DIGI- JA VÄESTÖTIETO-VIRASTO

Digiturvallisuuden hallinta

VAHTI hyvät käytännöt tukimateriaali

1.12.2021

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

VAHTI-sihteeristö

1.12.2021

Sisällysluettelo

VAHTI-sihteeristö

1.12.2021

Digiturvallisuuden hallinta

Tässä käsikirjassa ja sen liitteissä määritellään digitaalisen turvallisuuden viitekehys ja kuvataan malleja, joilla digitaalisen toimintaympäristön turvallisuutta kehitetään johdonmukaisesti. Erilaisilla organisaatioilla valmiudet ja resurssit digitaalisen turvallisuuden kehityshankkeiden toteuttamiseksi ovat hyvin erilaiset. Oppaassa on pyritty kuvaamaan mahdollisimman konkreettisia toimintamalleja ja ratkaisuja, jotka ovat sovellettavissa eri tyyppisten ja kokoisten organisaatioiden toimintaan. Oppaan liitteissä on tarkemmat kuvaukset riskienhallinnan ja jatkuvuuden hallinnan toteuttamiseksi niissä organisaatioissa, joilla on halua ja resursseja toteuttaa kansainvälisten standardien mukaisia hallintajärjestelmiä.

Tämä materiaali on tuotettu Digi- ja väestötietoviraston JUDO-hankkeessa yhteistyössä Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän alaisuudessa toimivan VAHTI-työryhmän kanssa. Se julkaistaan osana Digi- ja väestötietoviraston digiturvan hyvät käytännöt -julkaisusarjaa. Tätä tukimateriaalia ei saa sellaisenaan laittaa jakoon, mutta jokainen organisaatio voi hyödyntää ja soveltaa sitä oman toimintansa kehittämisessä.

Toivomme, että annat meille palautetta tästä materiaalista. Saatuamme riittävästi parannus ja korjausehdotuksia, julkaisemme tästä päivitetyn version.
Linkki palautekyselyyn.

Saatuamme riittävästi kehittämisideoita, korjauksia tai muuta palautetta, julkaisemme tästä tukimateriaalista päivitetyn version.

Tämä materiaali on tarkoitettu organisaatioiden digitaalisen turvallisuuden eri osa-alueista vastaaville asiantuntijoille.

1 Digitaalisen turvallisuuden viitekehys

Jokaisella organisaatiolla on tehtävä – olemassaolonsa tarkoitus. Julkisessa hallinnossa organisaatioiden päätehtävät on määritelty lainsäädännössä. Digitaalinen toimintaympäristö on nykyään olennainen osa kaikkien organisaatioiden toimintaa, eikä sitä pidä käsitellä irrallisena osana. Samoin digitaalisen toimintaympäristön turvallisuus (digitaalinen turvallisuus tai digiturvallisuus) on erottamaton osa tätä modernia toimintaympäristöä. Digitaalinen turvallisuus tukee organisaation tehtävän ja tavoitteen mahdollisimman häiriötöntä hoitamista, samoin kuin fyysisen maailmankin turvallisuusratkaisut. Organisaation turvallisuuden toteuttamisessa ja ylläpidossa tarvitaan monipuolista osaamista, mutta digitaalista turvallisuutta tulee kehittää yhteistyössä muun turvallisuuden kanssa. Niiden eriyttäminen voi helposti johtaa tehtävien siiloutumiseen, mikä ei palvele organisaation kokonaistarpeita.

Digitaalisen turvallisuuden viitekehys koostuu seuraavista osa-alueista:

1. Riskienhallinta
2. Toiminnan jatkuvuus ja varautuminen
3. Tietoturvallisuus
4. Tietosuoja
5. Kyberturvallisuus

Viimeisen 20 vuoden aikana toiminnan turvaamisessa on tapahtunut merkittävä muutos. 2000-luvun alkupuolella keskityttiin vahvasti **tietoturvallisuuteen**, erityisesti tiedon luottamuksellisuuden varmistamiseen, jolloin tiedon eheyteen ja saatavuuteen ei panostettu samassa määrin. Toiminnan digitalisaation myötä erityisesti tietojen ja palveluiden saatavuuden merkitys on noussut merkittävään asemaan. Tätä korostaa myös se, että entistä enemmän julkisen hallinnon tuottamasta tiedosta on julkista, ja näitä tietoja tarvitaan ajasta ja paikasta riippumatta kaikkina vuoden ja vuorokauden aikoina.

2010-luvulla fyysinen maailma ja digitaalinen toimintaympäristö ovat kietoutuneet yhä enemmän toisiinsa. Koska niihin kohdistuvat uhat voivat vaikuttaa yhteiskunnan ja organisaatioiden toimintaan laaja-alaisesti, **kyberturvallisuudesta** on tullut entistä merkittävämpi osa-alue. Tietoturvallisuuden lisäksi digitaaliseen toimintaympäristöön kohdistuu myös uusia uhkia, joita ovat mm. hybridiuhat, informaatiovaikuttaminen ja kybervaikuttaminen.

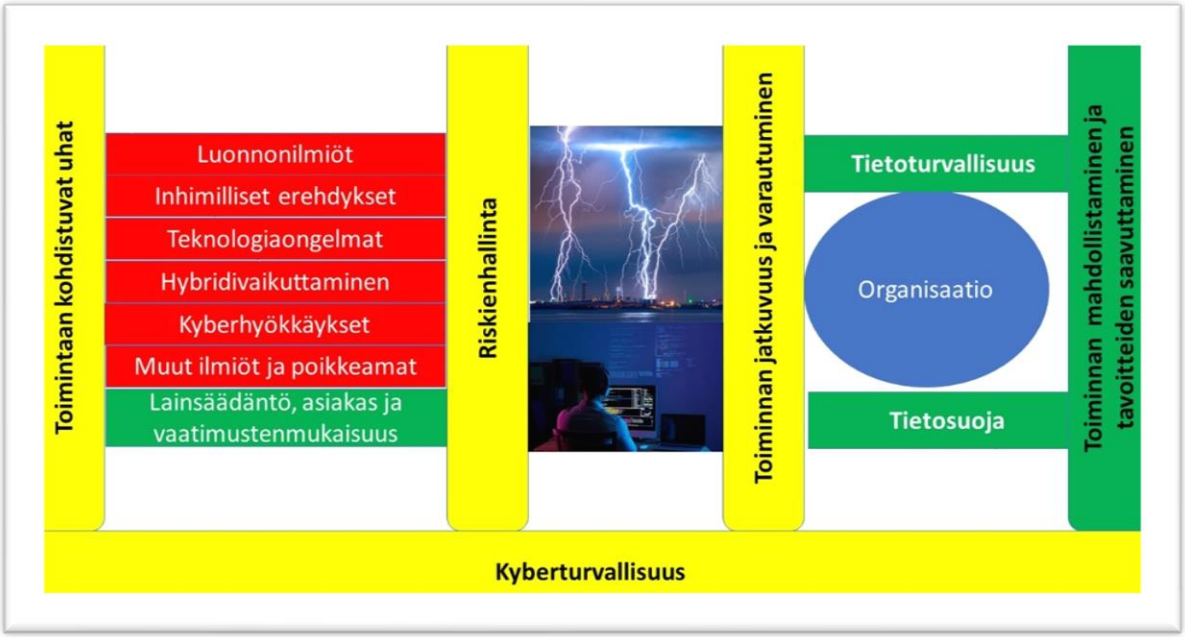
Julkisen hallinnon toiminnan digitalisoitumisen myötä yhä enemmän kansalaisten ja asiakkaiden henkilötietoja käsitellään sähköisesti – tämä on merkittävästi kasvattanut **tietosuojan** merkitystä. Erityisesti 25.5.2018 sovellettavaksi tullut EU:n yleinen tietosuoja-asetus on parantanut, ei pelkästään tietosuojan vaan samalla myös tietoturvallisuuden kehittämistä ja toteuttamista.

Kaikkiin edellä kuvattuihin digiturvan osa-alueisiin liittyy **riskienhallinta**. Organisaation jokapäiväisen toiminnan toteuttaminen ei voi tapahtua tarkoituksenmukaisesti, taloudellisesti ja turvallisesti ilman toimivaa riskienhallintaa. Sen avulla organisaatio pystyy paremmin varmistamaan sille asetettujen strategisten tavoitteiden

saavuttamisen sekä turvaamaan jokapäiväisen toiminnan niin fyysisessä kuin digitaalisessa toimintaympäristössä. Lisäksi riskienhallinnan avulla organisaatio pystyy kustannustehokkaasti kohdistamaan digitaalisen turvallisuuden kehittämistoimet sen toimintaa eniten uhkaaviin kohteisiin ja osa-alueisiin. Ilman jatkuvaa riskienhallintaprosessia turvallisuuden kehittäminen tapahtuu pistemäisesti, osin hallitsemattomasti ja ilmeisiä toimintaa uhkaavia tekijöitä saattaa jäädä tunnistamatta.

Digitaalisen turvallisuuden viidennen osa-alueen, **toiminnan jatkuvuuden ja varautumisen** avulla varmistetaan organisaation jokapäiväinen kyvykkyys selviytyä niistä riskeistä, jotka kaikista ennakoivista suojatoimista huolimatta pääsevät toteutumaan. Digiturvan osa-alueista toiminnan jatkuvuuden ja varautumisen merkitys on noussut kenties eniten tietosuojan ohella. Sen avulla huolehditaan kaikista organisaation toimintaan kohdistuvista ja vaikuttavista häiriöistä – ei pelkästään tietoturvallisuuden tai tietosuojan pettämisen takia syntyvistä poikkeamista, häiriöistä ja loukkauksista. Mitä enemmän otamme käyttöön fyysisten palveluiden ja toimintamallien sijaan digitaalisessa toimintaympäristössä toimivia palveluita, sitä enemmän niihin kohdistuvilla häiriöillä ja poikkeamilla on vaikutusta toimintaamme.

Lisätietoja: Valtioneuvoston periaatepäätös julkisen hallinnon digitaalisesta turvallisuudesta (VM/2020/47), Tiedonhallintalautakunta, Yhteiskunnan turvallisuusstrategia (YTS) 2017, Kyberturvallisuusstrategia 2019.



Kuva 1. Digitaalisen ja samalla fyysisen toimintaympäristön suojaaminen edellyttää tasapainoista kaikkien digiturvan osa-alueiden huomioimista ja kehittämistä.

2 Hallintajärjestelmistä

Digitaalisen turvallisuuden osa-alueita ylläpidetään ja kehitetään jatkuvan ja systemaattisen toiminnan avulla, mikä muodostaa hallintajärjestelmän tai hallintamallin. Tällä tarkoitetaan tässä käsikirjassa kokonaisuutta, jonka muodostavat ennalta

valmistellut menettelytavat ja niitä tukevat asiakirjat. Hallintamallissa kuvataan osa-alueen tavoitteet ja toimenpiteet, joilla tavoitteet saavutetaan sekä vastuiden jako. Hallintamallin tarkoitus on tukea määrämuotoista toimintaa organisaation digitaalisen turvallisuuden osa-alueiden tavoitteiden saavuttamiseksi.

