksellisessa kehittämistyössä voi olla piirteitä useammasta eri lähestymistavasta, koska tavat ovat osin päällekkäisiä. Lähestymistapaa ei ole tarpeen valita mustavalkoisesti, vaan kehittämistyötä voi tehdä useampaa tapaa hyödyntäen. (Moilanen ym. 2022, 68.)

5.1.1 Tapaustutkimus

Tapaustutkimuksella on monta erilaista määritelmää, mutta yhteistä kaikille määritelmille on se, että tapauksia tarkastellaan niiden luonnollisessa asiayhteydessä ja aineistoa kuhunkin tapaukseen kerätään runsaasti (Piekkari & Welch 2020, 200). Tutkimuksen kohde on useimmiten tapahtumakulku tai ilmiö (Laine, Bamberg & Jokinen 2007, 9). Piekkari, Welch & Paavilainen (2009, 569) ovat määritelleet, että:

> Tapaustutkimus on tutkimusstrategia, joka mahdollistaa ilmiön tarkastelun sen omassa luonnollisessa kontekstissa käyttäen useita tietolähteitä. Tapaustutkimuksen tavoitteena on tuoda teoria kosketuksiin empiirisen maailman kanssa.

Tapaustutkimus on muuntautumiskykyinen ja joustava tutkimusstrategia, joka joustavuudellaan muokkaantuu eri tutkimusympäristöihin sopivaksi (Piekkari & Welch 2020, 200). Tapaustutkimus on hyvä lähestymistapa, kun halutaan ymmärtää jonkin organisaation tilannetta syvällisesti ja tehtävänä on tuottaa kehittämisehdotuksia tutkimuksen keinoin tai ratkaista organisaatiossa ilmennyt ongelma. Tapaustutkimuksella etsitetään usein vastausta kysymyksiin ’miten’ ja ’miksi’. Puhtaassa tapaustutkimuksessa muutosta ei viedä käytännössä eteenpäin tai kehitetä vielä mitään konkreettista. (Ojasalo ym. 2014, 37.) Tapaustutkimuksessa tapauksen voi muodostaa esimerkiksi yksilö, ihmisryhmä, organisaatio, tapahtuma, toiminto tai prosessi (Moilanen ym. 2022, 70).

Tapaustutkimukselle on tyypillistä, että monenlaisia menetelmiä hyödyntämällä saadaan syvällinen, monipuolinen ja kokonaisvaltainen kuvaus tutkittavasta tapauksesta (Moilanen ym. 2022, 72). Tapaustutkimuksessa voidaan käyttää erilaisia aineistoja ja tutkimusmenetelmiä (Laine ym. 2007, 9). Tutkimusta voi tehdä sekä laadullisin että määrällisin menetelmin tai yhdistelemällä niitä. Tyypillisiä tiedonkeruumenetelmiä tapaustutkimukselle ovat haastattelut ja kyselyt sekä havainnointi. (Ojasalo ym. 2014, 55.)

Tässä opinnäytetyössä tarkoituksena on tuottaa organisaatiolle eli Luoville digiturvallisuusosaamisen parantamiseen kehittämisehdotuksia. Opinnäytetyön kohde eli tapaus on Luovin henkilöstö, jonka digiturvallisuusosaamista halutaan

kehittää, jotta Luovin toiminta on turvallista ja toimintaan voidaan luottaa. Henkilöstön digiturvallisuusosaamisen lisäämistä tutkitaan huomioimalla Luovin todellinen tilanne ja toimintaympäristö. Opinnäytetyö ei kuitenkaan ole puhdas tapaustutkimus, koska työssä luodaan konkreettinen tuotos digiturvallisuusosaamisen kehittämiseksi ja muutosta lähdetään jo viemään eteenpäin. Tämä opinnäytetyö sisältää siten piirteitä myös konstruktiivisesta tutkimuksesta.

5.1.2 Konstruktiivinen tutkimus

Konstruktiivisessa tutkimuksessa tavoitteena on ratkaista käytännön ongelma luomalla konkreettinen tuotos, kuten tuote, tietojärjestelmä, ohje, menetelmä, malli tai suunnitelma. Tuotoksia voivat olla esimerkiksi uusi kirja, henkilöstön koulutusmateriaali ja budjetointijärjestelmä, joiden avulla tuodaan käytännön ongelmaan teoreettisesti perusteltu ja uudenlainen ratkaisu, joka antaa liiketoiminnalle ja tiedeyhteisöön uutta tietoa. Konstruktiivisessa tutkimuksessa tyypillistä on vuoropuhelu teorian ja käytännön välillä. Kehitetyn ratkaisun toteuttaminen sekä sen käytännön toimivuuden ja hyödyllisyyden arviointi ovat olennaisia asioita konstruktiivisessa tutkimuksessa. (Ojasalo ym. 2014, 37–38, 65.)

Konstruktiivista tutkimusta kannattaa hyödyntää erityisesti silloin, kun käsillä olevan asian ratkaisemiseen tarvitaan teoreettista tietämystä ja osaamista (Ojasalo ym. 2014, 66). Kasanen, Lukka & Siitonen (1991) ovat määritelleet, että kehittämistyössä tutkijan tehtävänä on rakentaa organisaatiolle teoriaan pohjautuva ratkaisu, jonka toimivuus todetaan käytännössä (Virtanen 2006, 47). Tutkija toimii konstruktiivisessa tutkimuksessa muutosagenttina, joka toimii muutoksessa itse ja opastaa muutoksen kohteena olevia muutosprosessin toteutuksessa (Kananen 2017, 14). Tutkija luo uudenlaista todellisuutta tutkimustiedon pohjalta ja pyrkii hyvin käytännönläheiseen ongelmanratkaisuun (Moilanen ym. 2022, 85).

Kehittämistyössä toteutettavan ratkaisun tulisi osoittautua toimivaksi, parhaimmillaan myös muualla kuin ainoastaan kohdeorganisaatiossa (Ojasalo ym. 2014, 65). Kasasen, Lukan ja Siitosen (1991) mukaan tavoitteena on tuotoksen

käytännön hyödynnettävyys, yksinkertaisuus ja helppokäyttöisyys (Virtanen 2006, 50). Konstruktiivisessa tutkimuksessa onnistuminen edellyttää toimeksiantajan sitoutumista kehittämiseen. Konstruktiivinen tutkimus kaikkine vaiheineen voi kestää pitkään, jolloin se vaatii sekä kehittäjältä että kohdeorganisaatiolta pitkäjänteisyyttä. Joskus konstruktiivisesta tutkimuksesta voidaan jättää aikataulullisista syistä lähestymistavalle tyypillinen ratkaisun testaaminen pois. Erityisesti opinnäytetöistä on mahdollisuus jättää tekemättä ratkaisun testaus, jos aikataulu ei riitä siihen. (Ojasalo ym. 2014, 66–67.)

Käytettävät menetelmät konstruktiivisessa tutkimuksessa voivat olla monimuotoisia. Tyypillisiä menetelmiä ovat kysely, haastattelu, havainnointi ja ryhmäkeskustelut. Kehittämistyössä hyödynnetään usein myös yhteisöllisiä menetelmiä, koska usein on oleellista tuntea perusteellisesti tuotoksen käyttäjien tarpeet. Menetelmien valinnassa on keskeistä pohtia, millaista tietoa ja mihin tarkoitukseen tarvitaan. (Moilanen ym. 2022, 54–55, 89.) Menetelmät tulee valita siten, että asetetut tavoitteet saavutetaan (Anttila 2007, 12).

Tässä opinnäytetyössä luotava digiturvaosaamisen kehittämissuunnitelma pohjautuu vankasti digiturvallisuusteoriaan sekä osaamisen kehittämisestä kirjoitettuun teoriaan. Lisäksi suunnitelmassa huomioidaan vahvasti myös Luovin käytännön toiminta ja sen tuomat vaatimukset ja reunaehdot kehittämiselle. Kehittämissuunnitelma antaa uutta tietoa, koska digiturvallisuus on vielä tuoreehko käsite, jonka merkittävyyttä organisaation toiminnalle ei ole vielä kattavasti tunnistettu. Luovin johto on erittäin sitoutunut digiturvaosaamisen kehittämiseen. Yhteistyössä laaditun tuotoksen avulla Ammattiopisto Luovi ja mahdollisesti myös muut organisaatiot voivat kehittää henkilöstönsä digiturvaosaamista.

Opinnäytetyö ei kuitenkaan ole puhtaasti konstruktiivinen tutkimus, koska työssä ei ennätetä testaamaan digiturvaosaamisen kehittämissuunnitelman käytännön toimivuutta eikä siten sen hyödyllisyyden arviointia voida myöskään toteuttaa. Opinnäytetyötä voi kuitenkin luonnehtia konstruktiiviseksi tapaustutkimukseksi, koska siinä luodaan tuotos, jolla pyritään ratkaisemaan käytännön ongelmaa. Lisäksi toimin itse digipalvelujen tiimissä, jonka tehtävänä on olla mukana toteuttamassa digiturvallisuusosaamisen lisäämistä Luovissa.

5.2 Kehittämistyön menetelmiä

Kehittämistöissä käytettäviä menetelmiä ovat esimerkiksi kyselyt, haastattelut, havainnointi, dokumenttianalyysi, benchmarking, prosessikartat, yhteisölliset ideointimenetelmät sekä ennakointimenetelmät. Eri menetelmillä saadaan erilaista tietoa, eri näkökulmia ja erilaisia ideoita kehittämistyön tueksi. Asiantuntijatyön kehittämisessä käytetään usein yhteisöllisiä menetelmiä, sillä kehittämistä tehdään harvoin yksin. Yleensä työn tekijä kuuluu jollakin tavalla osaksi ryhmää, jolle kehitettävä asia kuuluu. (Moilanen ym. 2022, 55–60.)

Kehittämistyössä on suositeltavaa käyttää useita menetelmiä rinnakkain, koska ne täydentävät toisiaan ja tuovat varmuutta kehittämistyöhön liittyvään päätöksentekoon. Kehittämistyössä käytettävät menetelmät voidaan valita, kun kehittämisen tavoite on selvillä, kehittämistehtävä määritelty ja lähestymistapa pohdittu. Kehittämistyössä voidaan käyttää myös sellaisia menetelmiä, joita ei perinteisesti käytetä tieteellisessä tutkimuksessa. (Ojasalo ym. 2014, 40, 104.)

Tässä opinnäytetyössä käytettäviksi menetelmiä ovat verkkokysely, tutkimushaastattelu ja suunnittelupaja. Kyselyn avulla kartoitetaan henkilöstön näkemys omista digiturvakoulutustarpeistaan. Haastattelun avulla selvitetään johdon edustajien näkemyksiä digiturvakoulutuksen suunnittelun tueksi. Suunnittelupajoissa etsitään parhaat keinot digiturvallisuuskoulutuksen toteuttamiselle yhteistyössä Luovin eri asiantuntijoiden kanssa.

5.2.1 Verkkokysely

Kysely sopii aineiston keruun välineeksi tutkimuksissa, joissa ollaan kiinnostuneita esimerkiksi tutkittavien asenteista, kokemuksista, arvoista ja mielipiteistä (Tähtinen, Laakkonen & Broberg 2020, 25). Kyselylomake on yksi perinteisimmistä tutkimusaineiston keruumenetelmistä ja nykyään kyselyjä toteutetaan runsaasti sähköisinä kyselyinä (Valli 2018, 92). Kyselomakkeen voi laatia esimerkiksi Webropol-ohjelmistolla (Tähtinen ym. 2020, 25). Riippumatta siitä, miten kyselylomake toteutetaan, kysymykset on syytä suunnitella tarkkaan. Huonosti

suunniteltu tutkimuslomake voi pilata koko tutkimuksen. Hyvin suunnitellun lomakkeen laadintaa edeltää kirjallisuuteen tutustuminen, tutkimusongelman pohdinta, käsitteiden määrittely sekä tutkimusasetelman ja aineiston käsittelytavan valinta. (Heikkilä 2014, 45.) Kyselylomakkeen laadintaan täytyy varata tarpeeksi aikaa (Tähtinen ym. 2020, 26). Kiireellä tai huolimattomasti tehty lomake voi estää luotettavien tutkimustulosten saamisen (Heikkilä 2014, 30).

Kysely voidaan toteuttaa kokonaistutkimuksena, jossa tutkitaan jokainen perusjoukon jäsen tai otantatutkimuksena, jossa tutkitaan pieni osa perusjoukosta. Otoksen tulee olla edustava pienoiskuva perusjoukosta, jotta tulokset olisivat luotettavia. (Heikkilä 2014, 31.) Sähköinen kyselylomake on helppo lähettää koko perusjoukolle. Mikäli kyselylomake on suunniteltu huolellisesti, on tutkimusaineistoa nopeampaa ja helpompaa analysoida. (Hirsjärvi, Remes & Sajavaara 2009, 195.)

Kyselylomakkeen kysymykset voivat olla suljettuja, avoimia tai sekamuotoisia (Vilkka 2021, 86). Suljetuissa kysymyksissä vastausvaihtoehdot ovat valmiina. Avoimissa kysymyksissä vastaajilta halutaan saada spontaaneja mielipiteitä ja mahdollisia uusia näkökulmia asiaan. Sekamuotoisissa vastausvaihtoehdoista osa on annettu ja lisäksi mukana on yksi tai useampi avoin kohta. Esimerkiksi vaihtoehto ”Muu, mikä?” kannattaa lisätä, jos ei ole varmaa, että kaikki eri vaihtoehdot on keksitty. (Heikkilä 2014, 47–50.) Kysymyksiä kannattaa laittaa kyselyyn maltillisesti ja kaikkien kysymysten tulee olla tutkimuksen kannalta hyödyllisiä (Vilkka 2021, 87). Kysymysten laadinnassa täytyy olla huolellinen, sillä kysymykset luovat perustan tutkimuksen onnistumiselle (Valli 2018, 93).

Hyvän tutkimuslomakkeen tunnusmerkkejä ovat esimerkiksi siisti ulkoasu, selkeät vastausohjeet, kysymysten looginen järjestys ja numerointi, sopiva pituus ja kontrollikysymykset. Hyvä lomake on myös esitestattu ja se saa vastaajan tuntemaan kyselyyn vastaamisen tärkeäksi. (Heikkilä 2014, 47.) Esitestaus kannattaa tehdä erityisesti silloin, kun kyselylomake on tehty itse. Esitestauksella voi tarkistaa ymmärrettävyyden. (Tähtinen ym. 2020, 25–26.)

Tässä opinnäytetyössä yhdeksi aineistonkeruumenetelmäksi on valittu verkkokysely, koska se sopii hyvin tutkimukselliseen kehittämistyöhön. Verkkokyselyn avulla selvitetään suuren joukon eli Luovin koko henkilöstön (870 henkilöä) digiturvallisuuskoulutustarpeita ja mielipiteitä digiturvallisuutta koskien. Tarpeita saadaan selvitettyä Webropol-kyselynä. Kyselyn avulla saatavan aineiston lisäksi tarvitaan johdon mielipiteitä, joita kerätään haastattelun avulla.

5.2.2 Tutkimushaastattelu

Haastattelu kannattaa yleensä yhdistää kehittämistyössä muihin menetelmiin, koska useimmiten menetelmät tukevat hyvin toisiaan. Haastattelun avulla voidaan esimerkiksi selventää tai syventää asioita. Haastattelu sopii hyvin useisiin kehittämistehtäviin, koska sen avulla saadaan kerättyä syvällistäkin tietoa kehittämisen kohteesta nopeasti. (Ojasalo ym. 2014, 106.) Haastattelulla saadaan työn kohteesta aitoa käytännön tietoa, joka auttaa ymmärtämään ilmiötä ja sen kanssa toimivia henkilöitä. Haastattelujen tavoitteena on luoda tutkittaviin luottamuksellinen suhde ja samalla sitouttaa heidät varsinaiseen muutosprosessiin. (Kananen 2017, 48.)

Haastattelu on eräänlaista keskustelua, mutta se toteutuu tutkijan aloitteesta ja on tutkijan johdattelema tavoitteellinen tiedonkeruun tilanne (Eskola & Suoranta 2014, 86). Haastattelu on vuorovaikutustilanne, jonka avulla yritetään saada merkityksellistä tietoa (Hirsjärvi & Hurme 2022, 32). Haastattelut voidaan jakaa strukturoituihin, puolistrukturoituihin, avoimiin ja teemahaastatteluihin. Strukturoidussa haastattelussa kysymykset ja vastausvaihtoehdot ovat kaikille samat eli käytännössä kyseessä on ohjattu kyselylomakkeen täyttäminen. Puolistrukturoidussa haastattelussa kysymykset ovat kaikille samat, mutta haastateltavat vastaavat niihin itse omin sanoin. Avoimessa haastattelussa tilanne muistuttaa kaikista eniten tavallista keskustelua, koska niissä voidaan keskustella kunkin haastateltavan kanssa eri asioista. Teemahaastattelussa kaikkien haastateltavien kanssa keskustellaan samoista teemoista, mutta kysymyksillä ei ole tarkkaa muotoa tai järjestystä, vaan ainoastaan päätetyt aihealueet, joita haastattelussa nostetaan esiin. (Eskola & Suoranta 2014, 87.)

Tavallisin tapa tehdä haastatteluja ovat yksilöhaastattelut. Ryhmähaastattelut ja niiden alalaji parihaastattelut ovat kuitenkin myös käyttökelpoisia tapoja haastattelun toteuttamiseen. Ryhmähaastattelun etuna on tiedon saaminen samanaikaisesti useammalta vastaajalta. Haittana voi olla ryhmädynamiikka ja valtahierarkia voi vaikuttaa siihen, ketkä haastateltavat puhuvat ja mitä he puhuvat. (Hirsjärvi ym. 2009, 210–211.)

Haastattelukysymykset kannattaa muotoilla myönteisiksi (Hirsjärvi & Hurme 2022, 110). Haastattelukysymysten kannattaa olla yksinkertaisia ja suppeita (Brinkmann & Kvale 2018, 67). Tällöin haastattelun avulla saadaan todennäköisimmin vastauksia siihen asiaan, jota tutkitaan. Haastattelun onnistumista edesauttavat hyvä ennakkovalmistautuminen ja haastattelun esitestaus (Eskola & Suoranta 2014, 91).

Perinteisesti haastatteluja on toteutettu kasvotusten. Perinteiseen verrattuna verkkohaastattelu ei ole aito, koska tutkija ja haastateltava eivät ole samassa tilassa siten, että tutkija voisi havainnoida kehonkieltä kokonaisuutena. Verkkohaastattelun etuna voi pitää aika- ja kustannussäästöä sekä joustavaa haastatteluaikaa. Sekä perinteinen että verkkohaastattelu edellyttävät luottamuksellista suhdetta tutkijan ja haastateltavien välille syvällisen ja luotettavan tiedon saamiseksi tutkittavasta ilmiöstä. (Kananen 2017, 53.)

Tässä opinnäytetyössä yhdeksi aineistonkeruumenetelmäksi on valittu haastattelu, koska yhtenä tavoitteena on selvittää johdon edustajien näkemys digiturvallisuuskoulutusten järjestämisestä. Lisäksi haastattelulla on tavoite saada johdon edustajilta käytännön tietoa, jota voi hyödyntää digiturvaosaamisen kehittämissuunnitelman laadinnassa. Tavoitteena on saada myös johdon edustajat sitoutumaan digiturvaosaamisen kehittämiseen. Haastattelukysymykset luodaan puolistrukturoiduksi siten, että kysymykset ovat myönteisiä. Haastattelusta saatavaa tietoa hyödynnetään myös digiturvallisuuskoulutuksen suunnittelussa. Koulutuksen suunnittelussa hyödynnetään myös muiden Luovin asiantuntijoiden osaamista.

5.2.3 Suunnittelupaja

Kehittämistyössä voidaan hyödyntää myös muita kuin tieteellisen tutkimuksen menetelmiä. Erilaiset luovuusmenetelmät ja -työkalut sopivat hyvin kehittämiseen. Niiden avulla voidaan tuottaa uusia näkökulmia, ideoita ja ratkaisuja käytännössä kaikenlaisiin kehittämistöihin. (Moilanen ym. 2022, 192). Kehittämistöissä on hyvä hyödyntää myös erilaisia yhteisöllisiä ideointimenetelmiä, joiden avulla asiaan voidaan tuottaa uusia näkökulmia sekä saada uusia ideoita ja ratkaisuja (Ojasalo ym. 2014, 158). Eräs työväline luovaan käytäntöjen yhteiskehittämiseen on Innopaja.

Innopaja-toimintamalli on helposti käyttöönotettava toimintatapa ja työväline käytäntöjen yhteiskehittämiselle ensisijaisesti hyvinvointi- ja terveysalan kehittäjille ja ammattilaisille. Mallissa työskentelyllä on yhteinen kohde ja siihen osallistuvat asian kannalta keskeiset toimijat. Innopajassa kaikkien toimijoiden näkökulmat ovat keskenään samanarvoisia. (Peränen 2013, 3.)

Innopaja-mallia voi soveltaa myös muissa kuin hyvinvointi- ja terveysalan organisaatioissa. Tässä opinnäytetyössä sovelletaan Innopaja-toimintamallia siten, että yhdessä asiantuntijoiden kanssa pidettyjä suunnittelutilaisuuksia kutsutaan suunnittelupajoiksi. Pajoissa suunnitellaan ja kehitetään digiturvakoulutuksia siten, että kaikkien osallistujien näkökulmat huomioidaan samanarvoisina.

5.3 Kehittämistyön luotettavuus

Tutkimuksellisten kehittämistöiden luotettavuuden tarkastelu on haasteellista, sillä tutkimusmenetelmät ovat monimenetelmäisiä ja kyseessä on muutoksen aikaansaaminen. Luotettavuutta tulee tarkastella sekä kehittämistyön tuotoksen onnistumisen että tutkimusmenetelmien käytön kannalta. Tutkimuksellisissa kehittämistöissä tavoitteena on jokin muutos, jonka onnistuminen on tärkeää käytännön kannalta. Luotettavuutta voidaan arvioida siten muutoksen osalta ratkaisun toimivuudella ja onnistumisella. Lisäksi täytyy arvioida kehittämistyön tutkimusprosessin luotettavuutta tieteellisin perustein. (Kananen 2017, 69, 79.)

Hyvän tutkimuksen perusvaatimuksia ovat reliabiliteetti eli luotettavuus, validiteetti, objektiivisuus, tehokkuus ja taloudellisuus, avoimuus, tietosuoja, hyödyllisyys ja käyttökelpoisuus sekä sopiva aikataulu (Heikkilä 2014, 27–30). Kysymys luotettavuudesta kohdistuu tutkimuksessa käytettyihin menetelmiin, tutkimusprosessiin ja tutkimuksessa saatuihin tuloksiin (Toikko & Rantanen 2009, 121). Reliabiliteetti tarkoittaa tulosten tarkkuutta. Tutkimuksen tulokset eivät saisi olla sattumanvaraisia, vaan tutkimuksen tulisi olla toistettavissa. Tutkijan on oltava koko tutkimuksen ajan tarkka ja hänen on kyettävä tarkastelemaan asioita kriittisesti. Validiteetti tarkoittaa, että tutkimus mittaa sitä, mitä sen oli tarkoitus selvittää. Validius on varmistettava etukäteen huolellisen suunnittelun ja harkitun tiedonkeruun avulla. (Heikkilä 2014, 28.)

Tutkimuksen luotettavuutta voi lisätä triangulaation avulla. Kun tutkimuksen kohdetta tutkitaan useilla eri aineistonhankintamenetelmillä, puhutaan menetelmätriangulaatiosta. Menetelmätriangulaatio tarkoittaa sitä, että samassa tutkimuksessa voi yhdistää laadullisia ja määrällisiä menetelmiä. Parhaimmillaan tämä voi tuottaa mielenkiintoisia tuloksia, mutta samalla on pohdittava, onko erityyppisten aineistojen yhteensovittaminen soveliasta. (Eskola & Suoranta 2014, 70–71.) Tutkimuksellisissa kehittämistöissä tutkimusmenetelmien luottavuuden lisäksi tärkeää on kehittämistyön hyödyntämiskelpoisuus. Kehittämistoiminnassa luotettavuus tarkoittaa ennen kaikkea käyttökelpoisuutta. Kehittämistoiminnan yhteydessä syntyvän tiedon tulee olla todenmukaista ja hyödyllistä. (Toikko & Rantanen 2009, 121–122.)

