LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Selvitys hallinnollisen tietoturvallisuuden käytännöistä pelastuslaitoksille

Kaipainen, Lauri

2015 Leppävaara

Laurea-ammattikorkeakoulu
Leppävaara

Selvitys hallinnollisen tietoturvallisuuden käytännöistä pelastuslaitoksille

Kaipainen, Lauri
Turvallisuusala
Opinnäytetyö
Tammikuu, 2015

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Turvallisuusala

Tekijä Lauri Kaipainen

Selvitys hallinnollisen tietoturvallisuuden käytännöistä pelastuslaitoksille

Vuosi 2015 Sivumäärä 66

Hallinnollisen tietoturvallisuuden tarkoituksena on ohjata organisaation tietoturvallisuutta parantavia ja ylläpitäviä toimenpiteitä, jotka suojelevat tiedon yhtenäisyyttä, saatavuutta ja luottamuksellisuutta. Pelastustoimen osalta tiedon hallinnoinnissa tulee ottaa huomioon tiedon suojelun lisäksi sen saatavuus, koska pelastustoimen viranomaiset ovat velvollisia antamaan hallinnoimistaan asiakirjoista tietoa viranomaisten toiminnan julkisuudesta säätävän lain (621/1999) nojalla, jos sille ei ole lainsäädännön asettamaa estettä. Edellä kuvatun avoimuusperiaatteen tarkoituksena on edistää kansanvaltaa antamalla kansalaisille paremmat mahdollisuudet seurata viranomaisten toimintaa.

Opinnäytetyön tarkoituksena on tehdä selvitys hallinnollisen tietoturvallisuuden käytännöistä, minkä tulokset kootaan yhdeksi dokumentiksi. Tämän dokumentin tarkoituksena on antaa ohjeita, miten hallinnollisen tietoturvallisuuden hyviä käytänteitä voitaisiin toteuttaa. Ohjeessa esitetyt toimintatavat perustuvat Valtionhallinnon tieto- ja kyberturvallisuustyöryhmän (VAHTI) julkaisemiin ohjeisiin. Opinnäytetyön toinen tavoite on kartoittaa, mitä mahdollisia hyötyjä Pelastusopisto saisi käyttämällä VAHTI–ohjeita ja Kansallista turvallisuusauditointikriteeristöä (KATAKRI) tietoturvallisuutensa toteuttamisessa.

Selvityksen tilaaja on Pelastusopisto, joka haluaa yhtenäistää pelastuslaitosten tietoturvaohjeistusta, koska pelastuslaitokset ovat ottamassa käyttöön uudet tietojärjestelmät. Nykyisin pelastuslaitokset tukeutuvat tietoturvaohjeissaan sen alueella olevien kuntien ohjeisiin, mikä tarkoittaa epäyhtenäisiä käytänteitä. Pelastusopisto on tämän vuoksi käynnistänyt hankkeen, jonka tarkoituksena on kehittää ja yhtenäistää pelastuslaitosten tietoturvallisuustoimintaa, minkä osana opinnäytetyö on.

Selvitys toteutettiin asiantuntijahaastatteluilla, joista saatua aineistoa käytettiin suoraan tulkintamateriaalina. Haastattelumateriaalista tarkasteltiin asiantuntijoiden lausuntoja ja niissä toistuvia näkemyksiä ja teemoja. Näistä tehtiin johtopäätökset, mitkä ovat asiantuntijoiden tiedon perusteella olennaisia seikkoja hallinnollisen tietoturvallisuuden toteutukseksi. Nämä seikat kirjattiin edellä mainittuun hallinnollisen tietoturvallisuuden toteutusohjeeseen.

Selvityksen mukaan hallinnollinen tietoturvallisuus tulisi toteuttaa tietoturvallisuuden johtamis- ja hallintajärjestelmänä, joka koostuisi seuraavista seikoista: tietoturvapolitiikasta, laatujohtamisen periaatteista, riskienhallintasuunnitelmasta, mittaamisesta ja tiedon luokittelusta. Mikäli yksikin näistä elementeistä puuttuu, hallinnollisen tietoturvallisuuden toteuttamisesta tulee vajavaista, eikä se pystyisi vastaamaan organisaatioon kohdistuviin tietoturvauhkiin.

Selvityksen tuloksia hyödyntämällä Pelastusopisto saa hyvät edellytykset luoda pelastuslaitoksille tietoturvallisuuden hallinta- ja johtamisjärjestelmän. Tämän järjestelmän etuna on, että se mahdollistaa tietoturvallisuustoiminnan muokkaantumisen organisaation muutosten mukana. Toisin sanoen, tietoturvallisuuden johtamis- ja hallintajärjestelmän ansiosta organisaatio pysyy ajan tasalla tietoturvallisuuteensa kohdistuvista riskeistä. Toinen merkittävä etu on, että pelastuslaitokset eivät tämän järjestelmän avulla käyttäisi tietoturvallisuuteen enempää resursseja kuin on välttämätöntä, koska järjestelmä suhteuttaa tietoturvallisuuden laajuuden organisaation toimintaan ja tiedon arvoon.

Asiasanat Hallinnollinen tietoturvallisuus, asiakirja, viranomainen, riskienhallinta ja tieto

Laurea University of Applied Sciences
Leppävaara
Security management

Lauri Kaipainen

Abstract

Information Security Practices for Rescue Departments

Year 2015 Pages 66

The purpose of information security management is to guide and control all actions that maintain and improve organization's information security which means ensuring confidentiality, integrity and availability of data. Rescue departments, as public authorities are obliged to give openly information about their official documents based on legislation. The idea behind this principle is to ensure possibilities for citizens to follow actions of public authorities which is part of democracy.

The goal of this thesis is to carry out a study about practices of information security management. These findings will be assembled into a document that gives instructions and guidelines how these practices could be executed within an organization. These guidelines are made in the accordance of published guidelines by The Government Information Security Management Board (VAHTI).

The research is made for the Emergency Services College (Pelastusopisto) which aims to give common information security instructions for rescue department since they are using shared national databases. For this reason it would be sensible to use shared information security principles made by Emergency Services Collage to ensure a sufficient level of information security nationwide.

The research was conducted through expert interviews. The point was to gather all the data received from the statements and views of information security experts and find repeating themes, which formed the base for the findings. The result gave instructions for rescue departments to implement information security management practices.

According to the findings of the research information security should be executed as an information security management system, which includes following elements: Information security policy, the principles of quality management, risk management plan, measurement and classification of data. If one of these elements is missing, the organization cannot maintain its information security efficiently to defend against information security threats.

By utilizing these findings the Emergency Services College would gain a basis to create common information security management system for the rescue departments. Two advantages of the system comes from its ability to be modified for purposes of rescue departments and keep up with changing information security threats. The second benefit would be that organization would not use more resources than necessary to achieve a sufficient level of security.

Keywords Information security management, official document, authority, risk management and information

Sisällys

1 Johdanto

Tämän opinnäytetyön tarkoituksena on tehdä selvitys Pelastusopistolle hallinnollisen tietoturvallisuuden käytännöistä. Pelastusopisto haluaa käyttöönsä käytännöt, joita se soveltaisi tehdessään pelastuslaitoksille yhtenäistä hallinnollisen tietoturvallisuuden ohjeistusta. Pelastuslaitokset ovat ottamassa käyttöön uudet tietojärjestelmät, jotka tulevat olemaan kaikkien pelastuslaitosten käytössä. Tämän vuoksi Pelastusopisto näki tarkoituksenmukaiseksi, että pelastuslaitosten tietoturvallisuusohjeet olisivat yhtenäiset.

Pelastusopisto on suunnitellut käyttävänsä pelastuslaitosten tietoturvallisuutta kehittävässä hankkeessa apunaan KATAKRIa ja VAHTI-ohjeita. Selvityksen toinen tavoite on selvittää, mitä etuja Pelastusopisto saavuttaisi käyttämällä näitä kyseisiä asiakirjoja tietoturvallisuutensa kehittämisessä.

Tietojen käsittelyssä ja turvallisuustoiminnassa on noudatettava lainsäädäntöä, minkä vuoksi selvityksessä on otettava huomioon sen asettamat vaatimukset pelastuslaitokselle, joka on julkinen viranomainen, jonka toimintaan vaikuttavat muun muassa laki viranomaisten toiminnan julkisuudesta (621/1999). Julkisella viranomaisella tarkoitetaan valtion tai kuntien ylläpitämiä virastoja ja liikelaitoksia (Laki viranomaisten toiminnan julkisuudesta 621/1999, 4 §).

Alueellinen pelastustoimen toteuttaminen on kuntien vastuulla, minkä vuoksi pelastuslaitokset ovat kunnan viranomaisia (Kuntaliitto, 2014). Lainsäädännön asettamien vaatimusten tunteminen on tässä selvityksessä tarpeellista, jotta selvityksessä saataisiin käsitys, millaista tietoa pelastuslaitoksen viranomaiset käsittelevät työssään ja mitä lainsäädännön tuomia vaatimuksia siihen liittyy.

Tämän opinnäytetyön tuloksista Pelastusopisto hyötyy kolmella tavalla:

1) Pelastusopisto saa selvityksen, mitä seikkoja hallinnollisen tietoturvallisuuden tulee sisältää, jotta se olisi mahdollisimman toimiva.
2) Kartoituksen niistä eduista, joita pelastuslaitokset saisivat käyttämällä VAHTIa ja KATAKRIa hallinnollisen tietoturvallisuutensa kehittämiseen.
3) Pelastusopisto saa selkeät ohjeet hallinnollisen tietoturvallisuuden toteuttamisesta, jonka rakenne perustuu selvityksessä tehtyihin havaintoihin (Liite 2). Ohjeen sisältö perustuu VAHTI-työryhmän ohjeisiin.

Selvityksessä käytetään kirjallisuuskatsausta, jonka tarkoituksena on antaa vertailukohta asiantuntijoiden näkemyksille kartoittamalla kirjallisuudessa esitettyjä näkemyksiä hallinnollisen tietoturvallisuuden toteuttamisesta. Selvityksessä käytetty kirjallisuus on

englanninkielistä tietoturvallisuutta käsittelevää kirjallisuutta, jonka kirjoittajat ovat ansioituneita tietoturvallisuuden ammattilaisia, tai kirjojen näkemykset edustavat arvostettujen organisaatioiden näkemyksiä hallinnollisesta tietoturvallisuudesta.

Selvitys toteutettiin asiantuntijahaastatteluilla, joiden tarkoituksena on kerätä asiantuntijoiden näkemyksiä hallinnollisen tietoturvallisuuden hyvistä käytännöistä. Asiantuntijat valittiin niin, että he edustavat tasapuolisesti sekä VAHTIa että KATAKRIA, jotta haastatteluilla voidaan kerätä tietoa kumpaakin selvitystavoitetta varten.

Selvityksen tuloksista tehdään sisältöpohja, jota Pelastusopisto voi soveltaa hallinnollisen tietoturvallisuuden toteuttamiseksi. Opinnäytetyössä on liitteenä ohje, jonka avulla Pelastusopisto voi ryhtyä suunnittelemaan pelastuslaitosten hallinnollisen tietoturvallisuuden ohjeistuksen toteuttamista ja mitä se pitää sisällään. Toteutusohjeet perustuvat VAHTI-ohjeisiin. Toteutusohje on esitelty liitteessä 2.

2 Keskeiset käsitteet

Hallinnollinen tietoturvallisuus: Tietoturvallisuuden osa-alue, joka käsittää toiminta-linjaukset, periaatteet, organisaatiojärjestelyt, henkilöstön tehtävien ja vastuiden määrittelyn sekä tietoturvallisuuteen tähtäävän ohjeistuksen, koulutuksen ja valvonnan. (Helenius 2005, 60.)

Tieto(data): Data on koneellisesti käsiteltävää, viestittävää ja muokattavaa tietoa.

Huomautus: Yleiskielessä sanojen data, informaatio (engl. information) ja tieto (engl. knowledge) käytössä ei ole useinkaan selvää eroa. Tieto-sanalla voidaan viitata myös dataan ja informaatioon. (Sanastokeskus 2014)

Tieto(informaatio): Esitettyjä tai löydettyjä faktoja asioista tai henkilöistä. (Oxfordin verkkotietosanakirja 2014)

Riskienhallinta: Toiminta, joka pyrkii hallitsemaan ja ohjaamaan organisaatioon kohdistuvien riskien aiheuttamaa epävarmuutta. (ISO 31004 Riskienhallintastandardi)

Asiakirja: Laissa asiakirjalla tarkoitetaan kirjallisen ja kuvallisen esityksen lisäksi sellaista käyttönsä vuoksi yhteen kuuluviksi tarkoitetuista merkeistä muodostuvaa tiettyä kohdetta tai asiaa koskevaa viestiä, joka on saatavissa selville vain automaattisen tietojenkäsittelyn tai äänen- ja kuvantoistolaitteiden taikka muiden apuvälineiden avulla. (Laki viranomaisten toiminnan julkisuudesta 621/1999)

Viranomainen: Viranomaisia ovat julkisia tehtäviä toteuttavia ja julkista valtaa käyttäviä yhteisöjä, laitoksia, säätiöitä ja yksityishenkilöitä. (Mäenpää 2003, 281)

3 Tietoturvallisuus ja sen merkitys pelastustoimelle

3.1 Tietoturvallisuus

Vielä noin 20 vuotta sitten tietoturvallisuutta käsiteltiin tietokoneiden virusturvallisuuden kautta, mikä tarkoitti tietokoneiden suojaamista vahingollisilta tietokoneviruksilta, kuten madoilta ja troijalaisilta. Ajan kuluessa tietokoneet ovat pienentyneet, ja kannettavien tietokoneiden ansiosta työntekijät pystyivät käsittelemään työssään tarvitsemaansa tietoa työpaikan ulkopuolella. Tämän kehityksen vuoksi kehittyi tietoturvallisuuden käsite, koska nyt suojeltavana kohteena on tieto sitä käsittelevän laitteen sijaan. Tietoturvan ensisijaiseksi tehtäväksi muodostui tiedon suojaaminen. (Whitman 2008, 3-4)

Nykyisin tiedosta on tullut entistä arvokkaampaa organisaatioille. Tämän vuoksi tietoturvallisuuden tehtävänä on varmistaa, että organisaation käsittelemä tieto ja tietoon pohjautuvat palvelut ovat suojattuja, ja niiden toimivuus on varmistettu.(Cazemier 2010, 9-10.) Tietoturvallisuus koostuu tietoturvallisuuden johtamisesta, tietoverkkojen turvallisuudesta, laite- ja dataturvallisuudesta, ja näitä ohjataan politiikan kautta. (Whitman 2008, 5)

Tietoturvallisuus koostuu luottamuksellisuudesta, yhtenäisyydestä ja saatavuudesta. Asiasta käytetään kansainvälisesti lyhennettä C.I.A (confidentiality, integrity availability). Tiedon luottamuksellisuus tarkoittaa tiedon näkemisen ja käsittelemisen rajoittamista. Organisaation on ohjeistettava, ketkä käsittelevät tietoa, millaista tietoa kukin saa käsitellä ja millä ehdoilla. Organisaatiossa on kiinnitettävä myös huomiota, kuinka suuret valtuudet henkilöllä on tiedon käsittelemisessä. Saako esimerkiksi työntekijä puhua tiedon sisällöstä tai tehdä siitä fyysisiä ja digitaalisia kopioita? Olennaisinta on näiden vaatimusten valvonta. (Phleeger 2007, 9-10) Henkilötietolain (523/1999) 32 § velvoittaa rekisterin ylläpitäjää toteuttamaan tarpeelliset tekniset ja hallinnolliset toimenpiteet, jotta henkilötietoja voidaan suojata asiattomalta paljastumiselta.

Tiedon yhtenäisyyttä on vaikeampi määritellä, sillä tämän sanan tarkoitus on riippuvainen kontekstista. Yhtenäisyys voi tarkoittaa muun muassa tiedon täsmällisyyttä, tarkkuutta, johdonmukaisuutta tai tiedon muokkaamisen rajoittamista. Käytännössä yhtenäisyys on luonteeltaan varsin lähellä luottamuksellisuuden kanssa. (Phleeger 2007, 11) Henkilötietolain (523/1999) 9 § asettaa tiedon säilyttämiselle virheettömyysvaatimuksen, joka velvoittaa rekisterinpitäjää huolehtimaan henkilötietojen tiedon oikeudellisuudesta ja täsmällisyydestä.

Tiedon saatavuus tarkoittaa, että organisaation käsittelemä tieto on tarvittaessa saatavilla esimerkiksi tietojärjestelmästä. Yrityksessä tämä voi tarkoittaa esimerkiksi verkkopalveluun

kirjautumista. Henkilörekisterin ylläpitäjälle saatavuus tarkoittaa rekisteröidyn henkilön mahdollisuutta nähdä ja tarkistaa itseään koskevat henkilötiedot järjestelmästä. (Phleeger 2007, 12-13) Tiedon saatavuudesta määritellään henkilötietolain (523/1999) 26 §, jonka mukaan jokaisella on oikeus tarkistaa itseään koskevat tiedot salassapitosäännösten estämättä.

Viranomaisten toiminnan julkisuudesta (621/1999) annetun lain 18 § velvoittaa viranomaisia hyvään tiedonhallintatapaan, jonka mukaan viranomaisten on säilytettävä tietoa niin, että sen luottamuksellisuus, käytettävyys ja saatavuus eivät vahingoitu.

Viranomaisten tiedonkäsittelyssä saatavuus yhdistetään käytettävyyden kanssa. Lain taustaajatuksena on, että kansalaisilla olisi hyvät mahdollisuudet saada tietoa asiakirjoista, ja heille annetaan edellytykset tehdä niin. Hyvään tiedonhallintatapaan sisältyy olennaisena osana tiedon eheyden ja laadun varmistaminen, mikä tarkoittaa tiedon vahingollisten, tahallisten, tahattomien ja asiattomien muutosten estämistä. Luottamuksellisuus määritetään henkilön oikeuksien suojaamiseksi tiedon siirrossa ja käsittelyssä. Salaiseksi määritettyä tietoa eivät käsittele muut kuin asiaan kuuluvat henkilöt. Periaate koskee myös henkilötietoja. (Valtiovarainministeriön työryhmämuistioita 11/2000)

Tietoturvallisuuden osa-alueita on laajennettu nykypäivänä, koska on katsottu, että pelkästään C.I.A. ei ole riittävän kattava kuvailemaan tietoturvallisuuden nykyhaasteita, minkä vuoksi C.I.A:n rinnalle on nostettu P.I.A. (privacy, identification, authentication) eli yksityisyys, tunnistaminen ja todentaminen. Yksityisyys on noussut tietoturvallisuuden uudeksi näkökulmaksi, koska esimerkiksi asiakkaiden tietoja käytetään laajemmin markkinoissa, ja ovat tietoturvavarkauksien kohteina. Lisäksi tietojärjestelmät sisältävät nykyisin henkilöiden maksutietoja. (Whitman 2010, 8)

Yksityisyys on tärkeä arvo, jota suojataan perustuslain (731/1999) 10 §:ssä. Sen mukaan jokaisen yksityisyys on suojattu. Tarkemmin yksityisyyden suojasta säädetään henkilötietolaissa (523/1999), joka määrittää henkilötiedoiksi sellaisen tiedon, josta voidaan tunnistaa muun muassa henkilön ominaisuuksia.

Tunnistaminen tarkoittaa sitä, että järjestelmä tai henkilö kykenee tunnistamaan henkilön, joka haluaa käsitellä dataa. Käyttäjän tunnistaminen tietojärjestelmässä yleensä toteutetaan käyttäjänimellä taikka muulla henkilötunnisteella. Todentaminen tarkoittaa tietoturvallisuudessa käyttäjän henkilöllisyyden todistamista, kun hän kirjautuu järjestelmään. Tämä voidaan toteuttaa esimerkiksi sirullisella kortilla, joka käyttää kryptografista menetelmää vahvistamaan käyttäjän henkilöllisyyden. (Whitman 2010, 9) Kryptografia tarkoittaa tiedon salaamista matemaattisella kaavalla, joka on laskettavissa vain

yhteen suuntaan. Menetelmää käytetään muun muassa pankkikorteissa salamaan nosto- tai maksutapahtumaan tarvittavat tiedot. (Lek 2012, 7)

Seuraavaksi esittelen kaksi esimerkkiä tietoturvallisuuden pettämisestä. S-ryhmän kanta-asiakaskortti kerää tietoa asiakkaidensa ostokäyttäytymisestä, jotta ketjun kaupat pystyisivät kohdentamaan palveluitaan ja markkinointiaan tarkemmin. Kanta-asiakaskortti tallentaa tietoja muun muassa tuotteista, joita kanta-asiakas on ostanut. Näitä tietoja voidaan käyttää kohdistettuun suoramarkkinointiin. On kuitenkin muistettava, että S-ryhmä ei käsittele asiakkaan ostotietoja suoramarkkinointiin, jos asiakas sen erikseen kieltää. (S-ryhmän asiakasomistaja- ja asiakasomistajarekisteri 2014)

Sonyn tietojärjestelmiin tehtiin murto 17.-19.9.2011, jolloin järjestelmään murtautunut hakkeri sai haltuunsa Sonyn Online Entertainment-palveluun rekisteröityjen käyttäjien tietoja, kuten sähköpostiosoitteen ja ostohistorian. Pelkästään Suomessa Sonyn online entertaimentiin oli rekisteröitynyt arviolta 300 000 henkilöä. Arviolta 12700 palvelun käyttäjän luottotiedot menetettiin. (Viestintävirasto 2011)

3.2 Hallinnollinen tietoturvallisuus

Tietohallinnon tarkoituksena on ohjata organisaation tietovirtaa, mikä tarkoittaa tärkeän tiedon tunnistamista ja luokittelua. Sen on annettava ohjeet tiedon käsittelystä, säilyttämisestä ja hävittämisestä. Tietohallinto on myös vastuussa tiedon suojaamisesta, turvallisuudesta ja yksityisyydestä. Tietohallinnon tulee tietää ne lainsäädännön vaatimukset, jotka vaikuttavat sen hallitseman tiedon käsittelyyn, jotta organisaation toiminta olisi lainmukaista. Tietohallinto on siis se keino, millä organisaatio ylläpitää turvallisuutta, toimii lain mukaisesti ja osoittaa toimintansa eettisyyden. (Smallwood 2014, 5-7)

Tietohallinnon tiedonkäsittelypolitiikan ja toimintaohjelman tulee antaa ohjeita tiedon käsittelemiselle strategisella tasolla. Tiedon käsittelyssä käytettävä teknologia ja järjestelmät muuttuvat melko nopeasti, jonka vuoksi tietohallinnon periaatteiden tulisi olla käyttökelpoisia, vaikka tiedon käsittelyssä, määrässä tai tietojärjestelmässä ilmenisi muutoksia. Ohjeistuksen strategisuus vaatii myös sitä, että tietohallinnon toimintaympäristöä ja sen muutoksia tarkkaillaan jatkuvasti. Tämä tarkoittaa lähinnä lainsäädännön seuraamista. Tietohallinnon parantaminen on merkityksellistä mutta kysymys on, miten paljon ja miksi? Kysymystä voidaan lähestyä seuraavista näkökulmista:

1) Organisaation ei ole järkevää säilyttää kaikkea mahdollista tietoa tai poistaa kaikkea mahdollista tietoa. (Smallwood 2014, 7) Pelastuslaitoksille on annettu lainsäädännössä vaatimuksia tiedonsäilyttämisajasta. Laki viranomaisten toiminnan

julkisuudesta (621/1999) määrittää, että yleinen salassapitoaika on 25 vuotta (Laki viranomaisten toiminnan julkisuudesta 621/1999, 31 §).