Riskien hallintamallia esitellään tämän oppaan kappaleessa 2.2 ja se on kuvattu tarkemmin tämän oppaan liitteessä 1. Digitaalisen toimintaympäristön turvaamisessa tärkeitä osia ovat myös toiminnan jatkuvuuden, tietoturvallisuuden ja tietosuojan hallintamallit, joiden perusrakenteet esitellään tämän oppaan luvuissa 3 – 5. Jatkuvuuden hallinnan hallintamallin tarkempi kuvaus löytyy liitteestä 2. Edellä mainittujen hallintamallien kytkeytymistä kyberturvallisuuden kehittämiseen on kuvattu tämän oppaan luvussa 6.

Edellä mainituissa hallintamalleissa on useita yhteneviä osia, joten yhtä hallintamallia toteutettaessa saadaan sivutuotteena valmiita osia muihinkin. Tärkeimpiä yhteisiä osuuksia ovat toimintaympäristön tunteminen ja kuvaaminen, riskien hallinta ja jatkuva parantaminen.

Koska saman tiedon monistaminen useisiin paikkoihin johtaa nopeasti ristiriitaisuuksiin, hallintamallin dokumentaatiossa viitataan soveltuviin, olemassa oleviin asiakirjoihin aina kun tarvittava tieto löytyy niistä. Hallintamallin kuvauksessa määritellään hallintamallin tavoitteet, jotka voidaan kuvata esimerkiksi tietoturvapolitiikassa (tietoturvallisuus), jatkuvuussuunnitelmassa (toiminnan jatkuvuus) tai muussa soveltuvassa asiakirjassa. Tärkeintä on, että tavoitteet ovat kirjattuna, helposti löydettävissä ja kaikkien tiedossa.

Digitaalisen turvallisuuden hallintajärjestelmien rakentaminen noudattaa samaa kaavaa:

1) Tunnista toimintaympäristö (organisaation tehtävä, sidosryhmät)
2) Määrittele tavoitteet ylätasolla (strategiset linjaukset)
3) Arvioi riskit ja niiden vaikutukset (riskien arviointi ja vaikutusanalyysi)
4) Kohdista resurssit riskiarvion ja asetettujen tavoitteiden mukaisesti (hallintatavoitteet)
5) Määrittele toimenpiteet, joilla tavoitteisiin on tarkoitus päästä ja varmista tulokset (hallintakeinojen mittaus ja seuranta)
6) Kehitä hallintamallia havaintojen perusteella (jatkuva parantaminen)

2.1 Toimintaympäristö

Hallintamallien perustana on toimintaympäristön tunnistaminen, mikä on tavoitteiden määrittämisen edellytys. Toimintaympäristön tunnistamisen kolme keskeistä aluetta ovat:

1) organisaation oman tehtävän ja tarkoituksen kuvaaminen
2) keskeisten sidosryhmien ja niiden tarpeiden tunnistaminen

3) hallintamallin soveltaminen ja vastuut

Organisaation tehtävä ja tarkoitus ovat yleensä hyvin tiedossa, olipa kyseessä sitten kunta tai kaupunki, ministeriö, virasto tai laitos, tai muu julkishallinnon yksikkö. Säädöksissä, työjärjestyksissä tai johtosäännöissä kuvataan organisaation ja sen osien tärkeimmät tehtävät ja vastuut. Hallintamallin kuvauksessa dokumentoidaan edellä mainitut asiat ja siinä voidaan viitata soveltuviin, olemassa oleviin asiakirjoihin.

2.2 Riskienhallinta

Riskienhallinnalla tarkoitetaan prosessia, jossa tunnistetaan organisaation toimintaa ja tarkoitusta uhkaavia tekijöitä, arvioidaan uhkien toteutumisen todennäköisyyksiä ja vaikutuksia, sekä suunnitellaan toimenpiteet riskien hallitsemiseksi. Toteutettavaksi valittuja toimenpiteitä seurataan ja arvioidaan niiden vaikuttavuutta. Riskienhallintaa on kuvattu kattavasti tämän oppaan liitteessä 1. Riskienhallinnalle voidaan määritellä oma hallintamallinsa, mutta riskienhallintaprosessin sisällyttäminen muihin hallintajärjestelmiin on usein riittävä ratkaisu.

Riskejä on arvioitava jatkuvasti ja säännöllisesti. Arviointiin vaikuttavat tyypillisesti erilaiset organisaatiota, sen toimintaympäristöä tai koko yhteiskuntaa koskevat tapahtumat. Arvioinnissa on syytä katsoa myös eteenpäin ja arvioida riskejä esimerkiksi yhden ja kolmen vuoden tarkastelujaksolla. Esimerkiksi koneiden ja laitteiden vikaantumisen todennäköisyys kasvaa niiden ikääntymisen myötä ja toisaalta hyvin toteutettu varautuminen vähentää riskien toteutumisen vaikutuksia. Kaikille riskiarvioille on tärkeää, että koko organisaatiossa noudatetaan yhtenäisiä prosesseja ja arviointiasteikkoja sekä sovelletaan niitä samoilla periaatteilla vertailtavuuden mahdollistamiseksi.

2.2.1 Riskien tunnistaminen

Riskien tunnistamista ja arviointia tehdään organisaation kaikilla tasoilla; toiminnallisessa yksikössä tunnetaan todennäköisesti parhaiten käytännönläheiset, toimintaan vaikuttavat riskit, kun taas johdon vastuulla on tunnistaa koko organisaation toimintaa uhkaavat tekijät. Riskejä voidaan tunnistaa esimerkiksi ihmisten, toimitilojen, tietojärjestelmien, tai sidosryhmien näkökulmista. Organisaation riskit kootaan yhteen riskirekisteriksi, jonka avulla seurataan organisaation riskitasoa sekä riskienhallinnan toimenpiteitä ja niiden vaikuttavuutta. Riskirekisteriä voidaan ylläpitää järjestelmässä tai yksinkertaisimmillaan se voi olla Excel-taulukko, johon kootaan riskeistä tarvittavat tiedot.

2.2.2 Riskien arviointi

Kun riskit on tunnistettu, arvioidaan niiden toteutumisen **todennäköisyyksiä** ja vaikutuksia. Arvioinnin perusteella voidaan valita kriittisimmät riskit, joiden hallitsemiseen käytössä olevat resurssit (henkilötyö, osaaminen, rahat) kohdistetaan. Todennäköisyyden arvioinnissa käytetään yleisesti kolmi-, neli- tai viisiportaista asteikkoa, jossa arvo 1 kuvaa epätodennäköistä tai hyvin epätodennäköistä riskiä ja asteikon suurin arvo lähes varmasti toteutuvaa riskiä.

Riskien toteutumisen **vaikutuksia** arvioidaan eri näkökulmista organisaation tarpeiden mukaan. Tyypillisesti arvioidaan vaikutuksia julkisuuskuvalle tai maineelle, työyhteisölle (esim. menetetty työaika, lisääntyvä työn kuormittavuus), operatiiviselle toiminnalle ja palvelujen saatavuudelle (esim. lakisääteisten tehtävien hoitaminen),

sidosryhmille tai taloudelle (esim. menetetyt myyntitulot). Asteikkona käytetään edellä kuvatun tapaan 3 - 5 -portaista asteikkoa, jossa arvolla 1 kuvataan hyvin vähäistä tai lähes mitätöntä vaikutusta ja asteikon yläpäässä on erittäin suurta, lamauttavaa tai katastrofaalista vaikutusta riskin kohteelle (esim. henkilöstö, organisaatio, toiminto, palvelu tai järjestelmä). Lisäksi on syytä arvioida riskin toteutumisen taloudellisia vaikutuksia ts. minkä suuruisia taloudellisia menetyksiä riskin toteutuminen voi aiheuttaa.

Todennäköisyyden ja vaikutuksen avulla voidaan laskea riskille **riskiluku**, jonka perusteella riskien vakavuutta voi vertailla. Riskiluku sisältää kuitenkin epävarmuustekijöitä (esim. henkilökohtaiset näkemykset, tarkastelun aikaperspektiivi tai tietämys riskin kohteesta), mikä on hyvä ottaa huomioon riskilukujen vertailussa.

2.2.3 Riskien käsittely

Kun riskit on arvioitu ja niille muodostettu vertailtavat riskiluvut (esim. todennäköisyyden ja vaikutuksen tulona), voidaan riskit asettaa kriittisyyden mukaan järjestykseen. Riskien vähentämiseen tähtäävät toimenpiteet kohdistetaan kriittisimpiin riskeihin. Toimenpiteiden tarkoituksena (hallintatavoitteena) on pienentää riskin toteutumisen todennäköisyyttä tai vähentää toteutumisen vaikutuksia. Tätä varten valitaan käytettävissä olevien resurssien puitteissa toimenpiteitä (hallintakeinot), joiden avulla riskilukua saadaan pienennettyä. Tämä edellyttää myös vastuiden ja aikataulujen määrittämistä, joiden toteutumista tulee säännöllisesti seurata. Yleensä riskejä ei voida kokonaan poistaa, mutta riskitaso on saatava tuotua hyväksyttävälle tasolle. Hallintakeinojen avulla saavutetun tason (jäännösriskit) hyväksyy organisaation ylin johto.

Taulukko 1: Esimerkki riskien arvioinnista

Riski-luokka	Riskin kuvaus	Todennäköisyys (1-5)	Kokonaisvaikutus (1-5)	Riskiluku
Ihmiset	Suuri joukko ihmisiä ei tule töihin (syynä voivat olla esim. pandemia, työtaistelutoimi, tai onnettomuus, joka estää toimitilojen käytön)	3	4	12
Toimitilat	Tyrskylän kunnantalolla sattuu vesivahinko	1	4	4
Tietojärjestelmät	Tyrskylän kunnanvaltuuston työasemissa havaitaan haittaohjelma	2	5	10

Lisätietoja: ISO/IEC 31000, ISO/TR 31004, VAHTI 1/2017, Kansallinen riskiarvio 2018

2.2.4 Riskien seuranta ja raportointi

Riskienhallintakeinojen vaikuttavuus ja tehokkuus varmistetaan seurannan ja katselmoinnin avulla. Ne suunnitellaan osaksi riskienhallintaprosessia ja vastuut määritellään ja viestitään selvästi. Seurantaan ja katselmointiin kuuluu myös toimenpiteiden toteutumisen valvonta, jota voidaan tehdä määrävälein tai tapauskohtaisesti.