6 Opinnäytetyön toteutus

Aloin laatia opinnäytetyötä lokakuussa 2022, kun sovimme toimeksiannosta opinnäytetyön ohjaajan Ammattiopisto Luovin tieto- ja viestintäjohtaja Susanna Kankaan kanssa. Luovissa oli tunnistettu tarve digiturvaosaamisen kehittämiselle ja päätetty järjestää koulutusta digiturvasta. Opinnäytetyö oli helppoa yhdistää käytännön työhöni tiedonhallinnan asiantuntijana. Olen myös Ammattiopisto Luovi Oy:n osakkeet 100 prosenttisesti omistavan Hengitysliiton

tietosuojavastaava, sillä Luovi myy muun muassa tiedonhallinta- ja digipalveluja Hengitysliitolle. Työskentelen Luovin digipalvelujen tiimissä, johon kuuluu IT- ja digipäällikkö, IT-palvelupäällikkö, järjestelmäsuunnittelija, kaksi järjestelmäasiantuntijaa, IT-hankinta-asiantuntija, kuusi IT-tukihenkilöä, digiasiantuntija ja kaksi tiedonhallinnan asiantuntijaa. Digitiimiin kuuluu tällä hetkellä yhteensä 15 työntekijää. Keskeistä tiimin työskentelyssä on digiturvasta huolehtiminen.

6.1 Koulutustarvekyselyn toteutus

Aloitin opinnäytetyön laadinnan kyselylomakkeen valmistelulla. Liitteessä 1 esitetyn kyselyn avulla oli tarkoitus selvittää, millaisista digiturvallisuusasioista henkilöstö kaipaa lisätietoa. Kyselylomakkeeseen halusin laittaa taustatiedoksi kysymyksen, kuuluuko vastaaja koulutushenkilöstöön vai Luovi-palvelujen henkilöstöön. Tavoitteena oli selvittää, eroavatko Luovin ydintehtävän henkilöstön eli koulutuksen henkilöstön koulutustoiveet tukipalvelujen henkilöstön koulutustoiveista. Lisäksi halusin selvittää, eroavatko vastaukset digiturvallisuutta koskeviin väittämiin ydintehtävän henkilöstön ja tukipalvelujen henkilöstön kesken.

Luovissa on päädytty käyttämään digiturvasta määritelmää, jonka mukaisesti siihen kuuluvat tietosuoja, tietoturva, riskienhallinta, jatkuvuuden hallinta ja kyberturvallisuus. Lähdin miettimään koulutustarpeita näiden osa-alueiden pohjalta. Yhdistin tietosuojan ja tietoturvan aihealueet kysymykseen numero kaksi. Vaihtoehdot koulutusaiheiksi kokosin tietosuojaan ja tietoturvaan kuuluvista aiheista sekä asioista, jotka Luovin digiturvallisuussivustolla on niistä koottuna. Kolmanteen kysymykseen yhdistin muut kolme digiturvallisuuden osa-aluetta eli riskienhallinnan, kyberturvallisuuden ja jatkuvuuden hallinnan. Keräsin myös tämän kysymyksen aiheet kyseisten osa-alueiden sisällöistä ja Luovin digiturvasivustolla olevista asioista. Otin mukaan osa-alueista vain sellaiset sisällöt, joista ajattelin Luovin henkilöstön hyötyvän tässä vaiheessa. Kaikkien näiden osa-alueiden sisältöjen mukaan ottaminen olisi tehnyt kysymyksestä mielestäni liian laajan. Henkilöstön kiinnostus eri koulutusaiheisiin kartoitettiin, jotta koulutuksen sisältö saadaan luotua henkilöstöä kiinnostavaksi. Lisäksi saatua tietoa kiinnostavista aiheista voi hyödyntää Luovin digisivuston kehittämisessä.

Neljänneksi ja viidenneksi kysymykseksi laitoin koulutusmuotoa ja -tapaa koskevat kysymykset. Halusin selvittää, mikä olisi vastaajien mielestä paras tapa digiturvallisuuskoulutuksen järjestämiselle. Rajasin neljännen ja viidennen kysymyksen vaihtoehdot neljään, jotta kaikki vaihtoehdot näkyisivät näytöllä yhtä aikaa myös mobiililaitteilla kyselyyn vastatessa. Tiedossa oli, että koulutukset tullaan todennäköisesti järjestämään Teams-koulutuksina, koska live-koulutusten järjestäminen olisi liian työlästä toteuttaa ympäri Suomea. Halusin kuitenkin selvittää, kaipaisiko henkilöstö tietoa digiturvasta paikan päällä pidettävänä koulutuksena.

Kuudenneksi kysymykseksi laitoin neljä väittämää digiturvallisuutta koskien. Ajatuksena oli, että näitä väittämiä voitaisiin hyödyntää koulutusten jälkeen pyydettävässä palautteessa. Koulutusten palautelomakkeeseen voisi laittaa samat väittämät ja selvittää, ovatko vastaajien kokemukset digiturvallisuutta koskien muuttuneet koulutuksen ansiosta. Halusin väittämien avulla selvittää, ymmärtääkö henkilöstö, mitä digiturvallisuus tarkoittaa ja tietävätkö he, mitä seurauksia sen laiminlyönnillä voi olla. Lisäksi halusin selvittää, kokeeko henkilöstö tällä hetkellä digiturvallisuuden olevan osa heidän työarkeaan ja haluavatko he olla mukana huolehtimassa digiturvasta. Väittämien avulla oli tarkoitus saada tietoa henkilöstön mietteistä koulutuksen suunnittelun tueksi.

Kyselyn loppuun laitoin myös avoimen kysymyksen, jossa halusin tarjota vastaajille mahdollisuuden kertoa omin sanoin, millainen koulutus saisi heidät motivoitumaan digiturvallisuusasioista. Kannustin vastaajia ideoimaan rohkeasti ja kysyin, mitä mieltä he olisivat esimerkiksi digiturvallisuusteemaisesta pakohuoneesta. Avoimen kysymyksen tarkoituksena oli saada monipuolisesti ideoita koulutusten toteuttamiselle. Halusin nähdä, olisiko vastaajilla mielessä jotakin uudenlaisia koulutuksen toteuttamiskeinoja.

Kaikkiaan halusin pitää kysymyslomakkeen lyhyenä ja nopeasti vastattavana, jotta vastauksia saataisiin mahdollisimman monta. Pyysin kyselylomakkeen luonnoksesta palautetta muilta Luovin asiantuntijoilta sekä Luovin tieto- ja viestintäjohtajalta ja IT- ja digipäälliköltä. Lisäksi Luovin digijelpit eli digitukihenkilöt esitestasivat kyselyä. Luovissa on yli 20 digijelppiä. He ovat ohjaajia, opettajia

tai opintoneuvojia, jotka oman työnsä ohessa auttavat muuta henkilöstä arjen digikysymyksissä, kuten digitaalisten opetusohjelmien käytössä. Muokkasin hieman kyselyä saadun palautteen pohjalta ja laadin myös saateviestin sekä sanaston, jotta kyselyyn olisi helppo vastata, vaikka digiturvallisuus ei olisikaan vielä terminologisesti kovin tuttu. Tavoitteena oli selvittää henkilöstön koulutustarpeita kattavasti, jotta järjestettävä koulutus vastaisi niitä asioita, joista henkilöstö kaipaa lisää tietoa. Kun koulutuksen sisältö on luotu osallistujien tarpeista lähtien, osallistujien on helpompi motivoitua koulutukseen ja koulutettavat asiat jäävät todennäköisesti paremmin mieleen.

Kävin Luotsi-infossa perjantaina 18.11.2022 esittelemässä tarvetta digiturvallisuuden kehittämiselle ja koulutustarpeiden selvittämiseksi laadittua kyselyä. Luotsi-info on Luovin esihenkilöille tarkoitettu infotilaisuus. Esitin esihenkilöille toiveen, että he vastaisivat itse koulutustarvekyselyyn ja hoksauttaisivat kyselystä omaa henkilöstöään ja kannustaisivat työntekijöitä vastaamaan. Kerroin esihenkilöille, että tulosten perusteella johto linjaa, millä tavalla ja miten laajasti digiturvakoulutusta toteutetaan vuonna 2023.

Kyselystä julkaistiin maanantaina 21.11.2022 Satamassa (intra) seuraava uutinen: ”Vastaamalla kyselyyn ’Koulutustarpeiden kartoitus digiturvallisuudesta’ pääset vaikuttamaan oman osaamisesi kehittämiseen. Tulokset huomioidaan keväällä 2023 sisäisesti pidettävissä digiturvallisuuskoulutuksissa. Jätä arvokas vastauksesi tänne (linkki Webropol-kyselyyn). Voit hyödyntää vastatessasi myös kyselyyn liittyvää sanastoa (linkki sanastoon) toisella välilehdellä. Tarkemmat tiedot kyselystä löydät alta (kyselyn saate). Suuret kiitokset vastauksestasi 😊!”. Liitteessä 1 on kyselyn saate, kyselylomake ja kyselyyn liittyvä sanasto.

Tarkoituksenani oli muistuttaa kyselystä sen vastausajan loppupuolella ja pitää kyselyä esillä siten, että siihen tulisi mahdollisimman monta vastausta. Olin kuitenkin poissa työstä perheenjäsenen vakavan sairastumisen vuoksi juuri kyselyn vastausajan ollessa käynnissä. Sen vuoksi kyselystä ei valitettavasti muistutettu henkilöstöä.

6.2 Tutkimushaastattelun toteutus

Sovin marraskuun alussa haastatteluajan ylemmän johdon edustajan, tieto- ja viestintäjohtaja Susanna Kankaan sekä keskijohdon edustajan, IT- ja digipäällikkö Mervi Leinosen kanssa. He työskentelevät Oulussa ja tarkoitus oli, että menisin perjantaina 16.12.2022 Ouluun, jotta voisimme pitää haastattelun kasvotusten. Perhetilanteeni takia en kuitenkaan voinut lähteä Ouluun, vaan toteutin haastattelun Teams-kokouksena. Tilanteen takia en saanut myöskään valmisteltua haastattelukysymyksiä niin perusteellisesti kuin olisin halunnut. Mietin kysymykset myönteiseen muotoon siten, että saisin niiden avulla kartoitettua johdon edustajien näkemyksen digiturvakoulutusten sisällöstä ja koulutusten järjestämisestä sekä näkemykset digiturvallisuudesta. Tavoitteena oli, että opinnäytetyön tuotokset vastaavat myös johdon tarpeita. Haastattelukysymykset on esitetty liitteessä 2. Kävimme kysymykset keskustellen läpi yhdessä tieto- ja viestintäjohtajan sekä IT- ja digipäällikön kanssa.

Vuoden 2023 alussa pohdimme yhdessä IT- ja digipäällikön ja tieto- ja viestintäjohtajan kanssa, että osana digiturvallisuuden kehittämistä järjestettävä sisäinen koulutus voisi olla tehokkain, mikäli se järjestettäisiin koko henkilöstölle velvoittavana koulutuksena. Todennäköisesti vapaaehtoiseen koulutukseen ei saataisi niin monia osallistujia kuin velvoittavana sisäisenä koulutuksena järjestettävään koulutukseen. Koko henkilöstölle järjestettävä koulutus vaatii Luovissa johtoryhmän hyväksynnän, joten sovimme, että esittelisin asiaa johtoryhmässä.

Vierailu johtoryhmään saatiin sovittua torstaille 16.2.2023. Pidin johtoryhmälle esityksen, jossa perustelin, miksi digiturvallisuuskoulutus kannattaisi järjestää velvoittavana koko henkilöstölle. Esittelin johtoryhmälle luonnoksen digiturvakoulutuksen sisällöstä ja aikataulusta. Pohjaehdotuksena oli, että koulutusta pilotoitaisiin keväällä 2023 esimerkiksi henkilöstöpalvelujen tai taloushallintopalvelujen henkilöstölle ja varsinaiset koulutukset käynnistettäisiin syksyllä 2023. Poiketen kyselylomakkeessa ilmoitetusta aikataulusta varsinaiset koulutukset haluttiin siirtää syksylle, koska erityisesti Luovin koulutuksen henkilöstössä tapahtuu muutoksia työvuoden (lukuvuoden) vaihtuessa.

Johtoryhmä päätti järjestää digiturvallisuuskoulutuksen koko Luovin henkilöstölle siten, että pilottikoulutuksia järjestetään kaksi keväällä 2023. Toiseen koulutukseen osallistuivat henkilöstöpalvelujen ja taloushallinto- ja hankintapalvelujen sekä Kuopion ja Porin henkilöstöt. Toisen pilottiryhmän koulutukseen osallistuvat Tornion, Kittilän ja Rovaniemen henkilöstö. Johtoryhmä uutisoi päätöksestään Satamassa (intra) ja kertoi myös, että digiturvallisuuden parantamisella lisätään opiskelijoiden ja henkilöstön turvallisuutta.

Johtoryhmän kokous sujui oikein hyvin. Oli hienoa nähdä, kuinka hyvin Luovin johto ymmärsi digiturvallisuuden merkityksen. Tieto- ja viestintäjohtaja johtoryhmän jäsenenä on selkeästi pitänyt esillä myös digiturvallisuusasioita. Tapaaminen antoi myös hyviä eväitä koulutusten järjestämiselle sekä muille digiturvallisuusosaamisen kehittämissuunnitelmaan sisältyville kokonaisuuksille. Johtoryhmässä käydyn keskustelun perusteella pilottiryhmään päätettiin ottaa heti mukaan myös ydintehtävän henkilöstöä, koska heitä on 90 prosenttia Luovin henkilöstöstä. Lisäksi johtoryhmä otti ylös muun muassa ehdotuksen huomioida digiturva tavallista laajemmin jo jossakin kevään 2023 Luotsi-infossa (esihenkilöiden kokous) ja Luovi-infossa (koko henkilöstölle pidettävä infotilaisuus).

6.3 Suunnittelupajojen toteutus

Suunnittelupajat tulivat mukaan opinnäytetyöhön prosessin edetessä, kun aineistoa oli tarpeellista kehittää yhteistyössä muiden kanssa. Pajoja varten laadin luonnoksen digiturvakoulutuksen sisällöstä ja toteutuksesta henkilöstölle toteutetun kyselyn tulosten sekä johdon edustajille tehdyn haastattelun tulosten pohjalta. Otin luonnoksen sisällössä huomioon myös Digi- ja väestötietoviraston laatimia verkosta löytyviä työkaluja ja koulutuksia, joiden avulla digiturvaosaamista voi kehittää.

Digi- ja väestötietovirasto on laatinut viime vuosina useita selvityksiä ja raportteja, oppaita ja hyviä käytäntöjä, työkaluja ja mallipohjia sekä ohjeita digiturvaasioihin liittyen. Dokumenttien tarkoituksena on auttaa organisaatioita kehittämään digiturvallisuuden hallintaa. Otin Luovin digiturvakoulutusluonnokseen

mukaan muun muassa Digi- ja väestötietoviraston toteuttamaan koulutuskokonaisuuteen ”Digiturvallinen elämä” sisältyviä noin minuutin mittaisia ”Digiturma vai digiturva” -lyhytvideoita. Videoissa käydään läpi olennaisia digiturvalliseen toimintaan liittyviä tilanteita, kuten työpuhelujen puhumista. (Digi- ja väestötietovirasto 2023.)

Ensimmäinen suunnittelupaja pidettiin perjantaina 13.1.2023 tieto- ja viestintäjohtajan, IT- ja digipäällikön sekä toisen tiedonhallinnan asiantuntijan eli työparini kanssa. Pajassa esittelin luonnoksen, jonka mukaan digiturvakoulutus sisältäisi digisivuston esittelyn, teoriaosuuden, harjoitusosuuden, harjoitusten ratkaisujen läpikäynnin, kultajyväosuuden (tärkeimmät arjessa huomioitavat asiat) sekä osaamisen testauksen. Keskustelimme suunnittelupajassa myös koulutuksen toteuttavista henkilöistä sekä aikataulusta, jolla koulutukset järjestettäisiin.

Pidin suunnittelupajat myös perjantaina 20.1.2023 henkilöstöasiantuntijan kanssa ja perjantaina 27.1.2023 digiasiantuntijan ja digipedagogin kanssa. Näissä molemmissa pajoissa oli mukana myös työparini. Suunnittelupajoissa kävimme läpi tekemääni luonnosta koulutuksen rungoksi sekä toteutuksen käytännön asioita, kuten pienryhmätilojen käyttöä Teamsissa sekä Kahoot-testin laatimista osaamisen testausta varten. Pidimme vielä henkilöstöasiantuntijan kanssa yhden suunnittelupajan 15.3.2023 suunnitellaksemme sen, millaisiin ryhmiin henkilöstö kannattaa jakaa koulutuksissa. Koulutukset on suunniteltu toteutettavaksi paikkakunnille kohdistettuna siten, että yhteen Teams-koulutukseen osallistuu lähekkäisiä paikkakuntia, joiden yhteenlaskettu henkilöstömäärä on noin 100 henkilöä.

Viimeisen suunnittelupajan pidimme perjantaina 14.4.2023 henkilöstöasiantuntijan, digiasiantuntijan ja digipedagogin kanssa digiturvakoulutuksen sisältösuunnitelman viimeistelemiseksi, jotta digiturvakoulutus olisi osallistujille mahdollisimman höydyllinen ja helposti ymmärrettävissä. Kaiken kaikkiaan pajojen tavoitteena oli saada digiturvallisuuskoulutuksen sisältö ja toteutus mahdollisimman tarkoituksenmukaiseksi jokaiselle luovilaisille. Suunnittelupajojen tulokset näkyvät Digipurjeet-koulutuksen sisällössä (luku 8.2).

7 Opinnäytetyön tulokset

7.1 Koulutustarvekyselyn tulokset

Ammattiopisto Luovin henkilöstölle osoitettuun ”Koulutustarpeiden kartoitus digiturvallisuudesta”-kyselyyn tuli 100 vastausta. Kyselyn vastausprosentiksi muodostui 11,5 prosenttia, kun Luovissa työskenteli tuolloin noin 870 henkilöä. Koulutustarpeiden kartoituskysely toteutettiin Webropol-kyselynä, jonka vastausaika oli 21.11.–8.12.2022. Liitteessä 1 on esitetty koulutustarvekyselyn saate ja sen sisältö sekä vastaamisen helpottamiseksi laadittu sanasto. Kyselyn avoin kysymys on analysoitu laadullisesti ja muut tulokset määrällisesti.

Taustatieto

Taustatietona kyselyyn vastaajilta kysyttiin, ovatko he koulutuksen henkilöstöä vai Luovi-palvelujen henkilöstöä eli mihin henkilöstöryhmään he kuuluvat. Koulutuksen henkilöstöön määriteltiin kuuluvaksi ydintehtävän eli koulutuksen järjestämisen parissa työskentelevät esihenkilöt ja työntekijät. Luovi-palvelujen henkilöstöksi määriteltiin tukipalvelujen esihenkilöt ja työntekijät.

Taulukossa 1 on esitetty vastausten jakautuminen taustatietokysymykseen. Vastaajista 70 henkilöä oli koulutuksen henkilöstöä ja 30 Luovi-palvelujen henkilöstöä. Kyselyyn vastasi tukipalvelujen henkilöstöstä noin 34,5 prosenttia ja koulutuksen henkilöstöstä noin 8,9 prosenttia. Tuolloin Luovin työntekijöistä arviolta 90 prosenttia eli 783 henkilöä oli koulutuksen henkilöstöä ja 10 prosenttia eli 87 henkilöä tukipalvelujen henkilöstöä.

	n	Prosentti
Koulutuksen henkilöstö (ydintehtävän parissa työskentelevät esihenkilöt ja työntekijät)	70	70,0 %
Luovi-palvelujen henkilöstö (tukipalveluissa työskentelevät esihenkilöt ja työntekijät)	30	30,0 %

Taulukko 1. Kyselyyn vastaajien henkilöstöryhmä.

Tietoturvan ja tietosuojan koulutustarpeet

Taulukossa 2 on esitetty vastausten jakautuminen suosituimmuusjärjestyksessä kysymykseen, mistä tietoturvaan ja tietosuojaan liittyvistä asioista kaivataan koulutusta. Taulukossa vaaleanpunaisessa sarakkeessa on koulutuksen henkilöstön eli ydinpalvelujen ja vaaleansinisessä sarakkeessa Luovi-palvelujen eli sisäisten tukipalvelujen henkilöstön vastausten jakautuminen. Vihreässä sarakkeessa on henkilöstöryhmien yhteenlaskettu tulos. Kiinnostus koulutusaiheita kohtaan jakaantui vahvasti ja yhtäkään koulutusaihetta ei valinnut yli 50 prosenttia vastaajista.

Koulutusaihe	Koulutuksen henkilöstö		Luovi-palvelujen henkilöstö		Henkilöstö-ryhmät yhteensä	
	n	%	n	%	n	%
Riskien ja vaikutusten arviointi	24	35,8 %	13	43,3 %	37	38,1 %
Huijausviestien tunnistaminen	27	40,3 %	9	30,0 %	36	37,1 %
Henkilötietojen käsittelystä informointi (tietosuojaselost.)	22	32,8 %	13	43,3 %	35	36,1 %
Erityiset henkilötietoryhmät	23	34,3 %	10	33,3 %	33	34,0 %
Henkilötietojen käsittely	22	32,8 %	9	30,0 %	31	32,0 %
Tietosuojaperiaatteet	22	32,8 %	9	30,0 %	31	32,0 %
Turvatulostus	24	35,8 %	6	20,0 %	30	30,9 %
Henkilötunnuksen käsittely	18	26,9 %	8	26,7 %	26	26,8 %
Rekisteröidyn oikeudet	19	28,4 %	7	23,3 %	26	26,8 %
Tietoturvapäivitykset	15	22,4 %	7	23,3 %	22	22,7 %
Tietosuojatermit, kuten rekisterinpitäjä	13	19,4 %	6	20,0 %	19	19,6 %
Etätyö	14	20,9 %	4	13,3 %	18	18,6 %
Monivaiheinen tunnistautuminen	9	13,4 %	6	20,0 %	15	15,5 %
Tietoverkot	6	9,0 %	6	20,0 %	12	12,4 %
Sähköpostin käsittely	7	10,4 %	5	16,7 %	12	12,4 %
Käyttäjätunnus ja salasana	1	1,5 %	1	3,3 %	2	2,1 %
Jokin muu, mikä?	0	0,0 %	0	0,0 %	0	0,0 %
Vastaajia yhteensä	*70*		*30*		*100*	

Taulukko 2. Koulutustoiveet tietosuojaan ja tietoturvaan liittyvistä aiheista.

Suosituimmaksi koulutusaiheeksi tuli ”Riskien ja vaikutusten arviointi”, jonka valitsi yhteensä 37 vastaajaa eli 38,1 prosenttia kaikista vastanneista. Lähes yhtä suosittuja olivat ”Huijausviestien tunnistaminen” 36 valitsijalla ja ”Henkilötietojen käsittelystä informointi” 35 valitsijalla. Käyttäjätunnuksesta ja salasanasta koulutusta kaipaa ainoastaan kaksi vastaajaa. Sähköpostin käsittelystä ja tietoverkoista koulutusta vastasi kaipaavansa 12 vastaajaa.

Riskienhallinnan, kyberturvan ja jatkuvuuden hallinnan koulutustarpeet

Muista digiturvallisuuden osa-alueista tehdyt koulutusaihevalinnat on esitetty suosituimmuusjärjestyksessä taulukossa 3. Kyberuhkien tunnistamisen valitsi 54 henkilöä eli 56,3 prosenttia kaikista vastaajista. Suosittuja aiheita olivat myös ”Riskien tunnistaminen”, ”Sähköisiin häiriötilanteisiin varautuminen” ja ”Poikkeamien tunnistaminen”, jotka kiinnostivat yhteensä yli 40 henkilöä. Poikkeamista toipuminen oli selkeästi vähiten kiinnostava koulutusaihe, mutta senkin valitsi yhteensä 12 vastaajaa.

Koulutusaihe	Koulutuksen henkilöstö		Luovi-palvelujen henkilöstö		Henkilöstö-ryhmät yhteensä	
	n	Prosentti	n	Prosentti	n	Prosentti
Kyberuhkien tunnistaminen	37	56,1 %	17	56,7 %	54	56,3 %
Riskien tunnistaminen	37	56,1 %	12	40,0 %	49	51,0 %
Sähköisiin häiriötilanteisiin varautuminen	35	53,0 %	11	36,7 %	46	47,9 %
Poikkeamien tunnistaminen	28	42,4 %	14	46,7 %	42	43,8 %
Riskien pienentäminen	25	37,9 %	12	40,0 %	37	38,5 %
Poikkeamiin varautuminen eli jatkuvuussuunnittelu	21	31,8 %	10	33,3 %	31	32,3 %
Informaatiovaikuttaminen	23	34,8 %	7	23,3 %	30	31,3 %
Riskien analysointi	15	22,7 %	8	26,7 %	23	24,0 %
Poikkeamista toipuminen	6	9,1 %	6	20,0 %	12	12,5 %
Jokin muu, mikä?	0	0,0 %	0	0,0 %	0	0,0 %
Vastaajia yhteensä	*70*		*30*		*100*	

Taulukko 3. Koulutustoiveet muista digiturvan osa-alueista.