2) Hyvät tietohallinnolliset ohjeistukset selkeyttävät työntekijöille tiedon käsittelyä, mikä johtaa tehokkuuteen ja käsittelyvirheiden vähentymiseen. (Smallwood 2014, 8) Esimerkiksi Pelastuslaitosten ylläpitämien henkilörekistereiden tulee toteuttaa arkistolain (831/1994) ja henkilötietolain (523/1999) vaatimukset viranomaisia koskevan lainsäädännön lisäksi.

3) Hyvin tehdyllä ja jalkautetulla tietohallinnolla pystytään hallitsemaan tiedon käsittelyyn liittyviä riskejä. (Smallwood 2014, 8)

Luotettavuus on hyvän tietohallinnon perusta. Tietohallinnon julkaiseman tietoturvapolitiikan ja tiedonkäsittelyohjeiden tulisi edistää tiedon käsittelyn luotettavuutta, yhtenäisyyttä, turvallisuutta, tarkkuutta ja laatua. Nämä edellä mainitut elementit ovat luotettavan tietohallinnon perusteet, jotka tukevat luotettavuuden saavuttamista.

Vuonna 2009 Kansainvälinen tieto- ja rekisterihallinnon ammattilaisten yhdistys ARMA julkaisi kahdeksan kohdan listan hyvistä asiakirjan ylläpidon periaatteista (Generally accepted record keeping principles) Periaatteiden tarkoituksena on edistää hyvää tietohallintokulttuuria. ARMA on vuonna 1955 perustettu kansainvälinen yhdistys, jonka tarkoituksena on edistää hyvää tiedon hallintatapaa. Sen jäsenet koostuvat tietohallinnon, konsultoinnin ja valtionhallinnon ammattilaisista. ARMAlla on 27,000 jäsentä yli 30 maassa (ARMA international 2014).

1) Luotettavuus (Accountability): Organisaation johdon on tuettava tietohallinnon kehittämistä, jotta tietohallinto saa tarpeelliset valtuudet toteuttaa ja jalkauttaa tietohallinto-ohjeita ja periaatteita.
2) Avoimuus (Transparency): Tietohallintopolitiikan ja sen periaatteiden tulee olla jokaisen työntekijän nähtävillä. Tarpeen tullen myös sidosryhmille on annettava mahdollisuus tutustua tietohallinnon ohjeisiin.
3) Loukkaamattomuus (Integrity): Tietoja käsitellään niin, että tiedon luotettavuus, aitous ja turvallisuus säilyvät, ottaen huomioon tiedon arvon ja merkityksellisyyden
4) Suojelu (Protection): Organisaation tulee suojata sellaista tietoa, mikä on yksityistä, luottamuksellista, salaista taikka merkittävää toiminnan jatkuvuudelle
5) Laillisuus (Compliance): Organisaation tietohallinto-ohjeiden tulee kiinnittää huomiota lain asettamiin vaatimuksiin tiedon käsittelyssä.

6) Saatavuus (Availability): Tieto on säilytettävä niin, että se on käyttäjän saatavilla kohtuullisessa ajassa. Tiedon säilyttäjän tulee myös antaa tarkoituksenmukaiset keinot tiedon saamiseksi ja käsittelyksi.
7) Säilyvyys (Retantion): Organisaation tulee pitää huolta tiedon säilyvyydestä, joka päätetään tiedon arvon mukaan. Säilytyksessä tulee ottaa huomioon lain asettamat vaatimukset käsitellylle tiedolle.
8) Luopuminen (Disposition): Organisaatiolla tulee olla tiedon hävittämissuunnitelma, joka ottaa huomioon tiedon arvon, kun tietoa hävitetään. (Smallwood 2014, 27-28)

3.3 Tietoturvapolitiikka

Politiikka yleisesti määritellään suunnitelmaksi toimintatavasta esimerkiksi valtion hallinnossa tai yrityksessä. Sen tarkoitus on vaikuttaa ja määrittää minkälaisia päätöksiä ja toimenpiteitä tehdään. Politiikka edustaa organisaation johdon näkemystä ohjattavasta asiasta (Whitman 2008, 111). Edellisen väittämän ymmärtämisen vuoksi on huomattava, että politiikka on tässä tapauksessa käännetty suoraan sanasta policy, joka tarkoittaa toimintaperiaatetta, jonka mukaan yksilö tai organisaatio toimii. (Oxfordin verkkotietosanakirja, 2014). Suomen kielessä politiikka tarkoittaa näkemystä tai ideologiaa siitä, miten yhteiskunnan asioita ja valtioiden välisiä suhteita tulisi hoitaa (MOT, Gummerus, Uusi Suomen kielen sanakirja 2014). ISO 27000 standardi määrittää politiikan organisaation kokonaisvaltaiseksi päätökseksi ja aikeeksi, jonka johto on määrittänyt. (ISO 27000 2012, 7)

Whitmanin määritelmästä voidaan johtaa ajatus, että tietoturvapolitiikka on johdon kirjallisesti osoittama tahtotila tietoturvallisuuden toteuttamisesta. Tietoturvapolitiikan tulee antaa raamit, johon tietoturvallisuuden toteuttamisen ohjeet rajautuvat ja tukeutuvat. Tämä tarkoittaa käytännössä sitä, että organisaatio on määrittänyt, millaista tietoa halutaan suojella. Tietoturvapolitiikan onnistuminen edellyttää organisaation johdon tukea, joka on merkityksellistä, koska vain silloin tietoturvapolitiikalla ja sen linjauksilla on takanaan tarvittavat resurssit ja auktoriteetti toteutuakseen. Onnistunut tietoturvapolitiikka tukee organisaation tavoitteita ja määrittää vastuut tietoturvallisuuden toteuttamisesta ja ottaa huomioon tiedon käsittelijät ja omistajat. (Whitman 2008,108-111)

Tietoturvapolitiikka on korkeimman tason periaate, joka määrittää organisaation tietoturvallisuuden tavoitteet ja periaatteet. Organisaation tulee ottaa kantaa tietoturvapolitiikassaan seuraaviin asioihin: kuka saa käsitellä tietoa, millaisia tietoresursseja kukin henkilö voi tai saa käsitellä, millä perusteilla tietoa voi käsitellä ja millaisilla valtuuksilla käyttäjä voi käsitellä tietoa. Näiden kysymysten ratkaiseminen on edellytys sille, että tietohallinto hallitsee tietoa johdonmukaisesti ja organisoidusti. Tiedon käsittelyn

hallitsemisen ja ohjeistamisen tarkoitus on estää riskien eskaloituminen ja rajoittaa toteutuneen riskin vaikutuksia organisaation toimintaan. (Phleeger 2007, 510-511)

Hallinnollisessa tietoturvallisuudessa ohjeet jakautuvat kahteen tasoon: periaatteelliset ohjeet ja käytännön ohjeet. Periaatteellisten ohjeiden, kuten tietoturvapolitiikan, tulee antaa nimensä mukaisesti periaatteelliset raamit toiminnalle. Käytännön ohjeiden tulee ottaa kantaa yksittäiseen työtehtävään. (Cazemier 2010, 100)

Tietoturvapolitiikka ohjaa käytännön työtä sääntéleviä ohjeita, joita ovat esimerkiksi henkilötietojen poisto- ja tallentamisohje. Nämä työohjeet ovat tarpeellisia, jotta työntekijä saisi konkreettisen käsityksen, miten hänen tulee käsitellä tietoa työssään. Tämän vuoksi tietoturvapolitiikan on otettava kantaa sen suhteeseen alemman tason ohjeisiin johdonmukaisuuden vuoksi. (Cazemier 2010, 100-101) Esimerkiksi, jos tietoturvapolitiikka korostaa käyttäjien tunnistamista, kaikki toimenpiteet noudattavat kyseistä periaatetta vaikka se vaikuttaisi palvelun nopeuteen.

Tietoturvapolitiikka on kirjoitettava väljästi, jotta se olisi kaikenkattava. Tämä tarkoittaa sitä, että politiikka ei ole sidoksissa tiettyyn tietoon tai järjestelmään, mikä johtaisi politiikan toistuvaan muokkaamiseen. Tämän välttämiseksi politiikan tulee tunnistaa tiedon luonne esimerkiksi, millaiset lait vaikuttavat tiedon käsittelyyn, ja miksi organisaatio pitää hallussaan tietoa, jota pitää suojella. (Phleeger 2007, 547-548) Suomessa pelastusviranomaisten tiedonkäsittelyä ohjaa muun muassa laki viranomaisten toiminnan julkisuudesta (621/1999), joka määrittää viranomaisten tiedonantovelvollisuuden. Arkistolaki (831/1994) taasen velvoittaa asiakirjojen säilytyksestä niin sanottua arkistosuunnitelmaa, joka ottaa kantaa, miten tietoa säilytetään ja poistetaan. Lisätietoa lainsäädännön vaikutuksista viranomaisten tiedonkäsittelyyn on luvussa 4.

Tietoturvapolitiikan tulisi pystyä ohjeistamaan uusia työntekijöitä ja antaa koko organisaatiolle käsityksen tietoturvallisuuden toteuttamiseen liittyvistä vastuista kaikilla tasoilla. Politiikka toimii myös ulospäin, sillä se antaa tiedon omistajille ja sidosryhmille konkreettisen käsityksen organisaation periaatteista tiedon suojaamiseksi. (Phleeger 2007, 549-550)

Hyvin tehty tietoturvapolitiikka perustuu organisaation toimintaan kohdistuvien riskien kartoitukseen, jotta tietoturvapolitiikan periaatteet kohdistuvat sellaiseen tietoon, jonka suojaamisella on merkitystä organisaatiolle. Kaikkea tietoa ei voida suojella, koska se vaikeuttaisi organisaation toimintaa ja tuhlaisi resursseja. (Whitman 2008, 130)

Tietoturvapolitiikan asettamat vaatimukset tulisi myös suhteuttaa organisaation muihin ohjeisiin ja käytäntöihin esimerkiksi miten ja minne yrityksen tärkeitä dokumentteja arkistoidaan. Kun ohjeiden suhteutus on otettu huomioon, tietoturvapolitiikka saa todennäköisemmin organisaation johdon hyväksynnän, koska siitä tulee tarkoituksenmukainen ja sitä kautta ymmärrettävä. (Whitman 2008, 131)

Tietoturvapolitiikan asettamien periaatteiden tulee olla luonnollinen osa organisaation prosesseja, ja henkilökunnan tulisi sitoutua sen periaatteisiin. Tämä voidaan varmistaa esimerkiksi työntekijän allekirjoituksella, jossa hän vakuuttaa lukeneensa tietoturvapolitiikan ja tietoturvallisuuteen liittyvät ohjeet. Tämä mahdollistaa sen, että työntekijä ei voi kiistää tietoisuuttaan ohjeen olemassaolosta vahingon tapahtuessa. (Whitman 2008, 132)

Toisaalta, verrattuna Whitmanin (2008) ajatukseen, ISO 72001-standardi korostaa tietoturvallisuuteen panostamisen olevan strateginen päätös, minkä vuoksi tietoturvallisuuden suunnittelu, toteuttaminen ja seuranta ovat erityisesti johdon vastuulla. Heidän tulee tehdä tietoturvallisuuden takaavat toimenpiteet luonnolliseksi osaksi organisaation työtehtäviä. Tämän kautta työntekijöiden erillinen sitouttaminen ei ole tavallaan keskeisessä asemassa, koska tietoturva ei ole erillinen prosessi. (ISO 72001, 14,17)

4 Lainsäädännön asettamat vaatimukset pelastusviranomaisten tiedonkäsittelylle

4.1 Laki viranomaisten toiminnan julkisuudesta

Hallituksen esityksessä (30/1998) selvennetään, että viranomaistoimintaa koskevan julkisuusperiaatteen tarkoituksena on, että kansalaisilla on mahdollisuus saada tietoa viranomaisen toiminnasta asiakirjojen avulla. Tämän kaltainen avoimuus perustuu ajatukseen, että yhteisön on voitava käydä avointa keskustelua julkisen vallan käytöstä ja hallinnoinnista. Esityksen mukaan julkisuusperiaate viranomaisten asiakirjoille on tarpeellinen, sillä julkishallinto on kehittynyt suuremmiksi ja monimutkaisemmiksi kokonaisuuksiksi. (HE 30/1998, 42)

Jokaisella on oikeus saada tietoa julkisesta asiakirjasta. Asiakirjan pyytäjän ei tarvitse myöskään perustella tai kertoa, mihin asiakirjaa aiotaan käyttää tai miksi asiakirjasta halutaan tietoa. Edellä mainitut periaatteet johtuvat näkemyksestä, jonka mukaan viranomaisten asiakirjojen julkisuus on objektiivinen arvo. (Mäenpää 2003, 287.)

Asiakirjoilla viitataan viranomaisten ja virkamiesten hallussa olevaan tietoon tallennustavasta riippumatta. Viranomaiset ovat julkisia tehtäviä toteuttavia ja julkista valtaa käyttäviä yhteisöjä, laitoksia, säätiöitä ja yksityishenkilöitä. Viranomaisten asiakirjoiksi määritetään

viranomaisen tuottamat asiakirjat ja ne asiakirjat, jotka se on saanut haltuunsa virkaansa tehdessä. On muistettava, että viranomaiselle toimitetusta asiakirjasta ei tule suoraan julkista, jos lainsäädäntö määrittää tiedon luottamukselliseksi. Näin on esimerkiksi henkilötietojen kanssa, joita viranomainen säilyttää luottamuksellisena henkilötietolain (523/1999) vaatimuksesta. (Mäenpää 2003, 281-282)

Viranomaisasiakirjoista julkisuusperiaatteen ulkopuolelle jäävät keskeneräiset asiakirjat ja sisäisessä työskentelyssä syntyneet asiakirjat. Lakia viranomaisten toiminnan julkisuudesta (621/1999) valmisteltaessa on katsottu, että viranomaisten sisäisen viestinnän ei tule olla julkista, jotta sen toiminta olisi sujuvaa. Viranomainen voi antaa tietoa keskeneräisistä asiakirjoista oman harkintansa mukaan. (Mäenpää 2003, 283)

Viranomaisten toiminnan julkisuudesta annetun lain (621/1999) tarkoituksena on edistää hyvää tiedonhallintatapaa. Tämä merkitsee sitä, että viranomaistoiminnasta on saatava tietoa, ja viranomaisen on säilytettävä, käsiteltävä ja suojattava tietoa asianmukaisesti, jotta tiedon eheys, luottamuksellisuus ja yhtenäisyys säilyisivät. Kyseisessä laissa asetetaan erityisesti seuraavia velvoitteita viranomaisille:

1) Varmistaa, että julkiset asiakirjat ovat vaivattomasti löydettävissä pitämällä niistä luetteloa;
2) Pitää saatavilla kuvaukset ylläpitämistään tietojärjestelmistä ja siitä, mitä tietoa ne sisältävät, ellei laissa todeta toisin;
3) Selvittää, miten hallinnolliset, lainsäädännölliset ja tekniset uudistukset tulevat vaikuttamaan asiakirjojen säilytykseen ja reagoida niin, että asiakirjojen laatu ja turvallisuus on taattu;
4) Suunnittelemaan asiakirja- ja tietohallintonsa niin, että se varmistaa tiedon laadun, turvallisuuden ja vaivattoman käsittelyn. Viranomaisen on suunniteltava myös tiedon huolellinen hävittäminen. Toimenpiteissä tulee ottaa huomioon käsiteltävän tiedon laatu ja arvo, jotka määrittävät turvallisuustoimenpiteiden tason;
5) Viranomaisen on huolehdittava asiakirjoja ja tietoa käsittelevän henkilökunnan koulutuksesta, jolla varmistetaan tiedon oikea käsittely noudattaen hyvää tiedonhallintatapaa. (Laki viranomaisten toiminnan julkisuudesta 621/1999, 18 §)

Viranomainen voi asettaa asiakirjan salaiseksi vain lain perusteella, ja sen salassapito tulee perustua tiedon sisältöön ja välttämättömään tarpeeseen. Tämä tarkoittaa, että viranomaisen on aina perusteltava lailla tiedon salaiseksi asettaminen. Laki viranomaisten toiminnan julkisuudesta (621/1999). (Mäenpää 2003, 295)

Salassapito voidaan julistaa suojaamaan kolmea seikkaa: yksityistä, yleistä ja julkisyhteisön etua. Yksityinen etu kohdistuu henkilöiden yksityisyyden suojaan ja oikeushenkilöiden osalta

liike- ja ammattisalaisuuksiin. Yksityinen etu pyrkii eritoten suojaamaan tietoja yksityisen oikeushenkilön elinoloista, taloudellisesta asemasta ja niin edelleen. (Mäenpää 2003, 296)

Toinen kategoria on yleinen etu, joka perustelee salassapidon esimerkiksi viranomaisvalvonnan toteuttamisella. Ajatus on se, että tiedon julkisuus voisi vaarantaa tavoitteiden saavuttamisen. Esimerkiksi viranomaisten tiedot uhanalaisista eläin- ja kasvilajeista voidaan asettaa salaiseksi. Kuitenkin viranomaisen on arvioitava tiedon/asiakirjan salassapito sen julkisuuden tuoman mahdollisen haitan perusteella. Yleiseksi eduksi katsotaan myös Suomen ulkopoliittiset suhteet, joiden julkisuus voisi aiheuttaa vahinkoa kyseisille suhteille. (Mäenpää 2003, 296)

Kolmas kategoria on julkisyhteisön etu, jota sovelletaan, kun julkisyhteisö toimii esimerkiksi tarjouskilpailussa tai oikeudenkäynnin osapuolena. Tässä tilanteessa julkisyhteisö tulkitaan yksityiseksi oikeussubjektiksi. Tämä on nähty tarpeelliseksi, jotta tiedonantovelvollisuus ei saattaisi julkisyhteisöä yksityistä osapuolta heikompaan asemaan oikeudenkäynnissä. (Mäenpää 2003, 297)

Laki viranomaisten toiminnan julkisuudesta (621/1999) määrittelee 6 luvussa, missä tapauksissa tietoa tulee määrittää salaiseksi. Asiakirja määritetään salaiseksi, jos edellä mainittu laki tai muu lainsäädäntö niin määrittää. Lain 24 §:ssä säädetään salassa pidettävistä asiakirjoista, ellei erikseen toisin säädetä. (Laki viranomaistoiminnan julkisuudesta 621/1999, 24 §)

Pelastustoimelle merkityksellisiä momentteja 24 §:ssä ovat muun muassa 7 ja 8. Seitsemännen momentin mukaan henkilöiden rakennusten ja laitosten viestintä- ja tietojärjestelmiä ja turvallisuusjärjestelyitä koskevat tiedot ovat salaisia paitsi, jos katsotaan, että julkinen tieto näistä järjestelmistä ja järjestelyistä ei vaaranna niiden toimintaa. Momentin 8 mukaan onnettomuuksia, poikkeusoloihin varautumista, väestönsuojelua ja turvallisuustutkintaa käsittelevät dokumentit eivät ole julkisia, ellei katsota, että asiakirjojen julkisuus estäisi tavoitteiden toteutumisen. (Laki viranomaistoiminnan julkisuudesta 621/1999, 24 §)

Tiedon salaiseksi asettamisessa viranomaisella on käytössään myös niin sanottu vahinkolauseke. Vahinkolausekkeen tarkoituksena on velvoittaa viranomainen arvioimaan tiedon salaiseksi asettamisen tarpeellisuutta, jonka tavoitteena on tehdä asiakirjojen salaiseksi asettamisesta joustavampaa. Tämä harkinta toteutuu, jos salaiseksi asettamisen edellytykset löytyvät laista. Vahinkolauseke arvioidaan sen mukaan, kuinka paljon ilmeistä vahinkoa tiedon paljastuminen aiheuttaisi suojattavalle arvolle tai asialle. (Mäenpää 2003, 298-299)

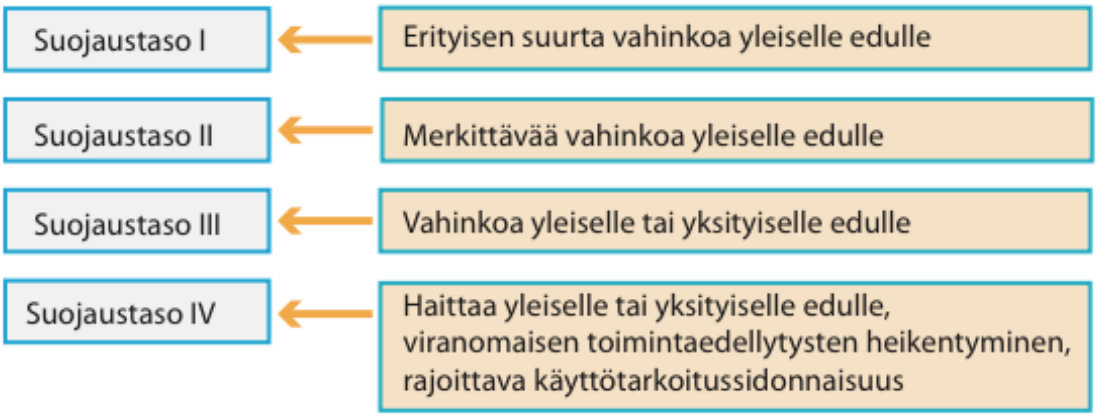
Poikkeuksena on niin kutsuttu ehdoton salassapito, joka tarkoittaa, että asiakirjan salaiseksi asettamisesta ei voida käyttää harkintaa. Ehto astuu voimaan esimerkiksi yksityisyyttä tai yksityisen omaisuutta koskevien asiakirjojen osalta. Viranomaistoiminnan on kuitenkin pyrittävä ensisijaisesti avoimuuteen, jonka vuoksi salattua tietoa sisältävä asiakirja voidaan julkaista, jos salaiseksi määritetyt osuudet poistetaan. Tämä tarkoittaa myös sitä, että asiakirjan olemassaoloa ei voida salata ehdottoman salassapidon perusteella. (Mäenpää 2003, 301)

Viranomaisten toiminnan julkisuudesta annettu laki (621/1999) asettaa 31 §:ssä vaatimuksia asiakirjojen säilyttämisajasta. Asiakirjasta tulee julkinen, kun laissa määritelty salassapitoaika on päättynyt tai salassapidon määrännyt viranomainen päättää salassapidon poistumisesta. Yleinen salassapitoaika on 25 vuotta. Henkilöä käsitteleviä tietoja tulee pitää salassa 50 vuotta henkilön kuolemasta tai 100 vuotta, jos henkilöstä ei ole tietoa esimerkiksi katoamistilanteissa.