Riskien tunnistaminen, analysointi ja niiden merkityksen arviointi edellyttävät arvioinnin kohteena oleviin riskeihin ja toimintaympäristöön liittyvien osapuolten välistä viestintää. Myös riskien käsittely edellyttää niihin liittyvien osapuolten välistä aktiivista ja säännöllistä tiedonvaihtoa niin kauan kuin riski on olemassa.

Riskienhallinnan tilanteesta raportoidaan säännöllisesti organisaation johdolle, jonka tiedossa tulee olla kokonaiskuva riskitilanteesta ja sen kehittymisestä. Johdolla on mahdollisuus ohjata resursseja tarkoituksenmukaisella tavalla riskitilanteen hallintaan.

2.3 Jatkuva parantaminen

Digitaalinen toimintaympäristö muuttuu jatkuvasti ja muutokset tapahtuvat nopeasti. Siksi hallintamalliakin kehitetään ja parannetaan jatkuvasti, jotta muutosten vaikutuksia organisaation toimintaympäristöön voidaan paremmin hallita.

Jatkuvaa parantamista toteutetaan usein ns. PDCA-mallin avulla. Suunnitteluvaiheessa (Plan) asetetaan hallintamallille tavoitteet ja toteutusvaiheessa (Do) toteutetaan suunnitellut toimenpiteet tavoitteiden saavuttamiseksi. Seurantavaiheessa (Check) kootaan yhteen seuranta- ja mittaustietoja hallintamallin toiminnasta ja verrataan näitä asetettuihin tavoitteisiin. Kehittämisvaiheessa (Act/Adjust) arvioidaan mm. mallin suorituskykyä ja mahdollisia poikkeamia, joiden perusteella tavoitteita voidaan tarkentaa seuraavaa päivityskierrosta varten.

Jatkuvan parantamisen tarkoituksen on ylläpitää hallintamallia toimintaympäristön muuttumisen myötä. Toteutus sidotaan organisaation kehittämisen vuosikelloon, mutta sykli asetetaan organisaation tehtävän, toimintaympäristön muutosten nopeuden tai laajuuden mukaisesti.

2.4 Vastuunjako

Hallintamallien tehtävien hoitamisen edellytyksenä on, että kaikki osapuolet tuntevat vastuunsa ja velvoitteensa. Yleensä tehtävänkuvaukset on kirjattu työjärjestyksiin tai vastaaviin asiakirjoihin, mutta vastuut on hyvä koota kuhunkin hallintamalliin helposti hahmotettavaksi kokonaisuudeksi. Vastuunjakotaulukko (RACI-malli) on yksi tapa esittää tehtävät ja niihin liittyvät vastuut tiivistetyssä muodossa.

Vastuunjakotaulukon ensimmäiseen sarakkeeseen kirjataan hallintamallin tärkeimmät tehtävät. Seuraavien sarakkeiden otsikkoina ovat hallintamallin tehtävien kannalta merkittävimmät roolit tai sidosryhmät. Kullekin riville merkitään vastuut seuraavasti:

- Kullekin tehtävälle määritellään **vähintään** yksi tekijä (R – responsible), joka on vastuussa tehtävän käytännön toteuttamisesta

- Jokaisella tehtävällä on **täsmälleen** yksi vastuutaho (A – accountable), joka on vastuussa siitä, että tehtävä hoidetaan, ja joka voi tehdä tehtävää koskevia päätöksiä ja hyväksyä tulokset
- **Tarvittaessa** voidaan kuvata yksi tai useampi konsultoiva rooli tai sidosryhmä (C – consulted), joilta voidaan saada mielipiteitä tai erityistietoja tehtävän suorittamista varten
- **Tarvittaessa** voidaan kuvata yksi tai useampi rooli tai sidosryhmä, jotka tarvitsevat tietoa tehtävän suorittamisesta (I – informed)

Taulukko 2: Esimerkki vastuunjakotaulukon käytöstä

Tehtävä	Johto-ryhmä	Viestintä	Tietoturva-vastaava	Tietosuoja-vastaava	Valmiusyk-sikkö	Tietohal-linto
Jatkuvuussuunnitelman laatiminen	A	C	C	C	R	C
Strategisten riskien arviointi	R/A		C	C	C	C
Tietoturvariskien arviointi	A		R	C		R
Kyberturvariskien arviointi	A		C		R	R/C
Tietoturvapolitiikan laatiminen	A	I	R	C	C	C
Tietosuojaloukkauksesta ilmoittaminen	I	I	I	R/A		C
Kyberturvallisuusharjoituksen valmistelu	A	C	C	C	R	C

2.5 Vaatimustenmukaisuus

Organisaation digitaalisen turvallisuuden osa-alueiden tavoitteet perustuvat usein johonkin yleiseen viitekehykseen. Perustana voi olla kansainvälinen standardi (esim. ISO/IEC 27001 Tietoturvallisuuden hallintamalli), kansallinen ohje tai suositus (esim. VAHTI 2/2016 Toiminnan jatkuvuuden hallinta), lainsäädäntö (esim. tiedonhallintalaki), tai näiden yhdistelmä. Noudatettiinpa mitä tahansa viitekehystä, on organisaation oltava selvillä siitä, miten siihen liittyvät vaatimukset toteutuvat.

Vaatimustenmukaisuuden osoittamiseksi organisaatiossa voidaan toteuttaa erilaisia tarkastuksia ja arviointeja. Itsearvioinnissa hallintamallin vastuuhenkilöt (esim. tietoturva- tai valmiuspäällikkö) arvioi toimintaa käytetyn viitekehyksen avulla. Organisaation sisäisiin arviointeihin kuuluvat myös sisäisen tarkastuksen (esim. controller-toiminto) tekemät arvioinnit. Sisäisten arviointien etuna on, että niissä voidaan mennä

syvälle toiminnan yksityiskohtiin. Sisäiset tarkastukset ja arvioinnit ovat tärkeä osa operatiivista seurantaa, mutta niiden tuloksia ei useinkaan hyväksytä osoittamaan vaatimusten toteutumista kolmansille osapuolille.

Ulkopuolisen tahon tekemän vaatimustenmukaisuuden arvioinnin tavoitteena on tuottaa riippumaton arvio siitä, vastaako hallintamalli sille asetettuja tavoitteita ja viitekehyksen vaatimuksia. Virallisia lausuntoja tietoturvallisuuden hallinnan viitekehysten (esim. KATAKRI) noudattamisesta voivat antaa Kyberturvallisuuskeskus ja sen NCSA-toiminnon hyväksymät tietoturvallisuuden arviointilaitokset. Kansainvälisen ISO-standardin (esim. ISO/IEC 27001, ISO/IEC 22301 tai ISO/IEC 31000) mukaisten hallintamallin mukaisesti toteutetulle hallintamallille voi hakea sertifikaatin, jolla vaatimustenmukaisuus voidaan osoittaa. Sertifiointi on hyödyksi erityisesti silloin, kun organisaation tulee osoittaa vaatimusten täyttäminen sidosryhmille tai sidosryhmissä on kansainvälisiä toimijoita.

Lisätietoja: Kyberturvallisuuskeskus, NCSA-toiminnon hyväksymät tietoturvallisuuden arviointilaitokset, Luottamuksen lähteillä (Kyberturvallisuuskeskus)

3 Toiminnan jatkuvuus

3.1 Toiminnan jatkuvuuden vaatimukset

Toiminnan jatkuvuuden hallintamallin tarkoituksena on varmistaa, että organisaatio pystyy hoitamaan tärkeimmät tehtävänsä normaaliolojen laajavaikutteisissa häiriötilanteissa ja tarvittaessa myös valmiuslain määrittelemissä poikkeusoloissa.

Toiminnan jatkuvuuden varmistamiseksi valmistellaan jo häiriöttömissä oloissa suunnitelmia (häiriönhallinta-, jatkuvuus- ja toipumissuunnitelmat), joissa kuvataan vastuut, tehtävät ja mahdolliset vaihtoehtoiset toimintatavat erilaisten tilanteiden varalle.

Nykyaikainen yhteiskunta toimii hyvin verkostomaisesti, minkä takia toimintaympäristön kartoitus sisäisine ja ulkoisine sidosryhmineen on jatkuvuuden hallinnan perusta. Toimintaympäristön tunnistamista on käsitelty tarkemmin kappaleessa 2.1.

3.2 Jatkuvuusriskien arviointi

Kun toimintaympäristö on tunnistettu, tarkastellaan toiminnan jatkuvuutta uhkaavia tekijöitä. Jatkuvuusriskejä arvioidaan esimerkiksi ihmisten, toimitilojen, tietojärjestelmien ja sidosryhmien näkökulmista, kuten kappaleessa 2.2 on kuvattu.

Riskiarvioon kytketään arvio riskien toteutumisen vaikutuksista. Yhden riskin toteutumisella voi olla vaikutuksia mm. operatiiviseen toimintaan, henkilöstön työkuormaan, organisaation julkisuuskuvaan tai organisaation tuottamien palvelujen saatavuuteen. Vaikutusarvion perusteella valitaan ne riskit, jotka vakavimmin uhkaavat toiminnan jatkuvuutta ja keskitetään hallintatoimet niihin.

Toiminnan jatkuvuuteen vaikuttavia riskejä arvioidaan usein vuosittain. Toimintaympäristön muutosten takia voi olla tarpeen tehdä myös pidemmän aikavälin arviointia. Esimerkiksi yhden vuoden tarkastelujaksolla yksittäisen koneen tai laitteen kuluminen voi nostaa vikaantumisen todennäköisyyttä, mutta kolmen tai viiden vuoden tarkastelussa todennäköisyys voi kasvaa huomattavasti. Myös vaikutukset voivat muuttua, kun tarkastellaan riskiä pidemmällä aikavälillä. Esimerkiksi organisaation

taloudellinen tilanne saattaa muuttua yhden vuoden kuluessa vain vähän, mutta lainojen suunnitelmien mukaan toteutuva takaisinmaksu pienentää riskien toteutumisen taloudellisia vaikutuksia tulevaisuudessa.

Taulukko 3: Esimerkki vaikutusten arvioinnista

Riskiluokka	Riskin kuvaus	Yhteisvaikutus (summa)	Palvelujen saatavuus (1-5)	Talous (1-5)	Julkisuuskuva (1-5)	Työyhteisö (1-5)
Henkilöstö	Suuri joukko ihmisiä ei tule töihin (syynä voivat olla esim. pandemia, työtaistelutoimi, tai onnettomuus, joka estää pääsyn toimitiloihin)	13	2	3	3	5
Toimitilat	Tyrskylän kunnanvaltuuston toimistotiloissa sattuu vesivahinko	9	1	4	1	3
Tietojärjestelmät	Tyrskylän kunnanvaltuuston työasemissa havaitaan haittaohjelma	14	4	3	5	2
Sidosryhmät	IT-palvelutoimittajan konkurssi	15	5	3	3	4

3.3 Toiminnan jatkuvuuden hallintatavoitteet

Jatkuvuuden hallinnan tavoitteiden toteuttamisen työvälineinä ovat hallintavoitteet ja niihin liittyvät hallintakeinot. Kutakin tunnistettua riskiä kohti määritellään yksi tai useampia hallintatavoitteita, jotka kuvaavat yleisesti, miten toiminnan jatkuvuudelle asetetut tavoitteet on tarkoitus saavuttaa. Hallintakeinot ovat puolestaan konkreettisia toimenpiteitä ja tehtäviä, joiden avulla riskejä pyritään pienentämään hyväksyttävälle tasolle.