Koulutustapavaihtoehdot

Neljännessä kysymyksessä vastaajia pyydettiin laittamaan koulutustapavaihtoehdot paremmuusjärjestykseen siten, että he antavat arvon yksi mieluisimmalle, arvon kaksi seuraavaksi mieluisimmalle ja arvon neljä vähiten mieluisalle. Taulukossa 4 on esitetty vastausten jakautuminen yhteenlaskettujen keskiarvojen mukaisessa järjestyksessä. Kyselyyn vastanneet antoivat useimmiten arvon yksi kuukausittaisille lyhyille tietoiskuille. Koulutuksen henkilöstöstä näin teki 47,8 prosenttia ja tukipalvelujen 63,3 prosenttia. Kuukausittaisten lyhyiden tietoiskujen yhteenlasketuksi keskiarvoksi muodostui 1,8. Molempien henkilöstöryhmien enemmistö valitsi vähiten mieluisaksi koulutustavaksi yhden laajan koulutuksen harvoin koko digiturvallisuuden kokonaisuudelle. Koulutuksen henkilöstöstä 69,6 ja Luovi-palvelujen henkilöstöstä 83,3 prosenttia antoi tälle vaihtoehdolle arvon neljä.

Koulutustapavaihtoehdot	1	2	3	4	Keski-arvo	n
Kuukausittaiset lyhyehköt tietoiskut						
Koulutuksen henkilöstö	47,8 %	30,4 %	11,6 %	10,2 %	1,8	69
Luovi-palvelujen henkilöstö	63,3 %	23,3 %	6,7 %	6,7 %	1,6	30
Henkilöstöryhmät yhteensä	52,5 %	28,3 %	10,1 %	9,1 %	**1,8**	99
Infopaketit puolivuosittain ajankohtaisista asioista						
Koulutuksen henkilöstö	26,1 %	43,5 %	23,2 %	7,2 %	2,1	69
Luovi-palvelujen henkilöstö	16,7 %	56,7 %	23,3 %	3,3 %	2,1	30
Henkilöstöryhmät yhteensä	23,2 %	47,5 %	23,2 %	6,1 %	**2,1**	99
Laajat koulutukset tietylle kokonaisuudelle						
Koulutuksen henkilöstö	14,5 %	18,8 %	53,6 %	13,1 %	2,7	69
Luovi-palvelujen henkilöstö	20,0 %	10,0 %	63,3 %	6,7 %	2,6	30
Henkilöstöryhmät yhteensä	16,1 %	16,2 %	56,6 %	11,1 %	**2,6**	99
Yksi laaja koulutus harvoin koko kokonaisuudelle						
Koulutuksen henkilöstö	11,6 %	7,2 %	11,6 %	69,6 %	3,4	69
Luovi-palvelujen henkilöstö	0,0 %	10,0 %	6,7 %	83,3 %	3,7	30
Henkilöstöryhmät yhteensä	8,1 %	8,1 %	10,1 %	73,7 %	**3,5**	99

Taulukko 4. Koulutustapavaihtoehtojen valinnat henkilöstöryhmittäin.

Koulutusmuodot

Viidennessä kysymyksessä vastaajia pyydettiin laittamaan neljä eri koulutusmuotovaihtoehtoa paremmuusjärjestykseen siten, että he antavat arvon yksi mieluisimmalle ja arvon neljä vähiten mieluisalle. Taulukossa 5 on esitetty vastausvaihtoehtojen saamat prosenttijakaumat yhteenlaskettujen keskiarvojen mukaisessa suosituimmuusjärjestyksessä. Tukipalvelujen henkilöstöstä 40,0 prosenttia valitsi parhaaksi koulutusmuodoksi etäkoulutukset Teamsilla. Koulutushenkilöstön suosituimmaksi koulutuksen muodoksi tuli toiminnallinen koulutus, jolle arvon yksi antoi 34,8 prosenttia. Tukipalvelujen henkilöstön keskuudessa toiminnallinen koulutus taas sai eniten arvoja 4 (46,7 prosenttia). Vähiten mieluisa koulutusvaihtoehto koulutushenkilöstölle oli koulutusympäristö, jossa tehtäviä tehdään itsenäisesti (39,1 prosenttia). Koulutusmuotojen suosituimmuudessa oli selkeitä eroja henkilöstöryhmien välillä ja niiden sisällä.

Koulutusmuotovaihtoehdot	1	2	3	4	Keski-arvo	n
Etäkoulutus Teamssilla						
Koulutuksen henkilöstö	31,9 %	27,5 %	23,2 %	17,4 %	2,3	69
Luovi-palvelujen henkilöstö	40,0 %	20,0 %	20,0 %	20,0 %	2,2	30
Henkilöstöryhmät yhteensä	34,3 %	25,3 %	22,2 %	18,2 %	**2,2**	99
Toiminnallinen koulutus, jossa esimerkiksi ryhmätöitä						
Koulutuksen henkilöstö	34,8 %	21,7 %	23,2 %	20,3 %	2,3	69
Luovi-palvelujen henkilöstö	30,0 %	20,0 %	3,3 %	46,7 %	2,7	30
Henkilöstöryhmät yhteensä	33,3 %	21,2 %	17,2 %	28,3 %	**2,4**	99
Koulutusympäristö, jossa tehtäviä tehdään itsenäisesti						
Koulutuksen henkilöstö	20,3 %	23,2 %	17,4 %	39,1 %	2,8	69
Luovi-palvelujen henkilöstö	26,7 %	13,3 %	50,0 %	10,0 %	2,4	30
Henkilöstöryhmät yhteensä	22,2 %	20,2 %	27,3 %	30,3 %	**2,7**	99
Live-koulutus luentomuotoisena						
Koulutuksen henkilöstö	13,1 %	27,5 %	36,2 %	23,2 %	2,7	69
Luovi-palvelujen henkilöstö	3,3 %	46,7 %	26,7 %	23,3 %	2,7	30
Henkilöstöryhmät yhteensä	10,1 %	33,4 %	33,3 %	23,2 %	**2,7**	99

Taulukko 5. Koulutustapavaihtoehtojen valinnat henkilöstöryhmittäin.

Digiturvallisuutta koskevat väittämät

Kyselyn kuudennessa kohdassa vastaajia pyydettiin kommentoimaan neljä eri digiturvallisuusväittämää. Kukaan vastaajista ei ollut täysin eri mieltä minkään väittämän kanssa (taulukko 6). Koulutuksen henkilöstöstä 4,4 prosenttia oli jokseenkin eri mieltä siitä, että he tietäisivät, mitä seurauksia digiturvallisuuden laiminlyönnillä voi olla.

Yhteenlaskettuna 67,7 prosenttia vastaa ymmärtävänsä, mitä digiturvallisuus tarkoittaa ja 86,9 prosenttia kokee, että digiturvallisuus on osa työarkea. Digiturvan laiminlyönnin seuraukset ilmoittaa tietävänsä 75,8 prosenttia. Koulutuksen henkilöstöstä 88,2 prosenttia ja Luovi-palvelujen henkilöstöstä 96,6 prosenttia on täysin samaa mieltä siitä, että haluaa olla mukana huolehtimassa digiturvallisuudesta.

Digiturvallisuusväittämät	Samaa mieltä	Joks. samaa mieltä	Joks. eri mieltä	Eri mieltä	n
Ymmärrän, mitä digiturvallisuus tarkoittaa					
Koulutuksen henkilöstö	68,1 %	31,9 %	0,0 %	0,0 %	69
Luovi-palvelujen henkilöstö	66,7 %	33,3 %	0,0 %	0,0 %	30
Henkilöstöryhmät yhteensä	67,7 %	32,3 %	0,0 %	0,0 %	99
Koen, että digiturvallisuus on osa työarkeani					
Koulutuksen henkilöstö	85,5 %	14,5 %	0,0 %	0,0 %	69
Luovi-palvelujen henkilöstö	90,0 %	10,0 %	0,0 %	0,0 %	30
Henkilöstöryhmät yhteensä	86,9 %	13,1 %	0,0 %	0,0 %	99
Tiedän, mitä seurauksia digiturvallisuuden laiminlyönnillä voi olla					
Koulutuksen henkilöstö	73,9 %	21,7 %	4,4 %	0,0 %	69
Luovi-palvelujen henkilöstö	80,0 %	20,0 %	0,0 %	0,0 %	30
Henkilöstöryhmät yhteensä	75,8 %	21,2 %	3,0 %	0,0 %	99
Haluan olla mukana huolehtimassa digiturvallisuudesta					
Koulutuksen henkilöstö	88,2 %	11,8 %	0,0 %	0,0 %	68
Luovi-palvelujen henkilöstö	96,6 %	3,4 %	0,0 %	0,0 %	29
Henkilöstöryhmät yhteensä	90,7 %	9,3 %	0,0 %	0,0 %	97

Taulukko 6. Vastaukset digiturvallisuusväittämiin henkilöstöryhmittäin.

Avoin kysymys

Koulutustarvekyselyssä oli viimeisenä vielä avoin kysymys, jossa kartoitettiin, millainen koulutus saisi vastaajat motivoitumaan digiturvasta. Avoimeen kysymykseen vastasi kaikkiaan 49 henkilöä. Kysymyksessä annettiin valmiina ideana digiturvallisuusteemainen pakohuone. Moni vastaajista kommentoi joko pakohuoneen puolesta tai vastaan. Pakohuonetta kannattavia vastauksia oli 24 ja vastustavia neljä kappaletta. Suurin osa vastaajista kannatti pakohuonetta vahvasti: ”Digiturvallisuusteemainen pakohuone kuulostaa loistavalta! Vuorovaikutusta ja yhdessä ongelman ratkaisua.”, ”Pakohuone kuulostaa erittäin hyvälle.”, ”Pakohuone kuulostaa hauskalta idealta.”, ”Tommonen pakohuone kuulostaa aivan loistavalta.”. Toisaalta joku koki pakohuoneen erittäin huonoksi: ”Olisi kamalaa joutua pakkohauskaan pakohuoneeseen.”.

Muita ideoita tuli yhteensä 22 kappaletta. Koulutuksen toivottiin pohjautuvan arkipäivän todellisiin tilanteisiin ja olevan vuorovaikutteista ja toiminnallista. Aineiston toivottiin sisältävän konkreettisia käytännön esimerkkejä ja olevan sellaista, johon voi palata myöhemmin. Esille tuli myös halu saada materiaalia digiturvasta opiskelijoiden kanssa läpikäytäväksi. Lisäksi toivottiin ennakoivaa koulutusta erilaisista tietoturvauhkista ja tietoiskuja ajankohtaisista asioista.

Avoimissa vastauksissa nousi esille myös tarve kartoittaa omaa osaamista jonkinlaisen testin muodossa. Toive vierailevasta asiantuntijasta mainittiin kerran. Mahdollisuutta osallistua koulutuksiin työajan ulkopuolella toivottiin ja koulutuksen toivottiin lisäksi olevan sellainen, jossa nousee esiin oman toiminnan merkitys. Digiturvasta huolehtimiseen toivottiin myös resursseja, kun kyseessä ei ole henkilön ydintehtävä. Avointen vastausten mukaan enemmistö henkilöstöstä odottaa innolla koulutusta ja digiturvallisuus koetaan tärkeäksi.

7.2 Tutkimushaastattelun ja suunnittelupajojen tulokset

Tieto- ja viestintäjohtaja Susanna Kankaalle sekä IT- ja digipäällikkö Mervi Leinoselle perjantaina 16.12.2022 pidetyssä Teams-haastattelussa kävimme läpi

liitteessä 2 esitetyt kysymykset keskustellen. Kangas on johtoryhmän jäsen ja edustaa ylempää johtoa. Leinonen edustaa keskijohtoa. Haastattelussa he toimivat johdon edustajina. Haastattelu kesti 40 minuuttia ja se tallennettiin. Alla oleva yhteenveto on koottu laadullisesti haastattelun litteroinnin pohjalta.

Digiturvallisuuden määritelmä

Luovin johdon edustajien määrittelyn mukaan digiturvallisuus tarkoittaa ennen kaikkea henkilöstön toimintamalleja eli sitä, kuinka henkilöstö tekee arjessa asioita. Digiturvallisuus koostuu viidestä eri osa-alueesta, jotka eivät ole vielä kovinkaan tuttuja kokonaisuutena. Digiturvassa tulee kuitenkin huomioida kaikki osa-alueet ja viedä ne henkilöstön arkeen heidän työnsä näkökulmasta.

Digiturvallisuus osana johdon työarkea

IT- ja digipäällikön arjessa digiturvallisuus näkyy teknisistä asioista lähtien, esimerkiksi siitä, mitä laitteita ja palveluita käytetään ja miten. Kaiken taustalla ovat sopimukset ja ymmärrys siitä, mistä asioista täytyy tehdä yhteistyösopimuksia eri toimittajien kanssa. Taustalla ovat tietyt asiat, jotka on hoidettava turvallisesti. Digiturvasta huolehtiminen vaatii jatkuvaa perehtymistä ja kouluttautumista. Asioita on seurattava ja selvitettävä. Maailman tapahtumia peilataan omaan toimintaan ja tehdään tarvittavia muutoksia omaan toimintaan. Keskeistä on osaamisesta huolehtiminen. Miten osataan hoitaa IT- ja digipalvelujen tehtäväkenttää. Kuinka varmistetaan oman (digi)porukan osaaminen ja ohjataan henkilöstöä toimimaan digiturvallisesti. Riskienhallinnan näkökulma on myös jatkuvasti läsnä. Kaiken taustalla on eri tahojen kesken käytävä vuoropuhelu, jonka avulla varmistetaan yhteistyön sujuminen.

Tieto- ja viestintäjohtaja kuuluu johtoryhmään ja hänellä digiturvallisuus näkyy työarjessa myös johtoryhmään äänitorvena toimimisena. Hän pitää digiturvaa esillä ja pyrkii varmistamaan, että Luovilla on kaikin puolin riittävät resurssit digiturvan edistämiseen. Tieto- ja viestintäjohtaja pitää esillä digiturvaa muissakin ryhmissä, kuten eLuovi-tiimissä, joka kehittää digin käyttöä Luovin opetuksessa

ja ohjauksessa yhteistyössä henkilöstön kanssa. Arjessa korostuu myös rooli muiden hoksauttajana. Omaa osaamista on tarpeen jakaa.

Johdon edustajien työarjessa digiturvallisuus näkyy myös tarpeena ennakoida asioita. Digiturvallisuudesta huolehtimisen ei pidä olla vain tulipalojen sammuttamista, vaan johdon edustajat haluavat tehdä asioita mahdollisimman paljon ennakoiden. Resurssit huomioiden varaudutaan mahdollisimman hyvin.

Seuraukset digiturvallisuuden laiminlyönnistä

Haastateltavat totesivat, että digiturvassa tärkeintä on Luovin opiskelijoiden ja henkilöstön suojaaminen. Sitä kautta myös koko organisaation suojaaminen. Tieto- ja viestintäjohtaja kokee, että vakavimmat seuraukset laiminlyönnillä on, jos opiskelijoiden tiedot joutuvat vääriin käsiin. Toisaalta laiminlyönti voi myös rampauttaa Luovin koko toiminnan, jos esimerkiksi mikään järjestelmä ei toimi.

Digiturvallisuuden laiminlyönti voi pahimmillaan aiheuttaa myös merkittävän mainehaitan Luoville. Tämän hetkinen hyvä maine on helppo menettää äkkiä. Maineen rakentaminen uudelleen vaatisi merkittävää työtä.

Digiturvallisuuskoulutustarpeet

IT- ja digipäällikön mielestä tärkeintä on tiedostaa, että ei puhuta kerran tapahtuvasta koulutuksesta, vaan tarvitaan toimintamalli, jonka avulla varmistetaan, että koulutus on jatkuvaa. Tulee huomioida myös se, että henkilöstö vaihtuu, kuten myös opiskelijat, sidosryhmät ja yhteistyökumppanit. Täytyy huolehtia siitä, että kaikilla on riittävä ja ajantasainen osaaminen.

Luovissa tarvitaan lisää tietoa henkilöstölle siitä, mitä mikäkin asia tarkoittaa heidän työntekemisensä näkökulmasta. On tärkeää, että henkilöstö ymmärtää, että digiturvallisuus ei ole jotakin, jonka joku muu hoitaa, vaan jokaisen täytyy osata toimia omassa työtehtävässään oikein ja tuoda kehittämistarpeita esiin. Tieto- ja viestintäjohtaja kokee, että digiturvan tulee olla jokaisen työarkeen sisäänkirjoitettuna esimerkiksi siten, että uuden opetusohjelman käyttöönottoa

suunniteltaessa henkilöstö osaa miettiä digiturvaa. IT- ja digipäällikkö täydentää tavoitteena olevan, että: ”Digiturvasta tulee itsestään selvää kuin turvavyön laittamisesta päälle autoa ajettaessa. Kun me käynnistetään koneet tai otetaan puhelin ja avataan joku sovellus, niin me ymmärretään se, mitä me siellä voidaan tehdä ja mitä me ehkä ei voida tehdä.”. Lisäksi henkilöstön täytyy huomioida, että työtehtävissä ei ole samanlaista valtaa päättää asioista kuin vapaa-ajalla. Työpaikalla on osoitettuna tietyt raamit, joiden mukaisesti jokaisen tulee toimia.

Digiturvallisuuskoulutusten yhteydessä on tärkeää saada esihenkilöt ymmärtämään heidän tärkeä roolinsa digiturvan kehittämisessä. Esihenkilöiden on tarpeen toimia esimerkkinä ja osoittaa henkilöstölle, että digiturvallisuus on merkittävä asia, joka tulee huomioida työssä. Kun esihenkilöt ymmärtävät asian merkittävyyden, on muu henkilöstö helpompaa saada mukaan digiturvatyöhön.

Digiturvakoulutusten järjestämistavat

Johdon edustajien mielestä parhaita digiturvakoulutusten järjestämistapoja ovat työpajatyyppinen työskentely ja tapausharjoitukset, joita henkilöstö pääsee itse ratkomaan. Tieto- ja viestintäjohtaja uskoo, että ihmiset oppivat paremmin itse tekemällä kuin ainoastaan kuuntelemalla. Toki kaikki oppimistavat olisi hyvä huomioida, mutta esimerkiksi livekoulutusten järjestäminen kymmenillä eri paikkakunnilla 870 työntekijälle paikan päällä ei olisi järkevää. Koulutusmateriaalin kannattaa olla sellaista, jota voidaan hyödyntää koulutuksen jälkeen. Kun massakoulutukset on pidetty, täytyy varmistaa, että uudet työntekijät saavat myös saman tiedon. Muutoinkin digiturvan tulee olla osana perehdytystä, koska se on olennainen osa kokonaisuutta.

Ylipäänsä tarvitaan useita eri vaihtoehtoja ja tapoja oppimiseen. Digiturvaa kannattaisi pitää esillä esimerkiksi Luotsi-infoissa (esihenkilöiden säännöllinen info), joihin voidaan tuoda periaatteellisiakin asioita sekä toistaa keskeisiä asioita. Kaiken kaikkiaan olisi tärkeää, että jokaiselta tulisi selkärangasta kyky tunnistaa poikkeavia tilanteita ja ryhtyä toimimaan tilanteen edellyttämällä tavalla. Kaikilla tulisi olla tieto, mistä löytää apua. Asioita ei tule vähätellä eikä peitellä, vaan henkilöiden tulee osata toimia ja lähteä ratkaisemaan asiaa.

Ulkoiset kouluttajat

Johdon edustajat suhtautuivat ulkopuolisten kouluttajien käyttämiseen varautuneesti. Ulkopuolisen kouluttajan täytyisi tuntea erityisopetuksen maailma todella hyvin, jotta siitä olisi oikeasti hyötyä. Ulkopuolisen kouluttajan käyttöön liittyy riski, että koulutus jäisi liian yleiselle tasolle. On tärkeää, että henkilöstölle pidettävä digiturvakoulutus sisältää oikeaa tietoa Luovin todellisesta arjesta.

Digiturvallisuuskoulutuksen tavoitteet

Tärkeimmäksi digiturvakoulutuksen tavoitteeksi johdon edustajat nostavat arjen digiturvan. Tavoitteena on saada kaikki toimimaan omassa arkityössä siten, että toiminta edistää digiturvallisuutta. Tavoitteena on kouluttaa myös ne pienet, periaatteessa itsestään selvät asiat, kuten kuinka koneelle kirjaudutaan ja millaista salasanaa voi käyttää. Lisäksi täytyy neuvoa, kuinka asioita käsitellään eri välineillä ja järjestelmissä. Henkilöstön tulee myös tunnistaa henkilötiedot ja erityisten henkilötietoryhmien tiedot sekä osata käsitellä niitä. Tärkeää on myös saada kaikille uskallus käsitellä henkilötietoja ja kyky tehdä yhteistyötä.

Digiturvakoulutuksen vaikuttavuuden mittaaminen

Digiturvakoulutuksen vaikuttavuus nähdään johdon edustajien mukaan parhaiten arjen työssä. Vaikuttavuutta voi selvittää myös palautekyselyn avulla, osaamisen testauksella ja sisäisellä valvonnalla. Palautekyselyyn liittyvänä riskinä on mahdollisuus, että vastaajat arvioivat oman osaamisensa todellisuutta suuremmaksi. Sisäiseen valvontaan liittyy haaste, että se voidaan ottaa kyttäämisenä, eikä kehittämistä tukevana asiana. Sisäinen valvonta on toimintamalli, jota Luovissa ei ole vielä juurikaan tehty. Sisäistä tarkastelua voisi IT- ja digipäällikön mielestä aloittaa kriittisimmistä kohteista.

Digiturvaosaamisen ylläpitäminen

Luovissa on käytäntönä käydä joka syksy henkilöstön kanssa tietyt asiat läpi kriisiviestinnästä uudelleen. Tieto- ja viestintäjohtaja pohtii, voisiko tämä sama

malli toimia digiturva-asioissa: ”Elikkä, että tietyistä asioista vaan muistutetaan joka ikinen syksy.”. Työvuoden alkaessa käytäisiin tietyt asiat läpi koko henkilöstön kanssa eli myös olemassa olevat henkilöt saisivat tietoa asioista, eivätkä ainoastaan uudet työntekijät perehdytyksen yhteydessä. Tieto muuttuu jatkuvasti, joten on tärkeää, että koko henkilöstöllä on ajantasainen tieto.

IT- ja digipäällikkö jatkaa, että jollakin tavalla on varmistettava myös niiden henkilöiden tavoittaminen, jotka eivät osallistu vapaaehtoisiin koulutuksiin. Työvuoden alkaessa on tarpeen käydä läpi arjen työvälineisiin liittyvät asiat sekä mahdolliset muutokset, jotka on tarpeen tiedottaa kaikille. Luovissa suurin osa henkilöstöä on koulutuksen henkilöstöä eli yhteisesti läpikäytävissä asioissa kannattaa huomioida erityisesti ne asiat, jotka vaikuttavat heidän arkeensa. Olisi hyvä käydä nostamassa asioita esiin myös eri tiimeissä. Silloin voitaisiin käydä läpi juuri sen tiimin asioita. Johdon edustajien mielestä tiimikeskustelut ovat toimintamalli, jonka voisi lisätä vuosikelloon, jotta toimintaan saataisiin jatkumo.

Digiturvallisuudesta huolehtiminen

Digiturvasta huolehtimisessa tavoitellaan johdon edustajien näkemyksen mukaan tilaa, jossa henkilöstö osaa neuvoa toisiaan. Tieto- ja viestintäjohtaja edistää digiturva-asioita hallinnollisesta näkökulmasta ja IT- ja digipäällikön työlistalla on erityisesti seurannan lisääminen. Johdon edustajat näkevät, että digiturvasta huolehtiminen on koko henkilöstön yhteinen asia. Digiturvallisuudesta huolehtiminen edellyttää hyvää yhteistyötä luovilaisten kesken. Yhteistyötä toteutettiin jo asiantuntijoiden kesken pidetyissä suunnittelupajoissa.

Suunnittelupajojen tulokset

Luovin johdon edustajien ja eri asiantuntijoiden kanssa pidetyissä suunnittelupajoissa kehitettiin erityisesti Luovin henkilöstölle pidettävän digiturvakoulutuksen sisältöä ja toteuttamista. Suunnittelupajoissa esille tulleita asioita on huomioitu osittain myös laaditussa Luovin henkilöstön digiturvaosaamisen kehittämissuunnitelmassa. Suunnittelupajojen tuloksia ei ole koottu erikseen, vaan ne sisältyvät luvuissa 8.1 ja 8.2 esiteltäviin opinnäytetyön tuotoksiin.