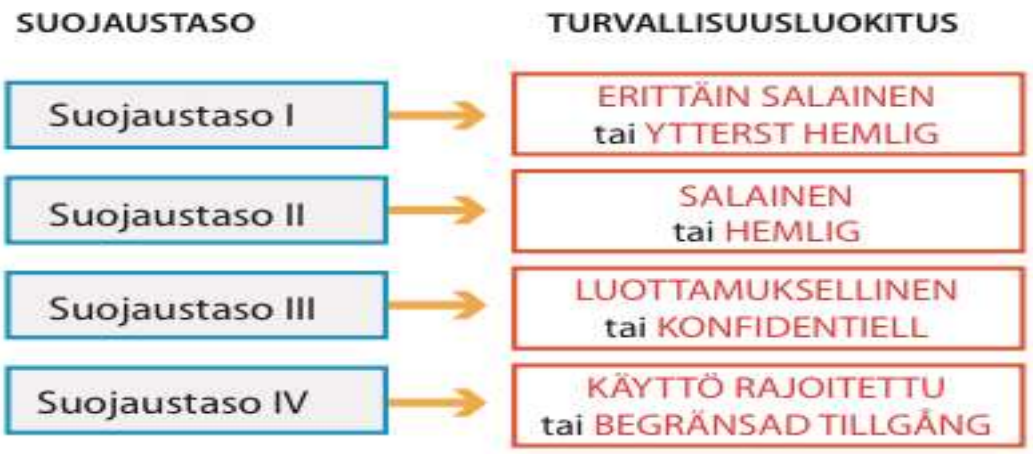
Laki viranomaisten toiminnan julkisuudesta (621/1999) määrittää 24 §:ssä momenteissa 2,7,8 ja 10, millaiset asiakirjat tulee pitää salassa. Asiakirjan salassapito lakkaa, kun sen sisältämät tiedot menettävät merkityksellisyytensä. Merkityksellisyyden arvioi salassapidon asettanut viranomainen (Laki viranomaistoiminnan julkisuudesta 621/1999, 31 §).

Tietoturvallisuuden kannalta edellä mainittu 31 § on erityisen merkityksellinen, sillä se antaa ohjeita tiedon säilytyksestä, joka määrittää tiedon elinkaaren. Tiedon elinkaari on tiedon käsittelyn prosessi, joka alkaa tiedon käytöstä ja päättyy sen hävittämiseen. Elinkaaren ymmärtämisen tavoitteena on se, että tiedon käsittely on suunnitelmallista. (Arkistolaitos 2014)

Laki viranomaisten toiminnan julkisuudesta (621/1999) säätää 25 § asiakirjan salassapidon merkitsemisestä. Jos asiakirja merkitään salassa pidettäväksi, tulee merkinnästä ilmetä, minkä lain nojalla salassapito on asetettu. Asiakirjoille voidaan antaa luokitusmerkintä, joka ilmaisee niitä tietoturvallisuusvelvollisuuksia, joita asiakirjan käsittely vaatii. (Laki viranomaisten toiminnan julkisuudesta 621/1999, 25 §) Luokitusmerkinnät voi toteuttaa esimerkiksi kansallisessa turvallisuusauditointikriteeristössä esitetyllä tavalla, joka on valtionhallinnon käytössä.



Kuva 1: KATAKRI II: Asiakirjojen suojaustasot (KATAKRI II 2011, 124)



Kuva 2: KATAKRI II: Asiakirjojen turvaluokitukset suojaustason mukaan (KATAKRI II 2011, 124)

Käytännössä tämän kaltainen lainsäädäntö on viranomaisten toiminnan kannalta tarpeellista. Tiedon luokittelu antaa organisaatiolle selkeän käsityksen, millaisia toimenpiteitä ja resursseja organisaation tulee käyttää tiedon eheyden, saatavuuden ja yhtenäisyyden varmistamiseksi. Suojaluokitukset selkeyttävät tiedonkäsittelyä, tekevät siitä sujuvampaa ja tarkoituksenmukaisempaa. Tiedon luokittelun tarkoituksena on, että organisaatio kykenee tunnistamaan luottamuksellisen tiedon ja siten käsittelemään tietoa oikein. Tiedonluokittelu antaa perusteet tiedonkäsittelyn ohjeille, jotka ulottuvat tiedon luomisesta sen hävittämiseen asti. (Smallwood 2014, 25-26)

4.2 Lainsäädäntöä henkilötietojen käsittelystä

4.2.1 Perustuslaki

”Perustuslaki määrittelee yksilön ja julkisen vallan välisen suhteen perusteet. Se sisältää myös säännökset julkisen vallan käytön periaatteista” (Oikeusministeriö 2014.) Suomen

perustuslain (731/1999) 12 § määrittää, että viranomaisen hallussa olevat asiakirjat ovat julkisia, ja jokaisella on oikeus saada tietoa asiakirjasta taikka tallenteesta. Kyseinen pykälän mukaan asiakirjan julkisuutta voidaan rajoittaa, jos siihen on lainsäädännölliset perusteet.

Perustuslain (731/1999) 10 §:n mukaan jokaisen kotirauha, yksityiselämä ja kunnia on turvattu. Myös puhelun ja luottamuksellisen viestin yksityisyys on turvattu. On kuitenkin huomioitava, että lailla voidaan säätää rajoituksia yksilöä, kotirauhan tai yhteiskunnan turvallisuutta uhkaavan rikoksen tutkinnassa. Rajoituksia voidaan lailla asettaa myös muun muassa turvallisuustarkastuksissa.

Jokaisella on oikeus saada tietoa nimenomaan viranomaisen julkisesta tallenteesta viranomaisten toiminnan julkisuudesta annetun lain 12 §:n mukaan. Hallituksen esityksestä korostetaan viranomaisen velvollisuutta edistää ja vahvistaa kansanvaltaa ja perusoikeuksia. (HE 1/1998) Näistä voi tulkita, että viranomaisten tulee parhaansa mukaan jakaa tietoa toiminnastaan, ja yksilöön kohdistuvat tiedot ovat ehdottomasti suojeltavia.

4.2.2 Arkistolaki

Arkistolaissa arkistonmuodostajalla tarkoitetaan tahoa, joka kerää, saa haltuunsa tai muodostaa itse tietoa ja säilyttää sitä toimintansa tai tehtävänsä toteuttamiseksi. Arkistonmuodostajan vastuulla on tehdä suunnitelma, joka ohjeistaa arkistossa olevan tiedon säilyttämisen, poistamisen, suojaamisen ja sen tarjoamisen ulkopuolisille. Arkistonmuodostaja on arkistolain mukaan julkista tehtävää suorittava taho, kuten esimerkiksi valtion ja kunnan viranomaiset. (Arkistolaki 831/1994 1, 7, 8 §)

Arkistolain (831/1994) mukaan kunnallisten viranomaisten tulee varmistaa asiakirjojensa säilytys niin, että asiakirjat ovat saatavissa eheinä. Arkistolaki (831/1994) velvoittaa arkistonmuodostajaa myös hävittämään tietoa riippuen sen arvosta. Arkistoa tulee ylläpitää niin, että se tukee arkistonmuodostajan toimintaa. Arkistoon taltioidaan sellaiset asiakirjat, jotka ovat syntyneet tai tulleet viranomaisen haltuun oman toimintansa yhteydessä. Arkiston ylläpitäjän on tehtävä arkistonmuodostussuunnitelma, joka ottaa kantaa, miten tietoa säilytetään ja kuinka kauan, mitä tarkoittaa tiedon elinkaaren tunnistamista. Kyseinen lainsäädäntö vaatii, että asiakirjojen säilyvyys, saatavuus ja tietosuoja on varmistettu. Sama vaatimus koskee myös tiedon hävittämistä. (Arkistolaki 831/1994 3, 7, 8, 11,12 §)

Arkistolain tavoite on säilyttää jälkipolville ainutkertaisia asiakirjoja, joilla on merkitystä kulttuuriperinnön vaalimiselle. Viranomaisen toiminnan kannalta arkistolaki (831/1994) velvoittaa viranomaisia kulttuuriperinnön suojelun lisäksi arkistoimaan tietoa, jolla on merkitystä yksilöiden ja yhteisöjen oikeusturvan kannalta ja mahdollistaa

viranomaistoiminnan julkisuuden, jotta yhteisö voisi sitä arvioida. Arkistolaki (831/1994) edistää arkistojen hoitoa rajoittamalla niiden kasvua määrittämällä, millainen tieto poistuu arkistosta ja missä ajassa. Tämä on oleellinen kysymys, sillä sähköiset tiedon tallennus- ja käsittelyvälineet ovat lisänneet huomattavasti viranomaisille tulevaa tietomäärää. (HE 187/1993)

4.2.3 Laki potilaan asemasta ja oikeuksista

Potilaan asemasta ja oikeuksista (785/1992) säätävän lain mukaan potilaan terveydentilaa ja hoitoa koskevia tietoja tulee käsitellä niin, että potilaan yksityisyys, vakaumus ja ihmisarvo eivät vahingoitu. Terveydenhuollon toimintaan osallistuvien viranomaisten on pidettävä lain mukaan potilasta koskevat tiedot salassa. Salassapidosta voidaan poiketa vain potilaan suostumuksella sillä ehdolla, että potilas on sellaisessa henkisessä tilassa, että hän voi tehdä päätöksen terveydentilastaan kertovien tietojen paljastamisesta sivullisille. (Laki potilaan asemasta ja oikeuksista 785/1992, 3,13 §)

Koska jotkin pelastuslaitokset hoitavat sairaanhoitokuljetuksia, niiden tulee toiminnassaan kiinnittää huomiota potilastiedon käsittelyyn. Hoitotilanteiden lisäksi pelastuslaitokset tallettavat sairaankuljetuspotilaan tietoja toimenpiderekisteriinsä. Pelastustoimen on huomioitava sairaankuljetuksissa laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007), jonka 4 § vaatii varmistamaan potilastietojen eheyden ja yksityisyyden. (Hassinen 2013, 24)

4.2.4 Henkilötietolaki

Koska pelastuslaitokset ylläpitävät henkilörekistereitä muun muassa sopimuspalokuntalaisista ja varautumiseen liittyvistä henkilöistä, tulee toiminnassa ottaa huomioon henkilötietolain (523/1999) vaatimukset. Henkilötietolain (523/1999) tarkoituksena on toteuttaa yksityiselämän suojaa luonnolliselle henkilölle, jonka tietoja (esimerkiksi henkilökohtaisia ominaisuuksia taikka häntä kuvaavia tietoja) tallennetaan rekisteriin. Rekisteröidyllä henkilöllä on oikeus tietojensa tarkistamiseen tiedon tallettajan tietokannasta, mikäli tietoja säilyttävä palvelin on Euroopan unionin rajojen sisällä. Henkilörekisterillä tarkoitetaan järjestelmää, jossa säilytetään yhteneviä joukkotietoja, joiden sisältöä voi tarkastella helposti. (Henkilötietolaki 523/1999, 2-7 §)

Henkilörekisteri ei saa sisältää arkaluontoista tietoa rekisteröidyn poliittisesta kannasta tai etnisestä taustasta. Tämä voidaan kumota henkilön nimenomaisella suostumuksella tai jos lainsäädäntö velvoittaa rekisterin ylläpitäjää kirjaamaan nämä tiedot tehtävänsä toteuttamiseksi. Tämän lisäksi rekisterinpitäjän tulee varmistaa, että tieto on suojattu

tuhoutumiselta ja paljastumiselta ulkopuolisilta, mikä tarkoittaa kyseisessä laissa velvoitetta suunnitelmallisuudesta ja huolellisuudesta. Tietoja voidaan kuitenkin luovuttaa eteenpäin sen henkilön suostumuksella, jota tieto koskee. Tässäkin tapauksessa henkilörekisterin ylläpitäjän on pidettävä rekisteriselostetta, jossa kerrotaan, mitä tietoja kerätään, miksi kerätään, keille tietoa välitetään ja miten tietoa suojataan. Turvatoimet suhteutetaan tiedon arvoon ja toimenpiteiden aiheuttamiin kustannuksiin. Henkilötietojen säilytysaika on niin kauan kuin tieto on tarpeellinen. (Henkilötietolaki 523/1999, 11-13 §)

Henkilötietolaissa todetaan, että yksilöllä tai rekisteröidyllä on lähtökohtaisesti päätösvalta tietojensa käsittelemisestä. Lakimuutos, joka korvasi 1987 henkilörekisterilain, pyrki selkeyttämään ja edistämään Euroopan unionin sisällä tapahtuvia henkilötietojen siirtoja harmonisoimalla jäsenmaitten säädäntöä keskenään. Tämä tavoite määriteltiin Euroopan unionin tietosuojadirektiivin kautta. Tämän lisäksi tietosuojasopimus velvoittaa suojaamaan etenkin yksityisyyttä asuinpaikasta tai kansalaisuudesta riippumatta. Ennen kaikkea henkilötietolaki (523/1999) suojelee perusoikeuksia ja yksityisyyttä henkilötietojen käsittelyssä. (HE 96/1998)

Henkilötietolain (523/1999) voimaantulo aiheutti joitakin muutoksia henkilörekistereiden käytöstä verrattuna entiseen henkilörekisterilakiin. Henkilötietolaki (523/1999) asettaa kiellon arkaluontoisten tietojen käsittelystä, kuten henkilön seksuaalisesta suuntautumisesta tai etnisestä alkuperästä. Lakimuutos aiheutti myös sen, että laissa tuli määrittää tarkasti, millaisissa olosuhteissa ja millä edellytyksillä henkilötunnusta ja sen tietoja käsitellään. Hallituksen esityksessä todetaan myös, että lakimuutoksen myötä laki ei saa estää henkilötietojen siirtämistä EU:n ulkopuolelle, jos siellä voidaan taata riittävä turvallisuuden taso. (HE 96/1998)

4.3 Pelastuslain asettamat velvollisuudet pelastuslaitokselle

4.3.1 Pelastustoimen järjestäminen ja pelastuslaitoksen tehtävät

Pelastustoimen tehtävistä, velvollisuuksista ja viranomaisvallasta säädetään pelastuslailla (379/2011). Pelastuslain (379/2011) tavoitteena on parantaa ihmisten turvallisuutta onnettomuuksilta ja pyrkiä rajoittamaan onnettomuuksien vaikutuksia. Pelastuslaki (379/2011) velvoittaa kaikkia Suomen kansalaisia ja oikeushenkilöitä edesauttamaan lain asettamia tavoitteita. Pelastuslain (379/2011) 2 § velvoittaa pelastusviranomaisia auttamaan, valistamaan ja valvomaan edellä mainittujen tavoitteiden saavuttamista.

Pelastustoiminnasta säädetään laissa seuraavasti: ”Kiireellisistä tehtävistä, joiden tarkoituksena on pelastaa ja suojata ihmisiä, omaisuutta ja ympäristöä onnettomuuden

uhatessa tai sattuessa sekä rajoittaa onnettomuudesta aiheutuvia vahinkoja ja lieventää onnettomuuden seurauksia" (Pelastuslaki 379/2011, 1-2 §)

Sisäasiainministeriö toimii pelastustoimen ylimpänä koordinaattorina ja valvojana. Se vastaa pelastustoimen tasosta ja saatavuudesta valtakunnallisesti pelastuslain (379/2011) 23 §:n mukaan. Aluehallintovirastot valvovat pelastuspalveluiden saatavuuden tasoa omalla alueellaan. Valtioneuvosto päättää pelastuslaitosten aluejaosta. Jokaisen alueen kunnan tulee tehdä sopimus pelastustoimen palveluista alueellaan. Pelastustoimen tehtävä on vastata palvelutason toteutumisesta sopimusalueellaan. Lain mukaan pelastuslaitoksen tehtävät ovat:

1) pelastustoimeen kuuluva neuvonta, valistus ja valvonta;
2) onnettomuuksien ja vaaratilanteiden vaikutusten rajaaminen;
3) väestön varoittaminen vaarasta taikka onnettomuustilanteesta;
4) suorittaa pelastustoimeen kuuluvia tehtäviä kuten pykälässä 2 on kuvattu;
5) suorittaa sairaanhoitokuljetuksia, mikäli sellaisesta on sopimus sairaanhoitopiirin kanssa;
6) tukea kunnan valmiussuunnittelua, jos sellaisesta on sovittu;
7) suorittaa öljyntorjuntaa ja muita sille säädettyjä tehtäviä.

(Pelastuslaki 379/2011, 24,27 §)

4.3.2 Pelastuslain vaikutus tiedon säilyttämiseen ja käsittelyyn

Pelastuslaki (379/2011) säätää, että kaikkia pelastuslaitoksen palveluksessa työskenteleviä virkamiehiä ja muuta sopimushenkilöstöä koskee vaitiolo- ja salassapitovelvollisuus. Vaitiolovelvollisuus asiakirjan sisällöstä on voimassa, jos tiedon salassapidosta on säädetty laissa. Salassapito astuu voimaan, kun:

1) asia koskee yksityistä liike- taikka ammattisalaisuutta tai jos
2) asia koskee henkilön olosuhteita taikka terveyttä.

Laki kuitenkin huomauttaa, että vaitiolovelvollisuus ei estä ilmaisemasta tai antamasta tietoa yksittäistapauksessa hengen tai terveyden suojelemiseksi, jos tiedolla voidaan estää merkittävä ympäristöön tai omaisuuteen kohdistuva vahinko. (Pelastuslaki 379/2011, 86-87 §)

Vaitiolo- ja salassapitovelvollisuus tarkoittaa, että pelastusviranomainen tai sen kanssa toimiva henkilö ei saa paljastaa, luovuttaa tai hyödyntää salaiseksi asetettua tietoa. Kielto koskee myös niin sanottua passiivista tiedon paljastamista, joka tarkoittaa esimerkiksi asiakirjan jättämistä näkyville ulkopuolisten silmäiltäväksi. Esimerkiksi kokoustilat tulee valita niin, että ulkopuoliset eivät voi kuulla tai nähdä vaitiolovelvollisuuden alaista tietoa. (Mäenpää 2003, 294)

Vaitiolovelvollisuuden osalta korostetaan myös, että suojattavasta asiasta ei saa paljastaa mitään, mikä johtaisi suojattavan tiedon jäljille. Salassapitoon kuuluu myös hyväksikäyttökielto. Esimerkiksi, jos viranomainen saa tietoonsa yrityksen liikesalaisuuksia, hän ei saa käyttää näitä tietoja hyväksi itsensä tai muiden lukuun. Tämä rajoitus on voimassa muulloinkin kuin virassa toimiessa, jos tieto on määritetty salaiseksi. Tiedon suojaaminen ei kuitenkaan estä tiedon omistajaa saamasta tietää itseään koskevia tietoja. (Mäenpää 2003, 294)

Pelastuslaki (379/2011) on säätänyt, että pelastuslaitokset voivat pitää tehtäviensä suorittamiseksi erilaisia henkilörekistereitä. Tämä tarkoittaa, että pelastuslaitosten hallinnon tulee ottaa huomioon henkilötietolain vaatimukset tietojen säilyttämisestä. Pelastuslaki (379/2011) sallii pelastuslaitoksen pitää yllä toimenpiderekisteriä, johon se voi kerätä hälytyskeskuksen tietojärjestelmän tallentamia tietoa.

Pelastuslaitos saa käyttää tietoja oman toimintansa kehittämiseen ja seurantaan. Varautumisrekisteri kerää pelastuslaitokselle rekisteriä niistä henkilöistä ja voimavaroista, jotka ovat käytössä varautumisessa poikkeustiloihin. Pelastuslaitos ylläpitää valvontarekisteriä rakennuksista ja kohteista, joissa se suorittaa sille laissa määrättyjä valvontatehtäviä. Myös sopimuspalokuntalaisista pidetään henkilörekisteriä. (Pelastuslaki 379/2011, 91-94 §)

4.4 Euroopan Unionin vaikutus tiedon käsittelyyn Suomessa

Henkilötietojen ja viranomaisten asiakirjojen käsittely pohjautuvat kahteen Euroopan yhteisön asettamaan vaatimukseen: EU-direktiivi yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkumisesta (EY 46/1995) ja Euroopan Neuvoston yleissopimus viranomaisten asiakirjojen julkisuudesta (Council of Europe Convention to access to official documents) (116/2014). Edellä mainittu tunnetaan myös CETS-sopimuksena numero 205 (Council of Europe Treaty Series).

EU:n direktiivi yksilöiden henkilötietojen suojaamisesta perustuu Unionin ideologiaan vapaudesta, demokratiasta ja ihmisoikeuksista. Unioni pyrki vastamaan tietosuojadirektiivillä tietotekniikan kehittymisen tuomiin haasteisiin, mikä mahdollistaa henkilötietojen tehokkaamman keräämisen ja siirtäminen. Koska Unionin perustamissopimus tavoittelee avoimuutta jäsenmaiden välillä, se haluaa henkilötietojen vaihdon olevan turvallista koko Unionissa ja sen jäsenten välillä. Tämän vuoksi jäsenmaiden lainsäädäntöä henkilötietojen käsittelystä haluttiin yhtenäistää. (EY 46/1995)

Unionin direktiivi korostaa yksilön oikeutta yksityiseen suhteessa muihin yksilöihin ja viranomaisiin. Tämän ideologian tulee näkyä kaikessa muussa kansallisessa lainsäädännössä.