Toiminnan jatkuvuuden hallinnalla pyritään siihen, että häiriöiden kestoa lyhennetään ja niiden vaikutuksia vähennetään. Häiriöt voivat olla yksittäisiä tapahtumia (esimerkiksi yksittäiset henkilön sairastuminen tai työaseman rikkoutuminen), tai laajavaikutteisia ja pitkäkestoisia (esimerkiksi työtaistelutoimenpiteet, organisaation toiminnan suuret muutokset tai tuotantolaitoksen vaurioituminen). Toiminnan jatkuvuuden kannalta organisaation on tiedettävä, kuinka pitkiä katkoja voidaan kestää ennen kuin sattuu peruuttamattomia vahinkoja (esimerkiksi ihmishenkien menetyksiä tai mittavia taloudellisia vahinkoja).

Yksittäisten häiriöiden ja erityisesti tietotekniikkaan liittyvien häiriöiden varalle laaditaan häiriönhallintaprosessi (käytetään myös nimeä MIM; Major Incident Management). Laajavaikutteisten häiriöiden varalle organisaatio toteuttaa toiminnan jatkuvuuden hallintamallin mukaisesti yhden tai useamman jatkuvuussuunnitelman, joka

sisältää organisaation tavoitteet normaaliaikojen vakavien häiriötilanteiden varalle. Jatkuvuussuunnitelmissa määritellään tyypillisesti henkilöstöä, toimitiloja, toimintoja ja prosesseja sekä sidosryhmiä koskevia vaihtoehtoisia toimintatapoja. Jatkuvuussuunnitelmassa kuvataan myös häiriön hallintaan osallistuvien henkilöiden tehtävät ja vastuut. Jatkuvuussuunnitelmat voidaan laatia esimerkiksi siten, että organisaatiotasoisen suunnitelman lisäksi kullekin (ydin)prosessille tai tärkeimmille palveluille laaditaan erilliset suunnitelmat. Jatkuvuussuunnitelmia täydentävät toipumissuunnitelmat, joissa kuvataan tietojärjestelmien palauttaminen normaaliin tilaan häiriötilanteen jälkeen.

Esimerkki: Toiminnan jatkuvuuden tavoitteena on säännöllisen harjoitustoiminnan kehittäminen. Tällöin hallintatavoitteina voivat olla esimerkiksi vuosikelloon kytketyn ja johdon hyväksymän harjoitusohjelman laatiminen sekä ohjelmassa määriteltyjen harjoitusten toteuttaminen. Hallintatavoitteiden toteuttamisen hallintakeinoina nimetään harjoitusohjelmalle vastuutaho, laaditaan harjoitusohjelma, joka sisältää organisaation toiminnalle keskeisten toimintojen varamenettelyjen testaamisen ja harjoittelun. Jatkuvuussuunnitelmaan kirjattuja harjoittelun periaatteita täydennetään tarvittaessa yksityiskohtaisemmilla linjauksilla ja ohjeilla, jotka liittyvät harjoitusten aikatauluihin, osallistujiin ja sidosryhmiin.

Taulukko 4: Esimerkkejä jatkuvuusriskien hallintatavoitteista

Riski	Hallintatavoite
Suuri joukko ihmisiä ei tule töihin	Kriittisten toimintojen henkilöstölle on nimetty varahenkilöt ja näiden osaaminen on varmistettu
Tyrskylän kunnanvaltuuston toimistotiloissa sattuu vesivahinko	Kriittiset toimitilat on tunnistettu ja tarvittavien väistötilojen käyttö on valmisteltu
Tyrskylän kunnanvaltuuston työasemissa havaitaan haittaohjelma	Valtuuston toiminnan kannalta tärkeimmät tietojärjestelmät on tunnistettu ja niille on laadittu toipumissuunnitelmat
IT-palvelutoimittajan konkurssi	Palvelutoimittajilta vaaditaan kattavat palvelukuvaukset ja ajantasainen dokumentaatio

3.4 Toiminnan jatkuvuuden seuranta, mittaaminen ja arviointi

Koska vakavia ja laajavaikutteisia häiriötilanteita sattuu harvoin, on harjoittelu ainoa keino varmistaa organisaation toimintakyky tositilanteessa. Harjoitusten avulla voidaan varmistaa organisaation kyky toimia häiriötilanteessa (työpöytäharjoitukset ja toiminnalliset harjoitukset), varmistaa varautumissuunnitelmien ja riskiarvioiden kattavuus (juurisyyanalyysit) ja harjoitella useiden organisaatioiden samanaikaista toiminta laajavaikutteisessa häiriötilanteessa tai poikkeusoloissa (yhteistoimintaharjoitukset). Sekä Digi- ja väestötietovirasto että Kyberturvallisuuskeskus ovat julkaisseet käytännöllisiä ohjeita harjoitusten ja harjoitusohjelmien toteuttamisen tueksi.

Taulukko 5: Esimerkkejä toiminnan jatkuvuuden hallintatavoitteiden hallintakeinoista

Riski	Hallintatavoite	Hallintakeino
Suuri joukko ihmisiä ei tule töihin	Kriittisten toimintojen henkilöstölle on nimetty varahenkilöt ja näiden osaaminen on varmistettu	Kriittiset toiminnot on tunnistettu ja kirjattu
		Avainhenkilöt osaamisvaatimukset on tunnistettu
		Avainhenkilöt ja varahenkilöt osallistuvat jatkuvuusharjoituksiin
Tyrskylän kunnanvaltuuston toimistotiloissa sattuu vesivahinko	Kriittiset toimitilat on tunnistettu ja tarvittavien väistötilojen käyttö on valmisteltu	Varatilojen tarve päivitetään säännöllisesti
		Varatilojen varustelu tarkastetaan säännöllisesti
		Varatilojen käyttöönottoa harjoitellaan vuosittain
Tyrskylän kunnanvaltuuston työasemissa havaitaan haittaohjelma	Valtuuston toiminnan kannalta tärkeimmät tietojärjestelmät on tunnistettu ja niille on laadittu toipumissuunnitelmat	Tärkeimmät tietojärjestelmät on tunnistettu ja kirjattu
		Tietojärjestelmille on asetettu palautumistavoitteet
		Toipumissuunnitelmia testataan vuosittain
IT-palvelutoimittajan konkurssi	Palvelutoimittajilta vaaditaan kattavat palvelukuvaukset ja ajantasainen dokumentaatio	Palvelusopimuksiin on kirjattu toiminnan jatkuvuuden vaatimuksista johdetut sopimusvelvoitteet
		Palvelutoimittajien ylläpitämää dokumentaatiota arvioidaan jatkuvasti
		Palvelutoimittajat osallistuvat jatkuvuusharjoituksiin

Lisätietoja: ISO/IEC 22301, VAHTI 2/2016, VAHTI 2/2012, Digitaalisen turvallisuuden harjoitusohjelman suunnittelu, Kyberharjoitusohje

4 Tietoturvallisuus

Tietoturvallisuudella tarkoitetaan tässä tietojen saatavuudesta, eheydestä ja luottamuksellisuudesta huolehtimista. Tietoturvallisuudesta huolehditaan menettelytapojen sekä operatiivisten tietojärjestelmien, erilaisten tukijärjestelmien ja tietoteknisten työkalujen muodostaman kokonaisuuden (hallintamallin) avulla. Tietoturvallisuus kattaa sekä hallinnollisia että teknisiä toimenpiteitä. Hallinnollista tietoturvaa toteutetaan

mm. tietoturvapolitiikan, ohjeistusten ja tarkastusten avulla. Teknisen tietoturvan työkaluja ovat mm. haittaohjelmasuojaukset, pääsynhallinta ja tiedon salaus. Ilman tietoturvallisuuden hallintamallia organisaation tieturvallisuuden toteutus on liian sattumanvaraista ollakseen tehokasta.

4.1 Tietoturvavaatimukset

Tietoturvallisuuden hallintamallin tarkoituksena on varmistaa organisaation tietojen saatavuus, eheys ja luottamuksellisuus. Toimivan hallintamallin toteuttamiseksi organisaation on tunnistettava toimintaansa kohdistuvat tietoturvavaatimukset. Lainsäädäntö on keskeinen tietoturvavaatimusten lähde. Tiedonhallintalain 4. luku asettaa julkisen hallinnon organisaatioille vaatimuksia mm. tietoaineistojen turvallisuudelle, käyttöoikeuksien hallinnalle ja lokitietojen keräämiselle. Myös organisaation toiminnasta ja toimintaympäristöstä johdetaan tietoturvavaatimuksia, joihin voivat vaikuttaa esimerkiksi jaettujen palveluiden käyttövelvoite, organisaation tehtävä tai tietoturvallisuuden kansainväliset kehitysnäkymät.

Koska erilaiset palveluntuottajat ovat tärkeä osa lähes jokaisen organisaation toiminnassa, tulee organisaation tietoturvavaatimukset sisällyttää mm. hankinta- ja palvelusopimuksiin. Sopimukseen voidaan kirjata tietoturvallisuutta koskevia kohtia tai sopimukseen voidaan laatia erillinen tietoturvallisuusliite. Tietoturvavaatimukset on hyvä kuvata mahdollisimman täsmällisesti sen sijaan, että sopimusvelvoitteisiin kirjattaisiin kategorinen vaatimus tietyn standardin tai viitekehyksen noudattamisesta.

Organisaation tietoturvavaatimukset kirjataan tietoturvapolitiikkaan. Se sisältää ylätason linjauksia organisaation tietoturvallisuuden johtamisesta, organisoinnista ja vastuista sekä menettelytavoista. Esimerkkejä tietoturvapolitiikan rakenteesta löytyy verkosta, esimerkiksi VAHTI 3/2007 Liite 4, Seinäjoen tietoturvapolitiikka 2018, Kouvolan Veden tietoturvapolitiikka 2018, Karvian tietoturva- ja tietosuojapolitiikka 2019

4.2 Tietoturvariskien arviointi

Organisaation tietoturvariskien arviointi on edellytyksenä sille, että käytettävissä olevat resurssit (henkilötyö, raha) voidaan kohdentaa tehokkaasti. Tietoturvariskien arviointi noudattaa kappaleessa 2.2 kuvattua yleistä mallia.