8 Opinnäytetyön tuotokset

8.1 Hyvää tuulta purjeisiin digimerellä -kehittämissuunnitelma

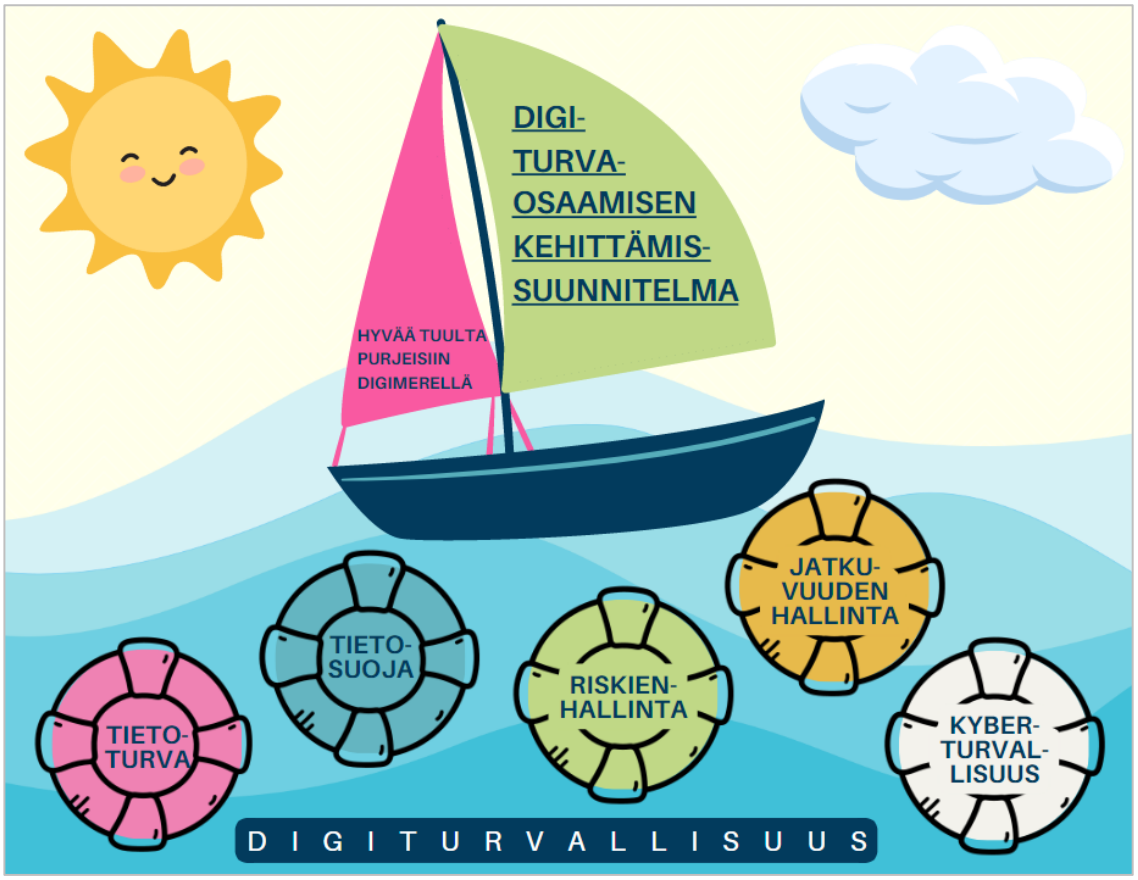
Opinnäytetyön toimeksiantona oli löytää keinoja henkilöstön digiturvaosaamisen kehittämiseen Ammattiopisto Luovin turvallisuuden parantamiseksi. Luvussa 8.1 esitellään työn tuloksena löydetyt osaamisen kehittämisen keinot ja luvussa 8.2 osaksi osaamisen kehittämissuunnitelmaa kuuluvan vuonna 2023 toteutettavan digiturvakoulutuksen runko. Luovin henkilöstön digiturvallisuusosaamisen kehittämissuunnitelma on koottu tekemällä johtopäätökset henkilöstölle toteutetun koulutustarvekyselyn ja johdon edustajille pidetyn haastattelun tuloksista. Kehittämissuunnitelmassa on hyödynnetty myös digiturvan ja osaamisen kehittämisen teoriatietoa ja verkossa jo olevaa digiturvallisuuden koulutusaineistoa. Lisäksi kehittämissuunnitelman laadinnassa on huomioitu muilta Luovin asiantuntijoilta saadut kommentit.

Luovin henkilöstön digiturvaosaamisen kehittämissuunnitelma on nimeltään ”Hyvää tuulta purjeisiin digimerellä”. Luovissa käytetään merellistä sanastoa ja strategia on nimeltään ”Hyvää tuulta purjeisiin”. Vuoden 2023 alussa digipalvelutiimissä lanseerattiin kuviossa 16 oleva slogan. Digiturvaosaamisen kehittämisen suunnitelman nimessä on huomioitu sekä strategia että digipalvelujen tiimin slogan, jotta se olisi johdolle ja henkilöstölle helposti ymmärrettävissä. Tuotos on laadittu mahdollisimman käytännönläheiseksi ja siinä on hyödynnetty myös Luovin brändivärejä. Tavoitteena on ollut saada kuivahko asia helpommaksi lähestyä. Digiturvaosaamisen kehittämissuunnitelman tavoitteena on auttaa Luovia seilaamaan digimerellä turvallisesti ja mahdollistaa menestyvä toiminta.

Kuvio 16. Luovin digipalvelutiimin slogan (Ammattiopisto Luovi 2023a).

Digiturvaosaamisen kehittämissuunnitelma on toteutettu Canva- ja ThingLink-ohjelmistoilla. Suunnitelman pohja on tehty Luovin brändivärejä hyödyntäen Canvalla, jolla tehdyt suunnittelumallit on siirretty ThingLinkiin, jossa ne on linkitetty toisiinsa. Tähän lukuun 8.1 on koottu kuvakaappaukset Canvan malleista.

Kehittämissuunnitelma ”Hyvää tuulta purjeisiin digimerellä” sisältää perusteltuja ehdotuksia toimenpiteiksi, joiden avulla henkilöstön digiturvallisuusosaamista voidaan kehittää. Suunnitelmassa esitellään toimenpiteitä uuden työntekijän perehdytyksestä lähtien aina digiturvaosaamisen ylläpitoon tarkoitettuun oppimisympäristöön asti. Kuviossa 17 on esitetty kehittämissuunnitelman kansi.



Kuvio 17. Digiturvaosaamisen kehittämissuunnitelman aloitussivu.

Kehittämissuunnitelma on tarkoitettu Luovin johtoryhmän ja esihenkilöiden työkaluksi henkilöstön digiturvaosaamisen kehittämisessä. Lisäksi Luovin asiantuntijat voivat hyödyntää suunnitelmaa. ThingLinkissä pelastusrenkaista aukeaa kunkin digiturvan osa-alueen määritelmä. Vihreässä purjeessa olevasta linkistä pääsee digiturvaosaamisen kehittämisen näkökulmat kokoavalle sivulle.

Digiturvallisuusosaamisen kehittämisen näkökulmat on valittu siten, että niihin sisältyvät asiat ovat käytännössä toteutettavissa. Näkökulmiksi on valittu perehdytys, digisivusto, työvuoden aloitustilaisuus, infotilaisuudet, kokoukset, tietoiskut, osaamisen testaaminen ja koulutukset. Digiturvaosaamisen kehittämisen näkökulmat on esitetty kuviossa 18. Kukin näkökulma on ThingLinkiin toteutetussa kokonaisuudessa linkki, josta aukeaa kyseistä näkökulmaa koskevat suunnitelmat digiturvaosaamisen kehittämiseksi.

Kuvio 18. Digiturvallisuusosaamisen kehittämisen näkökulmat.

On tärkeää, että uudet työntekijät tutustutetaan digiturvallisuuteen heti työsuhteen alkaessa. Digisivusto on erittäin keskeinen osa Luovin toimintaa, sillä se sisältää muun muassa erilaiset luovilaisille tarkoitetut digiohjeet. Työvuoden aloitustilaisuus koskee erityisesti koulutuksen henkilöstöä. Infotilaisuudet ja kokoukset ovat tilaisuuksia, joissa voidaan puhua suoraan henkilöstölle. Tietoiskuja on tarkoitus toteuttaa erilaisten sähköisten välineiden avulla. Osaamisen testaaminen ja koulutukset ovat keskeisessä roolissa digiturvaosaamisen ylläpitämisessä ja jatkokehittämisessä. Keskellä olevasta vihreästä laatikosta ”Digiturvallisuusosaamisen kehittäminen” aukeaa digiturvaosaamisen kehittämisen vuosikello.

Digiturvallisuusosaamisen kehittämisen vuosikelloon on aikataulutettu asioita työvuoden (lukuvuosi) mukaisessa järjestyksessä (kuvio 19). Vuosikello on jätetty riittävän yleiselle tasolle, jotta se mahdollistaa toiminnan suunnittelun ja asioiden toteuttamisen kulloinkin ajankohtaisten tarpeiden mukaisesti.

Kuvio 19. Digiturvallisuusosaamisen kehittämisen vuosikello.

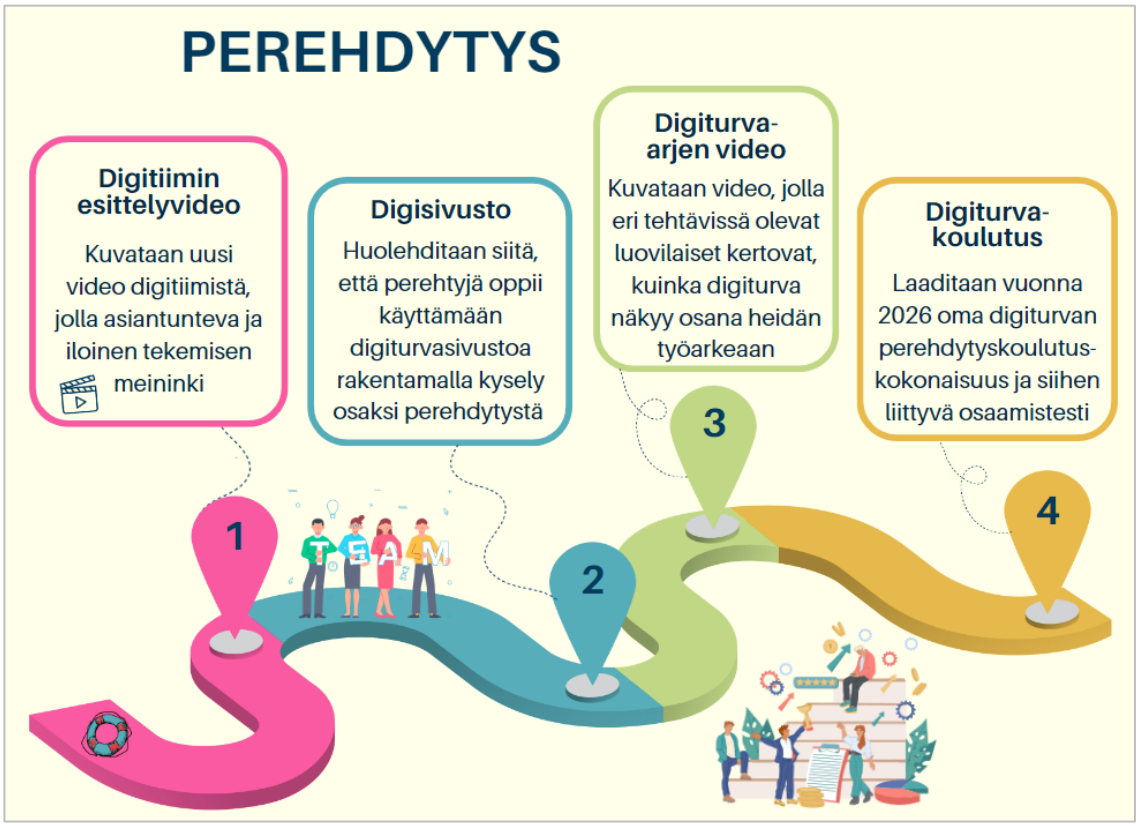
Digiturvallisuusosaamisen vuosikello sisältää sekä formaaleja että epäformaaleja osaamisen kehittämisen menetelmiä sekä yksilö- että työyhteisötasolla. Osaamisen kehittämistä on tarpeen edistää mahdollisimman monella tavalla, joten Luovin vuosikello sisältää monipuolisesti erilaisia tapoja. Keskeistä on Luovissa olevan digiturvallisuusosaamisen jakaminen.

Elokuussa on työvuoden aloitustilaisuus ja henkilöstön digiturvaohjeita sisältävän digisivuston päivitys. Digisivuston päivitystä tehdään tarpeen mukaan jatkuvasti, mutta vuosikellon mukaisina kuukausina digisivustoa on tarkoitus tarkastella laajemmin. Tietoiskujakin tehdään tarpeen mukaan, mutta vuosikelloon liitettynä varmistetaan, että henkilöstölle muistetaan pitää digiturva-asioita esillä myös yksinkertaisemmilla toteutuskeinoilla. Vuosikelloon on aikataulutettu kaksi Luotsi- ja Luovi-infoa eli esihenkilöiden ja koko henkilöstön infot, jotta digiturvan asiat saavat riittävän huomion. Työpaikkakokoukset ovat eri paikkakuntien yhteisiä kokouksia, joihin on ajatuksena osallistua vuosikellon mukaisina kuukausina työpaikkakokousta vaihdellen.

Johtoryhmän kanssa käytävä keskustelu on aikataulutettu syyskuulle, jotta tarvittavat digiturva-asiat voidaan huomioida budjetissa. Vuosittainen Digiturva-viikko sisältää runsaasti Digi- ja väestötietoviraston tuottamaa digiturvatietoutta ja se kannattaa huomioida myös osana Luovin toimintaa. Henkilöstölle kannattaa vähintään vinkata digiturvaviikon parhaista anneista, koska niidenkin avulla henkilöstö voi kehittää osaamistaan. Osaamista on tavoitteena testata vuosittain lokakuussa vaihtelevilla keinoilla.

Tiimikokoukset ovat aikavarauksia, jolloin voidaan tarpeen mukaan käydä digiturva-asioita läpi Luovin eri tiimeissä, kuten henkilöstöpalvelujen tiimissä tai haku- ja neuvontapalvelujen tiimissä. Ajatuksena on, että toisissa tiimeissä voidaan käydä useammin kuin toisissa, koska esimerkiksi henkilötietojen käsittelystä tarvittavan ohjeistuksen määrä vaihtelee tiimeittäin. Olennaista vuosikellossa on jatkuvuus ja myös heinäkuussa huolehditaan digiturvasta, vaikka siellä aurinko onkin. Digiturva on läsnä Luovin toiminnassa jatkuvasti ja siitä huolehtimiseksi on tarpeen toimia yhdessä. Yhteistyöllä on mahdollista kehittää työkäytäntöjä ja huolehtia turvallisuudesta.

Perehdytyksen kehittämisen pidemmän aikavälin suunnitelma on esitetty kuviossa 20. Tavoitteena on myöhemmin saada luotua kokonaan Luovin oma digiturvan koulutuskokonaisuus uusille työntekijöille. Tällä hetkellä Luovin työntekijät tekevät osana Luovin uusien työntekijöiden perehdyttämisen kokonaisuutta yleisen tason tietoa sisältävän Tietosuojan ABC-koulutuksen, joka on vapaasti saatavissa eOppivasta. Teoriatiedon mukaan tehokkaampi koulutus olisi juuri oman organisaation tietoa sisältävä koulutus.



Kuvio 20. Suunnitelma uusien työntekijöiden perehdytyksen kehittämisestä.

Ensimmäisenä toimenpiteenä perehdytyksen kehittämiseksi on uuden esittelyvideon laatiminen digipalvelutiimistä. Videolla osoitetaan, että digipalvelutiimiläisiä on helppo lähestyä. Digiturva on kuitenkin koko organisaation yhteinen asia, joten myöhemmin on perusteltua kuvata video, jossa eri alojen työntekijät tuovat esiin digiturva-asioita oman työnsä näkökulmasta. Tällöin uusi luovilainen näkee konkreettisesti, että digiturva-asiat kuuluvat kaikkien luovilaisten eli myös hänen työarkeensa. Jatkuvana perehdytysaineiston kehittämistoimena on digisivuston linkitys uusien työntekijöiden perehdytyskokonaisuuteen. On tärkeää, että uusi luovilainen saa heti käsityksen siitä, mitä tietoja digisivustolta löytyy.

Luovissa henkilöstön ohjeet löytyvät Satamasta eli intrasta. Tällä hetkellä Satamasta löytyy Digisivusto, jolla on digiturvallisuusosio (kuvio 4 sivulla 18). Tarkoituksena on päivittää digiturvallisuusosiota siten, että sinne lisätään nykyistä enemmän tietoa digiturvasta sekä erityisesti lisää käytännön ohjeita henkilöstön työarjen tueksi. Kuviossa 21 on esitetty suunnitelma uuden digiturvasivuston pääotsikoista.

Kuvio 21. Suunnitelma uuden digisivuston pääotsikoista.

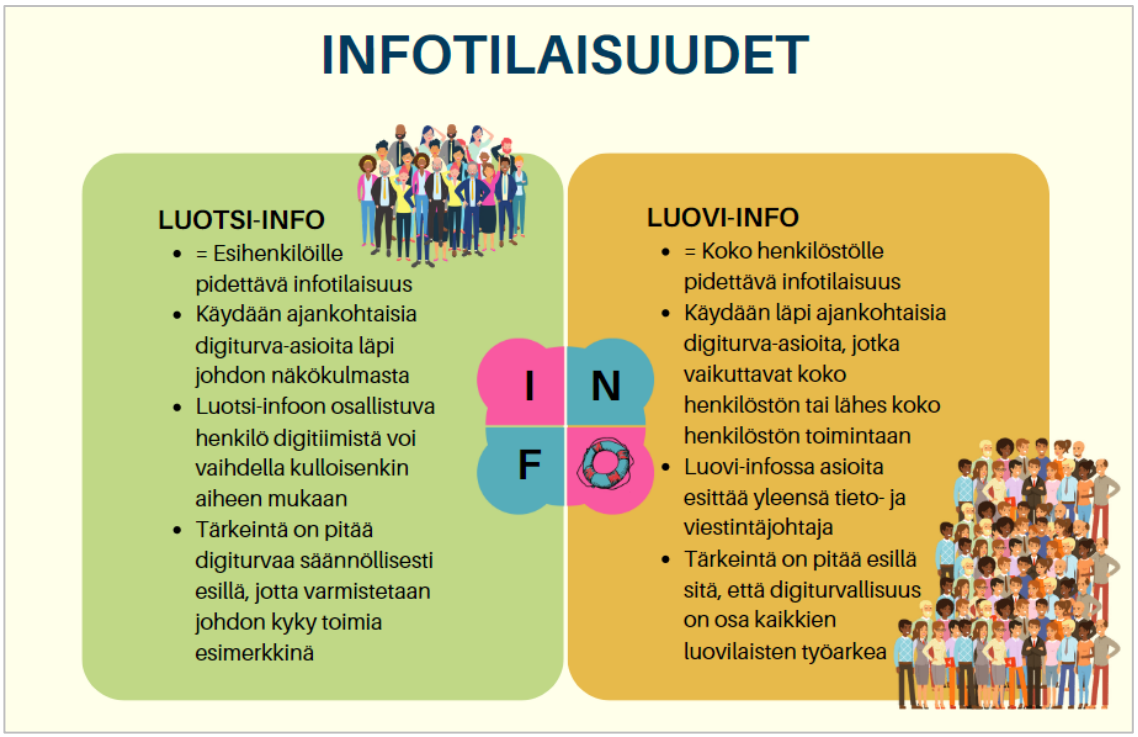
Ajatuksena on, että uudistettu digiturvasivusto sisältää digiturvallisuuden eri osa-alueet, jotta henkilöstö hahmottaa paremmin digiturvakokonaisuuden. Myöhemmin digisivustoa tulee kehittää siten, että digiturvallisuutta ei jaeta erillisiin osa-alueisiin. Ohjeet kannattaa antaa kokonaisuutena, jossa ei ole tarpeen erotella, minkä teeman alle mikäkin asia tai ohjeistus kuuluu. Kuvio 21 sisältää päivityksen ensimmäisen vaiheen suunnitellut pääotsikot. Alaotsikot on jätetty pois opinnäytetyöstä, koska ne sisältävät sellaista tietoa, joka on tarpeen jättää ainoastaan opinnäytetyön toimeksiantajan eli Ammattiopisto Luovin tietoon.

Työvuoden aloitustilaisuus on Luovissa joka syksy järjestettävä tilaisuus lukuvuoden alkaessa. Tilaisuus sisältää paljon asiaa, joten todennäköisesti tilaisuudessa ennättää esittää ainoastaan muutaman ydinasian digiturvasta. Oleellisinta työvuoden aloitustilaisuudessa on esitellä koontisivu, joka rakennetaan Satamaan. Ajatuksena on helpottaa työvuoden aloitusta siten, että Satamasta löytyy yhdeltä sivulta mahdollisimman helposti kaikki lukuvuoden alkaessa todennäköisesti tarvittavat asiat (kuvio 22).

Kuvio 22. Idea työvuoden aloitustilaisuudessa läpikäytävistä asioista.

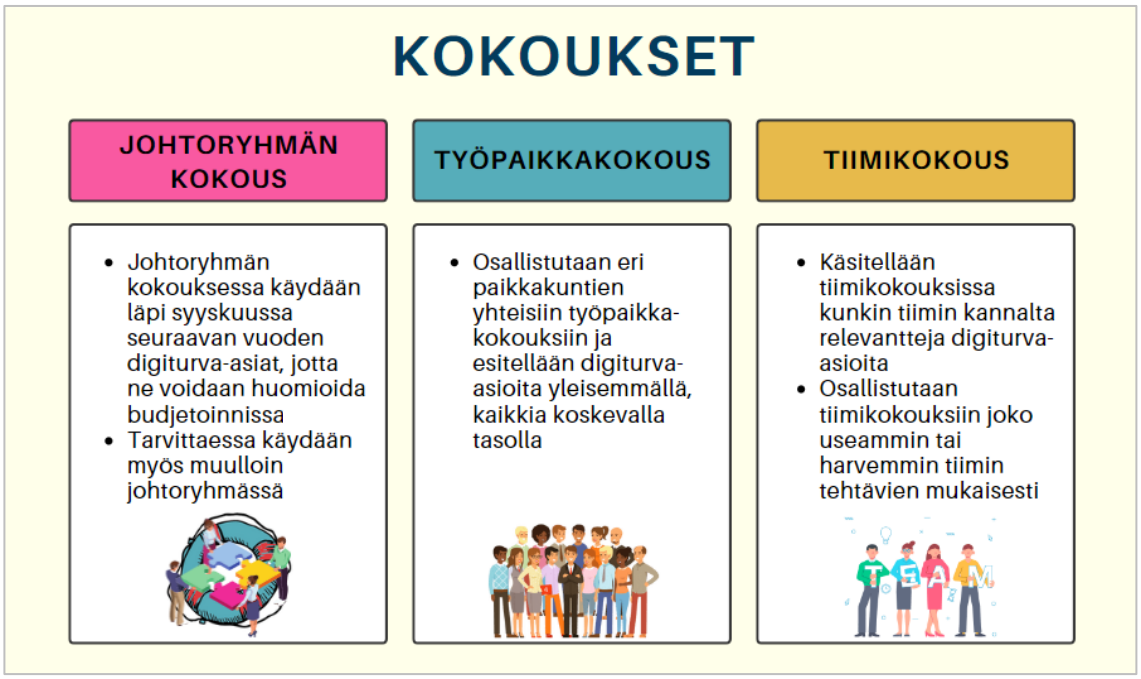
Kuviossa 22 on esitetty asiat, jotka digisivuston koontisivulle kannattaa nostaa. Tarkoituksena on rakentaa koontisivu siten, että se sisältää olennaisimpien asioiden ydintiedot ja linkit digiturvasivustolle kyseisten asioiden varsinaisille sivuille. Kokemuksen mukaisesti työvuoden alkaessa kysymyksiä tulee erityisesti kirjautumiseen liittyen. Henkilöstöä kannattaa myös muistuttaa heidän velvollisuudestaan ilmoittaa havaitsemistaan tietoturvapoikkeamista. Työvuoden aloitustilaisuus on hyvä mahdollisuus puhua suoraan henkilöstölle, kuten myös infotilaisuudet.

Luovissa järjestetään säännöllisesti infotilaisuuksia sekä esihenkilöille että koko henkilöstölle eli kaikille luovilaisille. Vuosikelloon on aikataulutettu säännölliset varaukset molemmille infoille. Johdon edustajat toivat haastattelussaan esille, että digiturvaa kannattaisi pitää esillä esimerkiksi Luotsi-infoissa, joihin voidaan tuoda myös periaatteellisia asioita käsiteltäväksi. Ajatuksena on, että digiturva-asioita pidetään säännöllisesti esillä, jolloin digiturva saa tarvittavaa huomiota. Infoissa voidaan käydä läpi kulloinkin ajankohtaisia asioita tai jos mitään erityisen ajankohtaista ei juuri silloin ole, voidaan käydä läpi teoriaa digiturvallisuudesta (kuvio 23).