Kuitenkin, direktiivin mukaan viranomaisilla on oltava kyky kerätä henkilötietoja ilman oikeushenkilön suostumusta, jos se on tarpeellista yleisen tai julkisen edun ja valtion turvallisuuden kannalta. Tämä ei kuitenkaan poista viranomaisen velvollisuutta ilmoittaa, että näin tehdään. (EY 46/1995)

CETS–sopimus 205:n tarkoituksena on taata kaikille EU-kansalaisille mahdollisuus saada tietoa viranomaisen toiminnasta, joka tarkoittaa yksilön oikeutta saada tietoa viranomaisten asiakirjoista pyydettäessä. Sopimus on merkittävä, sillä se on ensimmäinen kansainvälinen sopimus, joka velvoittaa viranomaisia avoimeen tiedonantoon omasta toiminnastaan. On kuitenkin huomattava, että tämän sopimuksen allekirjoittaminen ei juurikaan vaikuta Suomen lainsäädäntöön, koska Suomessa oikeus saada tietoa viranomaisten asiakirjoista on jo ilmaistu perustuslain 12 §:ssä (731/1999). Tämän lisäksi hallituksen esityksessä todetaan, että laki viranomaisten toiminnan julkisuudesta (621/1999) kattaa CETS-sopimuksen vaatimukset. (HE 116/2014, 3)

4.5 Hallinnollisen tietoturvallisuuden merkitys pelastuslaitokselle

Pelastuslaitokset voivat ylläpitää pelastuslain (379/2011) mukaan henkilörekistereitä ja tietokantoja tehtäviensä toteuttamiseksi ja toimintansa kehittämiseksi. Tällaisia rekistereitä ovat muun muassa toimenpiderekisteri, varautumistehtävien rekisteri, valvontarekisteri ja sopimuspalokuntalaisten henkilörekisteri. Näiden rekistereiden ylläpidossa pelastuslaitoksen tulee ottaa huomioon luonnollisten henkilöiden ja oikeushenkilöiden oikeus yksityisyyteen, mikä ilmaistaan lainsäädännössä.

Pelastuslain (379/2011) 91 § ilmaisee, että pelastuslaitokset saavat ylläpitää toimenpiderekisteriä oman toimintansa seuraamiseksi ja kehittämiseksi. Tähän henkilörekisteriin tallennetaan hätäkeskuksen tallentamia tietoja. Varautumisrekisterin tarkoituksena on 92 §:n mukaan pitää kirjaa henkilöistä ja kalustosta, jotka ovat pelastuslaitoksen käytettävissä poikkeusoloihin varautumisessa. Valvontarekisterin tarkoitus on 93 §:n mukaan mahdollistaa kohteiden ja rakennusten turvallisuusvalvontatehtävien toteuttamisen. Sopimuspalokuntalaisten henkilörekisteri pitää kirjaa muun muassa sopimuspalokuntalaisista 94 §:n mukaan.

Euroopan Unionin direktiivien ja sopimusten vaikutus yksityisyyden suojeluun heijastuu suoraan suomalaiseen lainsäädäntöön muun muassa henkilötietolakiin. Yksityisten tietojen salassa pitämisen lisäksi pelastustoimen viranomaisten on annettava asiakirjoistaan tietoa perustuslain (523/1999) ja viranomaisten toiminnan julkisuudesta säädetyn lain (621/1999) vaatimuksesta. Pelastusviranomaiset voivat asettaa tiedon salaiseksi vain lain nojalla.

Asiakirjojen salaiseksi asettamisesta ja tiedonantovelvollisuudesta säädetään tarkemmin laissa viranomaisten toiminnan julkisuudesta (621/1999).

Pelastuslaitoksen viranomaisten haasteena on yhdistää lainsäädännön vaatimus toiminnan avoimuudesta salaisen tiedon suojelemisen kanssa. Pelastusviranomainen joutuu käyttämään tiedon salaiseksi asettamisessa harkintaa, jonka tulee perustua tiedon julkisuuden vahingollisuuden arvioimiseen, joka olisi hyvä ohjeistaa selkeästi pelastuslaitoksen henkilöstölle.

Pelastuslaitokset pitävät hallussaan yksityistä tietoa, jota sen on kerättävä tehtäviensä toteuttamiseksi, mikä tuo painetta suojella tietoa. Näiden seikkojen vuoksi pelastuslaitos tarvitsee hyvän ja kattavan hallinnollisen tietoturvallisuuden ohjeen, joka antaisi pelastusviranomaisille selkeän käsityksen, millaista tietoa he käsittelevät, mikä on sen arvo ja millaisia riskejä heidän hallussa olevaan tietoon kohdistuu.

5 Kansallinen turvallisuusauditointikriteeristö, Valtionhallinnon tieto- ja kyberturvallisuustyöryhmä ja ISO-standardit

5.1 Kansallinen turvallisuusauditointikriteeristö

KATAKRI on Kansallinen turvallisuusauditointikriteeristö, jonka toinen versio valmistui 20.11.2009. Tätä versiota käytetään hankkeen hallinnollisen turvallisuuden ohjeistuksen pohjana. KATAKRI sisältää neljä auditointiosa-aluetta, jotka arvioidaan jokaisessa auditointitapahtumassa yhtenä kokonaisuutena. Osa-alueet ovat: hallinnollinen turvallisuus, fyysinen turvallisuus, henkilöstöturvallisuus ja tietoturvallisuus. KATAKRIssa jokainen vaatimus on ehdoton, joka tarkoittaa, että saavuttaakseen vaaditun turvallisuuden tason, kohteen on täytettävä kaikki vaatimukset jokaisessa neljässä osa-alueessa. Perustelu tälle on se, että näin organisaatioon ei jää tunnistamattomia ja kriittisiä riskejä. (KATAKRI II 2011, 4)

Turvallisuusauditointikriteeristöllä on kaksi päätavoitetta:

1) Yhtenäistää viranomaisten vaatimuksia, kun viranomainen suorittaa organisaation ja kohteen turvallisuustason tarkastuksen eli auditoinnin.
2) Auttaa yrityksiä, yhteisöjä ja viranomaisten sidosryhmiä kehittämään omaa turvallisuuttaan

Kansallisilla viranomaisilla tulisi olisi selkeät ja yhtenäiset vaatimukset yrityksille tietoturvallisuuden tasosta, jotta yhteistyö olisi mahdollista. Auditointikriteerien avulla viranomainen varmistaa, että yrityksellä on edellytykset käsitellä salaisia asiakirjoja turvallisesti. Jos yritys tahtoo tehdä kansainvälistä viranomaisyhteistyötä, se tarvitsee

yritysturvallisuustodistuksen (Facility Security Clearance, FSC). Tällöin Kansallinen turvallisuusviranomainen arvioi kansainvälisen viranomaispyynnön johdosta yrityksen turvallisuustason. Toisen päätavoitteen johdosta KATAKRI sisältää myös suosituksia elinkeinoelämällä, jotka eivät kuulu viranomaisten vaatimuksiin. (KATAKRI II 2011, 3-4)

FSC on Yhdysvaltojen liittovaltion hallinnoima todistus, jonka yritys tarvitsee voidakseen käsitellä valtiollisia asiakirjoja yhteistyön puitteissa. FSC on jaettu kolmeen tasoon sen mukaan, miten salaista tietoa yritys saa ja kykenee käsitellä. Tasot ovat: luottamuksellinen (confidential), salainen (secret) ja huippusalainen (top secret). (U.S Small Business Administration 2014) Vastaavaa järjestelmää käytetään myös Kanadassa. (Public works and Government services Canada 2014)

KATAKRI-kriteerit keskittyvät yksinomaan niin sanotun security-turvallisuuden auditoimiseen (KATAKRI II 2011, 4). Security-käsite voidaan kääntää seuraavasti: kansainvälinen atomienergiajärjestön IAEA mukaan, security tarkoittaa suojautumista ihmisen tai muun seikan aiheuttamaa vahinkoja vastaan. Safety taasen tarkoittaa turvallisuutta ihmiselle tai ympäristölle aiheutettua vahinkoa vastaan (Kansainvälinen atomienergiajärjestö IAEA 2014). KATAKRIn vaatimukset suojaavat ympäristön tai ihmisen aiheuttamilta vahingoilta.

5.2 Valtionhallinnon tieto- ja kyberturvallisuustyöryhmä

Valtioneuvoston periaatepäätöksen nojalla valtiovarainministeriö sai vastuulleen valtion julkishallinnon tieto- ja kyberturvallisuuden kehittämisen ja ohjaamisen. Tämän velvollisuuden toteuttamiseksi, valtiovarainministeriö asetti Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän eli VAHTIn. Sen tavoitteena on ohjata, suunnitella, toteuttaa ja kehittää valtion julkishallinnon tietoturvallisuutta. VAHTI-työryhmä tavoittelee tietoturvallisuuden integroimista kaikkiin valtionhallinnon prosesseihin, koska tietoturvallisuus on hyvän tiedonhallintatavan edellytys. VAHTIn tehtäviin kuuluu myös valtion kyberstrategian ja valmiuden suunnittelu ja toteuttaminen, jota se toteuttaa koordinoimillaan kehitysohjelmilla. (Valtiovarainministeriö 2014)

VAHTI-ohjeet ovat saaneet kansainvälistä tunnustusta OECD:n (Organisation for Economic Cooperation and Development) julkaisemassa tietoturvallisuuskulttuurin kehittämisraportissa, jossa Suomen VAHTI-työryhmän toimintaa on pidetty eurooppalaisittain esimerkillisenä. (VAHTI toimintakertomus 2013, 7)

VAHTIn kansallinen tunnettavuus on selitettävissä sen tekemien ohjeiden julkisuudella. Kuka tahansa voi lukea valtiovarainministeriön nettisivuilla voimassa olevien VAHTI-ohjeiden sisältöön, joka on lisännyt ohjeiden käytettävyyttä. VAHTIn arvostus näkyy käytännössä myös

siinä, että osa kansallisen turvallisuusauditointikriteeristön KATAKRIn audiointikysymykset pohjautuvat VAHTIn julkaisemiin ohjeisiin. VAHTIa on myös esitelty kansainvälisillä areenoilla Suomen kansainvälisessä tietoturvayhteistyössä muiden maiden kanssa. (VAHTI toimintakertomus 2013, 7)

5.3 Kansainvälinen ISO-standardi

5.3.1 Yleistä tietoa

ISO (the International Organisation for Strandardization) on kansainvälinen ei-valtiollinen jäsenorganisaatio, jonka tarkoituksena on luoda ja julkaista kansainvälisiä standardeja. Standardi tarkoittaa ohjeistusta jonkin asian toteuttamiseksi, jotta voidaan varmistaa esimerkiksi tuotteen tai toiminnan laatu, turvallisuus ja tehokkuus. ISO-järjestön julkaisemien standardien tavoitteena on toimia kansainvälisen yhteistyön mahdollistajana ja apuvälineenä. Ajatuksena on antaa kansainvälisiä toimintamalleja, joka mahdollistaa, että standardeja käyttävät eri maissa toimivat organisaatiot voivat ymmärtää toistensa toimintaa yksiselitteisesti. (Kansainvälinen standardisoimisliitto 2014)

ISO-järjestö julkaisee standardeja tarpeellisuuden periaatteella, joka tarkoittaa, että uuden standardin pitää olla kansainvälisesti relevantti. Tämä näkyy ISO-järjestön asettamana vaatimuksena standardi-työryhmille luomaan standardi niin, että sitä voitaisiin käyttää mahdollisimman laajasti maailmalla. Esitetty standardi-hanke asetetaan jäsenten arvioitavaksi, jotta nähtäisiin, onko ehdotetulle standardille oikeaa tarvetta kansainvälisesti. (Kansainvälinen standardisoimisliitto 2014)

ISO-järjestöllä on 165 jäsenvaltiota, joista jokaisella on yksi edustaja, joka ei voi olla yksilö tai yritys. Jäsenyys on jakautunut kolmeen tasoon: Täysimääräinen jäsen (full member), kumppanuusjäsen (Correspondent member) ja tilaajajäsen (Subscriber). Vain täysimääräisellä jäsenvaltiolla on oikeus osallistua ja äänestää standardien hyväksymiskokouksissa, ja heidän edustajansa voi myydä standardeja ja auttaa niiden soveltamisessa kansallisesti. (Kansainvälinen standardisoimisliitto 2014.) Suomea edustaa SFS eli Suomen Standardisoimisliitto täysin oikeuksin. SFS:n jäseniä ovat elinkeinoelämän järjestöt ja Suomen valtio (Suomen Standardisoimisliitto 2014.)

5.3.2 Tietoturvallisuus ja ISO-standardit

Standardiperhe tarkoittaa tiettyyn aihealueeseen keskittyviä standardeja. Tietoturvallisuutta ja sen johtamista käsitellään ISO 27000 -standardiperheessä, joka kuvaa tietoturvallisuuden johtamisjärjestelmän (Information Security Management System) eli ISMS:n sisältöä ja

soveltamista. Tähän standardiperheeseen kuuluvat esimerkiksi ISO 27002 (Code of practice for information security management) ja ISO 27003 (Information security management system implementation guidance). ISMS:n tavoitteena on antaa organisaatiolle ohjeet, miten tietoturvallisuutta voidaan pitää organisaatiossa aina ajan tasalla kohdistamalla ennalta ehkäiseviä resursseja relevanttien riskien torjuntaa. (ISO 27001)

Tietoturvallisuuden johtamisjärjestelmällä on läheinen suhde ISO 9000 johtamisen standardissa esitellyn jatkuvan kehittämisen mallin kanssa. Mallin tavoitteena on, että organisaation tietoturvallisuus kehittyy toiminnan seuraamisella ja säännöllisten riskiarvioiden tekemisellä.
Tämä pyrkii siihen, että tietoturvallisuus olisi osa organisaation ydintoimintaa ja sen tavoitteita ja sen vuoksi osa johtamisprosessia. (ISO 27001)

Riskienhallintaa käsitellään standardissa 31000, ja sen soveltamista käsitellään standardissa 31004. Riskienhallinnan standardi korostaa riskienhallinnan osaa organisaation johtamisessa. Tämä tarkoittaa, että riskienhallinta tulee yhdistää organisaation toiminnan tavoitteisiin ja sitä kautta kohdistua tavoitteiden saavuttamiseen kohdistuviin riskeihin. Tämä lähestymistapa johtaa riskienhallinnan keskittymisen organisaation kannalta relevantteihin riskeihin. (ISO 31004)

Standardin mukaan toinen oleellinen riskihallinnan elementti on jatkuvuus, joka edellyttää, riskienhallintaa, jonka tulee perustua säännöllisesti tehtyyn, organisaation toimintaan kohdistuvaan riskiarvioon, jotta riskienhallintatoimet kohdistuvat relevantteihin riskeihin. Tämä johtaa riskienhallintasuunnitelman jatkuvaan kehittämiseen ottamalla huomioon uusia riskejä ja jättämällä pois riskejä, jotka ovat muuttuneet ajan kuluessa epäolennaiseksi tai poistuneet. (ISO 31004)

6 Selvityksen tutkimusmenetelmät

6.1 Kirjallisuuskatsaus

Kirjallisuuskatsaus tarkoittaa olemassa olevan tieteellisen tiedon keräämistä. Tavoitteena on etsiä laadukkaita ja arvostettuja tutkimuksia, jotka käsittelevät tutkittavaa aihetta. Kirjallisuuskatsauksella voi olla useampi tarkoitus riippuen tutkijan tavoitteista. Tavoite voi olla kuvailla ja selostaa, mitä tutkittavasta aiheesta tähän mennessä tiedetään. Toinen tavoite voi olla tehokkaiden tutkimusmetodien tai käytäntöjen etsimisessä jonkin tutkimuksen tai hankkeen toteuttamiseksi. Kolmas mahdollinen tavoite voi olla tutkimusalan asiantuntijoiden tunnistaminen, joiden erityisosaamista voidaan käyttää hyväksi tutkimuksista nousseiden kysymysten tulkitsemiseen. (Fink 2009, 3-9)

On huomattava myös, että akateeminen työ aloitetaan hyvin usein kartoittamalla nykytietämys aiheesta. Tarkoituksena on siis saada hyvät taustatiedot, joilla voidaan perustella tutkimuksen tarpeellisuus, mikä vaatii, että aihepiiristä on löydetty vajavaista tai täysin puuttuvaa tietoa. (Jesson 2011, 18)

Kirjallisuuskatsaus jaetaan kahteen erilaiseen toteutustyyliin. Ensimmäinen näistä on niin kutsuttu perinteinen kirjallisuuskatsaus. Sen tavoite on kerätä olemassa oleva tieto aiheesta ja kuvata sen sisältöä kriittisesti arvioiden. Kriittisyydelle tulee antaa erityistä huomiota, koska se tuo järjestyksen kirjallisuuskatsaukseen. Kriittinen ajattelu perustuu ajatukseen, että mikään tieto ei ole syntynyt tyhjiössä, vaan siihen on vaikuttanut se ympäristö, jossa tieto on tuotettu. (Jesson 2011, 11)

Kriittinen ajattelu punnitsee väitettä sen mukaan, miten väite on perusteltu ja voiko väitteelle antaa järkevän esimerkin. Kirjallisuuskatsauksen ydinajatus on se, että katsauksen tekijä kerää asiallisella tavalla aiheeseen liittyvän relevantin tiedon edellä mainitulla kriittisellä ajattelutavalla. (Jesson 2011, 16)

Toinen kirjallisuuskatsauksen tyyli on systemaattinen kirjallisuuskatsaus. Tässä tapauksessa sana systemaattinen tarkoittaa sitä, että kirjallisuuskatsaukseen valittava materiaali valitaan ennalta määrätyillä kriteereillä tai tavoitteilla. Ennalta määrättyjen kriteerien tarkoituksena on, että kirjallisuuskatsauksen työprosessi on mahdollisimman läpinäkyvä, jolla pyritään varmistamaan objektiivisuus. Kirjallisuuskatsaukselle voidaan esimerkiksi asettaa tietty tehtävä, tavoite taikka lähestymistapa, jotka sitten rajaavat katsaukseen valitun kirjallisuuden (Jesson 2011, 12)

Laadukas kirjallisuuskatsaus koostuu kolmesta elementistä. Kirjallisuuskatsauksen pitää olla tarkka, kattava ja toistettava. Tarkkuus tarkoittaa sitä, että kirjallisuuskatsaukseen on valikoitu sellaista aineistoa, joka käsittelee tutkimuskysymystä. Liian laveasti valitun aineiston riskinä on, että tarkkaa ja kattavaa tietoa ei löydetä. (Fink 2009, 15)

Laajuus tarkoittaa, että kirjallisuuskatsauksessa on käytetty useita tietolähteitä tiedon etsimiseen. Toisin sanoen, kirjallisuuskatsaukseen tulisi valita useampi aihetta käsittelevä kirja ja useista tietokannoista löydettyjä julkaisuja tutkittavasta aiheesta. (Fink 2009, 16)

Kolmas tärkeä ominaisuus on toistettavuus. Toistettavuus tarkoittaa sitä, että henkilö, joka lukisi kirjallisuuskatsauksen, pääsisi samaan johtopäätökseen käyttämällä samoja lähteitä kuten kirjoittaja. Edellä mainitulla kolmella elementillä kirjallisuuskatsaus perustelee valintansa ja kestää subjektiivisen tarkastelun. (Fink 2009, 17)

Kestokyky subjektiiviselle tarkastelulle saavutetaan sillä, että kirjallisuuskatsauksen tekijä käyttää sellaista aineistoa, mikä on oman yhteisönsä kriittisesti arvioima ja julkaistu arvostetussa julkaisukanavassa. Aineiston arvoa voidaan arvioida myös sillä, kuinka monesti aineistoa on siteerattu muissa tutkimuksissa. Tämän vuoksi aineistoksi tulisi valita niin sanottuja puhtaita lähteitä, mikä tarkoittaa sellaisen aineiston käyttöä, joka on tehty niin sanotusti mahdollisimman lähellä tietolähdettä. (Jesson 2011, 20-22)

6.2 Kirjallisuuskatsauksen tavoitteet

Kirjallisuuskatsauksen tavoite on tässä opinnäytetyössä selvittää, miten tietoturvallisuutta käsittelevä kirjallisuus näkee hallinnollisen tietoturvallisuuden. Ajatuksena on tehdä kirjallisuudesta havaintoja niistä seikoista, jotka tietoturvallisuutta käsittelevä kirjallisuus näkee merkitykselliseksi hallinnollisen tietoturvallisuuden osalta. Näitä havaintoja vertaillaan asiantuntijahaastatteluiden tulosten kanssa.

Tarkoituksena on löytää mahdollisia näkemyseroja kirjallisuuden ja asiantuntijoiden välillä, ja mitä vahvuuksia ja heikkouksia kummassakin näkemyksessä on. Selvityksessä käytetään systemaattista kirjallisuuskatsausta. Pääkriteerinä on käyttää kirjallisuutta, jonka on tehnyt tietoturvallisuuden alalla pitkälle koulutettu (tohtoriksi koulutettu) tai työelämässä ansioitunut asiantuntija. Kirjan sisältö saa perustua myös arvostetun kansainvälisen organisaation näkemyksiin.

Kirjallisuuskatsaukseen valikoitui muun muassa Charles Pfleeger ja hänen kirjansa Security in computing ja Jacques Cazemier kirjalla Information security management with ITIL. Pfleeger on tietotekniikan tohtori, joka on opettanut Tennese yliopistossa. Tämän lisäksi hän on ollut kansainvälisen tekniikan alan järjestön IEEE:n (Institute of Electrical and Electronics Engineers) tietokoneyhdistyksen ja teknisen komitean turvallisuuden ja yksityisyyden komitean CSTCSP:n (Computer Society Technical Committee on Security and Privacy) hallituksen jäsen vuosina 1993-2004. Tämän lisäksi hän työskennellyt tietoturvakonsulttina omassa yrityksessään. (Dartmounthin Yliopisto 2014) Jacques Cazemier esittelee kirjassaan kansainvälistä tunnustusta saaneen ITIL-mallin (Information technology infrastructure library) soveltamista. Hän on työskennellyt useissa yrityksissä tietoturvallisuuskonsulttina (Cazemier 2010).