Tietoturvariskien arvioimiseksi on tunnistettava tietoturvan osa-alueihin kohdistuvat uhkat (ks. alla). Uhkia tunnistetaan eri lähteistä, joita voivat olla esimerkiksi henkilöstö, tilat, tietojärjestelmät ja sidosryhmät. Tunnistetuista uhkista muodostetaan riskejä liittämällä niihin todennäköisyydestä ja vaikutuksesta muodostettu riskiluku.

- Mitkä seikat voivat johtaa siihen, että tieto ei ole saatavilla? (esim. tiedon tarpeeton turvaluokittelu, tietoliikenne- tai muut ICT-ongelmat, vanhentunut ohjelmistolisenssi tai varmenne, kassakaapin avainkoodin puuttuminen)
- Mikä voi johtaa tiedon eheyden vaarantumiseen? (esim. käyttäjän virhe, ulkopuolinen hakkerointi, puutteellinen ohjeistus, laitevika, ohjelmistovirhe)
- Mikä vaarantaa tiedon luottamuksellisuuden? (esim. virheellinen tiedon luokittelu, huolimattomuus, tietomurto, tiedon kalastelu, tahallinen tiedon vuotaminen)

Taulukko 6: Esimerkkejä tietoturvariskeistä

Riskiluokka	Tietoturvariski	Todennäköisyys (1-5)	Vaikutus (1-5)	Riskiluku (tulo)
Tiedon luokittelu	Arkaluontoista henkilötietoa vuotaa sivullisille	2	4	8
Johtaminen	Tietoturvallisuuden tasoa ei tunneta	2	3	6
Työasemat	Työasemiin pääsee haittaohjelma	3	4	12
Tietovarannot	Tärkeää tietoa menetetään	2	5	10

Lisätietoja: OWASP Top Ten

4.3 Tietoturvan hallintatavoitteet

Tietoturvatavoitteiden toteuttamisen työvälineinä ovat hallintavoitteet ja niihin liittyvät hallintakeinot. Hallintatavoitteet kuvaavat yleisesti, miten asetetut tietoturvatavoitteet on tarkoitus saavuttaa. Hallintakeinot ovat puolestaan konkreettisia toimenpiteitä ja tehtäviä, joiden avulla riskejä pyritään pienentämään hyväksyttävälle tasolle.

Tietoturvallisen toimintaympäristön toteutus edellyttää niin teknisiä kuin hallinnollisiakin toimenpiteitä. Hallinnollisia toimenpiteitä ovat esim. ylimmän johdon hyväksymä tietoturvapolitiikka, jossa linjataan yleiset tietoturvallisuuden tavoitteet sekä hankintoihin liitettävät tietoturvallisuuden mallilausekkeet. Teknisiä tietoturvatoimenpiteitä puolestaan ovat mm. haittaohjelmasuojaus ja tietoliikenteen salauskäytännöt.

Esimerkki: Tietoturvatavoitteena on johdon sitoutuminen tietoturvallisuuden kehittämiseen. Tällöin hallintatavoitteena voi olla, että johdon on määriteltävä ja hyväksyttävä linjaukset organisaation tietoturvallisuuden kehittämiselle. Hallintatavoitteen toteuttamisen hallintakeinona laaditaan ja hyväksytään tietoturvapolitiikka, jossa määritellään tarvittavat tietoturvallisuuden prosessit, vastuut ja muu tarvittava ohjaus. Tietoturvapolitiikkaa täydennetään tarvittaessa yksityiskohtaisemmilla linjauksilla ja ohjeilla, jotka voivat koskea esimerkiksi tietoturvallisuuden teknistä toteuttamista, hyväksyttävän käytön periaatteita tai tietojen luokittelua.

Taulukko 7: Esimerkkejä tietoturvariskien hallintatavoitteista

Riski	Hallintatavoite
Henkilötiedon paljastuminen teknisten puutteiden takia	Teknisten haavoittuvuuksien hyödyntäminen estetään
Tietoturvallisuuden tasoa ei tunneta	Tärkeimmät toiminnot on tunnistettu ja kuvattu. Toimintoihin liittyvät tietoturvatavoitteet on määritelty ja vastuutettu.

Riski	Hallintatavoite
Työasemiin pääsee haittaohjelma	Varmistetaan työasemaympäristön turvallisuus
Tärkeää tietoa menetetään	Tietovarantojen saatavuus varmistetaan

Lisätietoja: ISO/IEC 27000 -standardiperhe (erityisesti ISO/IEC 27001, ISO/IEC 27002, COBIT

4.4 Tietoturvallisuuden seuranta, mittaaminen ja arviointi

Organisaation pitää olla selvillä tietoturvallisuutensa tasosta. Tietoturvallisuuden mittareina voidaan käyttää sekä hallintakeinojen suorituskykyyn että vaikuttavuuteen perustuvia mittareita, jotka voivat olla numeerisia tai laadullisia. Seurannan perustana ovat havaitut poikkeamat, joiden pohjalta laaditaan ehdotuksia tietoturvallisuuden hallintamallin kehittämiseksi. Mittaaminen perustuu tietoturvatavoitteisiin, joille asetetut mittarit voivat olla esimerkiksi numeerisia raja-arvoja (esim. palveluiden saatavuus vähintään 99 %) tai vaatimustenmukaisuuden todentamista (esim. vuosikellon mukaiset arvioinnit ja katselmoinnit on hoidettu suunnitellusti).

Tietoturvallisuuden arvioinnissa ja seurannassa hyödynnetään hallintakeinojen toteutumisesta kertyvää mittaustietoa (esimerkiksi haavoittuvuusskannauksissa havaitut puutteet, sisäisten auditointien toteutus tai tietoturvapolitiikan ajantasaisuus).

Taulukko 8: Esimerkkejä tietoturvallisuuden hallintatavoitteiden hallintakeinoista

Riski	Hallintatavoite	Hallintakeino
Henkilötiedon paljastuminen teknisten puutteiden takia	Teknisten haavoittuvuuksien hyödyntäminen estetään	Teknisten haavoittuvuuksien seurantaan on määritelty prosessi ja vastuuhenkilöt
		Kriittisten korjausten asentamiselle on määritelty prosessi
		Sovelluksille tehdään säännöllisiä haavoittuvuustestauksia
Tietoturvallisuuden tasoa ei tunneta	Tärkeimmät toiminnot on tunnistettu ja kuvattu. Toimintoihin liittyvät tietoturvatavoitteet on määritelty ja vastuutettu.	Johto on käsitellyt ja hyväksynyt kirjallisen yleisen tietoturvapolitiikan, jonka sisältö on koko henkilöstön tiedossa.
		Kriittiset ydintoiminnot ja -prosessit on tunnistettu. Toiminnoille on määritelty tavoitteet ja vastuuhenkilöt (prosessin omistajat).
		Tietoturvavastaava on nimetty ja hänellä on riittävät resurssit tehtävän hoitamiseksi.

Riski	Hallintatavoite	Hallintakeino
Työasemiin pääsee haittaohjelma	Varmistetaan työasemaympäristön turvallisuus	Hyväksyttävän käytön periaatteet on kuvattu.
		Kaikissa työasemissa on ajantasainen haittaohjelmasuojaus.
		Työasemien ohjelmistot on vakioitu.
		Ylläpito-oikeuksien myöntämisen prosessi on määritelty.
		Koko henkilöstölle järjestetään vähintään kahdesti vuodessa tietoturvallisuuden tietoiskuja ajankohtaisista aiheista.
Tärkeää tietoa menetetään	Tietovarantojen saatavuus varmistetaan	Varmistuspolitiikka on laadittu ja se on ajan tasalla. Politiikassa on huomioitu ISO27002:2017 kohdan 12.3.1 vaatimukset.
		Poikkeamat normaaleista varmistusrutiineista tunnistetaan ja kirjataan.
		Kriittisten järjestelmien palautustestit tehdään vuosittain.

Lisätietoja: ISO/IEC 27000 -standardiperhe (erityisesti ISO/IEC 27001, ISO/IEC 27003, ISO/IEC 27004), VAHTI 2/2010, VAHTI 2/2012

5 Tietosuoja

Tietosuoja on yksilön yksityisyyden ja luottamuksen turvaamista. Tietosuojaan kuuluvat muun muassa henkilötietojen oikeaoppinen käsittely ja henkilötietojen suojaaminen luvattomalta käytöltä ja käsittelyltä. Tietosuojan tarkoituksena on turvata rekisteröidyn yksityisyys, edut, oikeudet, vapaudet ja oikeusturva hänen henkilötietojaan käsiteltäessä. Tietosuoja on yksi Euroopan unionin keskeisiä perusoikeuksista, joka on vahvistettu myös Euroopan ihmisoikeussopimuksessa.

5.1 Tietosuojavaatimukset

Euroopan ihmisoikeussopimus on perusta Euroopan perusoikeusasiakirjalle (2012/C326/02). Perusoikeusasiakirjan 7 artiklan mukaan jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan ja viestejään kunnioitetaan. Lisäksi 8 artiklan mukaan jokaisella on oikeus henkilötietojensa suojaan, tietojenkäsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty ja saada

puutteelliset tiedot oikaistuksi. Riippumaton viranomainen, Suomessa tietosuojavaltuutettu, valvoo näiden sääntöjen noudattamista.

Suomessa perustuslain (731/1999) 10 §:ssä säädetään yksityiselämän suojasta. Sen mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla. Toukokuussa 2018 alettiin soveltaa EU:n yleistä tietosuoja-asetusta, yleisemmin tietosuoja-asetus tai GDPR (EU 2016/679). Se on suoraan sovellettavaa lainsäädäntöä koko EU:n alueella. Tämän lisäksi säädettiin EU-tasolla rikosasioiden tietosuojadirektiivi.

Suomessa tietosuojalainsäädäntö koostuu GDPR:n ohella kansallisesta tietosuojalaista (1050/2018), laista henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018) sekä muusta erityislainsäädännöstä. Tietosuojasääntelyä ohjataan EU:n tasolla, Suomen pitää muiden EU:n maiden ohella noudattaa Eurooppa tasoista tietosuojasääntelyä sekä muita Euroopan tietosuojaneuvoston antamia ohjeistuksia, suosituksia ja päätöksiä. Euroopan tietosuojaneuvosto vastaa tietosuojalainsäädännön yhdenmukaisesta soveltamisesta Euroopan unionissa sekä edistää yhteistyötä kansallisten tietosuojaviranomaisten välillä.