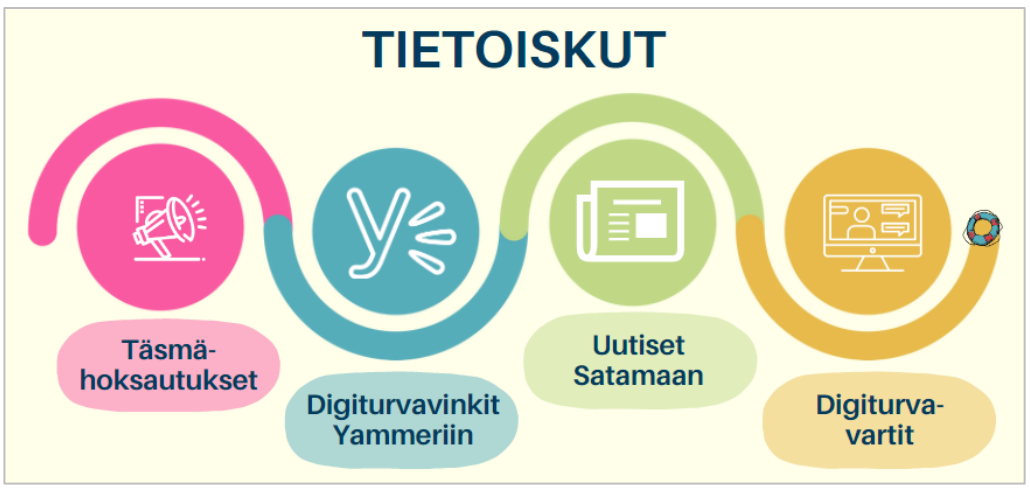
Kuvio 23. Infotilaisuuksien järjestämiseen liittyvät huomiot.

Luotsi-infoon digipalvelutiimistä osallistuvaa asiantuntijaa kannattaisi vaihdella, jotta esihenkilöt tutustuisivat paremmin koko tiimiin. Riippuen käsiteltävästä aiheesta Luotsi-infoon voisi osallistua esimerkiksi järjestelmäsuunnittelija tai hankinta-asiantuntija. Koko henkilöstölle pidettävässä Luovi-infossa digiasioista on usein puhunut tieto- ja viestintäjohtaja. Asiat saavat enemmän painoarvoa, kun niitä esittelee johtotason henkilö. Luovissa pidettävissä erilaisissa kokouksissa asioista voisivat käydä kertomassa suoraan digipalvelutiimin asiantuntijat kulloinkin käsiteltävän asian mukaisesti (kuvio 24).



Kuvio 24. Suunnitelma eri kokouksiin osallistumisesta.

Luovin eri tiimit käsittelevät eri verran esimerkiksi henkilötietoja. Siksi on perusteltua, että yhteistyö on tiiviimpää toisten tiimien kanssa. Digiturvaa on kuitenkin pidettävä säännöllisesti esillä koko henkilöstölle. Sitä voi toteuttaa arjessa ajankohtaisista asioista tehtävien tietoiskujen avulla. Niitä voi toteuttaa erilaisia sähköisiä kanavia pitkin (kuvio 25). Luovissa hoksautetaan henkilöstöä Digi- ja väestötietoviraston kuukausittain julkaisemista kaikille avoimista digiturvavarteista. Satamaan (intra) julkaistaan uutisia säännöllisesti digiturvan esillä pitämiseksi. Yammeria käytetään erityisesti liikkeellä olevista huijauksista tiedottamiseen ja lisäksi voidaan lähettää esimerkiksi kohdennettuja Teams-viestejä.



Kuvio 25. Erilaisia tietoiskuja.

Digiturvallisuusosaamisen kehittämisessä keskeistä on myös osaamisen testaaminen (kuvio 26). On tärkeää selvittää, millä tasolla henkilöstön osaaminen on, jotta digiturvasta voidaan ohjeistaa niiltä osin kuin osaamisessa on vielä vajetta. Tärkeä keino organisaation osaamisen tason selvittämiseksi ovat erilaiset harjoitukset. Erityisesti Digi- ja väestötietoviraston vuosittain järjestämä Taisto-harjoitus on hyvä tapa selvittää organisaation tilannetta.

Kuvio 26. Keinoja digiturvaosaamisen varmistamiseen erilaisilla osaamisen testaamisen keinoilla.

Osaamisen testaamiseen on tarkoitus liittää myös sisäistä valvontaa. Ajatuksena on, että sisäisen auditoinnin avulla saadaan lisätietoa osaamisen tasosta. Valvonnan tulosten mukaan voidaan kehittää esimerkiksi digisivustoa, jos valvonnassa selviää, että jostakin asiasta tarvitaan lisäohjeistusta. Johdon haastattelussa tuli ilmi, että sisäistä valvontaa voisi käynnistää kriittisimmistä kohteista. Valvontaa käynnistettäessä siitä on hyvä tiedottaa etukäteen, mutta myöhemmin todellisen tilannekuvan selvittämiseksi kannattaa hyödyntää myös yllätysvalvontaa. Henkilöstö on hyvä saada ymmärtämään, että valvontaa ei tehdä kenenkään syyllistämiseksi, vaan kaikkien turvallisuuden parantamiseksi.

Koulutukset ovat merkittävä asia osaamisen kehittämisessä. Kuviossa 27 on esitetty viisivuotissuunnitelma digiturvakoulutuksista. Tavoitteena on luoda Luoville oma oppimisympäristö digiturva-asioita varten ja sinne digitaalinen pakohuone, joka sai vahvan kannatuksen koulutustarvekyselyssä. Vuodelle 2026 on aikataulutettu Luovin oman digiturvan perehdytyskoulutuksen ja siihen liittyvän testin laadinta. Tavoitteena on luoda perehdytyskoulutus juuri Luovin työntekijöitä varten, jotta he saavat heti työsuhteen alkaessa konkreettista tietoa Luovin käytännöistä työarkeensa.

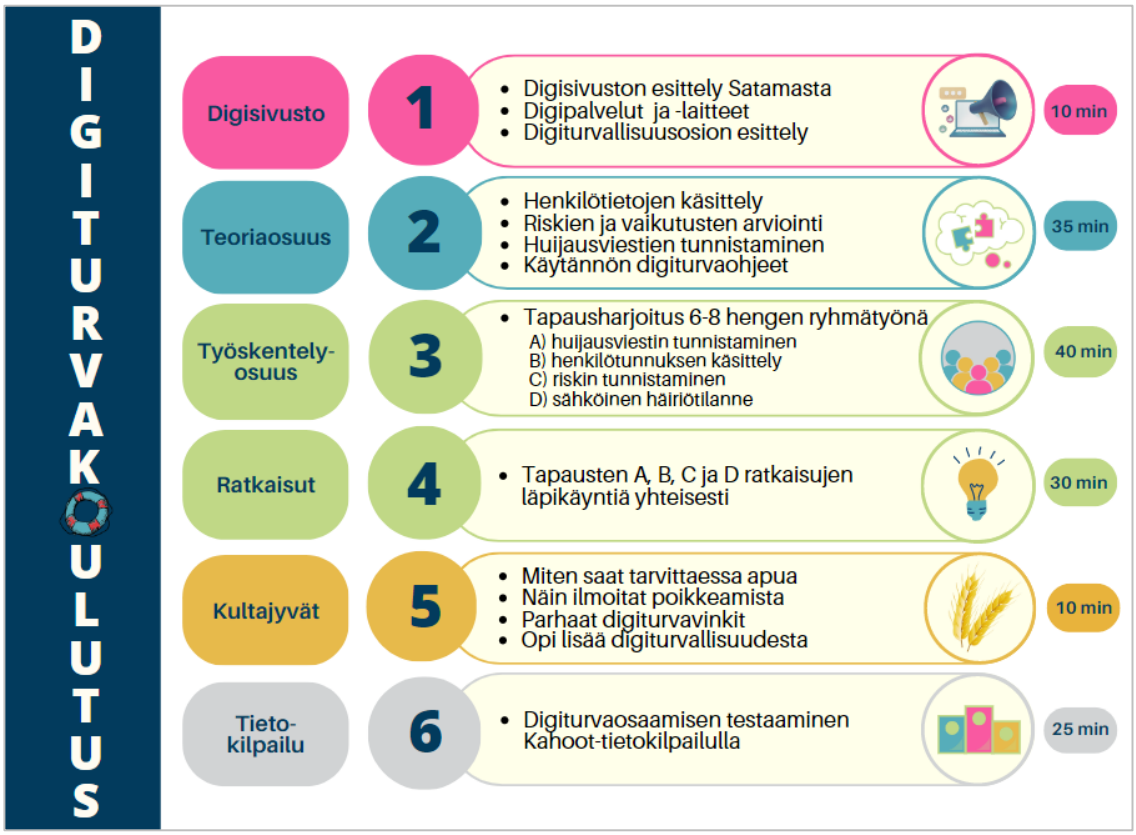
Kuvio 27. Digiturvakoulutusten kehittämisen viisivuotissuunnitelma.

Johtoryhmän päätöksen mukaisesti vuonna 2023 digiturvaosaamisen kehittämiseksi järjestetään koko henkilöstölle velvoittava digiturvakoulutus, jonka runko on esitelty luvussa 8.2. Tavoitteena on, että vastaavanlainen digiturvakoulutus voitaisiin järjestää uudelleen koko henkilöstöä velvoittavana vuonna 2027. Tavoitteena on varmistaa, että aivan koko henkilöstön digiturvaosaamista pidetään yllä, eikä osaamisen taso riipu ainoastaan työntekijän omasta motivaatiosta hyödyntää tarjolla olevaa digiturvallisuustietoa. Digiturvaosaamisen kehittäminen on parhaimmillaan organisaation kilpailuetu, joten digiturvakoulutusten jatkumo kannattaa turvata.

8.2 Digipurjeet-koulutus

Osaksi Luovin henkilöstön digiturvaosaamisen kehittämissuunnitelmaa on luotu sisäinen koulutus. Opinnäytetyöprosessin käynnistyessä oli tiedossa, että Luovissa halutaan järjestää digiturvakoulutusta henkilöstölle. Koulutuksen runko on rakennettu tekemällä johtopäätökset henkilöstön koulutustarvekyselyn ja johdon edustajille pidetyn haastattelun tuloksista. Koulutuksen sisällössä on huomioitu myös suunnittelupajojen tulokset sekä digiturvan ja osaamisen kehittämisen teoriatietoa ja olemassa olevia digiturvakoulutusaineistoja. Koulutuksen tavoitteena on henkilöstön digiturvallisuustietoisuuden lisääminen siten, että henkilöstö ymmärtää, mitä digiturva tarkoittaa ja kuinka he voivat huolehtia siitä.

Kuviossa 28 on esitetty vuonna 2023 toteutettavan Digipurjeet-koulutuksen eli digiturvakoulutuksen runko. Koulutus kestää 2,5 tuntia ja on tarkoitettu järjestettäväksi Teams-kokouksina neljän digipalvelujen työntekijän vetämänä. Koulutukset on tarkoitus järjestää lähekkäisten paikkakuntien henkilöstöille yhteisenä siten, että kuhunkin koulutukseen osallistuu noin sata työntekijää.



Kuvio 28. Digipurjeet-koulutuksen runko.

Digipurjeet-koulutus järjestetään organisaation sisäisenä koulutuksena, koska sisäinen koulutus mahdollistaa Luovin erityispiirteiden huomioimisen. Johdon edustajille pidetyssä haastattelussa tuli esiin, että johto toivoo sisäistä koulutusta, koska ulkopuolisen kouluttajan pitämä koulutus ei välttämättä huomioi kaikkia Luovin toiminnan erityispiirteitä. Sisäisenä koulutuksena Digiturvakoulutusta on mahdollista järjestää juuri henkilöstölle sopivana ajankohtana ja sen avulla saadaan myös kehitettyä samalla Luovin sisäistä yhteistyötä. Teoriatiedon mukaan hyvä tiedonjakamisen keino on hyödyntää koulutuksissa organisaation omia asiantuntijoita.

Digiturvallisuuskoulutuksen on tärkeää sisältää juuri Luovin arjessa eteen tulevia asioita. Konkreettiset arjen esimerkit auttavat ymmärtämään, mitä digiturvallisuudesta huolehtiminen on käytännössä ja ne lisäävät ymmärrystä digiturvan tärkeydestä. Konkreettisilla esimerkeillä henkilöstö on helppo saada ymmärtämään, että digiturvallisuus todella on osa myös heidän työtehtäviään. Kun henkilöstö ymmärtää digiturvallisuuden olevan osa myös heidän työarkeaan, oppivat he huolehtimaan paremmin digiturvallisuudesta ja siitä tulee heidän työssään tavallinen asia, josta he myös haluavat huolehtia.

Koulutuksen aluksi on tarkoitus esitellä Satamasta (Luovin intra) löytyvä digisivusto ja erityisesti sen digiturvallisuusosio. Tavoitteena on osoittaa henkilöstölle, että heidän tulee ja kannattaa hyödyntää digisivustoa työssään, koska se sisältää muun muassa käytännön ohjeita työarjen tueksi. Henkilöstön teoreettisen osaamisen lisäämiseksi koulutus sisältää teoriaa, joka on rakennettu henkilöstön koulutustarvekyselyn tulosten sekä digiturvan teoriatiedon pohjalta.

Luovin henkilöstö kaipaa koulutustarvekyselyn tulosten mukaan koulutusta henkilötietojen käsittelystä. Henkilötietojen käsittelyn osuus sisältää tietoa henkilötietojen käsittelystä yleisesti, käsittelystä informoinnista, erityisistä henkilötietoryhmistä ja tietosuojaperiaatteista. Riskien ja vaikutusten arviointi sekä huijausviestien tunnistaminen olivat suosituimmat koulutusaiheet, joten ne käydään myös läpi. Myös digiturvallisuusteoriassa tuli esiin, että käyttäjiä on tarpeen kouluttaa tunnistamaan huijauksia. Koulutuksen teoriaosuudessa on lisäksi muutamia käytännön digiturvaohjeita koskien muun muassa turvatulostusta ja

etätyötä. Teoriaosuus sisältää Digi- ja väestötietoviraston julkaisemista ”Digiturma vai digiturva”-videoista kolme, jotta osallistujat saataisiin pysymään mukana teoriaosuudessa paremmin, kun koulutus on elävämpi. Lisäksi teoriaosuudessa hyödynnetään Teamsin tarjoamia osallistavia menetelmiä. Osallistujia pyydetään esimerkiksi reagoimaan Teamsin reaktioista ylöspäin nostetulla peukalolla, jos he ovat saaneet joskus huijausviestin.

Koulutuksen ydinsisältöä ovat todellisiin tapahtumiin perustuvat tapausharjoitukset, joita koulutukseen osallistuvat pääsevät ratkomaan noin 6-8 hengen ryhmissä Teams-ryhmätyötiloissa. Tapausharjoituksia ratkovat ryhmät sekä ryhmille tulevat tapausharjoitukset tehdään satunnaisesti ryhmätoiminnon avulla. Yhtä tapausharjoitusta ratkoo aina useampi eri ryhmä, koska tapausharjoituksia on luotu alkuun neljä erilaista. Ne pohjautuvat todellisiin joko Luovissa tai muualla sattuneisiin tilanteisiin. Liitteessä 3 on esimerkki tapausharjoituksesta ”Huijausviestin tunnistaminen”.

Koulutuksessa on varattu eniten aikaa tapausharjoituksille. Tavoitteena on, että jokaista tapausharjoitusta käydään myös yhteisesti läpi. Läpikäynti aloitetaan tapausharjoituksesta A, johon tekemänsä ratkaisun jokin ryhmistä voi esitellä. Kouluttajat kommentoivat ryhmän ratkaisun ja esittelevät tapausharjoituksen malliratkaisun. Sen jälkeen käydään läpi vastaavalla tavalla tapausharjoitukset B, C ja D. Tavoitteena on, että kaikki neljä tapausharjoitusta jäävät osallistujille jollakin tasolla mieleen, vaikka he itse eivät olekaan ratkoneet kuin yhtä.

Käytännön osuuden jälkeen on tarkoitus esitellä vielä niin sanotut kultajyvät eli ne asiat, jotka jokaisen erityisesti tulisi muistaa vielä koulutuksen jälkeenkin. Osallistujille esitellään koonti parhaista digiturvavinkeistä heidän työarkeensa. Lisäksi henkilöstölle kerrotaan, kuinka he saavat digiasioissa tarvittaessa apua ja muistutetaan heitä tietoturvapoikkeamista ilmoittamisesta. Lisäksi vinkataan kohteita, joista voi oppia lisää digiturvallisuudesta.

Koulutuksen lopuksi osallistujille pidetään Kahoot-tietokilpailu, jossa testataan heidän osaamistaan. Tavoitteena on nähdä, millä tasolla digiturvaosaaminen on ja motivoida henkilöstöä keskittymään läpi koulutuksen, sillä parhaat osallistujat

palkitaan. Koulutuksen lopussa olevasta tietokilpailusta kerrotaan heti alussa henkilöstölle, jotta he tietävät olla tarkkana koulutuksen aikana ja valmistautua osoittamaan osaamisensa. Tietokilpailun edetessä kouluttaja kommentoi kysymysten oikean vastauksen ennen seuraavaa kysymystä. Tietokilpailun tuloksia voidaan hyödyntää esimerkiksi digisivuston kehittämisessä, kun nähdään, millä tasolla henkilöstön tietämys on. Liitteessä 4 on esimerkki digiturva-aiheisesta tietokilpailusta. Lukuun ottamatta liitteissä 3 ja 4 olevia esimerkkejä, digiturva-koulutuksen sisältö on jätetty pois opinnäytetyöstä, koska Digipurjeet-koulutus sisältää aineistoa, joka on tarkoitettu ainoastaan Luovin henkilöstölle.

Digipurjeet-koulutukset tulee toteuttaa henkilöstölle sopivasti aikataulutettuna. Suurin osa Luovin henkilöstöstä on koulutuksen henkilöstöä, joten toteutus kannattaa suunnitella osana työvuoden suunnittelua. Valmiiksi suunnitellut koulutukset on helppo toteuttaa. Teams-koulutus mahdollistaa osallistumisen myös johonkin toiseen koulutuksen, jos osallistuja ei pysty osallistumaan varsinaisena hänelle tarkoitettuna koulutuspäivänä.

Digipurjeet-koulutusten jälkeen henkilöstön tulisi mieltää digiturvan olevan osa heidän työarkeaan. Koulutuksesta kerätään osallistujilta palaute, joka sisältää myös koulutustarvekyselyssä olleet väittämät. Tavoitteena on, että aiempaa suurempi prosenttiosuus vastaajista kokee ymmärtävänsä, mitä digiturva tarkoittaa ja tietää, mitä seurauksia digiturvallisuuden laiminlyönnillä voi olla. Toivottavasti luovilaiset haluavat olla vahvasti mukana huolehtimassa digiturvallisuudesta ja kokevat, että digiturvallisuus on osa heidän työarkeaan. Digipurjeet-koulutuksen runko esiteltiin henkilöstölle 24.4.2023 pidetyssä Luovi-infossa ja ensimmäiset pilottikoulutukset ovat toukokuussa 2023.

Digiturvaosaamisen kehittämisen onnistumisessa on erittäin tärkeää johdon tuki asialle. Koulutuksen valmistelu ja järjestäminen vaativat aikaa ja resursseja. Panostukset ovat nähdäkseni erittäin kannattavia. On tärkeää ymmärtää, että tieto on arvokkainta, mitä Luovissa on. Tiedosta huolehtimisen tulisi kiinnostaa jokaista luovilaista ja kaikilla tulisi olla halu olla mukana niin sanotusti nostamassa purjeita. Digipurjeet-koulutuksen tavoitteena on kuvainnollisesti mahdollistaa Luovin purjeveneen pääsy liikkeelle ja kyky seilata turvallisesti digimerellä.

9 Yhteenveto digiturvallisuusosaamisen kehittämisestä

9.1 Digiturvallisuus osana työelämää

Digiturva on aiheena sellainen, että se mielletään usein kuuluvaksi vain IT-alan henkilöstölle. Nykyisessä muuttuvassa digitaalisessa yhteiskunnassa digiturvallisuustaidot ovat kuitenkin tarpeellisia myös muulle henkilöstölle. Jalava ym. (2021) toteavat, että työn sisällön muuttuminen vaatii myös osaamisen kehittämistä (Limnéll ym. 2022, 92). Digitaalisuus koskettaa kaikkia organisaatioita ja niiden on huolehdittava henkilöstönsä digiturvaosaamisesta (Hagert & Toivanen 2022, 230–231).

Tutkimuksissa on arvioitu, että yli 80 prosenttia erilaisista tietosuojaan ja tietoturvaan liittyvistä poikkeamista aiheutuu henkilöiden tahattoman, inhimillisen toiminnan takia (Kirves ym. 2022). Digitaalinen turvallisuus voikin olla vahva kilpailuetu tai merkittävä digitalisaation hidastaja ja epävarmuutta aiheuttava asia (Andreasson & Ylipartanen 2022, 54). Hyödyntääkseen digitalisaatiota kilpailuetuna, organisaatioiden on toteutettava rakenteellisia muutoksia (Vial 2019, 120). Digitalisaation hyödyntäminen edellyttää myös organisaation henkilöstöltä kykyä toimia digiturvallisesti. Digiturvasta huolehtiminen kuuluu kaikille ja se on jatkuvaa työtä. Siksi sen tulisikin olla luonteva osa koko henkilöstön työarkea.

Tämän tutkimuksellisena kehittämistyönä toteutetun opinnäytetyön tarkoituksena oli Ammattiopisto Luovin henkilöstön digiturvallisuusosaamisen syventäminen siten, että digiturvallisuudesta huolehtimisesta tulee luonteva osa heidän työarkeaan. Opinnäytetyön tavoitteena oli luoda digiturvakoulutuksen sisältävä henkilöstön digiturvaosaamisen kehittämissuunnitelma, jonka toteuttamisella henkilöstön digiturvaosaamista voidaan kehittää ja ylläpitää. Opinnäytetyölle määriteltiin seuraavat tutkimuskysymykset:

1. Mitkä ovat Luovin henkilöstön digiturvallisuuskoulutustarpeet?
2. Mitkä ovat johdon edustajien näkemykset digiturvallisuudesta?
3. Miten digiturvallisuuskoulutus kannattaa toteuttaa henkilöstölle?
4. Miten henkilöstön digiturvallisuusosaamista voidaan kehittää ja ylläpitää?

Kokonaisuutena opinnäytetyössä onnistuttiin löytämään vastaukset tutkimuskysymyksiin. Henkilöstön digiturvallisuuskoulutustarpeet kartoitettiin henkilöstölle toteutetulla kyselyllä ja johdon edustajien näkemyksiä digiturvallisuudesta selvitettiin haastattelulla. Digiturvallisuuskoulutuksen runkoa ja toteuttamistapaa suunniteltiin yhteistyössä johdon edustajien ja Luovin asiantuntijoiden kanssa. Digiturvakoulutuksen sisältävä henkilöstön digiturvallisuusosaamisen kehittämissuunnitelma sisältää kattavasti erilaisia toimenpiteitä, joiden avulla henkilöstön digiturvaosaamista voidaan kehittää ja ylläpitää. Osaamisen kehittämissuunnitelma laadittiin teoriatiedon ja opinnäytetyössä kerätyn aineiston ja niistä tehtyjen johtopäätösten pohjalta.

Koulutustarpeiden kartoitus digiturvallisuudesta -kysely antoi hyvin tietoa suunnittelun pohjaksi. Kyselyn vastausprosentti 11,5 on pieni, mutta lukumäärällisesti 100 vastausta on hyvä määrä. Kyselyyn vastasi tukipalvelujen henkilöstöstä noin 34,5 ja koulutuksen henkilöstöstä noin 8,9 prosenttia eli yhteenlasketuissa tuloksissa tukipalvelujen henkilöstön vastaukset korostuvat suhteessa koulutuksen henkilöstöön. Koulutuksen henkilöstöstä kyselyyn vastasi 70 ja tukipalvelujen henkilöstöstä 30 henkilöä eli lukumäärällisesti koulutuksen henkilöstön vastauksia on enemmän. Uskon, että kyselyyn tuli suhteessa enemmän vastauksia tukipalvelujen henkilöstöltä kuin koulutuksen henkilöstöltä, koska digiturvallisuus aiheena lienee tutumpi ja tukipalvelujen henkilöstön työarki mahdollistaa paremmin erilaisiin kyselyihin vastaamisen.

Johdon edustajat toivat haastattelussaan mielestäni erittäin hyvin esiin sen, kuinka tärkeää on ymmärtää, että digiturva ei ole jotakin, minkä joku muu hoitaa, vaan se kuuluu kaikille. Johdon edustajilla oli mielestäni realistinen käsitys myös digiturvakoulutusten järjestämistavoista. Tarvitaan monipuolinen koulutus sekä sellaista koulutusmateriaalia, jota voidaan hyödyntää myös koulutuksen jälkeen. Myös koulutustarvekyselyn tulokset osoittivat tarpeen monipuolisuudelle. Ihmisten erilaisuus oppijoina ilmeni koulutustarvekyselyn vastauksissa.