6.3 Teemahaastattelu ja asiantuntijahaastattelu

Tutkimushaastattelu on tutkimusmenetelmä, jossa tutkija on kielellisessä vuorovaikutuksessa henkilön kanssa. Tutkimushaastattelussa tutkija etsii tietoa haastateltavan ajatuksista,

tiedosta, kokemuksista tutkittavasta seikasta tai aiheesta, minkä jälkeen tutkija tulkitsee tutkimushaastattelussa saamiaan tietoja tutkimuksessaan. Haastattelun vahvuus onkin sen tavassa käyttää hyväksi ihmisen kykyä kielelliseen ilmaisuun asiasta. (Hirsjärvi 2010, 34, 41)

Tutkimushaastattelu voidaan menetelmänä jakaa kolmeen lajiin: strukturoitu, strukturoimaton ja puolistrukturoitu haastattelu. Strukturoitu haastattelu tarkoittaa, että haastattelun kysymykset ja väittämät ovat tarkasti ennalta määrättyjä. Strukturoimaton haastattelu on niin sanottu syvähaastattelu, jossa käytetään avoimia kysymyksiä, joista haastattelija aloittaa haastattelun rakentamisen. Puolistrukturoitu haastattelu taasen tarkoittaa, että vain jokin osa haastattelua on sama kaikille (esimerkiksi teema). (Hirsjärvi 2010, 43-46)

Tutkimushaastattelun etuna on sen joustavuus. Tutkija voi haastattelun aikana esittää tarkennettuja kysymyksiä ja pyytää lisätietoa haastateltavan vastauksista. Kielellisen vuorovaikutuksen lisäksi tutkija pystyy kiinnittämään huomiota ei-sanallisiin ilmaisuihin, jotka voivat kertoa esimerkiksi haastateltavan asenteista aihetta kohtaan. Tutkimushaastattelu on sopiva menetelmä keräämään syventyneitä ja tarkennettuja vastauksia. (Hirsjärvi 2010, 34)

Tutkimushaastattelu on aikaa vievä ja toteutukseltaan haastava menetelmä. Toisena heikkoutena on, että haastateltava voi antaa niin sanotusti sosiaalisesti hyväksyttyjä vastauksia, jolloin aineisto vakuuttavuus kärsii. Tekijä pyrkii välttämään tätä ilmiötä suunnittelemalla kysymykset niin, että ne eivät johdattele taikka kannusta tietynlaiseen sosiaalisesti hyväksyttävään vastaukseen. (Hirsjärvi 2010, 35)

Asiantuntijahaastattelun (elite interview) ajatuksena on, että tutkija pyrkii saamaan tietoa tutkimastaan aiheesta sellaisen henkilön kautta, jolla erityisosaamista tai tietämystä aiheesta. Yleensä tieteelliset julkaisut taikka kirjallisuus eivät edusta varsinaisesti viimeisintä tietoa aiheesta. Erityisasiantuntijalla voi olla tiedossaan tai itse tekemässä uutta tutkimusta, joka on osoittanut jo uutta ja lupaavaa tietoa aihepiiristä. Erona on vain se, että tiedot tai havainnot eivät ole vielä valmiita julkaistavaksi. (Gilham. 2005, 75-77)

Erityisasiantuntijoilla on myös henkilökohtaista kokemusta toimintaympäristössä, jossa he ovat tutkineet taikka työskennelleet. Esimerkiksi eri hallinnonalan johtavilla työntekijöillä on käytössään sisäpiiritietoa ja käsitystä, jota ei välttämättä ole saatavissa painetusta materiaalista. Asiantuntijahaastattelun heikkous on siinä, että he saattavat olla hyvinkin sidottuja antamaan valmiiksi mietittyjä ja huoliteltuja vastauksia, jotka voivat rajoittaa, mitä tietoa he potentiaalisesti voisivat kertoa. (Gilham. 2005, 78-80)

6.3.1 Haastattelumateriaalin purkaminen ja tulkitseminen

Tutkimushaastatteluissa saatava materiaalin määrä voi olla suuri, vaikka otos olisi pieni. Haastattelumateriaalin luonne on sellainen, että kaikkea kerättyä materiaalia ei ole välttämättä edes tarkoituksenmukaista käyttää. Haastattelumateriaalin purkamisessa olennainen kysymys on, että tutkija on suunnitellut etukäteen, millä tavalla hän purkaa eli litteroi aineiston. Tämä tarkoittaa, että tutkija suunnittelee tutkimushaastattelun rakenteen litteroinnin mukaan. Näin tutkija pystyy rakentamaan kysymykset tutkimuksen tavoitteiden kannalta mahdollisimman tarkoituksenmukaisiksi. Materiaalin litterointi ja purkaminen tulisi aloittaa mahdollisimman aikaisessa vaiheessa, kun haastattelu on vielä tuoreena mielessä. Käytännön syitä on myös se, että analyysia on helpompi muokata silloin jälkikäteen. (Hirsjärvi 2006, 135)

Haastateltavan materiaalin analysointi jaetaan perinteisesti kvantitatiivisiin ja kvalitatiivisiin menetelmiin, jotka eroavat toisistaan selkeästi. Haastattelun analyysi voidaan jakaa kolmeen pääpiirteeseen:
1) Analyysi tehdään suoraan litteroidusta aineistosta luottaen tutkijan kykyyn havaita olennainen tieto;
2) Aineiston analyysiä edeltää sen purkaminen ja koodaaminen;
3) Purettu ja koodattu tieto tuodaan yhteen, josta siirrytään analyysiin.
Laadullisella analyysilla on useita pääpiirteitä, jotka kuvaavat opinnäytetyössäni käyttämääni menetelmää. Kvalitatiivinen analyysi pyrkii siihen, että aineistoa käsitellään mahdollisimman paljon muokkaamatta. Eli toisin sanoen analyysi tehdään suoraan litteroidusta tekstistä. (Hirjärvi 2006, 136)

Asiantuntijahaastattelut analysoidaan selvityksessä käyttämällä ankkuroitua teoriaa (grounded theory). Menetelmän ajatuksena on, että tutkija vetää teoreettisen johtopäätöksen suoraan keräämästään aineistosta. Tämä tarkoittaa sitä, että johtopäätöksien tekeminen ei ohjaudu tukea antavan teorian mukaan. Tärkein ero muihin analysointitapoihin on se, että haastattelut eivät ole varsinaisesti tutkimuksen keskiössä vaan analyysissa itsessään. (Hirsjärvi 2010, 164)

Kerätessään materiaalia tutkija tarkastelee aineistoa, ja analyysinsa perusteella hän voi tehdä teorian, jota täydennetään, jos se nähdään tarpeelliseksi. Jotta teoria voitaisiin tehdä aineistosta, se on luokiteltava hyvin, jolloin voidaan osoittaa teorian pohjautuvan aineistoon. (Hirsjärvi 2010, 165)

Haastattelututkimuksen tekijällä on kaksi tapaa käsitellä aineistoaan. Ensimmäinen tapa on puhtaaksikirjoittaa eli litteroida haastattelumateriaali kirjalliseen muotoon. Toinen tapa on

koodata aineisto ja tehdä päätelmät suoraan materiaalista. Tavallista kuitenkin on, että aineisto litteroidaan ennen aineiston järjestämistä. (Hirsjärvi 2006, 138)

Litteroinnin tarkkuudesta ei ole yksiselitteistä ohjetta, jonka vuoksi suositellaan, että litterointitarkkuus päätetään tutkimustavoitteiden mukaisesti. Hyvänä ohjenuorana on pidetty sitä, että haastattelun litterointitarkkuus määritetään sen mukaan, kuinka relevanttia se on. Esimerkiksi keskusteluhaastattelussa on tärkeää kirjata muistiin nimenomaan keskustelun ominaispiirteitä, kuten taukoja, huokauksia ja niin edelleen. (Hirsjärvi 2006, 139-140)

Kuten aikaisemmin tässä opinnäytetyössä on todettu, asiantuntijahaastattelun auktoriteetti ja pätevyys perustuvat haastateltavan henkilön asemaan tutkittavassa kentässä. Gilham toteaa, että asiantuntijahaastattelussa saatava tieto tulisi käsitellä samaan tapaan kuin kirjallisuudenkin, eli käytetään suoraan sitä tietoa, joka materiaalissa on tullut ilmi. Tämä on yleisesti hyvä käytäntö, koska haastattelun asiantuntijat edustavat organisaatioitaan, joille he ovat vastuussa sanomisistaan (Gilham 2005, 76, 80)

6.3.2 Teemahaastattelun soveltaminen

Selvityksen tavoitteena on saada selville, mitä hallinnollisen tietoturvallisuuden toteuttamisessa pitää ottaa huomioon. Jotta Pelastusopisto saisi käyttöönsä mahdollisimman ajankohtaista tietoa, selvityksessä tehdään asiantuntijahaastatteluita. Tarkoituksena on vertailla kirjallisuuden ja asiantuntijahaastatteluiden tuloksia ja vetää kummankin hyvistä ja huonoista puolista johtopäätökset.

Asiantuntijahaastattelut analysoidaan niin, että heidän vastauksistaan pyritään löytämään toistuvia piirteitä, jotka eritellään esitettyjen kysymysten mukaan. Selvityksessä otetaan myös kantaa, mitä etuja Pelastusopisto saavuttaa tietoturvallisuutensa kannalta, jos se käyttäisi VAHTI-ohjeita ja KATAKRIA hallinnollisen tietoturvallisuuden toteuttamisen tukena.

Tutkimushaastattelu toteutettiin teemahaastatteluna. Tätä menetelmää käytettiin, jotta asiantuntijoiden vastauksia olisi ollut mahdollista verrata keskenään. Haastattelun rakenne oli kaikille sama. Haastattelu rakentuu kahdesta osasta: hallinnollisen tietoturvallisuuden toteuttamisesta ja VAHTIn ja KATAKRIn suhteesta hallinnolliseen tietoturvallisuuteen. Haastattelukysymykset on esitetty liitteessä 1. Haastattelija on mahdollisesti esittänyt tarkentavia kysymyksiä, jos haastateltava ei vastannut riittävän selkeästi kysymykseen.

Asiantuntijahaastattelut litteroitiin niin, että haastattelumateriaalista käy ilmi ne seikat ja väittämät, jotka asiantuntijat sanoivat haastattelussa. Tämän vuoksi litterointi tehtiin kirjakielellä, jotta aineiston tulkitseminen helpottuisi. Litteroinnissa noudatetaan tarkasti

asiantuntijoiden väitteitä, joka varmistetaan antamalla litteroitu materiaali haastateltaville tarkastettavaksi.

Haastatteluista kerätyn aineiston analyysissa käytettiin ankkuroitua teoriaa, jonka tarkoituksena oli vetää johtopäätöksiä suoraan asiantuntijoiden lausunnoista. Tämä nähtiin tarkoituksenmukaiseksi ottaen huomioon haastateltavien ammatillinen asema ja työn tavoitteet. Johtopäätösten vetämisen tarkoituksena oli saada ajankohtaisia näkemyksiä hallinnollisen tietoturvallisuuden toteuttamisesta.

Menetelmän käytön etuna on se, että tekijä kykenee arvioimaan tarvittavan aineiston määrän johtopäätösten vetämiseksi. Näin saatiin käsitys, mikä on selvityksen kannalta tarkoituksenmukainen määrä haastatteluita. Haastatteluaineistosta tehtävät johtopäätökset tehtiin tarkastelemalla haastattelun kysymyksiin annettuja vastauksia yksi kerrallaan. Näin pystyttiin helpommin huomamaan vastauksissa toistuvat teemat.

Haastateltavia asiantuntijoita valittiin tasaisesti edustamaan VAHTIa ja KATAKRIA, koska haastatteluilla piti saada vastauksia kysymyksiin hallinnollisesta tietoturvallisuudesta, KATAKRIsta ja VAHTIsta. Valitut asiantuntijat valittiin heidän korkean asemansa perusteella, jotta asiantuntijoiden vastaukset perustuisivat vahvaan tietoon ja kokemukseen hallinnollista tietoturvallisuutta käsittelevien kysymysten osalta.

Selvityksessä tehtiin neljä asiantuntijahaastattelua, joista kertyi litteroitua materiaalia 22 sivua. Kukin haastattelu kesti 30-45 minuuttia, jonka purkamiseen kului aikaa noin 5-6 tuntia. Haastattelut toteutettiin haastateltavien asiantuntijoiden työpaikoilla ja heille kerrottiin haastattelun tarkoitus ja haastatteluteemat etukäteen. Haastatteluiden litteroinnin jälkeen haastateltavalle annettiin mahdollisuus tarkistaa haastattelun sisältö, jota korjattiin, jos haastateltava tahtoi. Haastateltavat eivät esittäneet korjausvaatimuksia haastattelumateriaalin suhteen.

Neljännen haastattelun jälkeen huomattiin, että haastattelut eivät tuottaneet samoilla kysymyksillä uusia vastauksia. Tämä tarkoitti, että asiantuntijoiden antamat vastaukset alkoivat toistaa samoja teemoja. Tästä pääteltiin, että uusia teemoja ei ilmaantuisi, vaikka haastatteluiden määrää lisättäisiin. Tätä kutsutaan saturaatioksi. Kriittisesti arvioiden saturaatio on voinut muodostua näin aikaisessa vaiheessa haastattelukysymysten laajuuden vuoksi, jolloin vastaajat eivät ole voineet antaa mitenkään tarkasti rajattuja vastuksia. Kysymykset olivat kuitenkin tarpeellisia tutkimustavoitteen kannalta

7 Asiantuntijahaastatteluiden analysointi

7.1 Haastatellut asiantuntijat

Aku Hilve on VAHTI-työryhmän pääsihteeri, joka on toiminut julkishallinnon palveluksessa vuodesta 2003 lähtien. Ensin hän työskenteli Helsingin poliisihallinnon palveluksessa, kunnes hän siirtyi valtiovarainministeriön palvelukseen vuonna 2008. Vuodesta 2011 lähtien Aku Hilve on ollut VAHTI-työryhmän sihteeristön puheenjohtajana. Tämän lisäksi hän on vetänyt VAHTI-työryhmän aloitteesta tekemiä tietoturvahankkeita. Hän valmistui 90-luvun alussa upseeriksi Maanpuolustuskorkeakoulusta, mistä hän siirtyi ATK-turvallisuusupseeriksi. Hänellä on myös kokemusta yksityisestä tietoturvallisuusalasta muun muassa tietoturvakonsulttina ja tuotepäällikkönä. VAHTI-toiminnassa hän on ollut mukana sihteeristön johdon lisäksi myös poliisihallinnon edustajana vuosina 2004-2008.

Kimmo Rousku on Valtorin (Valtion tieto- ja viestintätekniikakeskus) riskienhallintapäällikkö. Hänellä on vahva tekninen tietoturvaosaaminen. Hänen uransa tietoturvallisuuden parissa alkoi vuonna 1992, kun hän tutki virusturvallisuutta. Hän siirtyi valtion palvelukseen 2000-luvun alussa tietohallinnon asiantuntijana, johon linkitettiin silloin tietoturvallisuus. Vuodesta 2009 alkaen hän siirtyi valtion IT-keskuksen palvelukseen, joka siirtyi Valtorin alaisuuteen 2014. Samassa yhteydessä hänen työtehtävänsä vaihtui riskienhallintapäälliköksi. Tämä laajensi hänen tehtäväkenttäänsä käsittelemään ns. perinteisiä yritysturvallisuuden osa-alueita. Vapaa-ajallaan hän kirjoittaa muun muassa blogia Tietoviikon turvasatama-osuudessa. Talentum on julkaisut hänen kirjoittamansa kyberturvallisuusoppaan vuonna 2014. Hän toimii nykyisin VAHTIn teknisen jaoston puheenjohtajana.

Heljo Laukkala on Metso Oyj:n riskienhallintapäällikkö. Hänen uransa turvallisuusalalla alkoi puolustusvoimista, jossa hän toimi muun muassa ilmavoimien turvallisuuspäällikkönä. Hän siirtyi Metson palvelukseen vuonna 2001, jolloin hänen ulkomailla keräämänsä kokemus turvallisuusneuvonantajana nähtiin hänelle eduksi. Vuodesta 2004 eteenpäin hän on toiminut Metso Oyj:n riskienhallintapäällikkönä. Hän on ollut KATAKRI II versiossa hallinnollisen turvallisuuden työryhmän puheenjohtaja. Elinkeinoelämän Keskusliiton yritysturvallisuustyöryhmän puheenjohtajuuden kautta Laukkala pyydettiin osalliseksi KATAKRI II- hanketta. Elinkeinoelämän Keskusliitto piti häntä sopivana, koska hänellä oli puolustusvoimista saatua osaamista niin sanotusta Total security -mallista, joka on hyvin samankaltainen yritysturvallisuuden elementtien kanssa.

Matti Kesäläinen on Suomen kyberturvallisuuskeskuksen erityisasiantuntija. Hänen työuransa on ollut pitkään puolustusvoimissa, jossa hän vastasi puolustusvoimien ja yritysten välisestä yhteistyöstä. Hän toimi KATAKRIn ensimmäisen version työryhmän puheenjohtajana. Hän päätyi työryhmän puheenjohtajaksi silloisen puolustusvoimien virkansa vuoksi. Ajatus KATAKRIn luomisesta lähti hänen ja elinkeinoelämän keskusliiton turvallisuusjohtaja Kalevi

Tiihosen huomaamasta tarpeesta. Toisena vaikuttimena KATAKRIn luomiseen oli hänen päättötyönsä Dipolin, nykyisen Aalto Pro:n, turvallisuusjohdon koulutusohjelmassa.

KATAKRIn osalta haastateltavat pyrittiin valitsemaan niin, että haastatteluun saataisiin edustaja viranomaisten ja elinkeinoelämän toiminnan kannalta. Kirjoittaja tavoitteli tällä lähestymistavalla monipuolista näkemystä. VAHTIn osalta näin ei tehty, koska VAHTIn käyttämisestä yritysmaailmassa ei ole virallista ja luotettavaa dokumentaatiota.

7.2 Haastatteluaineiston luokittelu

Tässä luvussa on asiantuntijahaastattelut on luokiteltu ääninauhoitteista litteroidusta aineistosta, jota tuli noin 22 sivua. Tässä esitetty luokittelu toteutetaan kysymyskohtaisesti eli tekijä on tarkastellut asiantuntijoiden vastauksia jokaisen kysymyksen (*kysymykset ovat kursivoituna*) kohdalla ja kirjoittanut ne auki. Luokittelussa on pyritty löytämään jokaisen kysymyksen osalta yhtenäisiä teemoja mutta yksittäisetkin näkemykset ovat kirjoitettuna ylös. Yhteneviä näkemyksiä ja teemoja on korostettu. Aineiston luokittelun päätavoite on osoittaa lukijalle tiivistetyssä muodossa, mitä asioita haastatteluissa on käynyt ilmi. Haastattelu jakautui kahteen osaan: hallinnollinen tietoturvallisuus ja VAHTI ja KATAKRI. Luokitellun aineiston yhteenveto on luvassa 7.4.

7.2.1 Aineiston luokittelu hallinnollisesta tietoturvallisuudesta

Mitä hallinnollinen tietoturvallisuus tarkoittaa? Asiantuntijat näkevät hallinnollisen tietoturvallisuuden päällisin puolin kaikiksi tietoturvallisuutta ylläpitäviksi toimenpiteiksi, joita ei toteuteta teknisesti. Kuitenkin, hallinnollinen tietoturvallisuus nähdään johtamisen välineenä, jonka tarkoituksena on kehittää tietoturvallisuutta. ”Hallinnollisella turvallisuudella on KATAKRIn selkeä yhtymäkohta laatujohtamisen kanssa” (Laukkala 2014.).

”Hallinnollinen tietoturvallisuus tarkoittaa tietoturvallisuuden johtamis- ja hallintajärjestelmää. Tämä järjestelmä tarkoittaa tietoturvallisuuden tavoitteellista johtamista sen kaikilla tasoilla ja toteutumisen seurantaa mittaamisella.” Hallinnollisen tietoturvallisuuden kautta tietoturvallisuuden johtamiseen perustuu riskienhallintaan. (Hilve 2014)

Mikä on hallinnollisen tietoturvallisuuden merkitys? Hallinnollisen turvallisuuden merkitys korostuu, koska hallinnollisen tietoturvallisuuden tulisi johtaa tietoturvallisuuden toteuttamista. Tämän saavuttamiseksi johdon tulee ilmaista selkeä tukensa ja tahtonsa kehittää tietoturvallisuutta. ”Hallinnollisen turvallisuuden sijaan voitaisiin puhua

turvallisuuden johtamisesta". Muuten tietoturvallisuus jää paikoilleen ilman johdonmukaista kehittämistoimintaa. (Laukkala 2014.)

"Hallinnollinen tietoturvallisuus on laatutyötä, jonka tarkoituksena on kehittää organisaation toimintaa" (Rousku 2014.). Hallinnollinen tietoturvallisuus voidaan nähdä organisaation tavoitteita ja strategiaa tukevana toimintaa. "Hallinnollinen tietoturvallisuus tukee organisaation strategisia tavoitteita" (Hilve 2014.)

Mitkä ovat hallinnollisen tietoturvallisuuden yleisimmät haasteet? Hallinnollisen tietoturvallisuuden haasteet liittyvät johtamisen vajavaiseen toteuttamiseen, mikä näkyy hankkeiden toteuttamisen puutteellisena valvontana. Toinen ongelma on henkilökunnan koulutuksen puute. "Tietoturvallisuutta kehittävissä hankkeissa tulisi luoda vaikuttavuutta ilmaisevia mittareita." Tällöin pystytään kriittisesti arvioimaan, mikä on tietoturvallisuuden taso. Hallinnollisen tietoturvallisuuden toteuttamisen haasteellisuus johtuu myös resurssien puutteesta. (Hilve 2014.)

"Organisaation johto ei ole ymmärrä tietoturva-asioiden merkitystä, vaan se nähdään pelkkänä kulueränä." Tämän kaltainen asennoituminen johtaa aineellisten ja henkisten resurssien puutteeseen, joka estää tietoturvallisuuden toteuttamisen organisaatiossa. Johdolla tulee olla tahtoa tietoturvallisuuden kehittämiseksi, minkä vuoksi johdon tulisi ymmärtää tietojärjestelmiensä merkitys (Rousku 2014.)

Uhkana on myös se, että organisaatio ei kohdista resurssejaan relevanttien riskien torjumiseen. "Liian usein turvallisuustoiminta keskittyy niin sanottuihin trendikkäisiin ja pinnalla oleviin aiheisiin. Näin sen ei pitäisi olla. Turvallisuusjohtamisen on aina perustuttava riskiarvioon." (Laukkala 2014.)

Mitä tulee ottaa huomioon hallinnollisen tietoturvallisuuden toteuttamisessa? Hallinnollisen tietoturvallisuuden asettamat ohjeet ja toimenpiteet ovat sitä varten, että organisaatio voisi luoda ja ylläpitää sellaisen järjestelmän, joka palvelee organisaation toiminnan tarkoitusta. Tulee tietää, mitä järjestelmää taikka tietoa suojellaan ja miksi. (Rousku 2014.)

Organisaation tulee kohdistaa tietoturvaan asetettavat taloudelliset panokset oikein. "Tietoturvallisuutta kehittävät tai toteuttavat hankkeet pitäisi mitoittaa riskienhallinnan perusteella. Näin saavutetaan tietoturvallisuudelle organisaation toimintaan nähden tarkoituksenmukainen taso."(Hilve 2014.)

"Hallinnollisen turvallisuuden ja kaiken muunkin turvallisuustoiminnan pitää lähteä organisaation omasta riskienhallinnasta, jotta organisaatio suojautuisi relevantteja uhkia

vastaan” (Laukkala 2014.). Hallinnollisen tietoturvallisuuden tulee kuitenkin kattaa koko toiminta. ”Tietoturvan tulee olla kokonaisuus, jonka laajuuden ja merkityksen johto ilmaisee tietoturvapolitiikalla” (Kesäläinen 2014.).