5.2 Hyvällä tietosuojalla rakennetaan luottamusta

Jokaisella on oikeus henkilötietojensa suojaan. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä. Rekisteröidyn tulee tietää miten ja mihin tarkoitukseen hänen henkilötietojaan kerätään ja käytetään. Hänen tulee voida luottaa henkilötietojen oikeaoppiseen ja asialliseen käyttöön. Luottamuksen rakentaminen ja ylläpitäminen ovat ensiarvoisen tärkeitä niin julkisen hallinnon asiakkaille kuin myös yksityisellä sektorilla. Ilman luottamusta asiakkaat eivät ehkä uskalla antaa henkilötietojaan käytettäväksi ja asiakkaiden palvelu heikentyy.

5.3 Tietosuojariskien arviointi

Henkilötietojen käsittelyyn liittyvien riskien arviointi on tehtävä lähtökohtaisesti rekisteröidyn näkökulmasta. Rekisterinpitäjän on arvioitava mitä rekisteröidyn vapauksia ja oikeuksia henkilötietojen käsittely voi vaarantaa ja mitä vahinkoa rekisteröidylle voi aiheutua suunnitellusta henkilötietojen käsittelystä. Nämä vahingot voivat olla fyysisiä, aineellisia tai aineettomia, kuten esimerkiksi potilasturvallisuuden vaarantuminen, petoksen kohteeksi joutuminen, maineen menetys tai taloudellinen menetys.

Rekisterinpitäjän on tehtävä henkilötietojen käsittelystä riskiarvio ja päätettävä tiedon suojaamiseen käytettävistä toimenpiteistä ja arvioitava niiden riittävyys. Riskianalyysi on välttämätön apuväline rajallisten resurssien tehokkaaseen kohdistamiseen. Arviossa on huomioitava henkilötietojen käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset. Alla on esimerkin mukaisesti kuvattu mitä asioita riskiarvioinnissa on huomioitava.

1. henkilötietojen käsittelyn luonne

a) käsitelläänkö erityisiin henkilötietoryhmiin liittyviä tietoja
b) rekisteröidyn mahdollisuus käyttää oikeuksiaan; läpinäkyvyyden puute ja tietosuojaperiaatteiden toteutumisen epävarmuus

c) käytetäänkö uutta teknologiaa ja innovaatioita
d) tietojenkäsittelyn ulkoistuksen luonne
e) onko rekisteröidyllä heikko asema, ymmärtääkö hän oikeuksiaan
f) henkilöstön osaaminen ja resurssien kohdentaminen

2. henkilötietojen käsittelyn laajuus

a) rekisteröityjen ja käyttäjien lukumäärä (paljon/vähän)
b) tiedon määrä ja tiedon kasautuminen
c) säilytysaika (lyhyt/määräaikainen/pysyvä)
d) maantieteellinen soveltamisala (paikallinen/alueellinen/kansallinen/kansainvälinen/globaali)

3. henkilötietojen käsittelyn tarkoitukset

a) rekisteröityjen tarkkailu, seuranta ja valvonta
b) henkilöiden arviointi tai pisteytys
c) automaattinen päätöksenteko, jolla on oikeusvaikutuksia rekisteröityyn

4. henkilötietojen käsittelyn asiayhteys

a) luottamuksellisuus (erityiset tai muuten erityisen henkilökohtaiset henkilötiedot)
b) yksityisyyden turvaaminen (kotirauha)
c) eri yhteyksistä kerättyjen henkilötietojen yhdistäminen

Lähde: Tietosuoja.fi

Riskien tunnistamisen jälkeen on arvioitava riskin ja siitä aiheutuvan haitan vakavuutta ja toteutumisen todennäköisyyttä. Mitä todennäköisempi loukkauksen tai haitan todennäköisyys rekisteröidylle on, sitä korkeammaksi riskit kasvavat.

		Loukkauksen tai haitan todennäköisyys		
Loukkauksen tai haitan vakavuus		**Kaukainen**	**Mahdollinen**	**Hyvin mahdollinen**
	Vakava	Keskimääräinen riski	Korkea riski	Korkea riski
	Tunnistettuja vaikutuksia	Matala riski	Keskimääräinen riski	Korkea riski
	Vähäisiä vaikutuksia	Matala riski	Matala riski	Keskimääräinen riski

Taulukko 9: Tietosuojariskien arviointi (tietosuoja.fi)

Riskien arviointia on tehtävä jatkuvasti ja varsinkin silloin, kun lainsäädäntö muuttuu tai toimintaa muutetaan, kuten otetaan käyttöön uutta teknologiaa. Rekisterinpitäjän tulee osoittaa, että se arvioi ja minimoi rekisteröidylle mahdollisesti aiheutuvia riskejä. Päätösten perusteet ja dokumentointi on osa osoitusvelvollisuuden toteuttamista.

Riskien arviointia on myös tietosuojaa koskeva vaikutustenarviointi. Vaikutustenarvioinnissa tunnistetaan, arvioidaan ja hallitaan henkilötietojen käsittelyyn liittyviä

riskejä. Vaikutustenarviointi on pakollinen vain silloin, kun suunniteltu käsittely voi aiheuttaa korkean riskin ihmisten oikeuksille ja vapauksille. Rekisterinpitäjä voi kuitenkin hyödyntää vaikutustenarviointia, milloin tahansa, kun se suunnittelee toimintoja, joissa on tarkoitus käsitellä henkilötietoja. Organisaation omaa tietosuojavastaavaa on kuultava, kun vaikutustenarviointia tehdään.

Joskus voi esiintyä tilanteita, joissa vaikutusarvioinnin mukaan riskit rekisteröidylle ovat korkeat eikä rekisterinpitäjä voi minimoida riskejä alhaisemmaksi. Tällöin rekisterinpitäjä on kuultava tietosuojaviranomaista. Tästä menettelystä käytetään nimitystä ennakkokuuleminen.

Helsingin kaupungin sivuilta löytyy lisätietoja vaikutusarvioinnista, hyviä käytäntöjä sen tekemiseen ja muun muassa vaikutustenarvioinnin työkalu sekä vaikutustenarvioinnin riskianalyysilomake: https://www.hel.fi/helsinki/fi/kaupunki-ja-hallinto/tietoa-helsingista/tietosuoja/tietosuojan-vaikutustenarviointi

Myös tietosuojavaltuutetun toimiston sivuilta löytyy ohjeistusta vaikutustenarviointiin sekä ennakkokuulemisen tekemiseen.

5.4 Tietosuojan hallintatavoitteet

Henkilötietojen käsittelyä koskevat tietyt GDPR:n 5 artiklan periaatteet, joita rekisterinpitäjän on noudatettava. Nämä periaatteet ovat:

a) lainmukaisuuden, kohtuullisuuden ja läpinäkyvyyden periaate
b) käyttötarkoitussidonnaisuuden periaate
c) tietojen minimoinnin periaate
d) täsmällisyyden periaate
e) säilytyksen rajoittamisen periaate
f) eheyden ja luottamuksellisuuden periaate

Rekisterinpitäjä vastaa tietosuojaperiaatteiden noudattamisesta ja sen on myös osoitettava, että näin tapahtuu (osoitusvelvollisuus). Käytännössä osoitusvelvollisuus voidaan toteuttaa erilaisilla dokumenteilla, joita ovat muun muassa:

a) seloste käsittelytoimista eli henkilötietojen käsittelyn yleinen kuvaus
b) tietosuojaperiaatteiden sisäänrakennettu toteutuminen
c) tietosuojapolitiikat, toimintaperiaatteet ja ohjeistukset
d) informointikäytännöt
e) käsittelyn oikeusperustetta koskevat arviot
f) riskiarvioinnit, vaikutustenarviointia ja ennakkokuulemista koskeva dokumentaatio
g) henkilötietojen tietoturvaloukkausten dokumentointi ja siihen liittyvä prosessi
h) tietosuojan hallintamalli
i) henkilötietojen käsittelyyn liittyvät sopimukset
j) yhteisrekisterinpitäjien vastuualueiden määritteleminen
k) mahdollinen johtavan valvontaviranomaisen määrittämistä koskeva dokumentaatio
l) henkilötietojen siirtoa kolmansiin maihin koskeva dokumentaatio
m) koulutussuunnitelmat ja -toteumat
n) varmennukset, auditoinnit ja sertifioinnit

Rekisterinpitäjän tietosuojavelvollisuudet koskevat kaikkia organisaation käsittelemiä henkilötietoja. Näitä ovat muun muassa asiakkaiden, potilaiden, yhteistyökumppaneiden ja henkilöstön tiedot. Rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että henkilötietojen käsittelyssä noudatetaan asetusta. Näitä toimenpiteitä on arvioitava ja päivitettävä tarvittaessa. Toimenpiteitä ovat muun muassa teknisen tietoturvan lisäksi henkilöstön osaamisesta huolehtiminen ja tietosuojaan liittyvien prosessien kuvaaminen ja käytäntöön vieminen. Osoitusvelvollisuus koostuu suunnittelusta, tekemisestä ja sen todistamisesta mitä ja miksi tehdään. Henkilötietojen käsittelylle tulee aina löytyä peruste, julkishallinnossa se on usein lakisääteinen.

5.4.1 Tietosuojan hallintamalli

Tietosuojan hallintamalli on kuvaus siitä, miten tietosuojan ohjaus ja hallinta organisoidaan, mitä rooleja ja vastuita siihen kuuluu ja millä prosesseilla sitä suunnitellaan, kehitetään ja miten sitä käytännön tasolla hallitaan. Tietosuojan hallintamallin avulla varmistetaan tietosuojan suunnitelman mukainen hallinnointi ja toteutus.

Jotta tietosuojasta voidaan huolehtia koko organisaation laajuisesti ottaen huomioon kaikki käsiteltävät tiedot, tulee tietosuojan hallinnointi vastuuttaa ja varata siihen riittävästi resursseja. Tietosuojavastaava on yksi keskeinen resurssi ja organisaation on huolehdittava, että hänellä on todellinen mahdollisuus tehdä työtänsä.

Tietosuojan hallinnointiin kuuluu huolehtia muun muassa alla olevista asioista:

a) johdon tuen varmistaminen
b) vastuiden ja raportointiketjujen määrittely
c) tietosuojavastaavan ja tietosuojaorganisaation nimittäminen
d) politiikkojen ja ohjeistusten tekeminen sekä niiden jalkautus
e) riskienhallinnan järjestäminen
f) sopimusten ja alihankkijoiden hallinta
g) henkilöstön osaamisesta huolehtiminen
h) valvonnan ja seurannan määrittely
i) vuosikello säännöllisen kehittämisen apuvälineeksi
j) jatkuva tietosuojan kehittäminen
k) auditointien ja arviointien käyttäminen kehittämisen apuvälineenä.

Hallintamalli sisältää kolme tasoa:

1. politiikka,
2. standardit/periaatteet ja
3. toimintaohjeet.