Esimerkiksi kyselyn avoimessa kysymyksessä näkyi selkeästi, että osa vastaajista olisi aivan innoissaan digiturvallisuusaiheisesta pakohuoneesta, kun taas osalle se olisi aivan kauhistus. Avoimeen kysymykseen ei olisi välttämättä

kannattanut laittaa esimerkkiä pakohuoneesta, koska moni vastaaja otti kantaa pakohuoneen puolesta tai vastaan. Pakohuonetta kannatti 24 ja vastusti neljä vastaajaa. Toisaalta tämäkin kysymys osoittaa hyvin sen, että digiturvallisuustietoisuutta on tarpeellista lisätä useammalla eri tavalla, jotta jokainen voisi oppia itselleen parhaiten sopivalla tavalla. Avoimista vastauksista tuli hyviä ideoita Digipurjeet-koulutukseen. Esimerkiksi toiveet siitä, että koulutus pohjautuisi arkipäivän todellisiin tilanteisiin ja olisi toiminnallista. Vastauksista oli hienoa havaita, kuinka paljon henkilöstö odottaa digiturvakoulutusta.

Ihmiset ovat organisaation tärkein pääoma (Nieto 2014, 163). Kehittyvä organisaatio huolehtii oppimisesta, sillä ilman oppimista työyhteisö voi jämähtää paikalleen eikä kykene toimimaan parhaalla mahdollisella tavalla jatkuvasti muuttuvassa maailmassa (Koskinen 2020, 17, 24). Valveutunut organisaatio huolehtii henkilöstönsä digiturvaosaamisesta ja sen kehittämisestä. Kehittämisessä voi hyödyntää vapaasti saatavilla olevaa koulutusmateriaalia, mutta lisäksi tarvitaan aina myös organisaation omaa materiaalia. (Kirves ym. 2022.) Digiturvaosaamista ei voida lisätä vain yhdellä tavalla tai koulutuksella, vaan tarvitaan säännöllistä ja jatkuvaa osaamisen kehittämistä eri tavoin.

Myös johdon edustajille toteutetussa haastattelussa nousi esille voimakkaasti tarve digiturva-asioiden kehittämisen jatkumolle. Johdon edustajien näkemyksen mukaan digiturva kuuluu kaikille ja se tulisi saada yhtä automaattiseksi osaksi työarkea kuin turvavyön kiinni laittaminen autolla ajettaessa. Tässä kannattaa huomioida, että monesti henkilö, joka ajaa ilman turvavyötä, vaarantaa vain itsensä. Mutta jos työntekijä ei muista laittaa kuvainnollisesti digiturvavyötä kiinni, vaarantaa hän koko organisaation. Muistelen, että joku digipalvelutiimiläisistä on käyttänyt vertauskuvaa aiemminkin eli tätä ajatusta on hyvä jalostaa Luovissa.

Digiturvallisuus on työyhteisössä kaikkien yhteinen asia, josta jokaisen täytyy huolehtia oman roolinsa mukaisesti. Valveutuneet organisaatiot huolehtivat digiturvasta ja kouluttavat ja ohjeistavat henkilöstöään. Silloin henkilöstö osaa toimia digiympäristön vaatimusten mukaisesti. (Rousku ym. 2019.) Digitaalisessa maailmassa varovaisuus ja terve epäily ovat taitoja, jotka henkilöiden on

tarpeen hallita (Haasio 2017, 75). Käytössä olevien ja uudenlaisten digityökalujen käyttö on turvallista, kun henkilöstö osaa toimia digiturvallisesti. Kokonaisuutena koulutustarvekyselyssä ilmi tullut Luovin henkilöstön halu olla mukana huolehtimassa digiturvallisuudesta oli erittäin ilahduttavaa. Tämän pohjalta Luovissa on hyvä lähteä kehittämään digiturvaosaamista ja varmistaa luottamus Luoviin, kun sen toiminta on turvallista.

9.2 Opinnäytetyöprosessin pohdinta

Opinnäyteprojekti käynnistettiin lokakuussa 2022, jolloin olimme jo osittain perheessämme tähänastisen elämämme vakavimman vastoinkäymisen edessä (toivottavasti tämä myös jäisi vakavimmaksi tilanteeksi). Tilanne pahentui marraskuussa ja etenemme edelleen asioissa päivän kerrallaan. Opinnäytetyö on välillä toiminut pakokeinona raskaasta arjesta ja sen avulla on voinut ajatella hetken muuta. Vaikea elämäntilanne ei ole kuitenkaan voinut olla vaikuttamatta opinnäytetyöhön käytettävissä olleisiin resursseihin. Alkuun halusin tehdä jotakin todella hienoa; jotakin sellaista, jota voitaisiin hyödyntää jopa valtakunnallisesti. Elämä on kuitenkin nyt opettanut aiempaa selvemmin, että sitä ei voi hallita. Tällä hetkellä olen kiitollinen siitä, että olen saanut ylipäänsä kirjoittaa opinnäytetyön ylempään ammattikorkeakoulututkintoon.

Varsinainen opinnäytetyöprosessi eteni kaikesta huolimatta kuitenkin pääsääntöisesti laaditun suunnitelman ja tyypillisen kehittämistyön prosessin (kuvio 15 sivulla 54) alkuvaiheiden mukaisesti. Opinnäytetyöstä jää aikataulusta johtuen puuttumaan osittain kehittämishankkeen toteuttaminen ja julkistaminen sekä kehittämisprosessin lopputulosten arviointi. Nämä asiat toteutetaan kyllä, mutta harmillisesti ne eivät ehdi tähän opinnäytetyöhön.

Kehittämistyön alussa toteutimme kyselyn koulutustarpeista. Koulutustarvekyselyn sisältöön olen tyytyväinen. Kysely on tehty huolellisesti teoriatietoon pohjautuen siistiksi ja sopivan pituiseksi. Lisäksi sitä paranneltiin vielä hieman esitestauksen perusteella. Valitettavasti kriisi perheessämme oli pahimmillaan juuri kyselyn vastausajan ollessa käynnissä, joten en pystynyt pitämään kyselyä

esillä siten kuin olisin halunnut. Uskon, että kyselyyn olisi saatu enemmän vastauksia, jos sitä olisi pidetty enemmän esillä. Ehkä kyselyn linkki olisi kannattanut lähettää myös henkilökohtaisesti jokaisen sähköpostiin, jolloin vastauksia olisi voinut tulla enemmän. Tai sitten olisi voitu sopia esihenkilöiden kanssa, että he ottavat kyselyyn vastaamisen osaksi omaa tiimipalaveriaan, jolloin jokainen olisi voinut vastata kyselyyn tiimipalaverin yhteydessä ja kyselyyn olisi saatu enemmän vastauksia.

Tutkimushaastattelua en voinut toteuttaa kasvotusten pidettävänä haastatteluna, vaan se piti perhetilanteen takia toteuttaa Teams-keskusteluna. Kysymysaiheet olivat kuitenkin riittävät johdon edustajien näkemysten keräämiseksi. Toki muokkaisin haastattelurunkoa nyt, jos se olisi mahdollista. Kysyisin esimerkiksi vielä tarkemmin johdon tarpeita digiturvakoulutuksen konkreettisesta sisällöstä sekä lisäisin kysymyksiä digiturvaosaamisen kehittämisestä laajemmin. Lisäksi toteuttaisin haastattelun kaikille johtoryhmäläisille sekä IT-palvelupäällikölle, jotta suunnittelun tukena olisi käytettävissä laajempi materiaali.

Mikäli voisin tehdä opinnäytetyön uudestaan, ottaisin myös henkilöstön vahvemmin mukaan digiturvallisuusosaamisen kehittämisen suunnitteluun. Esimerkiksi pidetyissä suunnittelutyöpajoissa olisi ollut hyvä olla mukana muutamia koulutuksen henkilöstön edustajia. Tällöin jo koulutuksen suunnitteluvaiheessa olisi voinut paremmin varmistua siitä, että koulutuksen sisältö tulee olemaan erityisesti myös koulutuksen henkilöstölle tarkoituksenmukainen. Lisäksi mukana olleet henkilöt olisivat voineet levittää myönteistä tietoa digiturvakoulutuksesta omassa työyhteisössään.

Digiturvaosaamisen kehittämissuunnitelmaa olen luonut kevään 2023 ajan ja sain siihen apua ja arvokkaita kommentteja muilta Luovin asiantuntijoilta. Yhteistyö muiden luovilaisten kanssa on ollut erittäin antoisaa. Olen oppinut heiltä paljon, ja he ovat auttaneet jaksamaan vaikeassa elämäntilanteessa. Tiedätte, keitä te erityisen ihanat työkaverit olette. Ennen kaikkea haluan kuitenkin kiittää äärettömän rakasta perhettäni. Tämä opinnäytetyö on tehty myös teitä varten, sillä olette kaikkeni. Nautitaan yhdessä elämästä!

9.3 Opinnäytetyön eettisyys ja luotettavuus

Tutkimusta voidaan pitää onnistuneena, jos sen avulla saadaan luotettavia vastauksia asetettuihin tutkimuskysymyksiin. Tutkimus tulee tehdä puolueettomasti ja rehellisesti siten, ettei vastaajille aiheudu tutkimuksesta haittaa. (Heikkilä 2014, 27.) Suomessa toimii tutkimuseettinen neuvottelukunta (Mäkinen 2006, 24). Tutkimuseettinen neuvottelukunta (TENK) on julkaissut maaliskuussa 2023 ohjeen ”Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa 2023.” Ohjeessa on huomioitu muun muassa kansainvälisyyden ja sähköisten työkalujen käytön lisääntyminen verrattuna aiempaan vuonna 2012 julkaistuun ohjeeseen. (Tutkimuseettinen neuvottelukunta 2023, 3.) Tämä opinnäytetyö on laadittu noudattaen TENKin vuoden 2012 ohjetta, sillä opinnäytetyön laadinta on aloitettu ennen vuoden 2023 ohjeen julkaisua. Lisäksi opinnäytetyössä on huomioitu TENKin ohje ”Ihmiseen kohdistuvan tutkimuksen eettiset periaatteet ja ihmistieteiden eettinen ennakkoarviointi Suomessa”.

Hyvän tieteellisen käytännön keskeiset lähtökohdat ovat rehellisyys, yleinen huolellisuus ja tarkkuus tutkimustyössä ja siihen liittyvissä toimissa. Lisäksi tulee huomioida muun muassa eettisesti kestävät tiedonhankinta-, tutkimus- ja arviointimenetelmät. TENKin laatiman ohjeen tavoitteena on hyvän tieteellisen käytännön edistämisen lisäksi ennalta ehkäistä tieteellistä epärehellisyyttä. (Tutkimuseettinen neuvottelukunta 2012, 6–7.)

Etiikka tarkastelee asioita moraalisesta näkökulmasta eli, mikä on oikein tai väärin tai sallittua tai kiellettyä (Pietarinen & Launis, 2002, 42). Tutkimusetiikka on mahdollista määritellä myös tutkijoiden ammattietiikaksi, johon kuuluvat eettiset periaatteet, hyveet, arvot ja normit, joita tutkijoiden olisi syytä noudattaa (Kuula 2011, 23). Luovissa eettisinä periaatteina toimivat Luovin arvot: luottamus, uudistajuus, osaaminen, ilo ja välittäminen. Eettiset periaatteet on huomioitava kaikessa sekä Luovin sisäisessä että ulkoisessa toiminnassa. (Ammattiopisto Luovi 2022.) Tämän opinnäytetyön laadinnassa on huomioitu hyvän tieteellisen käytännön lisäksi myös Luovin eettiset periaatteet.

Opinnäytetöiden laadinnassa tulee ottaa huomioon vaatimus luotettavuudesta. Kysymys luotettavuudesta kohdistuu tutkimuksessa käytettyihin menetelmiin, tutkimusprosessiin ja tutkimuksessa saatuihin tuloksiin (Toikko & Rantanen 2009, 121). Tutkimuksen tulokset eivät saisi olla sattumanvaraisia, vaan tutkimuksen tulisi olla toistettavissa. Tutkijan on oltava koko tutkimuksen ajan tarkka ja hänen on kyettävä tarkastelemaan asioita kriittisesti. (Heikkilä 2014, 28.) Tämän opinnäytetyön tulokset eivät ole sattumanvaraisia, vaan koulutustarvekysely ja tutkimushaastattelu voitaisiin toteuttaa myös uudelleen. Todennäköisesti tulokset olisivat hyvin samansuuntaisia, koska tutkimuksessa ei ole pyritty vaikuttamaan vastaajiin. Opinnäytetyössä asioita on tarkasteltu kriittisesti.

Tutkimuksellisen kehittämistyön päämääränä on tuottaa uusia ratkaisuja ja parantaa käytäntöjä. Siinä arvioidaan kriittisesti hankittua tietoa, erilaisia näkökulmia, prosessia ja tuloksia sekä omia valintoja. (Ojasalo ym. 2014, 19.) Tämä opinnäytetyö on tutkimuksellinen kehittämistyö, joka on laadittu konstruktiivisena tapaustutkimuksena. Koko prosessin ajan on huolehdittu siitä, että opinnäytetyön tuloksena syntyy myös uusia ratkaisuja, joita Luovissa ei ole vielä käytössä. Samoin on huolehdittu siitä, että tutkimuksen kohteena olevat ovat tienneet tutkimuksesta ja opinnäytetyön laadinnasta.

Opinnäytetyössä kartoitettiin koulutustarpeita anonyymilla kyselylomakkeella, johon koottiin valittavaksi valmiita aiheita ja annettiin mahdollisuus avoimeen vastaukseen. Kartoituskyselyssä oli myös neljä väittämää, johon toivottiin henkilöstön näkemys. Anonyymisti henkilöt lienevät uskaltaneet vastata totuudenmukaisesti. Toisaalta anonyymiin kyselyyn on helpompi jättää vastaamatta, kun vastanneiden henkilöllisyyttä ei selvitetä, eikä vastausta voida velvoittaa kaikilta. Kyselyyn vastasi 100 henkilöä, mutta kaikki heistä eivät vastanneet jokaiseen kysymykseen. Yhteensä kyselyssä oli kolme henkilöä, joilta ei saatu vastausta kaikkiin kysymyksiin. Kyselyyn saatiin lukumäärällisesti paljon vastauksia, joten vastauksia on käsitelty siten, että ne edustaisivat kaikkien luovilaisten näkemystä. Todellisuudessa kuitenkin tulokset voisivat olla erilaisia, mikäli kaikki luovilaiset olisivat vastanneet koulutustarvekyselyyn.

Opinnäytetyössä toteutettiin myös henkilötietoja sisältävä haastattelu tieto- ja viestintäjohtaja Susanna Kankaalle sekä IT- ja digipäällikkö Mervi Leinoselle. Kasvokkain tapahtuvaan haastatteluun sisältyy riski vastausten epätotuudenmukaisuudesta. Haastatteluun liittyen epävarmuudeksi jää se, onko mahdollista, että haastateltavat ryhtyivät tukemaan ensimmäiseksi kysymykseen vastanneen mielipidettä, vai sanoivatko he reilusti oman näkemyksensä asiaan. Haastateltavien välinen hierarkia voi vaikuttaa haastatteluvastauksiin. Valtahierarkia voi vaikuttaa siihen, ketkä haastateltavat puhuvat ja mitä he puhuvat (Hirsjärvi ym. 2009, 210). Uskon, että tässä haastattelussa tieto- ja viestintäjohtaja sekä IT- ja digipäällikkö ovat kertoneet rehellisesti omat ajatuksensa, mutta tieteellistä varmuutta asiasta ei ole mahdollista saada.

Opinnäytetyössä toteutettu tutkimushaastattelu olisi kannattanut toteuttaa useammalle johdon edustajalle. Nyt johdon edustajien näkemyksistä ei voida varmuudella yleistää koko johdon näkemyksiä. Lisäksi olisi ollut hyvä saada myös niiden johdon edustajien näkemyksiä, joille digiturva ei ole niin tuttu, jolloin digiturvaosaamisen kehittämiseen olisi voinut tulla uudenlaisia näkökulmia. Tieto- ja viestintäjohtajalla ja IT- ja digipäälliköllä on erinomainen tietämys digiturvasta ja Luovin tilanteesta, joten myös tutkimushaastattelun tuloksia on hyödynnetty digiturvakoulutuksen suunnitteluun ja digiturvallisuusosaamisen kehittämissuunnitelman laadintaan.

Opinnäytetyössä hyödynnettiin menetelmätriangulaatiota luotettavuuden parantamiseksi. Aineistoa kerättiin tieteellisesti kyselyllä ja haastattelulla sekä kehittämistöihin sopivalla suunnittelupajamenetelmällä. Eskolan & Suorannan (2014, 71) mukaan täytyy miettiä, onko erityyppisten aineistojen yhteensovittaminen soveliasta. Tässä opinnäytetyössä eri menetelmillä kerätty aineisto sopii mielestäni yhteen, koska aineisto kerättiin digiturvallisuuden kehittämistä tukemaan pyrkivästä näkökulmasta. Kehittämistyön luotettavuutta heikentää kuitenkin se, että suunnittelupajamenetelmä ei ollut alkuperäisessä tutkimussuunnitelmassa mukana, vaan se toteutettiin käytännön työn vuoksi. Siten suunnittelupajoista ei ole tehtynä dokumentaatiota, vaan sen tuomat ajatukset näkyvät tuotosten sisällössä. Puuttuva dokumentaatio suunnittelupajojen tuloksista estää suunnittelupajojen tulosten tieteellisen luotettavuuden arvioinnin. Suunnittelupajat on

kuitenkin toteutettu asianmukaisesti ja ne olisivat todennäköisesti toistettavissa siten, että niiden tulokset olisivat samankaltaisia kuin tämän kevään pajoissa.

Tutkimuksellisten kehittämistöiden luotettavuuteen vaikuttaa kehittämistyön hyödyntämiskelpoisuus eli käyttökelpoisuus (Toikko & Rantanen, 2009, 121). Kehittämistyön luotettavuutta voidaan arvioida tehdyn kehittämisratkaisun toimivuudella ja onnistumisella (Kananen 2017, 69). Tämän opinnäytetyön käyttökelpoisuutta ei voida arvioida tämän opinnäytetyöprosessin puitteissa. Digiturvaosaamisen kehittämissuunnitelman käyttökelpoisuuden arviointi vaatii suunnitelman toteuttamista pidemmällä aikavälillä, joten käyttökelpoisuutta voisi mielestäni arvioida aikaisintaan ensimmäisen hyödyntämisvuoden jälkeen.

Laadittua digiturvakoulutuksen runkoa hyödynnetään toukokuussa 2023 pidettävissä pilottikoulutuksissa. Rungon toimivuutta voisi arvioida alustavasti jo pilottikoulutuksista saatavien palautteiden ja koulutustiimiltä saatavan palautteen perusteella. Lopullinen rungon toimivuuden arviointi olisi mahdollista tehdä, kunhan kaikki suunnitellut koulutukset koko henkilöstölle olisi saatu pidettyä.

Ensimmäinen pilottikoulutus pidettiin 4.5.2023. Koulutuksesta tuli erinomaista palautetta: ”Mahtava kokonaisuus ja asiantuntevat, iloiset kouluttajat. Asiat esitetty tarpeeksi ytimekkäästi, jolloin olennainen jäi mieleen, ja materiaalia oli käytetty monipuolisesti (videot yms.). 2,5 tuntia meni todella nopeasti tässä koulutuksessa! Hyvää työtä 😊” ja ”Pilottikoulutus oli mielestäni oikein onnistunut. Kokonaisuus, jossa oli yhdistelty teoriaa ja toiminnallisia menetelmiä, toimi kohdallani varsin hyvin. Lopun Kahoot kruunasi koko koulutuksen ja sai adrenaliinin nousemaan. Loistavaa työtä!”. Pilottikoulutuksen palautekysely sisälsi myös koulutustarvekyselyssä olleet digiturvallisuusväittämät. Palautekyselyn tulosten mukaan yhtä vastaajaa lukuun ottamatta kaikki kokevat, että digiturvallisuus on osa heidän työarkeaan. On jännittävää nähdä, mitkä tulokset ovat, kunhan digiturvakoulutukset on saatu pidettyä kaikille luovilaisille.

Ensimmäiset johdon edustajien ja luovilaisten asiantuntijoiden kommentit digiturvallisuusosaamisen kehittämissuunnitelmasta ovat olleet erittäin myönteisiä ja rohkaisevia. Uskon vahvasti, että digiturvaosaamisen kehittämissuunnitelma

sisältää asioita, joita Luovissa lähdetään toteuttamaan, koska Luovi haluaa lisätä henkilöstönsä digiturvaosaamista muutoinkin kuin vuonna 2023 toteuttavalla digiturvakoulutuksella. Osaamisen kehittämistoimien aikataulu ja laajuus selviävät, kunhan digiturvaosaamisen kehittämissuunnitelma ennättää johtoryhmän käsittelyyn alkukesällä 2023. Osaamisen kehittämisen jatkumon varmistamiseksi on tärkeää, että johtoryhmä valitsee toteuttavaksi monipuolisesti asioita henkilöstön digiturvaosaamisen kehittämissuunnitelmasta. Lisäksi on tärkeää määritellä vastuuhenkilöt toteuttaville kehittämistoimille. Johtoryhmässä tulee myös suunnitella, kuinka digiturvaosaamisen kehittämisen suunnitelmaa arvioidaan. Kaiken kaikkiaan uskon, että opinnäytetyön tuotokset osoittautuvat hyödyllisiksi, koska ne on laadittu käytännönläheisiksi ja toteuttamiskelpoisiksi Luovin toiminnan reunaehdot huomioiden.

9.4 Työn vertaaminen aikaisempien opinnäytetöiden tuloksiin

Luvussa 1.4 on esitelty kaksi aiempaa opinnäytetyötä, joiden aiheena olivat digitalisaatio ja osaamisen kehittäminen. Kyllösen (2019) työssä tutkittiin pankin henkilöstön digitaalisen osaamisen kehittämistä itsensä johtamisen kautta ja Jokilammen (2018) työssä taloushallintoalan yrityksen henkilöstön osaamisen kehittämistä digitalisaation kontekstissa. Kummankaan opinnäytetyön aiheena ei ollut digiturvallisuus, mutta digiturvallisuus on osa digitalisaatiota, joten tuloksia voidaan peilata toisiinsa digitalisaatioon liittyen. Jokilammi laati työssään osaamisen kehittämisen suunnitelman digitalisaation näkökulmasta, joten Jokilammen osaamisen kehittämissuunnitelman sisältöä voi osin verrata tässä opinnäytetyössä laadittuun osaamisen kehittämissuunnitelmaan.

Sekä Kyllönen että Jokilammi toteuttivat työnsä tapaustutkimuksina. Tämä opinnäytetyö on konstruktiivinen tapaustutkimus. Kaikissa opinnäytetöissä oli tavoitteena luoda toimeksiantajalle uusia kehittämisehdotuksia. Töissä esiin nousseet kehittämisehdotukset olivat melko samankaltaisia. Kyllönen havaitsi, että osaamisen kehittämisen keinoja ovat esimerkiksi työparityöskentely, tiimipalaverit, sisäisen motivaation kehittäminen ja koulutuksen järjestäminen. Kyllösen työn tuloksissa tuli myös ilmi tarve osaamisen jakamiselle (Kyllönen 2019).

Jokilammen laatiman vuosikellon mukaisesti organisaatiossa tulisi muun muassa järjestää koulutuksia ja jakaa opittuja tietoja yhteisissä keskusteluissa (Jokilammi 2018). Myös tämän opinnäytetyön osaamisen kehittämisen keinoista ja vuosikellosta löytyvät tiimipalaverit ja koulutukset sekä osaamisen jakaminen.

Jokilammi havaitsi opinnäytetyössään, että investoinnit teknologian kehittämiseen eivät riitä, vaan organisaation tulee panostaa myös osaamisen kehittämiseen. Digiajan organisaatioissa edellytetään uudenlaista osaamista. Jokilammen työn tuloksissa tuli myös ilmi, että digitalisaatio vaikuttaa teknologian lisäksi myös muun muassa organisaatiokulttuuriin ja johtamiseen. (Jokilammi 2018.) Tämän opinnäytetyön lähtökohtana oli tarve kehittää Luovin henkilöstön digiturvaosaamista. Digitalisaation vaikutuksia ei tutkittu tässä opinnäytetyössä, mutta digiturvan osalta tuli myös ilmi tarve saada se osaksi organisaatiokulttuuria. Digiturva ei ole muista toiminnoista irrallinen kokonaisuus, vaan se näkyy useissa organisaation toiminnoissa. Digitalisaation täysimittainen hyödyntäminen edellyttää digiturvallisuuden huomioimista. Henkilöstön digiturvaosaamisen kehittäminen on kannattavaa, koska toimimme jatkuvasti muuttuvassa digitaalisessa toimintaympäristössä.