Mikä on hallinnollisen tietoturvallisuuden tärkein tekijä? Hallinnollisen tietoturvallisuuden tärkeimpiä tekijöitä on jo käsitelty varsin kattavasti aikaisempien kysymysten kautta. Kuitenkin, muutama seikka on esille tuomisen arvoinen. Hallinnollisen tietoturvallisuuden tulee olla yhdistettynä organisaation toimintaan, kohdistua relevanttien riskien torjumiseen ja huolehtia työntekijöiden valistuneisuudesta tietoturvallisuuden osalta. Lisäksi Matti Kesäläinen (2014) korosti tiedon luokittelun merkitystä, jotta työntekijät osaisivat käsitellä tietoa oikein ja ymmärtäisivät, että kaikki tieto ei kuulu kaikille organisaation sisällä.

7.2.2 Aineiston luokittelu VAHTI- ja KATAKRI-järjestelmissä

VAHTI

”VAHTI-ohjeistuksen tarkoituksena on kehittää valtionhallinnon virastojen palveluiden ja toiminnan laatua kehittämällä tietoturvallisuutta. Toinen tavoite on Euroopan Unionin tietoturva-asetuksen antamien vaatimusten toteuttaminen.” (Rousku 2014.). Näiden vaatimusten toteuttaminen on johtanut siihen, että VAHTI-työryhmä on tehnyt lukuisia ohjeistuksia tietoturvallisuuden parantamiseksi. (Hilve 2014)

VAHTI-ohjeita tehdään erillisissä työryhmissä, joissa tavoitteena on koota yhteen jokaisen ohjeen tekoa varten tarpeellista osaamista ja tietotaitoa. Tämän ansiosta ohjeita ei laadita sokeasti käyttämällä kansainvälisiä tietoturvastandardeja, sillä VAHTI-ohjeen on sovelluttava julkishallinnon tarpeisiin.

VAHTI-ohjeet ovat saaneet myös kansainvälistä huomiota. ”VAHTI-ohjeita on käytetty Euroopan Unionin itäisenkumppanuuden maissa julkishallinnon tietoturvallisuuden kehittämisen hankkeissa. Tämän lisäksi myös Viron hallinto on ottanut käyttöön VAHTIn ohjeistuksia.” (Hilve 2014.). Haastattelussa kummatkin VAHTIa edustavat asiantuntijat kuvailivat VAHTI-työryhmän tekemiä ohjeistuksia kansainvälisesti ainutlaatuisiksi. Näkemys perustuu tapaan, jolla Suomi on ryhtynyt VAHTI-ohjeiden avulla toteuttamaan EU:n tietosuoja-asetusta.

Kumpikaan asiantuntija ei nostanut tiettyjä standardeja esimerkiksi ISO-standardeja jalustalle, koska VAHTI-työryhmän johto ei ole erikseen kehottanut käyttämään niissä olevaa tietoa. Haastatteluiden perusteella ISO-standardien ja VAHTI-ohjeiden välillä ei ole erityistä suhdetta. Aku Hilven (2014) mukaan ISO-standardin käyttöä ei harkittu sen maksullisuuden

vuoksi. Toinen ja tärkeämpi syy oli kuitenkin valtiovarainministeriön tahto käyttää ohjeita, jotka ottaisivat mahdollisimman paljon huomioon julkishallinnon piirteet.

KATAKRI

Kesäläinen (2014) muistutti haastattelussa, että koko KATAKRIn tavoite on organisaatiossa käsiteltävän tiedon suojeleminen, joka on yllättävä toteamus, koska tätä ei todeta KATAKRIssa itsessään. Tästä voidaan päätellä, että KATAKRIn toinen versio on tietoturvallisuuden kannalta kattava auditointikriteeristö, koska se ottaa huomioon hallinnon, henkilöstön, fyysisen turvallisuuden ja teknisen tietoturvallisuuden.

Haastatteluissa ilmenneiden asioiden perusteella KATAKRI II -version hallinnollisen turvallisuuden asettamat kriteerit antavat edellytykset edistyksellisen tietoturvallisuuden hallinta- ja johtamisjärjestelmän luomiseen. ”KATAKRIn hallinnollisen turvallisuuden osuudessa minulla oli sen puheenjohtajana selkeä tahto luoda turvallisuudelle johtamisjärjestelmä” Tämä johtamisjärjestelmä korostaa riskienhallinnan ja laatujohtamisen merkitystä. (Laukkala 2014.)

Laatujohtamisen tarkoituksena on varmistaa tietoturvallisuustoiminnan jatkuva kehittäminen. ”ISO 31000 (laatujohtaminen) ja OHSAS 18001 (työturvallisuuden johtaminen) –standardeilla on voimakas analogia hallinnollisen turvallisuuden osuuden kanssa” (Laukkala 2014.) Laatujohtamisen elementti näkyy KATAKRIssa vaatimuksena suorittaa riskiarvioita säännöllisesti ja raportoida johdolle onnettomuuksista. Nämä ovat olennaisia seikkoja, jotta organisaation käsitys omasta tietoturvallisuuteen liittyvistä tarpeista ei jäisi paikoilleen.

Mitä KATAKRIssa käytettyjen tietolähteiden käyttämiseen tulee, periaate on sama kuin VAHTIssa. KATAKRIn vaatimuksien ja sisällön rakentamisessa käytettiin asiantuntijatyöryhmiä ja hyväksi tunnettuja standardeja. ”Ymmärrettävästi suuren tietomassan vuoksi auditointikriteereihin tulevia asioita karsittiin niin, että ne olisivat mahdollisimman sopivat suomalaisessa käyttöympäristössä” (Kesäläinen 2014.) Työryhmiin valittu asiantuntijat edustivat niin viranomaistoimintaa kuin elinkeinoelämää.

Haastatteluiden perusteella KATAKRIlla on selkeä suhde kansainvälisiin standardeihin ja sieltä tulleeseen ajattelutapaan, joka näkyy turvallisuustoiminnan korostamisena osana organisaation tavoitteita. Toinen huomattava elementti on johtamisen korostaminen, jota ajettiin Laukkalan (2014) mukaan vahvasti hallinnollisen turvallisuuden kriteereihin, kun KATAKRIn toista versiota tehtiin.

7.3 Johtopäätökset

7.3.1 Asiantuntijoiden näkemys hallinnollisesta tietoturvallisuudesta

Haastatteluiden perusteella voidaan todetta hallinnollisen tietoturvallisuuden olevan tietoturvallisuuden johtamisen väline. Muutama asiantuntija kuvaili hallinnollista tietoturvallisuutta tietoturvallisuuden hallinta- ja johtamisjärjestelmäksi, jonka tarkoituksena heidän mukaansa on ohjata tietoturvallisuustyötä niin, että se olisi mahdollisimman tarkoituksenmukaista. Tämän vuoksi riskienhallinta ja organisaation toiminnan tunteminen ja sen toiminnan ymmärtäminen korostuu. Näin mahdollistetaan, että tietoturvallisuuden ylläpitoon ja luomiseen ei käytetä yhtään enempää resursseja kuin on tarpeellista.

Asiantuntijat korostavat johdon sitoutumisen, ymmärryksen ja kiinnostuksen merkitystä tietoturvallisuuden kehittämisessä. Tietoturvallisuus ja sen kehittäminen ei saavuta tarpeellisia resursseja, jos sen merkitystä ei ymmärretä. Jotta tämä ymmärrys ja sen kautta resurssit saavutettaisiin, johdolle tulisi selventää, mitä tietoturvallisuus merkitsee organisaatiolle. Saavutettu ymmärrys antaa johdolle tarpeellisen tahtotilan ja tavoitteen tietoturvallisuuden kehittämiselle, joka ilmaistaan tietoturvapolitiikassa.

Asiantuntijat nostivat esille tarpeen määrätietoisesta johtamisesta. Heidän haastatteluistaan kerätyn aineiston perusteella tämä tarkoittaa hallinnollisen tietoturvallisuuden tarkoitusta olla tietoturvallisuuden kehittämisen ja ylläpidon mahdollistava johtamisväline. Metso Oyj:n riskienhallintapäällikkö Heljo Laukkala (2014) nosti esille, että hänen johtama hallinnollisen turvallisuuden työryhmänsä tavoitteli sitä, että hallinnollisessa turvallisuudessa pyrittäisiin jatkuvaan parantamiseen eli laatujohtamiseen. Jotta tällainen olisi mahdollista, mittaamisen merkitys korostuu, koska sen avulla pystytään konkreettisesti seuraamaan tietoturvallisuutta edistävien toimien vaikuttavuutta.

Asiantuntijahaastatteluiden tulosten perusteella hallinnollisen tietoturvallisuuden pitäisi muodostaa tietoturvallisuuden hallinta- ja johtamisjärjestelmä, jota ei ole Pelastusopiston käytössä. Aineiston perusteella seuraavat seikat ovat välttämättömiä tietoturvallisuuden hallinta- ja johtamisjärjestelmän toteuttamiseksi:

- Tietoturvapolitiikka
- Jatkuvankehittämisen periaate (laatujohtaminen)
- Riskienhallintasuunnitelma
- Mittaamissuunnitelma ja periaatteet
- Tiedonluokittelu

Edellä mainitut seikat ovat niitä asioita, jotka asiantuntijahaastatteluiden tulosten perusteella tulisi sisältyä tietoturvallisuuden hallinta- ja johtamisjärjestelmään, jotta hallinnollinen tietoturvallisuus toteutuisi parhaalla mahdollisella tavalla. Selvityksessä

ilmenneiden seikkojen perusteella Pelastusopiston tulisi käyttää hallinnollisen tietoturvallisuutensa toteuttamiseksi yllä luetelluista seikoista koostuvaa tietoturvallisuuden johtamis- ja hallintajärjestelmää. Tietoturvallisuuden hallinta- ja johtamisjärjestelmän käyttämisellä tietoturvallisuuteen pystyttäisiin kohdistamaan oikea määrä resursseja, jotka perustuvat organisaation toimintaan ja tavoitteisiin kohdistuvien riskien torjuntaan.

Esitetyn mallin vahvuutena on se, että se ei voi laatujohtamisen elementin takia vanhentua. Mikäli johto sitoutuu tämän mallin käyttämiseen, ohjeistus pysyy organisaation muutosten mukana. Tämä perustuu siihen, että laatujohtaminen edellyttää oman toiminnan säännöllistä arviointia, jonka ansiosta organisaatiolla olisi aina käsitys tietoturvallisuutensa nykytilasta ja sen asettamista vaatimuksista. Arviointia tulee peilata tiedonkäsittelyohjeiden ja tietoturvapolitiikan kanssa, jotta se vastaisi organisaatiolle ajankohtaisiin uhkiin. Selvityksen tulos tuo esille myös mittaamisen elementin, joka auttaa toiminnan jatkuvaa kehittämistä kuten myös tietoturvallisuuden kohteiden toiminnan seuraamista.

Vaikka laatujohtaminen on ISO-standardeista kehitetty järjestelmä, joka tarkoittaa sitä, että pelastuslaitokset voisivat ostaa standardin. Tämän selvityksen ansiosta pelastuslaitosten ei tarvitse käyttää varojaan sellaiseen. Tämän selvityksen ansiosta Pelastusopisto saa ohjeet tietoturvallisuuden hallinta- ja johtamisjärjestelmän toteuttamisesta KATAKRI:n ja VAHTI-ohjeiden avulla. Perustelut luvussa 8.

7.3.2 Kirjallisuuden ja asiatuntijanäkemyksien erojen tulkitseminen

Teoriaosuudessa esitetyn kirjallisuuden näkemyksen mukaan hallinnollista tietoturvallisuutta tulee ajatella tietohallinnon kautta, ja millä teknisillä ratkaisuilla se voi sitä toteuttaa. Tietohallinnon tehtävä on määrittää, ketkä saavat käsitellä tietoa ja millä oikeuksilla. Jotta tietohallinto pysyisi tiedonkäsittelyssään ajan tasalla, sen tulee seurata tiiviisti lainsäädännön muutoksia. Kirjallisuuden perusteella hallinnollinen tietoturvallisuus on tiedonkäsittelyä ohjaava tekijä.

Tämä näkökanta on verrattain kapea, kun sitä vertaa asiantuntijahaastatteluiden analyysin tuloksena syntyneeseen näkemykseen, koska heiltä saadun aineiston perusteella hallinnollinen tietoturvallisuus tarkoittaa koko tietoturvallisuuden hallinta- ja johtamisjärjestelmää. Tämä tarkoittaa toisin sanoen sitä, että tietoturvallisuuden hallinta- ja johtamisjärjestelmä pyrkii kehittämään ja vaikuttamaan kaikkiin niihin seikkoihin ja tekijöihin, jotka ovat merkityksellisiä organisaation tietoturvallisuuden kannalta. Organisaation panostus tietoturvallisuuteen tulisi olla suhteessa säilytetyn tiedon arvoon, siihen kohdistuviin uhkiin ja lainsäädännön asettamiin vaatimuksiin tiedon käsittelemiselle ja säilyttämiselle.

Toinen elementti, joka tuo eroja näiden näkemysten välille, on riskienhallinta. Kirjallisuuskatsauksessa esitetyn näkemyksen perusteella tietohallinnon ylläpitämä hallinnollinen tietoturvallisuus tarkkailee toimintaympäristönsä muutoksia lain tasolla. Asiantuntijoiden näkemyksen mukaan hallinnollisen tietoturvallisuuden tulee olla osa koko organisaation johtamisprosessia, joka vaatii, että tietoturvallisuuden eteen tehdyn työn on pohjauduttava koko organisaation toimintaan kohdistuvaan riskiarvioon.

7.3.3 Huomioita ISO-standardien suhteesta VAHTI-ohjeisiin ja KATAKRI-turvallisuusauditointikriteeristöön

Asiantuntijahaastatteluista kerätyn aineiston perusteella voidaan huomata, että VAHTI-ohjeet ja KATAKRI sisältävät ISO–standardiin verrattuna samanlaisia piirteitä. ISO–standardit toistavat tietoturvallisuuden johtamisjärjestelmän kiinteää yhteyttä organisaation strategiaan ja tavoitteisiin. Tietoturvallisuuden tulisi olla organisaatiossa jatkuvasti kehittyvä, joka on mahdollista säännöllisellä riskienhallinnalla. Kun tämä seikka toteutuu, tietoturvallisuudesta tulee luonnollinen osa organisaation toiminnan johtamista, eikä se siten jää vain erilliseksi toiminnoksi.

Haastattelumateriaali VAHTI–ohjeista ja kansallisesta turvallisuusauditointikriteeristöstä (luku 6) osoittaa, että molemmat pyrkivät samoihin edellä mainittuihin asioihin ISO –standardeja noudattamalla. Etenkin KATAKRIa koskevat haastattelut korostivat johtamisen merkitystä, jonka pitää perustua laatujohtamiseen.

Tietoturvallisuutta ja sen johtamista käsittelevä ISO 27000-standardi perustuu laatujohtamiseen, jonka peruselementti on jatkuvaparantaminen. Laatujohtamisen malli tunnetaan Plan-Do-Check-Act-prosessina (PDCA-prosessi), joka on peräisin ISO 9000-standardista. Prosessia toteutetaan toistamalla seuraavia vaiheita:

1) Suunnittelu (plan): Organisaatio tekee suunnitelman tietoturvallisuutensa toteuttamiseksi. Apuna voi käyttää riskiarviota;
2) Toteuta (do): Suunnitelma toteutetaan;
3) Valvo (check): Mittaan toteutetun suunnitelman toimivuutta;
4) Kehitä/Ylläpidä (act): Suunnittelua ja toteutusta kehitetään tai ylläpidetään valvontatulosten perusteella. (ISO 27000 2012, 14)

VAHTIa ja KATAKRIa käsittelevissä haastatteluissa nousi etenkin esille johtamisjärjestelmä-termin käyttäminen. Hallinnollisen tietoturvallisuuden merkityksestä kysyttäessä muun muassa Laukka ja Hilve (2014) korostivat hallinnollisen tietoturvallisuuden olevan nimenomaan toiminnan johtamista riskien mukaan. Myös jatkuva kehittäminen nousi haastatteluissa esille olennaisena osana. Todettiin, että tietoturvallisuutta tulee seurata mittaamalla ja raportoimalla, jotta tiedettäisiin, missä tilassa tietoturvallisuus on. Jokaisen haastatellun asiantuntijan mielestä turvallisuustoiminnan pitäisi olla osa organisaation normaalia johtamista, joka korostaa organisaation johdon tahtotilaa ja roolia. Tätä ilmaistaan tietoturvapolitiikalla.

Edellä mainitut seikat huomioon ottaen voidaan päätellä, että jos organisaatio päättää käyttää KATAKRIa ja VAHTIa tietoturvallisuutensa kehittämiseen, organisaatio toteuttaa

epäsuorasti ISO 27000-standardin suosituksia tietoturvallisuuden toteuttamisesta laatujohtamisen periaatteille. Tämä johtuu siitä, että VAHTIssa ja KATAKRIssa on sisällöllisesti niin paljon yhteneväisyyksiä ISO–vaatimusten kanssa.

Vaikka ISO-standardeilla on ollut tämän selvityksen valossa huomattava vaikutus VAHTIn ja KATAKRIn, kumpaakaan asiakirjaa edustavat asiantuntijat eivät korostaneet ISO–standardin merkitystä VAHTIssa ja KATAKRIssa. Asiantuntijat toteavat, että samankaltaisien periaatteiden esiintyminen ei ole tieten tahtoen tehty valinta, ja ISO-standardissa esiintyviä seikkoja on muokattu asiantuntijoiden toimesta. Koska asiantuntijat ovat omalla tietotaidollaan ohjanneet kummankin asiakirjan kehittymistä, voidaan päätellä, että vahva yhteys ISO–standardeihin tulee sen vahvasta vaikutuksesta tietoturvallisuuden ja turvallisuuden ammattilaisten ajatteluun.

8 Johtopäätökset ja jatkotutkimuksen aihepohdinta

8.1 Johtopäätökset

Edellä mainitusta voidaan huomata, että asiantuntijoiden näkemyksellä tehdyillä ohjeilla hallinnollisesta tietoturvallisuudesta muodostuu laajempi käsitys verrattuna nykyisen kirjallisuuden antamaan tietoon. Tämän selvityksen tuloksena saatiin selville ne seikat, jotka ovat tärkeitä hallinnollisen tietoturvallisuuden toteuttamiseksi. Näiden seikkojen avulla organisaatio pystyy ottamaan määrätietoisen otteen tietoturvallisuudestaan kokonaisuutena. Tällainen lähestymistapa luo tietoturvallisuuden johtamisjärjestelmän, jonka suurimpana vahvuutena on, että se korostaa tietoturvallisuuden tarkoituksenmukaisuutta suhteessa riskeihin. Näin organisaatio ei tee turhaa työtä tietoturvallisuuden eteen eikä tuhlaa resursseja.

Haastatteluiden perusteella VAHTIn ja KATAKRIn käyttäminen tietoturvallisuuden toteuttamisessa on tarkoituksenmukaista. VAHTI-työryhmän tekemät toteutusohjeet ovat korkealaatuisia ja ovat saaneet kansainvälistä huomiota. Tämän lisäksi ohjeet on tehty toteuttamaan EU:n tietosuoja-asetusta ja nimenomaan sopivaksi julkishallinnolle. Jos Pelastusopisto päättää käyttää VAHTI-ohjeita, pelastuslaitosten hallinnollisen tietoturvallisuuden ohjeisiin tulee VAHTIn asiantuntijatyöryhmissä työstettyjä ohjeita. KATAKRIn käyttäminen hallinnollisen tietoturvallisuuden kriteereinä mahdollistaa johdonmukaisen tietoturvallisuuden johtamisen, johon hallinnollisen turvallisuuden osuuden puheenjohtaja Heljo Laukkala pyrki, kun KATAKRI 2. versiota tehtiin.

Toinen varteenotettava havainto on, että KATAKRIn asettamat kriteerit pyrkivät yksinomaan tiedonkäsittelyn turvallisuuteen. Nämä asiat huomioon ottaen, Pelastusopiston on hyvä

käyttää VAHTI-työryhmän ohjeita ja KATKARI-kriteerejä. KATAKRIa ja VAHTIa käyttämällä Pelastusopisto tekee pelastuslaitoksista epäsuorasti ISO-kelpoisia, koska näillä kolmella asiakirjalla on yhteneväinen tapa tarkastella hallinnollista tietoturvallisuutta ja korostaa samanlaisten seikkojen tärkeyttä.

Yhdenkin tietoturvallisuuden hallinta- ja johtamisjärjestelmän elementin puuttuminen tekisi organisaation tietoturvallisuudesta vajavaista. Ilman riskienarviointisuunnitelmaa tietoturvallisuutta ei kohdistettaisi oikein, jolloin organisaation resursseja käytetään joko tarpeettoman paljon tai liian vähän suhteessa tiedon arvoon. Ilman jatkuvankehittämisen eli laatujohtamisen periaatetta tietoturvallisuudesta tulee passiivinen toiminta, joka kehittyisi vain silloin, kun se kohtaa ongelman. Laatujohtamisen periaate tuo organisaatioon jatkuvan kehityksen, joka perustuu jatkuvaan organisaation toimintaympäristön, tavoitteiden ja toimintojen arvioimiseen. Olennainen seikka näiden periaatteiden toteuttamisessa tietoturvallisuuden johtamis- ja hallintajärjestelmässä on säännöllinen riskienarviointi, vahinko- ja puuteraportointi, joiden avulla uhista on mahdollista saada realistinen käsitys.

Väite riskiarvion merkityksestä perustuu siihen, että sen avulla pystytään pureutumaan organisaation ydintoiminnan kannalta olennaisiin riskeihin. Riskienarviointisuunnitelmaan sisältyy esimerkiksi riskienarviointi, joka tulisi tehdä yhteistyössä organisaation työtekijöiden kanssa johdosta alaspäin. Kun riskienarviointi toteutetaan organisaation kaikilla tasoilla, pystytään tunnistamaan tietoon kohdistuvia uhkia kaikilta käsittelytasoilta ja tiedonkäsittelyvaiheista

Tietoturvapolitiikan puuttuminen aiheuttaisi sen, että vaikka organisaatiolla olisi tietoturvallisuudesta vastaava ryhmä, siltä puuttuisi organisaation johdon tuki ja tahto kehittää turvallisuutta. Tämän lisäksi tietoturvapolitiikan tarkoituksena on viestiä muulle organisaatiolle tietoturvallisuuden merkitys. Tämän kaltainen asenteen ulospäin osoittaminen on tärkeää, koska johdon on näytettävä esimerkkiä tietoturvallisuuden toteuttamisessa. Heidän tulee myös viestiä tietoturvapolitiikan avulla tietoturvallisuuden tärkeys ja miksi se on tärkeää organisaation toiminnalle. (ISO 27001)

Mittaaminen on jatkuvan kehityksen toteutumisen edellytys, jotta organisaatio kykenee arvioimaan, millaisessa tilanteessa sen tietoturvallisuus on esimerkiksi tietyn järjestelmän osalta. Hilve (2014) korosti mittaamisen merkitystä, koska mittaamalla pystytään keräämään dokumentaatiokelpoista tietoa tietoturvallisuuden tasosta, jota voidaan verrata esimerkiksi kustannusten kanssa. Vertailukelpoiset mittaukset antavat organisaatiolle mahdollisuuden seuraamaan kehitystään ja havaitsemaan ongelma-alueitaan. Mittaustuloksilla pystytään myös perustelemaan johdolle investointeja vaativia toimenpiteitä tietoturvallisuuden parantamiseksi (Hilve 2014.)