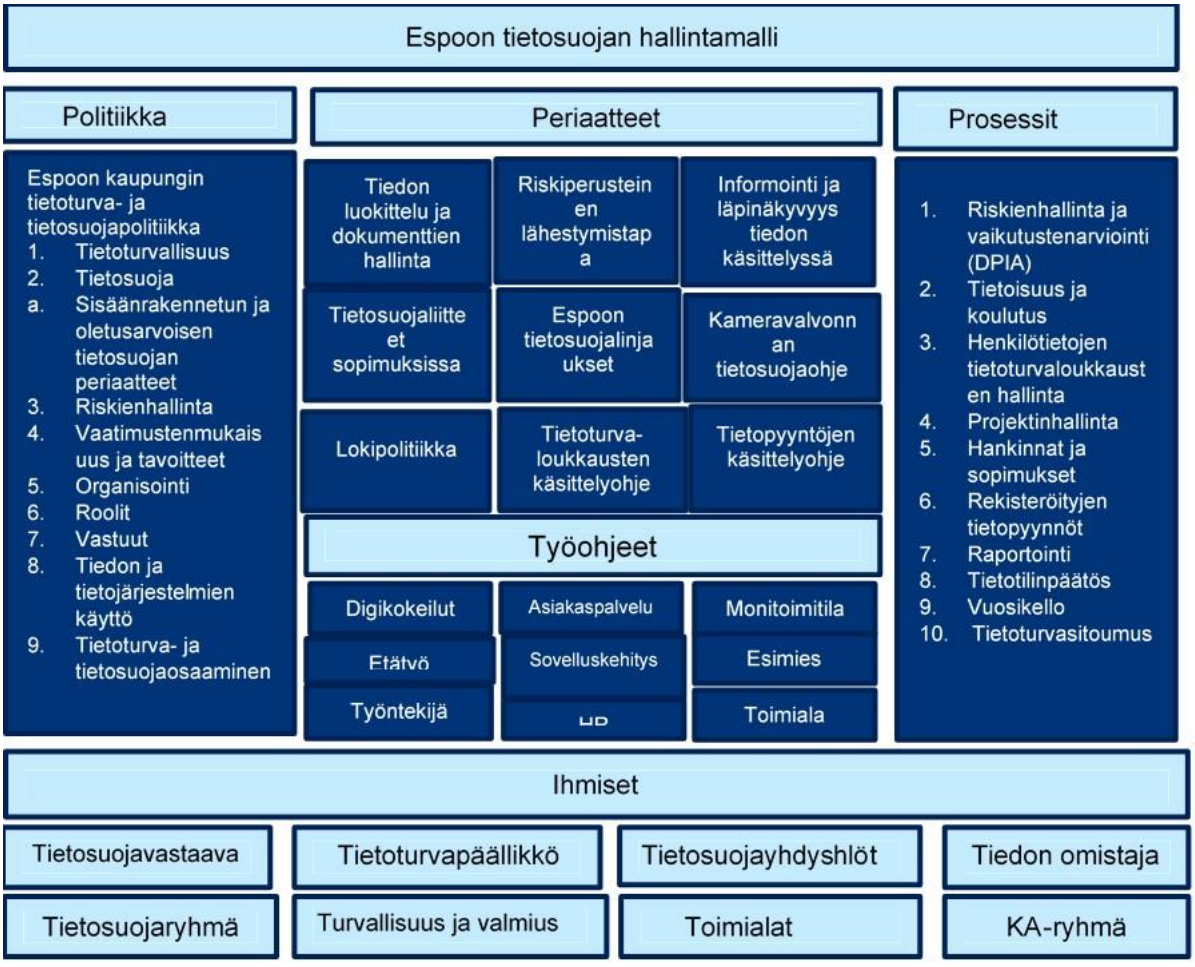
Politiikka muodostaa johdon kannanoton tietoturvallisuudelle ja tietosuojan puitteille, linjauksille ja vastuille. Johto osoittaa täten tukensa, tahtotilansa ja sitoumuksensa tietosuojan kehittämiseen julkaisemalla ja ylläpitämällä tietosuojapolitiikkaa. Politiikan tulee olla johdon hyväksymä ja allekirjoittama. Politiikka on lyhyt ja selkeä ja sen tulee olla myös henkilöstön tiedossa. Politiikka sisältää seuraavia asioita:

a) tietosuojan määritelmä, sen kokonaistavoitteet ja kattama alue

b) tietosuojan merkitys organisaation toiminnan kannalta ja oikeanlaisen toiminnan mahdollistajana
c) organisaation johdon tahtotila ja tavoitteet
d) tietosuojan kontrollitavoitteiden ja kontrollien viitekehys / toteutustapa
e) tietosuojapolitiikan, periaatteiden, standardien ja vaatimusten määritelmä
f) lainsäädännöllisten ja muiden säännösten asettamat vaatimukset
g) osaamisen ja tietoisuuden lisäämisen periaatteet
h) tietosuojaan liittyvät vastuut ja velvollisuudet sekä raportointikanavat
i) viittaukset täydentäviin dokumentteihin ja muihin tietolähteisiin

Periaatedokumentit muodostavat kuvauksen käytännön toteutuksesta ja periaatteista. Periaatteet ovat organisaation omia määrämuotoisia toimintatapoja ja politiikkaa tarkempia periaatteita.

Toimintaohjeet muodostavat yksityiskohtaisen ohjeistuksen tietoturva- ja tietosuoja-asioiden käsittelyyn ja käytännön toimintaan. Toimintaohjeet kuvaavat kuinka politiikkojen ja periaatteiden kuvaamat asiat tai tehtävät tulee käytännössä suorittaa. Toimintaohjeet liittyvät myös läheisesti prosessikuvauksiin ja ilmentävät sisäänrakennetun ja oletusarvioisen tietosuojan periaatteiden toteutumista. Alla olevassa kuvassa on esimerkkinä Espoon kaupungin tietosuojan hallintamalli.



Kuva 2. Espoon kaupungin tietosuojan hallintamalli.

5.5 Tietosuojan seuranta, mittaaminen ja arviointi

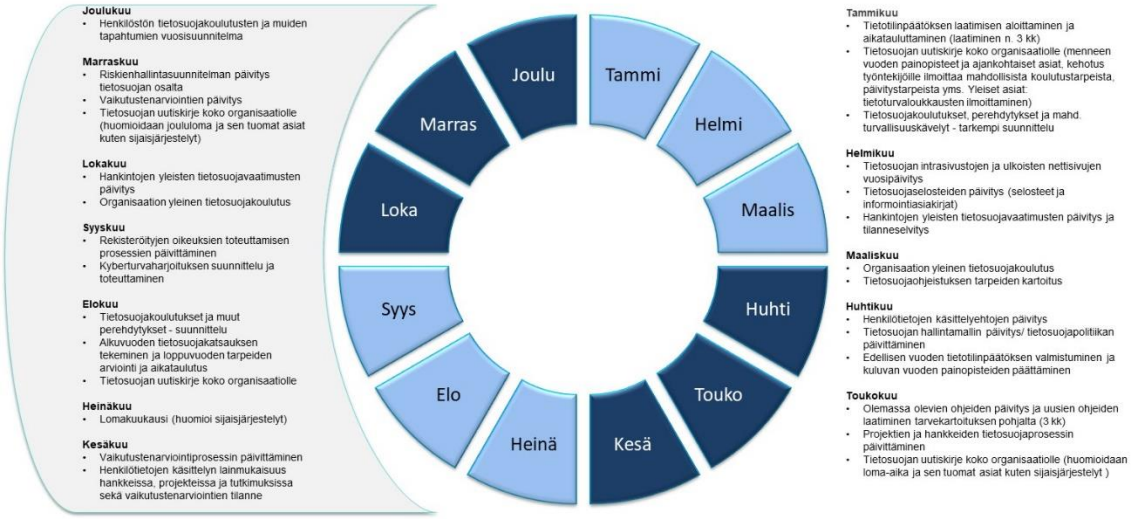
Rekisterinpitäjän on noudatettava tietosuoja-asetuksen säännöksiä ja pystyttävä osoittamaan se erilaisilla dokumenteilla ja toimintatavoilla. Rekisterinpitäjän on osoitettava, että se käsittelee henkilötietoja lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi. Organisaation koko, henkilötietojen määrä ja luonne vaikuttavat osoitusvelvollisuuden laajuuteen.

Rekisterinpitäjän on arvioitava miten vaatimukset toteutuvat, apukeinoina ovat erilaiset käytännesäännöt, sertifikaatit, tietoturvan ja tietosuojan omavalvontasuunnitelma ja säännöllinen raportointi. Organisaation tietosuojavastaavalla on myös tärkeä tehtävä tietojen annon ja neuvonnan lisäksi seurata, että organisaatiossa noudatetaan tietosuojasääntelyä.

5.5.1 Tietosuojan vuosikello

Eräs tapa parantaa tietosuojatyön suunnitelmallisuutta ja toteutumisen seurantaa on laatia tietosuojan vuosikello. Siihen kuvataan eri kuukausille tietosuojaan liittyviä tehtäviä. Vuosikello edellyttää myös selkeää vastuunjakoa aikataulutuksen lisäksi. Eli on sovittava siitä, kuka tietyn asian hoitaa. Vuosikellon avulla voidaan osoittaa johdolle ja henkilöstölle minkälaisista asioista tietosuoja koostuu. Sillä voidaan myös osoittaa, miten tietosuoja on sisäänrakennettu organisaation toiminnoissa.

Oheinen tietosuojan vuosikellomalli löytyy muokattavissa olemassa muodossa https://dvv.fi/vahti kohdasta VAHTI hyvät käytännöt tukimateriaali.



Kuva 3. Tietosuojan vuosikello.

5.5.2 Tietotilinpäätös

Tietotilinpäätös on yksi sisäisen ja ulkoisen valvonnan keinoista täyttää osoitusvelvollisuus ja arvioida omaa toimintaa. Tietotilinpäätös antaa tilannekuvan organisaation nykytilasta sekä arvioi tietosuojan toteutumista. Siinä voidaan kuvata

kehittämistarpeita ja niihin liittyviä toimenpiteitä. Tietotilinpäätös antaa johdolle ja sidosryhmille kuvan henkilötietojen käsittelyn tilasta. Se osaltaan edesauttaa tiedolla johtamista. Tietotilinpäätöksen avulla voidaan lisätä luottamusta organisaation kykyyn käsitellä henkilötietoja oikeaoppisesti.

Oikeiden tunnuslukujen ja mittareiden valintaan kannattaa kiinnittää huomioita. Hyvin valituilla mittareilla saadaan tietoa tietojenkäsittelyn tilasta ja tietosuojasääntelyn noudattamisesta. Hyviä mittareita ovat esimerkiksi henkilöstön suorittamat tietoturva- ja tietosuojakoulutuksen määrä (montako % henkilöstöstä suorittanut), tarkastuspyyntöjen lukumäärä ja vastaamiseen kulutettu aika, henkilötietojen tietoturvaloukkausten määrä ja tehdyt vaikutustenarvioinnit.