Osaamisen kehittämiskohteiksi Jokilammen työssä nousivat taloushallintoalan yrityksen henkilöstön teknologiaosaaminen sekä kyky analyyttiseen taitoon tulkita ja hyödyntää dataa (Jokilammi 2018). Sekä tässä että Jokilammen opinnäytetyössä havaittiin, että työn murros on muuttanut merkittävästi työn osaamisvaateita. Kaikissa kolmessa opinnäytetyössä näkyy digitalisaation merkitys muutosajurina ja työntekijöiden oman roolin tärkeys osaamisen kehittämisen onnistumisessa.

Tässä opinnäytetyössä ei tutkittu henkilöstön osaamisen tasoa, kuten Kyllönen teki. Molemmissa töissä kävi kuitenkin ilmi, että henkilöstö haluaa olla mukana työn muutoksessa ja on pääsääntöisesti kiinnostunut laajentamaan omaa digiosaamistaan. Tässä opinnäytetyössä kysyttiin Luovin henkilöstöltä halua olla mukana huolehtimassa digiturvallisuudesta, mikä käytännössä tarkoittaa myös henkilöstön digiosaamisen laajentamista. Luovin henkilöstölle tehdyn koulutustarvekyselyn vastauksissa kävi ilmi, että yhteensä 90,7 prosenttia kaikista

kyselyyn vastanneista työntekijöistä haluaa olla mukana huolehtimassa digiturvallisuudesta. Tämä on erittäin hyvä lähtökohta tämän opinnäytetyön hyödyntämiselle Luovissa.

9.5 Opinnäytetyön hyödyntäminen ja jatkokehityskohteet

Opinnäytetyössä syntynyttä henkilöstön digiturvallisuusosaamisen kehittämissuunnitelmaa voitaneen hyödyntää Luovin lisäksi erityisesti muissa ammatillisissa erityisoppilaitoksissa. Sovellettuna suunnitelma lienee hyödynnettävissä muissakin organisaatioissa. Ajatus siitä, että digiturva on osa jokaisen työntekijän arkea, on sellainen, jota soisi hyödynnettävän laajasti. Digitalisaatio koskee nyky-yhteiskunnassa käytännössä kaikkia organisaatioita, joten henkilöstön kouluttaminen digiturva-asioissa koskettaa monia. Tässä opinnäytetyössä löydettyjä kehittämistoimia on mahdollisista muokata kunkin organisaation omiin tarpeisiin sopivaksi.

Luovin henkilöstön digiturvallisuusosaamisen kehittämissuunnitelmaa voidaan hyödyntää myös Hengitysliitto ry:n henkilöstön digiturvaosaamisen kehittämisessä. Luovi tarjoaa tiedonhallinta- ja digipalveluja myös omistajansa Hengitysliiton muille toimintayksiköille. Koulutusta voidaan siten hyödyntää myös Hengitysliiton työntekijöiden digiturvaosaamisen kehittämisessä ja ohjauksessa digiturvan huomioimiseen osana työarkea.

Tähän opinnäytetyöhön liittyvänä jatkotutkimuksena voitaisiin selvittää Luoville laaditun digiturvallisuusosaamisen kehittämissuunnitelman toimivuutta esimerkiksi parin vuoden kuluttua tehtävällä seurantatutkimuksella. Henkilöstölle ja johdon edustajille voisi toteuttaa kyselyn, jonka avulla selvitettäisiin, onko digiturvallisuudesta tullut luonteva osa henkilöstön työarkea. Lisäksi voisi selvittää, mitä kehittämistoimia on toteutettu ja kuinka niiden toteuttaminen on onnistunut.

Opinnäytetyön aiheesta voisi tehdä toisen tutkimuksellisen kehittämistyön, jonka näkökulmana olisi opiskelijoiden digiturvallisuusosaamisen kehittäminen. Digiturvaosaaminen on keskeinen taito myös opiskeluarjessa. Opiskelijoiden

digiturvaosaamisen saaminen osaksi opiskeluarkea voisi olla ensimmäinen jatkokehitysmahdollisuus. Tämän jälkeen voisi tehdä kehittämistyön digiturvallisuusosaamisen ylläpitämisestä. Siinä työssä voisi selvittää, millä tavalla opiskelijoiden digiturvaosaamisen tasoa voidaan ylläpitää ja kuinka esimerkiksi digiturvakoulutusten jatkumo kannattaa toteuttaa. Kehittämistyön voisi tehdä myös kahtena erillisenä työnä. Toisessa voisi selvittää opiskelijoiden osaamisen ylläpitämistä ja toisessa henkilöstön. Olisi mielenkiintoista nähdä, millä tavalla osaamisen ylläpitämisen keinot mahdollisesti eroaisivat opiskelijoiden ja henkilöstön välillä. Kenties näissä kehittämistöissä voisi samalla selvittää opiskelijoiden ja henkilöstön digitaalisen älykkyyden tasoa, jolloin sitäkin voisi verrata toisiinsa.

Digitaalinen älykkyys on nyky-yhteiskunnassa verrattavissa luku- ja laskutaitoon. Digitaalinen osaaminen on perustaito, joka kuitenkin puuttuu monelta työelämässä olevalta. Jatkuvan oppimisen näkökulmasta on tärkeää, että koko aikuisväestö oppisi tarvittavat digitaaliset perustaidot, jotta digiosaaminen saadaan tulevaisuuden vaatimalle tasolle. (Kallonen & Kuhmonen 2021, 13.) Digitalisaation suuret edut paljastuivat esimerkiksi koronakriisissä, mutta digitalisaatio voi olla myös uhka. Digisyrjäytyminen on yhtä kuin lukutaidottomuus ja osa ihmisistä ei kykene, halua tai ehdi käyttää esimerkiksi digipalveluja. (Kangas ym. 2021, 215, 220-221.) Kun henkilö osaa toimia digitaalisessa yhteiskunnassa, voidaan puhua myös digitaalisesta sivistyksestä. Digitaalisesti sivistynyt henkilö osaa muun muassa arvioida verkossa olevaa sisältöä ja tunnistaa valeinformaation sekä ymmärtää datataloutta. (Dufva & Rekola 2023, 54.)

Ajatus digitaalisen osaamisen vertaamisesta luku- ja laskutaitoon on pysäyttävä. Mutta tämäkin opinnäytetyö osoittaa, että nykyajan työelämässä todella tarvitaan digitaitoja ja sen myötä digiturvaosaamista. Toivottavasti digiturvallisuus tulee näkymään vahvasti tulevissa työelämää varten tehtävissä kehittämistöissä. Organisaatioiden menestyminen teknologisessa myllerryksessä edellyttää digiturvallisen toiminnan hallitsemista, joten digiturvallisuus kannattaa saada kaikissa organisaatioissa luontevaksi osaksi henkilöstön työarkea.

Lähteet

Alapuranen, L. 2020. Työelämän henkilötietojen käsittelyedellytykset. Teoksessa Alapuranen, L., Lehtonen, L., Koskinen, S. & Wiberg, M. (toim.). Henkilötietojen käsittely työelämässä. Helsinki: Edita Publishing Oy, 7–168.

Alasoini, T. 2023. Koronan jälkeistä työelämää – mutta millaista? Teoksessa Mäkikangas, A. & Pyöriä, P. (toim.). Koronapandemia, työ ja yhteiskunta. Muuttuiko Suomi? Helsinki: Gaudeamus, 276–293.

Ammattiopisto Luovi. 2022. Luovin kurssi. Ammattiopisto Luovin henkilöstön intranet. Vain sisäiseen käyttöön. 27.1.2023.

Ammattiopisto Luovi. 2023a. Luovin digiturvallisuus. Ammattiopisto Luovin henkilöstön intranet. Vain sisäiseen käyttöön. 7.2.2023.

Ammattiopisto Luovi. 2023b. Luovin johtoryhmän päätös 18.1.2023. Ammattiopisto Luovin henkilöstön intranet. Vain sisäiseen käyttöön. 7.2.2023.

Ammattiopisto Luovi. 2023c. Luovin organisaatio. Ammattiopisto Luovin henkilöstön intranet. Vain sisäiseen käyttöön. 27.1.2023.

Ammattiopisto Luovi. 2023d. Tervetuloa Luoviin. https://luovi.fi/. 27.1.2023.

Anttila, P. 2007. Realistinen evaluaatio ja tuloksellinen kehittämistyö. Hamina: Akatiimi Oy.

Andreasson, A. & Ylipartanen, A. 2022. Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus (GDPR). Helsinki: Tietosanoma.

Anttolainen, V-H. 2023. Kyberhyökkäys Keudassa. Loppuraportti. Keski-Uudenmaan koulutuskuntayhtymä. https://urly.fi/34Au. 18.3.2023.

Barzilay, M. 2023. Crisis Management – best and worst practices. Tietoturva ry:n järjestämä Tietoturvakatsaus 2023 osa 1. Youtube-video. https://www.youtube. com/watch?v=k--Ic_rQ08s. 8.4.2023.

Brinkmann, S. & Kvale, S. 2018. Doing Interviews. The SAGE Qualitative Research Kit. 2nd Edition. Lontoo: SAGE Publications Ltd.

Bruun, N. 2022. Työoikeuden perusteet. Helsinki: Alma Talent.

Clegg, S., Kornberger, M., Pitsis. T. & Mount, M. 2019. Managing & Organizations. An Introduction to Theory and Practice. 5th Edition. London: SAGE Publications Ltd.

Digi- ja väestötietovirasto. 2022. VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön – esittely ja johdatusta riskiviestintään. https://dvv.fi/documents/16079645/110183105/VAHTI-riskienhallintasanasto.pdf/016e7906-f5ee-029f-f279-9bd23f9dc900/VAHTI-riskienhallintasanasto.pdf?t=1655187086298. 2.10.2022.

Digi- ja väestötietovirasto. 2023. Digiturvapalvelut. https://dvv.fi/digiturva. 18.3.2023.

Dufva, M. & Rekola, S. 2023. Megatrendit 2023. Ymmärrystä yllätysten aikaan. Sitran selvityksiä 224. https://www.sitra.fi/julkaisut/megatrendit-2023/. 18.3.2023.

Dufva, M., Wartiovaara, A. & Vataja, K. 2021. Työn tulevaisuudet megatrendien valossa. Sitra. https://www.sitra.fi/artikkelit/tyon-tulevaisuudet-megatrendien-valossa/. 16.10.2022.

Eklund, A. 2021. Osaamiskartta. Osaamisen kehittäminen työelämässä. Espoo: Brik.
Eskola, J. & Suoranta, J. 2014. Johdatus laadulliseen tutkimukseen. Tampere: Vastapaino.
Eulenberger, S. 2021. Vapaalla tyylillä taitajaksi. Helsinki: Basam Books.
Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus)
Gebremeskel, B. K., Jonathan, G. M. & Yalew, S. D. 2023. Information Security Challenges During Digital Transformation. Procedia Computer Science 219, 44-51. https://www.sciencedirect.com/science/article/pii/S1877050923002703. 25.3.2023.
Goran, J., LaBerge, L. & Srinivasan, R. 2017. Culture for a digital age. McKinsey Digital. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/culture-for-a-digital-age#/. 17.3.2023.
Haasio, A. 2017. Verkkorikokset. Vantaa: BTJ Finland Oy.
Hagert, K. & Toivanen, P. 2022. Duuniin. Kaikki mitä haluat tietää työn aloittamisesta, työelämän muutoksesta ja unelmien tavoittelemisesta. Jyväskylä: Atena.
Heikkilä, T. 2014. Tilastollinen tutkimus. Helsinki: Edita.
Hiila, I., Tukiainen, M. & Hakola, I. 2019. Tiimiäly. Opas muuttuvaan työelämään. Jyväskylä: Tuuma-kustannus.
Hiltunen, E. 2019. Tulossa huomenna. Miten megatrendit muokkaavat tulevaisuuttamme. Jyväskylä: Docendo Oy.
Hiltunen, E. 2023. Digitaalinen toimintaympäristömme muuttuu, miten valmistaudumme? Digi- ja väestötietoviraston järjestämä Digihumaus 2023. https://event.prospectumlive.com/digihumaus-2023/room/4980. 8.4.2023.
Hirsjärvi, S. & Hurme, H. 2022. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki: Gaudeamus.
Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. Helsinki: Kustannusosakeyhtiö Tammi.
Huoltovarmuuskeskus. 2023. Jatkuvuudenhallinta. https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/jatkuvuudenhallinta. 25.3.2023.
Hyppönen, M. 2021. Internet. Helsinki: Werner Söderström Osakeyhtiö.
Ilmonen, I., Kallio, J., Koskinen, J. & Rajamäki, M. 2022. Johda riskejä. Käytännön opas yrityksen riskienhallintaan. Helsinki: Finanssikoulutus.
Jokelainen, P. 2023. Opiskelijan digitaaliset oppimisen mahdollisuudet paikan ja ajan suhteen Luovissa. Ammattiopisto Luovin henkilöstön intranet. Vain sisäiseen käyttöön. 25.3.2023.
Joki, M. 2021. Henkilöstöasiantuntijan käsikirja. Helsinki: Helsingin Kamari Oy.
Jokilammi, A-M. 2018. Digiajan työntekijän kehittämissuunnitelma. Satakunnan ammattikorkeakoulu. Yrittäjyys ja liiketoimintaosaaminen. Yamk-opinnäytetyö. https://urn.fi/URN:NBN:fi:amk-2018061814039. 17.2.2023.
Juuti, P. & Puusa, A. 2020. Johdanto. Mitä laadullisella tutkimuksella tarkoitetaan? Teoksessa Puusa, A. & Juuti, P. (toim.). Laadullisen tutkimuksen näkökulmat ja menetelmät. Helsinki: Gaudeamus, 9–19.
Juuti, P. & Vuorela, A. 2010. Johtaminen ja työyhteisön hyvinvointi. Jyväskylä: PS-Kustannus.

Järvinen, P. 2017. Nettiturvallisuus. Teoksessa Järvinen, P. & Rousku, K. Työpaikan tietoturvaopas. Tunnista uhat, hallitse riskit. Helsinki: Alma Talent, 73–101.
Järvinen, P. 2022a. Digiajan tietosuoja. Turvaa henkilötietosi. Torju identiteettivarkaudet. Suojaudu urkinnalta. Helsinki: Tammi.
Järvinen, P. 2022b. Yrityksen tietoturvaopas. 50 aihetta käytännön tietoturvasta. Helsinki: Helsingin seudun kauppakamari.
Kaijala, M. & Tolvanen, R. 2020. Henkilöstö – strateginen investointi? Helsinki: Helsingin seudun kauppakamari.
Kallonen, T. & Kuhmonen, A. 2021. Jatkuva oppiminen – työelämän tärkein taito. Helsinki: Helsingin seudun kauppakamari.
Kananen, J. 2017. Kehittämistutkimus interventiotutkimuksen muotona. Opas opinnäytetyön ja pro gradun kirjoittajalle. Jyväskylän ammattikorkeakoulun julkaisuja 232. Jyväskylä: Jyväskylän ammattikorkeakoulu.
Kangas, R., Nenonen, M. & Välimaki, M. 2021. K niin kuin katastrofi. Länsimaiden seitsemän tulevaisuutta. Jyväskylä: Atena Kustannus.
Kasvi, J. J. J. 2019. Digi, digi, digi. Digitalisaatiossa on kyse organisaatiokulttuurinmuutoksesta. Se on tunnetusti vaikeaa. Tieke. https://tieke.fi/digi-digi-digi/. 17.3.2023.
Kirves, J., Pelttari, T. & Vänttinen, P. 2022. Digitaalinen turvallisuus järjestykseen arkkitehtuurin avulla. Digi- ja väestötietovirasto ja eOppiva. https://www.eoppiva.fi/koulutukset/digitaalinen-turvallisuus-jarjestykseen-arkkitehtuurin-avulla/. 8.4.2023.
Koskinen, J. 2020. Relewant: onnistutaan oppimalla. Helsinki: Ajantieto.
Korpiola, L. & Poutanen, P. 2021. Korona ja digitaalinen riskiyhteiskunta. Helsinki: Tammi.
Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. 2022. Tietosuoja. Helsinki: Alma Talent.
Kortesuo, K. 2010. Avaa tästä. Käytännön käsikirja kouluttajalle. Helsinki: Infor.
Krakau, T. & Haapalehto, S. 2020. Tietopyynnöt ja henkilötietojen luovuttaminen. Helsinki: Alma Talent.
Kuosmanen, M. 2022. Kyberhyökkäyksen anatomia – organisaatio hyökkäyksen kohteena. Digiturvaviikon webinaari 11.10.2022. https://www.mediaserver.fi/live/digiturvaviikko/10007/1ClZzA. 18.3.2023.
Kupias, P. & Peltola, R. 2019. Oppiminen työssä. Helsinki: Gaudeamus.
Kupias, P., Peltola, R. & Pirinen, J. 2014. Esimies osaamisen kehittäjänä. Helsinki: Sanoma Pro Oy.
Kuula, A. 2011. Tutkimusetiikka. Aineistojen, hankinta, käyttö ja säilytys. Tampere: Vastapaino.
Kyllönen, J. 2019. Digitaalisen osaamisen kehittäminen itsensä johtamisen kautta Pohjois-Karjalan Osuuspankissa. Karelia-ammattikorkeakoulu. Johtamisen ja liiketoimintaosaamisen koulutus. Yamk-opinnäytetyö. https://urn.fi/URN:NBN:fi:amk-2019062517520. 17.2.2023.
Kyberturvallisuuskeskus. 2020a. Tietoturva. https://www.kyberturvallisuus keskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva. 25.3.2023.
Kyberturvallisuuskeskus. 2020b. Toimi näin, jos havaitset tietoturvapoikkeaman. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/toimi-nain-jos-havaitset-tietoturvapoikkeaman. 25.3.2023.
Laine, M., Bamberg, J. & Jokinen, P. 2007. Tapaustutkimuksen käytäntö ja teoria. Teoksessa Laine, M., Bamberg, J. & Jokinen, P. (toim.). Tapaustutkimuksen taito. Helsinki: Gaudeamus, 9–38.

Limnéll, J., Hiltunen, E. & Dufva, M. 2022. Suomen tulevaisuudet. Suuret kysymykset ja vastaukset. Helsinki: WSOY.
Lindgren, J., Mokka, R., Neuvonen, A. & Toponen, A. 2019. Digitalisaatio. Murroksen koko kuva. Helsinki: Tammi.
Moilanen, T., Ojasalo, K. & Ritalahti, J. 2022. Methods fo Development Work. New kids of competencies in business operations. Helsinki: Books on Demand.
Mäkinen, O. 2006. Tutkimusetiikan ABC. Helsinki: Kustannusosakeyhtiö Tammi.
Nieto, M. 2014. Human Resource Management. Hampshire: Palgrave Macmillan.
Nyyssölä, M. 2020. Yksityisyyden suoja työsuhteessa. Helsinki: Alma Talent.
Ojasalo, K., Moilanen, T. & Ritalahti, J. 2014. Kehittämistyön menetelmät: Uudenlaista osaamista liiketoimintaan. Helsinki: Sanoma Pro.
Opetushallitus. 2023. Tietoturva ja -suoja koulussa. https://www.oph.fi/fi/ koulutus-ja-tutkinnot/tietoturva-ja-suoja-koulussa. 25.3.2023.
Otala, L. 2002. Oppimisen etu – kilpailukykyä muutoksessa. Helsinki: WSOY.
Otala, L. 2018. Ketterä oppiminen. Keino menestyä jatkuvassa muutoksessa. Helsinki: Kauppakamari.
Otala, L. & Meklin, S. 2021. Ketterä oppiminen 2. Strategiasta käytäntöön. Helsinki: Kauppakamari.
Paanetoja, J. & Salminen, J. 2022. Uudistunut yhteistoimintalaki. Helsinki: Edita Publishing Oy.
Peltomäki, J. & Norppa, K. 2015. Rikos meni verkkoon. Näkökulmia kyberrikollisuuteen ja verkkoturvallisuuteen. Helsinki: Talentum.
Peränen, N. 2013. Innopajaopas kehittäjälle. https://innokyla.fi/sites/default/ files/2020-02/Innopajaopas%20kehitt%C3%A4j%C3%A4lle%205%203%202013.pdf. 15.4.2023.
Piekkari, R. & Welch, C. 2020. Oodi yksittäistapaustutkimukselle ja vertailun moninaiset mahdollisuudet. Teoksessa Puusa, A. & Juuti, P. (toim.). Laadullisen tutkimuksen näkökulmat ja menetelmät. Helsinki: Gaudeamus, 197–205.
Piekkari, R., Welch, C. & Paavilainen, E. 2009. The case study as disciplinary convention. Evidence from international business journals. Organizational Research Methods 12 (3), 567-589. https://journals.sagepub.com/doi/abs/10.1177/1094428108319905?journalCode= orma. 2.4.2023.
Pietarinen, J. & Launis, V. 2002. Etiikan luonne ja alueet. Teoksessa Karjalainen, S., Launis, V., Pelkonen, R. & Pietarinen, J. (toim.). Tutkijan eettiset valinnat. Helsinki: Gaudeamus, 42–57.
Pyyhtiä, T. 2019. Digiajan johtajan käsikirja: käytännönläheinen, helppolukuinen ja tiivis opas digiajan johtamiseen. Helsinki: Books on Demand.
Ranta, R. 2021. Kehittyvä työyhteisö: kehittäminen, tiimityö ja ryhmän johtaminen muutoksessa. Helsinki: Suomen yrityskirjat Oy.
Rousku, K. 2017. Muutostekijät ja tietoturvallisuuden merkitys. Teoksessa Järvinen, P. & Rousku, K. Työpaikan tietoturvaopas. Tunnista uhat, hallitse riskit. Helsinki: Alma Talent, 5–44.
Rousku, K., Kirves, J. & Kinnunen, E. 2019. Digiturvallinen työelämä. Digi- ja väestötietovirasto ja eOppiva. https://www.eoppiva.fi/koulutukset/ digiturvallinen-tyoelama/. 8.4.2023.

Savolainen, T. & Lehmuskoski, K. 2017. Digimuutos.fi: 10 huippujohtajan tarina muutosjohtamisesta! Masala: Timo Savolainen.
Sinokki, M. 2016. Työmotivaatio. Innostusta, laatua ja tuottavuutta. Helsinki: Tietosanoma Oy.
Sitra. 2020. Sitran selvityksiä 162: Megatrendit 2020. https://www.sitra.fi/-app/uploads/2019/12/megatrendit-2020.pdf. 2.10.2022.
Sutela, H., Pärnänen, A. & Keyriläinen M. 2019. Digiajan työelämä – työolotutkimuksen tuloksia 1977–2018. Helsinki: Tilastokeskus.
Sydänmaanlakka, P. 2004. Älykäs organisaatio. Helsinki: Talentum Media Oy.
Tietosuojavaltuutetun toimisto. 2023a. Erityisten henkilötietoryhmien käsittely. https://tietosuoja.fi/erityisten-henkilotietoryhmien-kasittely. 25.3.2023.
Tietosuojavaltuutetun toimisto. 2023b. Rekisteröidyn oikeudet. https://tietosuoja.fi/rekisteroidyn-oikeudet. 18.3.2023.
Tietosuojavaltuutetun toimisto. 2023c. Tietosuoja. https://tietosuoja.fi/tietosuoja. 8.3.2023.
Tietosuojavaltuutetun toimisto. 2023d. Tietosuojavastaavat. https://tietosuoja.fi/tietosuojavastaavat. 8.3.2023.
Tietosuojavaltuutetun toimisto. 2023e. Tietoturvaloukkaukset. https://tietosuoja.fi/tietoturvaloukkaukset. 25.3.2023.
Tietosuojavaltuutetun toimisto. 2023f. Vaikutustenarviointi. https://tietosuoja.fi/vaikutustenarviointi. 25.3.2023.
Toikko, T. & Rantanen, T. 2009. Tutkimuksellinen kehittämistoiminta. Näkökulmia kehittämisprosessiin, osallistamiseen ja tiedontuotantoon. Tampere: Tampere University Press.
Traficom. 2020. Kyberturvallisuus ja yrityksen hallituksen vastuu. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf. 25.3.2023.
Traficom. 2023a. Näin suojaudut nettihuijaukselta. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-nettihuijaukselta. 18.3.2023.
Traficom. 2023b. Monivaiheinen tunnistautuminen suojaa käyttäjätilejäsi. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-opaat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi. 18.3.2023.
Tutkimuseettinen neuvottelukunta. 2012. Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa. https://www.tenk.fi/ sites/tenk.fi/files/HTK_ohje_2012.pdf. 16.10.2022.
Tutkimuseettinen neuvottelukunta. 2023. Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa 2023. https://tenk.fi/ sites/default/files/2023-03/HTK-ohje_2023.pdf. 16.4.2023.
Työterveyslaitos. 2022. Teknologinen muutos ja työ. https://hyvatyo.ttl.fi/muutosvoimat/teknologinen-muutos. 16.10.2022.
Työterveyslaitos. 2023. Varautuminen ja jatkuvuudenhallinta. https://www.ttl.fi/oppimateriaalit/resilienssi-ja-jatkuvuudenhallinta/varautuminen-ja-jatkuvuudenhallinta. 25.3.2023.
Tähtinen, J., Laakkonen, E. & Broberg, M. 2020. Tilastollisen aineiston käsittelyn ja tulkinnan perusteita. Turku: Turun yliopiston kasvatustieteiden laitos.
Valli, R. 2018. Aineistonkeruu kyselylomakkeella. Teoksessa Valli, R. (toim.). Ikkunoita tutkimusmetodeihin 1. Metodin valinta ja aineistonkeruu: virikkeitä aloittelevalle tutkijalle. Jyväskylä: PS-kustannus, 92–116.