Tiedon luokittelu taasen mahdollistaa sen, että työntekijät kykenevät tunnistamaan ja käsittelemään johdonmukaisesti luottamuksellista tietoa. Kesäläinen (2014) korosti, että tiedon luokittelu ja sen ohjeistaminen pitää sovittaa konkreettisilla esimerkeillä organisaation toimintaan, koska tiedon luokittelusta on vaikea antaa yleispäteviä neuvoja, jotka toimisivat aukottomasti kaikissa tilanteissa ja organisaatioissa.

8.2 Jatkotutkimuksen aihe

Opinnäytetyössä selvitettiin, mitkä ovat niitä tärkeitä seikkoja, jotka tulisi sisällyttää tietoturvallisuuden johtamis- ja hallintajärjestelmään. Seuraava luonnollinen vaihe olisi teoreettisen tiedon soveltaminen käytännössä, kun organisaatio ryhtyisi toteuttamaan tietoturvallisuuden johtamis- ja hallintajärjestelmän osioita käytännössä.

Tutkimuksen tavoitteena olisi selvittää, mitkä seikat ovat haasteellisia tietoturvallisuuden johtamis- ja hallintajärjestelmän toteuttamisessa, kun se luotaisiin kiinteäksi osaksi organisaation johtamista. Idea jatkotutkimukselle tuli Valtionhallinnon tieto- ja kyberturvallisuustyöryhmän pääsihteerin Aku Hilven haastattelussa, jossa hän totesi, että organisaatioiden yleisin ongelma hallinnollisen tietoturvallisuuden toteuttamisessa on ohjeistusten jääminen paperille.

Tietoturvallisuuden johtamis- ja hallintajärjestelmän soveltamisesta aiheutuvia haasteita ja vaikeuksia voitaisiin tutkia tapaustutkimuksena, joka kohdistuisi yhteen yksityiseen tai julkiseen organisaatioon, koska tarkoituksena olisi seurata tarkasti koko tietoturvallisuuden johtamis- ja hallintajärjestelmän jalkauttamista. Tutkimuksen menestyksellinen toteuttaminen vaatisi, että organisaatiolla ei olisi entuudestaan tietoturvallisuuden johtamis- ja hallintajärjestelmän kaltaista ohjetta, jolla hallinnollista tietoturvallisuutta toteutettaisiin.

Tutkimus tulisi tehdä tapaustutkimuksena yhdessä kohteessa, jotta organisaatiossa ilmenneitä toteuttamisongelmia pystyttäisiin tarkastelemaan lähemmin ja arvioimaan syvällisesti, mistä mahdolliset ongelmat johtuvat. Tämä edellyttäisi, että tutkimuksen tekijä olisi läheisessä yhteistyössä organisaation kanssa, kun se ryhtyisi toteuttamaan tietoturvallisuuden johtamis- ja hallintajärjestelmän vaatimuksia. Tutkijan pitäisi myös osallistua soveltamisprosessiin, jotta hänestä tulisi kiinteä osa projektia, jolloin hän pystyisi tarkkailemaan tietoturvallisuuden johtamis- ja hallintajärjestelmän soveltamisprojektin etenemistä sen kaikissa vaiheissa.

9 Tutkimuksen laadun arviointi

Selvityksen päämenetelmänä käytettiin asiantuntijahaastattelua, jota perusteltiin sillä, että saataisiin selville hallinnollisen tietoturvallisuuden toteuttamisen kannalta hyvät käytännöt, jotka olisivat myös ajankohtaisia, minkä vuoksi valittu menetelmä on tarkoituksenmukainen selvityksen tavoitteiden kannalta. Haastatteluaineistosta tehtyjä havaintoja ja johtopäätöksiä on verrattu kirjallisuuskatsauksessa tehtyjen havaintojen kanssa. Vertailun tavoitteena on antaa haastatteluaineistolle kontrasti, jotta mahdolliset hyödyt kirjallisuuden antamaan tietoon nähden pystyttäisiin toteamaan.

Kirjallisuuskatsauksen ja asiantuntijahaastattelun käyttäminen on selostettu perinpohjaisesti ja laajasti, mikä antaa lukijalle mahdollisuuden toistaa selvityksen tulokset. Kirjallisuuskatsaukseen valikoitui kirjoittajia, joilla on vahva kansainvälinen näkemys tietoturvallisuudesta. Lähdekirjojen kirjoittajat eivät ole kytköksissä haastateltaviin henkilöihin.

Haastatteluaineistosta tehdyt johtopäätökset on tehty selkeällä, perustellulla ja toistettavalla tavalla. Periaatteessa lukija voi päätyä samoihin johtopäätöksiin näillä menetelmillä. On kuitenkin otettava huomioon, että haastattelu on menetelmänä varsin henkilökohtainen eikä haastattelutilanteita voida varsinaisesti toistaa. Tosin kaikki haastatteluissa tehdyt lisäkysymykset on litteroitu, joten vuorovaikutuksenkin vaikutus haastatteluun on todennettavissa. Haastatteluissa käytettiin samoja kysymyksiä jokaisen asiantuntijan osalta ja kysymykset jätettiin tarkoituksella avoimiksi, jotta he kykenisivät ilmaisemaan näkemyksiään vapaasti. Tarkentavia kysymyksiä käytettiin vain liian laveiden vastausten tarkentamiseen tai, jos he käyttivät haastattelijalle vierasta termiä.

On kuitenkin huomattava, että haastattelumateriaali on epäilyttävän pieni. Neljästä haastateltavasta nousee epäilys siitä, että useammalla haastateltavalla olisi voinut saada mahdollisesti eriytyneitä näkemyksiä. Saturaation saavuttaminen neljällä haastattelulla voi johtua haastattelukysymysten luonteesta. Toisaalta, valitut haastattelukysymykset olivat tutkimuksen tavoitteiden kannalta välttämättömiä.

Selvityksen lopputulos antaa Pelastusopistolle pohjan tietoturvallisuuden johtamis- ja hallintajärjestelmän toteuttamisesta. On huomattava, että selvityksen tulokset ovat käyttökelpoisia mille tahansa pelastuslaitokselle. Tämä ominaisuus on ymmärrettävä, sillä tietoturvallisuus on kaikille pelastusalan toimijoille varsin samanlainen. Pelastuslaitosten osalta merkittävin tekijä on lainsäädännön asettama vaatimus viranomaisten asiakirjojen julkisuudesta.

Selvityksen arvo on sen onnistumisessa laittamaan yksiin kansiin tietoturvallisuuden asiantuntijoiden suositukset hallinnollisen tietoturvallisuuden toteuttamisesta. Kirjallisuuden tarjoamaan tietoon verrattuna haastatteluilla kerättyyn aineistoon perustuva tietoturvallisuuden johtamis- ja hallintajärjestelmä antaa pelastuslaitoksille edellytyksen toteuttaa tietoturvallisuutta niin, että se kehittyy organisaation mukana. Näiden tulosten perusteella Pelastusopisto voi ryhtyä välittömästi tekemään hallinnollisen tietoturvallisuuden ohjeistusta. Olen liitteessä 2 kirjoittanut Pelastusopistolle alustavat toteuttamisohjeet, jonka otsikot vastaavat selvityksen havaintoja. Ohjeet on tehty VAHTI-ohjeiden avulla.

10 Oppimiskokemukset

Opinnäytetyö oli opettavainen prosessi säntilliseen ja järjestelmälliseen työskentelyyn, koska se pakotti minut suunnittelemaan työskentelyäni. Haastavinta oli säilyttää käsitys opinnäytetyön sisällöstä, sillä se muuttui usein. Tämä johtui säännöllisesti tiedon täydentämisestä ja puutteiden korjaamisesta. Olen myös oppinut opinnäytetyöni metodisista heikkouksista. Uskon, että jatko-opinnoissani tämän jälkeen tekemään akateemisesti kypsempää ja vahvempaa tutkimusta.

Pidin opinnäytetyöni aikana päiväkirjaa, johon merkitsin tavoitteita ja korjausehdotuksia. Päiväkirjan pitäminen oli hyödyllistä, sillä sen avulla pystyin pohtimaan kriittisesti, miten käytän selvityksessä käytettyjä tutkimusmenetelmiä ja miten voin perustella niiden käytön.

Menetelmien osalta olen varsin tyytyväinen siihen, että pystyin perustelemaan kypsästi ja rationaalisesti menetelmien käytön. Asiantuntijahaastatteluita ja kirjallisuuskatsausta käytettiin perustelluista syistä, ja menetelmien tuottamien tulosten tuominen rinnakkain mahdollisti tietoon perustuvan vertailun.

Tutkimusmenetelmien valinnoissa tavoittelin tarkoituksenmukaisuutta, joka saavutettiin erityisesti tutkimushaastatteluiden osalta, koska asiantuntijahaastatteluista saadut tulokset antoivat Pelastusopistolle kattavan mallin hallinnollisen tietoturvallisuuden toteuttamiseksi. Haastattelumateriaalista tehdyt johtopäätökset ovat vahvasti perusteltuja vertaamalla niitä hallinnollista tietoturvallisuutta käsittelevän kirjallisuuden kanssa. Opinnäytetyöni vahvuutena on sen kyky havainnollistaa selvityksen vaiheita niin, että lukija kykenisi toistamaan selvityksen.

Toinen onnistuminen oli kansallisen turvallisuusauditointikriteeristön ja Valtionhallinnon tieto- ja kyberturvallisuustyöryhmän tietoturvaohjeiden voimakkaan periaatteellisen yhteneväisyyden todentaminen kansainvälisen tietoturvastandardin ISO 27000 kanssa. Kaikki kolme asiakirjaa pyrkivät tietoturvallisuuden johtamis- ja hallintajärjestelmän luomiseen,

joka perustuu organisaation resursseihin ja toiminnan kannalta relevantteihin riskeihin. Pystyin perustelemaan tämän kypsästi aineistoista tehdyillä havainnoilla, jotka on myös havainnollistettu selkeästi.

Lähteet:

Kirjalliset lähteet

Arkistolaki 24.9.1994/831

Cazemier, J., A. Overbeek, P., Peters, L. 2010. Information security management with ITIL. Wilco, Amerswood: Van haren Publishing.

Euroopan parlamentin ja neuvoston direktiivi yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 2.6.1995/46

Fink, A. 2009. Conducting research literature reviews: from internet to paper- 3rd edition. Washington DC: Sage publications.

Gilham, B. 2005. Research interviewing the range of techniques. Berkshire: Macgraw-hill education.

Hallituksen esitys eduskunnalle arkistolaiksi 23.9.1993/187

Hallituksen esitys eduskunnalle Euroopan neuvoston asiakirjojen julkisuudesta tehdyn yleissopimuksen hyväksymiseksi sekä yleissopimuksen lainsäädännön alaan kuuluvien määräysten voimaan saattamisesta 24.9.2014/116

Hallituksen esitys eduskunnalle perustuslaiksi 6.2.1998/1

Hallituksen esitys eduskunnalle laiksi viranomaisten toiminnan julkisuudesta 9.4.1998/30

Hassinen, M., Marttila-Kontio M., Päivinen, N. 2011. VARANTO ja tietoturva, VARANTO-hankkeen tietoturvaselvitys. Pelastusopisto.

Helenius, M. 2005. Tietoturvallisuus tutkimus ja opetus -nykytilanne ja kehittämismahdollisuudet. Tietojenkäsittelytieteiden laitos, Tampereen Yliopisto.

Hirsjärvi, S., Hurme, H. 2006. Tutkimushaatattelu- Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

Hirsjärvi, S., Remes, P., Sajavaara, P. 2010. Tutki ja kirjoita. Helsinki: Kariston kirjapaino Oy.

Henkilötietolaki 22.4.1999/523

International Standardization Organization. 2013. Information technology. Security techniques. Information security management systems. Requirements 27001

International Standardization Organization. 2013. Risk management –guidance for the implementation. 31004

Jesson, J. K. Matheson, L. Lacey, F. M. 2011. Doing your literature review. Traditional and systematic techniques. London: Sages publications.

Laki potilaan asemasta ja oikeuksista 17.8.1992/785

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 9.2.2007/159

Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621

Lek, K., Rajapakse, M. 2012. Cryptography, Steganography and Data Security : Cryptography : Protocols, Design, and Applications. Hauppauge NY: Nova Science Publishers, Inc.

Mäenpää, O. 2003. Hallintolaki ja hyvän hallinnon takeet. Helsinki: Edita Prima Oy.

Pelastuslaki 29.4.2011/379

Perustuslaki 11.6.1999/731

Pfleeger, C.P., Pfleeger, S.L. 2007. Security in computing fourth edition. Prentice Hall.

Puolustusministeriö. 2011. Kansallinen turvallisuusauditointikriteeristö KATAKRI II. Helsinki.

Valtiovarainministeriö hallinnon kehittämisosasto 2000. Valtiovarainministeriön työryhmämuistioita 11/2000 Hyvän tiedonhallintatavan merkitys. Helsinki

Valtiovarainministeriö. 2014. VAHTIn toimintakertomus vuodelta 2013. Helsinki: Suomen Yliopistopaino Oy.
Whitman, M. E., Mattador, H. J. 2008. Management of information security- Second edition. Massachusetts: Course Technology Cengage Learning.

Elektroniset lähteet

Arkistolaitos 2014. Keskeisiä käsitteitä. Viitattu 29.8.2014
http://www.arkisto.fi/fi/palvelut/julkaisuluettelo/d-verkko-oppaat/caf-itsearviointiopas/keskeisiae-kaesitteitae

Dartmounthin yliopisto 2014. Tietotekniikan Tohtori Charles Pfleeger. Viitattu 26.10.2014
http://www.ists.dartmouth.edu/events/ecampus/bios/cpfleeger.html.

Kansainvälinen atomienergiajärjestö IAEA 2014. Sanasto ja konsepti. 16.8.2014
http://www-ns.iaea.org/standards/concepts-terms.asp.

Kansainvälinen tieto- ja rekisterihallinnon ammattilaisten yhdistys (ARMA international) 2014. Yleistiedot. Viitattu 25.10.2014
http://www.arma.org/r2/who-we-are

Kansainvälinen standardisoimisliitto 2014. Liiton yleistiedot. Viitattu 1.11.2014
http://www.iso.org/iso/home/about.htm.

Kansainvälinen standardisoimisliitto 2014. Standardin kehittämisprosessi. Viitattu 1.11.2014
http://www.iso.org/iso/home/standards_development/resources-for-technical-work/support-for-developing-standards.htm.

Kansainvälinen standardisoimisliitto 2014. Liiton jäsenet ja jäsenyys. Viitattu 1.11.2014
http://www.iso.org/iso/home/about/iso_members.htm.

MOT kielitoimiston sanakirja 2014. Hakusana politiikka. Viitattu 2.11.2014
https://mot.kielikone.fi.nelli.laurea.fi/mot/laurea/netmot.exe.

Kuntien tietosivut 2014. Kuntien asiantuntijapalvelut. Viitattu 21.8.2014
http://www.kunnat.net/fi/asiantuntijapalvelut/yty/turvallisuus/Pelastustoimi/Sivut/default.aspx.

Oikeusministeriö 2014. Perustuslaki esite. Viitattu 25.10.2014
http://oikeusministerio.fi/fi/index/julkaisut/esitteet/perustuslaki.html

Oxfordin verkkotietosanakirja. Hakusana safety. Viitattu 16.8.2014
http://www.oxforddictionaries.com/definition/english/safety.

Oxfordin verkkotietosanakirja 2014. Hakusana security. Viitattu 16.8.2014
http://www.oxforddictionaries.com/definition/english/security.

Oxfordin verkkotietosanakirja 2014. Hakusana information. Viitattu 26.2014
http://www.oxforddictionaries.com/definition/english/information.

Oxfordin verkkotietosanakirja 2014. Hakusana policy. Viitattu 26.10.2014
http://www.oxforddictionaries.com/definition/english/policy

Sanastokeskus 2014. Hakusana data. Viitattu 26.10.2014
http://www.tsk.fi/cgi-bin/netmot.exe?UI=figr&height=160&qfind=Tieto

Suomen Standardisoimisliitto 2014. Perustiedot. Viitattu 1.11.2014
http://www.sfs.fi/sfs_ry

S-ryhmä 2014. Asiakasomistaja- ja asiakasrekisteri. Viitattu 5.11.2014
https://www.s-kanava.fi/web/s/s-kanavan-rekisteriseloste

Viestintäviraston tietoturvavaroitus 1/2011. Viitattu 22.11.2014
https://www.viestintavirasto.fi/tietoturva/varoitukset/2011/varoitus-2011-01.html

U.S Small Business Administration. Viitattu 26.11.2014
https://www.sba.gov/offices/district/fl/jacksonville/resources/obtaining-security-clearance-your-8a-company-andor-employees.

Public Works and Government Services Canada. Viitattu 26.11.2014
http://ssi-iss.tpsgc-pwgsc.gc.ca/msi-ism/ch3-prt2-eng.html

Julkaisemattomat lähteet:

Hilve, A. 2014. VAHTI-sihteeristön pääsihteeri, tietoturvallisuusasiantuntija. Valtiovarainministeriö. Haastattelu 23.9.2014

Laukkala, H. 2014. Riskienhallintapäällikkö. Metso Oyj. Haastattelu 2.10.2014

Rousku, K. 2014. Riskienhallintajohtaja. Valtori. Haastattelu 8.10.2014

Kesäläinen, M. 2014. Erityisasiantuntija. Kyberturvallisuuskeskus. Haastattelu 17.10.2014

Kuvat:

Liitteet

Liite 1: KATAKRI ja VAHTI-haastattelu kysymykset

Taustakysymykset

- Työhistoria turvallisuusalalla?
- Suhde KATAKRI/VAHTI-työryhmään?
- Miten päätyi työryhmään?

Hallinnollinen turvallisuus

- Mitä mielestänne hallinnollinen turvallisuus tarkoittaa?
- Mikä on mielestänne hallinnollisen turvallisuuden merkitys?
- Mitkä ovat hallinnollisen turvallisuuden yleisimmät haasteet?
- Mitä organisaatiosta tulisi ottaa huomioon sen hallinnollisen turvallisuuden suunnittelussa?
- Mikä on mielestänne hallinnollisen turvallisuuden tärkein tekijä?

KATAKRI:n ja VAHTI:n luominen

- Millaiseen ongelmaan tai tarpeeseen KATAKRI/VAHTI luotiin?
- Millaisiin tietolähteisiin hallinnollisen turvallisuuden sisältö perustuu? (KATAKRI)
- Mihin tietolähteisiin ohjeistuksien sisältö perustuu? (VAHTI)
- Millä perusteella auditointikysymyksen valittiin? (KATAKRI)
- Onko KATAKRI:lla/VAHTI:lla esikuvia?
- Onko KATAKRI:ssa /VAHTI:ssa asioita, joita tulisi kehittää?
- Millainen vaikutus KATAKRI:lla/VAHTI:lla on ollut Suomessa?

Liite 2: Tietoturvallisuuden hallinta- ja johtamisjärjestelmän toteuttamisohjeita

Tietoturvallisuuden hallinta- ja johtamisjärjestelmän toteutusohje

Ohjeistuksen tarkoituksena on antaa pelastuslaitoksen johdolle selkeän ohjeen tietoturvallisuuden johtamis- ja hallintajärjestelmän toteuttamisesta. Johtamis- ja hallintajärjestelmän tarkoituksena on antaa pelastuslaitokselle kyvyn ylläpitää tietoturvallisuutta ja kehittää sitä jatkuvasti. Ydinajatuksena on, että organisaatio toimisi jatkuvan kehityksen periaatteella, jolloin varmistetaan, että tietoturvallisuustoimenpiteet keskittyvät aiheellisiin riskeihin.

1.0 Tietoturvapolitiikka

Organisaation johdon tulisi kirjoittaa tietoturvapolitiikka, jossa johto ilmaisisi tavoitteensa ja tahtotilan siitä, mitä tietoturvallisuus tarkoittaa pelastuslaitoksille ja mitä sillä tavoitellaan. Tietoturvapolitiikan kautta johto asettaa tavoitteen kaikille tietoturvallisuuteen liittyville ohjeille, jotka seuraavat tietoturvapolitiikan periaatteita. Tietoturvapolitiikka tulisi kirjoittaa väljästi ja aikaa kestäväksi toisin kuin käytännön työohjeet, jotka voivat muuttua hyvinkin usein. Tämä tavoite johtuu tietoturvapolitiikan ohjaavasta luonteesta.

Mitä tietoturvapolitiikan kirjoittamisessa tulisi ottaa huomioon? Suositeltavaa olisi, että tietoturvapolitiikassa otetaan huomioon mahdollisimman hyvin lain asettamat vaatimukset. Huomion arvoisin, joka koskettaa pelastuslaitosta on laki viranomaisten toiminnan julkisuudesta (621/1999). Tämä lainsäädäntö velvoittaa viranomaisia asiakirjojen säilyttämisessä hyvään tiedonhallintatapaan, joka tarkoittaa viranomaisten asiakirjojen säilyttämistä niin, että tiedon eheys, saatavuus ja luottamuksellisuus eivät kärsi. Kyseinen lainsäädäntö korostaa viranomaisten tiedonantovelvoitetta, jonka tarkoituksena on antaa muulle yhteisölle mahdollisuuden seurata viranomaisen toimintaa. Tämän lisäksi laki viranomaisten toiminnan julkisuudesta (621/1999) säätää, että viranomainen voi asettaa asiakirjan salaiseksi vain lain nojalla.