Kuntaliitto on yhdessä kuntien kanssa laatinut tietotilinpäätösmallin. Malli pohjautuu Kati Suojasen ja Minna Järvisen tekemään opinnäytetyöhön. Mallin pohjalta on myös tehty kuvitteellinen Tyrskylän kunnan tietotilinpäätös. Mallit sisältävät myös laajasti erilaisia mittareita, joita voi hyödyntää. Molemmat mallit ovat tämän dokumentin liitteinä. Myös netistä löytyy lukuisia tietotilinpäätöksiä, joita kannattaa hyödyntää oman organisaation tietotilinpäätöstä suunniteltaessa.

Tietotilinpäätöksen sisällysluettelo voi olla seuraavanlainen:

Julkinen tiivistelmä
Johdon tiivistelmä
1. Johdanto
2. Tietosuojan ja tietoturvallisuuden toteuttaminen
3. Tiedonhallinta, tietovarannot ja tietovirrat
4. Lainsäädäntö ja muu ohjeistus
5. Rekisteröidyn oikeuksien toteutuminen
6. Arviointi, kehittäminen ja tiedon hyödyntäminen
7. Seuranta ja mittarit.

5.5.3 Muita arviointityökaluja

Tutustu muihin tietosuojan kehittämistä ja ylläpitoa edistäviin työkaluihin ja materiaaleihin https://dvv.fi/vahti sivustolla kohdasta VAHTI hyvät käytännöt tukimateriaalit.

6 Kyberturvallisuus

Tämän oppaan alussa todetaan, että tieto- ja kyberturvallisuus kuuluvat digitaalisen turvallisuuden viitekehykseen. Näitä termejä käytetään joskus toistensa synonyymeinä, vaikka niiden määritelmät ovatkin erilaiset. Organisaation digitaalisen turvallisuuden kannalta ei ole olennaista, tuleeko jokin asia käsitellyksi tietoturva- vai kyberturva-asiana. Tärkeintä on, että kaikki digitaaliseen turvallisuuteen liittyvät asiat huomioidaan ja kaikilla tässä oppaassa kuvatuilla toimenpiteillä edistetään kyseisen osa-alueen ja samalla kyberturvallisuuden toteutumista.

Infrastruktuuri on perusta, jonka varaan yhteiskunnan ja organisaatioiden toiminta ja palvelut rakentuvat. Infrastruktuurin ajatellaan yleisesti koostuvan konkreettisista asioista kuten esimerkiksi rakennuksista ja tuotantolaitoksista, liikenneväylistä ja -välineistä sekä vesi-, viemäri- ja sähköverkoista. Infrastruktuuriin voidaan katsoa kuuluvan myös yhteiskunnan keskeiset palvelut kuten mm. ruokatuotanto, terveydenhuolto, kuljetuslogistiikka, juomavesi ja energiantuotanto, joita tuottavat julkiset ja yksityiset organisaatiot. Fyysistä infrastruktuuria on perinteisesti suojattu konkreettisin keinoin (esim. lukitukset, varalaitteet ja varmuusvarastot) konkreettisia uhkia vastaan (mm. sään ääri-ilmiöt, vahingot ja onnettomuudet tai sotatila).

Nykyaikaisen tietoyhteiskunnan kehittyminen ja digitalisaatio tuottavat jatkuvasti digitaalisen toimintaympäristön palveluja, jotka muuttavat toimintatapojamme. Päivittäiset raha-asiat hoidetaan verkkopankissa, sanomalehdet luetaan älylaitteilta, sähkömittaria ei käy kukaan lukemassa ja tapaaminen toisella paikkakunnalla (tai toisessa maanosassa) voidaan toteuttaa etäkokouksena ilman matkustamista. Etätyöstä kotona on tullut pysyvä osa arkeamme. Digitaaliset palvelut sijoittuvat digitaaliseen toimintaympäristöön, jonka keskeisiä kokonaisuuksia ovat tietoverkot (mm. kansalliset tietoliikenneverkot ja Internet), tietotekniset järjestelmät, kuten vaikkapa sähköiset kauppapaikat, yhteiskunnan sähköiset perusrekisterit tai pilvipalvelut sekä palvelujen käyttäjät. Digitaalista infrastruktuuria turvataan tässä oppaassa kuvattujen hallintajärjestelmien avulla toiminnan jatkuvuutta, tietoturvaa ja tietosuojaa uhkaavilta tekijöiltä, kuten haittaohjelmilta, tietojen väärinkäytöltä tai tietojärjestelmien häiriöiltä.

Digitaalinen toimintaympäristö eli kybertoimintaympäristö on tullut kiinteäksi osaksi yhteiskuntaa, toimintoja ja palveluita. Tehtaissa, voimalaitoksissa ja tuotantolaitoksissa on paljon ohjaus- ja valvontajärjestelmiä, joiden häiriöt voivat pahimmassa tapauksessa pysäyttää koko laitoksen toiminnan. Liikennevalojen ohjauksen lamautuminen voi johtaa suuressa kaupungissa mittavaan kaaokseen, mikä voi edelleen johtaa esimerkiksi toimitusten viivästymiseen tai kasvaviin onnettomuuslukuihin. Tietoverkkoihin kytketyt prosessien ohjausjärjestelmät, kuluttajalaitteet (esim. web-kamerat, muut älykotilaitteet, jääkaapit tai lämpöpumput) tai sensorit voivat olla vihamielisen tai haitallisen toiminnan kohteina, jonka tavoitteena on niiden kautta häiritä tai vahingoittaa tietojärjestelmiä. Toisaalta kyberhyökkäysten tukena saatetaan käyttää esimerkiksi kuluttajien tietoturvattomien IoT-laitteiden verkkoja hyökkäyksen vahvistamiseksi.

Kyberturvallisuutta voidaan tarkastella merkittävästi tietoturvallisuutta laajempana kokonaisuutena. Kyberturvallisuudesta puhuttaessa ei rajoituta tarkastelemaan pelkästään tietoteknisiä järjestelmiä ja niiden hallintaa, vaan arvioidaan myös niiden muodostamia verkostoja ja näissä verkostoissa esiintyvien häiriöiden vaikutuksia yhteiskunnan rakenteisiin (mm. päätöksenteko, valtion suvereniteetti) tai infrastruktuuriin

(esim. sähköntuotanto tai terveydenhuolto) myös globaalilla tasolla. Kyberturvallisuuden uhkakuvissa mainitaan yleisesti esimerkiksi kybersodankäynnistä, kybervakoilusta tai kyberterrorismista.

Kybersotaa ei käydä asein ja ammuksin, vaikka päämääränä voikin olla valtion toiminnan lamauttaminen. Kybervakoilija ei murtaudu kohteeseensa voimapihtien avulla, vaan tunkeutuu tietojärjestelmiin verkon kautta ja varastaa tietoa. Kyberterroristi ei räjäytä pommeja tai ota panttivankeja, vaan hyödyntää kriittisten ohjausjärjestelmien heikkouksia levittääkseen haittaohjelmia, joilla lamautetaan esimerkiksi voimalaitoksen toiminta tai sähkönjakelu. Kyberturvallisuutta uhkaaviin tekijöihin kuuluvat myös luonnonilmiöt. Myrskyt ja tulvat voivat vaurioittaa niin sähkö- kuin tietoliikennekaapeleita. Koko digitaalinen yhteiskunta on pitkälti riippuvainen toimivasta tietoliikenneinfrastruktuurista, joka puolestaan tarvitsee toimiakseen varmistettua sähkön syöttöä. Laajamittaiset tietoliikennehäiriöt voivat estää tunnistautumispalvelujen käytön, ruuhkauttaa hätäkeskuslaitosten järjestelmiä tai haitata tiedonvälitystä.

Kyberhyökkäyksiin liitetään usein joukkoviestimien tai sosiaalisen median kanavien kautta tehtävää informaatiovaikuttamista (valeuutiset tai -videot, tahallinen väärän tiedon levittäminen, provosointi eli ns. ”trollaus”, henkilöiden maalittaminen tai vaalivaikuttaminen). Siinä missä tietotekniikan alkuaikojen haittaohjelmat olivat käyttäjiä haittaavaa vandalismia, on erilaisten kyberhyökkäysten takana nykyään usein taloudellisen edun tavoittelu tai yhteiskuntajärjestyksen horjuttaminen, ja toimijoina voivat olla yksittäiset henkilöt, ns. haktivistit, yhä useammin tietoverkkorikollisliigat tai valtiolliset toimijat, tai heidän palkkaamat alihankkijat (ns. APT-ryhmittymät).

Mikä siis on kyberturvallisuuden rooli digitaalisen turvallisuuden viitekehyksessä, joka on esitelty tämän oppaan alussa? Kuten tässä oppaassa on todettu, käytetään tietoturvallisuutta ja kyberturvallisuutta joskus toistensa synonyymeinä. Koska digitaalinen turvallisuus koostuu viidestä osa-alueesta, ne sisältävät samalla myös fyysisen toimintaympäristön turvallisuuden varmistamista. Kehittämällä riskienhallintaa, toiminnan jatkuvuutta ja varautumista, tietoturvaa ja tietosuojaa kehitetään ja edistetään samalla kyberturvallisuutta, sekä organisaation että samalla koko yhteiskunnan tasolla.

Yhteenvetona voidaan todeta, että tietoyhteiskunnan häiriöttömän toiminnan elinehto on, että digitaalisten tuotteiden ja palvelujen turvallisuus ja toiminnan jatkuvuus on varmistettu paikallisesti. Lisäksi johtamisen, osaamisen ja varautumisen yhteisellä kehittämisellä huolehditaan yhteiskunnan rakenteiden ja infrastruktuurin toimintavarmuudesta niin kansallisesti kuin kansainvälisessä yhteistyössä.

Lisätietoja: Kyberturvallisuusstrategia 2019, Kansallinen riskiarvio 2018, Kyberturvallisuuskeskuksen raportti automaatiojärjestelmistä 2019, Valtioneuvoston periaatepäätös julkisen hallinnon digitaalisesta turvallisuudesta (VM/2020/47), ISO/IEC 27032, NIS-direktiivi (1148/2016), EU:n kyberturvallisuusstrategia (2020), Digitaalisen turvallisuuden kansainvälinen vertailu 2020.

Liite 1 Riskienhallinnan kehittäminen

VAHTI-ohje riskienhallintaan 22/2017

https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-222017-ohje-riskienhallintaan

Liite 2 Toiminnan jatkuvuuden kehittäminen

Toiminnan jatkuvuuden hallinta VAHTI 2/2016

https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-22016-toiminnan-jatkuvuuden-hallinta