Valtioneuvosto. 2022. Valtioneuvoston selonteko: Digitaalinen kompassi. Valtioneuvoston julkaisuja 2022:65. https://julkaisut.valtioneuvosto.fi/handle/10024/164429. 12.3.2023.

Valtioneuvoston kanslia. 2019. Informaatiovaikuttamiseen vastaaminen. Opas viestijöille. Valtioneuvoston kanslian julkaisuja 2019:11. https://julkaisut.valtioneuvosto.fi/handle/10024/161512. 25.4.2023.

Valtiovarainministeriö. 2017. Valtiovarainministeriön julkaisuja 8/2027: Tietoturvapoikkeamatilanteiden hallinta. https://www.suomidigi.fi/ sites/default/files/2020-06/VM_8_2017.pdf. 25.3.2023.

Valtiovarainministeriö. 2020. Valtiovarainministeriön julkaisuja 20:23: Julkisen hallinnon digitaalinen turvallisuus. https://julkaisut.valtioneuvosto.fi/handle/10024/162169. 2.10.2023.

Vehkamäki, P., Lahtinen, M. & Vanttaja, U. 2018. Julkisuus ja tiedonhallinta opetustoimessa. Opas koulujen ja oppilaitosten käyttöön. Opetushallitus. Oppaat ja käsikirjat 2018:5a. https://www.oph.fi/ sites/default/files/documents/julkisuus_ja_tiedonhallinta_opetus toimessa.pdf. 12.3.2023.

Vial, G. 2019. Understanding digital transformation: A review and a research agenda. The Journal of Strategic Information Systems 28 (2), 118-144. https://www.sciencedirect.com/science/article/abs/pii/S0963868717302196. 25.3.2023.

Viitala, R. 2013. Henkilöstöjohtaminen. Strateginen kilpailutekijä. Helsinki: Edita Publishg Oy.

Viitala, R. 2021. Henkilöstöjohtaminen. Keskeiset käsitteet, teoriat ja trendit. Helsinki: Edita Publishing Oy.

Viitala, R. & Jylhä, E. 2019. Johtaminen. Keskeiset käsitteet, teoriat ja trendit. Helsinki: Edita Publishing Oy.

Vilkka, H. 2021. Tutki ja kehitä. Jyväskylä: PS-kustannus.

Virtanen, A. 2006. Konstruktiivinen tutkimusote. Miten koulutus ja elinkeinoelämän odotukset kohtaavat ammattikorkeakoulun opinnäytetöissä. Ammattikasvatuksen aikakauskirja 8 (1), 46–52.

Voutilainen, T. 2019. Oikeus tietoon. Informaatio-oikeuden perusteet. Helsinki: Edita Publishing Oy.

Warma-Lehtinen, E. 2021. Lukijalle. Teoksessa Andreasson, A. & Ylipartanen, A. Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus (GDPR). Helsinki: Tietosanoma, 9–12.

Yhteistoimintalaki 1333/2021

Koulutustarpeiden kartoitus digiturvallisuudesta

Saate kyselyyn

Teknologia kehittyy nopeasti ja se muokkaa työtä ja tapoja tehdä työtä. Teknologioiden kehittymisen myötä myös digiturvallisuus on tärkeä osa kaikkien työarkea. Hyvällä digiturvallisuudella haluamme turvata opiskelijoidemme ja henkilöstömme tietojen turvallisen käsittelyn.

Digiturvallisuuteen kuuluvat tietoturvallisuus, tietosuoja, riskienhallinta, toiminnan jatkuvuuden hallinta ja kyberturvallisuus. Digiturvallisuus on tavoitetila, jossa digitaaliseen toimintaympäristöön voidaan luottaa. Digiturvallinen toiminta on turvallista ja hallittua sekä normaalioloissa että häiriötilanteissa.

Luovin tiedonhallinnan asiantuntija Miia Kauppinen laatii osana yamk-opinnäytetyötään Luoville digiturvallisuuskoulutussuunnitelman.

Kyselyn kohderyhmä

Kysely on tarkoitettu Ammattiopisto Luovin **koko henkilöstölle** eli sekä ydintehtävän että tukipalvelujen parissa työskenteleville esihenkilöille ja työntekijöille. Kyselyn tuloksia hyödynnetään myöhemmin myös opiskelijoiden digiturvallisuuskoulutuksissa.

Kyselyn vastausaika

Kysely on avoinna **21.11. - 8.12.2022**. Kyselyn vastausaika on pitkä, sillä **toivomme jokaisen henkilöstöön kuuluvan vastaavaan kyselyyn**. Kysely on melko lyhyt ja vastaaminen vie aikaa ainoastaan noin 7 minuuttia.

Kyselyn hyödyntäminen

Kyselyn tuloksia hyödynnetään digiturvallisuuskoulutussuunnitelman laadinnassa sekä erityisesti **keväällä 2023 sisäisesti pidettävien digiturvallisuuskoulutusten suunnittelussa.** Koulutusten tavoitteena on jalkauttaa digiturvaosaamista osaksi koko henkilöstön tavallista työarkea.

Vastaamalla kyselyyn vaikutat osaamisesi kehittämiseen! Jokainen vastaus on erittäin tärkeä, koska luomme digiturvallisuuskoulutukset niiden avulla 😊

Vastauksistanne etukäteen kiittäen

Susanna Kangas
tieto- ja viestintäjohtaja

Mervi Leinonen
IT- ja digipäällikkö

Miia Kauppinen
tiedonhallinnan asiantuntija

AMMATTIOPISTO LUOVI

Koulutustarpeiden kartoitus digiturvallisuudesta

1. Taustatieto

Valitse kumpaan henkilöstöryhmään kuulut

- ◯ Koulutuksen henkilöstö (ydintehtävän parissa työskentelevät esihenkilöt ja työntekijät)
- ◯ Luovi-palvelujen henkilöstö (tukipalveluissa työskentelevät esihenkilöt ja työntekijät)

2. Mistä tietoturvaan ja tietosuojaan liittyvistä asioista kaipaat koulutusta? Voit valita niin monta aihetta kuin haluat.

- ☐ Käyttäjätunnus ja salasana
- ☐ Turvatulostus
- ☐ Tietoverkot
- ☐ Etätyö
- ☐ Henkilötietojen käsittely
- ☐ Tietosuojatermit, kuten rekisterinpitäjä
- ☐ Henkilötunnuksen käsittely
- ☐ Rekisteröidyn oikeudet
- ☐ Monivaiheinen tunnistautuminen
- ☐ Tietoturvapäivitykset
- ☐ Sähköpostin käsittely
- ☐ Huijausviestien tunnistaminen
- ☐ Henkilötietojen käsittelystä informointi (tietosuojaselosteet)
- ☐ Erityiset henkilötietoryhmät
- ☐ Tietosuojaperiaatteet
- ☐ Riskien ja vaikutusten arviointi
- ☐ Jokin muu, mikä?

3. Mistä riskienhallintaan, kyberturvallisuuteen ja jatkuvuuden hallintaan liittyvistä asioista kaipaat koulutusta? Voit valita niin monta aihetta kuin haluat.

- ☐ Riskien tunnistaminen
- ☐ Riskien analysointi
- ☐ Riskien pienentäminen
- ☐ Informaatiovaikuttaminen
- ☐ Sähköisiin häiriötilanteisiin varautuminen
- ☐ Kyberuhkien tunnistaminen
- ☐ Poikkeamien tunnistaminen
- ☐ Poikkeamiin varautuminen eli jatkuvuussuunnittelu
- ☐ Poikkeamista toipuminen
- ☐ Jokin muu, mikä?

Seuraava

1 / 3

AMMATTIOPISTO LUOVI

Koulutustarpeiden kartoitus digiturvallisuudesta

4. Aseta alla olevat koulutusvaihtoehdot paremmuusjärjestykseen siten, että annat arvon 1 sinulle mieluisimmalle ja arvon 2 seuraavaksi parhaalle jne.

Infopaketit puolivuosittain ajankohtaisista asioista	Valitse
Kuukausittaiset lyhyehköt tietoiskut digiturva-asioista	Valitse
Laajat koulutukset, joissa käsitellään tiettyä digiturvakokonaisuutta kerrallaan esimerkiksi jonkin työpaikkakokouksen yhteydessä	Valitse
Yksi koulutus harvoin, jossa käsitellään koko digiturvallisuuskokonaisuus kerralla	Valitse

5. Aseta alla olevat koulutustavat paremmuusjärjestykseen siten, että annat arvon 1 sinulle mieluisimmalle ja arvon 2 seuraavaksi parhaalle tavalle jne.

Toiminnallinen koulutus, jossa tehdään esimerkiksi ryhmätöitä	Valitse
Live-koulutus luentomuotoisena	Valitse
Koulutusympäristö, jossa tehtäviä tehdään itsenäisesti	Valitse
Etäkoulutus Teamssilla	Valitse

Edellinen Seuraava

2 / 3

AMMATTIOPISTO LUOVI

Koulutustarpeiden kartoitus digiturvallisuudesta

6. Kommentoi seuraavat väittämät

	Samaa mieltä	Jokseenkin samaa mieltä	Jokseenkin eri mieltä	Eri mieltä
Ymmärrän, mitä digiturvallisuus tarkoittaa	◯	◯	◯	◯
Koen, että digiturvallisuus on osa työarkeani	◯	◯	◯	◯
Tiedän, mitä seurauksia digiturvallisuuden laiminlyönnillä voi olla	◯	◯	◯	◯
Haluan olla mukana huolehtimassa digiturvallisuudesta	◯	◯	◯	◯

7. Kerro vielä omin sanoin, millainen koulutus saisi sinut motivoitua digiturvallisuusasioista? Ideoi rohkeasti! Miltä kuulostaisi esimerkiksi digiturvallisuusteemainen pakohuone?

Edellinen Lähetä

3 / 3

AMMATTIOPISTO LUOVI

Liite
Sisäinen

Miia Kauppinen

1 (1)

18.11.2022

Liite kyselyyn "Koulutustarpeiden kartoitus digiturvallisuudesta"

Tässä dokumentissa on määritelty keskeisimmät kyselyssä esiintyvät käsitteet, jotka eivät välttämättä ole kaikille vielä tuttuja. Tätä liitettä voi pitää auki toisella välilehdellä kyselyyn vastatessaan, jolloin käsite on helppo tarkistaa.

Monivaiheinen tunnistautuminen
Monivaiheisella tunnistautumisella tarkoitetaan sitä, että henkilöllisyytesi varmistetaan käyttäjätunnuksen ja salasanan lisäksi erillisen turvatiedon, kuten puhelinnumeron avulla. Vaikka rikollinen saisi tietoonsa käyttäjätunnuksesi ja salasanasi, palveluun ei pääse kirjautumaan ilman lisätunnistetta.

Turvatulostus
Monitoimilaitteiden turvatulostus-toiminnon kautta voit tulostaa asiakirjasi yhteiskäytössä oleville laitteille turvallisesti. Turvatulostuksen avulla voit vapauttaa ja tulostaa haluamasi tulosteet vasta noutaessasi ne monitoimilaitteelta.

Erityiset henkilötietoryhmät
Erityiset henkilötietoryhmät määritellään tietosuoja-asetuksessa. Niitä ovat esimerkiksi terveystiedot, rotu tai etninen alkuperä, ammattiliiton jäsenyys, poliittiset mielipiteet ja uskonnollinen tai filosofinen vakaumus

Tietosuojaperiaatteet
Tietosuojaperiaatteet määritellään tietosuoja-asetuksessa. Niitä ovat esimerkiksi henkilötietojen minimointi, tietojen päivitysvelvollisuus sekä luottamuksellinen ja turvallinen henkilötietojen käsittely.

Riskien analysointi
Riskien analysointi tarkoittaa riskien suuruuden ja luonteen arvioimista. Riskien luonteen arviointiin kuuluu riskin todennäköisyyden ja sen vaikutusten määrittely.

Informaatiovaikuttaminen
Informaatiovaikuttaminen on toimintaa, jolla pyritään järjestelmällisesti vaikuttamaan yleiseen mielipiteeseen, ihmisten käyttäytymiseen ja päätöksentekijöihin sekä sitä kautta yhteiskunnan toimintakykyyn.

Sähköiset häiriötilanteet
Sähköiset häiriötilanteet ovat tilanteita, jolloin sähköiset palvelut eivät toimi normaalisti. Sähköiset häiriötilanteet voivat olla ennakoimattomia tai ne voivat olla ennalta tiedossa, kuten ajoitetut sähkökatkot.

Kyberuhkat
Kyberuhka tarkoittaa digitaalisin keinoin toteutettavaa uhkaa, joka kohdistuu digitaaliseen omaisuuteen, järjestelmään tai palveluun. Toteutuessaan kyberuhkan vaikutukset ovat huomattavia sekä taloudellisesti että yhteiskunnallisesti.

Poikkeamien tunnistaminen
Poikkeamien tunnistaminen on normaalioloista poikkeavan toiminnan havaitsemista.

Poikkeamiin varautuminen
Poikkeamiin varautuminen tarkoittaa toimintaa, jolla pyritään ennakoimaan mahdollisia normaalitoimintaa häiritseviä tilanteita ja varautumaan niihin.

Poikkeamista toipuminen
Poikkeamista toipuminen tarkoittaa toiminnan palauttamista normaalitilaan erilaisten häiriötilanteiden jälkeen. Toipumissuunnitelmassa määritellään toimet, joiden avulla tekninen järjestelmä saadaan uudelleen toimivaksi.

Ammattiopisto Luovi
Y-tunnus 0201472-1

Sillmutie 20
83430 Käsämä

Puhelin 040 319 3000
www.luovi.fi

Tutkimushaastattelukysymykset

AMMATTIOPISTO LUOVI

Haastattelurunko
Sisäinen

Miia Kauppinen

15.12.2022

Haastattelu 16.12.2022 keskustellen

Läsnä: **tieto- ja viestintäjohtaja Susanna Kangas, IT- ja digipäällikkö Mervi Leinonen ja tiedonhallinnan asiantuntija Miia Kauppinen**

1. Mitä digiturvallisuus tarkoittaa?
2. Millä tavalla digiturvallisuus on osana työarkeasi?
3. Mitä digiturvallisuuskoulutustarpeita Luovilla on?
4. Mitkä ovat parhaat tavat järjestää koulutuksia?
5. Millainen koulutus saisi sinut motivoitua digiturvallisuusasioista?
6. Mitä mieltä olette ulkopuolisista kouluttajista?
7. Mitkä ovat keskeisiä asioita, joita digiturvallisuuskoulutuksilla tulisi saavuttaa?
8. Miten koulutusten vaikuttavuutta tulisi mitata?
9. Miten digiturvaosaamisen ylläpidosta voisi huolehtia?
10. Millä tavalla haluat olla mukana huolehtimassa digiturvallisuudesta?

Ammattiopisto Luovi
Y-tunnus 0201472-1

Silmutie 20
83430 Käsämä

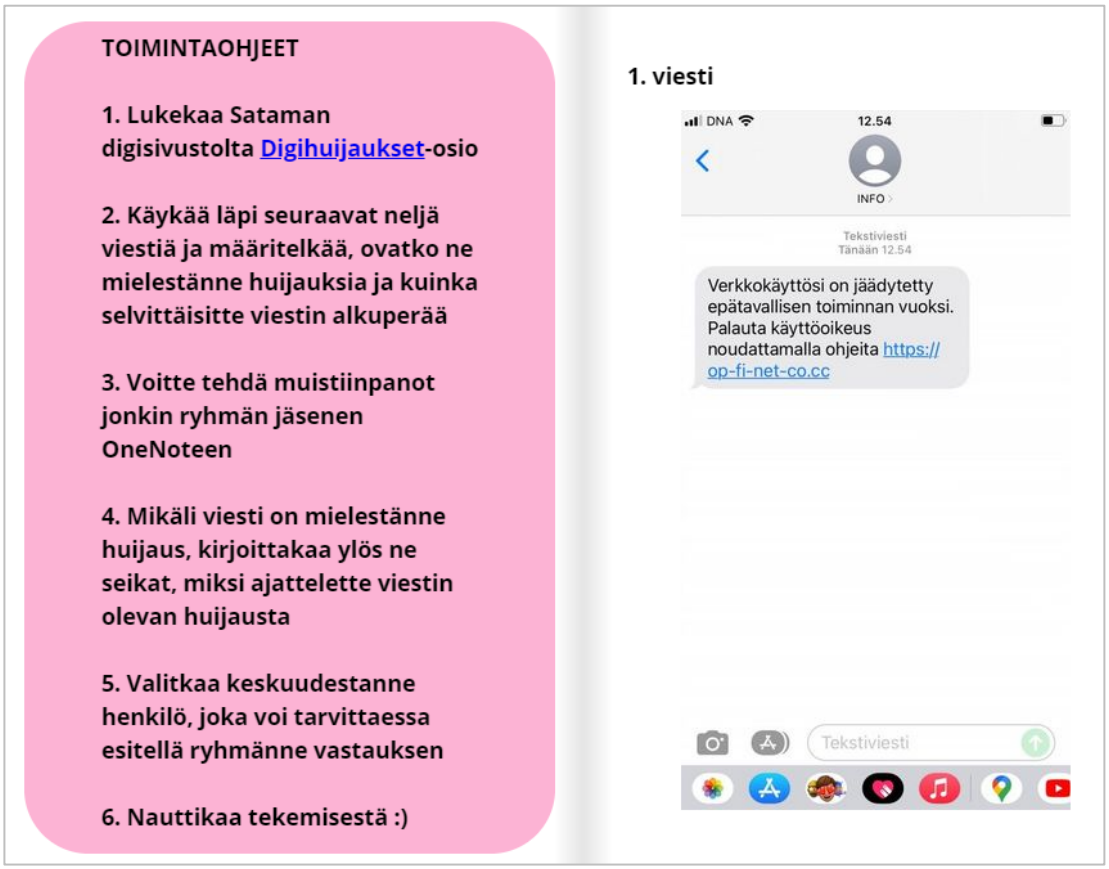
Puhelin 040 319 3000
www.luovi.fi

Esimerkki digiturvakoulutuksen tapausharjoituksesta

Tapausharjoitukset on toteutettu Book Creator -työkalulla, joka on Luovissa käytössä.

Tapausharjoitukset tallennetaan Luovin Sataman (intra) digisivustolle, jossa ne ovat henkilöstön hyödynnettävissä myöhemmin.

Halukkaat voivat suorittaa itsenäisesti ne kolme tapausharjoitusta, joita eivät tehneet digiturvallisuuskoulutuksessa.



2. viesti

Mahdollinen passiivisen tilin hälytys

SP S-pankki <pturner@thejewishnews.com>
Vastaanottaja

Jos tämän viestin näyttämisessä on ongelmia, napsauta tästä, niin viesti avautuu selaimeen.
Lataa kuvat napsauttamalla tätä. Outlook on estänyt joidenkin tässä viestissä olevien kuvien automaattisen lataamisen suojatakseen yksityisyyttäsi.

Mahdollinen passiivisen tilin hälytys

Hei

Meillä on ongelmia nykyisen puhelinnumerosi kanssa. Rekisteröity matkapuhelinnumerosi voi olla vanhentunut tai tilissäsi voi olla ongelmia. Yritämme uudelleen, sillä välin voit päivittää tietosi. Napsauta tätä päivittääksesi tietosi

Painakaa tästä, päivittääksenne tietonne

Et vastaa tähän viestiin. Tähän osoitteeseen lähetettyä postia ei käsitellä.

3. viesti

Toimenpiteitä vaaditaan: Sähköpostisi salasana on vanhentunut

MA Microsoft accounts <microsoft-accounts@microsoftonline.eu.com>
Vastaanottaja Miia Kauppinen

Vastaa | Vastaa kaikille | Lähetä edelleen | ...
ke 31.8.2022 15.19

Jos tämän viestin näyttämisessä on ongelmia, napsauta tästä, niin viesti avautuu selaimeen.

Huomio: Sähköpostisi salasana on vanhentunut. Päivitä se välittömästi.

Microsoft

Salasanan päivitysilmoitus

Käyttäjän ID: miia.kauppinen@luovi.fi

Hei,

Salasana tunnukselle miia.kauppinen@luovi.fi täytyy päivittää. Klikkaa alempaa löytyvää painiketta päivittääksesi sähköpostisi vanhentuneen salasanan, jotta et lukkiudu ulos sähköpostistasi, kalenteristasi sekä yhteystietolistastasi.

PÄIVITÄ SALASANA

Voit päivittää salasanasi tämän linkin kautta vain 12 tuntia tämän sähköpostin saapumisesta.

This is a mandatory service communication. To set your contact preferences for other communications, visit the email communications manager.
This message was sent from and unmonitored email address. Please do not reply to this message.
Privacy | Legal

Neljäs esimerkkiviesti on lähetetty Luovin yhteistyökumppanin nimissä, joten se on jätetty pois tästä esimerkistä.

Esimerkki digiturvallisuusteemaisesta tietokilpailusta

TIETOKILPAILU

DIGITURVALLISUUDESTA HUOLEHTIMINEN KUULUU

A) Digipalveluille
B) KAIKILLE
C) Toimitusjohtajalle
D) Palveluntuottajalle

HYVÄ SALASANA ON

A) Vähintään 32 merkkiä pitkä
B) Erikoismerkkejä
C) SALASANALAUSE, JOSSA ON MYÖS ERIKOISMERKKEJÄ JA MURRESANOJA
D) Numeroita ja kirjaimia

VOIT TEHDÄ TYÖASIOITA

A) TYÖNANTAJAN OSOITTAMILLA LAITTEILLA TYÖNANTAJAN KANSSA SOVITUISSA PAIKOISSA
B) Millä laitteella vaan, missä vaan
C) Yhteiskäyttökoneella kirjastossa
D) Kodin laitteilla kotona

LÄHETÄT SÄHKÖPOSTIA MAHDOLLISILLE YHTEISTYÖKUMPPANEILLE. MIHIN KENTTÄÄN KIRJOITAT VASTAANOTTAJAT?

A) Lähetät jokaiselle erillisen viestin
B) Vastaanottajakenttään
C) Kopiokenttään
D) PIILOKOPIOKENTTÄÄN

HUOMAAT, ETTÄ TYÖPUHELIMESI ON KADONNUT. MITÄ SINUN PITÄISI TEHDÄ?

A) Odotella, että puhelimesi löytyy
B) ILMOITTAA ASIASTA HETI ESIHENKILÖLLESI JA DIGITUKEEN
C) Ilmoittaa asiasta työkavereillesi
D) Jatkaa töitä omalla puhelimellasi

TYÖKAVERI KERTOO OLEVANSA VAKAVASTI SAIRAS. VOIT KERTOA ASIASTA

A) Lähityökaverillesi olosi helpottamiseksi
B) Kaikille muille työkavereillesi
C) Perheellesi
D) ET KENELLEKÄÄN, ELLEI TYÖKAVERI OLE SITÄ ERIKSEEN PYYTÄNYT

MITÄ OIKEUKSIA SOVELLUKSELLE TULEE ANTAA?

A) Millekään sovellukselle ei pidä antaa mitään oikeuksia
B) OIKEUS KÄYTTÄÄ NIITÄ TIETOJA, JOITA SOVELLUKSEN KÄYTTÄMISESSÄ TARVITAAN
C) Oikeus käyttää kaikkia tietoja
D) Oikeus käyttää mikrofonia

KUKA VASTAA HENKILÖTIETOJEN KÄSITTELYN LAINMUKAISUUDESTA LUOVISSA?

A) Tietosuojavastaava
B) Työntekijä
C) JOHTO
D) Tietosuojavaltuutettu

MIKÄ ON PARAS TAPA TUNNISTAA HUIJAUSVIESTI?

A) VIESTIN ÄÄREEN RAUHOITTUMINEN JA TUNNISTUSOHJEEN KERTAUS DIGISIVULTA
B) Rahavaatimus
C) Hoono soomenkeli
D) Kiireeseen vetoaminen

LUOVIN DIGITUKI SOITTAA JA KÄSKEE SINUN KERTOA KÄYTTÄJÄTUNNUKSESI JA SALASANASI PÄIVITYKSEN ASENTAMISEKSI. MITÄ TEET?

A) Lopetat puhelun ja jatkat töitäsi
B) LOPETAT PUHELUN JA TEET POIKKEAMAILMOITUKSEN
C) Annat tunnukset, jotta digituki saa hommansa tehtyä
D) Kysyt, mitä muita tietoja digituki tarvitsee