Tietoturvapolitiikkaan tulee määritellä organisaation sisäiset vastuut tietoturvallisuuden toteuttamisesta. Näin johto antaa tietoturvallisuudesta vastaaville tarvittavan auktoriteetin tietoturvallisuuteen liittyvien toimenpiteiden toteuttamiseksi ja antaa yksiselitteisen vastuun. Tämän lisäksi tietoturvapolitiikassa voidaan määritellä, mitkä ovat pelastuslaitoksen sisäiset velvollisuudet tietoturvallisuuden ylläpitämisessä. Johdon vastuulla on käytännössä tietoturvallisuuden kehittäminen ja resursointi, kun taasen työntekijöiden vastuulla on noudattaa ohjeita ja ylläpitää tietoturvallisuutta. Tästä esimerkkinä on pelastuslain

(379/2011) vaatimus vaitiolo- ja salassapitovelvollisuudesta, joka koskettaa kaikkia työntekijöitä, mikäli siihen on lain antama edellytys

2.0 Tietoturvallisuuden hallinta- ja johtamisjärjestelmä

2.1 Intro

Pelastuslaitos on vastuussa tietoturvallisuutensa ylläpidosta ja kehittämisestä, jotta tämä olisi mahdollista, johdon tulisi käynnistää säännöllisen väliajoin ulkoisia ja sisäisiä tarkastuksia, joiden tavoitteena olisi muodostaa johdolle käsitys organisaation tietoturvallisuuden tasosta. Tämän kaltainen seuranta on tärkeää, sillä ilman seurantaa organisaation tietoturvallisuuden taso ei pysy ajan tasalla. Tarkastuksia tulisi suorittaa säännöllisesti vuoden aikana, joissa tietoturvallisuuden taso arvioidaan määrällisillä ja laadullisilla mittareilla. Mittauksen toteuttamisen tarkemmat ohjeet esitellään myöhemmin tässä luvussa. (VAHTI 2/2004)

Laki viranomaistoiminnan julkisuudesta (621/1999) velvoittaa 18 §:ssä viranomaista noudattamaan tiedon käsittelyssä hyvää tiedonhallinta tapaa. Tämä tarkoittaa muun muassa, että organisaation on suojattava tietoa ja sitä säilyttäviä ja käsitteleviä tietojärjestelmiä. Henkilötietolaki (523/1999) asettaa 5 §:ssä henkilörekisterin ylläpitäjälle huolellisuusvelvoitteen, jonka mukaan rekisterin pitäjän on suojeltava keräämänsä tietoa. Arkistolaki (831/1994) velvoittaa arkistonmuodostajaa säilyttämään asiakirjoja eheinä. Mutta ennen kaikkea turvallisuus tulisi nähdä hallinnossa laatutekijänä, joka parantaa pelastuslaitoksen ulkoista ja sisäistä imagoa(VAHTI 3/2003).

Tietoturvallisuuden hallinta- ja johtamisjärjestelmää tulee ylläpitää jatkuvan kehittämisen periaatteella. Näin varmistetaan, että virastossa on asiaan kuuluva tietoturvallisuuden taso ja virasto pystyy havaitsemaan mahdolliset puutteet, ja tarpeen mahdollisesta muutoksesta tiedon hallinnassa. Jatkuvankehittämisen mallinna käytetään niin kutsuttua PDCA-mallia, joka on mallinnettu ISO 9001 standardista. PDCA-malli koostuu (plan) suunnittelusta ja kehittämisestä, (Do) toteuttaminen ja noudattaminen, (check) valvoa ja arvioida, (act) kehittäminen ja ylläpito.

Suunnittelu- ja kehittämisvaiheessa ajatuksena on arvioida tietoturvallisuuden nykytila ja tehdä parannusehdotuksia; toteuttamis- ja noudattamisvaiheessa tehdyistä havainnoista ja tarpeista tehdään suunnitelma, joka laitetaan täytäntöön; valvonta- ja arviointivaiheessa tarkistetaan toteutetun suunnitelman toimivuus käytännössä; lopuksi, kehittämis- ja ylläpitovaiheessa tehdään suunnitelma mahdollisten puutteiden korjaamiseksi. (VAHTI 3/2003)

2.2 Riskienhallintasuunnitelma

Riskienhallinnan tehtävänä on antaa organisaatiolle realistinen kuva organisaatioon kohdistuvista tietoturvauhista. Tunnistamalla tietoturvallisuuteensa liittyvät riskit, organisaatiolla on kykyä pienentää riskien eskaloitumisen mahdollisuutta ja rajoittaa niiden vaikutuksia. Tunnistamisen lisäksi organisaation tietoturvallisuustoiminnasta tulee riskienhallinnan avulla ohjatumpaa ja tarkoituksen mukaisempaa. Tämä perustuu siihen, että riskiarvion perusteella saadaan realistinen käsitys riskeistä, jolloin niiden torjumiseen ja rajoittamiseen ei käytetä enempää resursseja kuin on tarpeellista. (VAHTI 7/2003.)

Riskienhallinta toteutetaan riskiarvioilla, joka tarkoittaa järjestelmällistä toimintaa, jossa tunnistetaan uhkia ja haavoittuvaisuuksia. Arvioinnin tuloksena johdon tulisi saada käsitys riskein syistä, seurauksista ja kuinka todennäköistä riskin tapahtuminen on. Näillä tuloksilla riskit voidaan luokitella perustuen riskin eskaloitumisen todennäköisyyteen suhteessa sen seurausten vakavuuteen. (VAHTI 7/2003.)

Tietoturvallisuuteen käytetyt resurssit tulee olla suhteessa pelastuslaitoksen päätehtävään, joten koko organisaatioon kohdistuvalla riskiarviolla on merkitystä, jotta saataisiin käsitys asiakirjojen säilyttämiseen ja käsittelyyn tarvittavien ohjeiden ja järjestelmien merkityksestä. Kun tämä on tehty, riskiarviointia kohdennetaan merkityksellisiin järjestelmiin ja ohjeisiin. Näin organisaatio saa realistisen kuvan tietoturvallisuuden merkityksestä organisaatiolle. (VAHTI 7/2003.)

Johdon tulee tehdä osana tietoturvallisuuden johtamis- ja hallintajärjestelmää suunnitelma riskienhallinnan toteuttamisesta. Tämä tarkoittaa käytännössä sitä, että organisaatio suunnittelee, milloin riskiarvioita pidetään ja mitkä osa-alueet arvioidaan. On otettava huomioon, että sitä mukaan kun tunnistettuihin riskeihin reagoidaan, riskikenttä muuttuu, jonka vuoksi riskiarvio tulee uusia säännöllisesti. (VAHTI 7/2003.)

Kun riskit on tunnistettu, johto tekee päätöksen miten se toimii riskin suhteen. Riskienhallinta keinoja ovat pääasiassa riskin välttäminen, joka yleensä vaatii toiminnan lopettamista. Riskin merkitystä voidaan pienentää erilaisilla keinoilla, kuten koulutuksella, tekniikalla ja toiminnan kehittämisellä. Organisaatio voi myös yrittää poistaa riskin esimerkiksi Lopettamalla riskialttiin toiminnan, mikä on harvoin mahdollista tai poistamalla riskin aiheuttaman asian tai laitteen. (VAHTI 7/2003.)

Riski voidaan myös säilyttää eli hyväksyä, jos arvioidaan riskin vähentämisen tuovan kohtuuttomia kustannuksia hyötyyn nähden. Riskin aiheuttaman vahingon voi myös niin sanotusti siirtää esimerkiksi vakuutuksilla. Tämä kuitenkin siirtää vain taloudellisen vahingon. On kuitenkin muistettava, että kaikkiin riskeihin ei ole tarkoituksen mukaista reagoida.

Tärkeintä on säilyttää prioriteetit riskienhallinnassa, jotta organisaatiota voidaan suojella relevanteilta riskeiltä. (VAHTI 7/2003.)

Riskiarvion toteutus on suositeltavaa toteuttaa ryhmässä, joka koostuu henkilöistä, jotka ovat tekemisissä riskiarvion kohteen kanssa. Tämä tarkoittaa, että riskiarvioryhmässä tulee olla mukana henkilöitä organisaation kaikilta tasoilta, jos se on tarkoituksen mukaista. Riskienhallinnan suunnittelu on läheisessä suhteessa tietoturvallisuuden arvioinnin kanssa, jota käsitellään seuraavassa luvussa. Olennaista on se, että riskienarvioinnin avulla määritetään kohde arviointiprosessille. (VAHTI 7/2003.)

2.3 Arviointiprosessin kulku

Arvioinnilla tarkoitetaan prosessia, jonka tarkoituksena on todentaa kohteen sen hetkinen tila, jonka perusteella voidaan tehdä ehdotuksia, jotka johtava positiiviseen muutokseen. Arviointiprosessin vaiheet ovat: suunnittelu, toteutus, raportointi ja seuranta. Tämän osuuden tarkoituksena on ohjeistaa säännöllisen ja dokumentoidun riskienarvioinnin toteuttamiseen. Dokumentointi on merkityksellistä, koska silloin organisaatio voi käsitellä mahdollisia ongelmia johtoryhmän kanssa. Dokumentaation avulla organisaatio voi palata aikaisemmin tehtyihin arviointeihin ja siten nähdä tietoturvallisuuden kehittymisen. Dokumentointi toimii myös konkreettisena todisteena organisaation tietoturvatoiminnasta.(VAHTI 3/2003.)

Organisaation tulee tehdä myös omatoimista arviointia hallinnollisen tietoturvallisuutensa kehittämiseksi, jonka apuna käytetään ennalta tehtyä arviointilomaketta. Omatoiminen arviointi kehittää organisaation omaa turvallisuuskulttuuria, sillä tietoturvallisuudesta tulee näkyväosa organisaation toimintaa. Kuitenkin, ulkopuolisen asiantuntijan tekemä arviointi ei ole merkityksetön, sillä sen avulla organisaatio saa objektiivisen arvion tietoturvallisuutensa tilasta. Omatoiminen arviointi myös säästää resursseja, koska ulkoista asiantuntemusta voidaan kohdistaa sellaisille osa-alueille, joissa organisaatiolla itsellään ei ole tietotaitoa. (VAHTI 3/2003.)

Suunnitteluvaihe

Suunnitteluvaiheessa organisaation johdon tulee tehdä päätös siitä, että mihin arviointi kohdistetaan ja mistä näkökulmasta arviointi tehdään. Näkökulma tulee määritellä, sillä se määrittää arvioinnin tavoitteen. Arviointinäkökulmia ovat: organisaation tavoitteet ja niiden saavuttaminen, lain asettamien velvoitteiden toteuttaminen ja tietoturvallisuus. Tietoturvallisuutta tulee arvioida hallussa olevien viranomaisten asiakirjojen eheyden, saatavuuden, luottamuksellisuuden, kiistämättömyyden ja tunnistettavuuden kannalta.

Näkökulman lisäksi arviointia varten on valittava, että millaisilla mittareilla arviointi toteutetaan. Mittaus voidaan toteuttaa laadullisilla ja määrällisillä mittareilla. Laadullisilla mittareilla pyritään käytännössä arvioimaan ennalta määrätyillä kriteereillä, että millaisella tasolla jonkin asia on. Määrällisillä mittareilla kerätään numeraalista dataa, jotka indikoivat asian toimivuutta. (VAHTI 3/2003.) Lisää mittaamisesta luvussa 3

Tietoturvallisuus koostuu hallinnosta ja tekniikasta, jonka vuoksi tietoturvallisuuden arviointi pitäisi jakaa useampaan osaan, jotka toteutettaisiin yksittäisinä projekteina esimerkiksi vuoden aikana. Arvioitavat osa-alueet tulee valita riskienarvioinnin avulla, joka on esitelty omassa luvussaan. Riskiarvio tulisi tehdä säännöllisesti suunnitelman mukaisesti, jotta arvioinnin kohteet eivät olisi jatkuvasti samoja. Kun arvioitu osa-alue tai kohde on valittu, organisaation tulee rajata arviointikohdetta tarkoituksenmukaiseksi kokonaisuudeksi. (VAHTI 3/2003.)

Suunnitteluvaiheessa tulee perustaa arviointityöryhmä, jonka kokoonpano ja laajuus voidaan määrittää arvioitavan kohteen mukaan. Työryhmässä tulee olla puheenjohtaja, jonka vastuulla on arviointiryhmän vetäminen ja sen kokoaminen. Muita tehtäviä ovat: johdolle raportointi, arviointiryhmän kokousten vetäminen, arviointiryhmän perehdyttäminen ja haastateltavien valinta arviointikohteesta. Arviointiryhmän puheenjohtajan tulisi olla henkilö, jolla on teknistä ja hallinnollista tietoturvaosaamista. Arviointiryhmään tulee käyttää mahdollisia omia arvioijia ja niitä henkilöitä, joilla on tuntemusta arvioitavasta kohteesta.

Arvioinnissa tulee käyttää ulkopuolista asiantuntijaa, mikäli oma tietotaito ei riitä arvioinnin luotettavaan tekemiseen ja halutaan objektiivinen näkemys kohteesta. Ulkopuolisten arvioijien kanssa on pidettävä huolta salassapitosopimuksista, sillä arvioinneissa saadaan tietoa organisaation hallitsemasta tiedosta ja järjestelmistä. Ennen arviointi työn aloittamista ryhmän puheenjohtajan tulisi ilmoittaa ja sopia arvioinnista kohteen kanssa ja varmistaa, että tarvittavat resurssit ovat käytössä. (VAHTI 3/2003.)

Toteutusvaihe

Arvioinnin kattavuus toteutusvaiheessa on riippuvainen siitä, että miten hyvin kohteen kanssa tehty yhteistyö onnistuu. Parhaat tulokset saadaan silloin, kun kohdetta voidaan arvioida perinpohjaisesti ilman rajoituksia. Arvioinnin toteuttaminen aloitetaan avauskokouksella, jonka tarkoitus on sopia tavoitteista, aikataulusta, henkilöhaastatteluista, tarvittavista dokumenteista ja kohteeseen tutustumisesta. Työryhmän on syytä tutustua kohteeseen, jotta se saa käsityksen arvioitavan kohteen tarkoituksesta, miten se on toteutettu, millaisia vaatimuksia lainsäädäntö on asettanut, riskianalyysit ja aiemmat arviot. Tämän jälkeen arviointi toteutetaan sovitun aikataulun mukaisesti. (VAHTI 3/2003.)

Raportointi

Raportoinnissa arviointiryhmän on oltava havainnoissaan rehellinen ja muistettava raportoida myös kunnossa olevat asiat. Tarkoitus on luoda realistinen kuva arvioitavan kohteen tietoturvallisuudesta, jolle esitetään tarkoituksenmukaisia parannusehdotuksia. Parannusehdotuksissa tulee kiinnittää huomiota, mikä on tarkoituksen mukainen turvallisuuden taso. Näin mahdollistetaan kustannusten kohtuullisuus. Tämän vuoksi raportissa asiat tulee esittää oheisen taulukon mukaisesti

Kuvattu seikka	Selite
Havainto	Millainen puute taikka ongelma havaittiin ja missä järjestelmässä taikka ohjeessa
Kriteerit	Millä perusteella ilmoitettu puute on ongelmallinen. Onko se esim. jonkin ohjeen, standardin tai lain vastainen
Syy	Mistä kuvailtu ongelma johtuu
Merkitys	Millä tavalla havaittu puute on ongelma
Johtopäätös	Mitä arvioinnin tekijä suosittelee tehtäviksi puutteen korjaamiseksi
Vastine	Mitä asianosainen aikoo tehdä asialle. Huom. Tämä kirjoittaan erikseen raportin jälkeen. Vastineen kirjoittaa se taho, jolla on kyky päättää asiasta

Taulukko 1: Puutteiden raportointiohje arviointiraportissa

Kun arviointiryhmän raportti asetetaan johdolle luettavaksi, sen mukana tulee saatekirje, jossa selitetään, mistä on kysymys. Tämän jälkeen johto kirjoittaa raportille vastineen, jossa se määrittää mihin toimenpiteisiin se ryhtyy. Saatekirje sisältää konkreettiset toimenpiteet, aikataulun ja vasteesta vastaavan henkilön. Tietoturvallisuutta arvioidessa dokumentit on syytä luokitella vähintään luottamuksellisiksi. Arvioinnissa syntyneet dokumentit tulee säilyttää asianmukaisesti seuraavaa arviointia varten. (VAHTI 3/2003.)

Raportissa käytettävät luvut:

Tiivistelmä	Selostaa koko arviointiraportin tulokset pääpiirteittäin ja mahdolliset toimenpiteet johon tulisi ryhtyä

Johdanto	Selostetaan mikä on raportin tavoite ja millaisilla menetelmillä se on saavutettu. Eli mikä on näkökulma ja millaisia mittareita käytetään. Selostetaan myös kohde ja työryhmä.
Tulokset ja Johtopäätökset	Millaisia tuloksia löydettiin ja mistä ne johtuvat
Havainnot ja suositukset	Mitä havaituille puutteille tulisi tehdä

Taulukko 2: Arviointiraportin sisällysluettelo

2.4 Sisäinen ja ulkoinen arviointi

Tietoturvallisuuden laadun edistämiseksi voidaan tehdä sisäisiä ja ulkoisia arviointeja. Sisäisen- ja ulkoisenarvioinnin tavoitteena on kartoittaa tietoturvallisuuden nykytila, josta tehtyjen havaintojen perusteella voidaan tehdä kehittämisehdotuksia. On muistettava, että jokainen arviointi antaa kohteesta vain sen hetkistä tietoa, minkä vuoksi arviointeja tulee tehdä säännöllisesti erillisen vuosisuunnitelman mukaisesti. Näin varmistetaan, että tietoturvallisuus ei jää paikoilleen vaan kehittyy ajansaatossa. Näin koko organisaation tietoturvallisuus kehittyy ajan myötä. (VAHTI 3/2003.)

Sisäisen tarkastuksen pääsääntöinen ajatus on, että organisaatio itse arvioi tietoturvallisuutensa hallinta- ja johtamisjärjestelmän toimivuutta. Tämä tarkoittaa, että organisaatio arvioi vastaako hallinta- ja johtamisjärjestelmä organisaation tarpeita. Johtamis- ja hallintajärjestelmän arviointia varten on tehty erillinen dokumentti tätä varten. Esimerkiksi voidaan arvioida: onko tietoturvapolitiikka ajan tasalla, vastaako koulutussuunnitelma ongelmatarpeisiin, tarvitseeko poikkeamaohjeita päivittää ja niin edelleen. Olennaista on arvioida sellaisia kohteita, jotka ovat relevantteja riskiarvion mukaan. Arvioinneista voi tulla laajoja ja niitä voi tulla useita, minkä vuoksi arvioinnit on syytä jakaa osiin arviointisuunnitelmalla. (VAHTI 3/2003.)

Sisäisiä tarkastuksia voidaan kohdistaa myös merkityksellisiin tietojärjestelmiin ja tekniikkaan, jos organisaatiolla itsellään on osaamista sen toteuttamiseksi. Tällaista kutsutaan erityisvastuuhenkilöiden tekemiksi arvioinneiksi. Nimitys viittaa siihen, että heillä erityinen tehtävä tietoturvallisuuden ylläpidossa, henkilö on esimerkiksi tietoturvavastaava. Tällaista sisäistä toimintaa voidaan kuvailla sisäiseksi auditoinniksi, jos hän arvioi kohteen, joka ei liity suoraan hänen työtehtäväiin. Muutoin kyse on itse arvioinnista. (VAHTI 3/2003.)

Ulkoisen arvioinnin hyviä puolia on objektiivisuus, jolloin voidaan saada selville asioita, joita sisäisessä tarkastuksissa ei välttämättä käy ilmi. Toinen tavoiteltava hyöty on varmistettu

asiantuntijuus, jota organisaatiolla itsellään ei välttämättä ole. Ulkoista arviointia voi esimerkiksi tilata tilintarkastusyrityksistä, tietoturvakonsulteilta ja isoilta IT-yrityksiltä. On kuitenkin syytä harkita yhteistyön tekemistä muiden viranomaisten, kuntien ja valtion kanssa. Esimerkiksi henkilötietojen säilyttämisestä ja suojaamisesta, konsultaatiota saa tietosuojavaltuutetulta. (VAHTI 3/2003.)

3.0 Mittaaminen

Tietoturvallisuuden tasoa voidaan parantaa vain silloin, kun sitä voidaan mitata. Mittaamalla pystytään saamaan dokumentaatiokelpoista tietoa tietoturvallisuuden tasosta, jota voidaan myös verrata. Vertailukelpoiset mittaukset antavat organisaatiolle mahdollisuuden seurata kehitystään ja havaitsemaan ongelma-alueitaan. Mittaustuloksilla pystytään myös perustelemaan johdolle investointeja vaativia toimenpiteitä tietoturvallisuuden parantamiseksi. Esimerkiksi, jos arvioinnissa tehtävissä haastatteluissa huomataan, että henkilöstöllä ei ole selkeää käsitystä tietoturvallisuuden merkityksestä, sillä voidaan perustella koulutussuunnitelman luomiseen taikka kehittämiseen. (VAHTI 3/2003.)

Mittaus voidaan suorittaa joko laadullisilla tai määrällisillä mittareilla. Laadullisissa mittareissa mittaus tapahtuu tasolla, että onko asia tehty vai ei. Esimerkiksi laadullisissa mittareissa voidaan kysyä, onko organisaatiolla riskienhallintapolitiikka ja riskienhallintasuunnitelmaa. Laadullisessa mittauksessa tulisi myös tehdä henkilökunnan haastatteluita, jotta tietoa voidaan syventää. Esimerkiksi, haastatteluilla voidaan selvittää, kuinka tietoisia työntekijät ovat tietoturvallisuuden merkityksestä organisaatiolle. Laadullisen mittaamisen lopullinen tavoite on antaa organisaatiolle kypsyystaso, jotka ovat:
0 taso: Toimintaa ei ole
1 taso: Ad-Hoc tasolla, toimintaa ei ole organisoitu
2 taso: Toimiva prosessi, joka voidaan toistaa
3 taso: Toiminta on dokumentoitu ja tiedotettu
4 taso: Toimintaa voidaan arvioida
5 taso: Toimenpiteet ovat optimoituja ja osittain automatisoituja.
Päästäkseen tietylle tasolle, organisaation tulee saavuttaa sama taso kaikissa mitattavissa osa-alueissa. (VAHTI 3/2003.)

Määrälliset mittarit tuottava puhtaasti numeraalista dataa, jonka avulla voidaan saada yksityiskohtaista tietoa tietoturvallisuuden tasosta. Toinen tavoite on myös mitata korjaavien toimenpiteiden vaikutusta arviointikohteeseen tai tiettyyn järjestelmään. Näitä voi olla esimerkiksi raportit tietojärjestelmän toimintavarmuudesta ja vakaudesta. (VAHTI 3/2003.)

4.0 Tiedon luokittelu

Julkishallinnossa tiedon luokittelu pohjautuu pitkälti lainsäädäntöön viranomaisten toiminnan julkisuudesta (621/1999).(VAHTI 3/2007, 83). Koska tämän opinnäytetyön tekemä selvitys menee pelastusviranomaisten tietoturvallisuuden kehittämiseen, tietojen luokittelua käsitellään tässä luvussa lain asettamien vaatimusten kautta. Lain asettamia vaatimuksia on käsitelty luvussa 4.